

UNDERSTANDING FAILURE

Control systems are designed to keep the process within specified process parameters considered acceptable for normal and safe operation. When the process exceeds the normal operating limit, it may propagate into a hazardous event with potential consequence to human life, the environment, and plant assets. The risk assessment phase identifies hazardous events that pose significant consequences and defines the means used to prevent their occurrence. The identified risk may be reduced using an instrumented system implemented in the preventive layer, such as a protective instrumented function (PIF).

Example--Loss of vessel level

Consider the case where a loss of vessel level allows high pressure gas to pass to downstream equipment that is not rated for the gas pressure. Assume a PIF is specified to reduce the risk of this event. The PIF detects low level and responds by closing an outlet block valve to prevent the gas blow-by.

Three redundant level transmitters are used to detect a low level condition. Other independent level devices are used by the basic process control system to monitor and control the vessel level. When any two of the three (2oo3) PIF level transmitters detect low level, the PIF closes the outlet block valve. The PIF can still work if one level transmitter fails dangerously; however, if two transmitters fail dangerously, the PIF will fail to close the valve, allowing the level to be lost in the vessel with potential catastrophic consequences.

The dangerous failure of two level transmitters may be unlikely if the devices are designed, installed, operated, inspected, and maintained according to the requirements of the design and operating basis. When these requirements are not met, multiple simultaneous failures may occur. This is known as a common cause failure.

During a hazard and risk analysis, risk reduction is allocated to protective functions used to reduce the process risk below the owner/operator risk criteria. When the protective function is implemented as a protective instrumented function (PIF), the allocated risk reduction is related to its integrity level (IL). The risk reduction and IL establish a benchmark for the design and management practices used throughout the PIF life. This benchmark serves two purposes: 1) it defines the minimum performance that should be achieved with regard to random failures; and 2) it determines the rigor of the protective management system required to reduce the potential for systematic errors.

The required risk reduction establishes a minimum level of management system rigor that must be provided to reduce the potential for systematic errors to a sufficiently low probability. Systematic errors are caused, or indirectly induced, by human error or unforeseeable complex process conditions. Systematic failures are not random events and must be addressed by the management system, using

quality management processes to minimize systemic error. Most systematic errors are not easily included in the verification calculation.

The risk reduction can be used to establish a benchmark for the design and management practices used for any instrumented protective function (IPF). These requirements can be met with an IPF that is unreliable d