3. COMPONENT FAILURE AND BOUNDARY DEFINITIONS

3.1 Failure Definitions

While the terms “faults” and “failures” are casually used interchangeably, in the context of fault tree analysis, these terms have more distinct meanings. Thus, for data analysis, it is necessary for one to understand the distinctions. Generally speaking, all failures are faults, but not all faults are failures. To put it another way, failures comprise a subset of the larger set of faults. For probabilistic risk assessment (PRA) purposes, failures are regarded as basic (and undesired) events which render a component, subsystem, or system incapable of performing its intended function; which represents a basic fault tree input that is not analyzed further; and for which numerical estimates must be supplied if quantification is to be performed. Faults, on the other hand, are higher order events (representing the occurrence or existence of an undesired state of a component or set of components) which are analyzed further, and ultimately resolved into their constituent failures (Breeding, Leahy, and Young 1985; ANS and IEEE 1983; and Vesely, et al. 1981).

The failures modeled in PRA can have many causes or mechanisms. For example, failure of an motor-operated valve (MOV) to open on demand can occur due to physical problems with the valve (stem failure, disc separation, etc.), problems with the motor operator (motor failure, control circuit failure, breaker failure, etc.), or due to loss of motive or control power. In addition, the MOV may be unavailable due to test or maintenance on its constituent parts. As such, each failure (i.e., basic event) is the sum of the contributions from each piece-part included in the component boundary. Thus, it is critical to define what the component boundary is in order to get the right data.

3.2 Component Boundary Definitions

In order to collect failure data for components, it is necessary to define component boundaries by specifying the scope of each item to be considered as a single entity. The PRA model and the data collection should be coordinated so that the boundaries of the components are defined identically. For example, all pieces of a MOV are typically considered to be part of a single “component” when collecting reliability data even though the valve consists of various piece parts (e.g., electric motor, gearbox, limit switches, torque switches, reversing contacts and coils, stem, disc, valve body, etc.) that may be separately identified in the plant maintenance records. PRAs typically do not model failures of every switch, relay, or contact in a control circuit of a pump because that type of detail is difficult to obtain from the plant data. Instead, failures of these components are typically included with actual failures of the pump to establish a pump failure rate.

If generic data sources are used, it becomes the responsibility of the analyst to ensure that the component boundary definitions used in the generic data source are compatible with the boundary definitions used by the PRA being performed.

Some typical examples of component boundaries are shown in Table 3.l. The boundaries of a component should include all components specific to the component. However, the component boundary should not include piece-parts that are shared with other components modeled in the PRA. For example, emergency-actuated valves should include the valve control circuit. However, the components needed to generate an actuation signal that initiates multiple components modeled in the PRA should not be included as part of that specific valve boundary. Similarly, a diesel generator boundary will typically include the fuel day tank but the fuel oil transfer pumps are not included since they are required for operation of all the plant’s diesel generators.

3.3 Failure Severity

The raw data for a specific component will contain events some of which will not be relevant to the component failure modes being analyzed. These events can be screened from further analysis. Some of the events will be component failures that should be included in the data assessment. The type of component failures will determine how they are

Table 3.1 Examples of component boundaries.

Component	Component boundary
Diesel Generators	The diesel generator boundary includes the generator body, generator actuator, lubrication system (local), fuel system (local), cooling components (local), startup air system, exhaust and combustion air system, individual diesel generator control system, circuit breaker for supply to safeguard buses and their associated local control circuit (coil, auxiliary contacts, wiring and control circuit contacts) with the exception of all the contacts and relays which interact with other electrical or control systems.
Motor Pumps	The pump boundary includes the pump body, motor/actuator, lubrication system cooling components of the pump seals, the voltage supply breaker, and it's associated local control circuit (coil, auxiliary contacts, wiring and control circuit contacts).
Turbine-Driven Pumps	The turbine-driven pump boundary includes the pump body, turbine/actuator, lubrication system (including pump), extractions, turbopump seal, cooling components, and local turbine control system (speed).
Motor-Operated Valves	The valve boundary inc1udes the valve body, motor/actuator, the voltage supply breaker and it's associated local open/close circuit (open/close switches, auxiliary and switch contacts, and wiring and switch energization contacts).
Air-Operated Valves	The valve boundary includes the valve body, the air operator, associated solenoid-operated valve, the power supply breaker or fuse for the solenoid valve, and its' associated control circuit (open/close switches and local auxiliary and switch contacts).
Fans	The fan boundary includes the fan, the voltage supply breaker, and its' associated control circuit (open/close switches and local auxiliary and switch contacts).
Batteries	The battery component boundary typically just includes the battery. Battery chargers are modeled as separate components.
Bus Circuit Breakers	A bus circuit breaker boundary includes the breaker and it's associated control circuit (open/close switches and local auxiliary and switch contacts)

classified and subsequently used to generate the required component failure data.

Component malfunction events are commonly classified into one of the following three event severity categories:

1. catastrophic failures
2. degraded failures
3. incipient failures

A **catastrophic (complete) failure** is one that prevents the component from performing its mission as defined in the PRA (Whitehead 1993). Catastrophic failures require some kind of repair or replacement action on the component in order to restore the component to operability. For example, a valve that fails to open due to a valve operator mechanical failure is a catastrophic failure.

A **degraded failure** is such that a component can perform its mission, but at less than the optimum performance level (Whitehead 1993). An **incipient failure** is such that there is no significant degradation in performance but there are indications of a developing fault (Whitehead 1993). The difference between the two is generally a matter of severity. For example, an event involving pump shaft vibration indicates possible damage to the pump bearings. Severe vibration may be considered as degraded failure if the pump produces less than maximum flow. Shaft seizure or other failures could occur within a few hours if the pump remains running and thus would likely be removed from operation for corrective maintenance. In contrast, minor vibration may not result in degraded flow. This would thus be an incipient failure. The significance of this event is that it also could result in removal of the pump from operation for inspection, lubrication, or some other corrective action. Information about the types of repairs made, the parts replaced, and the urgency of the repairs often provides important insight about the severity of these two types of component failures.

Although both degraded and incipient failures will typically lead to a corrective action, the corrective action may or may not make the component unavailable to perform its function. For example, maintenance on the operator of a valve that is normally open will not lead to the unavailability of the valve if is required to be open for system operation. This illustrates the importance of ascertaining from event records the modes of a component operation that a corrective action would prevent.

Sometimes the event information is so unclear and incomplete that a definite classification of the severity of a component malfunction event is not possible. For example, Mosleh (1985) cites one maintenance work request issued at a nuclear power plant that described the problem as follows: “Check valve RHR-V-1A is leaking badly.” The maintenance foreman’s description of the corrective action read: “Fixed it, not leaking anymore!” No further information was available. From the description given, one cannot say for sure whether the leak was internal or external, or whether it was large enough to result in functional failure of the check valve.

Unfortunately, the above example is not uncommon. Descriptions of the malfunctions and repairs are often very brief. The data analyst, then, is faced with the difficult task of deciding whether to call a malfunction a failure or not. The inability to distinguish between severity levels of failures is particularly important as the difference between the probabilities of catastrophic and degraded modes of failures can be significant. Therefore, in the absence of sufficient information, the conservative assumption should be made that all such events be recorded as catastrophic failures. Unfortunately, conservative categorization of uncertain events can lead to significantly higher failure rates.

Ultimately, the definition of failure from the system analysis decides the classification of the data. Thus, the failure of a component must match the definition of the failure as described in the PRA model. A component must fail to perform its function as defined in the model. For example, a relief valve that opens at 1,115 psig instead of the required 1,110 psig is not failed, although it may be described as failed by the governing technical specifications, and a pump that delivers 645 gpm instead of the required 700 gpm is not failed if 645 gpm is sufficient for the function that it is required to perform.