Implementing Control

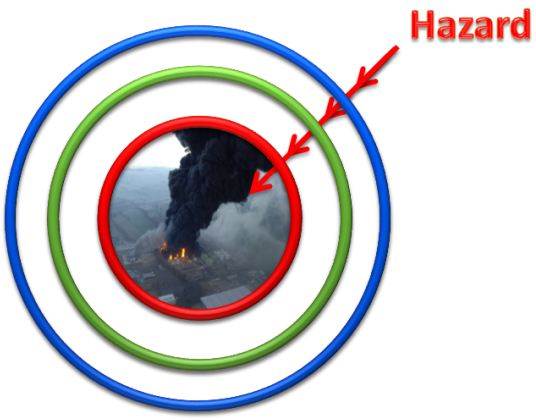
Implementing control should focus on determining control through the elements of Prevention and Mitigation of the major hazards using the risk profile as a guide to the strength and depth of barriers required.

These barriers will need to be multi-layered addressing technical, managerial and procedural arrangements, through the three core areas of Plant, Process and People.

Barrier Thinking

Layers of Protection

Measures designed to prevent and control potential major accidents that if applied consistently will mitigate the effect



Aims of Layers of Protection

Inherent Safety

First principle – Design it out!

If not look at four key elements to:

Minimise | Substitute | Moderate | Simplify

Prevention

Prevent initiation of a sequence of events that could lead to major accidents

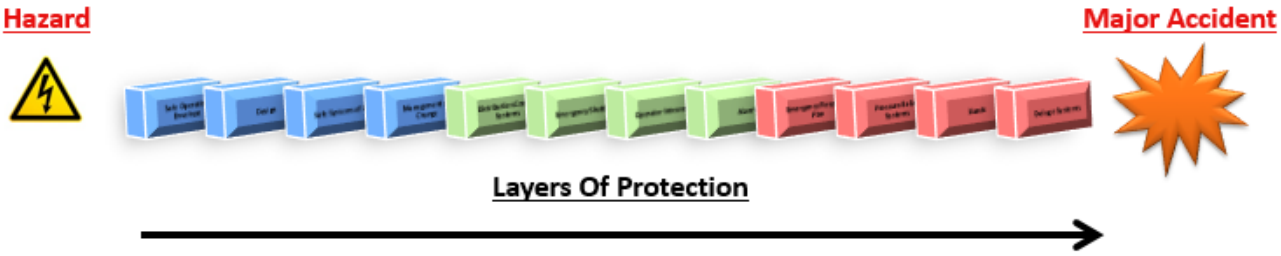
Control

Stop a hazardous event sequence progressing further

Mitigation

Reduce the consequences once they have occurred

Protective Layers



The basic structure of Layers of Protection covers three main areas:

1. **Prevent**– These provide safety through the design and development of Basic Process Control Systems (BPCS), such as operational personnel, procedures, and engineering aspects all working in harmony to achieve the desired outcome.

2. **Control** – This focuses on the safe close down of a process should it begin to operate outside of key parameters and can be achieved through:

   a. **Operator intervention** – This could come from warning systems, level indicators or alarms but usually requires direct intervention by the operator to bring the system back under control – i.e. Operator hears high level alarm siren and stops the vessel discharging

   b. **Independent Emergency Shutdown** – Provided through a Safety Instrumented System (SIS) which is independent of the main process control system with a role that is focused on safety – i.e. Independent high level alarm linked to a ROSOV (Remotely Operated Shut-off Valve)

3. **Mitigation** – This deals with reducing the impact of the event covering three key areas:

   a. **Active Protection** – This deals with any part of the system that will exert influence or change on the event, for example relief valves or rupture discs designed to provide a relief point that will prevent catastrophic tank failure through over pressure

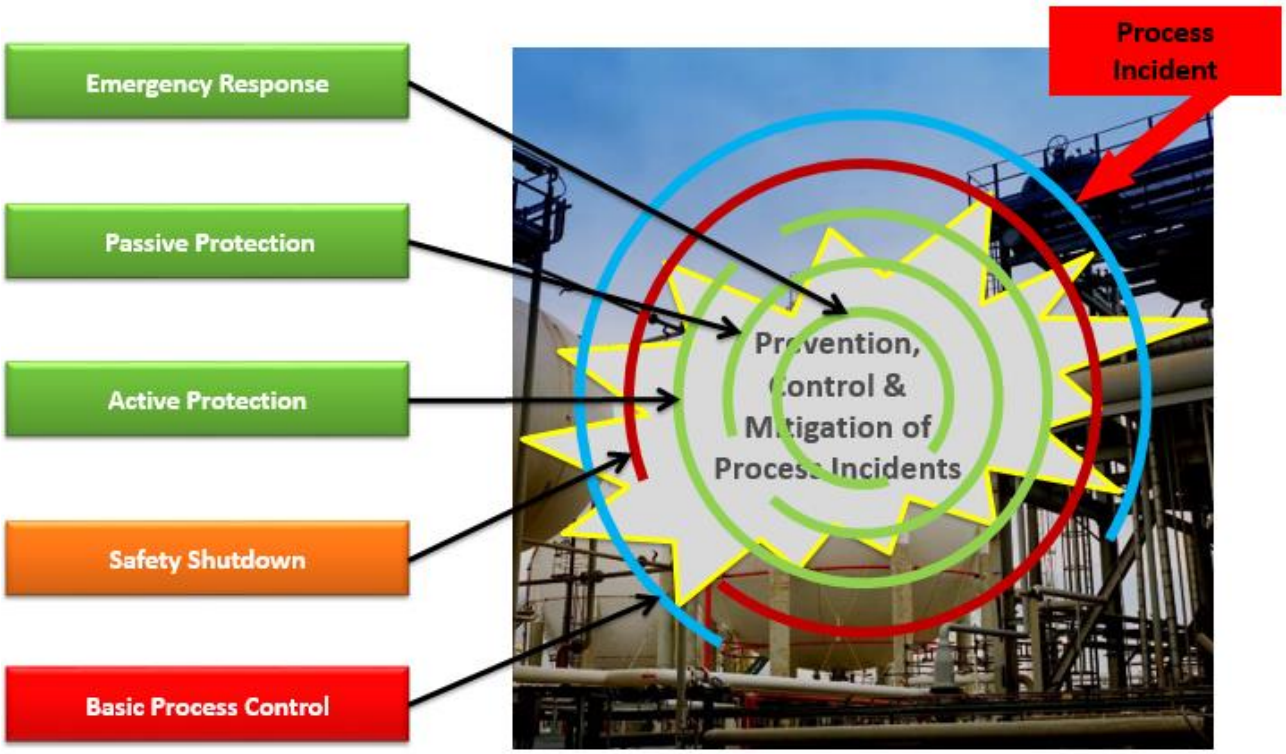
   b. **Passive Protection** – This can be seen as containment within the site boundary, such as impermeable bunds, dikes, drainage and interceptors

   c. **Emergency Response** – Should an incident occur, this area deals with minimising the ongoing damage, it will include initial response, roles, responsibilities, offsite response, and emergency services. The response should be prioritised on the principle of PEAR:

The safety of any facility is measured by how these differing aspects work together; it is key that systems are in place to review these ensuring that the close integration is maintained.

Protecting Processes

These layers of protection wrap themselves around processes to keep the hazard potential at bay, through control systems, preventing escalation or mitigating the effect should an incident occur.



But it is recognised that systems, processes, and procedures have the potential to fail, be it human error, equipment malfunction, procedural failure or other unforeseen aspect. Each layer should provide a stop point should the previous key controlling aspect fail.

If these protection elements are inadequate, then incidents can quickly escalate into major process incidents!

Types of Barriers

Layers are focused on prevention, control and mitigation of the affect, through:				
Plant	Process	People		
Example barriers include:				
Pressure Relief	Readouts	Deluge	Trips	Emergency Shutdown
Built to design standard	Gauges	Training	Alarms	Checklists
ROSOV	Bunds	Communication	Management of Change	
Blast walls	Drains	Operating Envelope	Emergency Response	
Ensure that safety critical equipment is identified and:	**Appropriate testing, inspection and maintenance regimes to maintain design integrity**	**ensure that safety not compromised during periods of testing, inspection maintenance**		
Care must be taken that safety critical equipment is correctly reinstated (Buncefield high level switch!)				