

3.3 BASIC WORK PROCESS

The hazard and risk analysis should be started as early as feasible within the project lifecycle to minimize the cost of implementation. When projects are in scoping and front-end loading phases, the cost of making changes to the design or to the protection layers is relatively low, and numerous options for risk reduction can be evaluated on a cost/benefit basis. As the project proceeds toward full implementation, the cost associated with making changes increases dramatically and the options for change decrease sharply. Consequently, it is important to begin hazard identification early in a project life to identify options that lower the cost of safe operation.

During process design, the risk associated with potential hazardous events should be reduced, when practical, through inherently safer design. The process designer should consider inherently safer design strategies, such as minimize, substitute, moderate, and simplify, to reduce the risk or to eliminate the potential event. These design strategies are best employed during the earliest stages of process design, where the opportunities for process modification are greatest and the cost of design change is least. However, inherently safer design can be employed during any lifecycle stage.

Inherently safer design provides substantial benefits by reducing long-term operational and maintenance cost. Further, if the process is inherently safer, it is generally more reliable, because the process is more tolerant to operational upsets. Refer to *Inherently safer chemical processes: A lifecycle approach* (CCPS/AIChE 1996) for more information. Inherently safer design has economic and engineering limitations. For example, it is sometimes necessary to use a specific process chemistry or technology to produce a product.

If the inherent risk is higher than the specified risk criteria, protection layers are implemented to control the risk in accordance with good engineering practice. *Guidelines for Safe Automation of Chemical Processes* (CCPS/AIChE 1993) introduced the concept that protection layers can be used to avoid the occurrence of or to reduce the effect of an identified hazardous event. When significant hazards cannot be avoided by inherently safer design, protection layers are used to reduce the frequency of the event. The identification, design and management of protection layers is, consequently, very important.

The protection layers (Figure 3.2) are as follows:

- Inherently safer design--reduction or elimination of hazardous events through effective use of process technology, design methods, and/or operational techniques;
- Control--standard operating procedures, basic process control systems, and process alarms--this layer is generally focused on maintaining the process within the normal operating limits;

- Supervisory--protective alarms, operator monitoring and supervision, and process actions--this layer is designed to achieve or maintain a safe state of the process to reduce the frequency of the hazardous event;
- Preventive--protective instrumented systems, such as safety instrumented systems, environmental protective systems and asset protective systems--this layer is designed to achieve or maintain a safe state of the process to reduce the frequency of the hazardous event;
- Mitigative--mechanical equipment, such as pressure relief devices, and instrumented systems, such as life safety systems, high integrity protective systems, and reactor kill systems--this layer is designed to reduce the frequency and/or consequence severity of the hazardous event;
- Barriers--dikes, berms, bunds, and explosion barriers--this layer minimizes the consequence severity due to its physical design;
- Limitation--fire & gas, fire protection, water/steam curtain, deluge, emergency dump, and emergency shutdown systems--this layer acts to reduce the consequence severity of the hazardous event; and
- Response--emergency response systems--this layer notifies personnel and/or the community to shelter-in-place or to evacuate to safe zones and musters emergency response personnel.

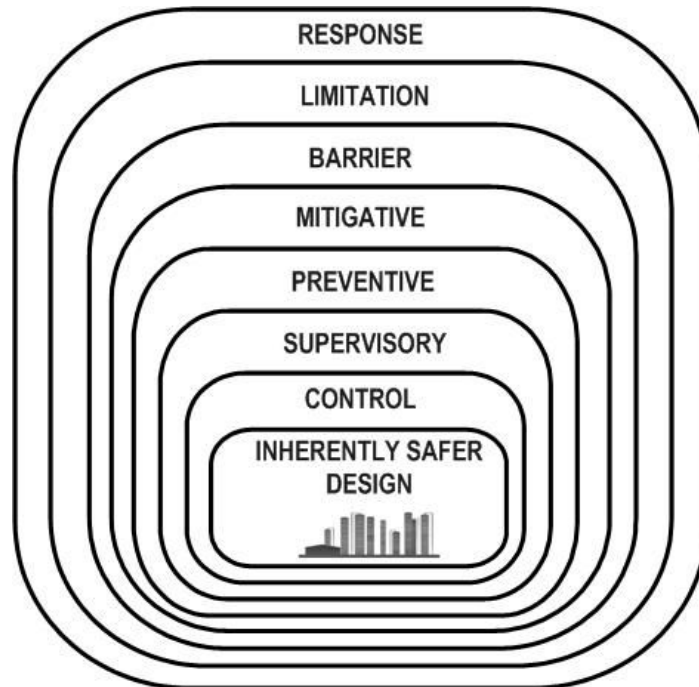


Figure 3.2. Protection Layers.

Some protection layers are more effective than others in reducing the risk. A protection layer may only partially mitigate the event, resulting in an undesirable, though reduced severity, event. Some layers are not sufficiently effective in detecting and responding to the particular types of events. Other layers can achieve predictable risk reduction based on proven design and management practices.

Protection layers are known as IPLs when they are designed and managed to achieve the following seven core attributes (see Appendix C):

- Independence--the performance of a protection layer is not affected by the initiating cause of a hazardous event or by the failure of other protection layers;
- Functionality--the required operation of the protection layer in response to a hazardous event;
- Integrity--related to the risk reduction that can rea