# Operability in Process Design: Achieving Safe, Profitable, and Robust Process Operations

## Chapter 5: Safety

Chemical Safety Board Report No. 2005-04-I-Tx, BP Texas City Refinery Explosion, March 23, 2005

**Thomas Marlin**

**Safety release 2.6 on August 2014**



This material is provided to promote education in the general field of "process operability" via the Internet site www.pc-education.mcmaster.ca . It is one of the chapters of an integrated presentation of selected operability topics. The author would like to hear from readers on how they are using this material. In addition, he would appreciate suggestions for improvements and extensions. He can be contacted at marlint@mcmaster.ca .

**Acknowledgements**

- The Center for Chemical Plant Safety of the AIChE for the use of copyrighted tables
- Everyone who publishes via Creative Commons

Disclaimer

*While care has been taken in the preparation of the information contained in this chapter, the author cannot guarantee its accuracy or applicability for a specific application. Persons accessing and using this information do so at their own risk and indemnify the author from any and all injury or damage arising from such use.*

# Table of Contents

# Symbols


CONTROL ROOM BOARD MOUNTED INSTRUMENT


LOCAL BOARD MOUNTED INSTRUMENT

MEASURED VARIABLE:
L: LEVEL
P: PRESSURE
A: ANALYZER
F: FLOW
T: TEMPERATURE

FUNCTIONS:
I: INDICATOR
C: CONTROLLER
A: ALARM
(H =HIGH, L=LOW)

EXAMPLES:


PRESSURE RECORDER CONTROLLER: I.D. NUMBER 100, MOUNTED IN CENTRAL CONTROL ROOM.


TEMPERATURE ALARM: ACTIVATED AT HIGH TEMPERATURE.


LOCAL FLOW INDICATOR

VALVE

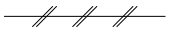
DIAPHRAGM VALVE: CONTROLLED BY AIR LINE

CHECK (ONE-WAY) VALVE


SOLENOID VALVE CONTROLLED BY ELECTRICAL SIGNAL

THREE-WAY VALVE

SPRING LOADED SAFETY VALVE

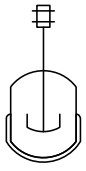


AIR LINE

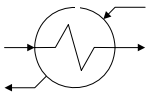


ELECTRICAL SIGNAL

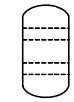

ELECTRICAL (CURRENT) TO PNEUMATIC SIGNAL CONVERTER



STIRRED TANK

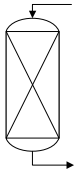


SHELL AND TUBE HEAT EXCHANGER

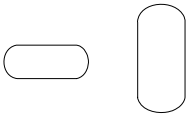


TRAYED COLUMN

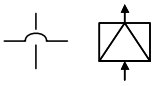
CENTRIFUGAL PUMP



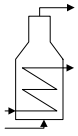
PACKED TOWER OR PROCESS VESSEL (SUCH AS A REACTOR).



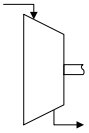
GENERIC TOWER OR PROCESS VESSEL (SUCH AS A REACTOR).



RUPTURE DISK, BURST DIAPHRAGM

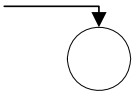


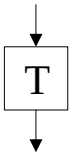
FIRED HEATER (FURNACE)



AXIAL COMPRESSOR


CENTRIFUGAL FAN

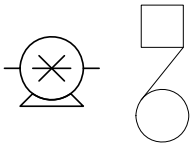

HEADER (STEAM OR CONDENSATE)



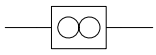
STEAM TRAP

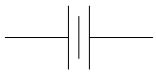
MOTOR

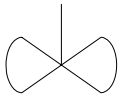

DRAIN TO SEWER

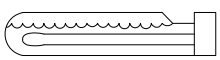

POSITIVE DISPLACEMENT PUMP


CONDENSER


TURBINE FLOW METER

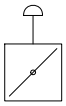

ORIFICE PLATE

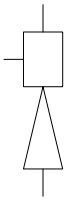

IMPELLER

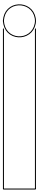

VAPORIZER OR REBOILER

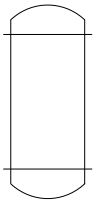

FILTER AND DRAIN

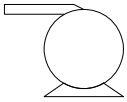

CYCLONE


DAMPER OR BUTTERFLY VALVE

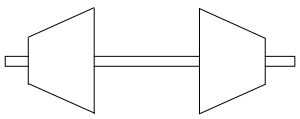

STEAM EJECTOR


FLARE STACK


SHELL AND TUBE HEAT EXCHANGER


FAN OR BLOWER


FAN


TURBINE USED TO PROVIDE WORK TO DRIVE COMPRESSOR

# Nomenclature

| | |
|---|---|
| AIChE | American Institute of Chemical Engineers |
| API | American Petroleum Institute |
| BPCS | Basic Process Control System |
| CCA | Cause-Consequence Analysis |
| CCPS | Center for Chemical Process Safety<br>American Institute of Chemical Engineers |
| CSTR | Continuous (flow) stirred tank reactor |
| DOE | US Department of Energy |
| ET (EVA) | Event Tree Analysis |
| F&EI | Dow's Fire and Explosion Index |
| $f^I_i$ | Frequency of initiating event for scenario i |
| $f^C_i$ | Frequency of consequence from event for scenario i |
| $f^{max}_i$ | Maximum acceptable frequency of occurrence of consequence for scenario i |
| F-N | Fatality- Number of fatalities per year |
| FMEA | Failure Modes and Criticality Analysis |
| FT (FTA) | Fault Tree Analysis |
| HAZOP | Hazard and Operability Study |
| HRA | Human Reliability Analysis |
| IPL | Independent Protection Layer |
| ISA | Instrumentation, Systems and Automation Society<br>(Formerly, Instrument Society of America) |
| LOPA | Layer of Protective Analysis |
| MTTF | Mean time to failure |
| P&ID | Piping and instrumentation drawing |
| PHA | Process Hazards Analysis |
| PFD | Used here: Probability of Failure on Demand<br>(Also used frequently in chemical engineering for Process Flow Diagram) |
| PID | Proportional-integral-derivative controller |
| SIS | Safety Instrumented System<br>(Safety interlock system, emergency shutdown system) |

| | |
|---|---|
| $\lambda^D$ | Failure frequency in dangerous state |
| $\lambda^S$ | Failure frequency in safe state |

# Chapter 5 Safety

## 5.0 To The Student

Safety is not a new topic for you because you have received instruction on laboratory safety starting with your chemistry and physics laboratory courses. In those courses, the emphasis is typically on the safe operation of the laboratory equipment. In addition to ensuring a safe learning environment, this training is useful to engineers, who are responsible for the safe operation of manufacturing equipment.

This chapter extends the safety topic to address designing safe industrial processes, which is essential because the process industries involve hazardous materials, e.g., acids and combustible materials, and process conditions, e.g., high pressures and temperatures. With responsible design and operation, the processes can be operated without harm; with careless or uninformed design and operation, hazards will occur and harm will inevitably occur to workers and/or people in the community.

As we will see, safety requires the application of engineering principles that you have learned in prior courses and new methods introduced in this chapter. As you study this material, please keep two thoughts in mind.

- First, every engineer is responsible for safety. You will manage the design, construction and operation of equipment and must ensure that your work contributes to safety. Also, you will participate in team reviews of designs and existing equipment and will apply your special expertise to identifying and eliminating potential sources of hazards.
- Second, you have the option of training to become a safety specialist. If you do, this chapter will provide a valuable introduction to the body or skills and knowledge you will require to set corporate safety standards and to lead team safety studies.

Safety is a vast topic that cannot be covered thoroughly in one chapter. An overview of the major safety topics is given in Figure 5.1. Also highlighted in the figure are the key topics for this chapter that were selected to provide instruction in the knowledge and skills that you will most likely apply in your career. Part I introduces the safety hierarchy, where you will use prior learning and new knowledge to master the method used at each layer of the hierarchy to prevent events from leading to hazards. Part II introduces systematic methods for identifying hazards and designing the safety hierarchy to achieve the desired safety performance.

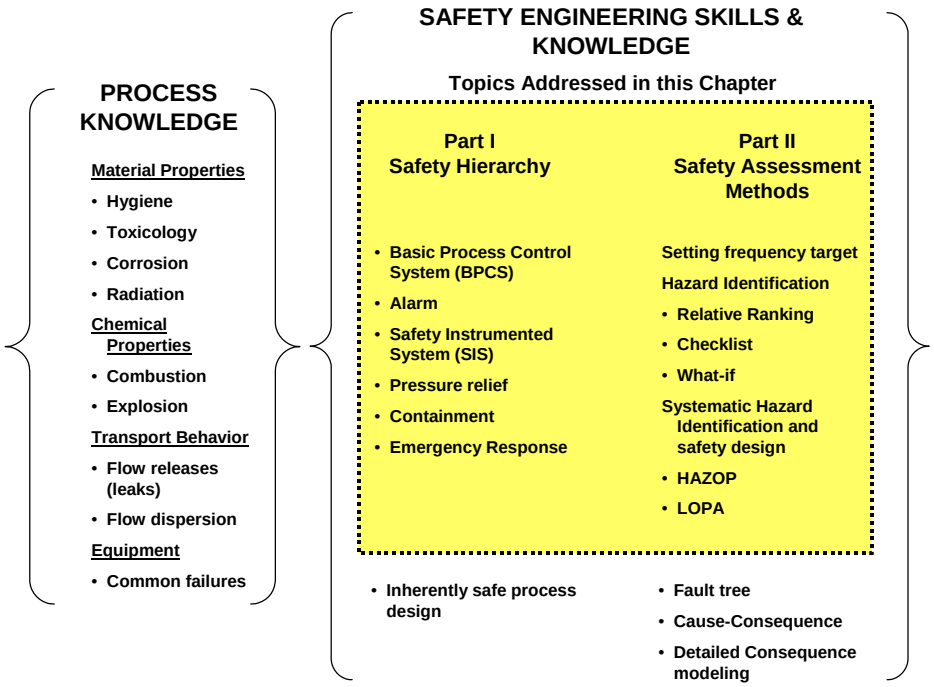



**Figure 5.1**. Overview of key safety topics with chapter contents highlighted.

The importance of safety is self-evident. To prepare yourself, you might want to quickly review one major industrial accident from the references provided at the end of the chapter to see how errors in design and operation of plants can lead to substantial harm to workers, the surrounding communities and the environment. You will see that major accidents have occurred in plants that have been operated for decades by international companies with extensive technical resources. From these examples, we can learn the dire consequences possible when safety principles are disregarded. So, let's get started preparing ourselves to practice engineering safely!

# Part I: The Safety Hierarchy

## 5.1 Introduction to the Safety Hierarchy

We will begin with the safety hierarchy shown in Figure 5.2. The hierarchical design has the following advantages.

- Since each layer is independent, a failure of one layer can be compensated by other layers in the hierarchy; therefore, the hierarchy has good reliability.
- A hierarchy provides some protection against human error, since if a person incapacitates or ignores one layer, subsequent layers may provide adequate protection.

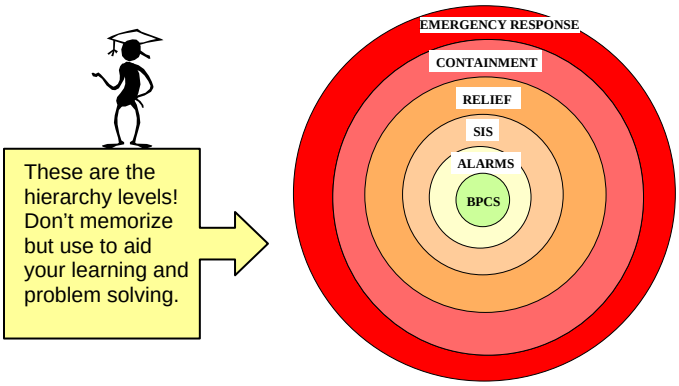



**Figure 5.2** "Onion diagram" of the safety hierarchy.

- Moderate responses are implemented in the lower layers, so that in many cases, no adverse effect on production and product quality occurs while safe operation is ensured. In response to infrequent large disturbances higher layers will implement strong actions, which in the extreme will involve automated shutdown of process units or the entire plant.
- The hierarchy integrates human actions with fully automated responses, and the hierarchy is easily understood by plant operating personnel.

As deviation from normal operation increases, higher layers in the safety hierarchy take action. The responses of the layers are shown in Figure 5.3 for a hypothetical scenario in which deviation from normal operation increases over time.

Each layer of the hierarchy represents a general approach that can be achieved by one of many designs. In Part I, the goal and technology for each layer will be explained, some typical designs will be introduced, and process examples will be presented.

## 5.2 Basic Process Control System (BPCS)

The lowest level of the safety hierarchy is process control, which you have learned in a prior course. Process control technology relies primarily on continual feedback control using reliable process sensors and computing elements implementing standard algorithms like the Proportional-integral-derivative (PID) controller, and automated control values. Process control contributes to safety by controlling key variables like pressure, temperature, ratios of flows to combustion processes, and so forth. In fact, guidelines for designing control systems begin with safety as the first objective (e.g., Marlin, 2000). The following variables should be controlled for safety.

- **Unstable** – Unstable process variables do not reach a steady state, even when all input variables are constant. The most common is liquid level in a tank with

outflow being pumped. Without feedback control, the liquid would overflow or run dry because the flows in and out would not be balanced.

- **Rapidly changing** – Some variables are stable, but could rapidly exceed their acceptable range of values. Common examples are pressures in closed vessels and temperatures in chemical reactors.

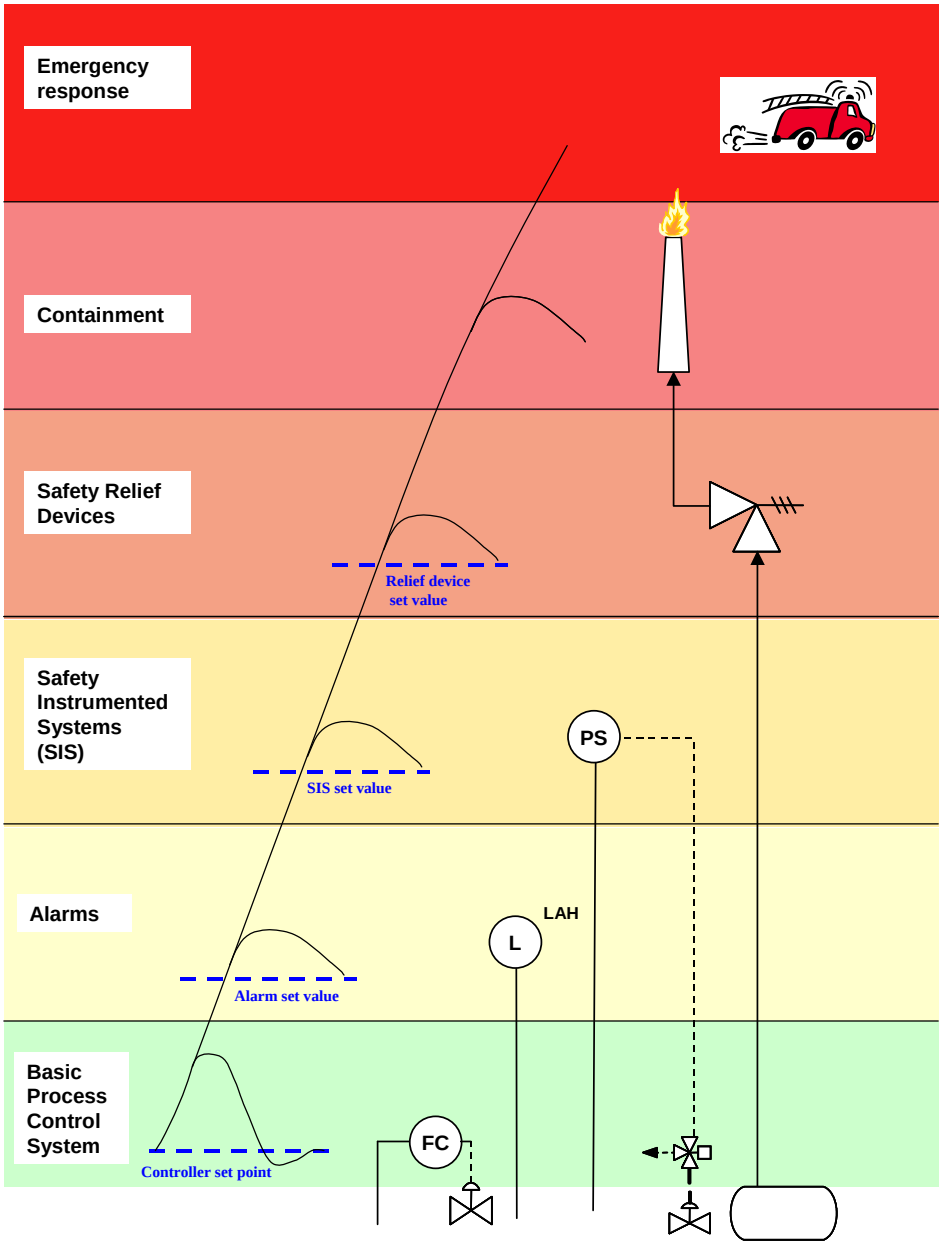



**Figure 5.3** Trend plot of the safety hierarchy showing when each layer takes action as the deviation from normal operation increases.

- **Defining equipment limitations** – Process equipment is designed to function over a specific range of conditions. Outside of the allowable range equipment does not function correctly and may be damaged. For example, a positive displacement pump will be damaged if an outlet valve stops the flow, and a compressor will be damaged by surge if the gas flow rate is too low. Also, most process equipment is limited to a range of conditions to operate properly; for example, a distillation tower tray provides proper contact for mass transfer over a limited range of the liquid and vapor flow rates.

Not all variables require automatic control. If a variable changes very slowly, observation and occasional action by a person is acceptable. Examples include liquid inventory in a very large tank and corrosion occurring over years. Let's look at a process example to see how process control contributes to safety.

**Example 5.1** All students have performed flash calculations in their thermodynamics class. The process in Figure 5.4 is used to effect a rough separation of components by differences in vapor pressure. It involves heating a multicomponent fluid stream, reducing the pressure, and allowing the vapor and liquid streams to separate in a drum. The figure includes a basic control system that is discussed in detail in Marlin (2000, Chapters 2 and 24). How do these controls contribute to safety and operability?

- ***PC-1 is a feedback controller that measures the pressure in the closed vessel and manipulates the vapor exit valve to achieve the desired pressure. This improves safety (preventing excessive pressure) and operability (maintaining a desired flash separation).***

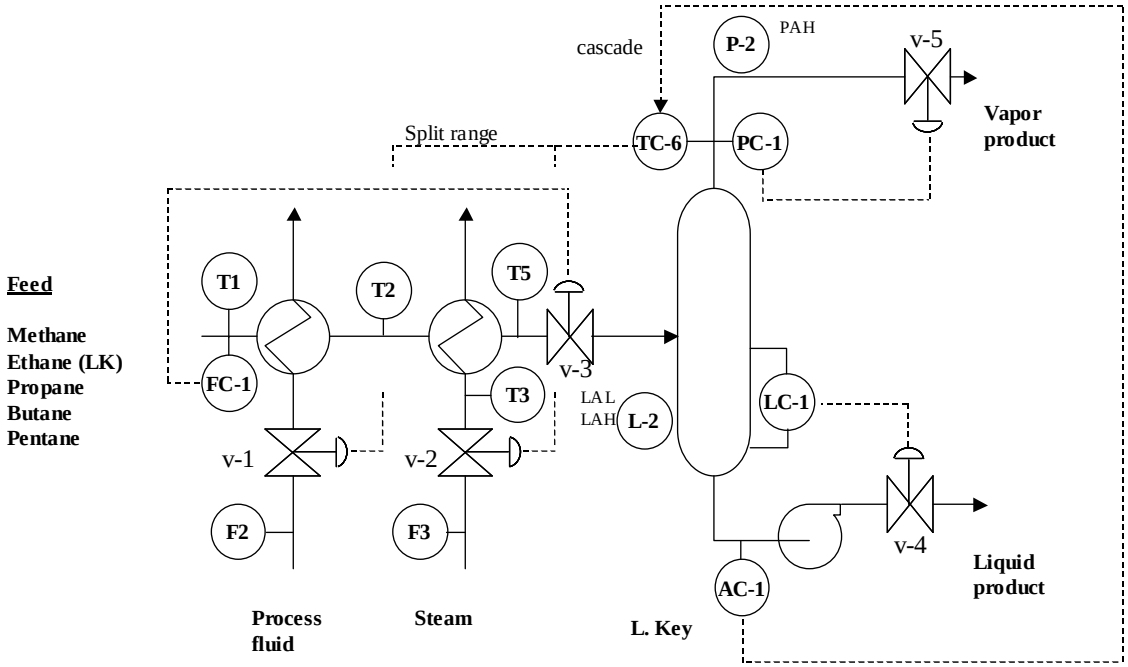



**Figure 5.4** Flash process with process control.

- ***LC-1 is a feedback controller that measures the liquid level in the vessel and adjusts the liquid exit valve to achieve the desired level. This will prevent (a) liquid exiting via the vapor line (which could be hazardous in some situations) and (b) the pump running without liquid (which could lead to equipment damage and a hazard).***

***Other controllers contribute to maintaining process variables within normal values and avoid major upsets that might lead to hazards.***

**While the controllers in Example 5.1 greatly improve process safety, they are only one of the layers of the hierarchy. Design of the flash process with only this control layer would be unacceptable.**

Now that we have an idea of the good contribution to safety made by process control, let's consider why we need additional layers in the hierarchy. What potential deficiencies exist at the process control layer? To answer this question, we will consider the elements in the feedback loop.

- **Sensor** – We should always take care to ensure that the sensor reports a value that is close to the actual process variable. Proper sensor technology and correct sensor location will ensure that appropriate accuracy and reproducibility can be achieved. However, sensors can experience faults, such as a thermocouple that has its circuit opened due to a break in the wire. If maintaining a process variable within limits is critical for safety, we may decide to install two sensors to protect against a sensor failure. We must also provide automatic control that selects the sensor with the "worst" value (e.g., the highest value if we want to prevent exceeding a high limit) for use by the controller (see Marlin, 2000, Chapter 22).
- **Signal transmission** – Currently, most signal transmission is through individual electrical wires, but wireless transmission is gaining acceptance. In any case, the transmission could be lost or corrupted, which could lead to improper actions by the controller.
- **Control calculation** – The hardware and software for digital controllers is highly reliable, but it could fail, resulting in no control action being made. Also, each feedback controller requires proper values for the "tuning constants" (gain, integral time, and derivative time), which if improper could lead to poor dynamic performance; too slow, too aggressive, or even unstable. (Since you worked diligently in your process control course, it is unlikely that you would make this mistake!)
- **Final control element** – The most common final element is the pneumatic control valve, which can fail due to loss of air pressure or can stick at a current position.
- **Process design capacity** - The combination of pump, pipe size, and valve size results in a maximum flow that can be achieved. If this flow is not sufficient to return the process to normal operation, the deviation from normal operation may

continue to increase until higher layers in the safety hierarchy will be called upon to take action.

- **People** – Automatic control is supervised by plant personnel, who are required to turn controllers on and off (automatic and manual). For example, when a sensor is periodically calibrated (to manual) and then returned to service (to automatic). The person could forget to return the controller to automatic.
- **Power for automation** – Electrical and pneumatic power are required for process control, and these systems are typically provided with redundancy through backup systems. However, they could fail.

This long list of possible faults should *not* be interpreted as an indication that process control is very unreliable. Faults occur very infrequently; however, we must consider the large number (100's to 1000's) of control loops in a plant and the potentially severe hazards resulting from one fault over many years of plant operation. Therefore, a strong foundation for safe operation is provided by basic process control, but many more layers of protection are required to achieve acceptable safety for industrial systems.

A process control system can be designed to react in a safe manner when a fault occurs in the final control element without degrading its performance under normal conditions. Two control valves are shown in Figure 5.5. Recall that the controller output adjusts the air pressure that acts to change the position of the valve stem and the valve plug; the position of the plug changes the resistance to flow. Let's consider the control valve fault in which a loss of air pressure occurs. When the loss of air pressure fault occurs, the force from the spring will determine whether the valve is fully closed or opened; the position with zero air pressure is called the "failure position". We can select either fully opened or fully closed. A third option, unchanged from current, is also possible, but not often selected.

**During the design, we define the failure position for every control valve to yield the safest process conditions.**

**Example 5.2** An engineer must define the failure position for each control valve in the flash process in Figure 5.4. What do you recommend?

***The failure position is its fully open or closed state after the air pressure to the actuator falls to atmospheric. This defined failure position is determined by the actuator and the valve seat design. A process engineer selects from these design from options provided by valve manufacturers.***

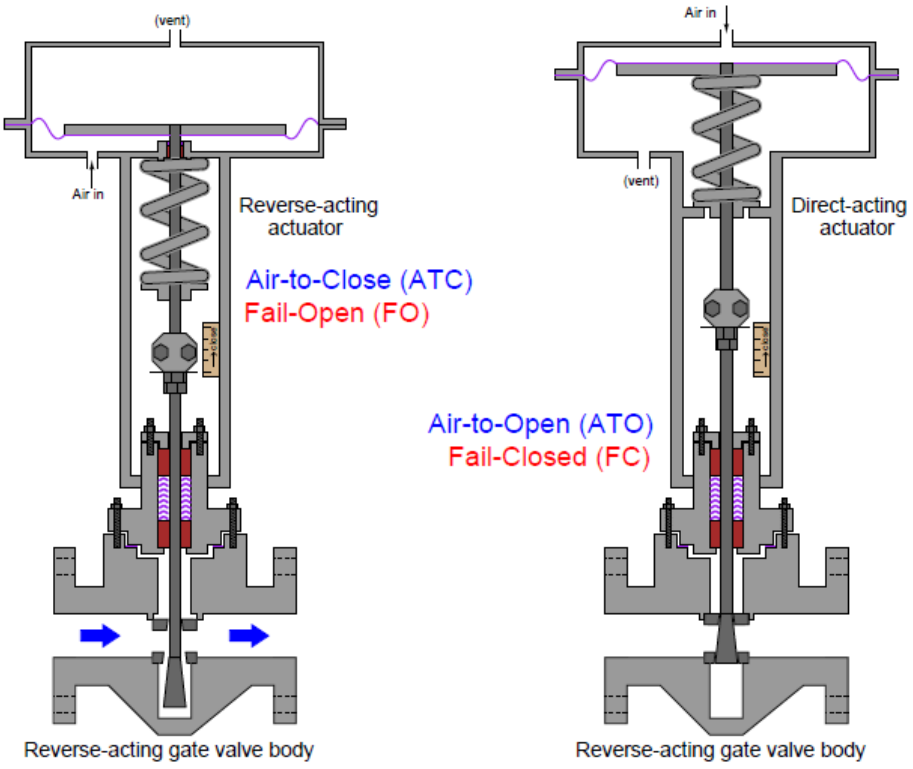



**Figure 5.5** Control valves with pneumatic actuators. The failure position depends on the actuator and the body design. Here, both fail open (fo) and fail closed (fc) designs are shown. Kuphalt (2012)

***In the example flash process, we select the following positions.***

- ***v-1 provides heat transfer to the system. It should be fail closed to reduce the build up of pressure.***
- ***v-2 provides heat transfer to the system. It should be fail closed to reduce the build up of pressure.***
- ***v-3 provides feed to the vessel. The proper failure position requires analysis of the entire process. When considering only the flash process, the safest is fail closed to prevent material entering the vessel.***
- ***v-4 provides an exit of liquid from the system. The proper failure position requires analysis of the entire process. When considering only the flash process, the safest is fail-open, to allow material to exit the vessel.***
- ***v-5 provides an exit of vapor from the system. The proper failure position requires analysis of the entire process. When considering only the flash process, the safest is fail-open, to allow material to exit the vessel.***

***These decisions can be documented on a P&I drawing by placing either "fo" (fail open) or "fc" (fail closed) by each control valve.***

In summary, basic process control provides continuous adjustment of final elements to maintain selected measurements near their set points. It responds well to most disturbances to the process, preventing the activation of higher layers in the safety hierarchy for nearly all (but not all) disturbances influencing the process. Generally, process control compensates for the effects of most disturbances, but it does not compensate for disturbances with very large magnitudes and naturally, for faults in the process control equipment itself.

## 5.3 Alarms

The next layer in the hierarchy is alarms, which are important because one person can be responsible for a large, complex plant section with hundreds of measurements. Ideally, this person monitors all of the variables simultaneously, which is not possible. An alarm is designed to alert the person to potential safety issues associated with a measurement.

An alarm requires a sensor and a calculation that compares the measured value to a predefined limit, and equipment to gain the attention of plant personnel. A typical alarm sequence is shown in Figure 5.6.

1. We start with the measurement within the acceptable range, i.e., below the upper limit. No annunciator or visual signal is active.
2. The measurement exceeds the limit. The annunciator sounds, and the light blinks.
3. A person acknowledges the alarm. The annunciator stops, and the light no longer blinks but stays lighted, indicating that the variable exceeds its limiting value.
4. The measurement returns within the acceptable region; the light is extinguished.

Other alarm sequences are possible; for example, an audible alarm could be sounded when the measurement returns to its acceptable range (CCPS, 1993). Also, small variations in the measurement value around the limiting value could cause frequent alarms; therefore, a deadband is often included in the sequence.

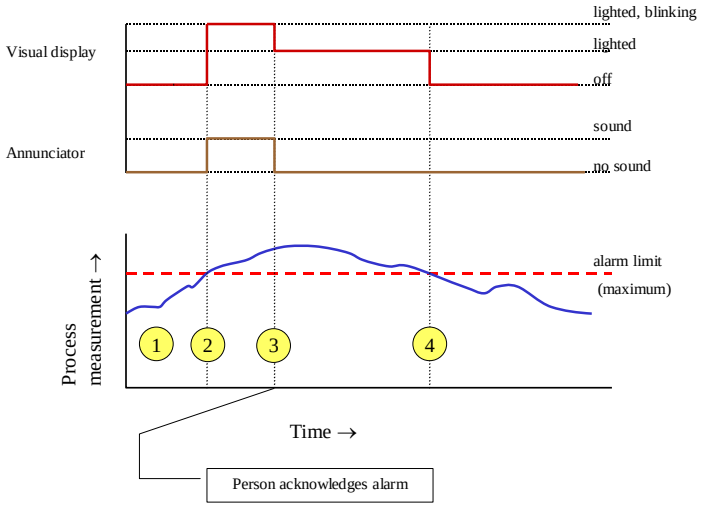



**Figure 5.6** Typical sequence of an alarm response during a transient.

For digital control systems, a record is retained of all alarm occurrences. This record can be useful in auditing the performance of safety equipment and plant personnel during a process incident.

The limiting value for each alarm is determined by the process engineer based on the equipment, such as the maximum pressure rating of a closed vessel or the chemistry of the process, e.g., temperature at which a runaway reaction might occur. Alarms provide essential early warnings that enable people to diagnose and correct unusual process situations before they lead to serious consequences. Therefore, the alarms must occur early enough in a scenario to give people time to analyze and respond; an alarm that is too close in time to a critical consequence will not provide sufficient time for people to diagnose the problem and take corrective action. Therefore, a careful analysis of the process and its dynamic responses are required to decide which variables should have alarms and for each alarm, the appropriate limiting value.

**It is important to recognize that no automatic response is provided by the alarm; people must diagnose the situation and implement appropriate corrective actions.**

Alarms need to be grouped and displayed according to a priority ranking, to enable people to quickly distinguish critical situations from typical variability. The following priority ranking is typical (CCPS, 1993B).

- **High** – Hazard to people, equipment and/or community, action is required
- **Medium** – Significant financial loss, careful monitoring required, action depends on subsequent process behavior
- **Low** – Variability away from desired operation but not critical, diagnose when time allows

Usually, only high and medium alarms have visual and sound indication. Low priority alarms are recorded for periodic review by plant personnel. Let's look at a process example to see how alarms contribute to safety.

**Example 5.3** Design the alarms for the flash process in Figure 5.7.

***When assigning alarms and priority levels, we consider the severity of a deviation from normal operation in the direction of the hazardous (upper or lower) limit.***

- ***PAH (P-2 pressure alarm high) – A high pressure would be hazardous. The alarm priority would be a high, since an immediate operator action would be required.***

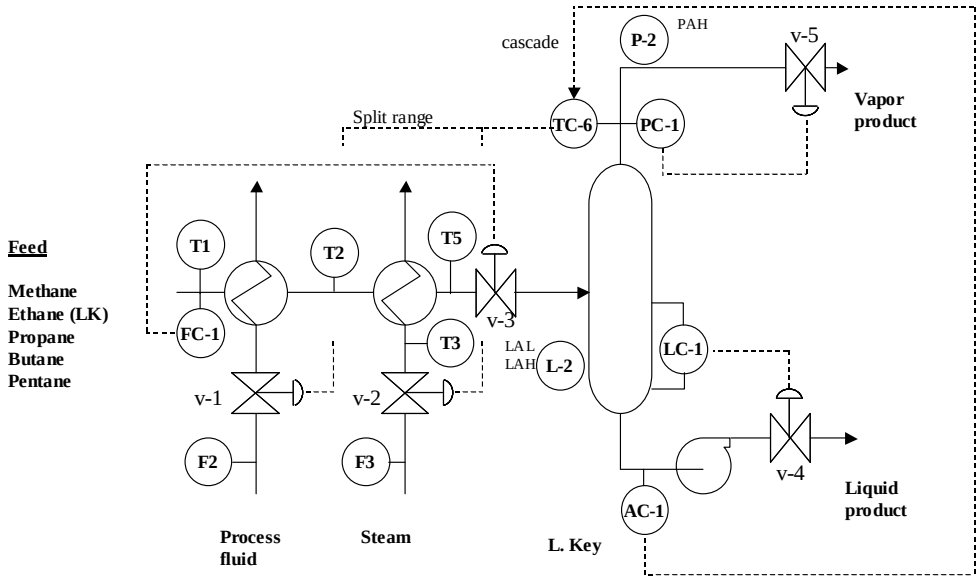



**Figure 5.7** Flash process with process control and alarms.

- ***LAH (L-2 level alarm high) – A high level could be hazardous since liquid could be carried over to the overhead pipe. The alarm priority would be medium (or high depending upon the downstream process).***
- ***LAL (L-2 level alarm low) – A low level could lead to the centrifugal pump running without liquid. The alarm would be high, since equipment damage could lead to a hazard.***
- ***Other variables could be alarmed if significantly affecting downstream processes. For example, if the light key measured by AC-1 posed a hazard to downstream equipment, an alarm would be appropriate.***

***To provide independence between the control and alarm layers, the three alarms should use independent sensors, as shown in Figure 5.7.***

Now that we have an idea of the good contribution to safety made by alarms, let's consider potential deficiencies at the alarm layer.

- **Hardware** - Since the alarm relies on sensors and signal transmission, the potential faults given above for process control equipment are applicable to alarms as well.
- **People –** The greatest strength of alarms is the problem-solving ability of the plant personnel. However, people are not perfect, and experience has shown that people can make serious errors, especially when under stress. In addition, we need time to think; if a response is required quickly, it will not occur reliably through the action of a person, who could be distracted when the event occurs.

When engineers design alarms, they must be aware of a common mistake, *too many alarms*. Recall that each time an alarm activates, the people must direct their attention to the alarm and analyze the variable. One study showed that a plant experienced 17 alarms/hour and that the people took action on only 7.5 percent of the alarms (Kragt and Bonten, 1983). If alarms occur too often when the process experiences minor deviations and the process recovers automatically through process control without intervention, people begin to ignore alarms. *An ignored alarm is a useless alarm*!

**Remember Aesop's Fable of the shepard boy who to annoy others, cried "wolf!" when no wolf was present. As a result, when the wolf actually appeared, no one paid attention to his alarm, and the wolf ate many of the boy's sheep!**

The plant personnel must diagnose the situation and take appropriate action. He/she will use all information available (all measurements for sensors, laboratory analysis, people observing equipment, etc.) in the diagnosis procedure. The appropriate action could be close monitoring, small changes to operation, substantial changes to operation, or extreme actions such as shutting down some equipment. For further discussion on alarms in process plants, see Bradsby and Jenkinson (1998) and Reising and Mongomery (2005).

In summary, alarms provide a warning that measurements are trending outside of their acceptable ranges. The alarm limits are defined to give plant personnel time to diagnose and respond to disturbances. Activation of a few alarms during a shift is common, and plant personnel have training and experience in recognizing causes and taking corrective actions.

## 5.4 Safety Instrumented Systems (SIS)

As the deviation from normal conditions becomes large, we may have to take drastic action to maintain safe conditions, perhaps even stopping the operation of some equipment. Since this action will prevent continued manufacture of saleable material, it is costly and is implemented only when required. However, most processes have serious potential consequences that must be avoided. Since there is often little time for decision making and alarms have not elicited a sufficient corrective action, these actions are automated through safety instrumented systems (SIS), also called safety interlock systems (SIS) and emergency shutdown systems (ESS).

Safety instrumented systems employ the feedback principle.

**Feedback**: **A feedback system uses information on a process output (measured dependent) variable(s) to influence a process input (manipulated) variable(s). A feedback loop contains a sensor, control calculation and final element (Marlin, 2000).**

We recall that process control compensates for variability through often small, continuous changes to valve openings, sometimes called modulating control. Process control maintains production rates and product qualities at desired values. In contrast, actions automated by an SIS typically involve discrete decisions implementing strong actions that fully open or close valves, stop/start motors, and so forth. The SIS actions quickly stop critical variables from approaching unsafe regions and return process variables to safe conditions, albeit not to a condition that necessarily provides on-specification products. The SIS maintains the valves in the stated positions until plant personnel intervene, i.e., the SIS does not provide automatic return to normal operation.

We have emphasized that each layer of the safety hierarchy must be independent. Therefore, the sensor used by the SIS and the final element implementing the action must not be shared by the process control or alarm systems. It is recommended that the computer used for implementing the logic is also independent of the process control computers. Finally, the valve actions should require no power, which is achieved by having the valve failure position be its position (open or closed) when the SIS has activated. With this design feature, a loss of pneumatic air will result in the safest process state, equivalent to activating the SIS, which will likely stop plant production but place the process is a safe condition.

SIS systems typically implement strategies using simple logic. For example, if a chemical reactor temperature is too high, the cooling water valve is automatically opened fully, which could override a temperature controller. While the logic is simple, the design requires careful analysis. The SIS must have a sufficiently strong effect (e.g., a large enough maximum cooling flow) and be activated soon enough (at a low enough temperature) that the reactor temperature will be reduced. If the effect is too weak and/or the action taken too late, the process could continue on its path toward a hazardous condition.

**Aren't you glad that you learned process dynamics, so that you can predict the path taken by variables when disturbances and SIS corrective actions occur!**

We recognize that the SIS is implemented automatically, without confirmation by a person, and takes strong action. Therefore, when an SIS activates, an alarm informs the plant personnel that the SIS measurement has exceeded its limiting value and the SIS has sent commands to the plant. Each alarm associated with an SIS would be in the category of high priority alarms.

Let's look at a process example to see how a safety instrumented system (SIS) contributes to safety.

**Example 5.4** An exothermic reaction occurs in the CSTR in Figure 5.8. The reactant and cold solvent flow to the reactor and the product is withdrawn from the bottom. During startup only, hot water flows to the reactor. After the reactor is warm enough for the reaction to begin, the hot water flow is stopped and the cooling water flow rate is

adjusted to control the reactor temperature. The control system is for the operation after startup. Your task is to design an SIS for a high temperature in the reactor.

***First, we provide an independent temperature sensor to measure the reactor temperature for the SIS. This temperature sensor is the only measurement to SIS 102, although an SIS can use multiple sensors. When the measured value is below the limit (the process is operating safely), the SIS sends a signal that energizes four solenoid valves that provide air pressure to the actuators so that the valves remain in their non-safe positions. When the measurement exceeds its limiting value, the SIS 102 sends signals to de-energize four solenoid valves, resulting in zero air pressure (gauge) to their actuators. The valves move to their failure positions.***

***In this example, the hot water is closed (it should be closed in normal operation, but let's be sure), the cooling water is opened, the reactant flow is stopped and the cold solvent is opened. Note that this is NOT a blue print for all CSTR reactors. The engineer must analyze the dynamic response for each equipment individually when designing an SIS.***

***As previously noted, the SIS does not reset automatically. Because of the extreme action taken by the SIS, a person must intervene by diagnosing the fault, correcting the underlying problem, returning the process to normal operation, and resetting the SIS, which will then serve as a safety layer again.***

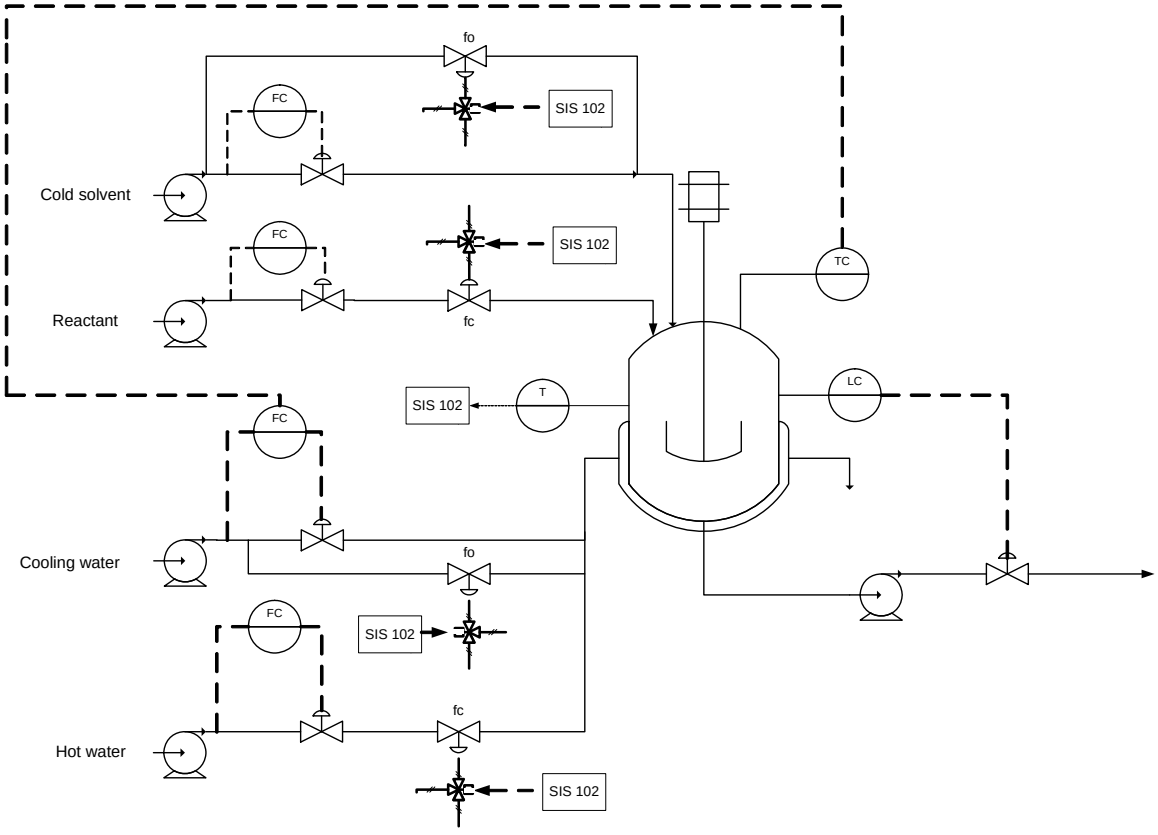



**Figure 5.8**. CSTR in Example 5.4 with safety instrumented system (SIS).

To ensure that the SIS layer is independent, the sensor, logic calculation (e.g., computer) and the final element must be independent of the process control and alarm layers. This principle was followed in the previous example. The control valves could also be manipulated when the SIS activates to provide a "double effect" to ensure that the flow paths are open/closed, as appropriate.

Now, let's consider some special factors in designing an SIS. First, before the process has been started up, many process variable values will be outside of their normal operating conditions. Without special features, the SIS would activate when the process is shutdown, and it would be impossible to startup the process! Therefore, a by-pass to the SIS logic must be provided for startup. Usually, the bypass will allow only a limited amount of time and will then automatically implement the SIS. For example, an SIS for a combustion system will seek an indication of a flame; if the flame is not sensed, the SIS will activate and stop the fuel flow. A startup bypass will allow fuel to flow for a few seconds to enable a fully developed flame to occur; if the flame is not sensed in a few seconds, the SIS will stop the fuel and the startup procedure must be performed again, after purging the equipment of uncombusted fuel.

A second common issue is that a SIS sensor could indicate a fault for a very brief time, while for all other times the measurement is within acceptable limits; this situation might occur when a flame flickers. In such situations, a delay can be included in the logic to require that the measurement limit be violated over a specific time period before the SIS is activated. Naturally, the time period must be very small compared with the time for the process to reach a hazardous condition.

A third issue occurs when violating any one of several different measurement limits can indicate a potential hazard that all have the same action. In such a situation, the individual SIS are combined through an (inclusive) OR logic, which means that if any one or several of the limits are violated, the SIS is activated. One can think of the inclusive OR to mean "AND/OR".

As the final issue, some critical SIS applications require protection against a sensor fault to achieve acceptable safety. Many designs are possible; here, we will note one common design, two out of three SIS. In this highly reliable SIS design, three separate sensors measure the same process variable. All are compared to the same limiting value, and the SIS is activated when at least two of the sensors exceed the limit. This design yields high reliability for action when the process variable exceeds the limit with a low probability that sensor faults will cause the SIS to activate when the true process variable is in its acceptable range.

We recognize that the SIS takes automated actions for one equipment. However, this action will strongly affect the entire process. Therefore, an alarm is activated along with the SIS automated actions. Plant personnel will be involved in diagnosing the problem, resetting the SIS, and returning the entire process to normal operation.

**While the SIS action is automated, all actions required for diagnosis and ultimate recovery to normal operations are not!**

In summary, the SIS layer is above process control and alarms, which means that these two layers have not been able to prevent further deviation from acceptable operation. Naturally, the limiting values used by the SIS are further from normal than the alarm limits. The SIS automates rather strong actions based on designed logic when measurements violate predefined limits. These actions are designed to return the process to a safe condition, but they usually result in lost production, so the actions are costly and are to be prevented when possible. After the SIS activates, the process control system and the plant personnel will undoubtedly be required to maintain the process in a safe

status, which should be a good starting point for returning to normal operation after the root cause has been diagnosed and corrected.

## 5.5 Pressure relief

Process equipment consists of many closed vessels because we want to prevent foreign materials from entering the manufactured materials, we want to prevent hazardous materials in the process from affecting personnel, and we process materials at pressures different from atmospheric. Fluids flow into and out of the vessels and reactions occur in the vessels. As a result, the pressure within the vessel can change, sometimes rapidly, and exceed the strength of the vessel walls, which has been constructed to satisfy a rating determined during the process design.

Pressure should approach the maximum (or minimum) limiting values infrequently because of the actions of the lower layers of the safety hierarchy. However, relief is essential for closed vessels to prevent explosions. To provide rapid and highly reliable actions at this layer, two design criteria are required. First, pressure relief must be automated because pressure can change quickly and responses must be fast. Second, the actions must not require external power, such as electricity or compressed air; this requirement contributes to high reliability since the relief systems can function during times when power is not available to the process. The second requirement eliminates the application of computers (or people) in pressure relief. So, how is relief achieved?

Relief systems take advantage of the difference between the internal process equipment pressure and atmospheric pressure (or some other pressure where the material will be vented). Let’s look at the most common relief equipment, the pressure relief safety valve in Figure 5.9. We will consider the situation in which the pressure in the vessel is above atmospheric and the relief system must vent fluid from the vessel when the pressure exceeds an upper limit. Under normal conditions, when the vessel pressure is below the limit, the spring exerts sufficient force to maintain the valve closed. Note that the desired set pressure spring tension can be achieved by adjusting a screw or nut.

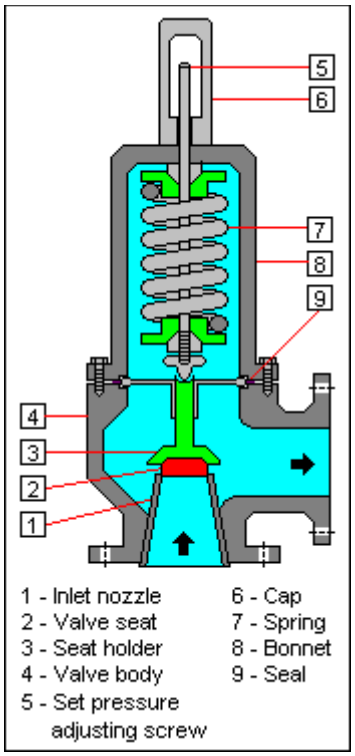



**Figure 5.9** Schematic of typical safety relief valve. Mbeychok (2012a)

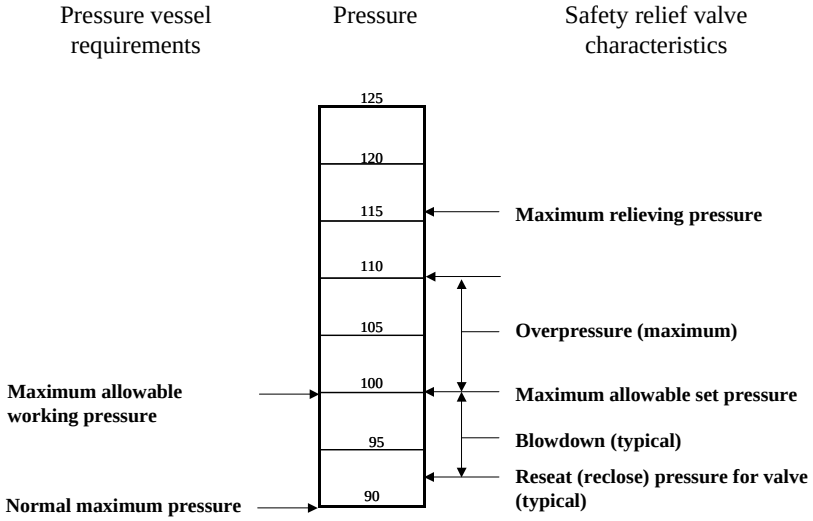



**Figure 5.10** Some typical safety relief valve characteristics (simplified from API RP 521, Guide to Pressure-Relieving and Depressurizing Systems (2nd Ed.), Washington, DC, American Petroleum Institute, 1982.)

When the internal pressure increases to or above its limiting value, the force against the valve seat will be sufficient to overcome the spring force, and the valve will open, allowing fluid to escape the vessel. When enough fluid has exited the vessel, the pressure and force against the valve will decrease sufficiently, and the valve will close. After it has closed, normal process operation can resume, and the safety valve is able to function at anytime in the future.

**The safety relief valve has several key features; (1) the fluid release is accomplished automatically, without intervention by a person, (2) no external power is required, and (3) the relief valve closes when the process pressure returns below the limit.**

Safety valves are the most commonly used relief device. However, the engineer should be aware of disadvantages of relief valves. First, the valve might not close perfectly, which would allow some leakage after it has once been opened; soft seat material or an "O-ring" in the valve seat can improve the tight closing. For this reason, we try to avoid high pressures that lead to opening safety valves. Second, a safety valve can "chatter", which occurs when the valve experiences the following sequence quickly and repeatedly; rapidly opens, vents some fluid, and then closes again. This behavior can damage the valve and require a process shutdown for repair. One way to avoid chattering

is to ensure that the safety valve capacity matches the process needs; although a very large valve with a high flow capacity is "safe", it can lead to chattering. Third, safety valves can become sealed due to corrosion or a lay down of process materials; if this occurs, the valve could fail to function when needed. As a result, safety valves are not recommended for application with corrosive fluids. Fourth and finally, safety valves are typically limited to pressures below about 135 MPa (20,000 psi).

The behavior of a safety relief valve is shown schematically in Figure 5.10. All values are relative to the valve set pressure that has the arbitrary value of 100%. The maximum usual operating pressure is 90% of the valve set pressure, although the vessel can be operated at any lower pressure. Since the valve opening is proportional to the vessel pressure, the pressure can exceed the set pressure, with values shown. Also, the pressure where the valve closes (reseats) is less than the set pressure because of frictional forces.

An alternative and complementary relief device is the rupture disk or burst diaphragm shown in Figure 5.11. When the pressure inside the vessel exceeds the upper limit, the disk will rupture, and the fluid will escape the vessel. The desired pressure limit is achieved by adjusting the disk material and its thickness. Naturally, the disk must

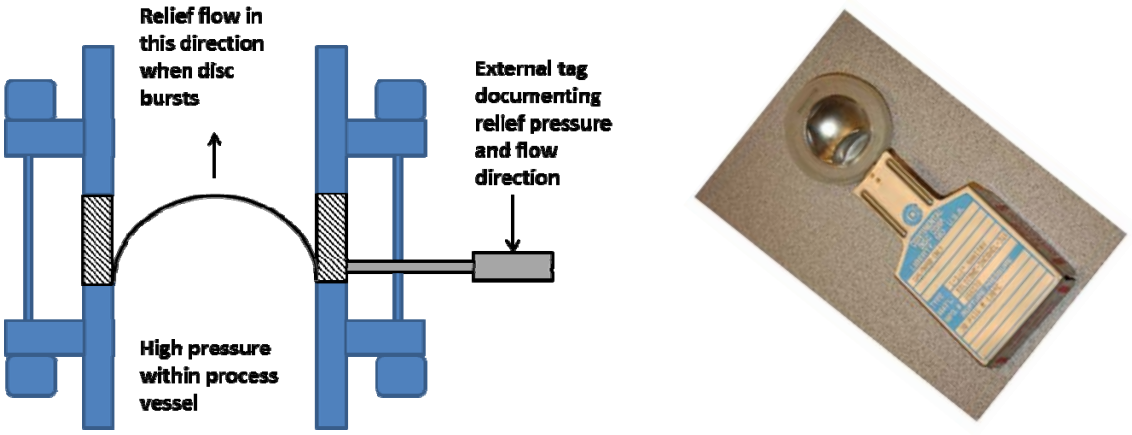



**Figure 5.11** Schematic and picture of rupture disc relief device. Picture due to Kuphalt (2012).

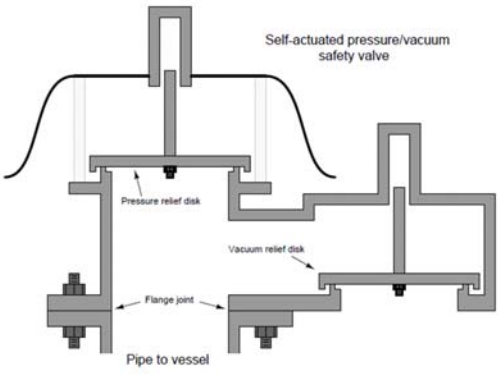



**Figure 5.12** Schematic of buckling pin relief device. Kuphalt (2012)

be replaced after it has ruptured. Advantages of the disk are no leakage, handling corrosion fluids, rapid release of high volumes of fluid, and application to high pressures. Disadvantages include process shutdown for replacement and poorer accuracy of the pressure limiting value.

A third type of relief device is the buckling pin; two of these devices are shown in Figure 5.12. In this figure, the vessel is protected against both high pressure and low pressure by two buckling pins. Remember that a low pressure could cause a vessel to collapse or "implode" just as a high pressure could cause an explosion.

Relief devices should be located on any closed vessel, i.e., any significant space having a potentially restricted access for relief. For example, a vessel that vents to atmosphere through a pipe that has an isolation valve must have pressure relief, even if the isolation valve is normally fully opened. Remember, the process must be safe even when a person or control system makes a mistake and improperly closes the valve. We should provide relief devices for vessels that normally would not experience high pressures because the vessel could experience excessive pressures in the event of faults, such as a runaway chemical reaction, valve failure or plant fire. Procedures for identifying relief locations will be presented in Part II of this chapter, but some guidance is provided here in Table 5.1.

**Table 5.1** Typical Locations for safety relief.

| Location and Reason | Process Examples |
|---|---|
| Vessel or large pipe that can be isolated by existing valves (including manual values that should be open) | Distillation tower<br>Chemical reactor<br>Flash drum |
| Vessel due to loss of cooling (e.g., loss of cooling water due to pump failure or power loss) | Distillation<br>Chemical reactor<br>Vapor compression refrigeration |
| Vessels, pipes (liquid filled) due to external heating from fluid or fire | Water side in condenser<br>Jacket cooling stirred tank (loss of water flow) |
| Pipe overpressure due to failure of valve or regulator with upstream pressure above downstream limits | Equipment using steam at lower pressure than steam source<br>Exhaust of turbine |
| Pipe or vessel due to high pressure from equipment | Exit of positive displacement pump<br>Exit of compressor |
| Heat exchanger shell due to rupture of tube | Shell and tube heat exchangers |
| Vaporizers due to excess vapor | Distillation<br>Flash drum |
| Reactors due to sudden condensation (protect against low pressure) | Equipment being cleaned with steam that can condense when contacting cold metal |

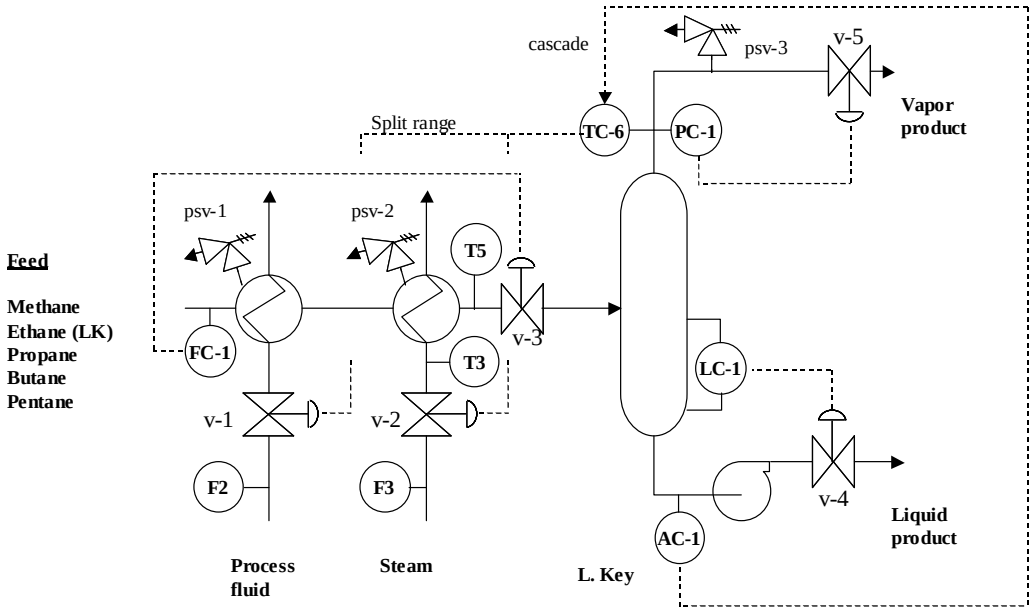



**Figure 5.13 Flash process with process control and safety relief.**

**Example 5.5** Define where relief devices are required for the flash process in Figure 5.13. In addition, select a device type. The feed pressure in 4.5 MPa and the flash vessel pressure is 1.0 MPa; determine the safety valve set values.

***When the feed, top vapor effluent and bottoms liquid effluent valves are closed, the flash drum would be enclosed. Therefore, the drum should have a high-pressure relief. Since the fluids are clean and low viscosity, a safety relief valve would be used, since it will reclose when the process pressure returns below the limiting value.***

***The utility side of the heat exchangers is hotter than the process side. We noted in a previous section of the operability material, that isolation (and bypass) valves would normally be provided to remove a heat exchanger for maintenance. Therefore, the process fluid could be a closed volume and heated by the utility stream. Therefore, safety relief valves should be provided on the process side of each heat exchanger.***

***The locations of the safety relief valves are shown in Figure 5.13. Since the process fluid is combustible, all relief devices must be connected to a containment and/or disposal process (see Example 5.7).***

Now, let's consider the relief device capacity. The principle for sizing the device is that the "worst case" process scenario (set of events), including likely faults, should not lead to an unsafe process condition. This requires the engineer to define the worst-case scenario and to determine the maximum possible flow through the relief device during the scenario. Generally, the worst-case scenario is the combination of faults that results in the largest flow rate through the relief device. If the same relief device attenuates

several independent faults, the engineer must decide whether the worst case for the device is the largest single fault or a combination of several faults.

**Example 5.6** Determine the worst-case scenario for the safety relief valves in the flash drum in Figure 5.13.

***For the liquid-filled heat exchangers, the relief is required for a scenario in which the utility fluid is flowing at its maximum and the process fluid cannot flow because the block valves are closed (when they should be opened). Therefore, the maximum relief flow rate depends upon the maximum heat transfer rate, Q, (the maximum likely temperature driving force and heat transfer coefficient) and the coefficient of thermal expansion of the process fluid.***

***Fmax = (Mass of feed in the exchanger/density)*(thermal expansion coefficient) *Q (energy/time)***

***For the flash vessel, the maximum vapor flow would be the maximum vapor generation with no flow exiting the vessel, which could occur when the heating utility valves failed open (non-failsafe) and the vapor valve, v-5, failed closed (non-failsafe).***

***Fmax = maximum feed flow*(max % vapor/100)***

When the maximum relief flow rate and conditions (composition and pressures) are known, the engineer can determine the proper relief capacity. For most devices, the design decision to achieve the desired relief capacity is the orifice area when the device is fully opened. The detailed correlations and guidelines are not presented here; however, the following summarize the approaches for safety relief valves. Details for the calculations and complete information for rupture disks are available in Crowl and Louvar (1990). The calculation follows the same principles for any valve, so you are familiar with the general calculation procedure. The appropriate general equation is given below when the flow through the orifice is below sonic velocity.

$$F = C_0 A \sqrt{\frac{2 g_c \Delta P}{\rho}} \tag{5.1}$$

with

| | | |
|---|---|---|
| $A$ | = | *Area of the relief valve orifice* |
| $C_0$ | = | *discharge coefficient (usually between 0.61-1.0)* |
| $F$ | = | *Flow through the relief valve* |
| $\Delta P$ | = | *pressure difference across the relief valve* |
| $\rho$ | = | *gas density* |

- **Liquid flow** through a relief valve

The general equation above can be rearranged to solve for area, with several correction factors are included; the values for these factors are available from process design correlations.

*Non-flashing liquid flow*

$$A = \frac{F}{C_0 K_v K_p K_b} \sqrt{\frac{\rho / \rho_{ref}}{(\ 1.25\ P_s\ -\ P_b\ )}} \qquad (5.2)$$

*with*

| | | |
|---|---|---|
| $C_0$ | = | *discharge coefficient (usually between 0.61-1.0)* |
| $(\rho/\rho_{ref})$ | = | *specific gravity of liquid* |
| $F$ | = | *Flow through the relief valve* |
| $P_S$ | = | *set pressure ; $P_b$ = back pressure (gauge)* |
| $K_V$ | = | *viscosity correction ( approaches 1.0 as Re is large, > 30,000)* |
| $K_p$ | = | *overpressure correction, depends on the overpressure from relief device (lower overpressure gives a smaller Kp and larger area)* |
| $K_b$ | = | *back pressure correction, □ 1.0 for balanced valve = 1.0 for conventional valve* |

- **Vapor flow** through a relief valve

Since the flow through relief valves typically involves large pressure drops, the vapor flow is typically sonic, resulting in chocked flow. In this situation, the flow is independent of the downstream pressure, and the following expression can be used to determine the orifice area.

*Sonic (chocked) vapor flow*

$$A = \frac{F}{C_0 P} \sqrt{\left(\frac{T}{M}\right) \Big/ \left[\frac{\gamma g_c}{R_g}\left(\frac{2}{\gamma+1}\right)^{(\gamma+1)/(\gamma-1)}\right]} \qquad (5.3)$$

with

| | | |
|---|---|---|
| $C_0$ | = | *discharge coefficient (usually between 0.61-1.0)* |
| $F$ | = | *Flow through the relief valve* |
| $P$ | = | *upstream pressure (absolute)* |
| $T$ | = | *temperature* |
| $M$ | = | *molecular weight* |
| $\gamma$ | = | *heat capacity ratio* |
| $g_c$ | = | *gravitational constant* |
| $R_g$ | = | *gas constant* |

- **Two-phase flow** through a relief valve

It is important to be aware that two-phase flashing flows have a complex relationship between pressures and flow rate. Considerable experimental effort

has been invested to develop design methods for relief of two-phase flows, and reliable correlations are available (Crowl and Louvar, 1990).

**When relief valves were improperly sized using single-phase methods for two-phase relief flows, designs were provided with relief capacities that were too small, resulting in explosions of vessels. Death, injuries and major damage resulted from these under-sized relief systems.**

The discussion so far has concentrated on the relief devices that prevent explosions from vessel failures. When any of these devices activate, process material escapes the containment provided by the process vessels. To prevent hazards, the process design must provide appropriate effluent handling for the material released. Some examples of proper effluent handling are given in Table 5.2. Naturally, a combination of these steps may be required.

**Table 5.2. Examples of Effluent Handling**

| Type of material | Effluent Handling |
|---|---|
| Contaminated Water | Divert to biological wastewater treating process in the plant.<br><br>If the contaminant may degrade the biological treating, it can be diverted to a holding pond and slowly processed at low rates |
| Combustible gases | Divert for combustion (flare or incinerator).<br><br>In many instances, the gas can be collected and used as fuel in the plant; however, safety requires reliable effluent processing when the process does not require fuel. |
| Strong acid or base | Divert to containment and/or neutralize through pH control |
| Hazardous materials | Appropriate neutralization and/or containment are required.<br><br>A separation process can be used to concentrate the toxic material, allowing hazardous materials to be captured (stored or returned to the process) and benign components to be released. |
| Any material | When possible, the material can be recycled in the process. This can be a low-cost option that eliminates release outside of the process equipment. However, recycle may not always be possible, depending on the fault occurring in the process. |
| Benign material such as clean water, steam or air | Can be released directly to the environment<br><br>The design should direct the flow so that no person can be harmed when the flow occurs.<br><br>Noise suppression may be required. |

**Example 5.7** The relief flows from the flash process are hydrocarbons and must not be released to the atmosphere. Sketch the major equipment required for effluent handling.

***The hydrocarbons can be combusted to benign components. We will consider a flare system that handles effluents from the entire plant. These streams can contain vapor and liquid from various process control and relief valves. The key equipment are shown in Figure 5.14.***

***The piping from each process is connected to a knockout drum, where liquid and vapor are separated. The liquid is pumped to a containment tank, with a level controller used to regulate the flow. The vapor exits the drum and proceeds to a sealing device that acts as a pressure controller and prevents backflow; note that no valve should be placed in this pipe so that a highly reliable path exists to the flare without the possibility of back flow of air into the drum. Then, the stream flows to the flare that has a continuous flame. Further details for the design of the individual equipment are given in CCPS (1993).***

***We note that many governments are legislating "zero-flare" policies, which requires that effluents be recycled for use as fuel or be processed in another manner. Under normal circumstances and for mild disturbances, this policy is possible; however, major faults will generate flow rates of effluent hydrocarbons beyond the capacity of recycle systems. Therefore, a flare is required for safety. For an example of when inadequate effluent handling led to loss of life and major equipment damage, see reports on the BP Texas City tragedy (e.g., CSB, 2007).***

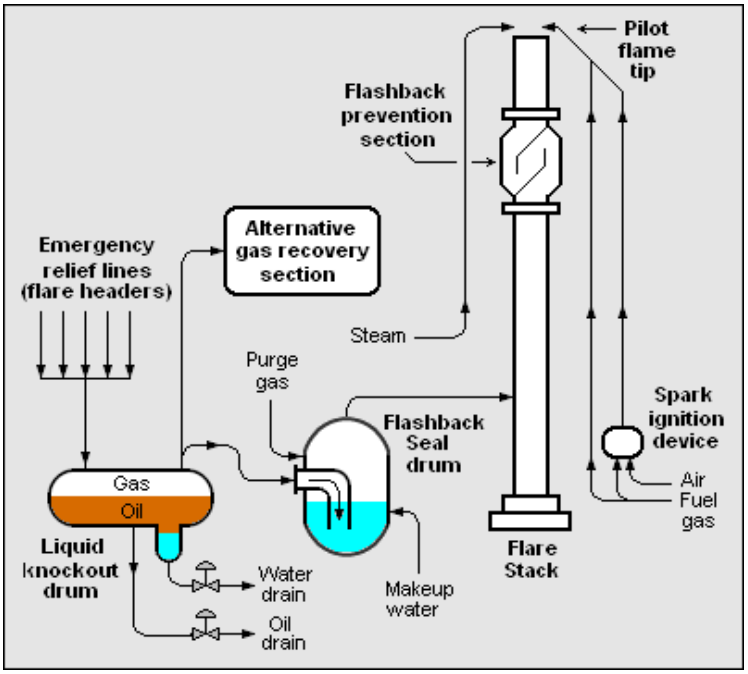



**Figure 5.14** Schematic of a flare system with knock drum and pressure seal. For much greater detail, see Grossel (1990). Mbeychok (2012b)

The capacity of the effluent handling must be adequate for a worst-case plant scenario. For example, the loss of cooling water in a plant could result in lack of condensing in distillation towers, loss of cooling in reactors, and loss of vapor compression refrigeration. The result would be a very large flow of vapor from many relief devices. The piping, vapor-liquid separation (knockout drum), and flare must have sufficient capacity to process all effluents. In situations in which effluents can be stored, such as water-based effluents, the storage volume must be adequate to contain the "worst case" release.

For further discussion and design details for pressure relief, see CCPS (1998), API (2007) and Crosby (1997).

There are a few cases where a process vessel may fail and a large amount of material must be released rapidly, perhaps due to an explosion. In these situations, the building containing the process must be designed accordingly. In some cases, a blast wall can be integrated in to the building; the blast wall is a "weak link" in the building so that an explosion will vent by destroying the wall (or displacing a wall on hinges). The pressure wave resulting from a dusk or vapor explosion can be estimated (Crowl and Louvar, 1990). Naturally, this design is appropriate only when release of the material to the environment is acceptable (as a last resort) and the space outside the building can be isolated to prevent injury to people and critical equipment.

## 5.6 Containment

The first four layers in the hierarchy provide multiple, independent safety systems, and they will reduce to a very low value the likelihood of a fault leading to a severe consequence. However, the likelihood will not be reduced to zero. Therefore, the fifth layer is designed to reduce the impact of a fault not completely ameliorated by the first four layers. Some containment designs provide complete protection from hazardous conditions, while others only reduce potential harm to workers, the local community, and the environment.

As already discussed in relief systems, the material allowed to flow out of a vessel to reduce pressure should be safely processed, which can include containment for later processing. Examples of containment include holding ponds for water-based streams, constant volume drums or tanks for liquids, and constant or variable volume closed vessels for gases. In some cases, the containment might be used to store part of a stream, as with a mixed liquid-vapor stream, with the liquid being contained and the vapor passing to further processing, such as a flare.

Chemical plants often have dikes surrounding process equipment and/or tanks. This is a form of containment that does not prevent all hazardous conditions because, for example, the stored liquid could combust. However, dikes can reduce the more deleterious consequences of an accident.

In extreme cases (such as a nuclear power plant), the release could be a large quantity of material that cannot be released; in such situations, the building must be designed and constructed so that it can contain the effects of the explosion. This situation could also apply to very hazardous materials being manufactured within a building.

**Example 5.8** A company produces ammonia using the well-known Haber-Bosch process (Britannica, 2010). This type of plant usually involves large storage of liquid ammonia at a low temperature. A release of ammonia would be hazardous to the workers and community. What special design would be appropriate?

> ***The storage tanks could be constructed with double walls, so that a failure of the inner wall would not immediately release ammonia. However, the initial failure would result in ammonia contacting the outer wall, which could also fail after some time; how could we know that the inner wall has failed? The design must also include a sensor to measure for the presence of ammonia in the space between the two walls. The combined design of double-walled tanks with inter-wall sensors for ammonia will provide highly reliable containment. (Cheresources, 2010)***

## 5.7 Emergency Response

No safety system will eliminate all hazards; for example, a pipe could fail and release hazardous materials, lightening could strike a process, or a plane could crash into a process. We must admit that a small probability exists that fires and releases of hazardous material will occur. Therefore, we must have a response plan for the industrial site and for the surrounding community. The planning is outside of the scope of this presentation of operability. Please refer to the coverage in CCPS (1993A).

**Example 5.9** The ammonia plant considered in Example 5.8 has a large volume of liquid ammonia stored. Emergency personnel from local fire departments must enter the industrial site in case of an emergency. Would there be any barriers?

> ***In the worst case, a cloud of ammonia could block entrance to the site. Therefore, multiple roads from different directions are required to provide access during times with different wind directions.***

## 5.8 Reviewing the Safety Hierarchy

Now that we have learned about each layer of the safety hierarchy, we will briefly review the layers in this section. The hierarchy is shown in Figure 5.15, which is an expanded version of Figure 5.3. We note that the set values, where actions occur, are increasingly further from normal operation as we progress up the hierarchy. Therefore, each layer has an opportunity to limit the deviation from normal before the next higher layer is reached. Please note where actions are automated and where they depend on the intervention of a

person. Also, note where external power (electrical, air pressure) are required for the layer to function properly.

Figure 5.15 is misleading in one aspect; it shows only one process variable. However, many hazardous conditions depend on a combination of variable values. In response, the plant personnel observe many variables when diagnosing the process and deciding on proper actions. In addition, the process control layer involves many controllers adjusting many valves simultaneously. Also, the SIS systems can be based on several measurements. Generally, relief devices are based entirely on pressure, although they do not require a separate measurement device of the pressure.

## 5.9 Summary of the Safety Hierarchy

Chemical processes involve temperatures, pressures and materials that can be hazardous to plant personnel and, in extreme situations, the surrounding community. Engineers must ensure safe operation by designing equipment and training plant personnel. Since all equipment can fail and humans are fallible, we must consider the possible failure of any element in the safety system. Therefore, we always provide a hierarchy of independent safety layers, so that the likelihood of all layers failing simultaneously is very low.

The most common safety hierarchy in the process industries has been introduced in this chapter. Examples have shown typical equipment used at each layer. However, the key learning goal is mastery of the concepts for the hierarchy and for each layer. Achieving safety will require different designs for processes handling toxic vapors, combustible liquids, dust, high pressures, cryogenic temperatures, pharmaceuticals, food, etc.

**When reviewing process safety, use the safety hierarchy. Be sure that the goals of each layer have been achieved in the completed design.**

The new engineer will have to learn from industrial experience. However, accidents occur infrequently; in fact, an accident may not occur during many years of operation with an unsafe design. This “time bomb” is waiting for a specific set of events to “ignite the fuse”. Therefore, the engineer must research the topic thoroughly, understand the chemistry and physics, and ensure that an adequate hierarchy is designed, installed, and maintained. To reinforce experience within one company and plant, professional references, training courses and published materials from outside a specific company should be consulted.

**You should review the important accidents in process engineering and recognize that some common design approaches (employed by large industrial companies) have been shown to be faulty, with the proof being accidents involving lost of life, damage to surrounding communities, and billions of dollars of economic losses.**

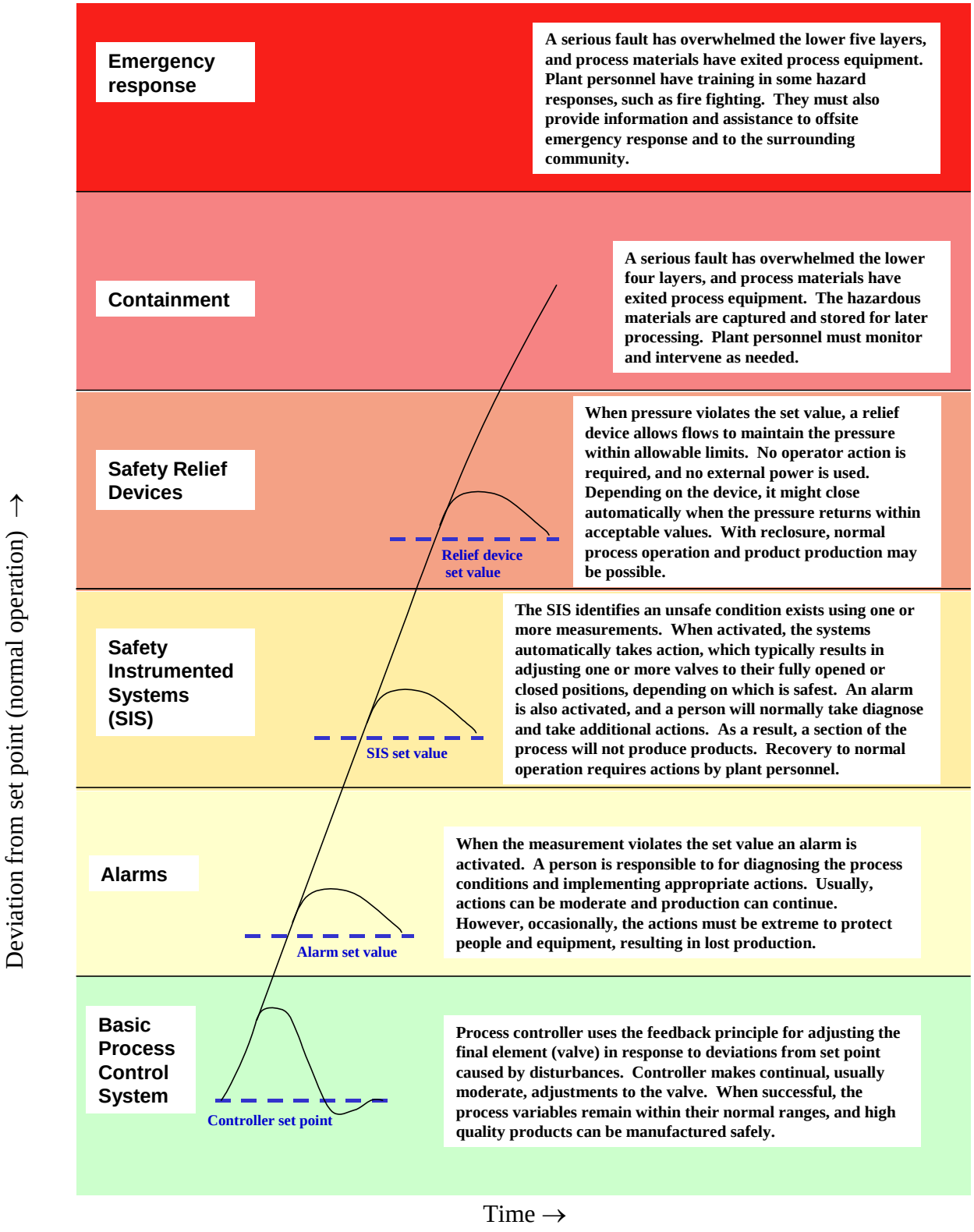



**Figure 5.15** Summary of the safety hierarchy with comments for each layer.

Part I of this chapter provided basic concepts and example designs for each layer of the hierarchy. We must put these concepts and methods together in an integrated design for a specific process; no single safety design is appropriate for all processes. If the safety design is too limited, the process will not be safe; if it is too complex, it could be unreliable, difficult to understand, and costly. Since the design requires a wide range of expertise, the design is usually reviewed and completed by a team. The team procedures for safety design are presented in Part II of this chapter.

# Part II: Managing the Process Hazard Analysis

## 5.10 Introduction to Process Hazard Analysis

In Part I of this chapter, we learned about the safety hierarchy and the most common designs used at each layer of the safety hierarchy. In Part II, we will learn methods for reviewing a process, defining the required safety performance, identifying potential hazards, determining causes and consequences of each hazard, and if required, modifying the design at the appropriate layer(s) of the safety hierarchy to achieve the target safety performance.

Before discussing safety reviews, we need to understand the few basic terms given below, because they are used in common discussions with subtle differences in meanings.

- **Hazard** – A characteristic of the system that has potential for causing harm to people, equipment or the environment. A "characteristic" should be considered broadly, for example, chemical or biological effects of materials, electrical, mechanical (e.g., high pressures), thermal or a procedure performed by plant personnel.
- **Incident** – Undesired circumstances that have the potential to cause an accident. Note that this includes near misses.
- **Accident** – This is an incident that led to safety consequences, e.g., injury, equipment damage, environmental harm, or severe economic loss.
- **Risk** – The risk of an event is the likelihood of the event occurring under specified conditions within a specified period of time. Generally, we consider the undesired event and express risk as a fraction, such as 0.01 occurrences/year.

The general anatomy of an accident is shown schematically in Figure 5.16. The Hazard exists because of the design, and it can be thought of as latent until an event occurs. The Cause is a fault or action that can lead to an accident; since a series of events can occur, we seek the root (or initiating) cause. The Deviation from safe (normal) operating conditions results from the cause, and this deviation has the potential for leading to an accident if sufficiently large. The Accident is the result of the large deviation that can injure people or damage equipment or the environment. There can be a series of accidents with different severities depending on the size and duration of the deviation. The Consequence is the effect measured as injuries, deaths, damage, effluent

HAZARD → CAUSE → DEVIATION → ACCIDENT EVENT → CONSEQUENCE

| Material and energy during operation | Initiating event or Root Cause | From design operating conditions* | Physical condition yielding harm | Severity of consequences |
|---|---|---|---|---|
| • Toxicity<br>• Flammability<br>• Reactivity<br>• Elevated Pressure<br>• Elevated temperature | • Action by person<br>• Mechanical failure<br>• Design flaw<br>• Process change (e.g., fouling)<br>• External change (force, fire, etc.) | • Flow variations (to zero or maximum)<br>• Material compositions (or improper materials)<br>• High/low pressure or temperatures<br>• Improper mixture of materials | • Combustion/ explosion<br>• Fire<br>• Hazardous material released<br>• Equipment damaged | • Injury<br>• Death<br>• Undesired releases to environment<br>• Disease<br>• Equipment damage<br>• Recycle/scrap of materials in production<br>• Loss of production |

* We should also challenge the design conditions by asking, "Have they been properly selected for safety and profit?"

**Figure 5.16.** Anatomy of an Accident with some typical entries in each column (Modified from DOE (2004))

releases, lost production, and so forth. Naturally, the severity of the consequence is important in determining the proper design.

The sequence in Figure 5.16 represents the behavior without proper safety modifications. Proper designs will prevent or dramatically reduce the frequency of proceeding to a large deviation and accident. The range of possible design modifications depends on the specific situation and stage of the project as explained in the following.

- Process development - changes to chemistry, e.g., changing catalyst to avoid very high pressures
- Process design - moderate changes in process structure (e.g., adding additional cooling capacity to an exothermic reaction system
- Existing plant – Elements in the safety hierarchy that substantially reduce the deviation from normal operation.

The safety modifications can be thought of as interrupting the sequence in the "anatomy" shown in Figure 5.16 to prevent serious consequences.

The process industries apply a wide range of safety analysis methods to identify, assess qualitatively and assess quantitatively hazards, and only a few of these will be presented in this Chapter. A summary of the most prominent analysis methods is given

in Figure 5.1, with the methods introduced in this chapter indicated. The methods most commonly used to identify potential hazards and qualitatively determine the proper designs are emphasized in this coverage. Because of the wide application of the methods, most engineers will participate in team studies using these methods. The methods not covered here tend to involve more quantitative methods for establishing hazard occurrences and are used by specialists to refine on the results of the methods presented here.

## 5.11 Setting Safety Targets

Determining the proper level of reliability to achieve desired safety is likely the most difficult and controversial task in all of engineering practice. Here, some common terminology and typical methods for expressing risk will be introduced and general principles affecting the target risk level are explained. Some typical target risk values are reported, but no definitive recommendation is presented. The practicing engineer must set the proper target for a specific system using all information available about the system.

We can establish ranges of risk for various activities from historical data. The following metrics are often used when reporting risk.

- Fatal Accident Risk (FAR) is the number of fatalities per $10^8$ hours of exposure, which is approximately equivalent to fatalities for 1000 people working a lifetime. This measure is used in the United Kingdom.
- Individual risk (IR) is the probability of an injury per a defined time period; here, a one-year time period will be used.
- OSHA Incidence Rate gives the number of incidences for one hundred work years. This is used in the United States.

Now we encounter the difficult task of defining the level of risk for a specific consequence. A general goal of industrial design is to expose people to a lower risk while at work than they experience in their personal activities. Some sample data on individual risks are given in Table 5.3. We must recognize that each individual person has a unique attitude about the risk of an accident. Some people engage in highly risky behavior, such as rock climbing, while others choose to lead a low-risk lifestyle. Therefore, we should ensure that work risk is lower than the conservative lifestyle risk, since the work risk is not entirely voluntary and balanced to achieve the benefits of earning a wage.

We will seek to achieve a low risk in our designs. A common term for this is “acceptable risk”; however, some concern has been raised about who “accepted” the risk voluntarily.

**Table 5.3 Sample data on individual risks (fatalities/year)***

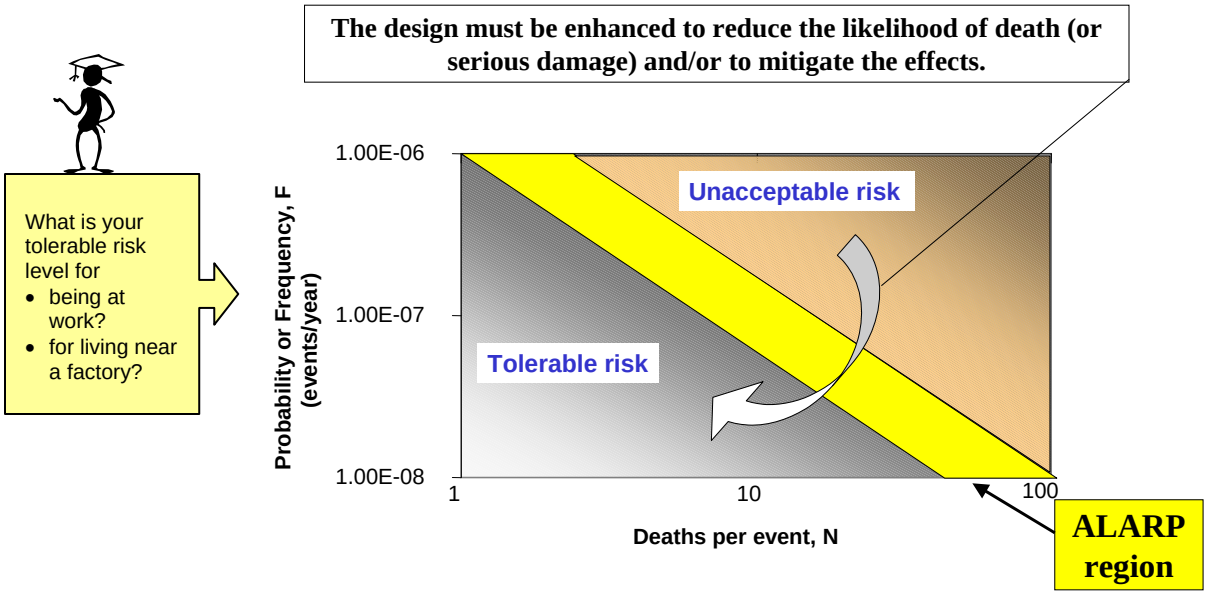
| | |
|---|---|
| Rock climbing (200 hours per year) | $80 \times 10^{-4}$ |
| Highway accidents | $4.0 \times 10^{-4}$ |
| Accidents in private homes | $1.0 \times 10^{-4}$ |
| Lightning | $0.001 \times 10^{-4}$ |
| | |
| Coal mining | $1.1 \times 10^{-4}$ |
| Construction | $0.90 \times 10^{-4}$ |
| Manufacturing industries | $0.20 \times 10^{-4}$ |
| Office work | $0.04 \times 10^{-4}$ |

* Data from the UK reported by Wells (1996)

**Therefore, the term "tolerable risk" will be used here, with tolerable meaning that the risk has been understood and that people are willing to live with the risk to achieve certain benefits.**

When considering risk, the number of people affected by an accident as well as the accident frequency must be considered. Naturally, a lower frequency should be associated with risks involving more severe consequences. The typical manner for representing this relationship is the F-N graph on which the accident frequency is plotted versus the number of people affected (i.e., the fatalities) on a log-log scale. An example F-N graph is given in Figure 5.17. After the engineering team has determined a consequence of an accident (in potential fatalities), the F-N graph can be used to determine the target frequency; then, the process design, especially the safety hierarchy, can be designed to meet or exceed the desired safety performance, which is less than or equal to the target frequency.

The frequency-fatality (F-N) plot in Figure 5.17 contains three distinct regions. The lower triangle involves low frequencies of occurrence and defines the tolerable region; some say that the risk is negligible in this region. The upper triangle involves high frequencies for high consequences; this region is not acceptable. In some ranking systems, this region is further subdivided into a region requiring immediate correction and a region that can be corrected within a defined time, such as one year (Pasman and Vrijling, 2003). The middle band includes situations where we want to achieve the risk "as low as reasonably practicable" or ALARP, which requires that the risk will be continually reviewed and lowered whenever practically possible. "Practically possible" depends on the technology commonly used in the process industries.




**(The coordinate values here are not "standard" or recommended; they must be selected by the professional and organization.)**

**Figure 5.17** Example of F-N (Frequency-Consequence) Graph

When the frequencies of occurrence are defined for a specific consequence, we must consider the following additional issues.

- The total risk for a person is the sum of the frequencies of (independent) accidents. The frequency of one accident should not be set at the maximum tolerable risk for a person.
- The failure data for establishing the frequency of an accident contains considerable uncertainty. We must be conservative and not design up to the boundary of intolerable risk. (See Appendix 5.A.)
- The frequency of a person being injured is the frequency of an accident multiplied by the frequency of a person being in the area affected by the accident.
- Society places great importance on accidents involving multiple causalities, so that engineering should reflect these values. Therefore, the F-N curve generally drops more steeply at higher consequences (not shown in Figure 5.17).
- Consequences other than human death influence our selection of tolerable frequency. For example, a once per year frequency of an accident would not be acceptable for a situation leading to zero deaths but thousands of animals killed or hundreds of square kilometers of land uninhabitable for centuries. Therefore, other consequence scales (e.g., equipment damage, economic loss, environmental harm) could be superimposed on the fatalities coordinate.

No generally accepted boundaries for the three regions in the F-N plot exist, so the engineer must define the boundaries for each design.

**No specific recommendations for tolerable risk and F-N boundaries are provided here. Figure 5.16 and examples in this chapter use values that are within the range of values used in the engineering literature.**

While no single standard for the F-N plot exists, governments are beginning to define safety performance targets (Trbojevic, 2005). Some trends are clear; (1) governments are beginning to establish risk targets, leaving individual companies with the freedom to determine designs to achieve the targets, (2) new plants are being held to lower risk frequencies than existing plants, and (3) tolerable frequency limits are being lowered over time.

The remainder of Part II of this chapter addresses interrelated topics for satisfying a specific F-N risk performance, principally through the design of the safety hierarchy. The remaining topics are (a) managing the safety study method (Section 5.12), (b) identifying hazards (Sections 5.13 and 5.14), and (c) designing a safety hierarchy to achieve tolerable risk (Section 5.15).

## 5.12 Managing the Safety Analysis

Safety analysis requires both broad and deep knowledge of chemistry, process equipment, instrumentation and control, and how a complex plant is operated. Therefore, a team of engineers and plant operators are needed for a thorough safety analysis. At least one member of the team must be expert in the analysis method being used and experienced in leading safety studies; this person is responsible for preparing information, managing meetings, enabling all members to share their expertise, and ensuring the proper documentation is completed. For details on the organization and management of safety analyses, refer to DOE (2004) and CCPS (1992).

In addition, considerable information must be available to the team, with the available information depending on the time the analysis is performed, e.g., process development to existing plant. Various safety analyses are performed during process development, process design, construction, and operation. Earlier analyses have less specific information, but much greater flexibility in improving designs at low cost; for example, materials of construction or equipment structures can be modified during the development and design stages at low cost. After equipment has been designed and ordered, such changes can be very costly.

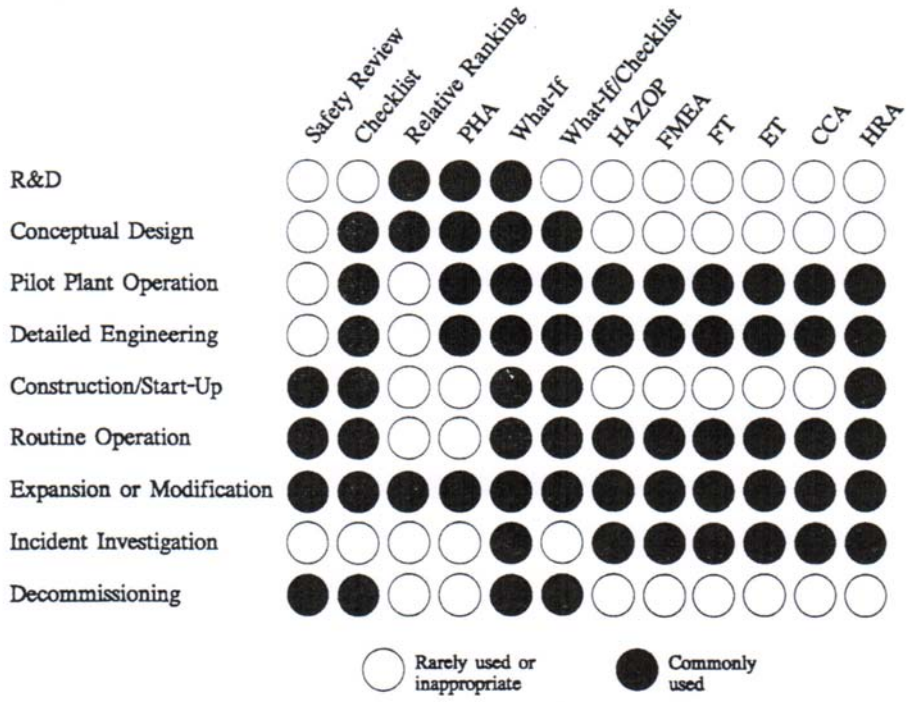



Figure 5.18 Typical safety analysis methods applied at each stage of a project. (Reprinted by permission. Copyright @ 1992 Wiley, CCPS (1992) *Guidelines for Hazard Evaluation Procedures (2nd Ed.)*, American Institute of Chemical Engineers, New York, Figure 6.1)

Different methods for safety analysis are typically performed at different stages in a project. A summary of these methods is given in Figure 5.18. As expected, methods requiring more information and engineering effort, HAZOP and beyond, are reserved for when the information is available.

In all safety analyses, appropriate documentation of findings must be prepared. Along with each finding, responsibility for follow up investigation is assigned. The conclusion after further investigation must be documented to enable proper modifications to be implemented.

## 5.13 Preliminary Safety Analysis Methods

The methods in this section require limited process knowledge and engineering effort. They can identify many potential hazard sources and suggest some remedial designs. In addition to solving some problems, they provide invaluable guidance for the more detailed and time-consuming methods. Therefore, they should be applied for nearly all safety reviews.

**Checklist**: A checklist of common issues is very useful for an initial safety analysis. It has the following advantages.

- Requiring a short time
- Requiring limited expertise to apply (although expertise is required to assemble the checklist)
- Applying past experience in similar processes
- Applying past experience with common incidents and accidents

Naturally, a company should continually update the checklist as new data and experience become available to ensure that the engineers take full advantage of hard-won, real-world experience. Separate checklists should be prepared for all important topics, such as site location and layout, each unit operation, individual equipment, special material and chemistry issues (e.g., corrosion), instrumentation and controls, electrical and building structures, and operating policies. Forty-five pages of general checklists are available in CCPS (1992), and references to checklists for a wide range of topics is available in Lees (Section 8.3, 1996).

**What-if Analysis**: In this method, the team poses "What if" questions to uncover potential hazards. Not every question must start with "What if", but each should address a safety issue. Samples of What-if questions are available in CCPS (1992).

The quality of the What-if study depends on the expertise and experience of the team. With a skilled team, the What-if study could be rapid and address most important issues. However, because the team does not systematically formulate What-if questions for the entire process, the results could be incomplete. The systematic alternative HAZOP method is presented in the next section.

**Relative Ranking**: Relative ranking involves evaluating key attributes of a process design to determine the relative hazards of the design. The basic concept is that process's hazard depends on the attributes regardless of the specific design, assuming that good design practices are followed. Generally, a score is given for each attribute in the process, and the total score provides an indication of the level of hazards posed by the process. Since detailed process designs are not required, the relative ranking methods are especially useful during process development and early stages of a process design, enabling the management team to select the best process for commercialization based on the safety and economics of competing process candidates. In addition, relative ranking method can be used to determine insurance rates.

The skill and engineering time requirements are modest for relative ranking. Also, one engineer can complete the relative ranking for a process. The complex team approach required for most other safety analyses is not required because of the well-defined scoring procedures.

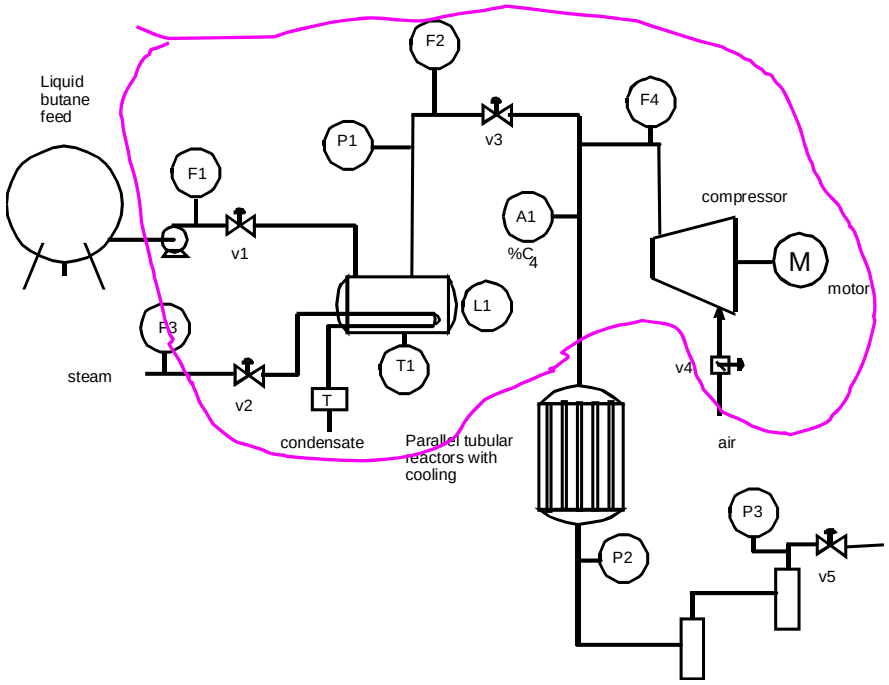



**Figure 5.19**. Butane vaporizer process for a maleic anhydride process. The equipment considered in enclosed in the envelope.

There are many methods that apply this general concept, each considering different key attributes. The more prominent are the following.

- Dow's Fire and Explosion Index, Dow's F&EI (AIChE, 1994)
- Dow's Chemical Exposure Index, Dow's (AIChE, 1994)
- Mond Index (Tyler, 1985)

These indices were developed by Dow Chemical Company. The first two have been made available to the public through the American Institute of Chemical Engineers, and a good reference for the Fire and Explosion Index is Suardin (2005).

Only one of these indices, the Dow's F&EI, will be discussed here. The method uses the form shown in Table 5.4, with supporting guidance given in the supporting manual (AIChE, 1994).

**Example 5.10** We will evaluate the DOW F&EI for a sample process, which is the butane vaporization process for a butane to maleic anhydride process in Figure 5.19. For the general hazard section, there are no reactors in the vaporizer section. For the special hazard section, (a) butane and air are mixed, (b) the maximum pressure is about 485 kPa, (c) about 30 gallons of butane is stored in the vaporizer vessel, and (d) a pump and compressor add some risk of leaks.

**Table 5.4. Dow Fire and Explosion Index completed for a vaporizer process.**

| **Material Factor (Butane)** | | **21** |
|---|---|---|
| **1.0 GENERAL PROCESS HAZARDS** | **Penalty Factor range** | **Penalty factor used** (0 is no penalty) |
| **BASE FACTOR** | 1.0 | 1.0 (if T > 140 F, see page 14) |
| A. Exothermic reaction **(not a reactor)** | 0.30-1.25 | 0 |
| B. Endothermic reaction **(not a reactor)** | 0.20-0.40 | 0 |
| C. Material handling **(not in this unit)** | 0.25-1.05 | 0 |
| D. Enclosed unit | 0.25-0.90 | 0 |
| E. Access | 0.20-0.35 | 0 |
| F. Drainage **(not defined in problem statement)** | 0.25-0.50 | 0 |
| **General Hazards Factor (F1) = sum of individual factors** | | 1.0 |
| **2. SPECIAL PROCESS HAZARDS** | | |
| **BASE FACTOR** | | 1.0 |
| A. Toxic materials **(0.20 * $N_h$ = 0.20*0.0 = 0 ($N_h$ = 0.0, short exposure under fire conditions has no toxic hazard)** | 0.20-0.80 | 0.0 |
| B. Sub-atmospheric pressure | 0.50 | 0 |
| C. Operation in near flammable range | | |
| 1. Tank farms | 0.50 | 0 |
| 2. Upset | 0.30 | 0 |
| 3. Always in flammable range (after mix point) | 0.80 | 0.80 |
| D. Dust | 0.25-2.0 | 0 |
| E. Pressure **(safety relief at 70 psig, 485 kPa; see Figure 2, page 22 in guidebook to obtain result)** | Based on Figure 2 | 0.25 |
| F. Low temperature | 0.20-0.30 | 0 |
| G. Quantity of flammable material | | |
| 1. In process (See Figure 3) **(30 gal of butane is below lowest value of x coordinate in Figure 3 on page 27 of guidebook, lowest value for the penalty is used: BTU = .0029 x $10^9$)** | | 0.10 |
| 2. In storage (See Figure 4) **(butane tankage not considered in this problem)** | | 0 |
| 3. Solids (See Figure 5) **(none)** | | 0 |
| H. Corrosion and erosion **(Don't have all data, used the lowest value)** | 0.10-0.75 | 0.1 |
| I. Leakage **(pump, no sight glass on vaporizer)** | 0.10-1.50 | 0.10 |
| J. Fired Heaters (See Figure 6) **(none)** | | 0 |
| K. Hot Oil System (See Table 5) **(none)** | 0.15-1.15 | 0 |
| L. Rotating Equipment **(compressor)** | 0.50 | 0.50 |
| **Special Hazards Factor (F2) = sum of individual factors** | | 2.85 |
| | | |
| **F3 = (F1) (F2)** | | F3 = (1.0) (2.85) = 2.85 |
| | | |
| **Fire and Explosion Index** | | **F&EI** = (F3 ) (MF) =(2.85) (21) = **60** |

**Table 5.5 Interpretation of Dow's Fire and Explosion Index (AIChE, 1994)**

| Dow F&EI | Degree of Hazard |
|---|---|
| 1-60 | Light |
| 61-96 | Moderate |
| 97-127 | Intermediate |
| 128-158 | Heavy |
| 159 up | Severe |

***In Table 5.4, the intermediate factors F1 and F2 give the contributions of the general and special process hazard factors, respectively. The intermediate factor F3 gives the contribution from the process conditions to the index. The final index value is the product of F3 multiplied by the material factor (MF) for butane that is 21 based on the guidebook. Using the interpretation Table 5.5, we conclude that the process is ranked to have a degree of hazard on the boundary between "light" and "moderate".***

Note the assumption that butane and air were in the flammable range. In reality, a control system is implemented to prevent the mixture from being in the flammable region; therefore, the analysis is conservative for the process section considered. Naturally, the entire plant, including raw material and product storage and highly exothermic chemical reactions would be analyzed to obtain a comprehensive hazard index.

In summary, the preliminary methods covered in this section provide good results for limited engineering effort and knowledge of process details. The checklists and What-if methods are useful for collecting experience from many professionals and from plant operations in a manner than can be easily applied to new designs. The relative rankings are especially useful in the early process develop of a plant. If the result of the evaluation indicates an unacceptably high risk, the engineer can modify the process, using different unit operations, solvents, reaction conditions, inventories, and so forth to reduce the risk to a tolerable level.

**Every engineer should apply these easy-to-use preliminary methods; however, these methods should not be used exclusively to verify the safety of a proposed design. Other, more systematic and detailed methods are required.**

Methods (HAZOP and LOPA) introduced in the next two sections enable engineers to identify potential hazards and integrate safety layers to achieve process designs that provide desired safety performance.

## 5.14 Hazards and Operability Analysis (HAZOP)

HAZOP has become the basic method for identifying potential hazards and defining design modifications to improve safety in the process industries. The method does not prescribe solutions; it provides a method for a team of engineers and operators to analyze a process, enabling everyone to focus their knowledge and experience in a systematic manner with the goal to ensure that all issues are addressed. Therefore, this general method can be applied to essentially all process plants.

A HAZOP analysis concentrates on safety issues, but it also seeks to uncover "operability" issues that could lead to poor economic performance, even if they do not lead to unsafe conditions. Examples of operability issues could be excessive manual operations that would delay production, lack of sufficient equipment for rapid startup, and inadequate measuring devices to enable plant personnel to monitor and diagnose potential incidents before they lead to equipment damage or large economic loss. In addition to improving economics, reducing operability problems contributes to safety, as discussed in the following examples.

- Operability deficiencies lead people to "quick fixes" that lead to accidents; for example, using an inappropriate hose for flow when the required pipe is not available (or has too small a diameter).
- Exceeding operating conditions of equipment can damage equipment and injure plant personnel; for example, operating a compressor at too low a flow rate can lead to surge (unstable flow) that could cause vane damage and metal flying around the equipment.
- Operability problems lead to frequent shutdowns that reduce the plant service factor; when the service factor is already low, the engineers are less likely to stop production to fix a potential safety issue.

While the HAZOP method was originally developed for process design, it is now routinely used for periodic safety reviews of existing plants and experiments. Since a multidisciplinary team collaborates on the analysis, nearly all chemical engineers will participate in HAZOP studies of designs, existing plants, or experimental equipment.

**Since HAZOP is widely applied for safety analysis and the general HAZOP method has been adapted for many additional applications, every engineer needs to be prepared to participate in HAZOP studies.**

To perform the HAZOP analysis, detailed information on the process is required. Therefore, HAZOP is applied to completed designs (before construction begins) and periodically to existing plants (where changes may have been made). Preparation for a HAZOP would include collecting the following information before the team begins its meetings.

- Production goals (rates, product qualities, etc.)
- Variability in inputs (feed materials, production rates, etc.)
- Chemistry (biochemistry) of reactions and separations
- Material and energy balances with pressures and temperatures (flowsheet)
- Physical and chemical data for materials, including toxicology and hygiene
- Process flow diagram
- Piping and instrumentation drawing (P&ID)
- Vessel drawings with materials of construction and pressure ratings
- Operating policies
- Inventory quantities
- Plot plan of equipment layout
- Experience with similar materials, units, and plants

When the plant (or experimental equipment) exists, the team should tour the equipment, control room, and other associated process equipment (flare, liquid waste treatment, and hydrogen generation units, boilers, so forth).

The essence of the HAZOP procedure is to investigate all significant deviations from a base case operation to determine (a) potential hazards, (b) the consequences of each hazard, and (c) modifications to eliminate or reduce the likelihood of the hazard. The procedure tacitly assumes that a safe and operable base operation is known; however, the base operation should also be evaluated during the HAZOP analysis. In fact, everything should be "challenged"; many (most) preliminary design features will be found adequate, but only through challenging everything does the team uncover the areas for improvement.

The results of the HAZOP are recorded on the form in Table 5.6. Some column headings in Table 5.6 use two terms because each of the two are used in documentation of HAZOP forms. The HAZOP team considers every node (location, procedure, etc.), selects important parameters (variables) of the node, and for every node/parameter combination considers key deviations or guidewords. When a hazard is identified, causes are clearly stated, consequences are described, safeguards in the initial design that tend to prevent the hazard or mitigate its consequence are identified, and new actions to improve the design are defined. In some versions of HAZOP documentation, the form in Figure 5.6 is expanded to include (1) a column that assigns follow-up actions to a specific person (essential for good management but not required for textbook problems) and (2) columns to define severity, likelihood, and risk (used in some forms to clearly document the basis for actions recommended). Whether or not the columns are included in the form, engineers must consider these consequences when proposing corrective actions appropriate for each possible event.

## Table 5.6 HAZOP form for Example 5.11*

| Company: XYZ Polymer Limited | | | Facility: Hamilton Works | | |
|---|---|---|---|---|---|
| Design Intent: Raise circulating oil stream temperature flowing at 100 $m^3$/h from 250 to 400 °C | | | HAZOP Team Members: | | |
| Drawing: Figure 5.20 | | | | Date: Jan 2, 2011 | |
| **1.0 Node: Pipe after feed pump before entering heater** | | | | | |
| **Parameter: Flow** | | | | | |
| ID. No. | Guideword / Deviation | Causes | Consequences | Safeguards/ checks | Actions |
| 1.1 | No Flow | a. pump motor failure | a. Fluid in pipe being overheated<br><br>pipe metal overheated and damaged<br><br>Pipe bursting and releasing oil into the firebox (in contact with flame)<br><br>Shutdown and loss of production | a. Reliable power supply to motor<br><br>low flow alarm | a. feed flow sensor and SIS on low flow<br>• Close fuel valves<br>• Open air valve<br>• Alarm with SIS<br>• Manual reset<br>• Short delay to guard against noise<br>• Manual activation of SIS possible<br>• Open stack damper<br><br>Low flow alarm using controller sensor |
| | | b. coupling failure | b. Hazard from metal pieces at high velocity | | b. Install guard over coupling |
| | | c. feed valve closure | See (a) above | c. Flow controller, valve fail open | See (a) above |
| | | d. Foreign material blocking flow | See (a) above | d. Filter upstream in process | See (a) above |
| | | e. No fluid available to pump | See (a) above | e. Level low alarm on vessel supplying pump | See (a) above |
| 1.2 | Further deviations ….. | | | | |

* The HAZOP form must contain an additional column on the far right that defines the person responsible for each action and the time when it should be completed. It is deleted here to save space.

Some HAZOP forms include columns to provide detail on the importance of the consequences. The columns document the severity, likelihood, and risk, usually using a numerical scale for each. These columns would be located between the “safeguards” and “actions” columns.

## Table 5.7 HAZOP form for Example 5.11 (continued)

| Company: XYZ Polymer Limited | | | Facility: Hamilton Works | | |
|---|---|---|---|---|---|
| Design Intent: Raise circulating oil stream temperature flowing at 100 $m^3$/h from 250 to 400 °C | | | HAZOP Team Members: | | |
| Drawing: Figure 5.20 | | | | Date: Jan 2, 2011 | |
| **2.0 Node: Pipe between the air compressor and control valve** | | | | | |
| **Parameter: Flow** | | | | | |
| ID. No. | Guideword / Deviation | Causes | Consequences | Safeguards/ checks | Actions |
| 2.1 | No Flow | a. compressor motor failure | a. no air to burner<br><br>fuel gas continues to flow into the hot firebox<br><br>explosion hazard<br><br>Shutdown and loss of production | a. Reliable power supply to motor | a. air flow sensor and SIS on low flow<br>• close fuel valves<br>• Alarm with SIS<br>• Manual reset<br>• Short delay to guard against noise<br>• Manual activation of SIS possible<br>• Open stack damper<br><br>Low flow alarm using controller sensor |
| | | b. coupling failure | b. Hazard from metal pieces at high velocity | | b. install guard over coupling |
| | | c. air valve closure | See (a) above | c. air controller, valve fail open | See (a) above |
| | | d. foreign material blocking flow | See (a) above | | d. install screen in compressor air inlet |
| | | | | | |
| 2.2 | Further deviations ….. | | | | |
| | | | | | |

* The HAZOP form must contain an additional column on the far right that defines the person responsible for each action and the time when it should be completed. It is deleted here to save space.

**Table 5.8 HAZOP form for Example 5.11 (continued)**

| Company: XYZ Polymer Limited | | | Facility: Hamilton Works | | |
|---|---|---|---|---|---|
| Design Intent: Raise circulating oil stream temperature flowing at 100 $m^3$/h from 250 to 400 °C | | | HAZOP Team Members: | | |
| Drawing: Figure 5.20 | | | | Date: Jan 2, 2011 | |
| **3.0 Node: flue gas stack above the air preheater** | | | | | |
| **Parameter: Temperature** | | | | | |
| ID. No. | Guideword/ Deviation | Causes | Consequences | Safeguards/ checks | Actions |
| 3.1 | Low temperature | a. excessive heat transfer in air preheater | a. condensation occurs in the stack<br><br>condensed water is very acidic<br><br>rapid corrosion of stack materials | | a. temperature sensor at node with display in remote control room, with low alarm, and values stored in history data base (T5) |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| 3.2 | Further deviations …….. | | | | |
| | | | | | |

* The HAZOP form must contain an additional column on the far right that defines the person responsible for each action and the time when it should be completed. It is deleted here to save space.

The most frequently used parameters (process variables) and guidewords (deviations) are given in Tables 5.9, and more extensive listings are available in Wells (1996) and Cameron and Raman (2005). The systematic use of node/parameter/guideword assists in identifying potential hazards. However, the proper evaluation of all causes and consequences relies on the HAZOP team's expertise and diligence. For example,

Node: pipe location specified (exactly)
Parameter: Flow
Guideword: No
Deviation: No flow rate

The team needs to consider all causes. Some typical causes for no flow in a pipe are given in the following.

- Blockage with process or foreign materials
- Control valve closed (caused by instrument air loss, controller or sensor malfunction, etc.)
- Manual isolation valve closed that should be open (Note, we must consider the possibility of human error.)
- No pressure differential (caused by cavitation in pump, pump or compressor stoppage, excessive upstream pressure, etc.)
- Leak in pipe
- Incorrect installation of one-way valve (allows flow in wrong direction)

In some cases, there will be a sequence of causes; for example, what caused the pump to not produce a head (pump motor, coupling between motor and pump, massive pump leak, etc.). Engineers improve their hazard identification through experience, use of checklists, and reference to technical references on equipment. Helpful guidance on causes of failures for typical process equipment is given in Wells (1996) and CCPS (1997).

Generally, the nodes are considered in a logical sequence, such as following the flow of material through the process, which ensures that all nodes are evaluated. The HAZOP procedure is systematic because it ensures that every node is evaluated, and it provides team coordination by having the entire team consider the same node at the same time, so that ideas can be shared. The price paid for thoroughness and teamwork is considerable engineering time; the study can be time-consuming and thus costly. Also, engineers consider HAZOP analysis demanding, which leads to a common recommendation that the team work on the HAZOP only a limited time per day, e.g., four hours/day, to keep the members fresh and productive.

**Table 5.9 Selected HAZOP parameters and guidewords**

| Parameter (variable) | Applicable Guidewords |
|---|---|
| Flow | No, more, less, reverse, |
| Temperature | Higher, lower (more, less) |
| Pressure | Higher, lower (more, less) |
| Level | Higher, lower (more, less) |
| Composition | No, more of, less, more than, other than |
| Chemical reaction | No, more of, less, more than, other than |
| Phase(s) | No, more of, less, more than, other than |
| pH, viscosity, humidity and other properties | Higher, lower (more, less) |
| Time sequence | Sooner, later, longer shorter |
| Sampling, checking, maintenance | No, more, less, more than, other than |

**To determine whether HAZOP analysis is worth the cost, you can imagine yourself standing in a location in the process and asking, "How thoroughly would I like the safety of this equipment to have been analyzed?"**

The HAZOP procedure is demonstrated in the following example.

**Example 5.11** The temperature of a process fluid in a pipe is increased from 250 to 400 °C in a fired heater shown in Figure 5.20. Fuel gas is combusted in the burner, and heat is transferred through radiation and convection to the fluid flowing through the pipe. You have been asked to perform a HAZOP analysis on the proposed design in Figure 5.20.

***We note that all information is not provided in this example; for example, we do not have detailed physical layout of the heater, nor do we have the material and energy balances. However, we have a simplified piping and instrumentation diagram with instrumentation and controls. So, we will proceed. (For some tutorial material on fired heaters, please refer to PGThermal (2010).)***

***We also recognize that a fault could occur upstream or downstream of the process considered that could affect the safety and operability of the heater process. Therefore, the documentation of the analysis must clearly define the process considered and what has not been considered. Only the process in the figure will be considered in this analysis.***

***A complete HAZOP study would be too lengthy to present here; so, only a few important issues will be considered in the example. The completed HAZOP forms for this example are given in Tables 5.6 to 5.8. The procedure is discussed in the following.***

***First Entry:***

- ***Node 1: Let's start by selecting a node. An exact definition of the node is important; for example, "the pipe at the exit of feed pump P-120 before entering the convection section" is better than "the pipe through which the feed flows", which does not define a specific location.***

- ***Node 1; Parameter 1: Now, we select a parameter. The most logical to start with is the flow rate.***
- ***Node 1; Parameter 1; Guideword 1: Now, we apply all appropriate guidewords to this node and parameter. Let's select "No" as the first guideword and enter "no flow" in the "deviation" column. Now, we proceed with an analysis of the situation.***
    - ***+ The causes of "No flow" could be***
        - ***(a) pump motor failure***
        - ***(b) coupling failure***
        - ***(c) feed valve closure***
        - ***(d) foreign material blocking the flow***
        - ***(e) upset upstream that stops feed availability***

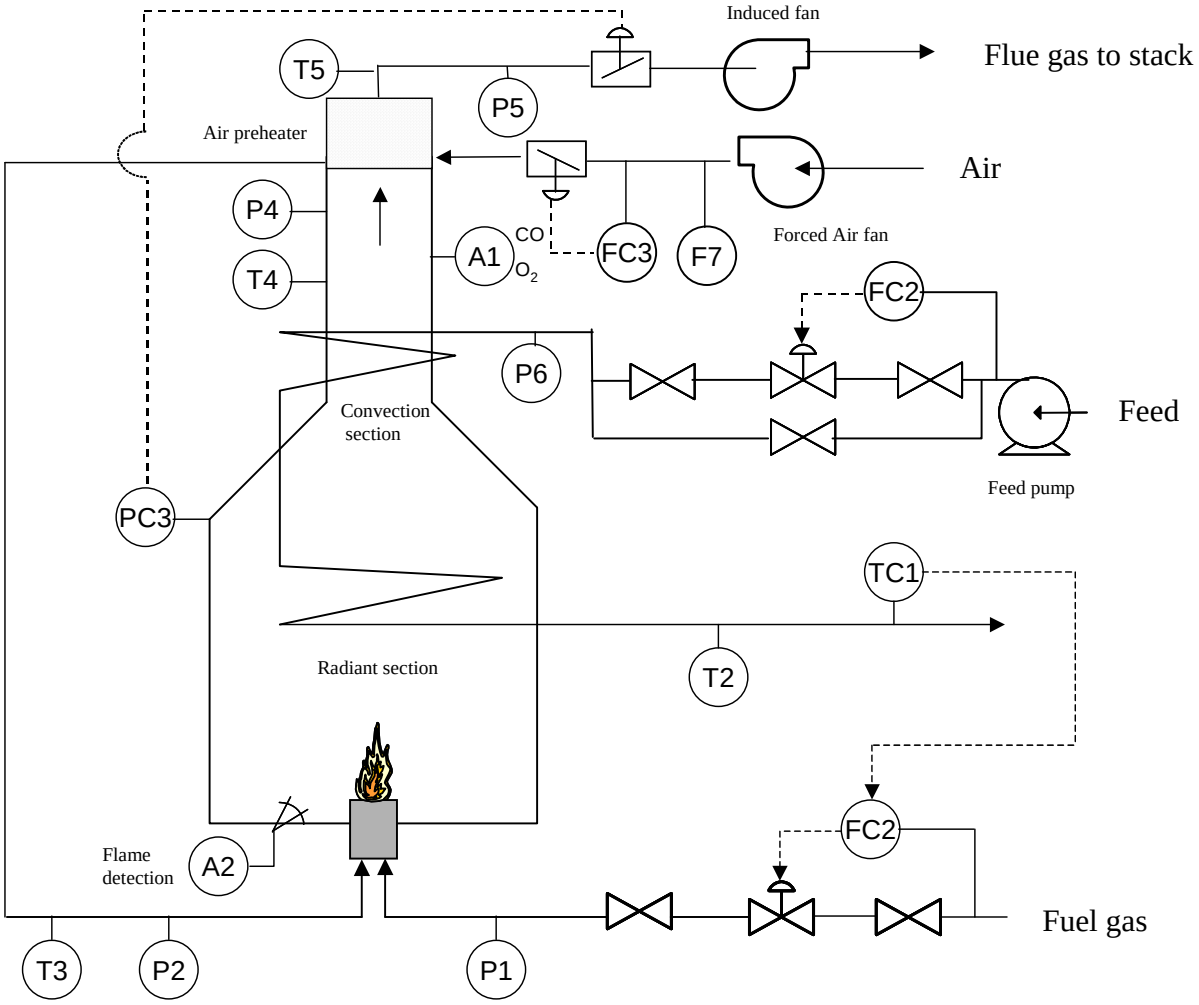



**Figure 5.20** Fired Heater drawing for Example 5.11
(Drawing has less detail than a P&ID and has only simplified instrumentation)

***+ The Consequences of "No flow" would be***

***(a) to (e)***

- ***fluid in pipe being overheated and decomposed***
- ***pipe in fire box being overheated and damaged***
- ***pipe in fire box rupturing, releasing fluid into fire box, leading to uncontrolled combustion***
- ***loss of production to downstream units***

***(b) metal pieces from broken, high-speed equipment could injure people and damage equipment***

*+ The Safeguards already in the design that contribute to safety*

*(a) reliable power supply to pump motor*

*(b) low flow alarm (but, using the same sensor for alarm and control)*

*(c) flow controller with fail open control valve*

*(d) level alarm low on feed tank*

***Before defining actions, the severities of the possible consequences are considered. The consequences for the node/parameter/guideword are severe; we conclude that changes must be made to reduce the risk significantly.***

*+ Node 1; Parameter 1; Guideword 1; Actions: We recognize that serious safety concerns and economic losses are associated with this scenario. Therefore, we must provide improvements that are termed "Recommendations" or "Actions".*

*(a) provide a SIS*

- *stopping fuel flow*
- *continuing air flow to the burners*
- *provide an alarm when the SIS activates, which should be common practice*
- *requiring manual operation for restarting the fired heater combustion system*
- *redundant flow sensor in the feed pipe*
- *providing a very short delay on the SIS, so that high frequency noise ("blip") in the measurement does not cause unrequired activation (so-called "nuisance trip")*
- *Open the stack damper*

*(b) provide a low feed flow alarm to give operators an early warning*

***As noted previously, to properly manage a large number of actions, the person responsible for each action and a deadline for the action to be completed. To reduce the size of the tables, this column is not included in the HAZOP forms in this chapter.***

***The HAZOP study would complete all parameters and relevant guidewords for the first node before proceeding to another node. To introduce new process concepts, we will select another node, parameter and guideword.***

***Second Entry:***

- ***Node 2: The pipe between the air compressor and the control valve in the system providing air to the burner.***
- ***Node 2; Parameter 2: Now, we select a parameter. The most logical to start with is the flow rate.***
- ***Node 2; Parameter 2; Guideword 1: Now, we apply all appropriate guidewords to this node and parameter. Let's select "No" as the first guideword and enter it in the "deviation" column. Now, we proceed with an analysis of the situation.***

*+ The causes of "No flow" could be*

*(a) compressor motor failure*
*(b) coupling failure*
*(c) air control valve closure*
*(d) foreign material blocking the flow into the compressor*

*+ The Consequences of "No flow" would be*

*(a) to (d)*

- *no air to the burner, resulting in the flame extinguishing, while fuel gas continues to flow into the firebox*
- *leaking air into the fire box could support combustion /explosion, resulting in extremely hazardous conditions*
- *major damage to large-scale and expensive equipment, shutdown to repair damage, resulting in loss of production*

*(b) metal pieces from broken, high-speed equipment could injure people or damage equipment*

*+ The Safeguards already in the design that contribute to safety*

*(a) reliable power supply to compressor*
*(c) air flow controller with air control valve fail open*

***Again, the severity of the possible consequences are considered, but not documented, before defining actions.***

*+ Node 2; Parameter 2; Guideword 1; Actions: We recognize that serious safety concerns and economic losses are associated with this scenario. Therefore, we must provide improvements that are termed "Recommendations" or "Actions"*

*(a) to (d) Provide SIS that will prevent damage on very low flow rate by*

- *providing a redundant flow sensor in the air pipe*
- *stopping fuel flow*
- *providing an alarm when the SIS activates, which should be common practice*
- *providing a very short delay on the SIS, so that high frequency noise ("blip") in the measurement does not cause unrequired activation (so-called "nuisance trip")*
- *requiring manual operation for restarting the burner flame*

*(a) to (d) Provide a low flow alarm that is significantly higher than the SIS activation value to give operators a chance to prevent SIS from activating, if possible.*
*(b) install guard over coupling*
*(d) install a screen at the compressor inlet to prevent foreign materials from entering the compressor.*

***A third node is included in the HAZOP form in Table 5.8, the stack above the convection section. The fired heater exchanges heat between the hot flue gas and the cool air in the convection section; naturally, this improves the efficiency of the heater by requiring less fuel to heat the air (in the flame). The flue gas consists of predominantly carbon dioxide and water, but it also contains sulfur oxides. Therefore, if the flue gas temperature falls below a limit, water will condense and the water will be acidic, causing severe corrosion of the convection section. The temperature sensor T5 is provided with a medium priority alarm to alert operators to monitor the stack conditions. When the convection section temperature exceeds its lower limit, and the operators are trained to make an appropriate response, such as***

***increase the air flow rate, which would lower heater efficiency but raise the stack temperature. For information on flue gas dew point see DKL (2010).***

**Readers can solidify their learning in this example by completing a node/ parameter/ guideword in a HAZOP form. It would be best to form a small team for this exercise.**

The three examples in Tables 5.6 to 5.8 constitute only a small part of the completed HAZOP study of the fired heater. Naturally, we do not have the space (and the reader might not have the patience) to cover all tabular entries. However, even this brief coverage demonstrates the following key strengths of the HAZOP method.

- A team leader with HAZOP training ensures that proper procedures are followed
- A multi-disciplinary team brings knowledge in many areas
- The method enables all team members to share concerns as they focus on one issue at a time
- The method is systematic in raising essentially all potential concerns for every node in the process.
- The method is very flexible, enabling engineers to apply it to essentially any process.
- As a well-accepted method, HAZOP results are easily interpreted and readily accepted by management

Although HAZOP has many advantages and is widely applied, engineers must recognize limitations in the method and guard against over reliance on HAZOP. Some potential weaknesses are noted in Table 5.10, along with factors that ameliorate the HAZOP method in response to each potential weakness.

As we see from the example, the HAZOP procedure enables engineers to thoroughly evaluate a process by systematically considering every location and process variable. Some arguments against HAZOP with replies are given in the Table 5.11.

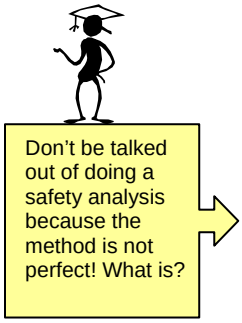
Engineers (and students) who learn the HAZOP method are gaining valuable knowledge for industrial practice. In addition, they are gaining much more. They are learning how to apply their basic engineering knowledge to solve new problems. They are also gaining appreciation for the importance of equipment behavior and detailed design. For example, the control valve failure position is no longer an abstract issue; it is critical to process safety. Also, a bypass valve location can either (1) provide needed flexibility with no effect on safety or (2) subvert an important safety barrier, resulting in an unsafe process. When performing HAZOP studies, engineers learn about the many types of failures that occur in process plants. The limited experience in HAZOP provided here should motivate and prepare engineers to learn much more through their experiences and self study.

**Table 5.10 Summary of HAZOP potential weaknesses with enhancements.**

| Weakness | Enhancement or complementary method |
|---|---|
| The procedure might not identify a low-frequency, high-consequence hazard caused by multiple, simultaneous failures. | Fault tree analysis is recommended for accidents that may be caused by multiple failures/events (CCPS, 1992). |
| The risks are not quantitatively estimated; thus, considerable judgment is required in deciding the actions. | Several complementary safety analysis methods can provide improved estimates, leading to better HAZOP action choices; one of these methods is the Layer of Protection Analysis (LOPA) covered in the next section. |
| Hazards will not be identified for a process fault that influences a nearby process. | Kletz (1999) recommends new guidewords such as “nearby” and “passing through”. |
| Since HAZOP is typically performed on finished designs or operating processes, fundamental changes to chemistry or equipment is usually not possible, without incurring large costs. | Preliminary methods were described previously in this chapter, and Kletz (1999) suggests a preliminary (coarse-scale) HAZOP to identify material and process synthesis issues early in the design procedure, when flexibility exists to address severe hazards. |
| The team may tend to provide overly complex safety barriers, especially control and SIS systems, that could have low reliability. Also, they might recommend a large number of alarms. | This is one reason for control and instrumentation engineers to participate in the HAZOP team. |
| HAZOP does not evaluate chronic hazards | This seems to be a valid point. The HAZOP team typically does not have expertise to evaluate the effects of long-term exposure to process materials, noise, and so forth. A separate review performed by a team with proper expertise is required. |

**Table 5.11. Some objections to HAZOP with responses**

| Objection | Responses |
|---|---|
| Our process is too simple | Example of a simple process is given by Kletz (1999). A proposed design is shown in Figure 5.20. Can you find hazards? |
| Our people are skilled | HAZOP requires skilled people and manages the process to obtain a thorough review, without inadvertent oversights |
| We use standard designs | Nearly every process has unique features. Only exact copies would not require an independent HAZOP analysis. |
| We haven't had an accident | Place "yet" at the end of the sentence! We recognize that most of the major industrial accidents in the last 40 years involved processes that had not previously experienced a serious accident. Infrequent, high consequence accidents are not avoided by learning from experience; they are prevented by removing hazards. |
| Human errors are not accounted for | Human errors can be accounted for under the "causes" column. (See also the next section on Layers of Protection Analysis.) |
| HAZOP is too expensive | Engineers abide by ethical standards in the practice of their profession. Safety is required by ethics and by law.<br><br>Even if human life had no value (an indefensible proposition!) the prevention of hazards would be justified by the economic savings. Costs are very high for damaged equipment, lost production, recovery of the environment, and so forth. |
| HAZOP depends on the skills and creativity of the team | This is true for nearly all human endeavors. The HAZOP procedure ensures excellent team participation and results documentation, which reduces the dependence on individuals to some extent. |
| The results depend on the veracity of the information provided | Well, of course! The study preparation is essential, and some follow up after the meeting may be required. |



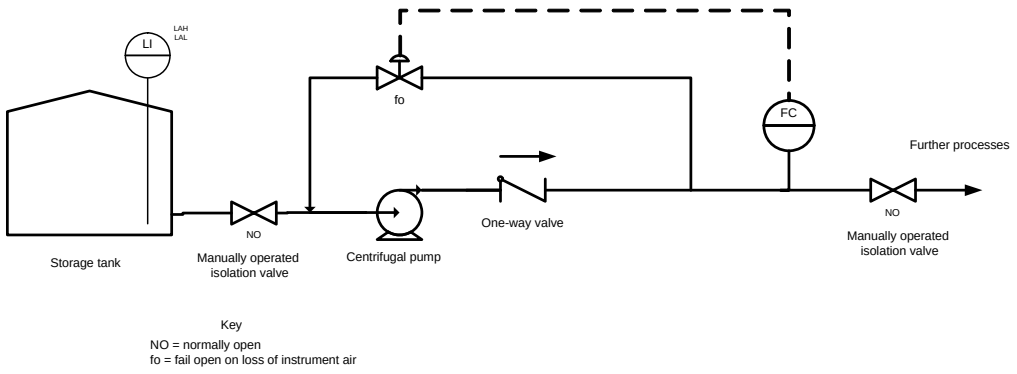




**Figure 5.21** Some people might (incorrectly) decide that a HAZOP study is not required for this simple process.

The troubleshooting topic will also reinforce the importance of equipment and detailed design!

**After studying the basics of HAZOP, engineering students will recognize the importance of learning about equipment behavior and detailed design.**

**Example 5.12** Let's complete this section with another HAZOP example. We will look at the simple process in Figure 5.21. The intent of the design is to provide fluid from a storage tank to a downstream unit. Some goals include (1) controlling the flow to the downstream process, (2) maintain a minimum flow through the pump, (3) prevent backflow into the tank, and (4) be able to isolate the pump for maintenance without draining fluid from the tank and downstream unit.

***The HAZOP form with a few entries is given in Table 5.12. The original design did not satisfy the goals defined in the problem statement; it allowed backflow into the tank, did not ensure minimum flow through the pump and could not control the flow rate to the downstream unit. A modified design is shown in Figure 5.22. Controller FC-2 determines the flow rate to the downstream process. Controller FC-1 has a set point equal to the minimum required flow rate through the pump. It will open the recycle valve only when the flow measurement is below the set point. This design improves energy efficiency by recycling only when necessary.***

At the completion of the HAZOP study, many potential hazards have been identified, and corrective actions have been defined. However, each action typically involves a cost and an increase in complexity, so that each action should be justified by an improvement in operability and safety performance. Therefore, we might say that at the completion of the HAZOP, a set of "possible actions" has been defined. In the next section, a method is presented that can be applied to select the appropriate actions for each event.

That is how you become expert in safety analysis as well!

**A musician was in a hurry to arrive at the famous Carnegie Hall for her first performance. She lost her way (and was the only person in New York City without a GPS). She saw a person on the sidewalk with a violin case, so she asked, "How do I get to Carnie Hall?"**

**The answer she received was, "Practice, practice, practice!"**

**Table 5.12 HAZOP form for Example 5.11***

| Company: ABC Chemical Company Limited | | | Facility: Niagara Falls Works | | |
|---|---|---|---|---|---|
| Design Intent: Supply fluid at 20 $m^3$/h from tank to further processing. (Note: storage tank not included in analysis.) | | | HAZOP Team Members: | | |
| Drawing: Figure 5.21 | | | | Date: Jan 2, 2011 | |
| **1.0 Node: Pipe between tank and isolation valve** | | | | | |
| **Parameter: Flow** | | | | | |
| ID. No. | Guideword / Deviation | Causes | Consequences | Safeguards/ checks | Actions |
| 1.1 | No flow | a. isolation valve closed<br><br>b. liquid level in tank below the exit pipe connection | No flow to downstream process<br><br>Damage to pump when operated without flow too long | Recycle (kick-back) around pump, but designed improperly<br><br>Level alarm low (LAL) to warn operator that tank is nearly empty | Correct the flow control design.<br>• Minimum flow controller measures the flow through pump and adjusts the recycle valve<br>• Process flow controller measures flow to downstream and adjusts a control valve in the pipe. |
| 1.2 | High flow | a. Flow controller opens control valve | none | | None |
| 1.3 | Reverse flow | Pump stops | Improper material allowed to enter the tank | One-way (check) valve is in process pipe, but in the wrong location | Move the one-way valve downstream of the recycle pipe at exit of pump |
| | Further deviations considered …. | | | | |

* The HAZOP form must contain an additional column on the far right that defines the person responsible for each action and the time when it should be completed. It is deleted here to save space.

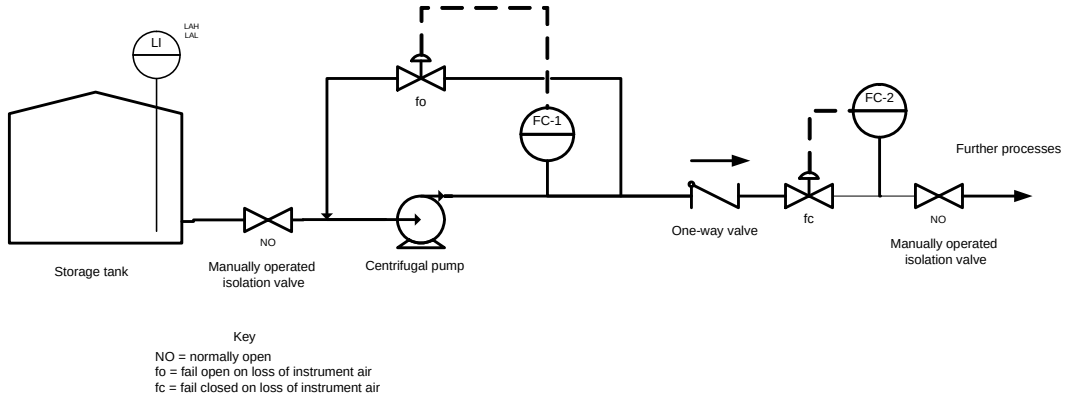



**Figure 5.22.** An improved design for the simple flow process in Example 5.12.

# 5.15 Layer of Protection Analysis (LOPA)

In layer of protection analysis (LOPA), we build on the results from the hazard identification and safety recommendations produced in the HAZOP study. The actions recommended in the HAZOP study should reduce the risk, but by how much? If too high a risk remains, we have not achieved a safe design. If the safety recommendations reduce the risk much lower than the target, we may unduly increase the cost and complexity of the design. (Naturally, an effective, inexpensive and simple design modification would never be rejected because it reduced the risk too much!) LOPA is used to ensure that the safety hierarchy with several layers of protection satisfies the desired (low) accident frequency. In predicting the accident frequency, LOPA applies a systematic, semi-quantitative method using established values for the performance of each layer. When performing the LOPA, the engineer may have to modify the preliminary HAZOP result to achieve the desired accident frequency.

In practice, LOPA is applied to only 5-10% of the HAZOP scenarios (CCPS, 2001), with the results of the remaining HAZOP scenarios accepted without further study. However, the HAZOP team uses the LOPA principles (and practical experience) in their qualitative analysis leading to proposed designs. When they feel that their experience is not adequate to ensure the design will perform safely, the team requires a LOPA analysis for the scenario.

We will apply LOPA concepts throughout process hazards analysis

**Therefore, mastery of LOPA methods is required for HAZOP (where we do a qualitative "LOPA in our head") and for more complex, selected scenarios with a formal, quantitative LOPA analysis.**

The basic approach of LOPA is to estimate the risk for the process with modifications proposed in the Prior HAZOP study included. Then, the total (mitigated) risk is determined, which is easily evaluated when each protective layer is effective and independent of the others layers. The concept is shown in Figure 5.23. The independent protection layers (IPLs) are designed in a series, so that the unsafe condition occurs only when all layers fail to function simultaneously. The following criteria have to be satisfied for a barrier to qualify as an IPL.

- **Effective** –To ensure an IPL layer qualifies as an effective IPL, the following must be satisfied.
  - + **Sufficient Capacity** – The process equipment associated with the protection layer (valves, piping, exchanger area, flare combustion, etc.) must have sufficient capacity to prevent the worst-case disturbance from leading to an accident.

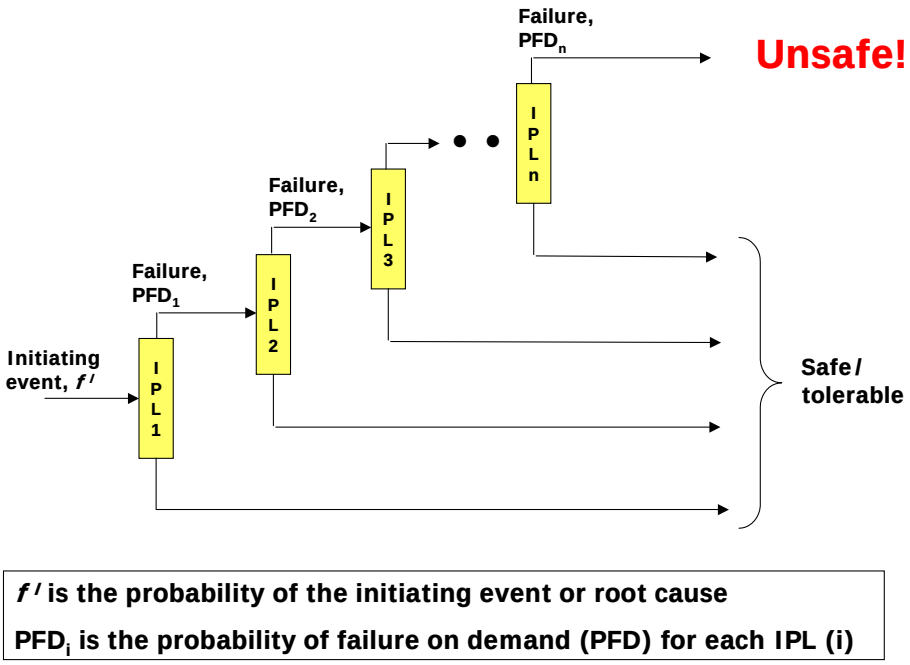



**Figure 5.23** Schematic of safety barriers between an initiating event and an unsafe condition. The independent protective layers (IPL) are in series, so that the success of any one of the barriers prevents the accident. The IPL probabilities of failure on demand (PFD) are independent for well-designed systems.

+ **Timely detection and compensation** – An IPL must detect the situation early enough so that the accident can be prevented or mitigated by action associated with the IPL, either automatically or by through people's actions. Thus, the dynamics of the process are important; the corrective action must have a fast enough effect to prevent the undesired consequence.

- **Independence** – Each IPL must be independent of all others. For independence, IPLs should not share a power supply, use the same equipment, rely on the same person for activation, or require the same maintenance actions. For example, the functioning of an alarm is independent of the functioning of a safety valve. Lack of independence could be caused by the use of a common (electrical or air) power supply, sensor, signal transmission, maintenance procedure, and so forth.
- **Auditable** – An IPL's performance must be able to be tested periodically. It might be necessary to place the IPL out of service for a very short time during the audit; if so, the safety of the process must be analyzed during the audit; perhaps, a parallel system, such as a second safety valve, would be required.
- **Reliability** – The equipment must perform its function with a high likelihood of success.

- **Access Security** – The ability to modify the functionality of the IPL must be limited by key lock, secure password, lockout, or other method to prevent unauthorized changes that could degrade safety performance.
- **Management of Change** – Changes to the IPL must be reviewed and authorized by an acceptable safety review process.

**Note that achieving the IPL criteria is the result of careful design and installation to provide high reliability; the criteria are <u>not</u> chosen arbitrarily to simplify the calculations.**

We seek to determine the probability of the accident, i.e., a consequence that leads to harm or damage. We must know or estimate the frequency of the root cause of the potential initiating event and the frequency that the failure will proceed to an accident, which is the probability of all protective layers failing to function properly. The method for calculating the frequency for a single initiating event is given in the following equation.

$$f_i^C = f_i^I \left[ \prod_{j=1}^{n} (PFD)_{ij} \right] \tag{5.4}$$

where
$i$ = scenario or event
$j$ = IPL layer
$f^I_i$ = frequency of initiating event (I) for scenario i
$f^C_i$ = frequency of consequence (C) for scenario i
$PFD_{ij}$ = frequency of failure on demand of layer j in scenario i

Clearly, this analysis must be performed individually for each key initiating event (i). The event identification has already been performed in the HAZOP study. As previously noted, the HAZOP team will be confident that they can provide a design based on qualitative analysis and experience for many scenarios. However, the team likely will not be confident in such analysis for very high consequence scenarios and for scenarios with which the team has limited or no experience. These more complex, higher consequence scenarios will be selected for the more through LOPA analysis. The relationship between HAZOP and LOPA is shown in Figure 5.24.

To perform the LOPA, we must have a target (maximum) accident probability and all of the data to calculate the accident probability likely to occur with a candidate design. When the LOPA is performed for safety, the F-N plot (similar in format to Figure 5.17) can be used to determine the frequency of occurrence that provides a tolerable risk. Some companies extend the application of HAZOP and LOPA analysis to ensure a low frequency of accidents that result in either environment harm or large economic loss. When LOPA is used for these purposes, the company must establish a maximum tolerable risk for various severities of environmental harm or economic loss. CCPS (2001) gives some examples for non-safety risk categories.

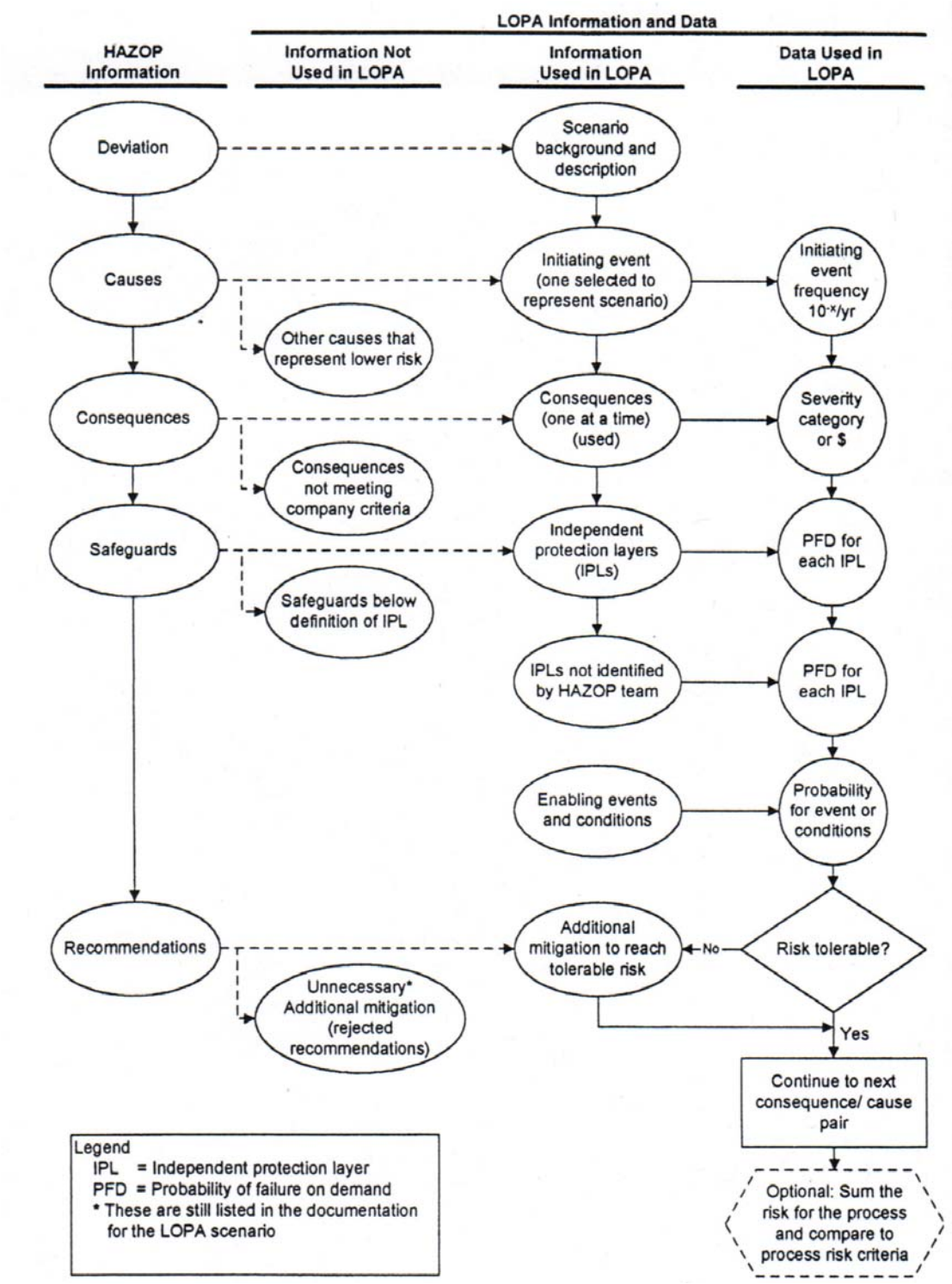



**Figure 5.24** Relationship between HAZOP and LOPA.
(Reprinted by permission. Copyright 2001 Wiley, CCPS (2001) *Layer of Protection Analysis*, Simplified Process Risk Assessment, American Institute of Chemical Engineers, New York Figure 4.6)

When the tolerable risk has been evaluated, the design must achieve this performance, which requires the following inequality to be satisfied.

$$f_i^C = f_i^I \left[ \prod_{j=1}^{n} (PFD)_{ij} \right] \leq f_i^{\max} \qquad (5.5)$$

with

$f_i^{max}$ = the maximum acceptable likelihood of mitigated occurrence

If necessary, we modify the design to achieve a sufficiently low consequence frequency. (If the risk were much below the maximum tolerable risk ($f_i^{max}$), we would not eliminate a low-cost layer to increase $f_i^C$!) The modifications tend to be either the addition of layers in the safety hierarchy layers or the "strengthening" of an existing layer (usually the SIS) that reduces its probability of failure on demand, $PFD_{ij}$. If the target safety performance cannot be achieved through these methods, a more fundamental change to the process equipment, flowsheet or chemistry would be required.

Note that the frequency from the F-N plot represents the cumulative risk from all causes, so that the frequency for a single potential accident must be lower. The frequency or risk that an accident will occur ($f_{accident}$) is the sum of all consequences from all initiating events identified in the HAZOP, if each initiating event is independent.

The LOPA calculation table is shown in Figure 5.25. Clearly, we need values for the terms in equation (5.5). Typical sources are summarized below.

| Data | Source |
|---|---|
| • The maximum frequency or probability of an accident, $f_i^{max} = F$ | The F-N plot or similar analysis. (A sample F-N plot is given in Figure 5.17.) |
| • Each event leading to significant hazard in the process ($i$) | HAZOP study |
| • Frequency of each event, $f_i^I$ | Historical data from a company or from publications |
| • The risk that each barrier to the accident propagation will fail on demand, $PFD_{ij}$ | Historical data from a company or from publications |

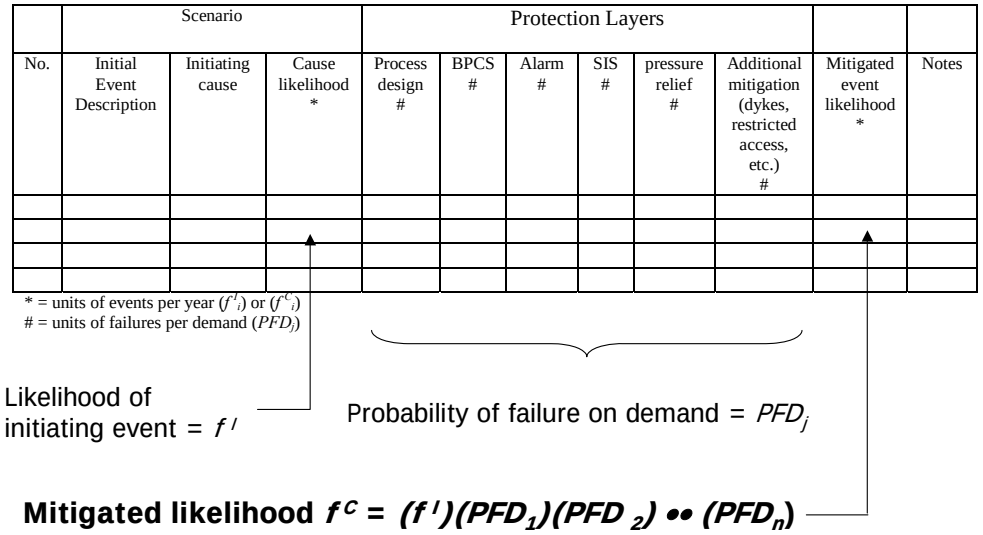



**Figure 5.25.** Layer of Protection Analysis (LOPA) worksheet. (Many variations of this worksheet are used in references and in practice.)

The applicable frequency data depend upon the design, installation and operation of the process equipment, and companies have differing standards for this detailed engineering. Therefore, the best source of data is the history for the company. However, a company may not have sufficient installations to collect a statistically meaningful amount of data, especially for equipment with low failure rates. Also, a company may begin a new business, in which it has no plant operating experience. Therefore, the use of some published data and guidelines seems unavoidable. Some typical data frequency data is given in Table 5.13, and more comprehensive data are given in CCPS (1989), Lees (1996, Appendix 14), and Skelton (1997). The reader is cautioned that these values are "typical", so that the frequency for a specific installation can differ significantly from the tabular value for an individual situation.

We need typical failure (PFD) values for the most often used technologies in each layer of protection, which are discussed in the following.

- **Process design** – The process structure and specific equipment design can affect the hazard, and if designed well could be a safety barrier. Some companies have detailed, documented design standards that provide better than average barriers. These companies claim a PFD of $10^{-1}$ to $10^{-2}$ for their designs, presumably based on historical data. These design standards are not available to the public, and different companies have different standards; therefore, we will use $10^0$ in this book to indicate no special reduction in consequence likelihood due to the application of standard process design technology, recognizing that lower values are possible with inherently safe design.

**Table 5.13 Typical Frequencies of Initiating Events ($f^I_i$)**
**(Data from CCPS, 2001, Table 5.1)**

| Initiating Event | Frequency (events/year) |
|---|---|
| Pressure vessel failure | $10^{-5}$ to $10^{-7}$ |
| Piping failure (full breach) | $10^{-5}$ to $10^{-6}$ |
| Piping failure (leak) | $10^{-3}$ to $10^{-4}$ |
| Atmospheric tank failure | $10^{-3}$ to $10^{-5}$ |
| Turbine/diesel engine overspeed (with casing breach) | $10^{-3}$ to $10^{-4}$ |
| Third party intervention (impact by backhoe, etc.) | $10^{-2}$ to $10^{-4}$ |
| Safety valve opens spuriously | $10^{-2}$ to $10^{-4}$ |
| Cooling water failure | 1 to $10^{-2}$ |
| Pump seal failure | $10^{-1}$ to $10^{-2}$ |
| BPCS loop failure | 1 to $10^{-2}$ |
| Pressure regulator failure | 1 to $10^{-1}$ |
| Small external fire | $10^{-1}$ to $10^{-2}$ |
| Large external fire | $10^{-2}$ to $10^{-3}$ |
| Operator failure (to execute routine procedure, assuming well trained, unstressed, not fatigued) | $10^{-1}$ to $10^{-3}$ (units are events/procedure) |

- **Basic Process Control (BPCS)** – The continuous control of flows, temperatures, pressures, levels, and compositions certainly has a major stabilizing effect on process operations. Most processes could not operate safety without the BPCS layer. Assuming good practice in the design, the PFD for this layer is typically $10^{-1}$, which means that 10% of the time that an initiating event occurs, the control system will fail to fully prevent the consequence. A lower (better) PFD could be achieved through redundant control loop designs; however, some standards restrict the PFD of the BPCS layer to greater than or equal to $10^{-1}$. The engineer should consult national standards when claiming a PFD less than $10^{-1}$ for process control.

- **Alarm** – The reliability of this layer depends on the instrumentation (sensor, signal transmission, and display) and the person. Since the instrumentation is typically much more reliable that the person (in an emergency), the PFD is basically the reliability of the plant operator to quickly and correctly diagnose the problem and implement an action that prevents the consequence. Some data on operator reliability is given in Table 5.14, and much more data is given in Kletz (2001). We note that PFD is strongly affected by the time before a corrective action is required and the stress level on the person. As discussed by Kletz (2001) the layout of the control interface can have a significant impact on the performance of the operator.

**Table 5.14 Human failure data***

| PFD | Situation description |
|---|---|
| 1.0 | Rapid action based on complex analysis to prevent serious accident. |
| $10^{-1}$ | Busy control room with many distractions and other demands on time and attention |
| $10^{-2}$ | Quiet local control room with time to analyze |

*Based on Kletz(1999)

- **SIS** – Recall that the safety instrumented system (SIS) automates logic-based, extreme actions to place the process in a safe condition. Typical actions of an SIS include stopping some equipment, maximizing cooling, stopping feed flow rate and/or diverting product flows to safe storage, processing, or destruction (e.g., combustion). Therefore, the cost of activation is high, which is why the two lower layers of protection exist to prevent the need for SIS to activate in all but the most extreme situations. As a result, we seek a SIS design that provides good (low) PFD and in addition, low frequency of expensive "false activation" or "spurious trip". False activation occurs when the process is safe but the SIS activates because of a failure in one of its components.

  The SIS is a computer-based control system that uses logic-based algorithms to decide the actions taken. We note some key SIS features, (1) the sensor(s) is independent of the control and alarm functions, (2) the signal transmission is independent from the control system (BPCS), (3) and at least one final element is independent of the BPCS loop. In addition, the calculation is performed in an independent computer, usually termed a programmable logic controller (PLC) or programmable electronic system (PES) that has software designed to be easily program logic-based decisions and control. The computer hardware and software are usually designed to ensure all control calculations and outputs are performed within some guaranteed maximum execution period, for example, 50-100 milliseconds.

  One of the key decisions made during a LOPA is whether an SIS is required and if so, what design is required to achieve the required mitigated frequency. Typically, the maximum tolerable frequency is determined by the consequence of the accident, and the frequency without SIS is determined. Then, the SIS design is determined (defining the PFD for the layer) to ensure that the mitigated frequency is lower than the tolerable maximum.

  The design of the SIS should achieve the desired PFD and simultaneously experience a very low frequency of activations (trips) due to SIS equipment failure when the process is operating safely. Remember that spurious activations can be very costly. Let's look at the sample SIS designs in Figure 5.26 that should activate and maximize a flow rate when a single process variable exceeds its limiting value.

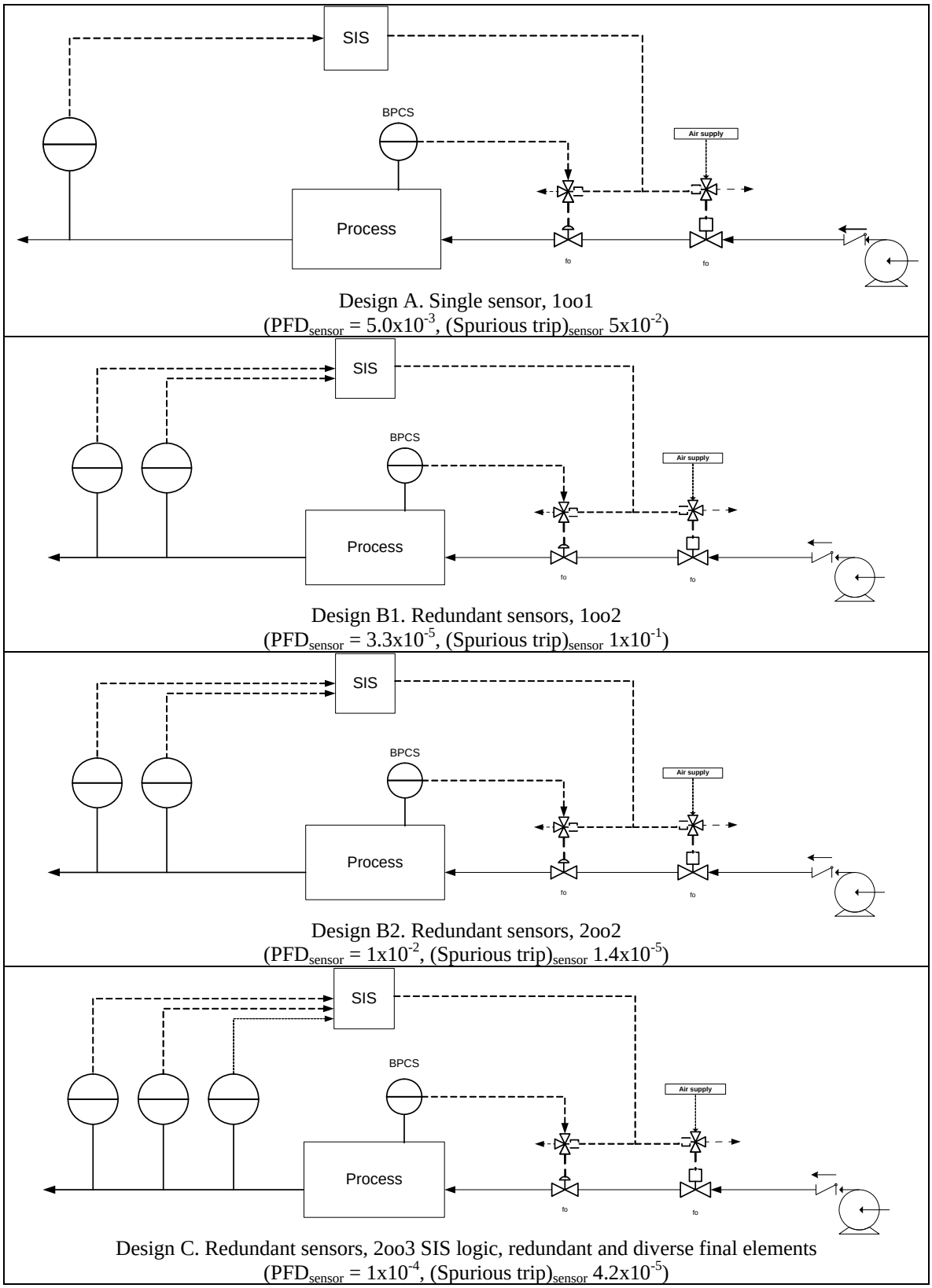



**Figure 5.26** Typical SIS designs with representative reliability values for sensors.
(Note "moon" means at least m sensors out of n total sensors must violate the limit for SIS activation.)

**Table 5.15 Typical Failure and Spurious trip frequencies***

| System configuration | System description*** | Probability of failure on demand (dangerous) | Spurious trip frequency |
|---|---|---|---|
| Single sensor | 1oo1 | $\frac{\lambda^D(TI)}{2}$ | $\lambda^S$ |
| Dual sensors, activation if one or two exceed limit (inclusive OR) | 1oo2 | $\frac{(\lambda^D)^2(TI)^2}{3}$ | $2\lambda^S$ |
| Dual sensors, activation only if both exceed limit# (exclusive OR) | 2oo2 | $\lambda^D(TI)$ | $2(\lambda^S)^2 MTTR$ |
| Three sensors, activation if two or three exceed limit** (voting logic) | 2oo3 | $\left[\lambda^D(TI)\right]^2$ | $6(\lambda^S)^2 MTTR$ |

* Equations from ISA (2002) and Beckman (1995)

** Repair for one sensor failure is assumed to be rapid

*** For moon, at least m measurements (of n total) must exceed the limit for the SIS to activate

The results for SIS sensor reliability in Figure 5.25 are determined using the "simplified" reliability formulas for various system configurations in Table 5.15 (ISA, 2002; Beckman, 1995) and the following data, which is typical for standard sensors (ISA, 2002).

Mean time to failure in dangerous condition = $MTTF^D$ = 50 years (=$1/\lambda^D$)
Time period between inspection/maintenance = TI = 0.5 year
Mean time to failure in safe condition = $MTTF^S$ = 20 years (=$1/\lambda^S$)
Mean time to repair after failure = MTTR = 24 hours = 1 year

Various references in the professional literature use different symbols for variables in these calculations. Therefore, both are introduced here.

$$\left(f^C\right)_{i=unsafe} = \lambda^D = \text{failure to activate for plant in a dangerous state}$$
$$\left(f^C\right)_{i=safe} = \lambda^S = \text{activate for plant in a safe state}$$

- **Design A** is the simplest; it has a single sensor. The SIS logic activates if the single measurement exceeds the limit. Design A has a relatively high PFD. It also has a moderate frequency of false or spurious activations; note that a single sensor failure can lead to activation.
- **Design B1** has moderate complexity; it has two sensors. The SIS logic activates if either (or both) of the measured values exceeds the limit. Here, the PFD is lower, because the SIS is less sensitive to a single sensor failing to indicate a fault, but the frequency of spurious activations is higher.
- **Design B2** has moderate complexity; it has two sensors. The SIS logic activates only if both measured values exceeds the limit. Here, the PFD is

much higher, even worse than the single sensor, because both sensors must sense a limit violation for the SIS to activate. However, the frequency of spurious activations is lower.

- **Design C** is of higher complexity; it has three sensors. The SIS logic requires two (or more) of the three measured values to exceed the limit for activation. This design has much lower PFD and lower frequency of spurious activations! The performance of Design C is superior, which is achieved through higher cost and complexity.

Note that the reliability results are for only the sensor component of the SIS. The reliability would be lower for the entire SIS system because of the many other components (SIS logic solver, signal transmission, final elements, power supplies, etc.) that could also fail. See Example 5.13 for a more complete analysis.

Calculation of the PFD for an SIS design requires knowledge of reliability and maintenance-time data for a specific company. Some sample PFDs for specific designs in this chapter use public-domain data; they give representative results for demonstration purposes. In addition, the PFD values demonstrate the relative performances of the SIS structures and can be used as typical values for well-designed SIS systems. Green and Dowell (1995) have developed some SIS designs using publicly available reliability and maintenance data and rigorous reliability calculations methods to determine the PFDs. These designs provide valuable examples, and their rigorous methods can be applied when a problem's data differs from that used in their designs. Definitive presentation of simplified and detailed reliability calculations for SIS is presented in ISA (2002).

It becomes apparent that considerable care is required in designing the safety hierarchy. The team that performs a HAZOP study will likely have considerable engineering experience, and they will be able to select final designs for many scenarios without a LOPA. However, their experience is based on designs and guidelines completed using LOPA data and methods. As Green and Dowell (19995) point out, companies can have "cookbook" SIS designs to achieve common target failure and spurious trip frequencies. For unique scenarios in a HAZOP that involve high consequences and novel issues, cookbook designs cannot be applied, and a LOPA is required to finalize the safety hierarchy.

**The probability of failure on demand for a specific SIS design at a specific location should be determined using company-dependent reliability and maintenance data.**

A team is not required for the LOPA. Typically, one or two engineers with special training in LOPA methods will perform the calculations. One of the people doing the LOPA should have participated in the HAZOP study.

Finally, the SIS design and evaluation methods are rapidly coming under directives from international professional organizations. The general approach and

specific reliability equations in Table 5.15 conform to the ISA TR84.00.02 standard (ISA, 2002). However, this standard is being superseded by IEC 61511.

**The reader is cautioned to follow the most up-to-date standards for SIS analysis and design.**

Although some equations may change, the reader of the material herein should be able to understand and apply the new directives. The trend is clear, requiring more thorough analysis and detailed engineering for all layers of the safety hierarchy, especially the SIS.

- **Pressure Relief** – Safety relief valves and burst diaphragms are very reliable devices requiring no external power. The PFD usually used for these devices is $10^{-2}$. Note that achieving the desired value of the mitigated event likelihood without pressure relief does not justify a lack of pressure relief where required by government regulations or good engineering practice, e.g., on closed vessels or pipes.

- **Additional IPL systems** – Other equipment can reduce the undesired event likelihood; examples include dikes, containment buildings, and flame arrestors. The LOPA engineer must document the design, demonstrate that it satisfies the requirements for an IPL, and justify the PFD claimed.

  The values for each layer's probability of failure on demand, PFD, are summarized in Table 5.16. These are typical values; updated values for a specific design, installation, and maintenance should be determined for each company and location based on its data and procedures.

All sources of reliability data involve uncertainty, as discussed in Appendix 5.A. Given the uncertainty in the data, how can we be sure of the results? Well, we cannot be absolutely sure, but we can use the results as a best estimate, use the higher value of failure rates from a range of reported values (especially when dealing with high consequence accidents), and engage consultants with experience in specific equipment and safety designs. Engineers deal with uncertainty in economics, project scheduling, and technical calculations, so uncertainty in safety analysis is expected.

Kletz (2001) emphasizes the necessity to avoid "jiggling" the values, i.e., selecting the values (usually by using lower failure rates) to justify a simpler, less costly design. Such a practice would be unethical and could lead to serious consequences.

**Engineers are urged to, "call them like you see them" (CCPS, 1992), which means to make your best safety recommendations without being unduly influenced by cost, project deadlines, management's preconceived ideas and so forth.**

**Table 5.16 Typical PFD values for safety layers (IPLs)**

| Safety Layer (IPL) | Probability of failure of demand (failure/demand) |
|---|---|
| BPCS (process control) | $10^{-1}$ |
| Alarm | $10^{-1}$ to 1.0 (depends on stress and time) |
| SIS (safety instrumented system) | $10^{-1}$ to $10^{-4}$ (depends strongly on details of design and maintenance) |
| Pressure relief | $10^{-2}$ |
| Containment * | $10^{-2}$ for dike that will reduce consequences of spill<br>$10^{-2}$ for drainage system that will reduce consequences of spill |
| Other layers (IPLs) * | $10^{-2}$ for fireproofing<br>$10^{-2}$ for blast wall |

* These layers reduce only the major consequences of an accident. When doing a LOPA, the PFD would be 1.0 for many consequences; for example, a dike would not prevent a fire. The tabular values would be applied for only the worst consequences, e.g., for a dike, a spill flowing into the entire facility or the local community.

Now that the basics of the LOPA method have been introduced and typical data for initiating events and reliability of each layer supplied, we will demonstrate the LOPA method by evaluating a proposed design.

**Example 5.13** A few entries in the HAZOP form were completed for a fired heater in Example 5.11. In this example, we will follow-up on one of the entries, specifically Node 2, low/no air flow from the air fan to the burner.

The initiating event will be loss of air. The root causes could be inlet blockage, motor stoppage, coupling break, air valve to the non-fail-safe position, etc. Therefore, all of these HAZOP entries could be covered by this LOPA. Without mitigation, the air will stop and the fuel will continue to flow through the burner and into the hot firebox. This situation is a hazard because the fuel could mix with air leaking in to the firebox and explode. Based on the consequence, this qualifies as a major event deserving LOPA analysis.

***We begin our LOPA by setting a maximum mitigated frequency for this initiating event; again, this value depends on a consequence analysis, local legislation, and company policy.***

$$f^{\max} = 10^{-4}\, incidences / year$$

***Second, we determine the frequency of the initiating event.***

- ***Initiating event – From CCPS Taxonomy 3.3.4 (1989), the failure rate for an electric motor-driven centrifugal fan in continuous operation is 9.1 failures/$10^6$ hours. Using 8500 hr/year, the failure frequency is estimated to be 0.08 failures/year, which we will round to the following.***

$$f^I = 0.10 \text{ failures/year}$$

***Third, we consider each layer to the safety hierarchy except the SIS.***

- ***Process design – The design shown in Figure 5.19 conforms to general industrial practice, although it contains much less detail than an industrial design. The air flow rate would be more reliable if a second air fan with automatic startup were provided. However, the fan would be very costly; therefore, we will decide not to have the spare (at least for this initial analysis).***
- ***BPCS – The process control is typical. The control system will have no effect on the air flow after the flow has stopped for any of the root causes. If fact, since the cold fuel will not be combusted, the process temperature at the outlet of the heater will decrease, and the temperature controller will increase the fuel flow! This action exacerbates the hazard!***
- ***Alarm – A low flow alarm will bring the operators attention to the situation. This should be a high priority alarm. The correct action would be to immediately stop the fuel flow to the burner.***
- ***Pressure relief – The fired heater is not a pressure vessel. Any explosion would likely rupture the walls.***
- ***Containment – The hazard occurs within the process firebox; therefore, containment will not reduce the consequence. (Since the heater is several stories high, building a containment building around the heater is not practical.)***
- ***Emergency response – The fire crew should be trained in fighting fires for this process. Prompt action would prevent a fire from spreading, but it would not be in time or effective in stopping the fuel flow rate.***

***Fourth, we determine whether our preliminary design is adequate, as shown in Table 5.17 and below.***

$$f_i^C = f_i^I \left[ \prod_{j=1}^{n} (PFD)_{ij} \right] = (.10) * (1.0 * 1.0 * 0.10 * 1.0 * 1.0 * 1.0) = 10^{-2}$$

***We note that the consequence rate is too high (failure rate is too high), so that we conclude that the design without SIS is not adequate. This result is often communicated by the Gap defined below, which must be less than or equal to one for an acceptable design.***

| | | |
|---|---|---|
| ***This Gap is for the preliminary safety hierarchy design and is unacceptably large.*** | | $Gap = \frac{f_i^C}{f_i^{\max}} = 10^2 \geq 1.0$ ***Not acceptable!*** |

***A Gap of $10^2$ exists. This Gap can be satisfied by an SIS system, since the range of PFD for a SIS is given in Table 5.16 to be $10^{-4}$ to $10^{-1}$. The design to achieve the required PFD depends on the failure data for specific equipment, detailed design, and maintenance in a company. A typical design is given in Figure 5.27. The SIS activates when any one or more of the following conditions occur, which is a 1oo3 system.***

- ***The air flow rate sensor value is below its minimum value***
- ***The air pressure sensor value to the burner is below its minimum value***
- ***The flame detector does not locate a flame***

***The SIS activation reduces the air signal to two valves to atmospheric; since the valves are fail closed, the fuel flow will be reduced to zero. The design assumes a single SIS logic solver (computer). Typical reliability values and simplified calculation procedures (ISA, 2002) are used in the following calculations.***

***Sensor data: (all three sensors assumed to have the same failure rates)***
***Mean time to failure in dangerous condition = $MTTF^D$ = 30 years (=1/$\lambda^D$)***
***Time period between inspection/maintenance = TI = 1.0 year***
***Mean time to failure in safe condition = $MTTF^S$ = 5 years (=1/$\lambda^S$)***
***Mean time to repair after failure = MTTR = 24 hours***

***Valve data:***
***Mean time to failure in dangerous condition = $MTTF^D$ = 50 years (=1/$\lambda^D$)***
***(separate for block and solenoid)***
***Time period between inspection/maintenance = TI = 0.5 year***
***Mean time to failure in safe condition = $MTTF^S$ = 25 years (=1/$\lambda^S$)***
***(total for block and solenoid)***
***Mean time to repair after failure = MTTR = 24 hours***

***SIS Logic solver:***
***Mean time to failure in dangerous condition = $MTTF^D$ = 100 years (=1/$\lambda^D$)***
***Mean time to failure in safe condition = $MTTF^S$ = 10 years (=1/$\lambda^S$)***

***Power supplies: (De-energize is fail safe for air and electrical power)***
***Mean time to failure in dangerous condition = $MTTF^D \cong \infty$ years (=1/$\lambda^D$)***
***Safe failure rate = $\lambda^S$ = 0.05 (1/year)***

***Failure on demand calculations***

| | | |
|---|---|---|
| ***Sensors (1oo3 system)*** | $\frac{(\lambda^D)^3 TI^3}{4}$ | ***$3.7 \times 10^{-5}$*** |
| ***Final elements (block and solenoid in series, two sets in parallel*** | ***Series set*** $\lambda_{series} = \lambda_{block} + \lambda_{solenoid}$ ***Parallel (1oo2)*** $\frac{(\lambda_{series})^2 TI^2}{3}$ | ***$1.13 \times 10^{-4}$*** |
| ***SIS Logic solver*** | $\lambda^D$ | ***$0.5 \times 10^{-3}$*** |
| ***Power supply*** | $\lambda^D$ | ***~ 0*** |
| | | |
| ***SIS system dangerous failure rate*** | ***$f^D_{SIS}$ = Sum of individual failure of demands (occurrence/year)*** | ***$0.61 \times 10^{-3}$*** |

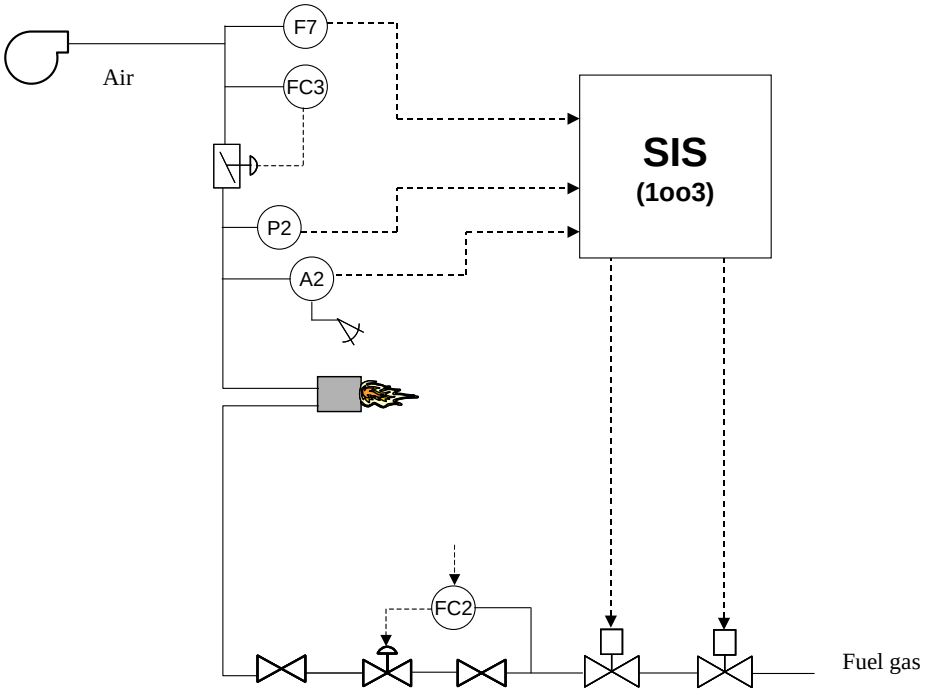



**Figure 5.27** Sketch of the SIS design for Example 5.13.

**Table 5.17 Layer of Protection Analysis for Example 5.13**

| | Scenario | | | Protection Layers | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| No. | Initial Event Description | Initiating cause | Cause likelihood * | Process design # | BPCS # | Alarm # | SIS # | pressure relief # | Additional mitigation (dykes, restricted access, etc.) # | Mitigated event likelihood * | Notes |
| | Loss of combustion air flow to burner | Fan, Valve, sensor | 0.10 | 1.0 | 1.o | 0.10 | | | | 0.01 | Original Design; Gap = 100! |
| | | | | | | | | | | | |
| | Loss of combustion air flow to burner | Fan, Valve, sensor | 0.10 | 1.0 | 1.0 | 0.10 | 0.01 | 1.0 | 1.0 | .0001 | Modified design for Example |
| | | | | | | | | | | | |

* = units of events per year ($f^{I}_{i}$) or ($f^{C}_{i}$)
# = units of failures per demand ($PFD_j$)

***Spurious trip calculations***

| | | |
|---|---|---|
| ***Sensors (1oo3 system)*** | $3\lambda^S$ | ***0.60*** |
| ***Final elements (block and solenoid in series, two sets in parallel*** | ***Series set*** $\lambda^S_{series} = \lambda^S_{block} + \lambda^S_{solenoid}$ | ***0.16*** |
| ***SIS Logic solver*** | $\lambda^S$ | ***0.10*** |
| ***Power supply*** | $\lambda^S$ | ***0.05*** |
| | | |
| ***SIS system safe failure rate*** | ***$f^S_{SIS}$ = Sum of individual failure rates (occurrence/year)***<br><br>***MTTFS = 1/failure rate (year)*** | ***0.91***<br><br>***1.1*** |

***The following performance for the SIS is predicted.***

***For modified design:*** $f_{SIS} = PFD_{SIS} = 0.60x\ 10^{-2}$ ***incidents/year***
$f^C = 0.60x10^{-4}$***..incidents/year***
***Gap = 0.60 < 1.0 OK!***

***Spurious trip period for SIS = 1.1 year***

***We see that the modified design satisfies the failure frequency target. Therefore, we would accept this design based on safety (with the caveat that the design should not be applied to a specific system without verifying the PFD using local reliability data). The relatively high frequency of a spurious trip would be of concern and could be reduced by including redundant sensors with voting logic.***

**For further discussion of SIS design and determination of the proper reliability, see Marzal, et. al. (1999) and Kenexis (2010).**

## 5.14 Conclusions

We have reached the end of a long and complex chapter, which is justified by the importance of the safety topic and the many engineering systems employed to achieve a safe design. The safety analysis covered in this chapter is summarized in Figure 5.28, which shows the major steps, key details at each step, and the people involved. This process is followed for both new designs and for periodic safety reviews of existing processes.

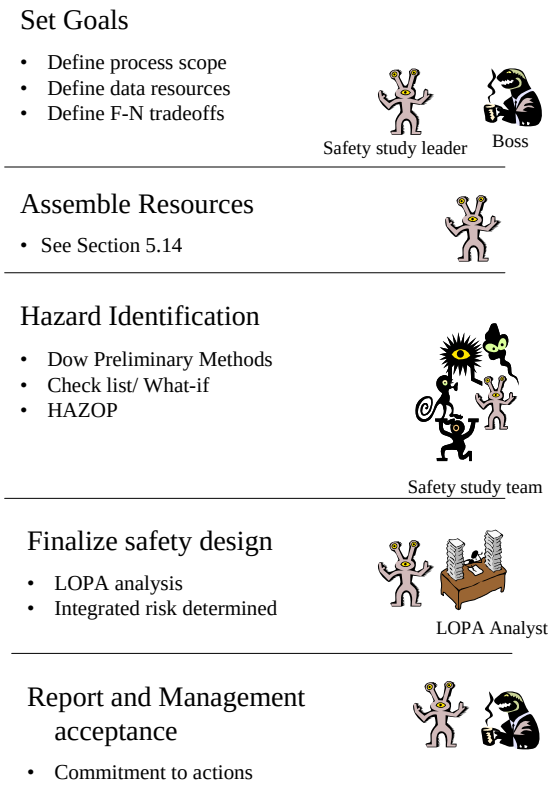



**Figure 5.28** Major steps in safety project with participants in each stage.

The engineer has much to gain from studying the safety hierarchy, methods for hazard identification and techniques to quantify risks and select appropriate designs. The following gives some benefits for the engineering student.

- **Safety is of primary importance** –Given the paramount importance of safety, we need to be sure that we master the topic and are aware of good practices, so that we can quickly identify and correct preliminary design errors before they become part of an installation. Sadly, engineers have made errors, and these errors have led to serious consequences for workers, environment and surrounding communities. In addition, major accidents have led to the restructuring of multinational companies and to a loss of confidence in engineers on the part of the public; for examples, investigate the accidents at Bhopal and BP Texas City. The material in this chapter is only the beginning, albeit an important first step, in building your safety competence.
- **Safety is everyone's business** – If you practice any type of engineering, you will need the skills and knowledge from this chapter. These safety designs and analysis methods apply to all industries, chemical, petroleum, food, minerals, pharmaceutical, and so forth. The emergence of new process technologies in biological and sustainable systems will result in many novel processes requiring

safety analysis without the benefit of decades of experience, an exciting but challenging task. Also, these principles also must be applied when making a device, such as an artificial kidney (dialysis unit). Finally, since safety reviews apply to operating processes as well as new designs, almost every chemical engineer will participate in HAZOPS, and many will consult during LOPA.

- **Problem solving** – HAZOP and LOPA are models for systematic problem solving. Strengths of the methods include a focused team approach, a systematic use of key words, a tabular form to summarize results as developed, and the quantitative analysis of complex issues. As a result, the HAZOP procedure has been adapted to many other applications, such as HACCP (Hazard Analysis and Critical Control Point) for product safety in food (FDA, 2010) and pharmaceuticals (WHO, 2003) and CHAZOP, HAZOP for plants with digital computer-based control systems (Schubach, 1997).
- **Integrated Operability** – Safety requires the application of the prior operability topics.
  + First, the safety systems, e.g., relief valves, cooling systems, and flares, must have the *capacity* (operating window) to compensate for the largest anticipated accident.
  + Second, the safety hierarchy must have the *flexibility* to utilize the equipment in the sequence intended by the hierarchy.
  + Third, the *reliability* of the integrated safety hierarchy must provide the overall reliability. As we will see, safety also relies on fast responses, so the dynamics of the process and safety equipment must be evaluated.
- **Engineering principles** – When working as a safety engineer, you will call upon all of the principles in the chemical engineers toolkit, and then some.
- **Equipment is important** – Engineers must understand the behavior of process equipment during both normal and fault conditions. The safety topic provides ample incentive to learn considerable detail about process equipment, especially how and why they fail. (The importance of equipment is further reinforced in Chapter 8 on Trouble Shooting.)
- **Becoming a safety expert** – While every engineer contributes to safety, every company needs engineers with special expertise to set standards, lead teams, and solve problems beyond the knowledge of the generalist.

**Perhaps, this chapter has whetted your appetite, and you would like to build a career as a safety engineer.**

BP Deepwater Horizon, April 20, 2010

## References


AIChE (1994) *Dow's Fire and Explosion Index Hazard Classification Guide, 7th Ed.*, American Institute of Chemical Engineers, New York

AIChE (1994) *Dow's Chemical Exposure Index, 1st Ed.*, American Institute of Chemical Engineers, New York

API (2007) Pressure Reliving and Depressuring Systems, ANSI/API Standard 521, 5th Ed., January 2007

Beckman, L. (1995) Match Redundant System Architecture with Safety Requirements, *CEP*, 54-61, Dec 1995

Bradsby, M. and J. Jenkinson (1998) The Management of Alarm Systems, Health and Safety Executive (UK) Contract Report, (1998) http://www.hse.gov.uk/humanfactors/topics/alarm-management.htm

Britannica: http://www.britannica.com/EBchecked/topic/250771/Haber-Bosch-process

Cameron, I. and R. Raman (2005) *Process Systems Risk Analysis*, Elsevier Academic Press, Amsterdam

CCPS (1992) *Guidelines for Hazard Evaluation Procedures (2nd Ed.)*, American Institute of Chemical Engineers, New York

CCPS (1993A) *Guidelines for Engineering Design for Process Safety*, American Institute of Chemical Engineers, New York

CCPS (1993B) *Guidelines for Safe Automation of Chemical Processes*, American Institute of Chemical Engineers, New York

CPPS (1989) *Guidelines for Process Equipment Reliability Data with Data Tables*, American Institute of Chemical Engineers, New York

CCPS (1998) *Guidelines for Design Solutions for Process Equipment Failures*, American Institute of Chemical Engineers, New York

CCPS (1998) *Guidelines for Pressure Relief and Effluent Handling Systems*, American Institute of Chemical Engineers, New York

CCPS (1998) *Guidelines for Design Solutions for Process Equipment Failures*, American Institute of Chemical Engineers, New York

CCPS (2001) *Layer of Protection Analysis*, Simplified Process Risk Assessment, American Institute of Chemical Engineers, New York

CSB (2007) Investigation Report, Refinery Explosion and Fire, Report No. 2005-04-I-TX, March 2007, U.S. Chemical Safety And Hazard Investigation Board http://www.csb.gov/assets/document/CSBFinalReportBP.pdf

Cheresources (2010), Last viewed December 2010, (http://www.cheresources.com/refnh3tanks.shtml)

Christofidies, P.D., Smart Plant Operations: Vision, Progress, and Challenges, *AIChEJ*, 53, 11, 2007.

Crosby (1997) *Pressure Relief Valve Engineering Handbook*, Technical Document No. TP-V300, Crosby Valve Inc. http://www.tycovalves-na.com/ld/CROMC-0296-US.pdf

Crowl, D. and J. Louvar (1990) *Chemical Process Safety: Fundamentals with Applications*, Prentice Hall

DOE (2004) US Department of Energy (DOE) Safety Handbook, DOE-HDK-1100-2004 http://www.hss.energy.gov/nuclearsafety/techstds (Search for: - Process hazard analysis, in list find - DOE-HDK-1100-2004)

DKL Engineering, Sulfuric Acid on the WEB™, http://www.sulphuric-acid.com/techmanual/Contact/contact_preheat.htm

FDA (2010) http://www.fda.gov/Food/FoodSafety/HazardAnalysisCriticalControlPointsHACCP/default.htm

Kenexis (2007) *Safety Instrumented System Engineering Handbook*, Kenexis Consulting Corporation, http://www.kenexis.com

Kuphalt, T. (2012) *Lessons in Industrial Instrumentation*, distributed under creative commons license, (**Thanks!**) http://www.openbookproject.net/books/socratic/sinst/

Green, D. and A. Dowell, How to Design, Validate and Verify Emergency Shutdown Systems, *ISA Trans*., 34, 261-272

Grossel, S. (1990) *J. Loss Prevention Process Industries*, 3, 112-124

Illidge, J. and Wolstenholme (1978), Hazards of the Oxyhydrochlorination Process for the Production of Vinyl Chloride, *AIChE Loss Prevention Symposium*, Atlanta, Ge, Feb 28-Mar 2, 1978.

ISA (2002) *TR84.00.02 Safety Instrumented Functions (SIF)-Safety Integrity Level (SIL) Evaluation Techniques, Parts 1-5*, Instrumentation, Systems and Automation Society, Research Park

Kletz, T. (2001) *An Engineer's View of Human Error*, Taylor and Francis, Rugby, UK.

Kletz, T. (1999) *HAZOP and HAZAN*, Institution of Chemical Engineers, Rugby, UK

Kragt, H. and J. Bonten, Evaluation of a Conventional Process-Alarm System in a Fertilizer Plant, *IEEE Trans Sys, Man & Cyber,* SMC-13, 586-600.

Lees, F.P. (1996) *Loss Prevention in the Process Industries, Volumes 1-3*, Butterworth-Heinemann, Oxford, UK

Marlin, T. (2000) *Process Control, Designing Processes and Control Systems for Dynamic Performance*, McGraw-Hill, New York

Mbeychok, (2012a) distributed under creative commons license, (**Thanks!**) http://en.wikipedia.org/wiki/File:Relief_Valve.png

Mbeychok, (2012a) distributed under creative commons license, (**Thanks!**) http://en.wikipedia.org/wiki/File:FlareStack_System.png

Marzal, et. al. (1999) Comparison of Safety Integrity Level Selection Methods and Utilization of Risk Based Approaches, *Process Safety Progress*, 18, 4, 189-194.

Pasman, H. and J. Vrijling (2003) Social Risk Assessment of Large Technical Systems, *Human Factors and Ergonomics in Manufacturing*, 13 (4), 305-316.

Reising, D and T. Mongomery (2005) Achieving Effective Alarm System Performance: Results of ASMÒ Consortium Benchmarking against the EEMUA Guide for Alarm Systems, P*roceedings of the* 20th Annual CCPS International Conference*, Atlanta, GA, 11-13 April 2005.*

PGThermal (2010), Furnaces and Fired Heaters, http://www.heaterdesign.com/design0.htm

Schubach, S. (1997) A Modified Computer Hazard and Operability Study Procedure, *J. Loss Prev. Process Ind*., 10, 5-6, 303-307.

Skelton, B. (1997) *Process Safety Analysis*, Gulf Publishing, Houston

Suardin, J., The Integration Of Dow's Fire And Explosion Index Into Process Design And Optimization To Achieve An Inherently Safer Design, M.S. Thesis, Texas A&M Universiy, August 2005. (http://repository.tamu.edu/bitstream/handle/1969.1/4145/etd-tamu-2005B-CHEN-suardin.pdf?sequence=1)

Trbojevic, V. (2005) Risk Criteria in the EU, ESREL'05, Poland, June 2005 http://www.risk-support.co.uk/B26P2-Trbojevic-final.pdf

Tyler, B. J. (1985) Using the mond index to measure inherent hazards, *Plant/Operations Progress*, Volume 4, Issue 3, pages 172–175.

Wells, G. (1996) *Hazard Identification and Risk Assessment*, Gulf Publishing, Houston

WHO (2003) *Application of Hazard Analysis and Critical Control Point (HACCP) methodology to pharmaceuticals,* World Health Organization Technical Report Series, No. 908, Annex 7 http://apps.who.int/prequal/info_general/documents/TRS908/WHO_TRS_908-Annex7.pdf

Woods, D. (1995) *Process Design and Engineering Practice*, Prentice-Hall, Englewood Cliffs

## Additional Learning Topics and Resources

The student or new practitioner might (mistakenly) assume that all current process designs are safe, so that copying a recent design ensures good safety practice. A review of the history of recent industrial accidents will dissuade the engineer, who can learn a great deal by reviewing accidents and locating design and procedural errors. The following is a book summarizing some industrial accidents.

King, R., *Safety in the Process Industries*, Butterworth-Heineman, London, 1990

Atherton, J. and F. Gil (2008) *Incidents that Define Process Safety*, CCPS/AIChE, Wiley, Hoboken

How about doing a little investigation on major industrial accidents? To get started, you can search the following accidents using one or more of the following key words using an Internet search engine.

Flixborough, Bhopal, Seveso, Three Mile Island, Chernobyl, BP Texas City, Piper Alpha, BP Deepwater Horizon

Two Internet sites with links to several accident reports: http://slp.icheme.org/incidents.html http://www.unu.edu/unupress/unupbooks/uu21le/uu21le00.htm#Contents

Trevor Kletz has been a leader in promoting safety in plant design and operations. We can all learn from the excellent case studies in his books and articles. The following is just one of his books.

> *Kletz, T. (2009) What Went Wrong? Case Histories of Process Plant Disasters and How They could have been Avoided (5th Ed.)*, Elsevier

Further information about Mr. Kletz and his publications can be found at (with the usual caution about information from Wikipedia) http://en.wikipedia.org/wiki/Trevor_Kletz

Inherently safe process design is an important first component of safe process design. The goal of inherently safe design is to eliminate or significantly reduce the causes of hazards, rather than just building a safety hierarchy around the plant. The principles of inherently safe design are introduced in the following references.

> CCPS (1993) Guidelines for Engineering Design for Process Safety, American Institute of Chemical Engineers, New York
>
> Kletz, T. and P. Amyotte, Process *Plants: A Handbook for Inherently Safer Design (2nd Ed.)*, CRC Press, 2010.

As chemical engineers concluded that safety should be strengthened in the undergraduate education, the need for a textbook became clear. Fortunately, the following books have been prepared.

> Cameron, I. and R. Raman (2005) *Process Systems Risk Analysis*, Elsevier Academic Press, Amsterdam
>
> Crowl, D. and J. Louvar (1990) *Chemical Process Safety: Fundamentals with Applications*, Prentice Hall, Englewood Cliffs
>
> Lees, F. (1996) Loss Prevention in the Process Industries, Volumes 1-3, Butterworth-Heinemann, Oxford (This is a massive resource, too expensive to purchase, but with very comprehensive coverage.)
>
> Wells, G. (1980) Safety in Process and Plant Design, Godwin, London

The Internet is a terrific source of information on Industrial safety and reports on industrial accidents. Here are just a few sites you may find interesting.

| Source of information | Internet address |
|---|---|
| Government and professional organizations providing reports and standards for manufacturing safety | |
| U.S. Chemical Safety Board that makes excellent reports and videos available without charge | http://www.csb.gov/ |
| US AIChE Center for Chemical Process Safety that publishes books of safety (at exorbitant prices) | http://www.aiche.org/ccps/ |
| American Institute of Chemical Engineers assists undergraduate safety education through the SACHE (member password required) | http://sache.org/index.asp |
| US Occupation and Safety Health Administration (OSHA), key OHSA site for industrial safety | http://www.osha.gov/pls/oshaweb/owasrch.search_form?p_doc_type=STANDARDS&p_toc_level=1&p_keyvalue=1910 |
| UK Health and Safety Executive provides many excellent studies and makes many available free for download. | http://www.hse.gov.uk/comah/sragtech/techmeascontsyst.htm |
| The European WEB Portal for Process Safety | http://www.safety-s2s.eu/index.php |
| World Health Organization<br>International Program on Chemical Safety | http://www.who.int/ipcs/en/ |
| International Society of Automation (ISA) safety standards | http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=8998 |
| International Electrotechnical Commission sets standards for safety instrumented systems | http://en.wikipedia.org/wiki/International_Electrotechnical_Commission |
| | |
| Additional Internet Resources | |
| US Public Broadcasting Network<br>Animation of Three Mile Island Incident | http://www.pbs.org/wgbh/amex/three/sfeature/tmiwhat.html |
| Many downloads with practical guidance on safety | http://www.iapa.ca/Main/Resources/resources_downloads.aspx |
| International Labor Organization (ILO) encyclopedia on Safety | http://www.ilo.org/safework_bookshelf/english/ |

# Test Your Learning

5.1. Proposed design for a distillation tower separating methane and ethane overhead from propane, butane and hexane bottoms is shown in Figure Q5.1. The separation is achieved at a pressure of 1.7 MPa. Critique the design and define changes required, if any.

5.2 HAZOP Study – A process has been designed to vaporize liquid butane and mix the butane vapor with air. The mixture will be fed to a chemical reactor to produce maleic anhydride. The preliminary design is presented in Figure Q7. The mixture of butane and air is critical because of the need to avoid the flammability composition region.

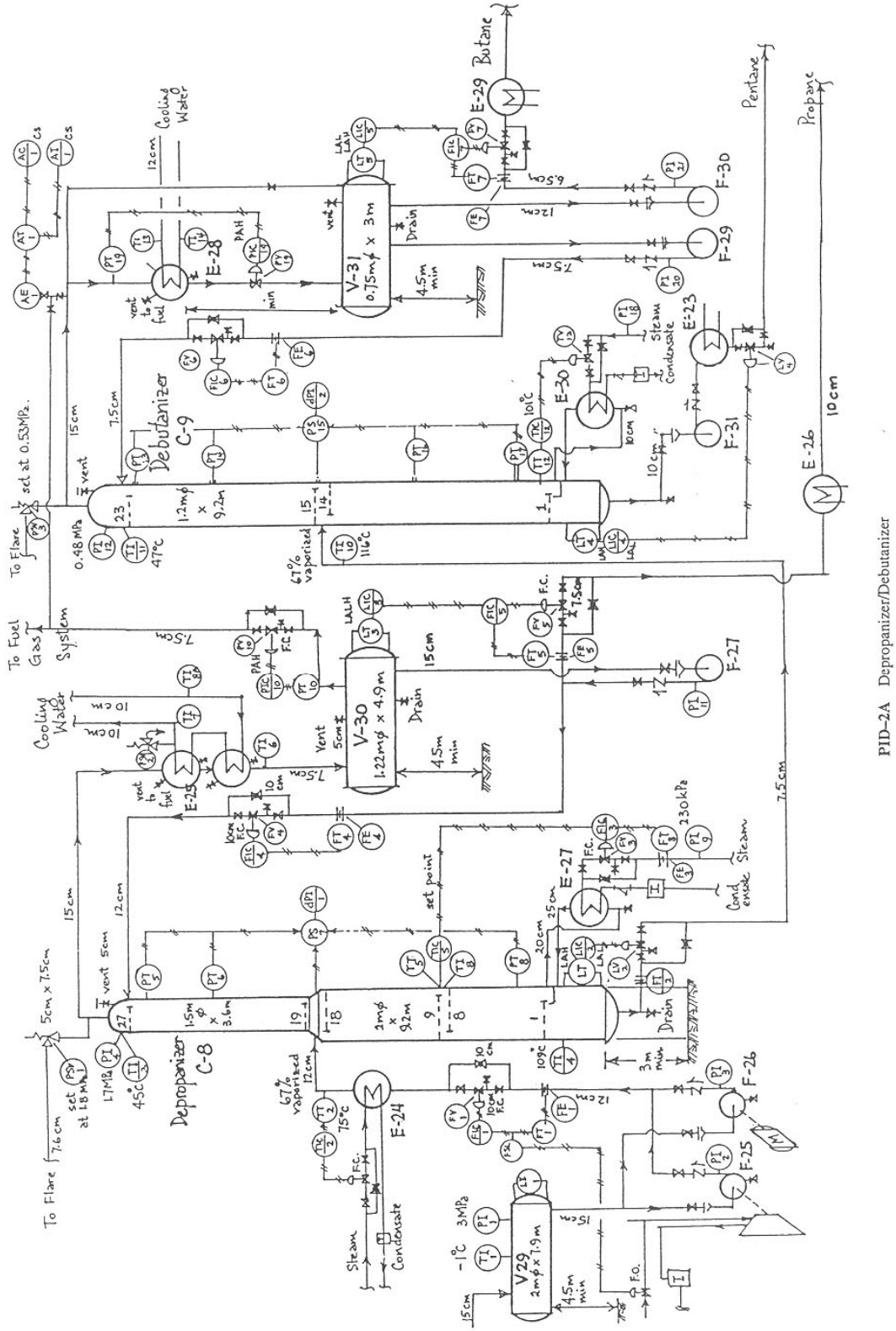



Figure Q5.1 Distillation Design
(From Woods, 1995)

You are asked to perform a HAZOP study of this process. Due to time limitations, please complete two different nodes with one parameter per node and one guideword per parameter. You should select nodes-parameter-guideword combinations that have a significant effect on safety.

Some references for the process:

- *http://www.che.cemr.wvu.edu/publications/projects/large_proj/maleic.PDF*
- *http://www.chemsystems.com/about/cs/news/items/PERP%200708_8_Maleic%20Anhydride.cfm*
- *http://www.sric.ch/PEP/Public/Reports/Phase_IV/RP046/RP046_toc.pdf (1969)*
- *T. C. Bissot, K. A. Benson, Ind. Eng. Chem. Prod. Res. Dev., 1963, 2 (1), pp 57–60*
- *DOI: 10.1021/i360005a014; Publication Date: March 1963*

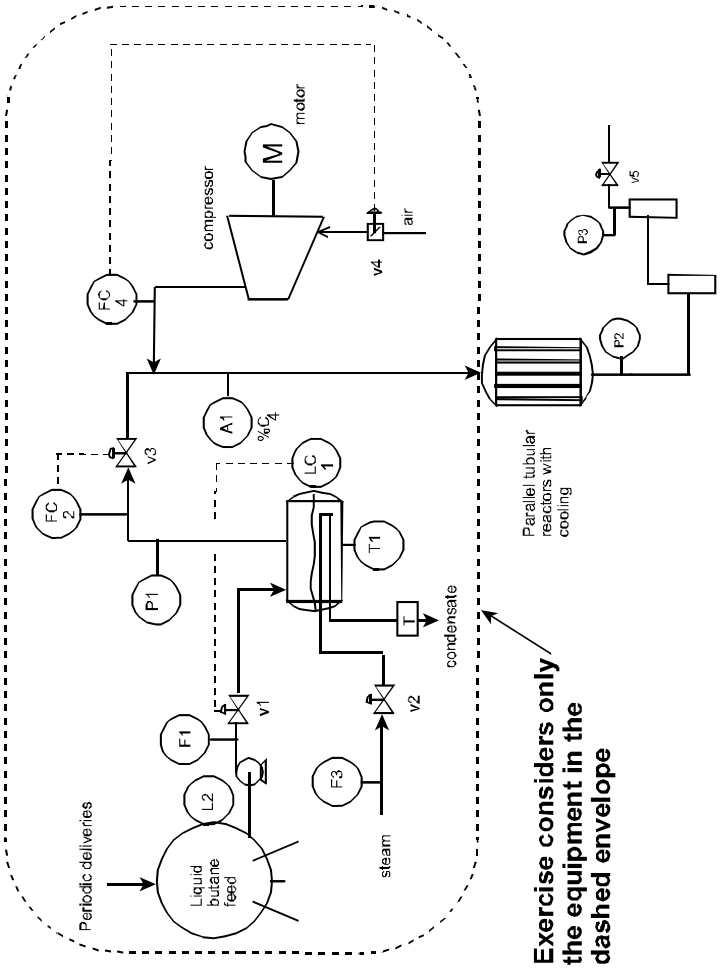



**Figure Q5.2** Proposed design for feed vaporization (may contain errors).

5.3.

a. Process control and SIS systems rely on sensors to provide reliable and accurate measured values. However, sensors can fail for a variety of reasons. Discuss several causes for a sensor to fail to provide a correct value.

b. Consider the temperature process controller in the CSTR reactor in Figure 5.8. If the temperature control were very important (for safety or product quality) and the possibility of sensor failure were not negligible, how could the design be modified to improve the reliability of the control system?

c. Consider the temperature SIS system in the CSTR reactor in Figure 5.8. If the temperature SIS were very important (for safety) and the possibility of sensor failure were not negligible, how could the design be modified to improve the reliability of the SIS system?

5.4.

a. In your first few days of work after graduation, you encounter the pressure relief design shown in Figure Q5.4a for a polymerization reactor. It contains a rupture disc and a safety relief valve in series! This seems strange to you. Is it correct?

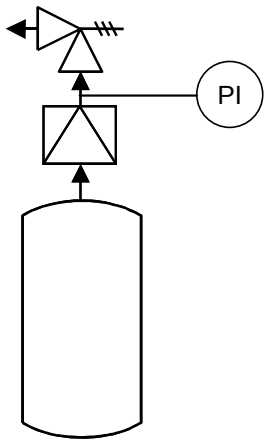



**Figure Q5.4a** Vessel with series rupture disc and safety relief valve.

b. In your first few days of work after graduation, you encounter the pressure relief design shown in Figure Q5.4b. The fluid in the vessel is a clean fluid, steam. The design includes two safety relief valves in parallel! This seems strange to you. Is it correct?

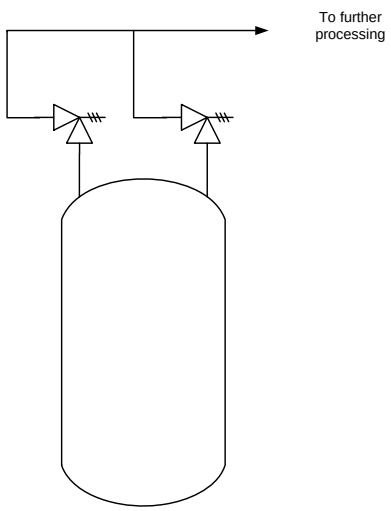



**Figure Q5.4b** Vessel with two parallel safety valves

5.5. The chapter has emphasized the importance of containing hazardous materials in vessels. However, piping and vessels can fail, resulting in releases to the atmosphere. How do we know when such a failure occurs and what can be done?

5.6. In some industries (for example, food processing and pharmaceutical manufacture), the process material can become contaminated. Discuss some special design features needed for food processing.

5.7. This chapter has not explicitly discussed how the process design affects the safety of a plant. Recently, engineers have inherently safer process plants by following the guidelines below.

- Intensification
- Substitution
- Attenuation
- Limitation of effects
- Simplification/Error tolerance

Discuss each of the guidelines and give a process example.

5.8. You have been asked to design a knockout drum like the one shown in Figure 5.13. The liquid level will be controlled by the sensor-pump-valve feedback control system, so that the liquid does not accumulate and overfill the drum. What information must you collect about the process and what calculations will you perform?

5.9. You have been asked to determine the height for a flare like the one shown in Figure 5.13. What information must you collect about the process and what calculations will you perform?

5.10. Process control and safety instrumented systems rely on feedback control systems. Discuss delays in the control equipment and how these delays could influence the effectiveness of each system.

5.11. Your supervisor has asked you if the process control, alarms, and safety instrumented systems in your design have appropriate **redundancy** and **diversity**. What is the meaning of these terms and how are they provided in typical process designs?

5.12. The importance of a valve failure position was discussed in the chapter. Is the sensor value upon failure important? Discuss and give reasons for special concerns.

5.13. When an alarm activates, no automated action is initiated, and plant personnel are required to diagnose and respond to the situation. Shutting down and subsequently restarting a process can require a long time and lead to substantial economic loss. Therefore, plant personnel seek to direct the process to a safe condition with the following properties: (1) safe, (2) smallest possible economic loss, and (3) fast return to normal operation. This is sometimes called “Safe Park” (Christofidies, 2007). The

proper actions for Safe Park are tailored for each specific process and root cause of the situation. Discuss some characteristics of a safe park condition for each of the three properties above.

5.14. Let's assume that a typical control loop has a failure frequency of once every ten years. For a plant with 700 control loops, how many control loop failures would occur during the thirty-year life of the plant. You may assume that all loops have the typical failure rate and that the loop failures are independent.

5.15. Complete the following table of key features for each layer of the hierarchy. Explain where the answer is not a straightforward "yes" or "no".

| Hierarchy layer | Power required | Action automated | Production continues (after layer activates) | Sensor needed | Final element needed |
|---|---|---|---|---|---|
| BPCS | | | | | |
| Alarm | | | | | |
| SIS | | | | | |
| Relief | | | | | |
| Containment | | | | | |
| Emergency response | | | | | |

5.16 Often, the control of a ratio is important for safety. Consider the case in which flow A must be maintained at a desired ratio to flow B, with flow B allowed to change (by manipulations from another control system or an operator). Your control system must adjust A to achieve the desired ratio.

a. Design a control strategy to satisfy the basic ratio objective.

b. Now, consider a situation in which the following are important for safety reasons: (i) the ratio of A/B should not fall below the desired value, even during transients and (ii) the flow of A can be limited by equipment, e.g., pump or compressor capacity. Enhance your design in part (a) to achieve ratio control and the two new objectives.

5.17 A proposed SIS design for a combustion control system is given in Figure Q5.17. Discuss the design and recommend changes, if needed.

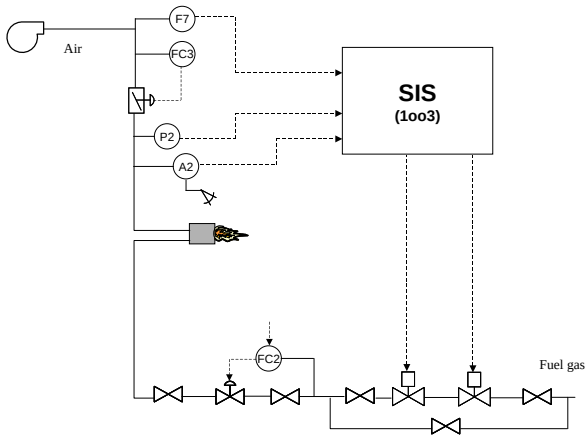



Figure Q5.17

5.18 The relief valve in Figure Q5.18 needs periodic maintenance and must be replaced every few years. We learned in the Chapter on flexibility how to provide isolation valves to enable repairs without shutting down the process. Sketch an appropriate design modification and discuss safety implications.

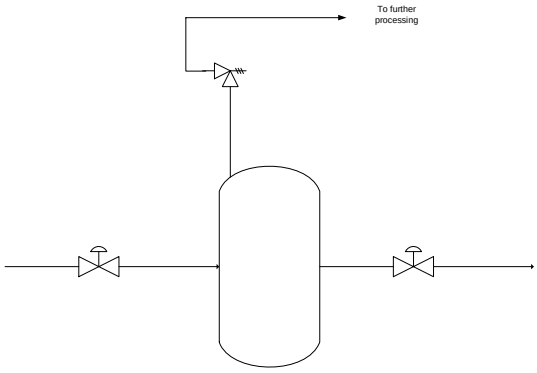



Figure Q5.18

5.19 Typically, process plant equipment and operating procedures change often in response to new understanding, changing economics, variation in feed materials, and so forth. How can we ensure safety in such a changing environment?

5.20 Previous Operability topics are given below. Discuss the importance of these for the safety hierarchy.

a. Operating window/equipment capacity
b. Flexibility
c. Reliability

5.21 The Oxychlorination process for the production of vinyl chloride involves a reactor with hydrochloric acid, oxygen and ethylene as feeds that are mixed. Mixing oxygen and hydrocarbons must be done carefully to prevent an explosion. The mixture percent oxygen is measured, and if the oxygen concentration is above a limit, the flow of oxygen must be stopped. Design a SIS for this very critical (high consequence upon failure) process to achieve a very low PFD in the unsafe condition.

5.22 A design for a feed section of an olefin dimerization plant is shown in Lawley , H. (1974) Operability Studies and Hazard Analysis, *Chem. Eng. Prog.*, 70, 4, 45-56. Perform a HAZOP study on this design.

5.23 Investigate the BP Texas City explosion using resources available through the Internet. Discuss the design of the distillation tower, pressure relief system, and downstream relief material processing. What layers of the safety hierarchy were properly and improperly designed and operated? You may use Figure Q5.23 to aid your discussion.

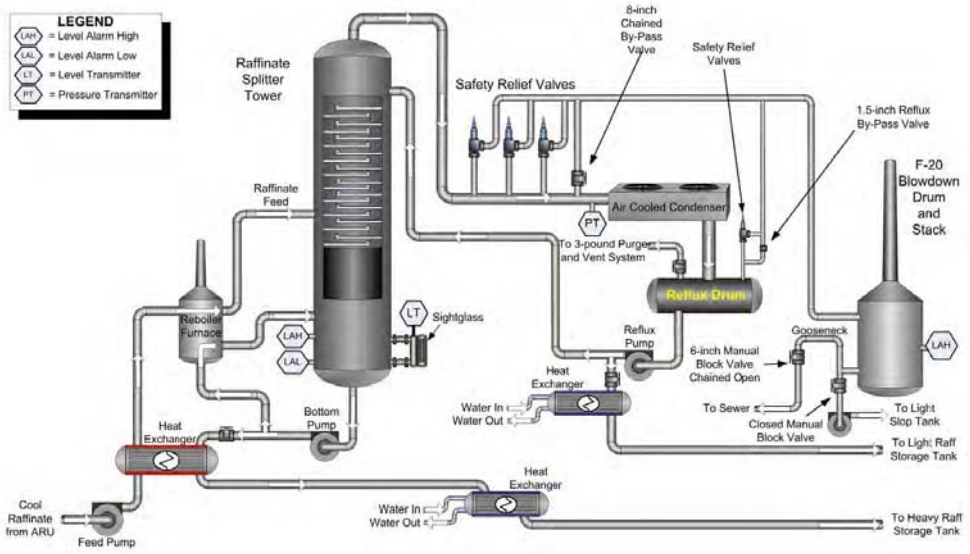



**Figure Q5.23** Schematic of BP Texas City Distillation and Blowdown system.
(from U.S. Chemical Safety And Hazard Investigation Board Investigation Report No. 2005-04-I-Tx, March 2007)

5.24 Example 5.13 presented an analysis of a proposed SIS for low air flow to the burner in a fired heater. Answer the following questions for the same heater.

a. Identify other conditions for the heater that would lead to hazards or equipment damage and require the heater to be shutdown.
b. Determine all actions that should be taken when the heater shutdown activates.
c. What is needed to enable the plant personnel to shutdown the process using the SIS?
d. What must be provided to alert the plant personnel that the SIS has activated?

5.25 An engineer could design a vessel with 10 safety valves in parallel. The standard calculation for the probability of failure on demand would give a PFD for the relief system of $(.01)^{10}$, which is $1x10^{-20}$. Discuss this result and whether 10 valves would have ten times lower PFD.

5.26 The design in Figure Q5.26 was placed in operation, and a high pressure occurred that resulted in an explosion. Critique the design and recommend improvements.

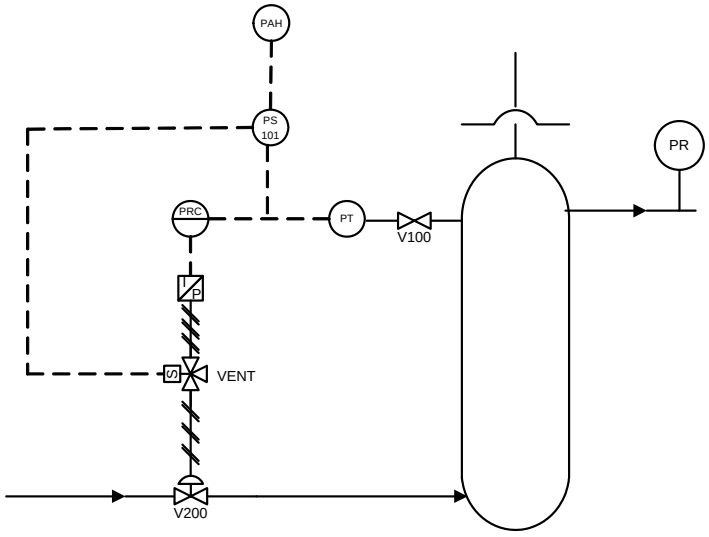



Figure Q5.26

5.27 Engineers have to make difficult decisions. Answer the following questions that define the goals of a safety study on a vinyl chloride monomer plant being designed to be located in your home city, within one kilometer of your family's house.

a. Sketch a F/N plot with values on the coordinates. Show the tolerable, ALARP, and unacceptable regions.
b. On the x-axis, define the equipment damage values for each factor of 10 change in the mitigated frequency.
c. On the x-axis, define the environmental harm (in words) for each factor of 10 change in the mitigated frequency.

5.28 HAZOP requires a skilled team. Propose a list of knowledge that should be included in the team.

5.29 Alarms and sensors for process monitoring are very important for plant operators when they have to diagnose and respond to abnormal situations. Consider each of these designs compare competing methods, both of which are used in practice. Discuss the advantages and disadvantages for each and recommend one of the designs.

a. The level alarm in the flash process could have either of the designs in Figure Q5.29a. In design (A) a separate light and annunciator are provided for the high level and for the low level; in design (B) one light and one annunciator are activated for either high or low level.

b. An alarm reports a discrete decision for the operator; however, the signals from the process can be continuous or discrete, as shown in Figure Q5.29b. In design (A) the sensor and transmitter determine whether the variable has exceeded its limit; if yes, it sends on discrete signal; if no, it sends a different discrete signal. For example, a level float could in normal conditions be below a switch, and in abnormal conditions, the float would rise with the liquid level and change the state of a switch. In design (B) the sensor

measures the variable and sends a signal to the control room for display. When the continuous measurement violated a limit, computing equipment in the control room could activate the alarm. The sensor could be any type of continuous sensor; for example, for a level measurement could be based on float position, differential pressure, or displacement.

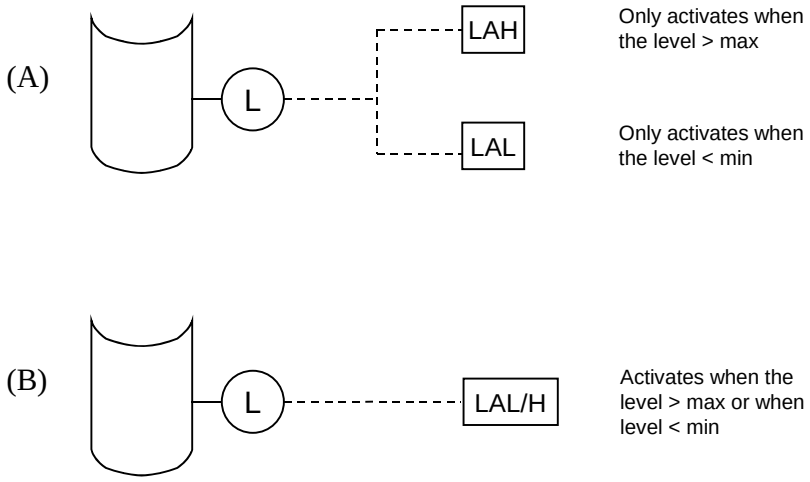



Figure Q5.29a

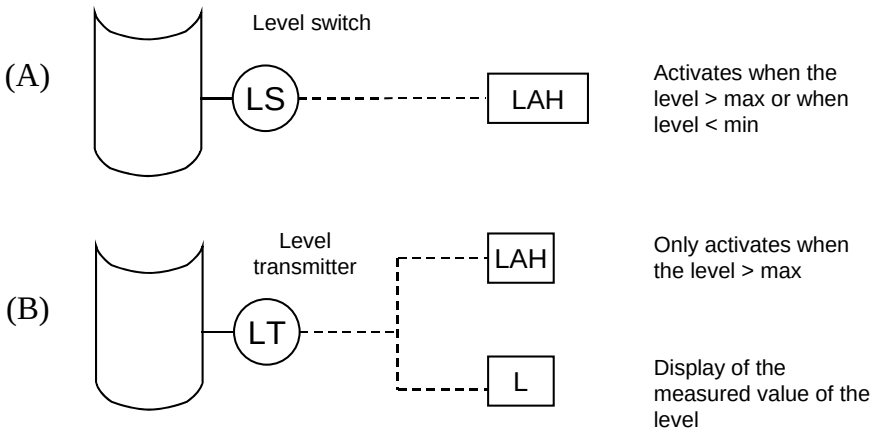



Figure Q5.29b.

c. For critical actions, the instrumentation system can confirm that the action has been taken. Consider the situation in Figure Q5.29c. In design (A), a light in the control room confirms that the signal is being sent to a remote operated valve to open. In design (B), a light confirms that the valve stem position has moved to the open position. What do we know and not know for each?

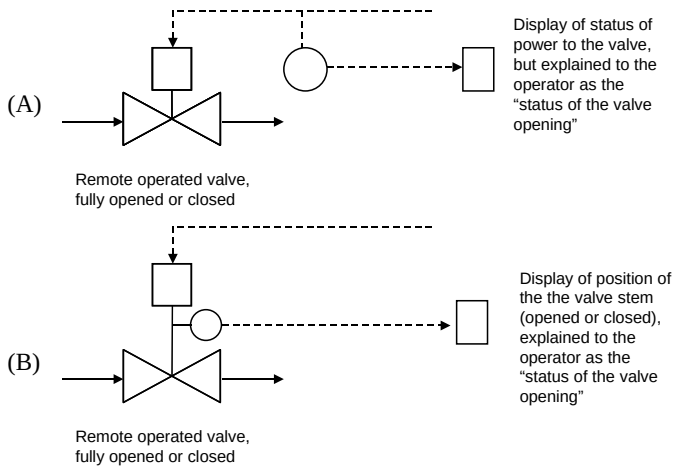



Figure Q5.29c

d. "Human factors" is a general term involving the ease (or lack of ease) of understanding and operation of a technical system by a human being. Here, we consider the human factors for the layout of a display used by a plant operator, but designed by an engineer. Figure Q5.29d shows the physical layout of four fired heaters. It also shows the layout of the manual SIS activation buttons in the control room for the heaters in design (A) and Design (B).

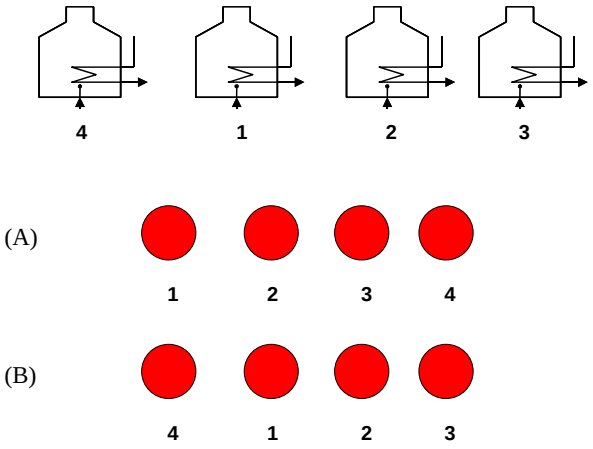



Figure Q5.29d.

5.30 **Layer of Protection analysis**: The preliminary design of the Debutanizer tower shown in Figure Q5.30 has been completed. You have been asked to perform a Layer of Protection Analysis (LOPA) on the reflux drum V-31. The specific initiating incident is the incorrect operator action, resulting in the closing of the manual valve indicated in the drawing to be "normally open".

- The failure rate of the operator action will be taken to be $10^{-3}$ events/yr.
- The target mitigated accident rate will be taken to be $10^{-5}$accidents/yr.

a. Perform a LOPA on the proposed design and state your conclusion
b. If improvements in the safety hierarchy are needed, define these so that the LOPA result meets the target mitigated accident rate.

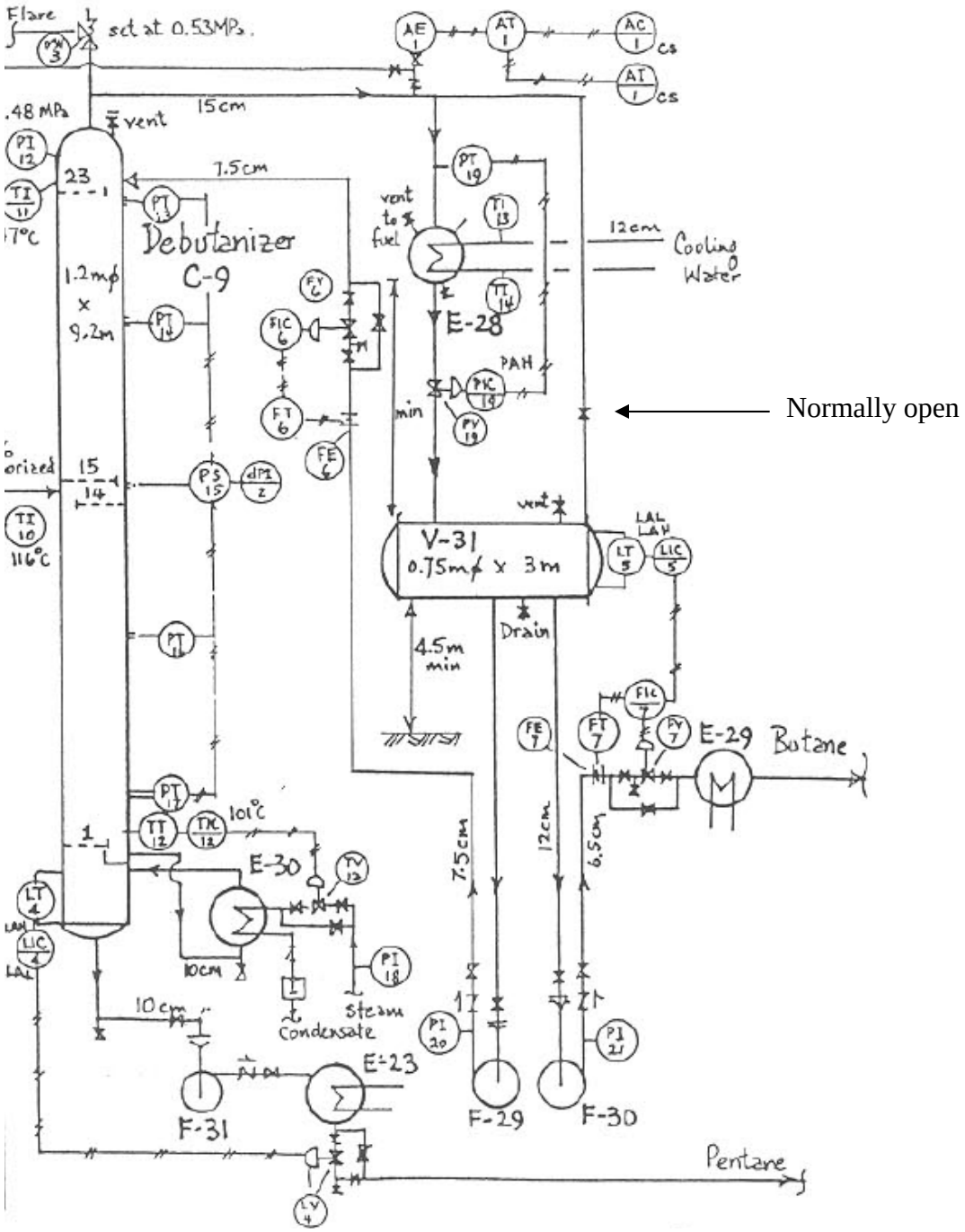



Figure Q5.30. Debutanizer Tower proposed P&ID. (Woods, 1995)

5.31 Which of the following is true for the term “ACTION” in the HAZOP form? Explain your answer.

a. The action recommended to be taken by operating personnel to prevent an accident when the scenario occurs in the plant.
b. The design modification recommended by the HAZOP team.
c. The follow-up investigation required by the HAZOP team before confirming a specific recommendation.
d. None of the above.

# Appendix 5. A Discussion of Uncertainty in Reliability Data

Reliability data is required for proper safety analysis and process design. Until recently, this information has not been collected and reported. Thus, the engineer is cautioned that the data available is contains considerable uncertainty, which must be considered in all hazard analyses. A few of the cautions are given in the following.

- **Uncertainty** – Failure data from various sources often do not agree. The differences can be substantial, over a factor of 10.
- **Root cause of faults** – The data may report the faults of equipment, for example a valve or level float sensor. However, there is great variability in the skill and care by engineers selecting equipment, selecting materials of construction, and managing design, installation and maintenance. In addition, the process conditions influence the failure rate; a pipe or flange leak would occur more frequently when handling highly corrosive fluids. Usually, databases do not report the underlying design, operation, and maintenance policies associated with the data.
- **Specificity of fault type** – Most databases report a single fault frequency for each equipment. However, most equipment experience many types of failures, with the different failure types having very different influences on the safety performance. For example, a control valve failure could include (1) going to its designed failure (fail-safe) position, (2) sticking and hysterisis so that the actual valve position would "stick and jump" as the command changed, and (3) going to its "fail-unsafe" position. Clearly, the last failure is very bad, but most data does not report the variety of faults separately.
- **Currency of data** – As manufacturing and maintenance methods improve, the failure rates decrease. However, many sources report decades-old data or are unclear regarding when the data was collected.
- **Maintenance** – The failure rate of a device is strongly affected by installation and maintenance. The databases do not define the detailed engineering and maintenance for the facilities from which the data was collected.
- **Dynamics of failure** – There is very little data on the duration of a failure. Some failures can be diagnosed and repaired before the fault progresses to a safety issue, while others may proceed quickly to a catastrophic event; these faults will be lumped into one failure rate.
- **Hidden dependencies** – A highly reliable SIS, for example, a system with many parallel paths, may have an extremely low PFD. However, these systems share some common features that lead to lack of completely independent failure modes, such as the same people performing maintenance. Therefore, engineers are cautioned against assigning one IPL with a PFD lower than commonly recommended, such as values in Table 5.16.
- **Human failure rates** – These depend on the specific situation; a quick decision under stress is much more likely to be incorrect.

- **Units for risk** – Some risk data is presented without a clear explanation of the meaning. For example, a risk of 0.05 physical harm from exposure to a specific dose of hazardous material is not specific enough. What is the duration (events/single-time exposure, events/life-time exposure)? Is skin contact important? This type of incomplete data is often reported in stories appearing in newspapers and magazines.

Kletz (1999) and (2001) has very useful cautions concerning reliability data and its use by engineers. The reader will benefit from his non-mathematical, common sense discussions and recommendations.

# Appendix 5.B. Application of safety analysis methods for equipment protection.

The methods presented in this chapter have been developed for the analysis and improvement of process safety performance. During hazard identification (check list, what-if, and HAZOP), the team is likely to encounter events leading to potential equipment damage. Many of these also lead to safety issues, because equipment damage can cause loss of containment of hazardous materials (e.g., a vessel leak) or debris that could injure people (e.g., breaking a vane in a compressor). Even when the equipment damage does not lead to a hazard, the team should thoroughly analyze the event and where necessary, recommend design changes to reduce the consequence likelihood. After all, equipment repair can be expensive, and loss of production during repair can cause enormous economic loss.

A few examples of equipment protection are given in this appendix, and further discussion is available in CCPS (1998), as well as references on each equipment type (pumps, compressors, heat exchangers, trayed towers, etc.).

- **Positive displacements pumps** – Positive displacement pumps rely on the movement of pump components to displace fluid from the pump internals to the pump exit. If the fluid is prevented from leaving the pump, the pump component that should displace the fluid is prevented from moving. The result is a very large force on the component and usually, damage to the pump. Therefore, a minimum fluid flow through the pump should be ensured, even if the flow to downstream units is stopped. A typical design to ensure flow is shown in Figure 5.B.1, which includes a flow controller that regulates the flow to downstream processes by adjusting the recycle flow. In case the flow is too low, the pump outlet pressure will increase rapidly, and a pressure relief valve will open to send the material to a drain for safe disposal.
- **Compressors** – Compressors are used to increase the pressure of a gas. At low flow rates, an unstable flow can occur, potentially leading to oscillations between forward and backward flow of the gas, termed a “surge”; this can lead to serious mechanical damage to the compressors vanes. Therefore, a minimum flow rate is required to prevent surge. A typical, simple design to prevent surge is shown in Figure 5.B.2, where the set point to the flow controller is the minimum flow through the compressor. More complex designs are possible that more accurately determine the minimum flow rate, thus reducing work when operating near the minimum flow.
- **Boiler water** – A boiler stores water in a drum from which water flows through tubes for heat exchange with large area in the firebox. If the water flow through the tubes were to stop, the tubes would quickly overheat and be damaged; therefore, the drum must always contain water. The water level is controlled under normal operation by adjusting the flow rate of the make-up water; however, equipment faults, such as a pump failure or inadvertent valve closure, could stop

the flow to the drum. Therefore, an alarm and SIS are required to prevent damage to the boiler by stopping the fuel flow to the burner.

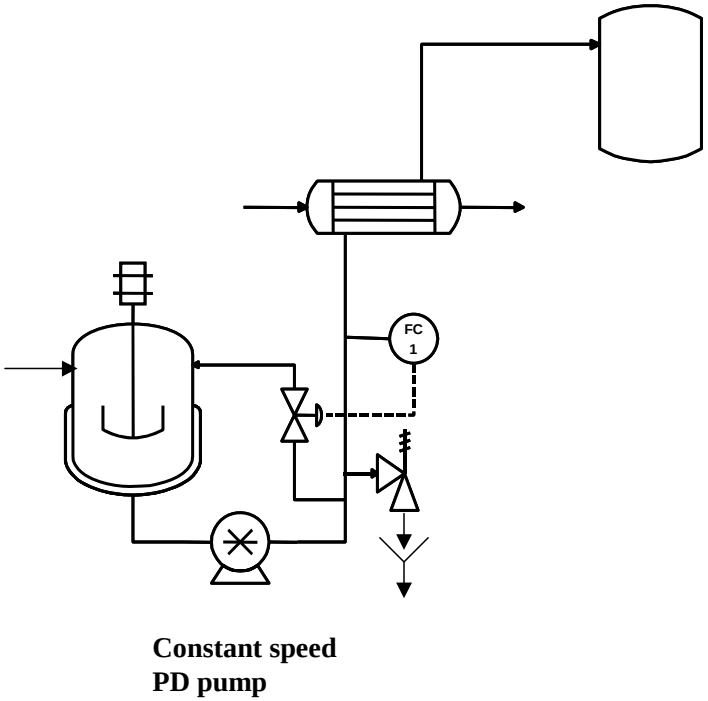



**Figure 5.B.1** Protection for positive displacement pump.

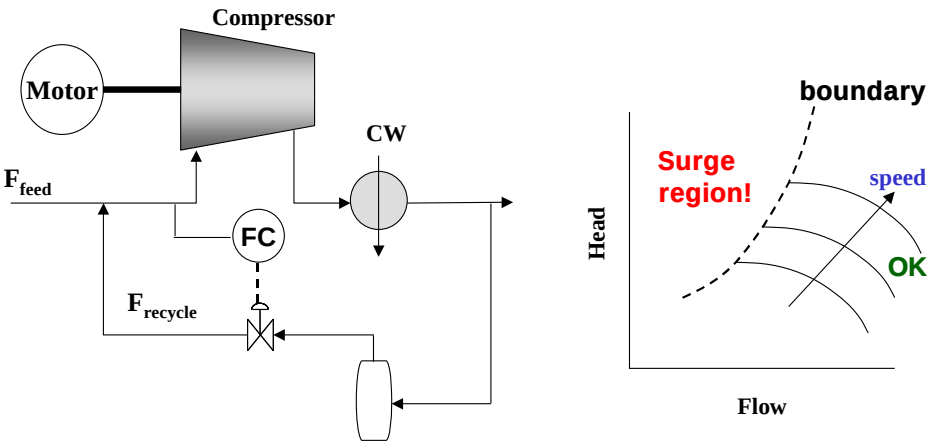



Figure 5.B.2 Surge protection for a centrifugal compressor.

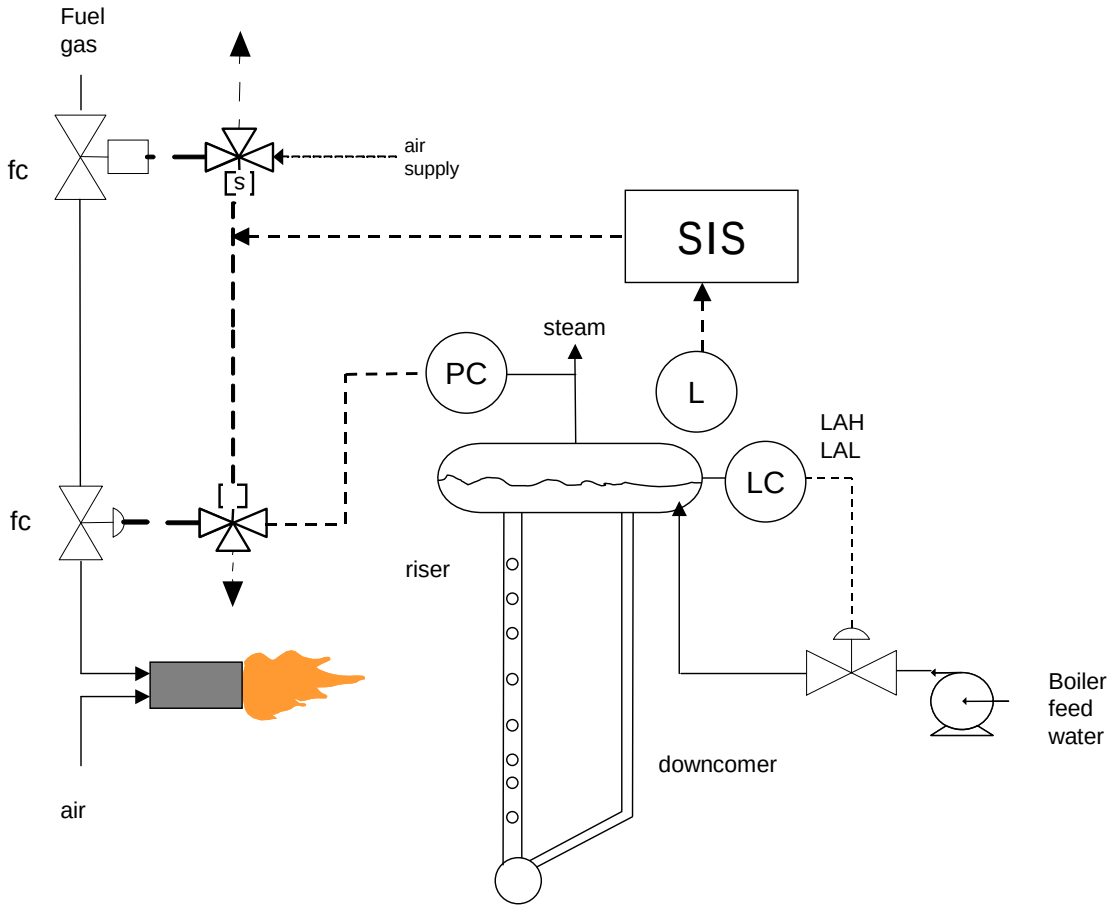



Figure 5.B.3. Boiler protection based on drum water level.
(Redundancy not shown)