SAFETY HIERARCHY

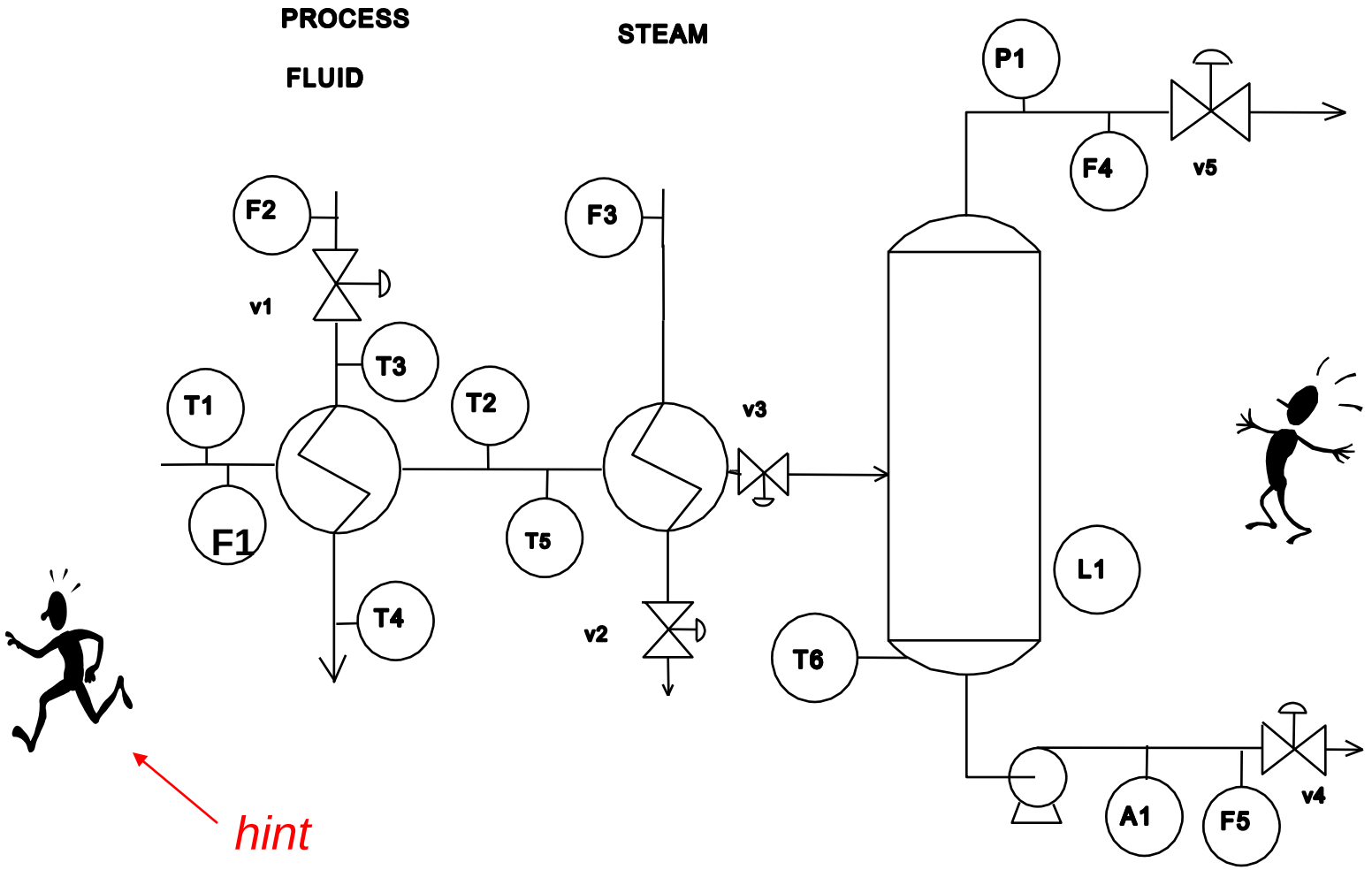
Essential for every plant and engineered device

- **Safety must account for failures of equipment (including control) and personnel**
- **Multiple failures must be covered**
- **Responses should be limited, try to maintain production, if possible**
- **Automation systems contribute to safe operation**

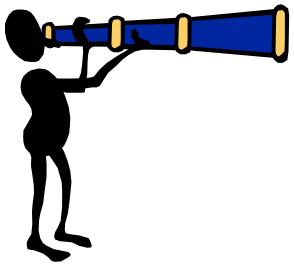
  (if they are designed and maintained properly!)

Let's consider a flash drum

Is this process safe and ready to operate?
Is the design complete?



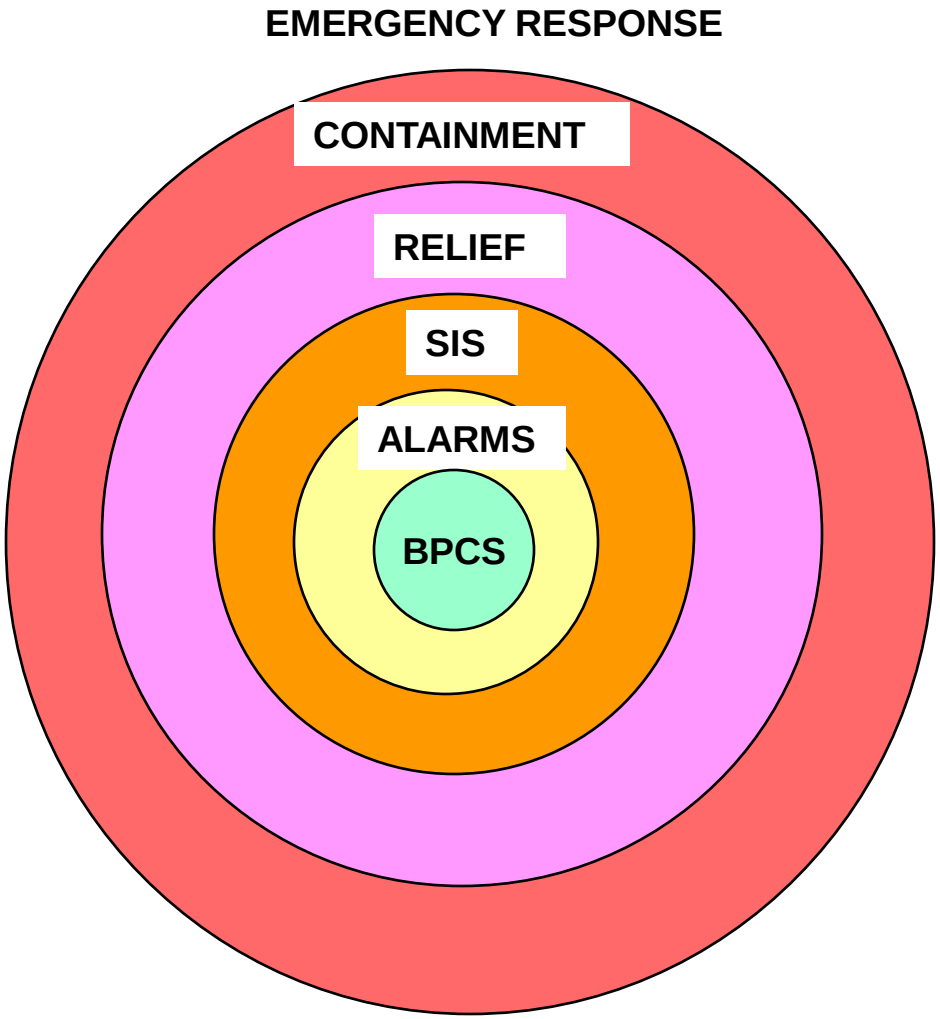
Safety through automation



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**

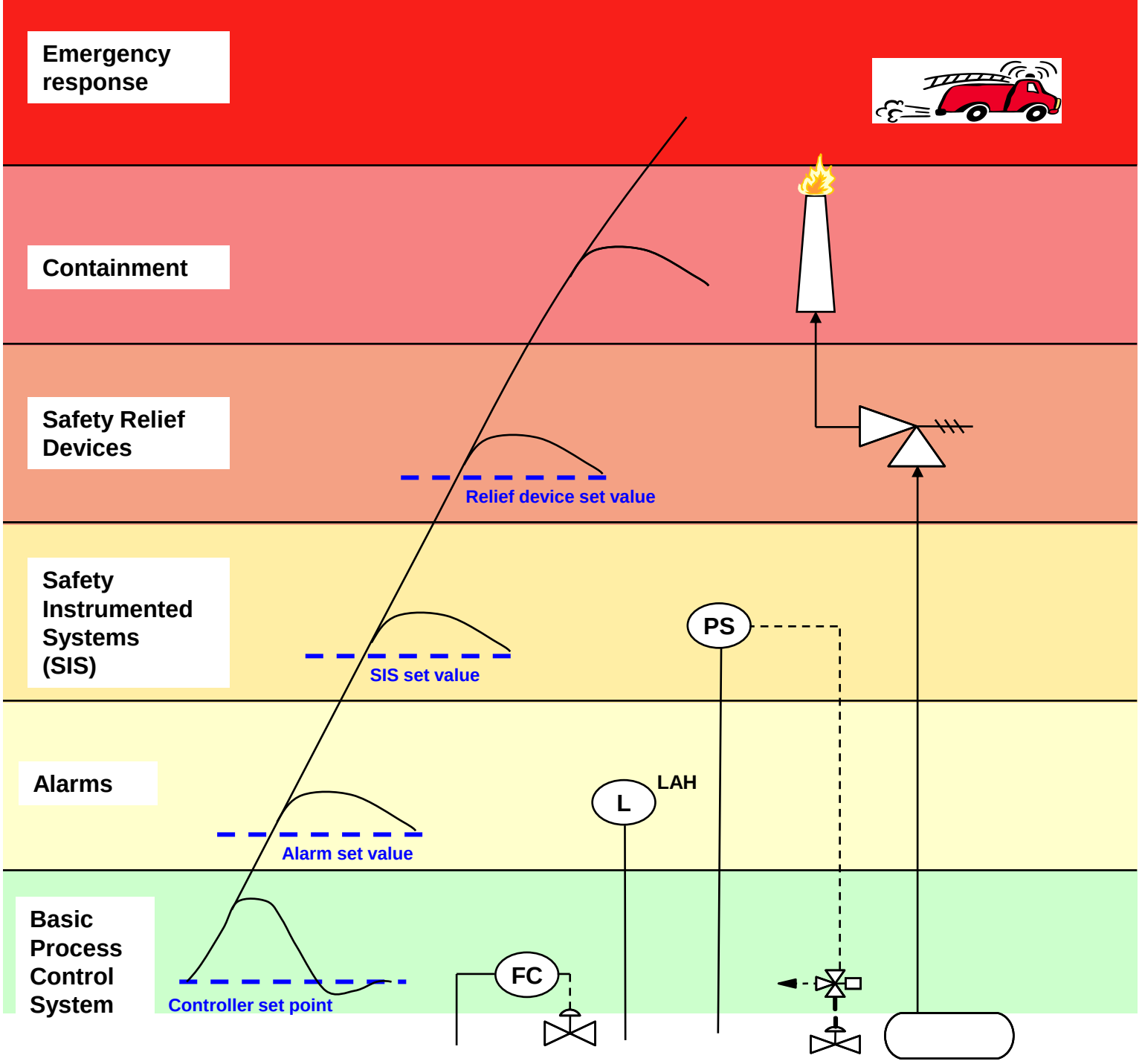
Safety involves many layers to provide high reliability



Control

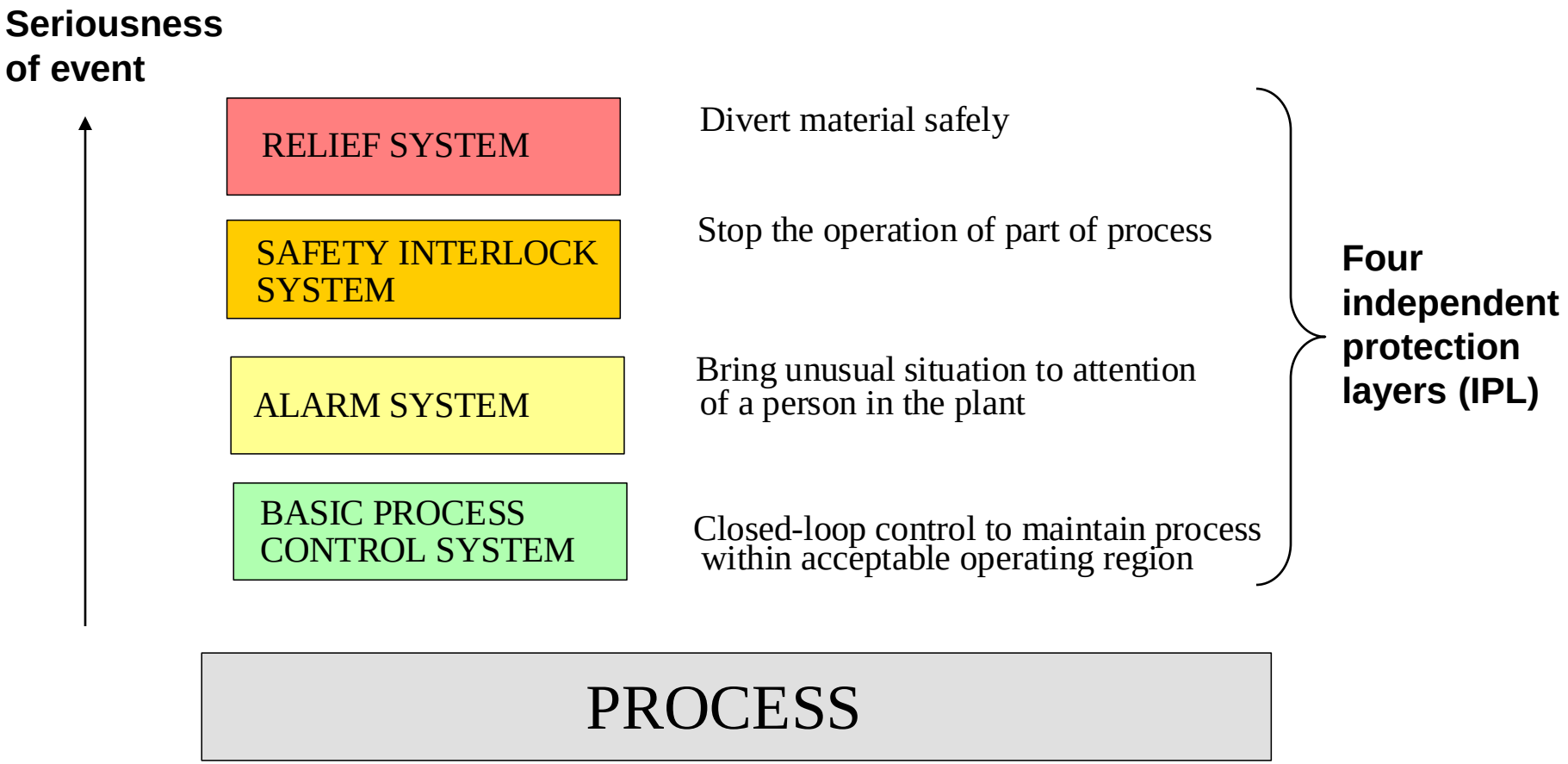
Strength in reserve

- BPCS - Basic process control
- Alarms - draws attention
- SIS - Safety instrumented 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.


Emergency response
Containment
Safety Relief Devices
Safety Instrumented Systems (SIS)
Alarms
Basic Process Control System
Relief device set value
SIS set value
Alarm set value
Controller set point
PS
LAH
L
FC

Key concept in process safety - redundancy!

SAFETY STRENGTH IN DEPTH !



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 and production rate
5. Product quality
6. Profit
7. Monitoring and diagnosis

We are emphasizing these topics

Since people are involved, this is also important

1. Basic process control system (BPCS)

- Technology - Multiple PIDs, cascade, feedforward, etc.
- Always control unstable variables
- Always control “quick” safety related variables

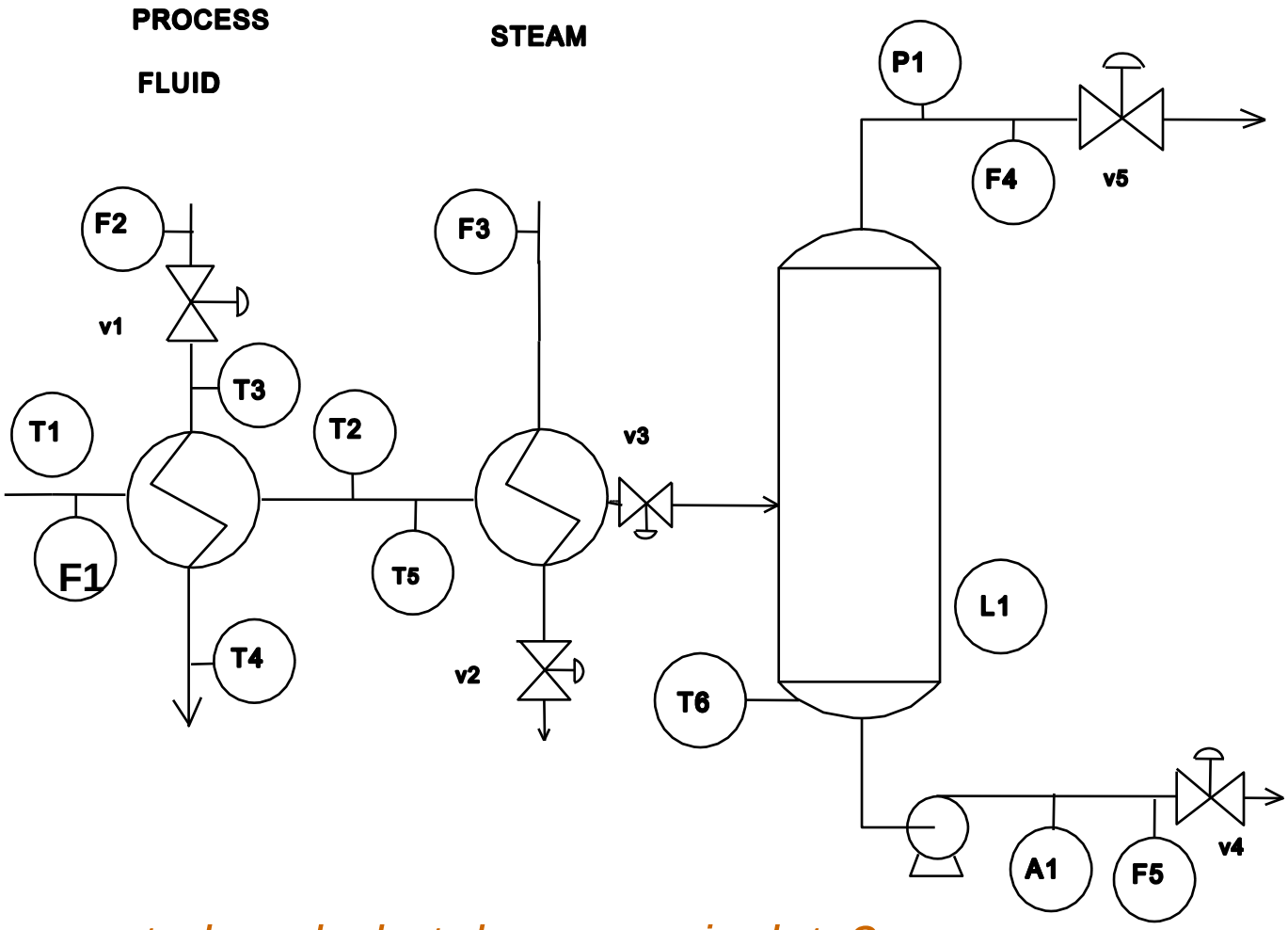
  - Stable variables that tend to change quickly (examples?)
- Monitor variables that change very slowly

  - 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)

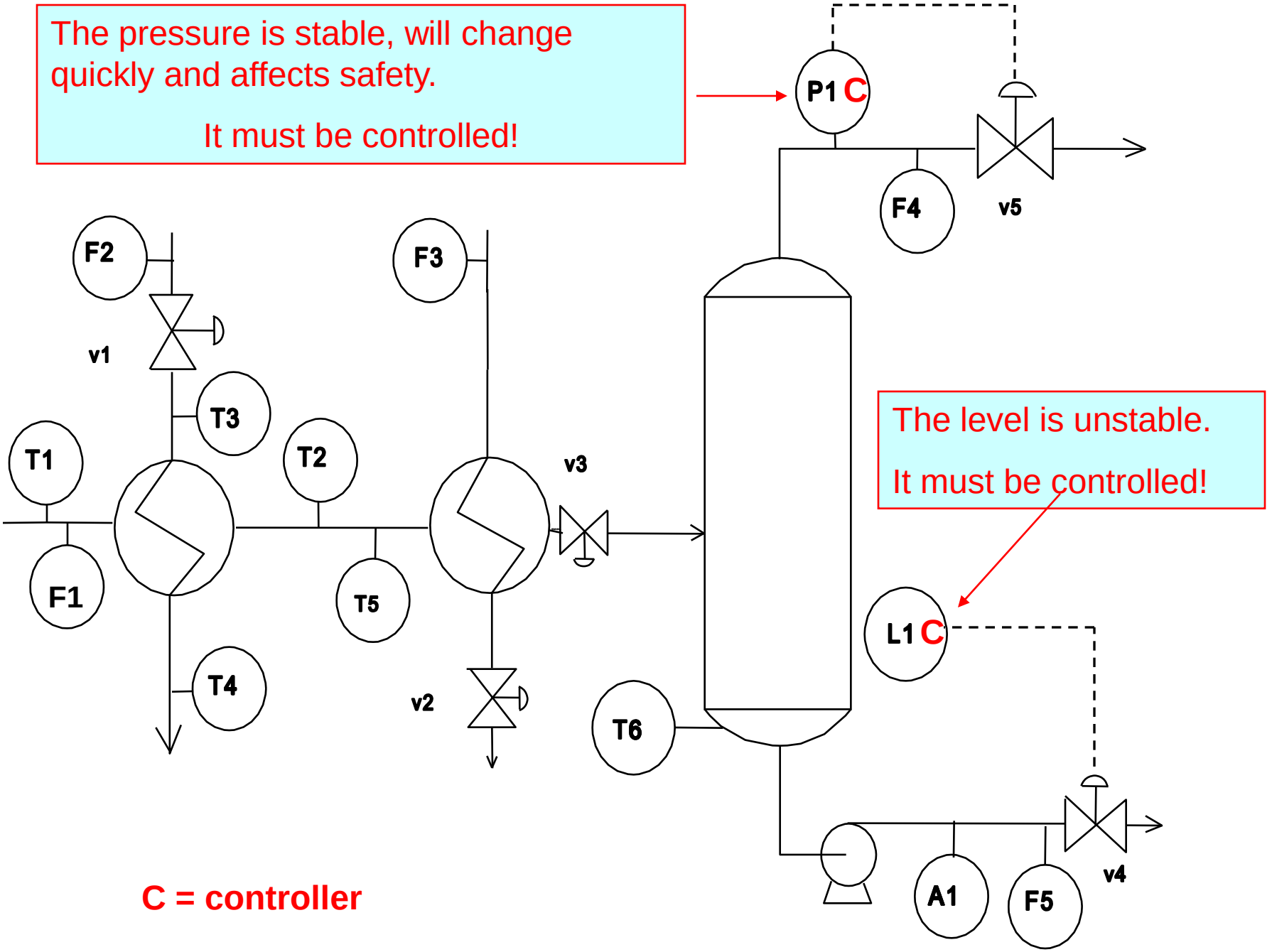
Workshop: Where could we use BPCS in the flash process?



What do we control, and what do we manipulate?

The pressure is stable, will change quickly and affects safety.

It must be controlled!



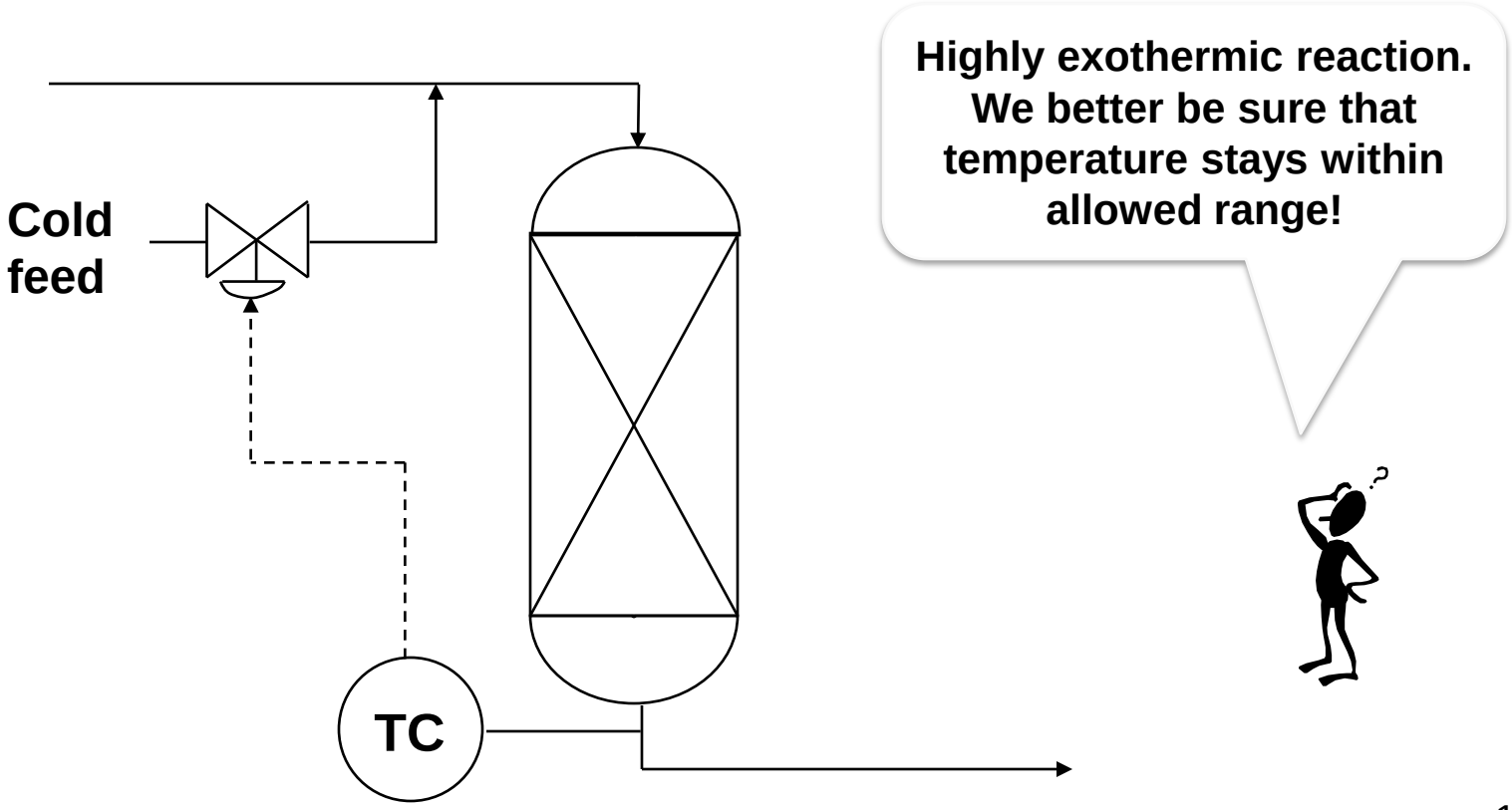
The level is unstable.

It must be controlled!

C = controller

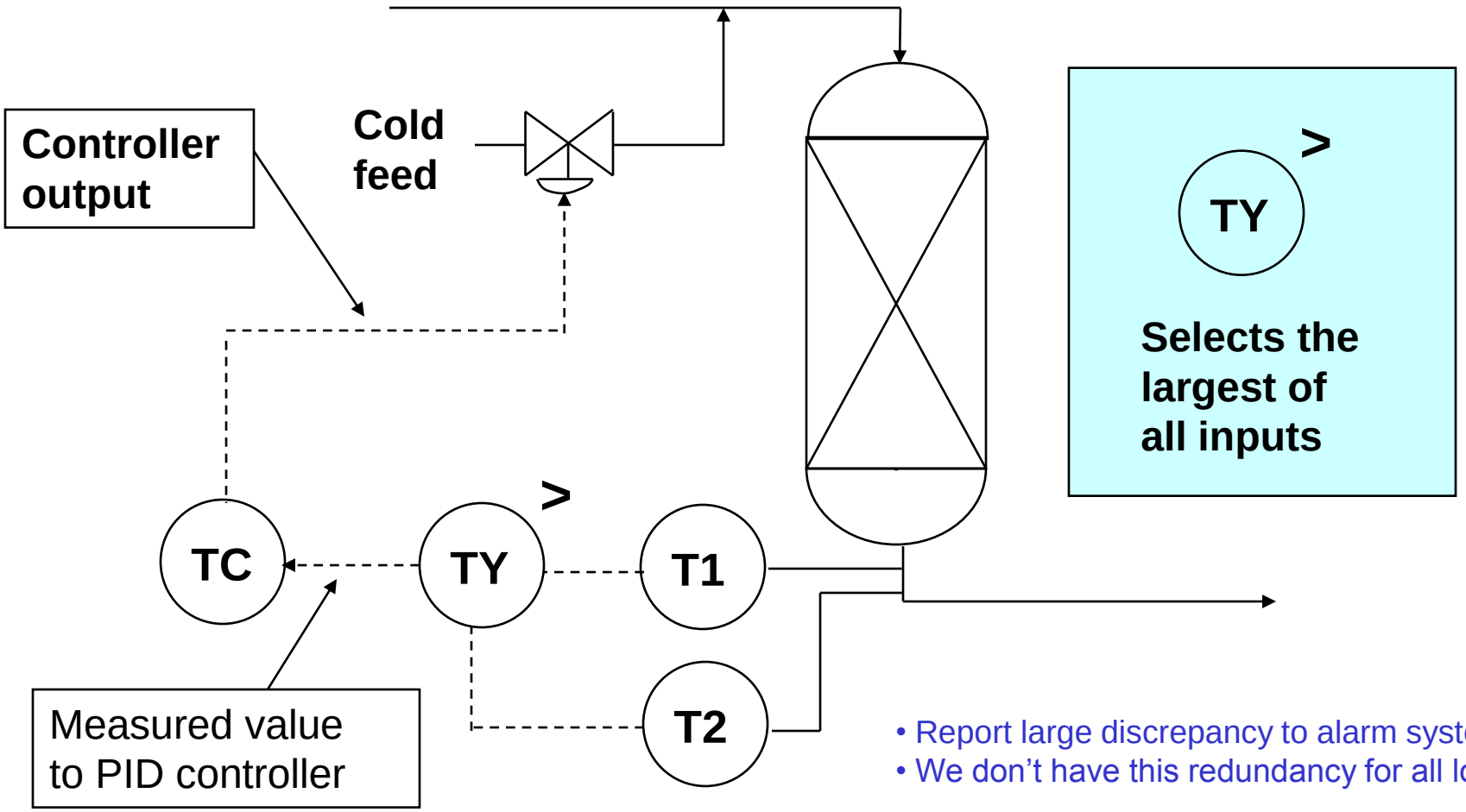
1. Basic process control system (BPCS)

How would we protect against an error in the temperature sensor (reading too low) causing a dangerously high reactor temperature?



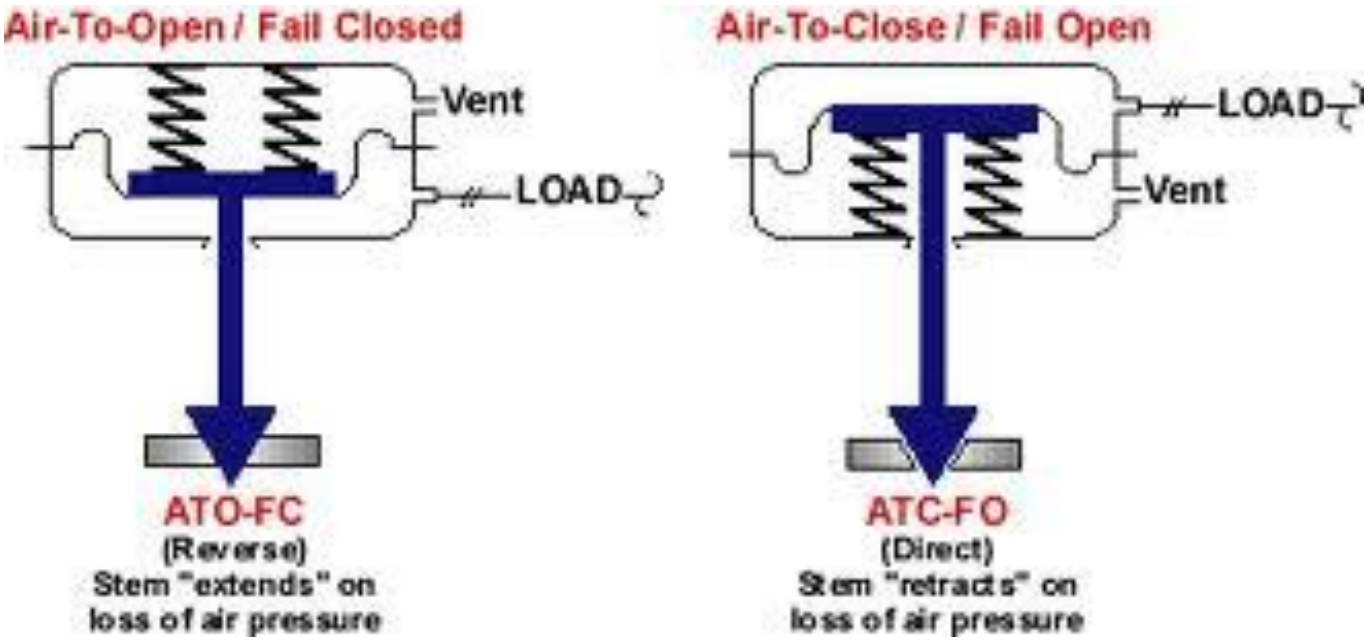
How would we protect against an error in the temperature sensor (reading too low) causing a dangerously high reactor temperature?

Use multiple sensors and select most conservative!



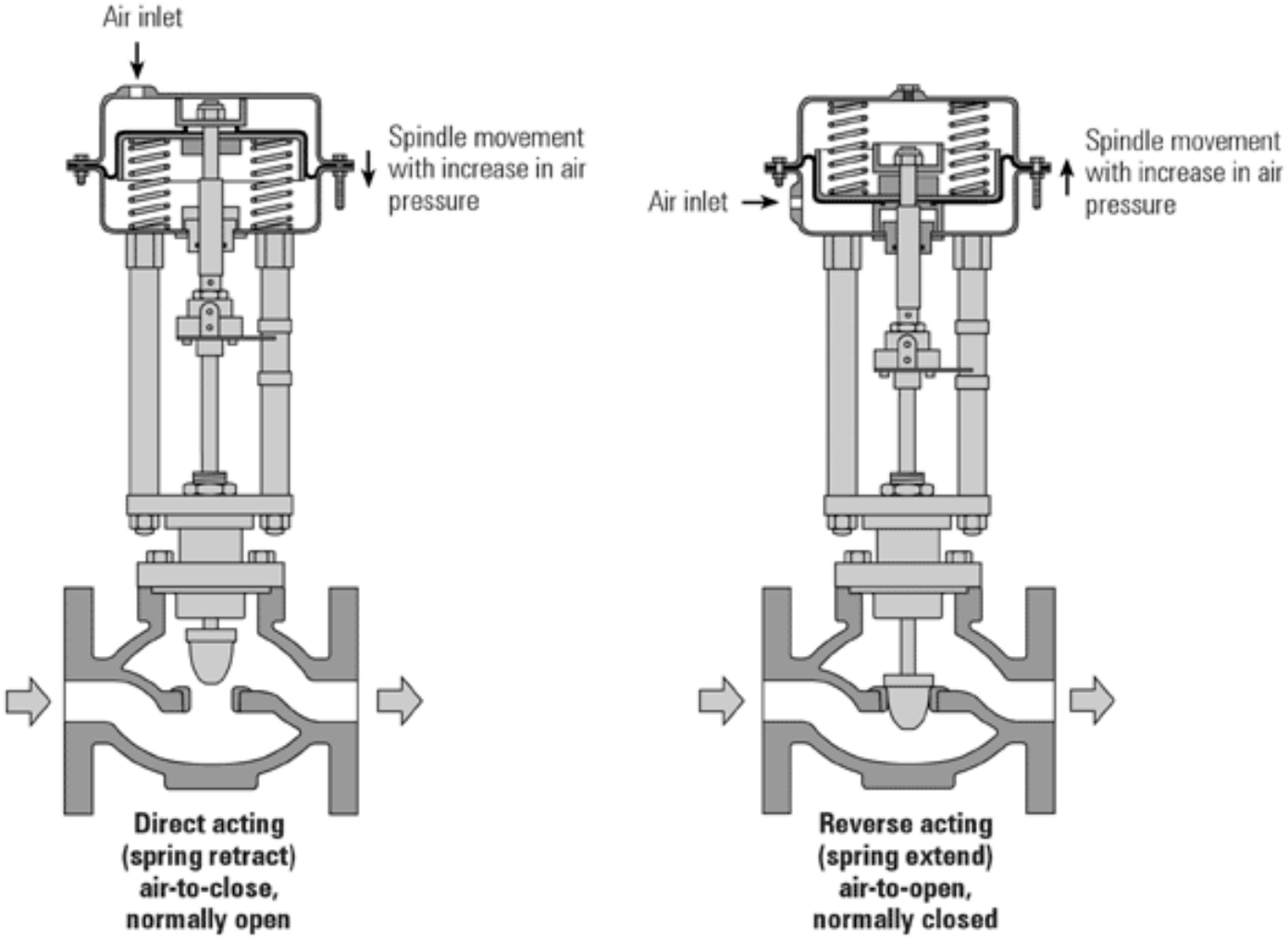
- Report large discrepancy to alarm system
- We don't have this redundancy for all loops

Pneumatic control valves can be designed to fail open or fail closed



http://www.maintenanceresources.com/referencelibrary/controlvalves/cashcoactuatorop.htm

Pneumatic control valves can be designed to fail open or fail closed



http://www.spiraxsarco.com/resources/steam-engineering-tutorials/control-hardware-el-pn-actuation/control-valve-actuators-and-positioners.asp

1. Basic process control system (BPCS)

How do we select fail opened or closed?

The failure position of a control valve is selected to

yield the safest condition in the process. We must consider the entire process context (downstream and upstream) when selecting the valve design.

What is the better failure position for the previous packed bed chemical reactor with exothermic reaction?

To maximize cooling, the valve should be fail open.

2. Alarms that require analysis by a person

- Alarm has an annunciator (audible) and visual indication

  - No action is automated by the alarm!

  - A plant operator must decide on a suitable action.

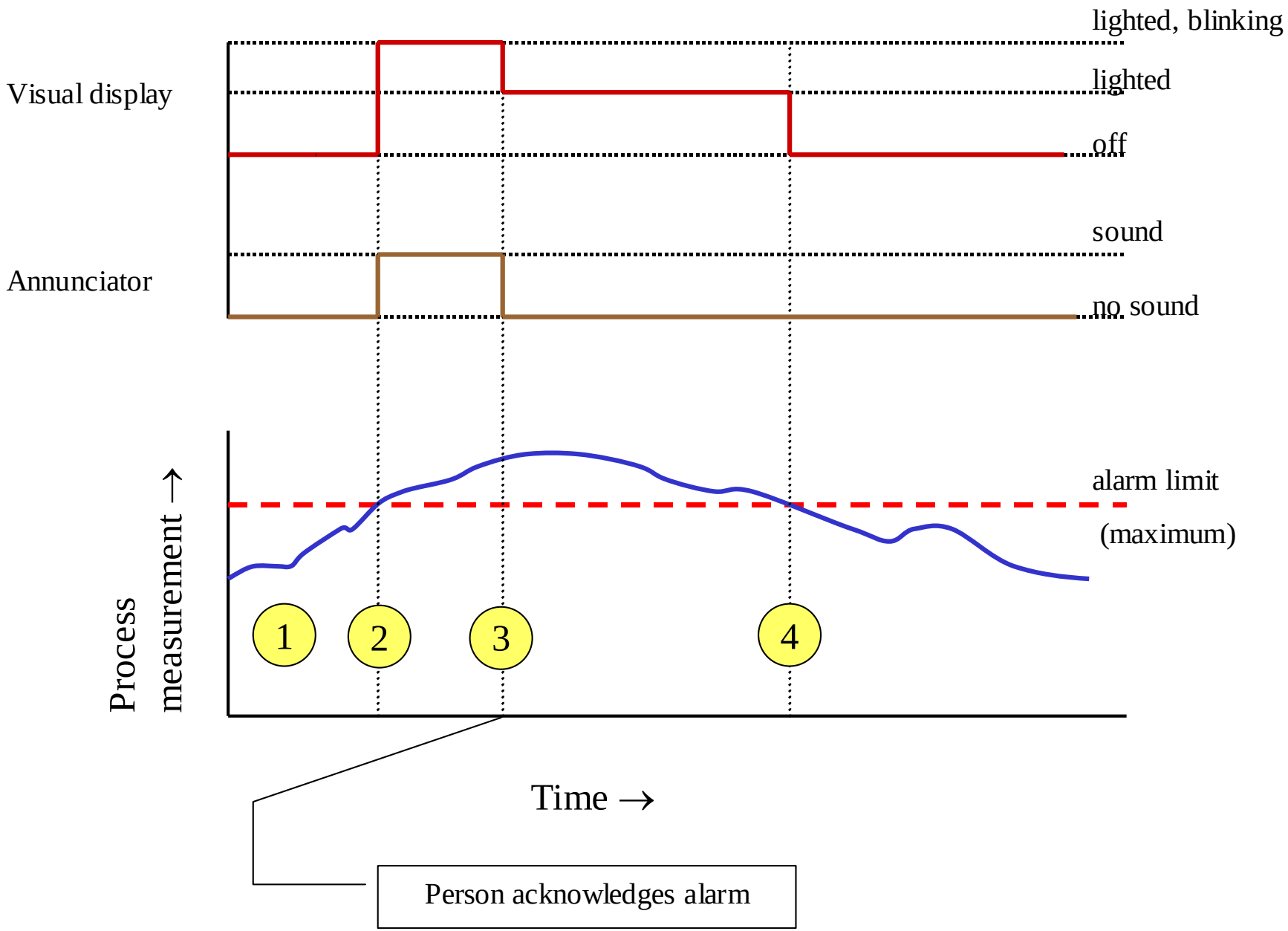
- Digital computers stores a record of recent alarms

  - These should also be immediately recorded off-site

- Alarms should catch sensor failures

  - But, sensors are used to measure variables for alarm checking?

Alarm trend in response to a process measurement



2. Alarms that require analysis by a person

- Common error is to design *too many alarms*

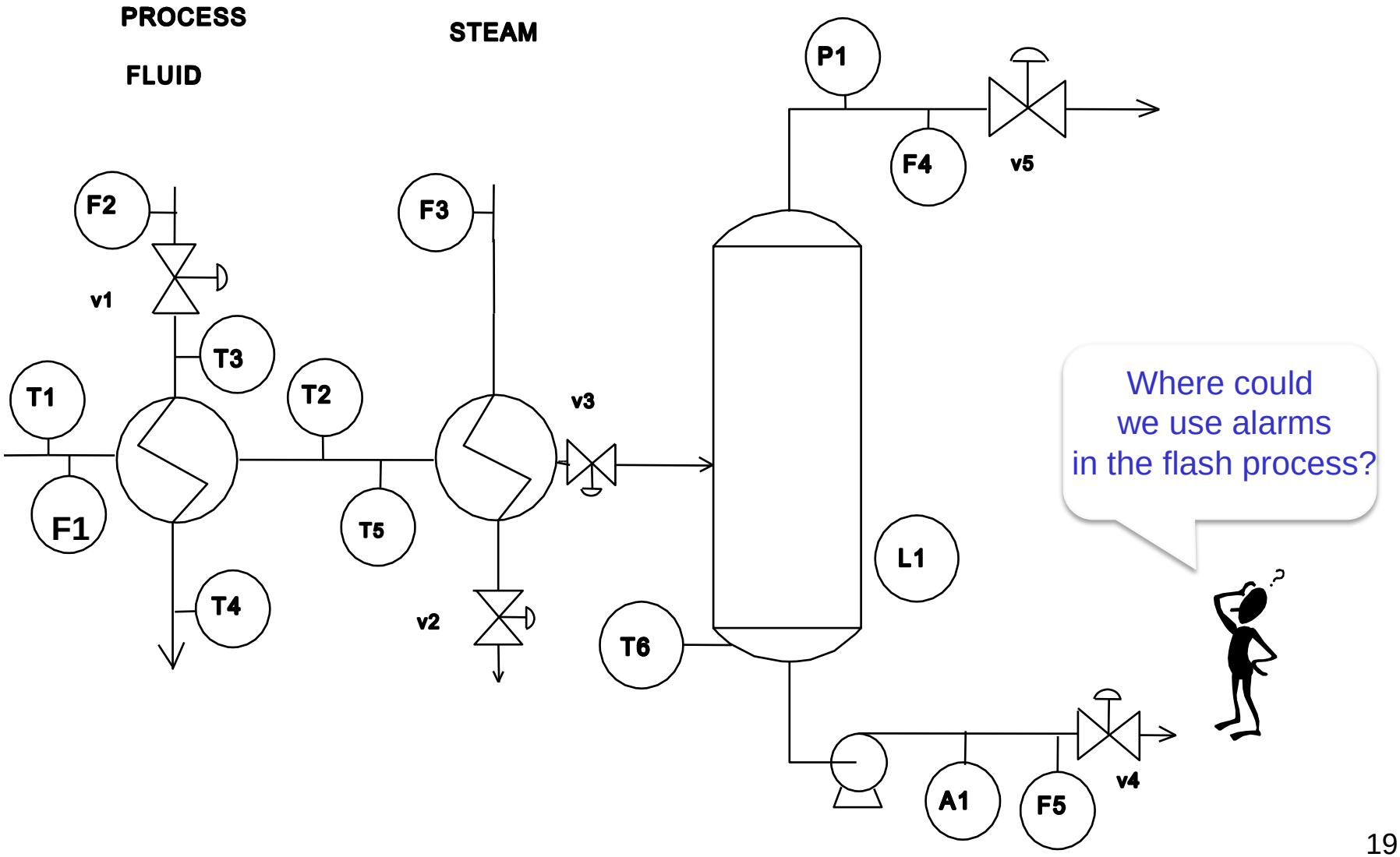
  - Easy to include; often done as a simple (perhaps, incorrect) fix to prevent repeat of a prior safety incident

  - One plant had 17 alarms/h - operator acted on only 8%

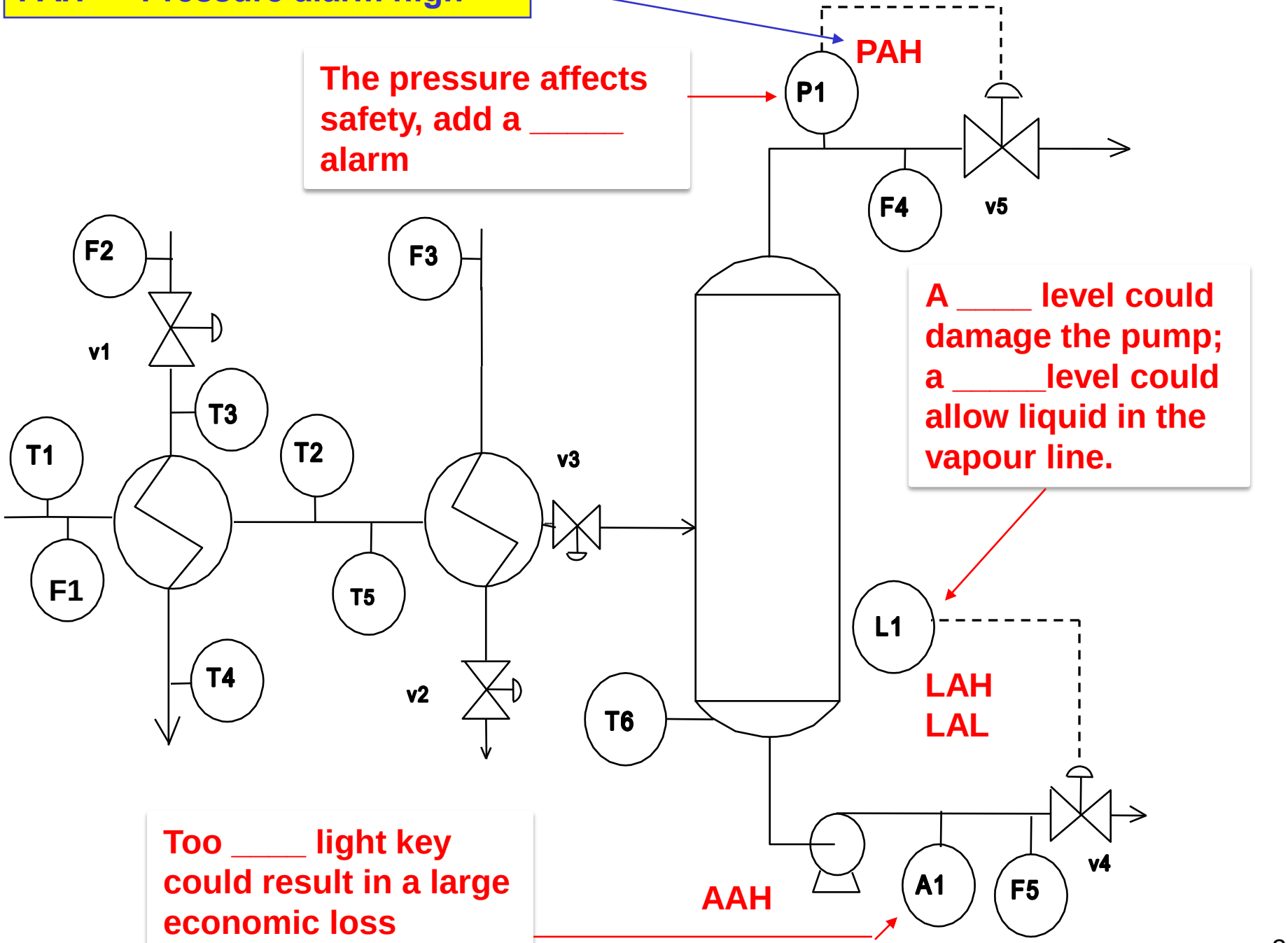
- Establish and observe clear priority ranking

- 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



PAH = “Pressure alarm high”



The pressure affects safety, add a _____ alarm

A ____ level could damage the pump; a _____level could allow liquid in the vapour line.

Too ____ light key could result in a large economic loss

3. Safety instrumented (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, but ….

3. Safety instrumented (interlock) system (SIS)

- SIS prevents “unusual” situations

  - We must be able to start up and shut down
  - Very fast “blips” might not be significant

Allow short-term violations for special conditions, e.g., fuel can flow for 5 seconds after “start-up button pushed.

Add delay to ignore very short-term violation due to, for example, flow fluctuation.

3. Safety instrumented (interlock) system (SIS)

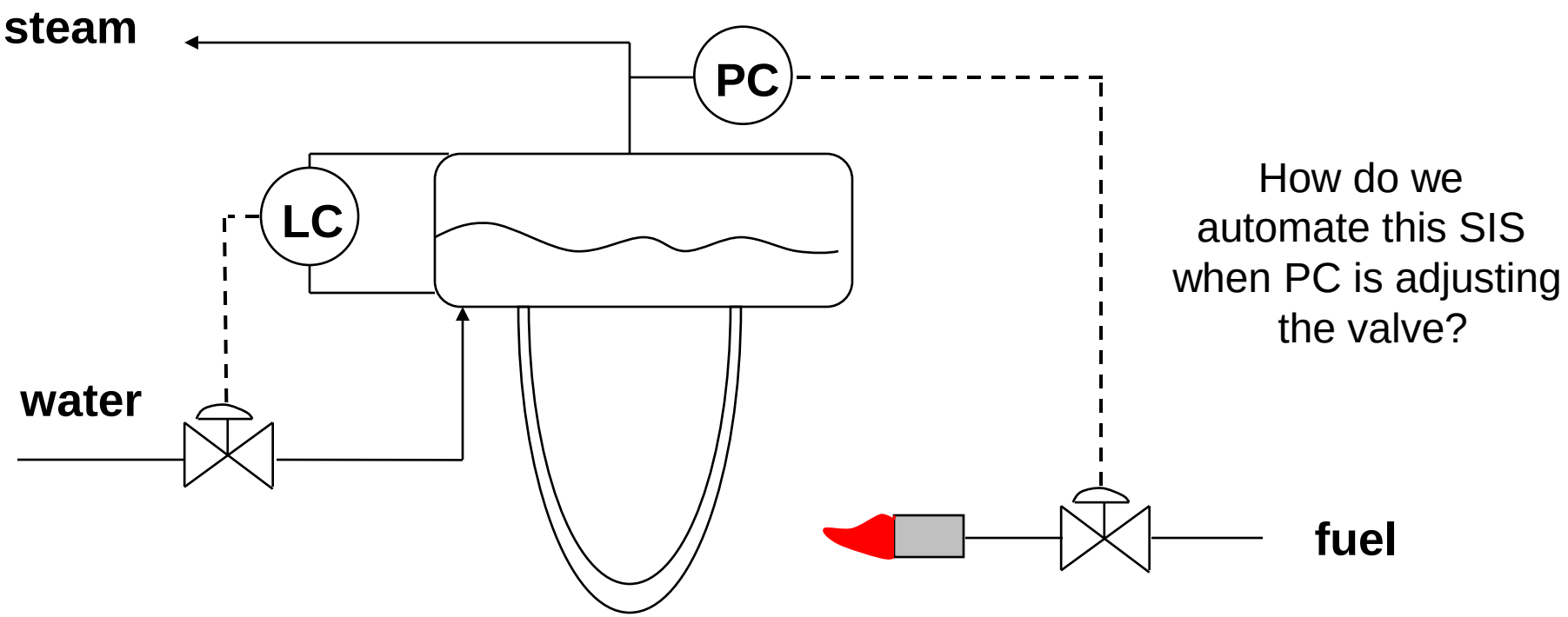
- Also called emergency shutdown system (ESS)

- SIS should respond properly to instrumentation failures
  - But, instrumentation is required for SIS?
  - Use redundancy ***and*** diversity of sensor principle
- Extreme corrective action is required and automated
  - More aggressive than process control (BPCS)
- Alarm to operator when an SIS takes action
- Video: `http://www.youtube.com/watch?v=cvk8Tv38y28`

3. Safety instrumented (interlock) system (SIS)

The automation strategy is usually simple, for example,

If L123 < $L123_{min}$; then, reduce fuel to zero

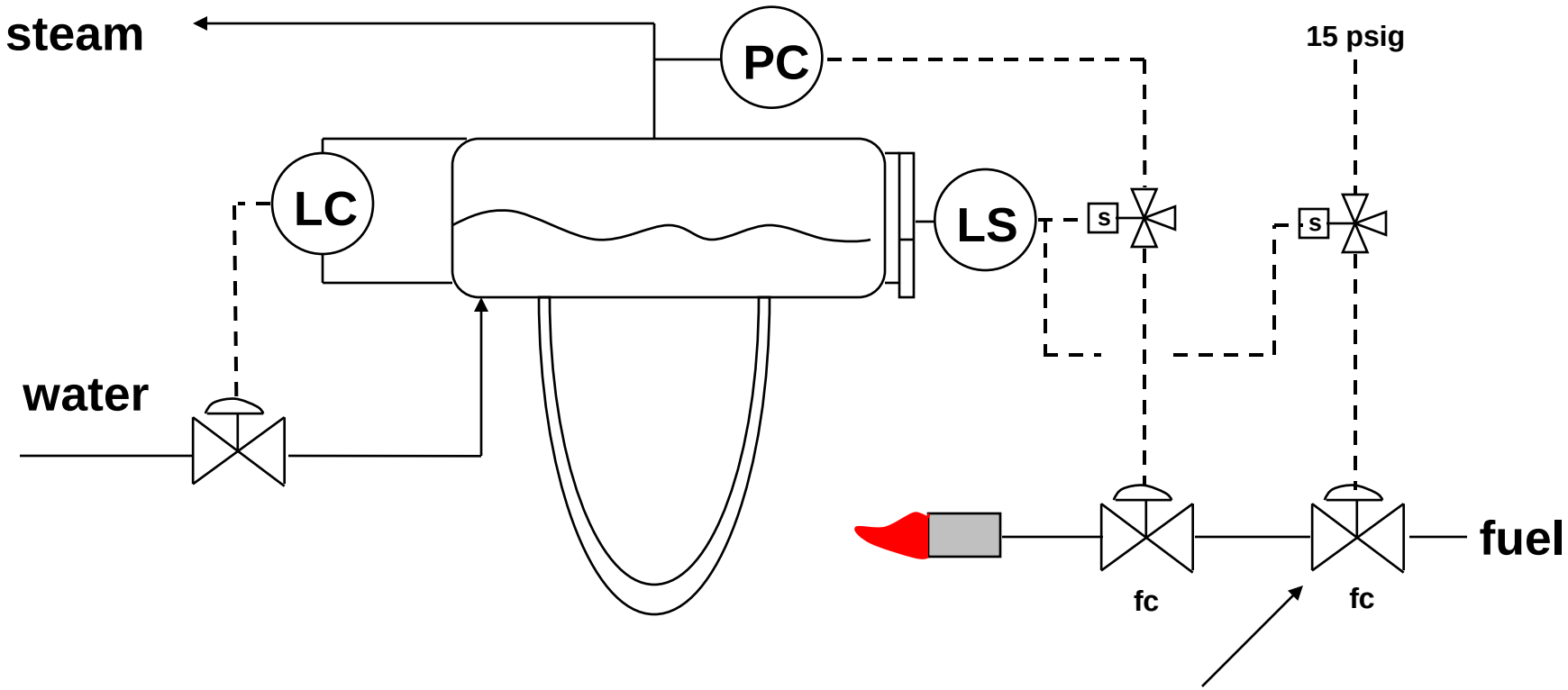


If L123 < $L123_{min}$; then, reduce fuel to zero

LS = level switch, note that separate sensor is used

= solenoid valve (open/closed)

fc = fail closed



3. Safety instrumented (interlock) system (SIS)

Three-way solenoid valve

http://www.electric-valves.cn/3-way-brass-ball-valve.html

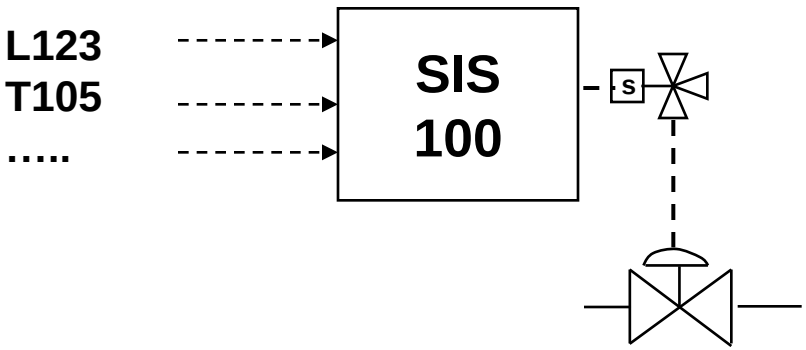
Question: how do you maintain these systems?

- Annual checks on valves
- Calibration for sensors
- Sensor failure?

3. Safety instrumented (interlock) system (SIS)

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

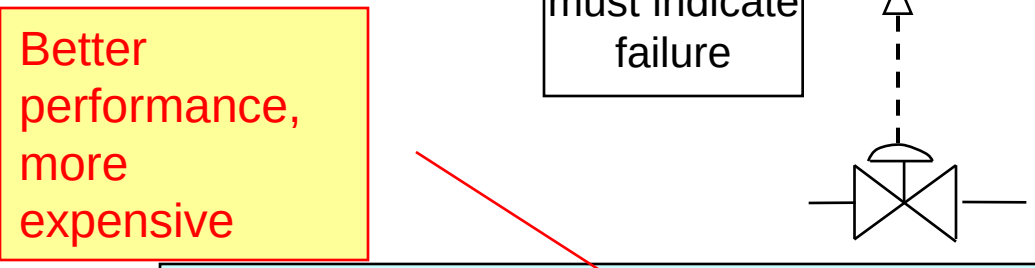
If L123 < $L123_{min}$; or
If T105 > $T105_{max}$
…….
then, reduce fuel to zero

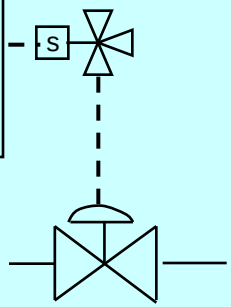


3. Safety instrumented (interlock) system (SIS)

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

	False shutdown	Failure on demand
T100 ---------> 1 out of 1 must indicate failure	5×10^{-2}	5×10^{-3}
T100 ---------> 2 out of 3 must indicate failure T101 ---------> T102 --------->	4.2×10^{-5}	1.0×10^{-4}





Same variable, multiple sensors!

Risk matrix for selecting SIS design

Event severity

	low	moderate	high
extensive	Medium 2	Major 3	Major 3
serious	Minimal 1	Medium 2	Major 3
minor	Minimal 1	Minimal 1	Medium 2

Event likelihood

Table entries

word = qualitative risk description

number = required safety integrity level (SIL) ⟶

Safety Integrity Levels

(Prob. of failure on demand)

1 = .01 to .1

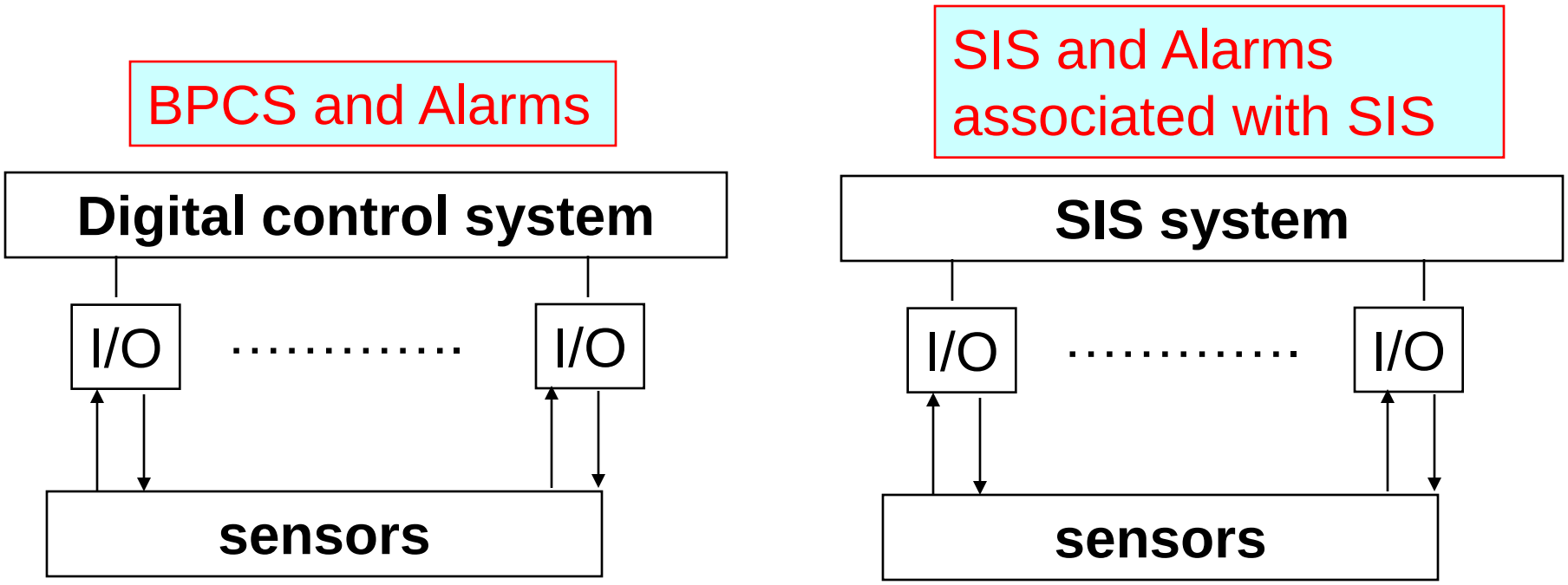
2 = .001 to .01

3 = .0001 to .001

Selection documented for legal requirements

3. Safety instrumented (interlock) system (SIS)

We desire independent protection layers, without common-cause failures - Separate systems

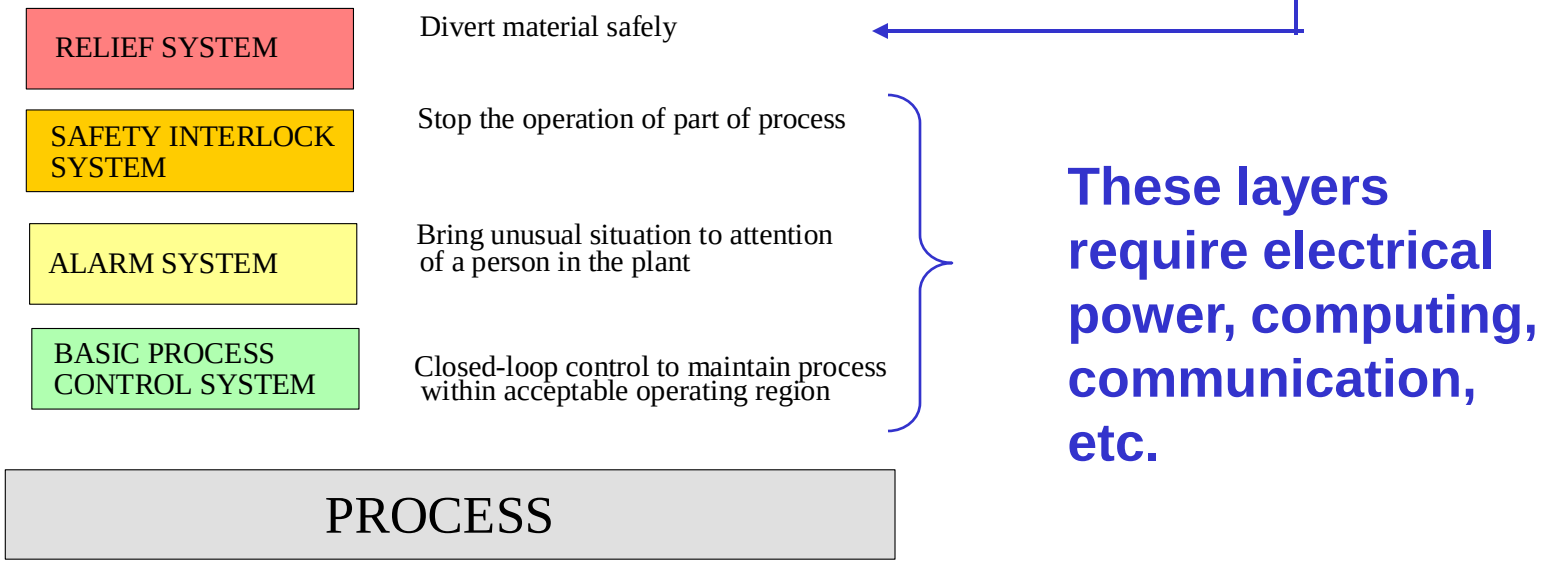


Key concept in process safety - redundancy!

What do we do if a major incident occurs that causes

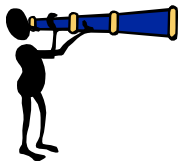
- loss of power or communication
- a computer failure (hardware or software)

SAFETY STRENGTH IN DEPTH !



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

4. Safety relief system



What's in this topic?

RELIEF SYSTEM

SAFETY INTERLOCK SYSTEM

ALARM SYSTEM

BASIC PROCESS CONTROL SYSTEM

- Location
- Equipment selection
- Documenting on drawings
- Maximum capacity

Relief systems in process plants

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

  - Also, we must protect against unexpected vacuum!

- Naturally, best to prevent the pressure increase

  - large disturbances, equipment failure, human error, power failure, ...

- Relief systems provide an exit path for fluid

- Benefits: safety, environmental protection, equipment protection, reduced insurance, compliance with governmental code

Location of relief systems

- 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

  - **these do not count as relief**: hand valve, control valve (even fail open)

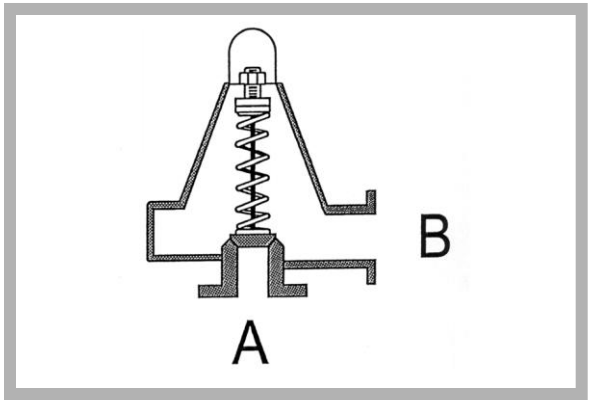
- Remember, this is the **last resort**, when all other safety systems have not been adequate and a fast response is required!

Standard relief methods

- Basic principle: No external power required - **self actuating** - pressure of process provides needed force!

- **Valves** - close when pressure returns to acceptable value
  - Relief valve - liquid systems
  - Safety valve - gas and vapour systems including steam
  - Safety relief valve - liquid and/or vapour systems

- Pressure of protected system can exceed the set pressure.



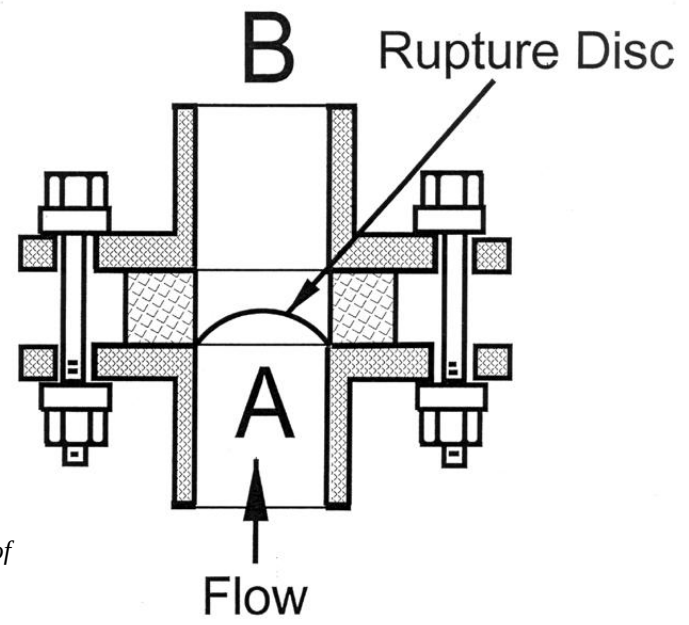
Safety relief control valve

http://www.yongyivalves.com/High-Pressure-and-High-Temperture-Safety-Relief-Valve-59.html

Standard relief methods

- Basic principle: No external power required - **self acting**

- **Rupture disks or burst diaphragms** - must be replaced after opening



Rupture disks or burst diaphragms

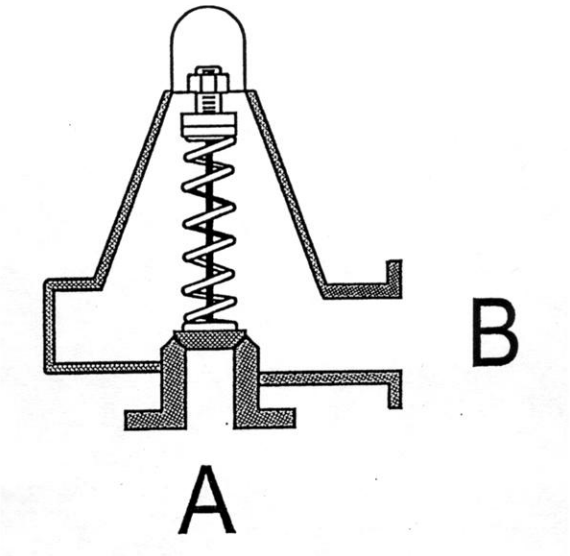
http://www.valvecenter.co.uk/products.html

Some information on relief valves

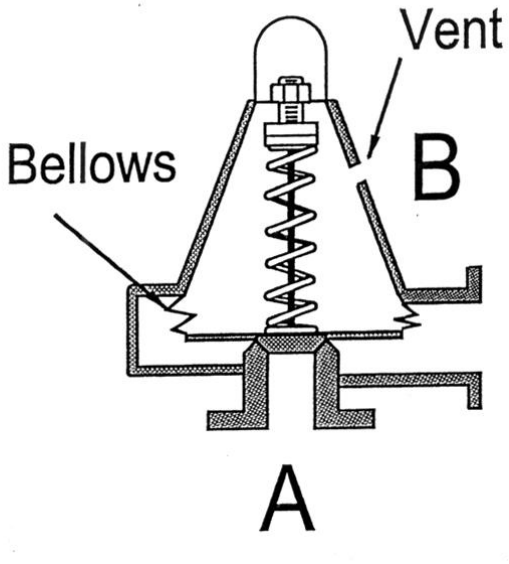
Two types of designs determine influence of pressure immediately after the valve

- Conventional valve -pressure after the valve affects the valve lift and opening
- Balanced valve - pressure after the valve does not affect the valve lift and opening

Conventional



Balanced



Some information on relief valves

Advantages

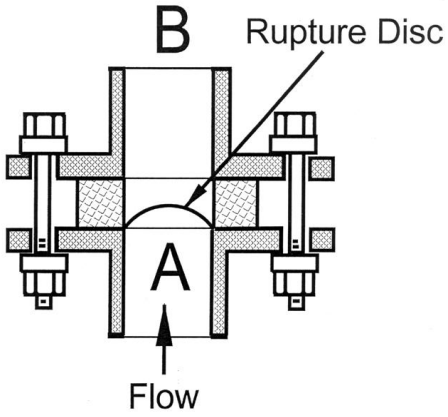
- simple, low cost and many commercial designs available
- regain normal process operation rapidly because the valve closes when pressure decreases below set value

Disadvantages

- can leak after once being open (O-ring reduces)
- not for very high pressures (20,000 psi)
- if oversized, can “chatter”, leading to damage and failure (do not be too conservative; the very large valve is not the safest!)

Some information on rupture disks/ burst diaphragms

- A wide range of materials and designs are available

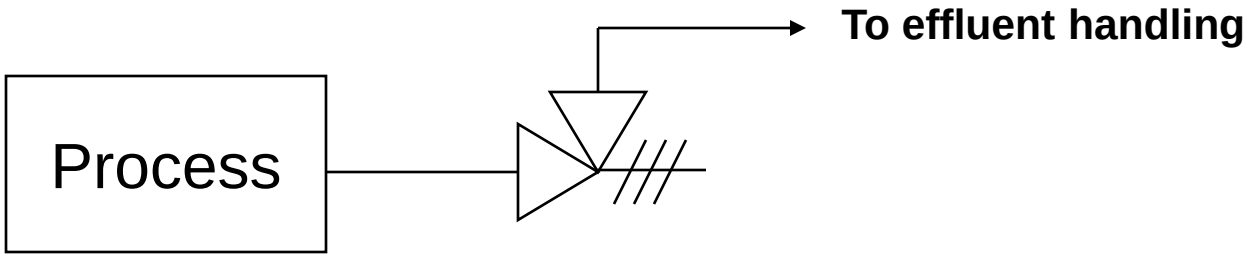


- **Advantages**
  - no leakage until the burst
  - rapid release of potentially large volumes
  - high pressure applications
  - corrosion leads to failure, which is safe
  - materials can be slurries, viscous, and sticky

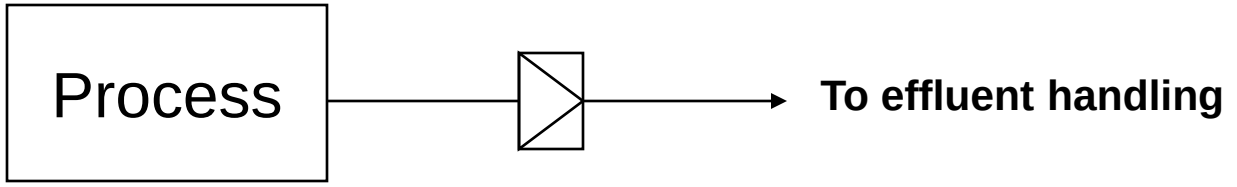
- **Disadvantages**
  - must shutdown the process to replace
  - greater loss of material through relief
  - poorer accuracy of relief pressure

Showing relief systems on process & instrumentation (P&I) drawings

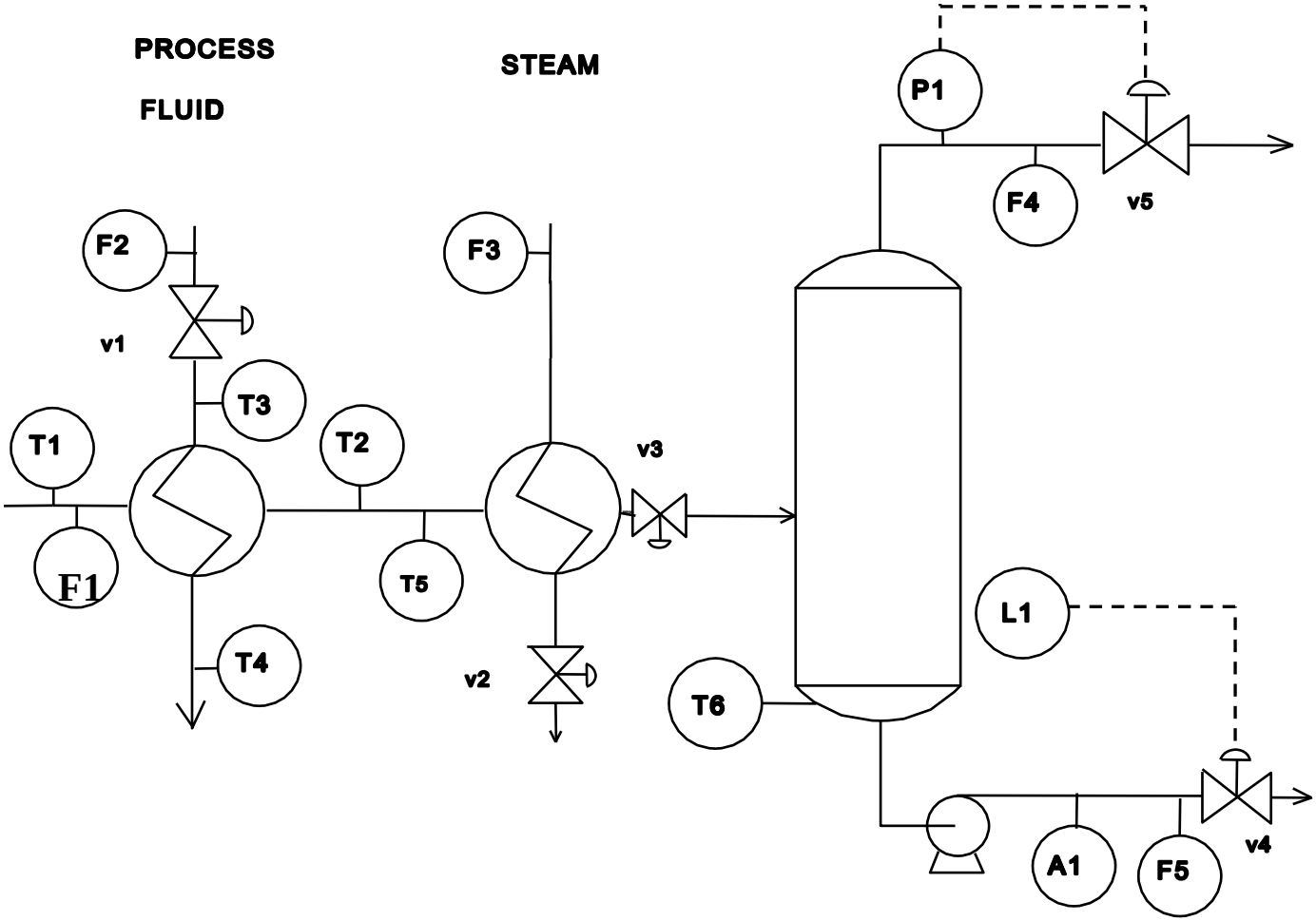
Spring-loaded safety relief valve

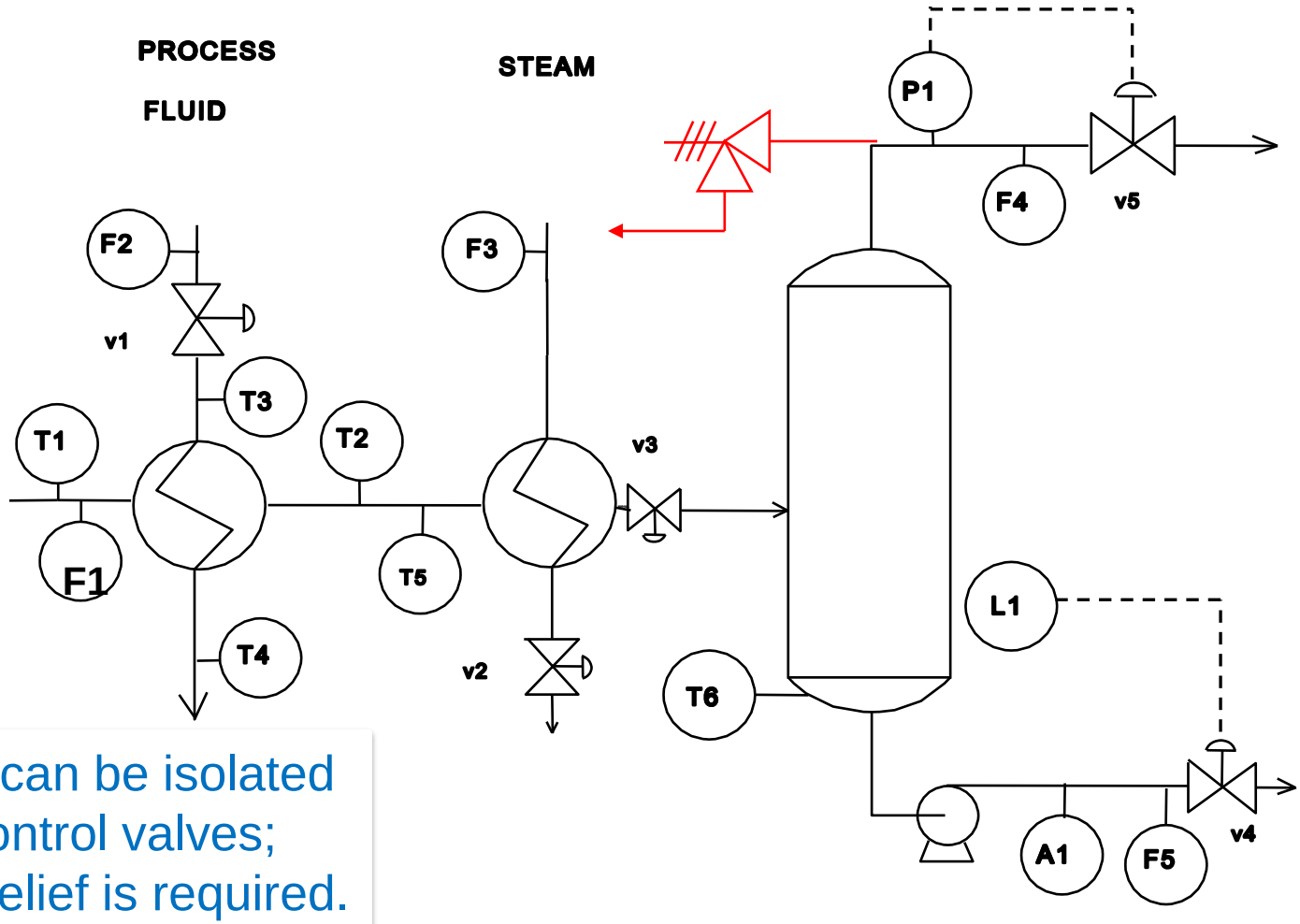


Rupture disc



Add relief system to the following process drawing

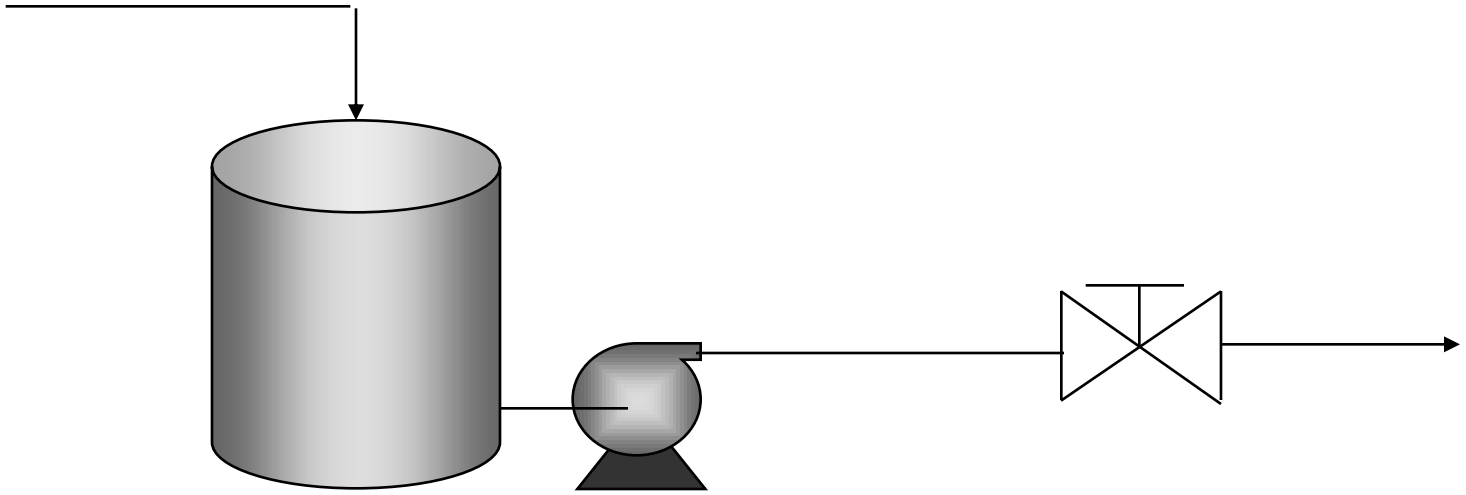




The drum can be isolated with the control valves; pressure relief is required.

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

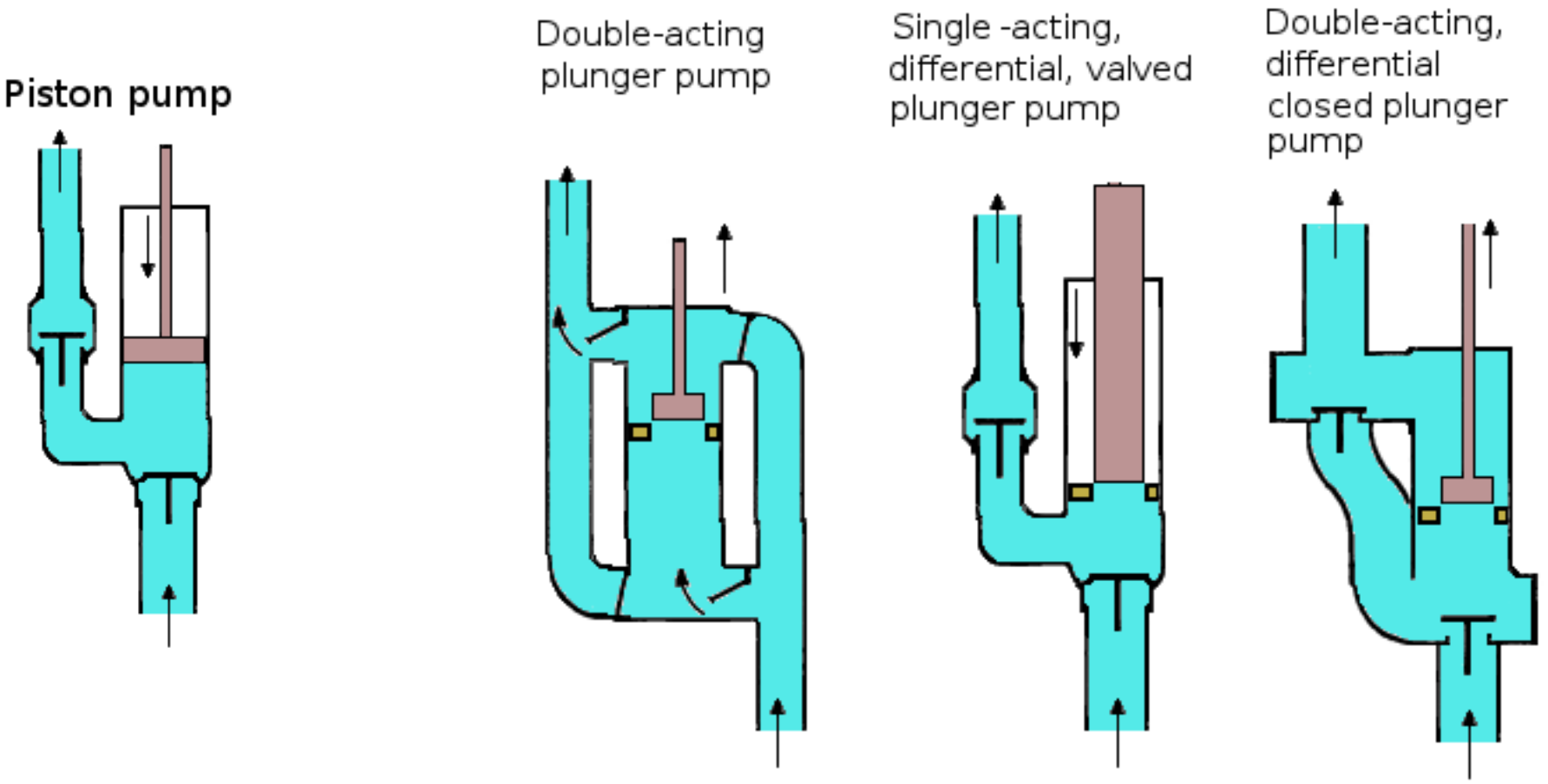
Add relief system to the following process drawing



Positive displacement pump

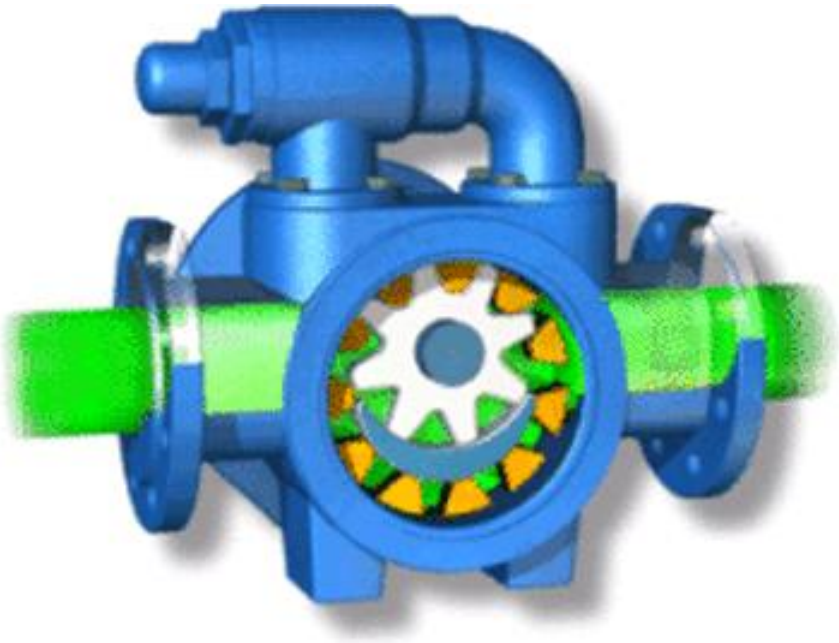
***Hint*: relief does not always need to be wasted**

Positive displacement piston pump



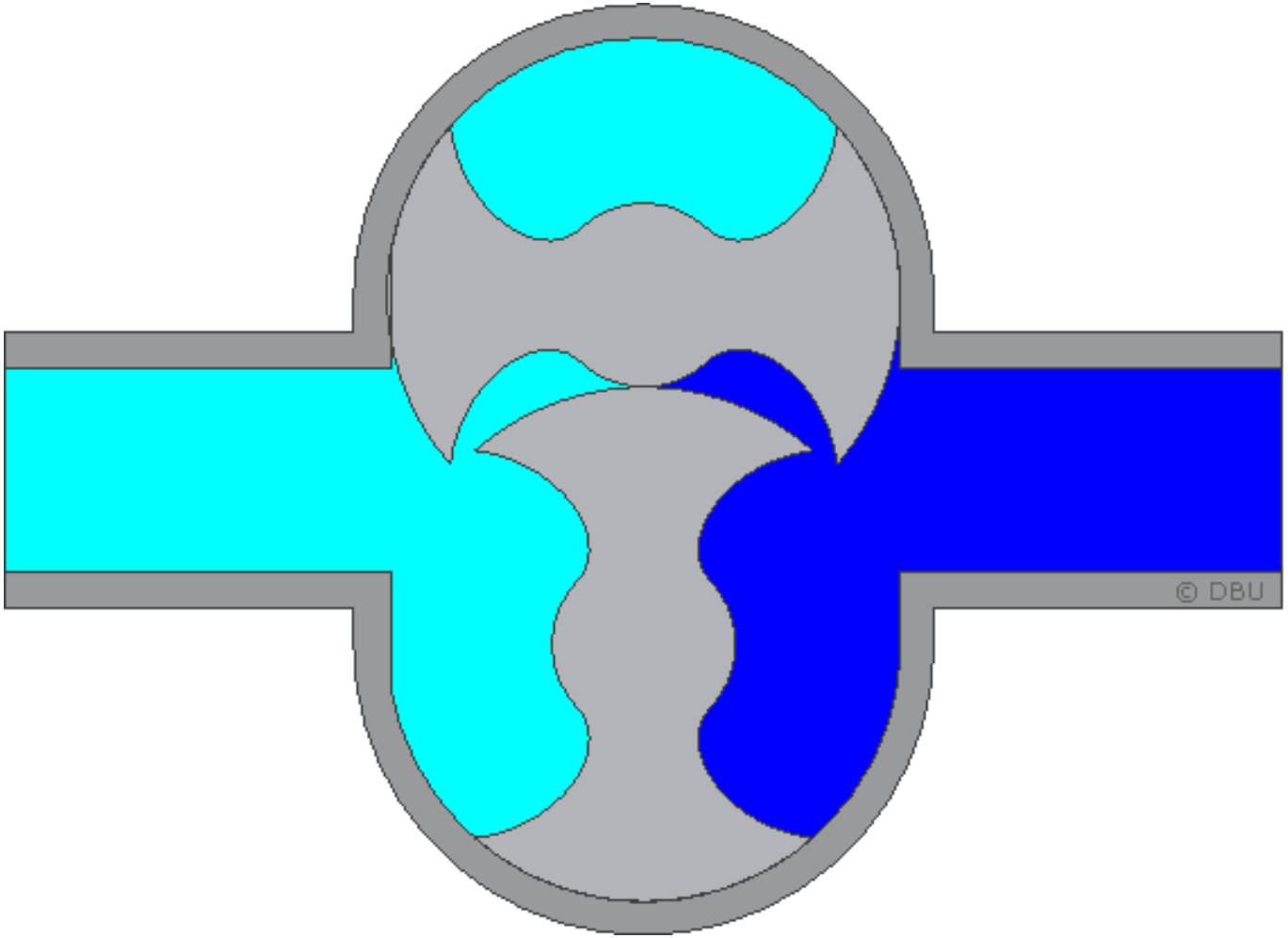
http://upload.wikimedia.org/wikipedia/commons/9/94/Piston_VS_Plunger_Pump.png

Positive displacement gear pump



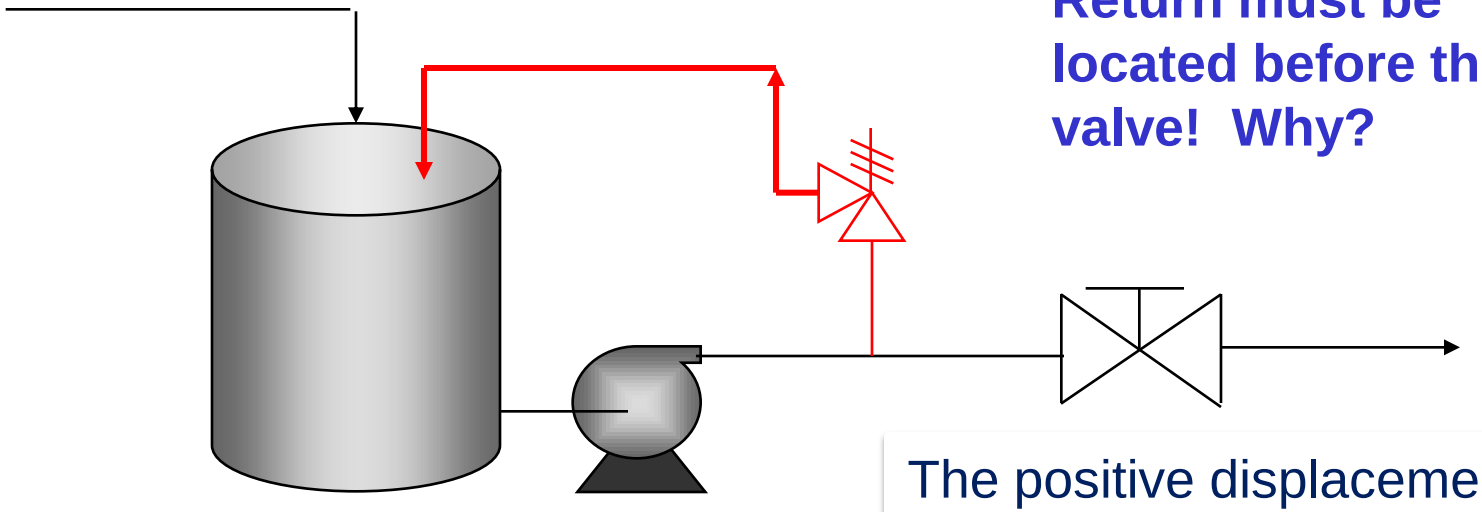
http://liquidprocess.com/

Positive displacement lobe pump



http://en.wikipedia.org/wiki/File:Lobbenpomp.gif

Add relief system to the following process drawing



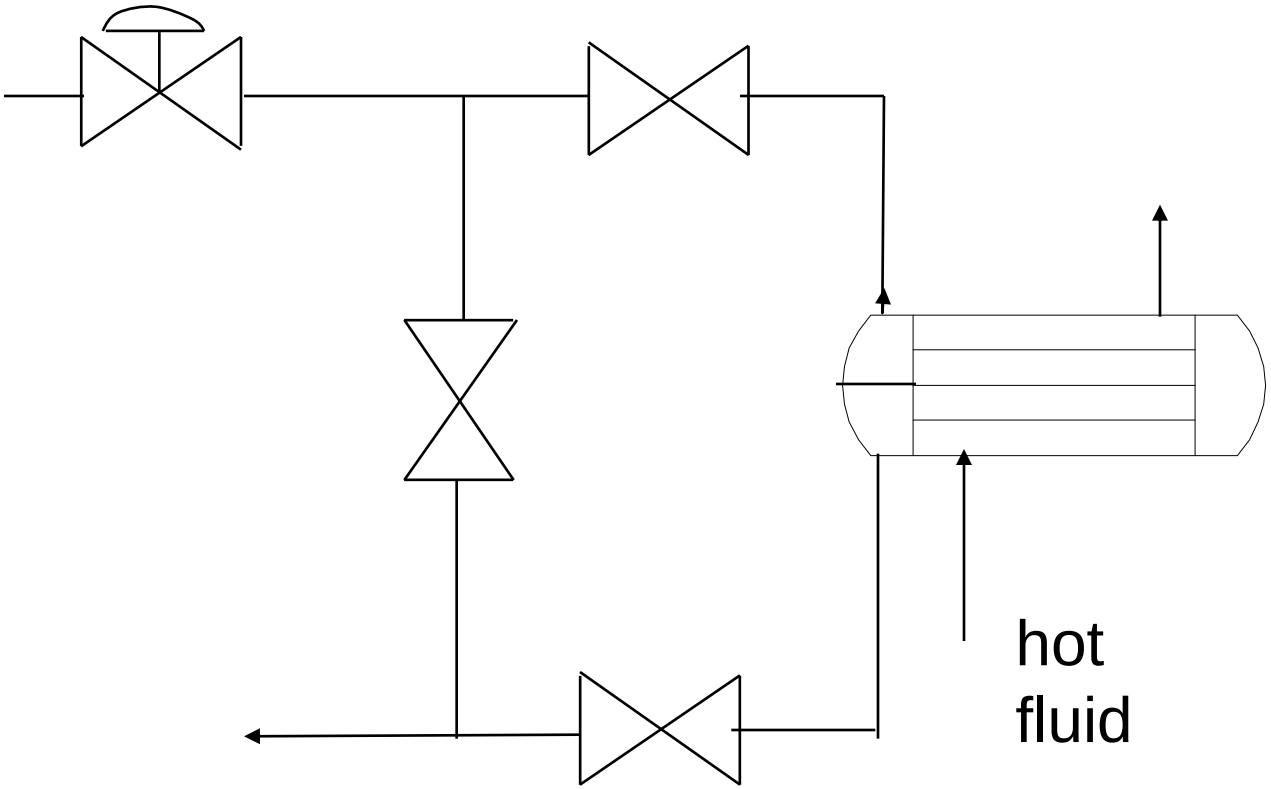
Return must be located before the valve! Why?

Positive displacement pump

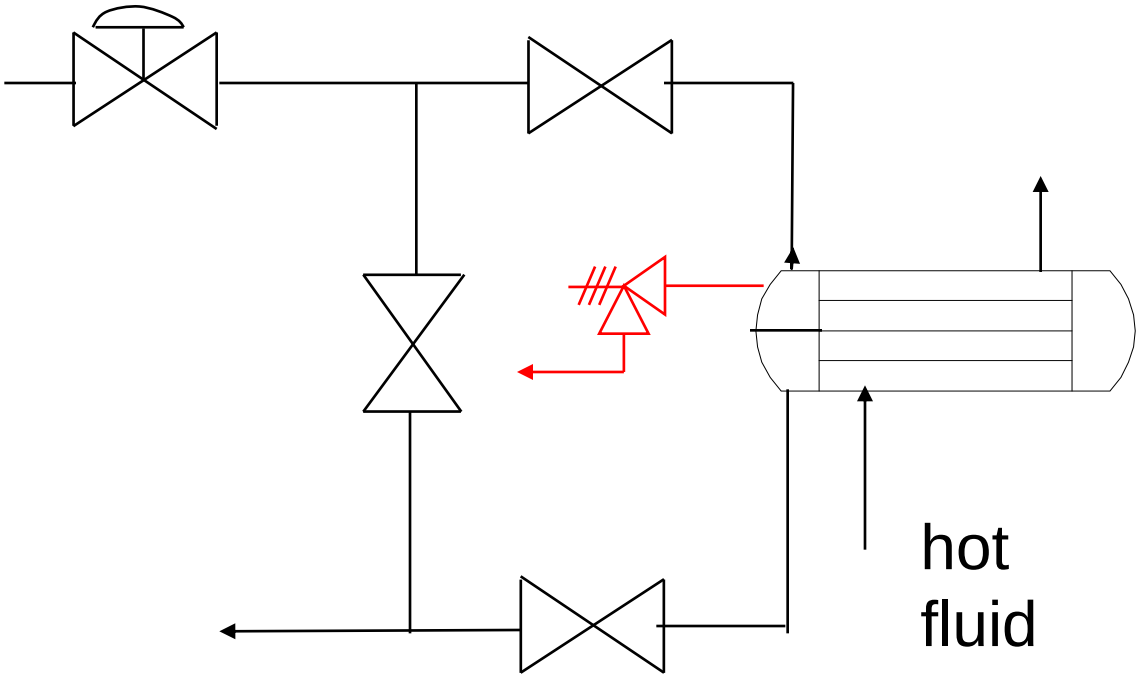
The positive displacement pump will be damaged if the flow is stopped; we need to provide relief.

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

Add relief system to the following process drawing



Add relief system to the following process drawing



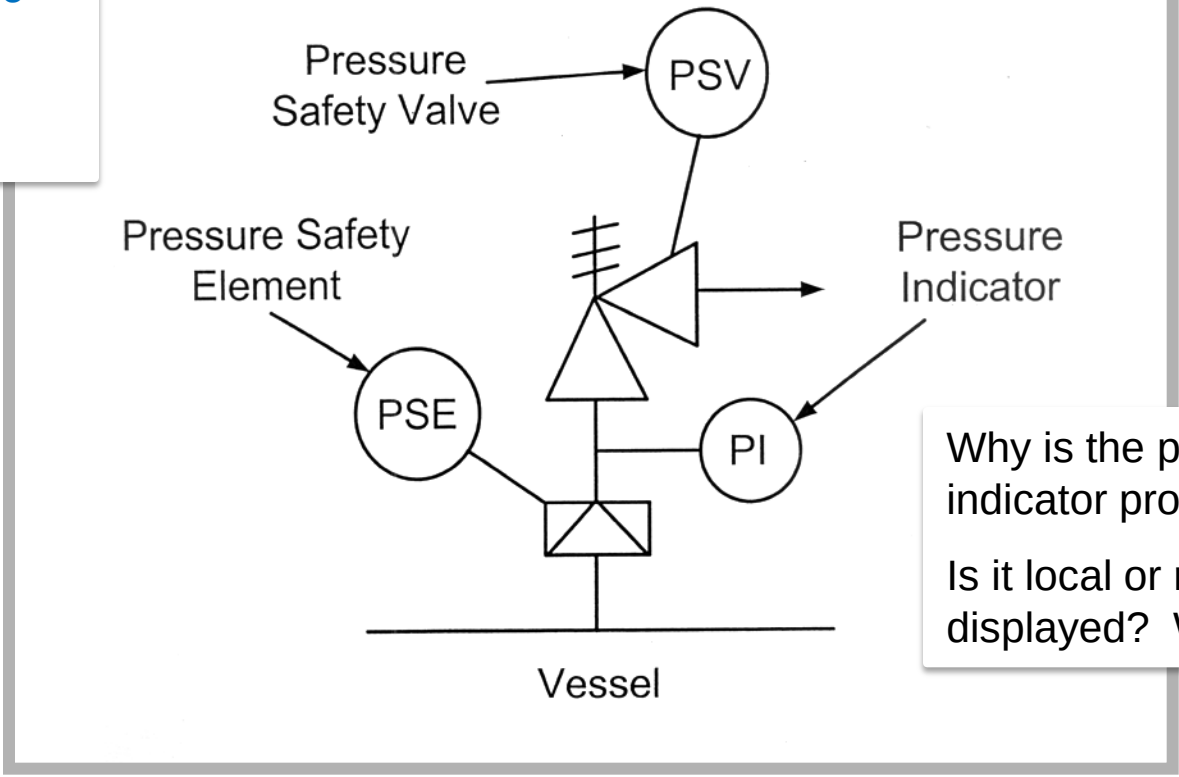
The extra “hand” valves enable us to isolate and remove the heat exchanger without stopping the process.

The shell side of the heat exchanger can be isolated; we need to provide relief.

We would like to recover without shutdown.

In some cases, relief valve and diaphragm are used in series - why?

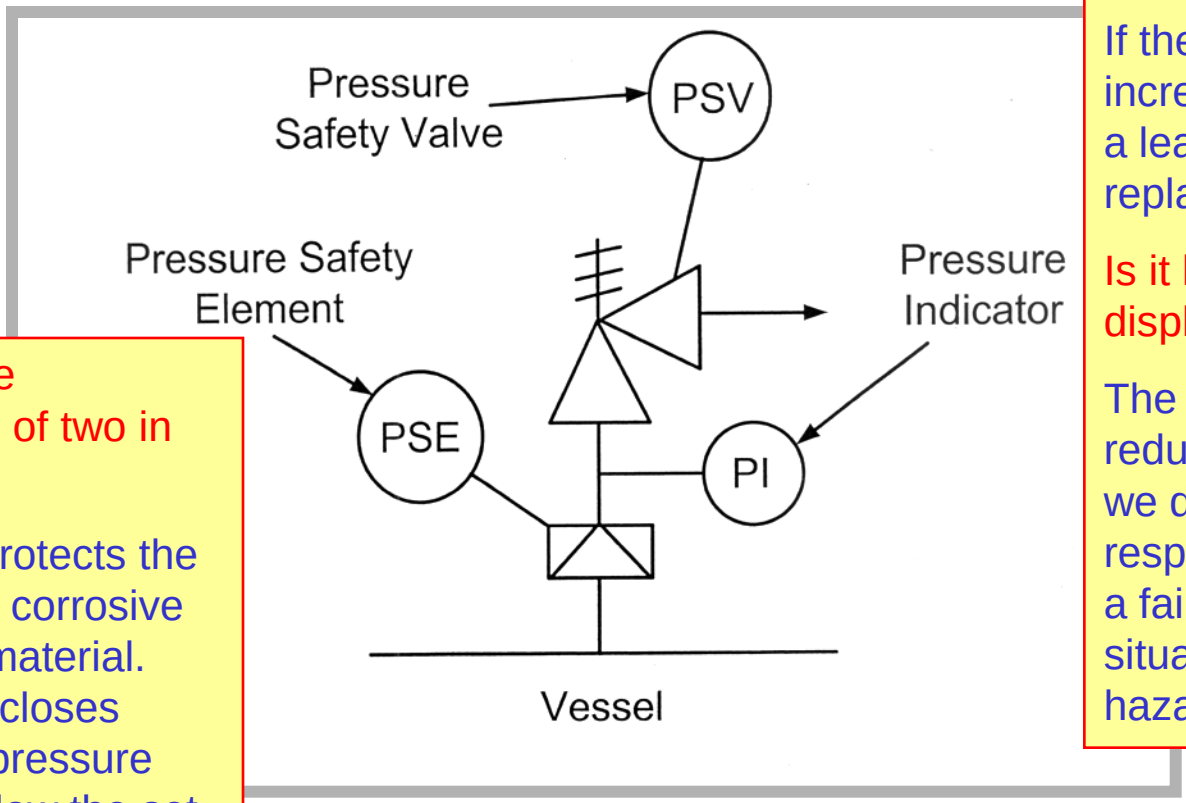
- What is the advantage of two in series?
- Why not have two relief valves (diaphragms) in series?



Why is the pressure indicator provided?

Is it local or remotely displayed? Why?

In some cases, relief valve and diaphragm are used in series - why?



- 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.

Why is the pressure indicator provided?

If the pressure increases, the disk has a leak and should be replaced.

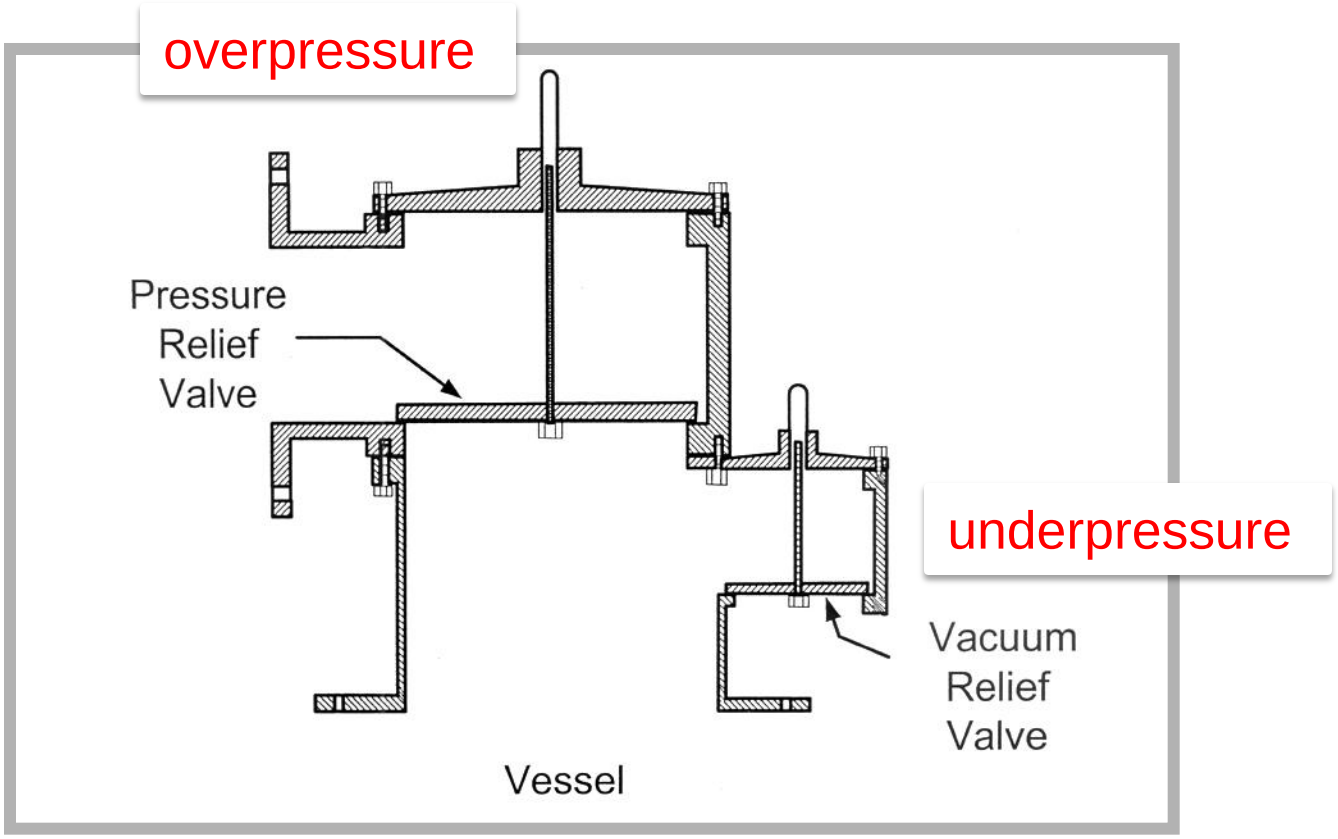
Is it local or remotely displayed? Why?

The display is local to reduce cost, because we do not have to respond immediately to a failed disk - the situation is not hazardous.

by CCPS/American Institute of Chemical Engineers and copied with the permission of

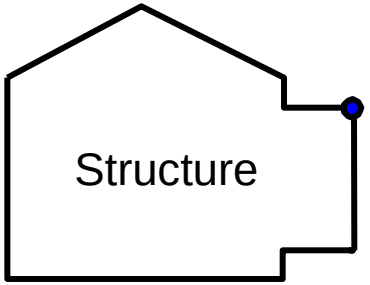
We should also protect against excessive vacuum

The following example uses buckling pins

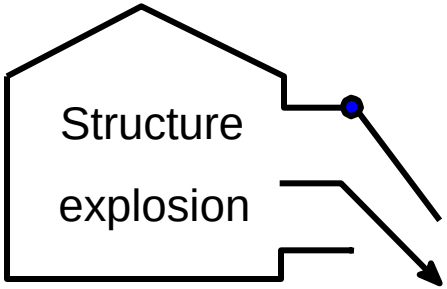


Some vapour and dust explosions require vents

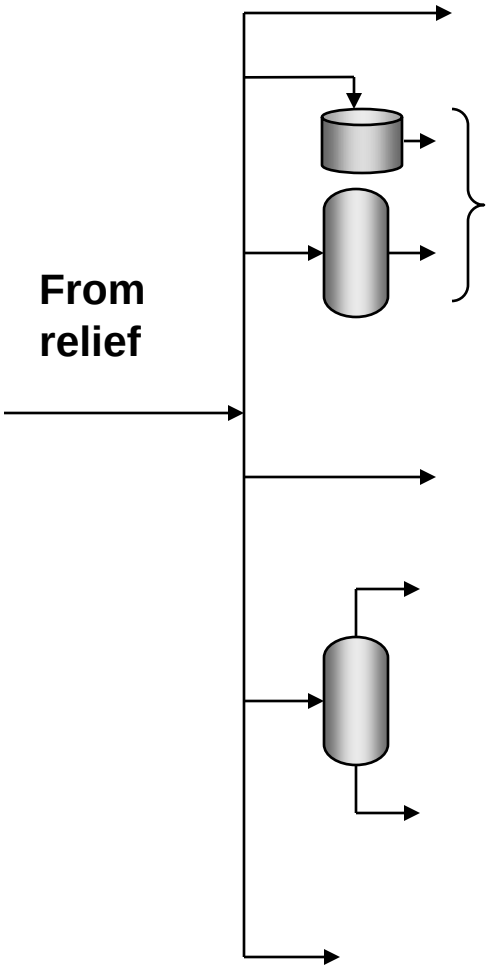
Control and direct the explosion



vent closed



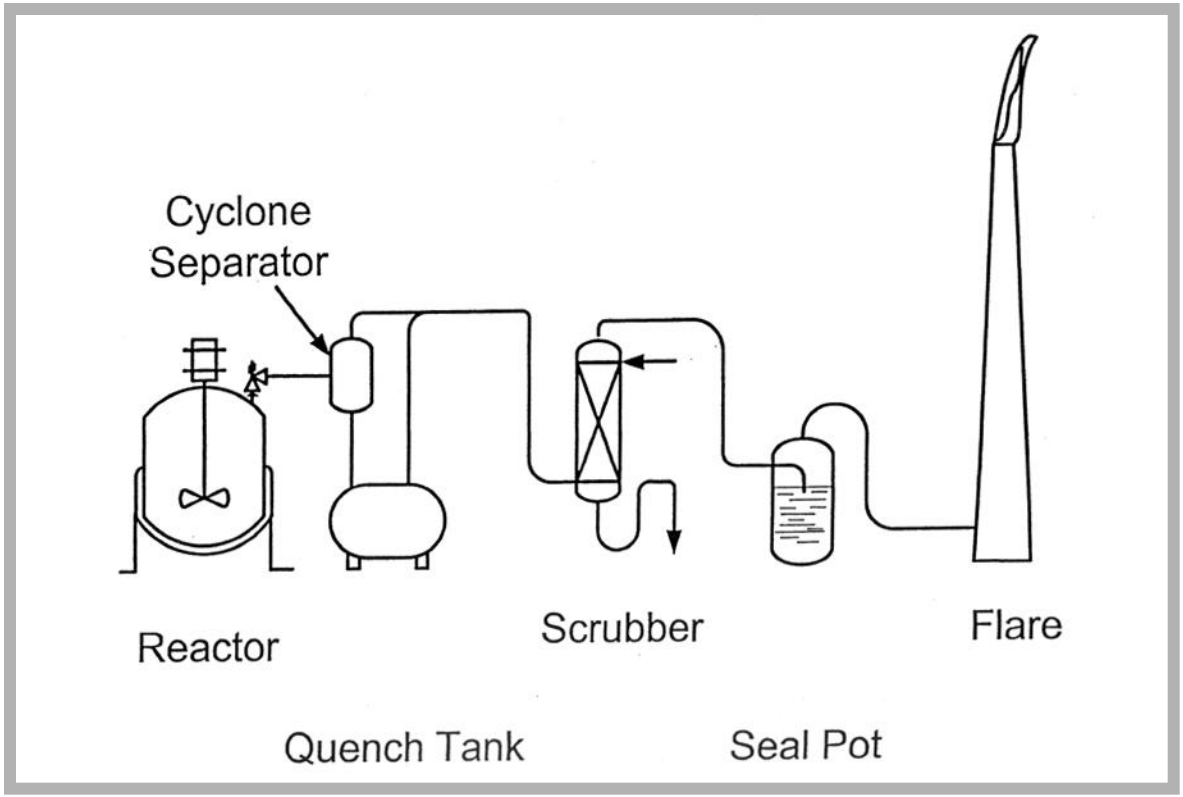
We must safely process or dispose of material from relief system!



To environment	Vent steam, air
Holding for later processing	Waste water treating
Recycle to process	Fuel gas, fuel oil, solvent
Recover part to process	Fuel gas, fuel oil, solvent
Immediate neutralization	Flare, toxic materials, pH

We must safely process or dispose of material from relief system!

A process example with several forms of effluent handling

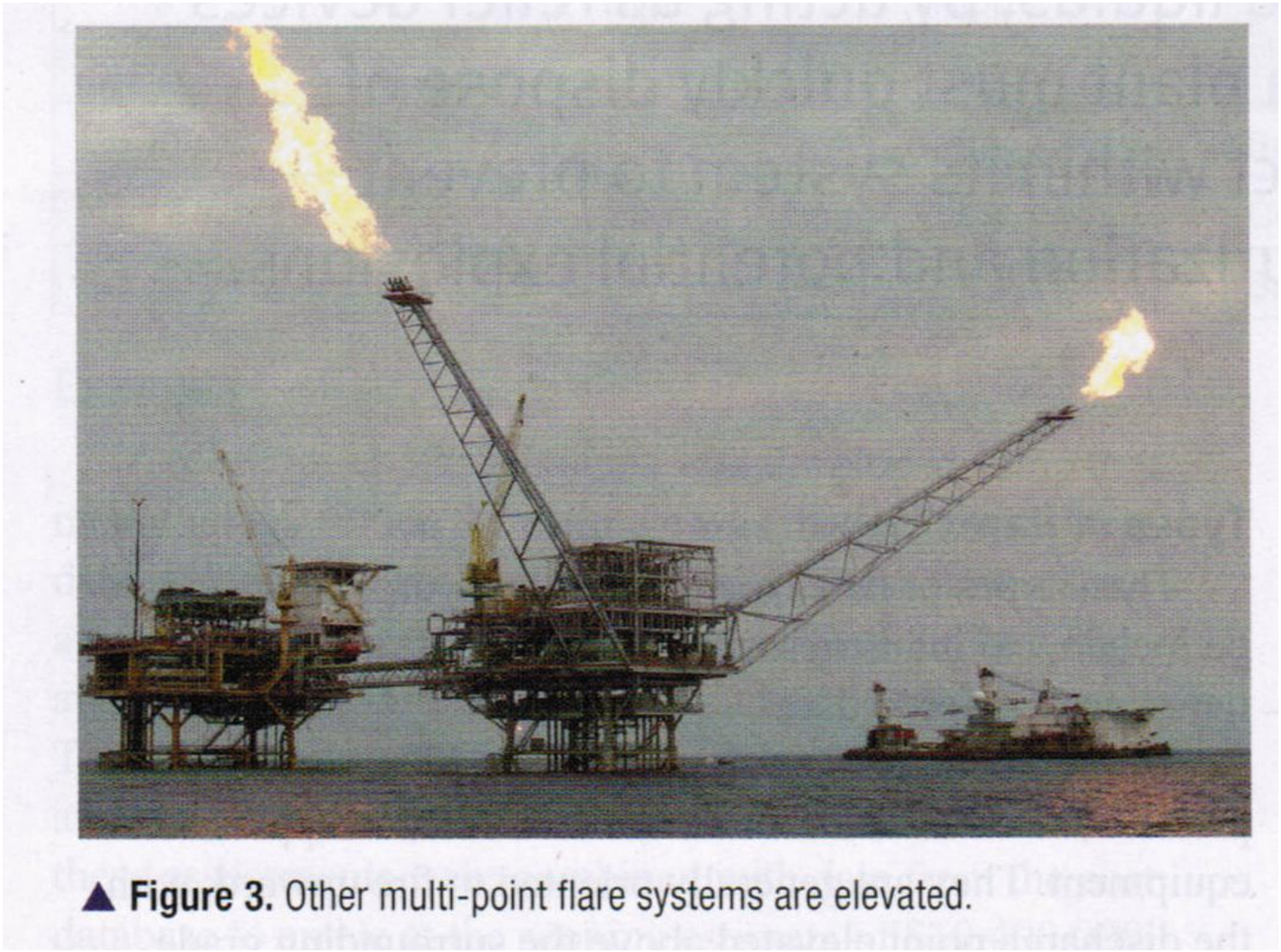


Picture of typical elevated process flare

▲ **Figure 1.** Typical elevated single-point flares fire upward.

Bader, A., C. Baukal, and W. Bussman, Chem. Engr. Progress, July 2011, Pg 45-50.

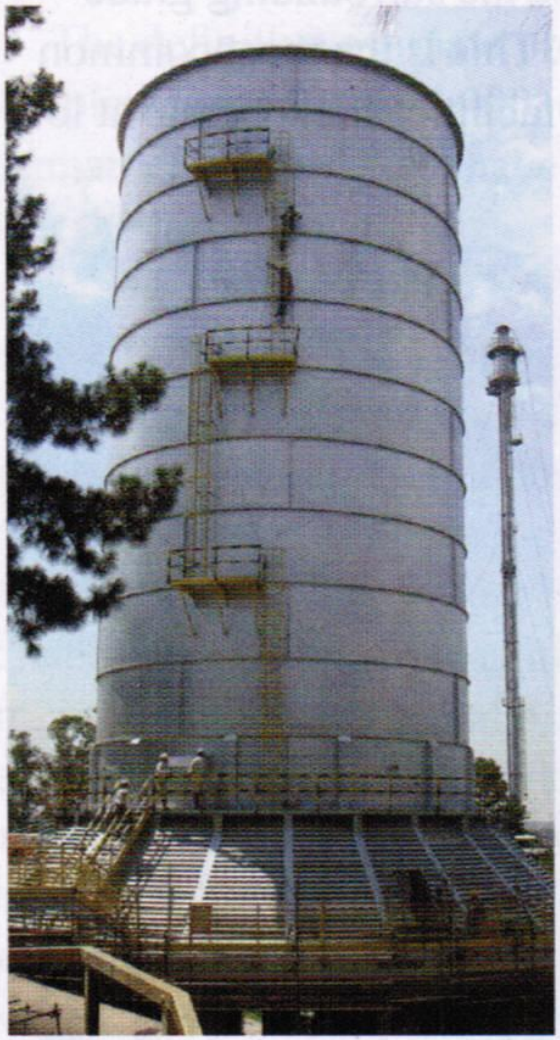
Everything is more difficult on a platform



▲ **Figure 3.** Other multi-point flare systems are elevated.

Bader, A., C. Baukal, and W. Bussman, Chem. Engr. Progress, July 2011, Pg 45-50.

Ground flares



▲ **Figure 4.** Enclosed ground flares shield the surrounding community from radiation and noise. Here, an enclosed ground flare is seen with an elevated flare in the background.

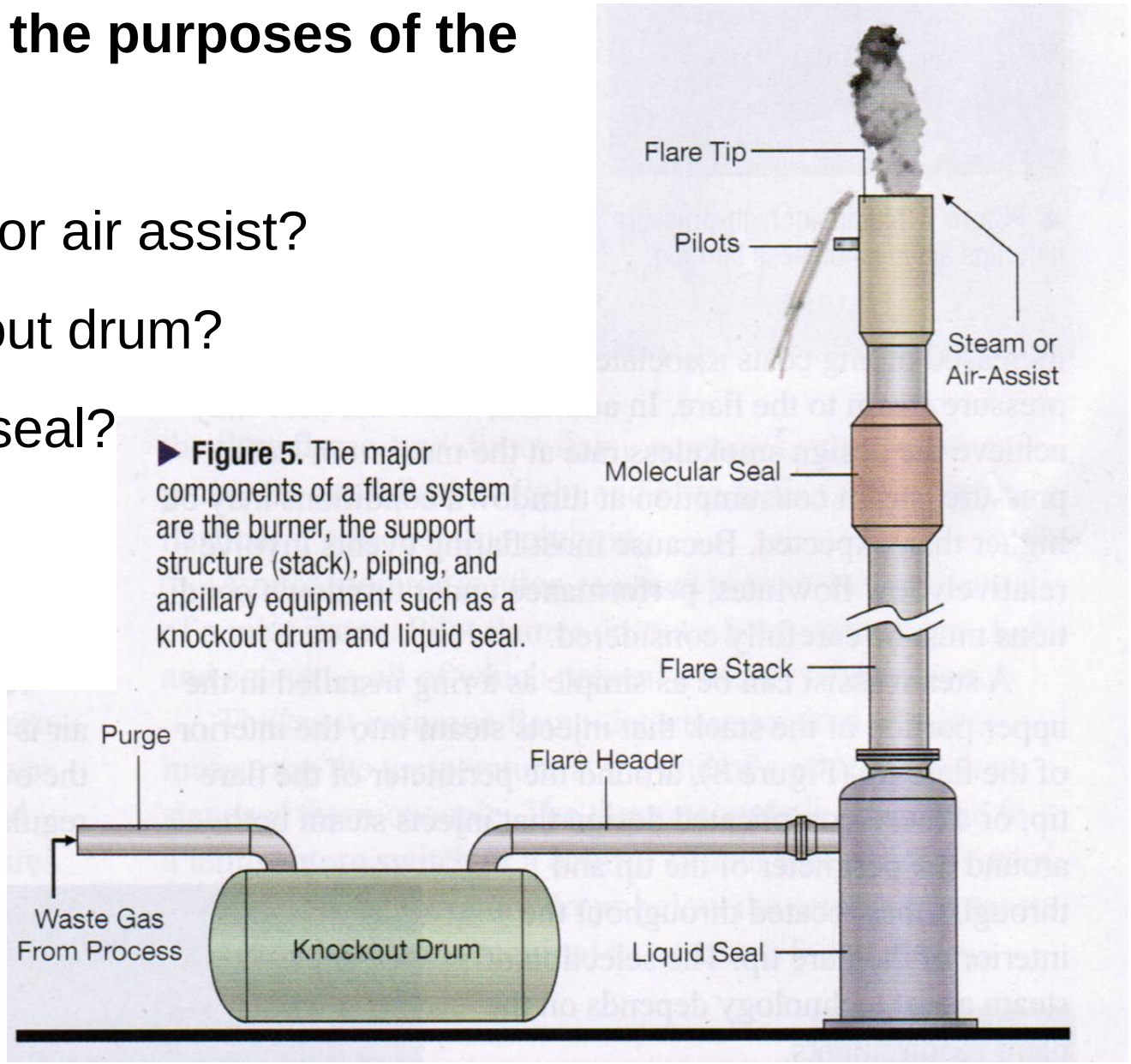
If you lived near a process plant, you would want the plant to use ground flares.

What are advantages?

Bader, A., C. Baukal, and W. Bussman, Chem. Engr. Progress, July 2011, Pg 45-50.

What are the purposes of the

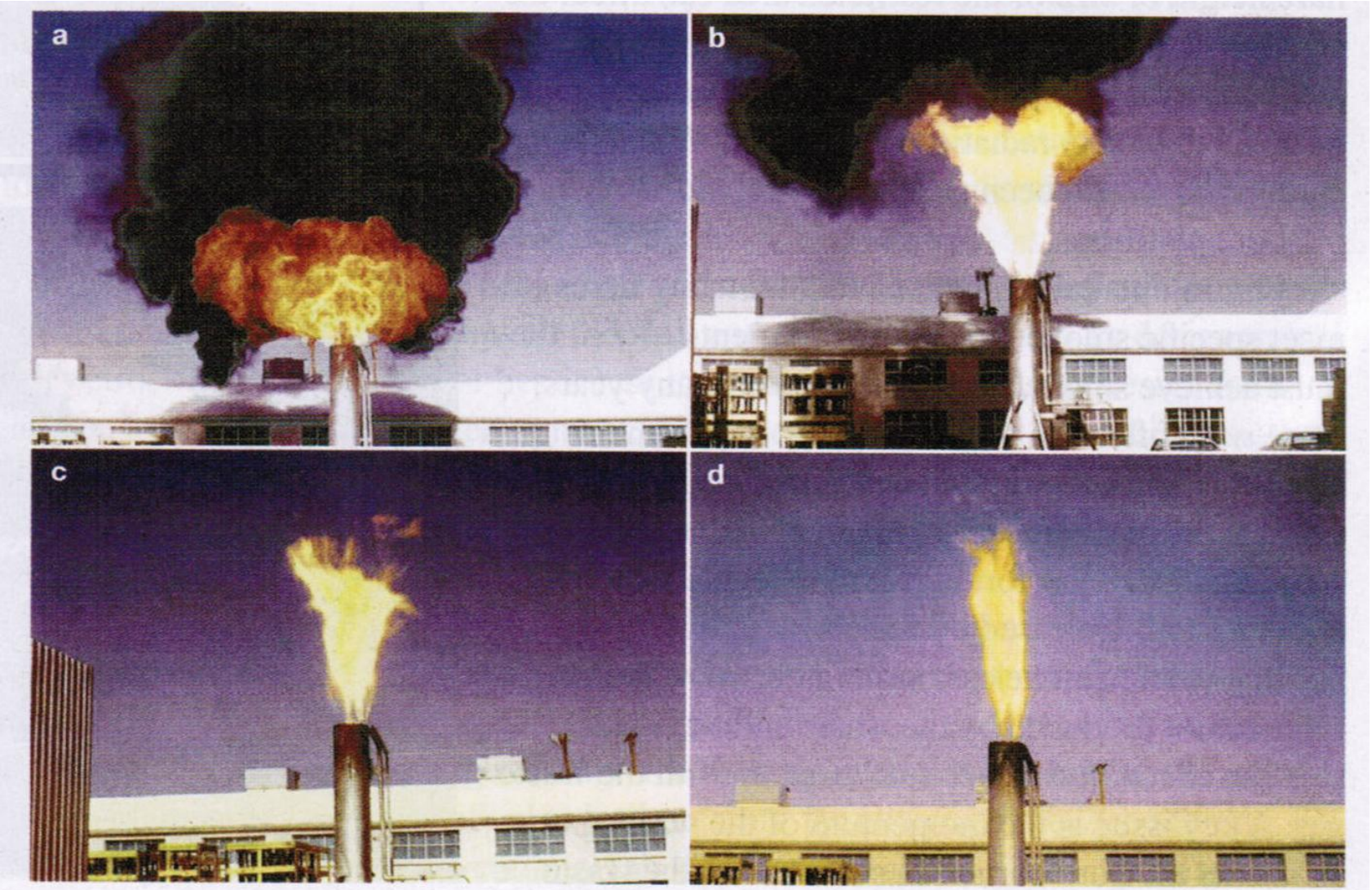
- Pilot?
- Steam or air assist?
- Knockout drum?
- Liquid seal?



▶ **Figure 5.** The major components of a flare system are the burner, the support structure (stack), piping, and ancillary equipment such as a knockout drum and liquid seal.

Bader, A., C. Baukal, and W. Bussman, Chem. Engr. Progress, July 2011, Pg 45-50.

When we do flare, we want clean combustion



▲ **Figure 9.** Air assist is effective at smoke suppression: (a) no blower air; (b) blower is started; (c) air flow is increasing; (d) smokeless burning. Image courtesy of CRC Press *(7)*.

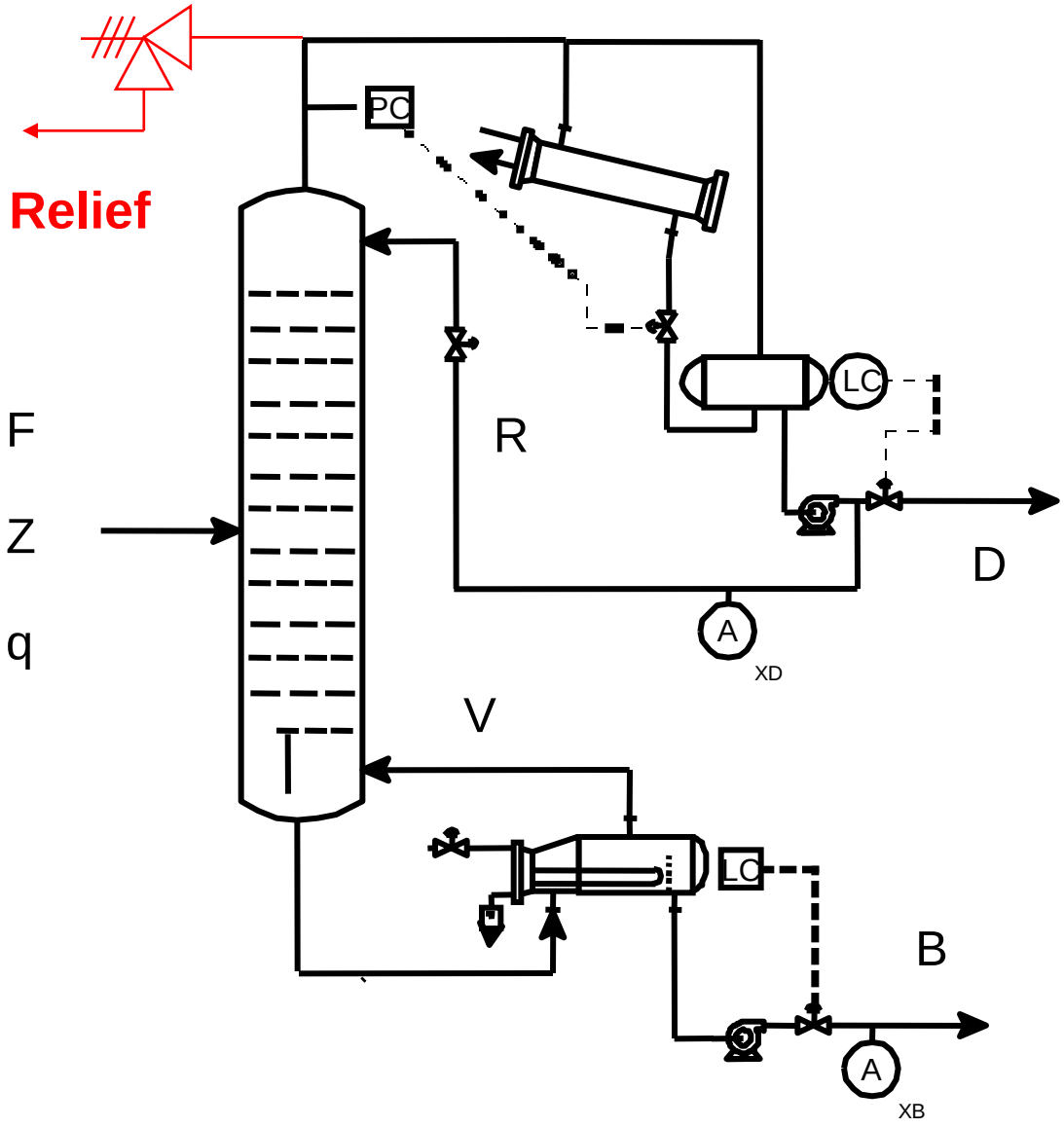
Bader, A., C. Baukal, and W. Bussman, Chem. Engr. Progress, July 2011, Pg 45-50.

Sizing relief systems

- Determine the relief flow (maximum possible)
- Determine the set pressure
  - based on process needs and equipment materials and construction
- Select the relief valve type
  - based on advantages/disadvantages of both
- Calculate the required area for flow
- Select the commercial device from vendor's specifications

Read the article posted on the course website

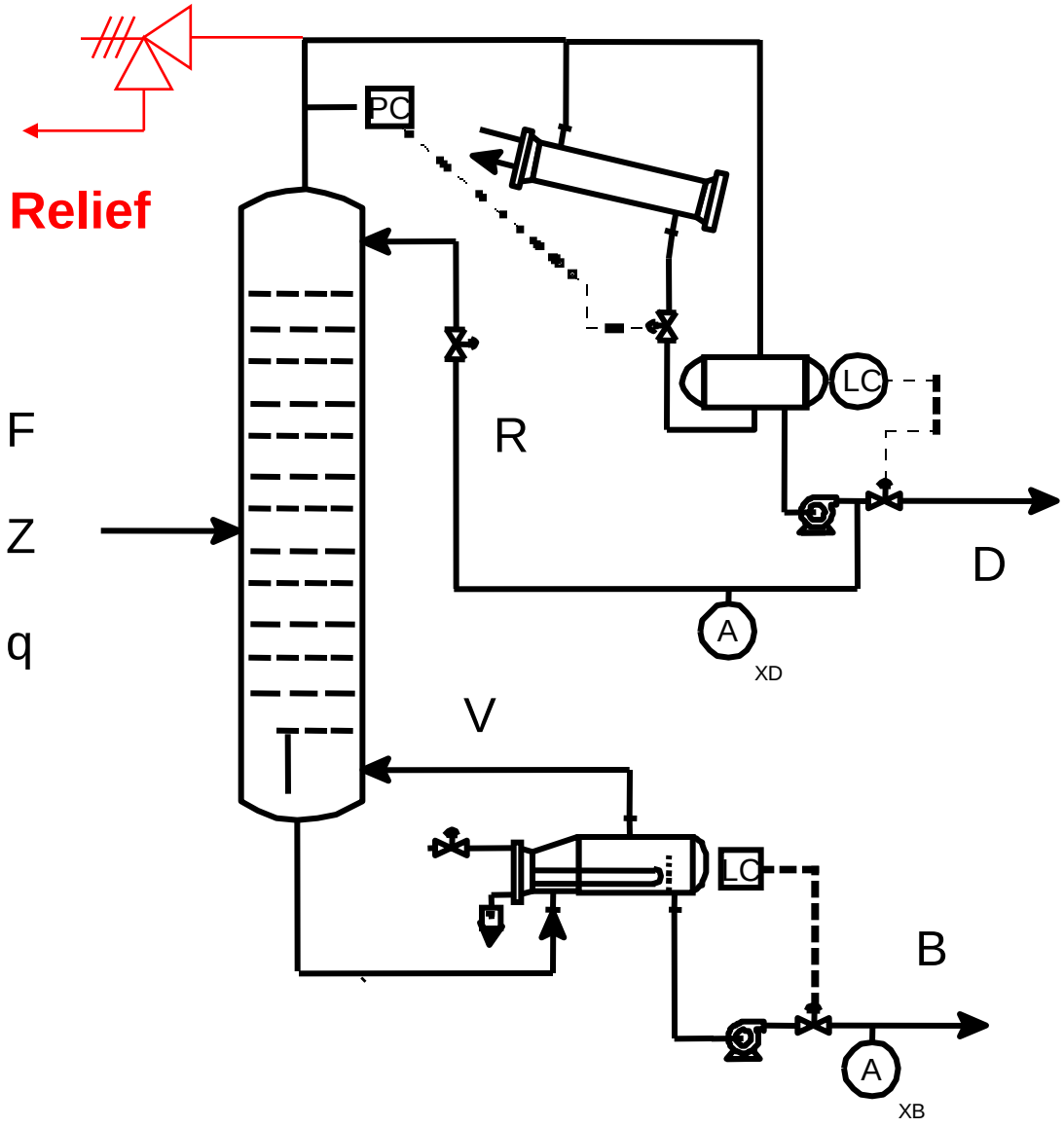
Determine the maximum flow for overhead vapour



Under what conditions is the vapour at its maximum?

[3 simultaneous conditions]

Determine the maximum flow for overhead vapour

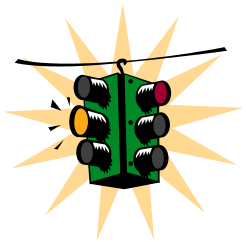


The maximum vapour occurs when

1. Maximum feed vapour.
2. Maximum reboiler duty.
3. Complete loss of condensation (loss of cooling water).

Determining the areas for valves and diaphragms For exothermic reactors

Caution!



- Two-phase venting has proved difficult to model reliably
  - DIERS, (Design Inst. for Emergency Relief Systems) formed by companies and AIChE. Goals are to determine sizing methods, verify experimentally, and prepare program.
- Experience has shown that
  - Two-phase flow occurs often. Two-phase flow during runaway reactions requires a much larger area than predicted by one-phase methods

Safety relief systems, What have we learned?

- Entirely self-contained, no external power required
- The action is automatic - does not require a person
- Two major devices are relief valve and rupture disk
- We must divert material to an adequate handling system
- Usually, goal is to achieve reasonable pressure

  - Prevent high (over-) pressure
  - Prevent low (under-) pressure

- The capacity should be for the “worst case” scenario

References on relief systems

Andrew, W. and H. Williams, Applied Instrumentation in the Process Industries, Volume I: A Survey, Gulf Publishing, Houston, 1979

Andrew, W. and H. Williams, Applied Instrumentation in the Process Industries, Volume II: Practical Guidelines, Gulf Publishing, Houston, 1980

Crowl, D. And J. Louvar, , Chemical Process Safety: Fundamentals with Applications, Prentice Hall, Englewood Cliffs, 1990

Driskell, L., Control Valve Selection and Sizing, Instrument Society of America, 1983

Fauske, H. And J. Leung, New Experimental Technique for Characterizing Runaway Chemical Reactions, CEP, p. 39-46, August 1985

Fisher, H., DIERS Research Program on Emergency Relief Systems, CEP, p. 33-36, August 1985

Issaca, M., Pressure-Relief Systems, Chem Engr., p.113-124, February 22, 1971

Jenett, E., Design Considerations for Pressure-Relieving Systems, Chem. Engr., Part I, p. 125-130, July 1963; Part II, p. 151-158, August 19, 1963

Kern, R., Pressure-Relief Valves for Process Plants, Chem.. Engr., p. 187-194, February 28, 1977

King, R., Safety in The Process Industries, Butterworth Hieneman, Oxford, 1990

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

References on the Safety Hierarchy

AIChE, Guidelines for Engineering Design for Process Safety, American Institute of Chemical Engineers, New York, 1993, Chapter 9.

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

AIChE, International Symposium and Workshop on Safe Chemical Process Automation, American Institute of Chemical Engineers, New York, 1994

Englund, S. and D. Grinwis, Provide the Right Redundancy for Control Systems, CEP, Oct. 1992, 36-44.

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

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

International Symposium and Workshop on Safe Chemical Process Automation, Sept 27-29, 1994, American Institute of Chemical Engineers, New York, 1994

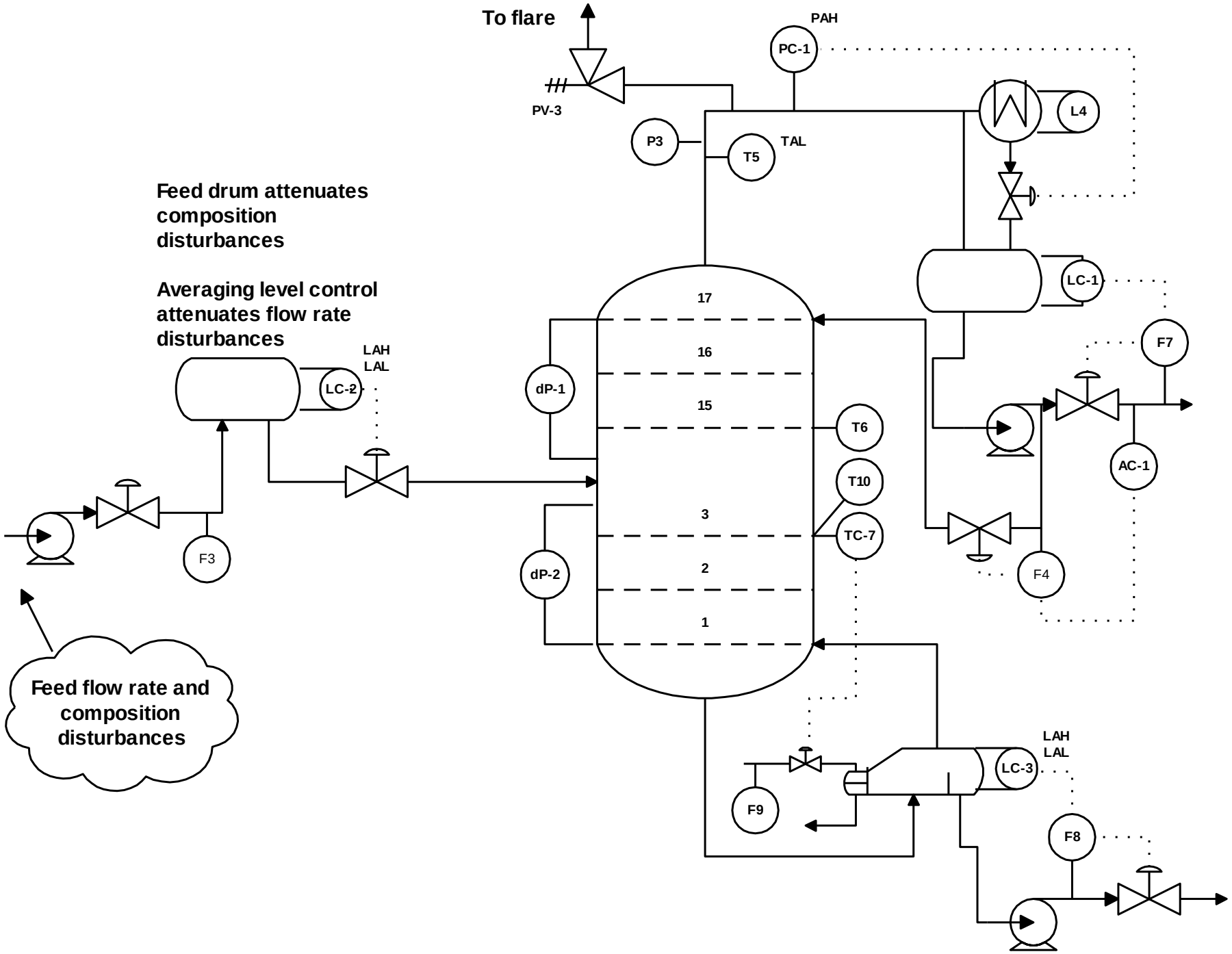
Marlin, T., Process Control: Designing Processes and Control Systems for Dynamic Performance 2nd Ed., McGraw-Hill, New York, 2000, Section 24.8 - p. 794-799.

Summers, A., Techniques for Assigning a Target Safety Integrity Level, ISA Transactions, 37, 1998, 95-104.

Relief system practice problems

1. Review the distillation process on the next page.
2. Locate at least one example of each of the four layers of safety automation.
3. Evaluate each relief system for proper location and choice of relief device.
4. Find a location that should have a relief system but does not.

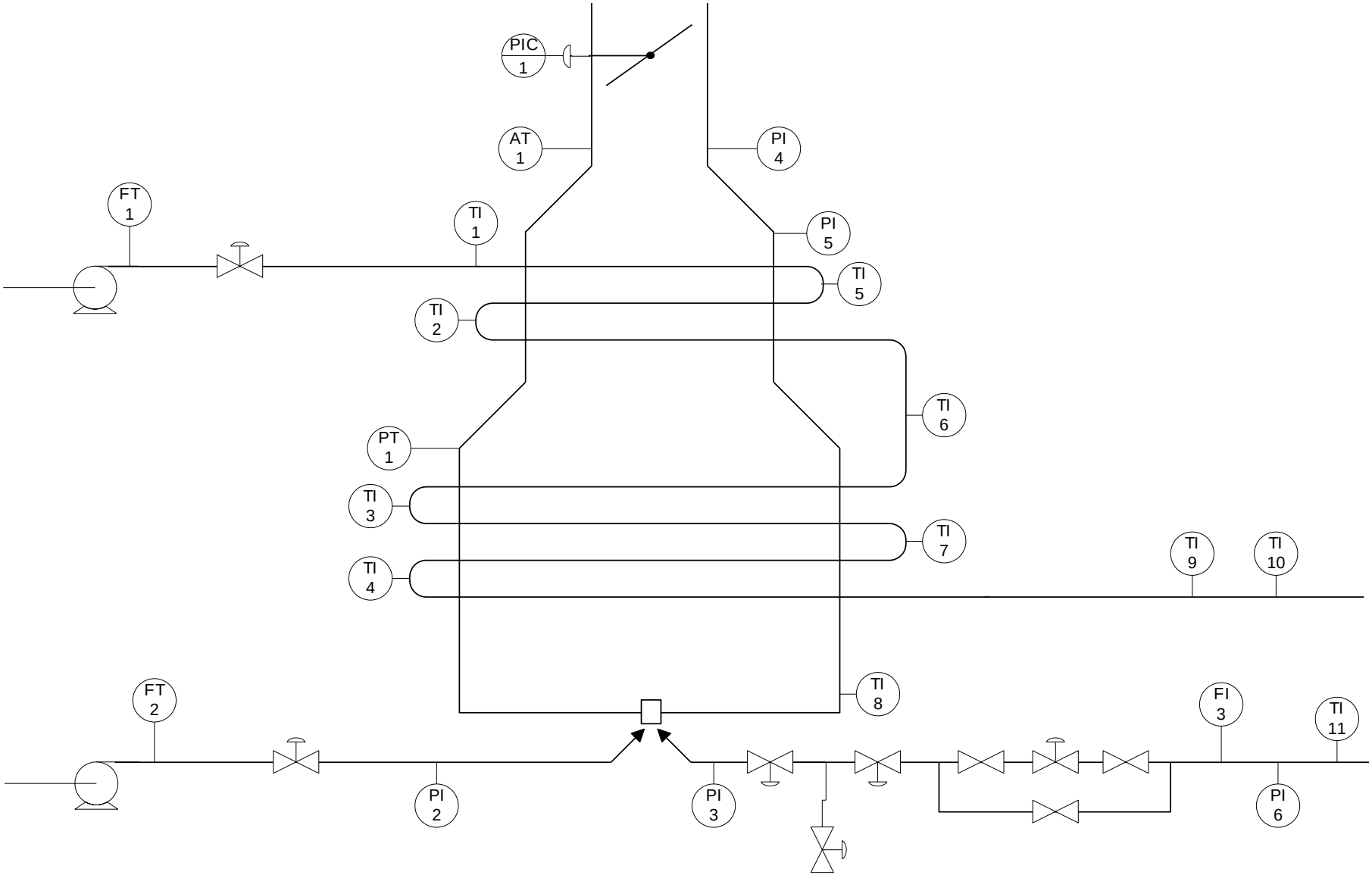
Remember, the figure could have errors for teaching/learning purposes.


To flare
PAH
PC-1
PV-3
L4
P3
T5
TAL
Feed drum attenuates composition disturbances
Averaging level control attenuates flow rate disturbances
LC-1
17
16
15
3
2
1
LAH
LAL
LC-2
dP-1
T6
T10
TC-7
F7
AC-1
F3
dP-2
F4
Feed flow rate and composition disturbances
LAH
LAL
LC-3
F9
F8

Safety through automation practice problem

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.


PIC 1
AT 1
PI 4
FT 1
TI 1
PI 5
TI 5
TI 2
TI 6
PT 1
TI 3
TI 7
TI 4
TI 9
TI 10
TI 8
FT 2
FI 3
TI 11
PI 2
PI 3
PI 6