

## 4.9 SPECIAL TOPICS

### 4.9.1 Independence Evaluation

Many owner/operators mandate independence and separation between protection layers, because it is the simplest approach to implement and maintain. It follows a defense-in-depth strategy to reduce the potential that a systematic error can disable more than one protection layer.

The owner/operator should document internal practices to ensure a consistent approach for assessing and achieving independence. The approach should be clear and unambiguous, so everyone assigned responsibility for the IPS operation can easily recognize the IPS from other systems.

Practices should be established that are easy to implement, rely on common sense, and are simple to verify. For example, internal practice may allocate a particular controller in an overall system for IPFs and require that this particular controller be managed under stricter requirements than the overall system. However, this segregation relies on personnel discipline, so training and administrative controls are more important. Personnel must understand the reason for and importance of the dedicated controller. Any deviations from approved practices should require justification and approval prior to implementation.

Most hazard and risk analysis assume the layers are independent. Simple qualitative and semi-quantitative analysis may not be sufficient to evaluate the residual risk if the layers are not independent. This is particularly true if the IPF and initiating cause are in the same layer. In this latter case, the hazard rate for the overall system should be determined and compared to requirements.

The decision to combine layers should consider many factors including:

- Hazard rate claim limit when random failures and systematic errors are considered,
- Restrictions or requirements related to the protection layer defined by applicable good engineering practice,
- The equipment failure rate based on the operating environment,
- Restrictions identified during user approval process, and
- Required fault tolerance against dangerous failure to achieve claimed hazard rate.

When other layers are combined with the IPS, the associated systems must be managed under the IPS management system. This means that any shared components including hardware and software must be traceable to information, documents and procedures, which demonstrate that the design, maintenance, inspection, testing, and operation practices are sufficient to meet the IPS requirements. Further, when the IPF and initiating cause are allocated to the same

layer, the IPF may be operating in a continuous mode. Continuous mode systems have special design and operating basis requirements.

#### **4.9.2 Continuous and Demand Mode Operation**

IPF operate in one of two modes of operation: continuous or demand. The mode of operation impacts the fault detection and response strategy. Some IPFs are designed to operate in demand mode, but operate very frequently due to the process demand rate. Some literature refers to these IPFs as operating in a “high demand mode.” However, rather than being another distinct operating mode, the frequency of the IPF operation is typically indicative of either excessive control layer failures or a misclassified control function. Often, the IPF is acting as a control function rather than a protective function under certain operating conditions or modes.

High demand mode IPF should be identified and means should be implemented to reduce the demand rate. Chapter 6.10 of this guidelines book discusses the monitoring and tracking of process demands so that their frequency can be minimized. For example, a high tank level IPF shutdown of a pump may be specified to reduce the risk of the operator failing to stop the pump at the specified control set point. In practice, the operator may be allowing the IPF to trip the pump due to other distractions or tasks. By recording and investigating the pump trips, the procedure deviation can be identified and its root causes can be assessed and corrected.

A continuous mode system is one whose dangerous failure leads to a hazardous event without further failure. This operational mode is best exemplified by the inherently safer and control layers. These layers are continuously active and when compromised, tend to be initiating causes for hazardous events.

If IPS equipment failure can initiate the hazardous event and cause the IPF to fail to operate, the shared IPS equipment is operating in a continuous mode. The design and user approval process should specify how dangerous undetected, systematic, and common cause failures are reduced to a sufficiently low likelihood. When dangerous failures are detected in continuous mode equipment, the affected equipment must be taken to the specified safe state.

The vast majority of IPFs operate in the demand mode, where the IPF only acts when another layer has failed to maintain the process within the normal operating range. For example, when a BPCS