PART 1.2 HARDWARE SYSTEM

Dr. AA, Process Control & Safety
How to Ensure that Process Plant is Safe

1. Preliminary Decision
   – Process Selection, site selection etc

2. Process Design
   – Inherent safety

3. Process Safety Management
PROCESS SYSTEM

Many different scenarios
• Fully Automated vs manual plant
• Fully integrated continuous plant vs batch plant
• Onshore vs offshore
PART 1.2 HARDWARE SYSTEM

Topic 1 Inherently Safe Design
Inherent Safety

• To make the concept more understandable, the following four words have been recommended to describe inherent safety

  – Minimise (intensification)
  – Substitute (substitution)
  – Moderate (attenuation and limitation of effects)
  – Simplify (simplification and error tolerance)
Minimise (example)

- Change from larger batch reactor to smaller continuous reactor
- Reduce storage inventory of raw materials
- Improve control to reduce inventory of hazardous intermediate chemicals
- Reduce process hold-up
Substitute (example)

- Use mechanical pump seals vs packing
- Use welded pipe vs flanged
- Use solvent that are less toxic
- Use mechanical gauges vs mercury
- Use chemicals with higher flash point, boiling points, and other less hazardous properties
- Use water as heat transfer fluid instead of hot oil
Moderate (example)

- Use vacuum to reduce boiling point
- Reduce process temperature and pressure
- Refrigerate storage vessel
- Dissolve hazardous materials in safe solvent
- Place control rooms away from operation
- Operate at conditions where runaway reactions are not possible
- Separate pump rooms from other rooms
- Barricade control rooms and tanks
• Keep piping systems neat and visually easy to follow
• Design control panels that are easy to comprehend
• Design plants for easy and safe maintenance
• Pick equipment with low failure rates
• Separate systems and controls into blocks that are easy to comprehend and understand
• Label pipes for easy ‘walking the line”
• Label vessels and controls to enhance understanding
• Add fire and explosion resistant barricades
Inherent Safety Concept

- Reduce the risk at early stage of design

Diagram:
- Potential hazard
  - Layers of protection
  - Damage layers of protection
  - Final risk
  - Higher final risk
- Reduced potential hazard due to inherently safer design
Safety issues must be embedded within all project life-cycle

Relationship of six-stage process study system to project life-cycle:

Stage 1: Concept
Stage 2: Process design
Stage 3: Detailed Engineering
Stage 4: Construction
Stage 5: Pre-Commissioning
Stage 6: Post-Commissioning
Many hazard identification techniques can be used at appropriate cycle.

- Checklist
- LOPA
- HAZOP
- RR
- PHR
- What-if
- FTA
- ETA
- FMEA
## Hazard identification technique and project phase

<table>
<thead>
<tr>
<th>Method used</th>
<th>Project life cycle stage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Checklist</td>
<td>X</td>
</tr>
<tr>
<td>RR</td>
<td>X</td>
</tr>
<tr>
<td>What-If</td>
<td>X</td>
</tr>
<tr>
<td>FTA</td>
<td>X</td>
</tr>
<tr>
<td>ETA</td>
<td>X</td>
</tr>
<tr>
<td>FMEA</td>
<td>(X)</td>
</tr>
<tr>
<td>LOPA</td>
<td>X</td>
</tr>
<tr>
<td>HAZOP</td>
<td>(X)</td>
</tr>
<tr>
<td>PHR</td>
<td>X</td>
</tr>
</tbody>
</table>
PART 1.2 HARDWARE SYSTEM

Topic 2 Plant Operation System
Typical Objectives of Plant Operation

1. Protect people
2. Protect Environment
3. Protect Equipment
4. Maintain Smooth operation
5. Achieve Product rates and quality
6. Profit = optimising first five
7. Monitoring & diagnosis

These are Achieved Through Process Control…
DCS Architecture

System Consoles

Host Computer

Data Storage Unit

PLC

Data Highway
(Shared Communication Facilities)

Local Console

Local Control Unit

Local Control Unit

Local Console

Process Transmitters and Actuators

4-20 mA

4-20 mA
Fieldbus Technology

- Introduced 1988 but underwent many development
- Standard IEC61158 introduced in 1999
- Based upon smart valves, smart sensors and controllers installed in the field.
- Uses data highway to replace wires from sensor to DCS and to the control valves.
- Less expensive installations and better reliability.
- Can mix different sources (vendors) of sensors, transmitters, and control valves.
- Now commercially available and should begin to replace DCSs.
Fieldbus Architecture

High Speed Ethernet

- PLCs
- Local Area Network
- H1 Fieldbus
  - Smart Sensors
  - Smart Control Valves and Controllers
  - H1 Fieldbus Network
- Data Storage
- Plant Optimization
- Local Area Network
- H1 Fieldbus
  - Smart Sensors
  - Smart Control Valves and Controllers
  - H1 Fieldbus Network
PLC Architecture

- Processor
- Power Supply
- Data Highway
- PLC Cabinet
- Programming Interface
- I/O Modules
- Input Devices
- Output Devices
We desire independent protection layers, without common-cause failures - Separate systems

- DCS handles controls and alarms functions.
- PLC handles SIS and Alarms associated with SIS
Layer of Protection

DR. AA
Process Control & Safety Group
Strength in Reserve

- **BPCS** - Basic process control
- **Alarms** - draw attention
- **SIS** - Safety interlock system to stop/start equipment
- **Relief** - Prevent excessive pressure
- **Containment** - Prevent materials from reaching, workers, community or environment
- **Emergency Response** - evacuation, fire fighting, health care, etc.
Safety Through Automation

- Four Layers in the Safety Hierarchy
- Methods and equipment required at all four layers
- Process examples for every layer
- Workshop
All Processes must have Safety Through Automation

• Safety must account for failures of equipment (including controller) and personnel

• Multiple failure must be covered

• Responses should be limited, try to maintain production if possible

• Automation systems contribute to safe operation
SAFETY STRENGTH IN DEPTH!

- RELIEF SYSTEM: Divert material safely
- SAFETY INTERLOCK SYSTEM: Stop the operation of part of process
- ALARM SYSTEM: Bring unusual situation to attention of a person in the plant
- BASIC PROCESS CONTROL SYSTEM: Closed-loop control to maintain process within acceptable operating region

Seriousness of event

Redundancy – Key Concept in Process Safety
Objective of process Control

Control systems are designed to achieve well-defined objectives, grouped into seven categories.

1. Safety
2. Environmental Protection
3. Equipment Protection
4. Smooth Operation & Production Rate
5. Product Quality
6. Profit
7. Monitoring & Diagnosis

We are now emphasizing these topics
1. Basic process Control System (BPCS)

- Technology - Multiple PID, cascade, feedforward, etc.
- Always control **unstable variables** (Examples in flash?)
- Always control “quick” safety related variables
  - Stable variables that tend to change quickly (Examples?)
- **Monitor** variables that change very slowly
  - Corrosion, erosion, build up of materials
- Provide safe response to critical **instrumentation failures**
  - But, we use instrumentation in the BPCS?
Control Strategy

• Feedback Control
  – Single-loop feedback

• Overcoming disturbances
  – Cascade
  – Feed forward
  – Ratio

• Constraints
  – Split-range, override/select control

• Multivariable
  – multi-loop
  – Decoupling
  – Multivariable control
Level Control on a Tank

**Ordinary Feedback Control**

Without a cascade level controller, changes in downstream pressure disturb the tank level.

**Cascade Control**

With cascade level controller, changes in downstream pressure will be absorbed by the flow controller before they can significantly affect tank level because the flow controller responds faster to this disturbance than the tank level process.
This approach works because the flow control loop is much faster than the temperature control loop which is much faster than the composition control loop.
Feedback-only must absorb the variations in steam usage by feedback action only.

Feedforward-only handle variation in steam usage but small errors in metering will eventually empty or fill the tank.
Combined feedforward and feedback has best features of both controllers.
Sometimes a single flow control loop cannot provide accurate flow metering over the full range of operation.

Split range flow control uses two flow controllers

- One with a small control valve and one with a large control valve
- At low flow rates, the large valve is closed and the small valve provides accurate flow control.
- At large flow rates, both valve are open.
Therefore, for accurate pH control for a wide range of flow rates for acid wastewater, a split range flow controller for the NaOH is required.
Override/Select Control

- Override/Select control uses LS and HS action to change which controller is applied to the manipulated variable.
- Override/Select control uses select action to switch between manipulated variables using the same control objective.
Furnace Tube Temperature Constraint Control

![Diagram of furnace tube temperature control system]
Lower value of flowrate is selected to avoid column flooding
How would we protect against an error in the temperature sensor (reading too low) causing a dangerously high reactor temperature?

Highly exothermic reaction. We better be sure that temperature stays within allowed range!
How would we protect against an error in the temperature sensor (reading too low) causing a dangerously high reactor temperature?

Use multiple sensors and select most conservative!
Summary of Control Strategies

- Feedback Control
- Enhancement of single-loop Feedback control
  - Cascade, split-range, override control
- Feedforward and Ratio Control
- Computed Control (e.g. reboiler duty, internal reflux etc)
- Advanced Control
  - Inferential control
  - Predictive control
  - Adaptive control
  - Multivariable control
2. Alarms that require actions by a Person

- Alarm has an annunciator and visual indication
  - **No action is automated!**
  - A plant operator must decide.

- Digital computer stores a record of recent alarms

- Alarms should catch sensor failures
  - But, sensors are used to measure variables for alarm checking?
2. Alarms that require actions by a Person

- **Common error is to design** *too many alarms*
  - Easy to include; simple (perhaps, incorrect) fix to prevent repeat of safety incident
  - example: One plant had 17 alarms/h - operator acted on only 8%

- **Establish and observe clear priority ranking**
  - **HIGH** = Hazard to people or equip., action required
  - **MEDIUM** = Loss of RM, close monitoring required
  - **LOW** = investigate when time available
3. Safety Interlock System (SIS)

- Automatic action usually stops part of plant operation to achieve safe conditions
  - Can divert flow to containment or disposal
  - Can stop potentially hazardous process, e.g., combustion

- Capacity of the alternative process must be for “worst case”

- SIS prevents “unusual” situations
  - We must be able to start up and shut down
  - Very fast “blips” might not be significant
3. Safety Interlock System

- Also called emergency shutdown system (ESS) or safety instrumented system (SIS)
- SIS should respond properly to instrumentation failures
  - But, instrumentation is required for SIS?
- Extreme corrective action is required and automated
  - More aggressive than process control (BPCS)
- Alarm to operator when an SIS takes action
The automation strategy is usually simple, for example,

If $L_{123} < L_{123,\text{min}}$; then, reduce fuel to zero

How do we automate this SIS when PC is adjusting the valve?
If $L_{123} < L_{123\text{min}}$; then, reduce fuel to zero

$LS = \text{level switch, note that separate sensor is used}$

$s = \text{solenoid valve (open/closed)}$

$fc = \text{fail closed}$

Extra valve with tight shutoff
The automation strategy may involve several variables, any one of which could activate the SIS

If $L123 < L123_{\text{min}}$; or
If $T105 > T105_{\text{max}}$

......

then, reduce fuel to zero

Shown as “box” in drawing with details elsewhere
SIS: measurement redundancy

- The SIF saves us from hazards, but can shutdown the plant for false reasons, e.g., instrument failure.

Better performance, more expensive

Same variable, multiple sensors!
We desire independent protection layers, without common-cause failures - Separate systems

Digital control system

SIS system

BPCS and Alarms

SIS and Alarms associated with SIS
4. Safety Relief System

• Overpressure
  – Increase in pressure can lead to rupture of vessel or pipe and release of toxic or flammable material

• Underpressure
  – Also, we must protect against unexpected vacuum!

• Relief systems provide an exit path for fluid
  – Benefits: safety, environmental protection, equipment protection, reduced insurance, compliance with governmental code
4. Safety Relief System

- Entirely self-contained, **no external power required**
- The action is automatic - **does not require a person**
- Usually, goal is to achieve reasonable pressure
  - Prevent high (over-) pressure
  - Prevent low (under-) pressure
- The capacity should be for the “worst case” scenario
4. Safety Relief System

- No external power required - self actuating - pressure of process provides needed force!
- Valve close when pressure returns to acceptable value
- Relief Valve - liquid systems
- Safety Valve - gas and vapor systems including steam
- Safety Relief Valve - liquid and/or vapor systems
- Pressure of protected system can exceed the set pressure.
Rupture Disk

- No external power required
- Self acting
- Rupture disk / burst diaphragm must be replaced after opening.
4. Safety Relief System

- Spring-loaded safety relief valve

- Rupture disc

Process → Spring-loaded safety relief valve → To effluent handling

Process → Rupture disc → To effluent handling
4. Safety Relief System

- What is the advantage of two in series?
- Why not have two relief valves (diaphragms) in series?

Why is the pressure indicator provided? Is it local or remotely displayed? Why?
4. Safety Relief System

IN SOME CASES, RELIEF VALVE AND DIAPHRAGM ARE USED IN SERIES - WHY?

- Why is the pressure indicator provided?
  If the pressure increases, the disk has a leak and should be replaced.

- Is it local or remotely displayed? Why?
  The display is local to reduce cost, because we do not have to respond immediately to a failed disk - the situation is not hazardous.

- What is the advantage of two in series?
  The disc protects the valve from corrosive or sticky material. The valve closes when the pressure returns below the set value.
WE SHOULD ALSO PROTECT AGAINST EXCESSIVE VACUUM

- The following example uses buckling pins
Location of Relief System

- Identify potential for damage due to high (or low) pressure (HAZOP Study)

- In general, closed volume with ANY potential for pressure increase
  - may have exit path that should not be closed but could be
  - hand valve, control valve (even fail open), blockage of line

- Remember, this is the last resort, when all other safety systems have not been adequate and a fast response is required!
Flash Drum Example
LET’S CONSIDER A FLASH DRUM

Is this process safe and ready to operate?
Is the design completed?
Where could we use BPCS in the flash process?
The level is unstable; it must be controlled.

The pressure will change quickly and affect safety; it must be controlled.
Where could we use alarms in the flash process?
A low level could damage the pump; a high level could allow liquid in the vapor line.

The pressure affects safety, add a high alarm

Too much light key could result in a large economic loss
Safety Relief System

Add relief to the following system
The drum can be isolated with the control valves; pressure relief is required.

We would like to recover without shutdown; we select a relief valve.