Boas práticas para segurança de plantas, do ponto de vista do controle e automação !

Table 10.1 Failure Rates for Selected Components (Mannan and Lees, 2005)

Instrument	Failure Frequency (faults per year)
Control valve	0.60
Valve positioner	0.44
Current/pressure transducer	0.49
Pressure measurement	1.41
Flow measurement (fluids)	
Orifice plate & D/P transmitter	1.73
Magnetic flowmeter	2.18
Temperature measurement	
Thermocouple	0.52
Mercury-in-steel thermometer	0.027
Controller (electronic)	0.29
Flow switch	1.12
Pressure switch	0.34
Alarm indicator lamp	0.044
Gas-liquid chromatograph	30.6

Intertravamento

O objetivo do sistema de intertravamento é o de prover a segurança para o pessoal, os equipamentos e o processo.

Para realizar isso, ele causa automaticamente e/ou manualmente um conjunto previsível de operações, quando os limites do processo forem excedidos, os equipamentos mecânicos e elétricos falharem, a energia de alimentação faltar cair ou os instrumentos falharem ou individualmente ou em combinação.

O intertravamento é usado para superpor ao controle do processo e por isso eles devem ter fontes de alimentação e medições isoladas e independentes de modo que seja improvável a falha simultânea dos dois sistemas.

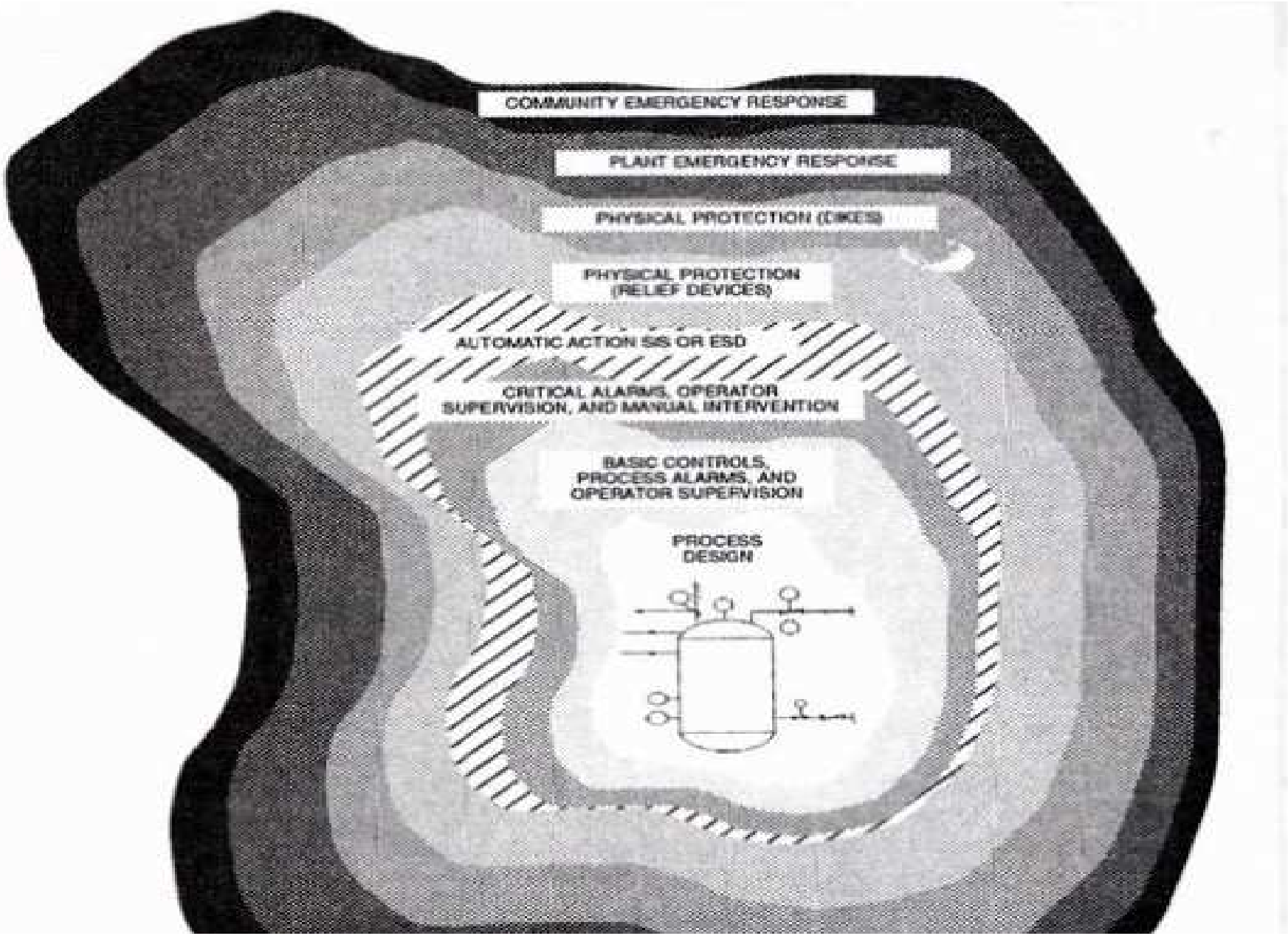
- *Basic process control system* (BPCS) is augmented with two levels of alarms and operator supervision or intervention.
- An alarm indicates that a measurement has exceeded its specified limits and may require operator action.
- *Safety interlock system* (SIS) is also referred to as a *safety instrumented system* or as an *emergency shutdown* (ESD) system.
- The SIS automatically takes corrective action when the process and BPCS layers are unable to handle an emergency, e.g., the SIS could automatically turn off the reactant pumps after a high temperature alarm occurs for a chemical reactor.
- Rupture discs and relief valves provide physical protection by venting a gas or vapor if over-pressurization occurs (also flares for combustibles).

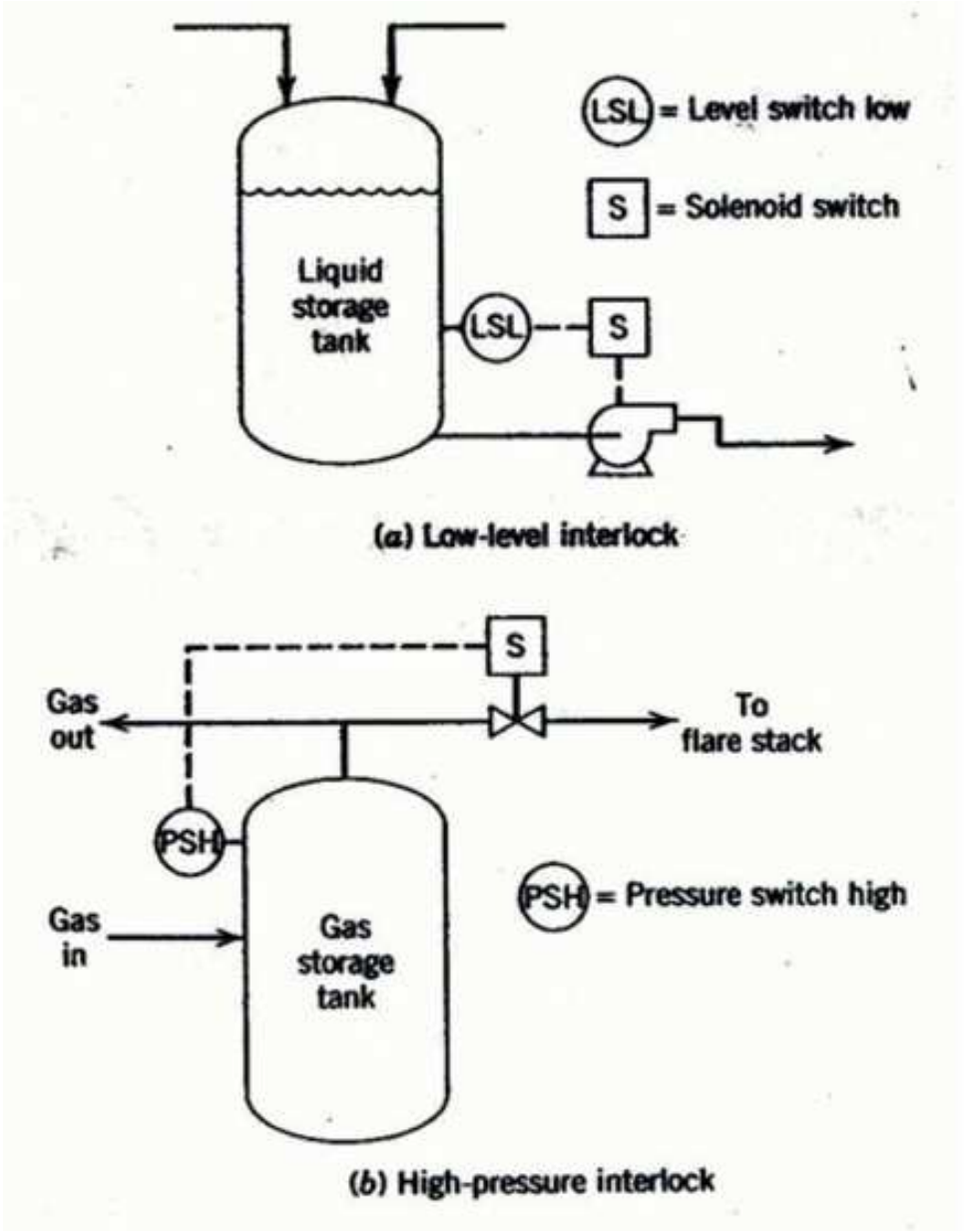
Safety Interlock (Instrumented) System (SIS)

- The SIS in Figure 10.1 serves as an emergency back-up system for the BPCS.
- The SIS automatically starts when a critical process variable exceeds specified alarm limits that define the allowable operating region (starting or stopping a pump or shutting down a process unit).
- Only used as a last resort to prevent injury to people or equipment.
- SIS must function *independently* of the BPCS; (e.g., due to a malfunction or power failure in BPCS). *Thus, the SIS should be physically separated from the BPCS and have its own sensors and actuators.*

Multiple Protection Layers

- In modern plants, process safety relies on the principle of *multiple protection layers*; see Figure 10.1.
- Each layer of protection consists of a grouping of equipment and/or human actions, shown in the order of activation.


COMMUNITY EMERGENCY RESPONSE
PLANT EMERGENCY RESPONSE
PHYSICAL PROTECTION (DIKES)
PHYSICAL PROTECTION
(RELIEF DEVICES)
AUTOMATIC ACTION SIS OR ESD
CRITICAL ALARMS, OPERATOR
SUPERVISION, AND MANUAL INTERVENTION
BASIC CONTROLS,
PROCESS ALARMS, AND
OPERATOR SUPERVISION
PROCESS
DESIGN



Two interlock configurations.

Types of Alarms

Type 1 Alarm: Equipment status alarm. Pump is on or off, or motor is running or stopped.

Type 2 Alarm: Abnormal measurement alarm. Measurement is outside of specified limits.

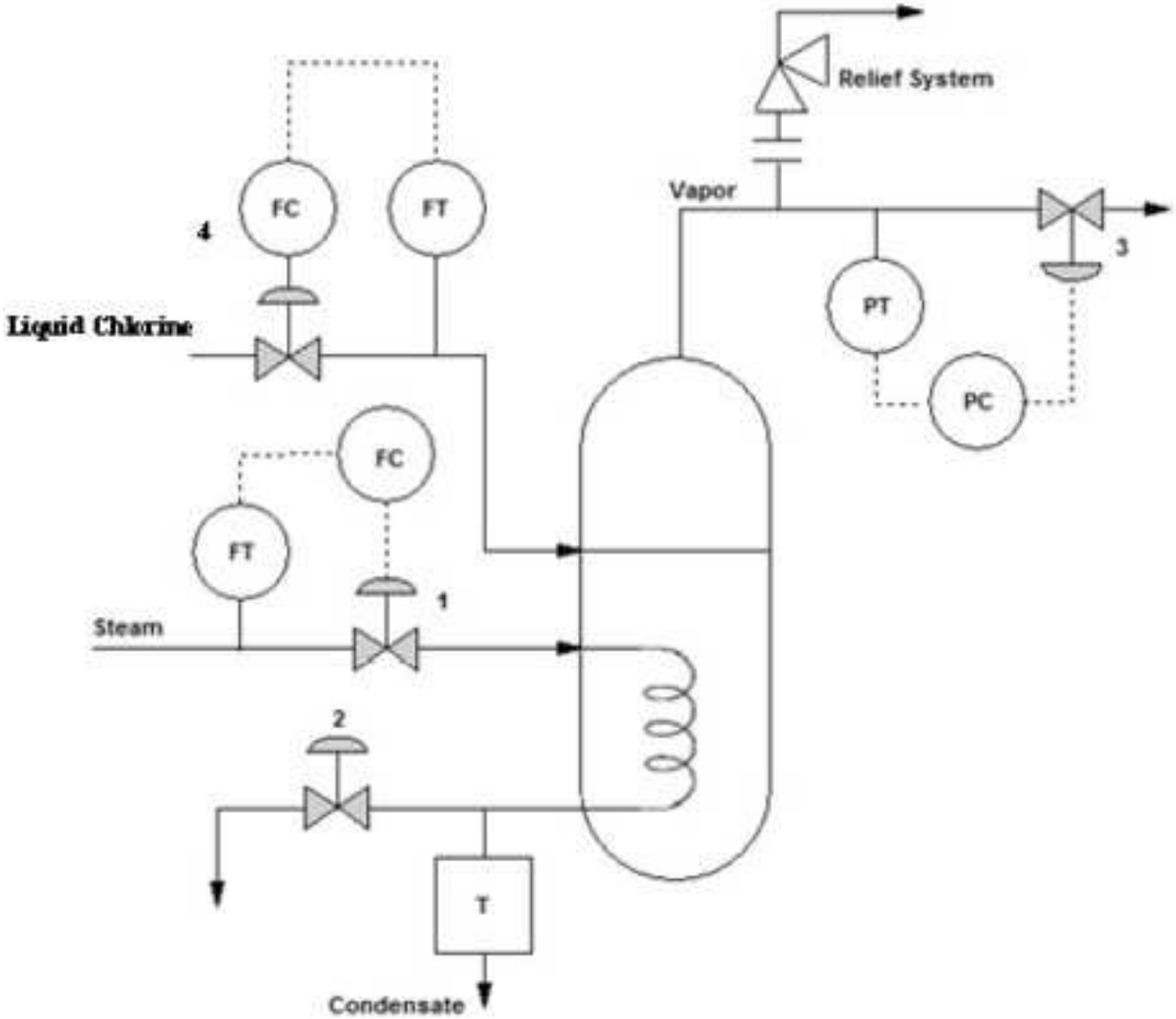
Type 3 Alarm: An alarm switch without its own sensor. When it is not necessary to know the actual value of the process variable, only whether it is above (or below) a specified limit.

Type 4 Alarm: An alarm switch with its own sensor. This serves as a backup in case the regular sensor fails.

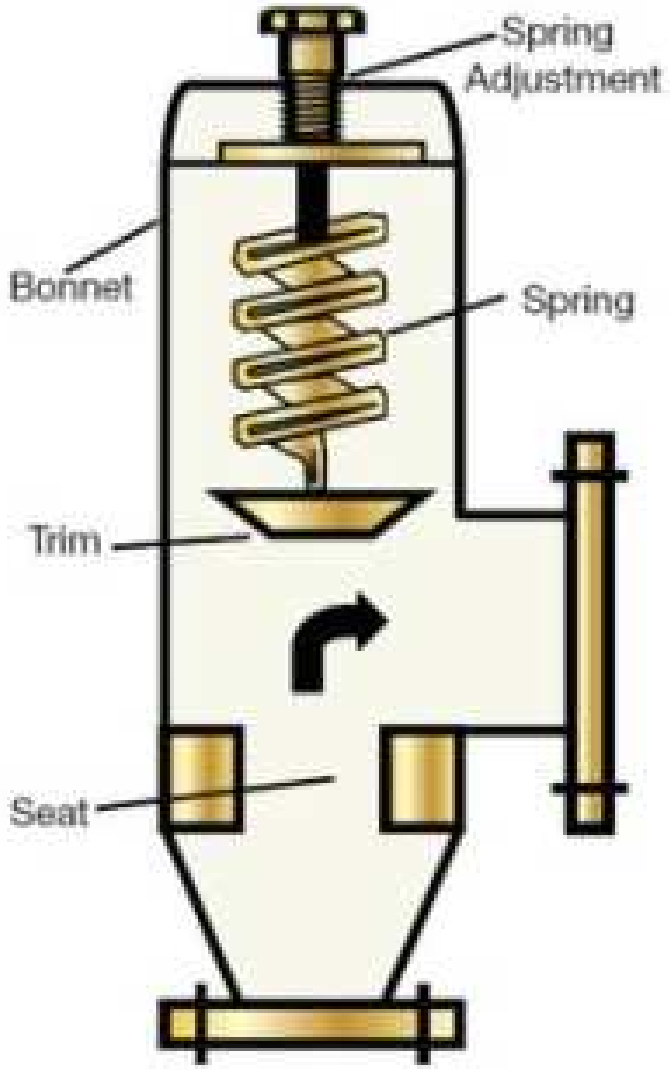
Type 5 Alarm: Automatic Shutdown or Startup System.

Typical Complaints from Operators

- Inadequate precision of temporal information (e.g., lack of true alarm order).
- Excessive nuisance alarms
- Inadequate anticipation of process disturbances.
- lack of real-time, root-cause analysis (symptom-based alarming).
- Lack of distinctions between instrument failures and true process deviations.
- Lack of adequate tools to measure, track, and access past records of abnormal situations.



Chlorine Vaporizer



pressure relief valve

("What Pressure Relief Really Means." *Chem. Engr. Progress*, Sept. 2010)

Good Control Practices for Plant Safety

Design

1. Avoid using the same sensor for control, alarm, and SIS.
2. Use independent equipment for each safety layer, including computing equipment.
3. Select and group alarms carefully; too many can be almost as detrimental as too few.
4. Use redundant equipment for critical functions.

Operation

5. Never disable the SIS system.
6. Never mechanically block a control valve so that it cannot close or open.
7. Never manually open the bypass valve around control and shutdown valves.
8. Never disable the alarm acknowledgment button so that new alarms will not require action by an operator.
9. Test safety systems on a regular basis; they are normally on a standby basis.

Source: Modified from Marlin, 2000.

Fontes:

Process Dynamics and Control - Dale E. Seborg, Thomas F. Edgar, Duncan A. Mellichamp

https://pt.slideshare.net/enautena/57768-1289-28022012-13360903nomenclaturasimbologiar1
Por Carlos Alvarez

Aiche: https://www.aiche.org/resources/publications/cep/2010/september/what-pressure-relief-really-means