ALL PROCESSES MUST HAVE SAFETY THROUGH AUTOMATION

- SAFETY MUST ACCOUNT FOR FAILURES OF EQUIPMENT (INCLUDING CONTROL) & PERSONNEL

- MULTIPLE FAILURES MUST BE COVERED

- RESPONSES SHOULD BE LIMITED, TRY TO MAINTAIN PRODUCTION, IF POSSIBLE

- AUTOMATION SYSTEMS CONTRIBUTE TO SAFE OPERATION

(if they are designed and maintained properly!)
LET’S CONSIDER A FLASH DRUM

Is this process safe and ready to operate?
Is the design compete?
SAFETY THROUGH AUTOMATION

What’s in this topic?

• Four Layers in the Safety Hierarchy
• Methods and equipment required at all four layers
• Process examples for every layer
• Workshop
SAFETY INVOLVES MANY LAYERS TO PROVIDE HIGH RELIABILITY

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 STRENGTH IN DEPTH!

KEY CONCEPT IN PROCESS SAFETY - REDUNDANCY!

Seriousness of event

- 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

Four independent protection layers (IPL)

PROCESS
CATEGORIES OF PROCESS CONTROL
OBJECTIVES

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 emphasizing these topics since people are involved, this is also important.
1. BASIC PROCESS CONTROL SYSTEM (BPCS)

- Technology - Multiple PID(s), 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?
1. BASIC PROCESS CONTROL SYSTEM (BPCS)

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.
1. BASIC PROCESS CONTROL SYSTEM (BPCS)

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!

![Flow diagram showing the protection system]
2. ALARMS THAT REQUIRE ANALYSIS 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 ANALYSIS BY A PERSON

- Common error is to design *too many alarms*
  - Easy to include; simple (perhaps, incorrect) fix to prevent repeat of safety incident
  - 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 $$, close monitoring required
  - **LOW** = investigate when time available
2. ALARMS THAT REQUIRE ANALYSIS BY A PERSON

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
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 (SIS)

- Also called emergency shutdown system (ESS)
- 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
3. SAFETY INTERLOCK SYSTEM (SIS)

- The automation strategy is usually simple, for example,

If \( L123 < L123_{\text{min}} \); 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.

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

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

$fc = \text{fail closed}$

Extra valve with tight shutoff
3. SAFETY INTERLOCK SYSTEM (SIS)

- The automation strategy may involve several variables, any one of which could activate the SIS

If \( L_{123} < L_{123\text{min}} \); or
If \( T_{105} > T_{105\text{max}} \)

......

then, reduce fuel to zero

Shown as “box” in drawing with details elsewhere
3. SAFETY INTERLOCK SYSTEM (SIS)

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

- Better performance, more expensive

<table>
<thead>
<tr>
<th>False shutdown</th>
<th>Failure on demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 x 10^{-3}</td>
<td>5 x 10^{-3}</td>
</tr>
<tr>
<td>2.5 x 10^{-6}</td>
<td>2.5 x 10^{-6}</td>
</tr>
</tbody>
</table>

- T100
- T100
- T101
- T102
- 1 out of 1 must indicate failure
- 2 out of 3 must indicate failure
- Same variable, multiple sensors!
## RISK MATRIX FOR SELECTING SIS DESIGN

<table>
<thead>
<tr>
<th>Event Likelihood</th>
<th>Event Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>low</td>
<td>extensive</td>
</tr>
<tr>
<td>moderate</td>
<td>serious</td>
</tr>
<tr>
<td>high</td>
<td>minor</td>
</tr>
</tbody>
</table>

### Table entries
- word = qualitative risk description
- number = required safety integrity level (SIL)

### Safety Integrity Levels
(Prob. Of failure on demand)
- 1 = .01 to .1
- 2 = .001 to .01
- 3 = .0001 to .001

Selection documented for legal requirements
3. SAFETY INTERLOCK SYSTEM (SIS)

- We desire independent protection layers, without common-cause failures - Separate systems
KEY CONCEPT IN PROCESS SAFETY - REDUNDANCY!

What do we do if a major incident occurs that causes
- loss of power or communication
- a computer failure (hardware or software)

SAFETY STRENGTH IN DEPTH!

<table>
<thead>
<tr>
<th>RELIEF SYSTEM</th>
<th>SAFETY INTERLOCK SYSTEM</th>
<th>ALARM SYSTEM</th>
<th>BASIC PROCESS CONTROL SYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Divert material safely</td>
<td>Stop the operation of part of process</td>
<td>Bring unusual situation to attention of a person in the plant</td>
<td>Closed-loop control to maintain process within acceptable operating region</td>
</tr>
</tbody>
</table>

These layers require electrical power, computing, communication, etc.
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

- Two general classes of devices
  - Self-Closing: design provides for closing of flow path when the system pressure returns within its acceptable range; operation can resume
  - Non-self-closing: Remains open. Typically, the process must be shutdown and the device replaced

Example: Spring safety valve

Example: Burst diaphragm

Next lesson covers these in more detail
GOOD PRACTICES IN CONTROL FOR SAFETY

1) never by-pass the calculation (logic) for the SIS, i.e., never turn it off
2) never mechanically block a control, SIS valve so that it can not close
3) never open manual by-pass values around control and shutdown valves
4) never "fix" the alarm acknowledgement button so that new alarms will not require the action of an operator
5) avoid using the same sensor for control, alarm, and SIS. Also, avoid using the same process connection (thermowell, tap, etc.) for all sensors.
6) avoid combining high and low value alarms into one indication
7) critically evaluate the selection of alarms, do not have too many alarms
8) use independent equipment for each layer, including computing equipment
9) select emergency manipulated variables with a fast effect on the key process variable
10) use redundant equipment for critical functions
11) provide capability for maintenance testing, since the systems are normally in "stand-by” for long times - then must respond as designed!
SAFETY AUTOMATION SYSTEMS, WHAT HAVE WE LEARNED?

• Typically, four layers are designed for a process
• Each layer has special technology and advantages
• Layers must be part of process design
• Layers contribute to safety, but if incorrect, can be unsafe

We are now ready to gain experience in designing and evaluating safety automation systems.
SAFETY THROUGH AUTOMATION

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

By the way, which of the four layers uses the feedback principle?

PROCESS
REFERENCES


AIChE, Guidelines for Safe Automation of Chemical Processes, American Institute of Chemical Engineers, Research Triangle Park, NC, 1994


Fisher, T. (Ed), AControl System Safety@ISA Transactions, 30, 1, (special edition), 1991

Goble, W., Evaluating Control System Reliability, Instrument Society of America, Research Triangle Park, 1992


Summers, A., Techniques for Assigning a Target Safety Integrity Level, ISA Transactions, 37, 1998, 95-104.
SAFETY THROUGH AUTOMATION WORKSHOP 1

1. Review the distillation process on the next slide.

2. Locate at least one example of each of the four layers of safety automation

3. Evaluate each example that you find.
   (Remember, the example is for educational purposes which could include errors for workshops.)
Feed drum attenuates composition disturbances

Averaging level control attenuates flow rate disturbances

Feed flow rate and composition disturbances

To flare
1. Review the fired heater process on the next slide.

2. Equipment would be damaged and personnel could be injured if the combustion continued when the process is not operating properly. Determine a mal-operation that could lead to unsafe operation.

3. Determine the sensors, the final element(s) and SIS logic to provide a safe system.