Chapter 22
Safety

Abstract The aim of this chapter is to outline the main factors involved in general safety issues related to asset management. Safety critical systems are also considered and techniques applicable to high-risk plant are introduced. *Outcomes* After reading this chapter you will be aware of safety issues in two main areas. First there are general safety concepts which apply to all physical assets. Second, there are concepts such as safety integrity levels which apply to high-risk plant. You will also be aware of the need for approved engineering standards to be applied by competent personnel when developing repair specifications.

22.1 Safety Requirements and Competence[1]

Safety of users, operators, and maintainers is a general requirement for asset-based systems.

The management of safety requires the existence of an organizational capability that is competent to determine and apply the procedures necessary to meet the related safety standards. Personnel must be aware of safety regulations that are applicable to the relevant assets and their uses. These regulations will provide guidelines for the conduct of operations and maintenance.

Personnel engaged in the operation or maintenance of systems must adhere to safety regulations and practices that are applicable. Competency is to be assured by a combination of a qualifications framework, competency standards, and competency assessment procedures.

Training programs are needed to deliver and support safety knowledge and practices. Staff members require documented records which identify the training and competencies achieved. Regular reviews or audits must be carried out of safety competencies required and achieved by staff members. This provides the opportunity to correct skill gaps if any.

[1] ISO 55002 Clause 4.4 Asset management systems: "A factor of successful asset management is the ability to integrate with …other functions e.g.….safety…".

N.A.J. Hastings, *Physical Asset Management*,
DOI 10.1007/978-3-319-14777-2_22

Contractor competency in regard to safety is reviewed as part of the contract tendering process with ongoing contractor performance reviews and workplace assessments.

22.1.1 Safety Practices

Identify, publicize, and enforce good safety practices in relation to the following:

- Standard operating conditions
- Actions when deviations occur
- Incident reporting procedures
- Accident reporting procedures
- Isolation procedures
- Emergency procedures
- Electrical safety
- Radio use
- Fire protection
- Driving rules
- Manual handling rules
- Use of protective clothing: Helmets, Footwear, Goggles, Gloves, Ear Muffs, and Respirators
- No smoking areas
- Behavior: No horseplay, alcohol, drugs, walk do not run, and hold the hand rail
- Good housekeeping
- Color coding of pipes and valves
- Paint the name of the fluid inside on the pipe or valve
- Label equipment which is supplied from a switch or valve
- Identify water quality as potable or otherwise
- Remove hazardous material
- Check that concentrations of toxic substances are low enough for safety
- Remove items that may collect foreign objects, toxic material or corrosion, e.g., dead ends of old pipes
- Keep unnecessary people away
- Have a works modification approval procedure and form
- Use portable gas detector alarms
- Avoid having welding or grinding sparks in potentially dangerous places.

All maintenance work is to be carried out under appropriate isolation with all the hazards identified and risks assessed. Nonroutine maintenance tasks are to be subject to appropriate job safety hazard analysis and risk management procedures.

Specify and apply testing and acceptance criteria for when repair is complete.

22.1.2 Training and Information

Provide training in:

- Safety procedures
- Protective clothing
- Personal equipment
- Permits
- Follow-up actions.

Consider physical factors such as:

- Weight to be lifted,
- Accessibility,
- Reach,
- Visibility, and
- Hazards.

Make instructions available in simple forms:

- check lists,
- photographs,
- videos,
- graphics.

Carry out test runs of procedures with novices.
Check for possible missing steps, ambiguity.

22.1.3 Permits

A system of permits is required covering work in hazardous circumstances, such as:

- Confined space
- High level
- Ground opening
- Hot work
- Permit to work (from operations).

The person who signs the permit should always check first to assess the potential hazards involved and the current conditions. For confined spaces, there should be a standby person. Possible sources of danger include low level of oxygen; toxic gas; and flammable gas.

22.1.4 Tags

Tags are used to as a sign that equipment is out of service or under repair. Tags indicate that equipment is not to be switched on except by, or on the authority of, the person who placed the tag.

- *Out of service tag* Placed on a switch indicating plant must not be switched on because it needs repair. This is to prevent damage to plant.
- *Personal danger tag* Placed on a switch indicating that a (named) person is working on the machine. This is to prevent personal injury.

22.1.5 Danger Indications

Operators and maintainers should have a general awareness of possible indicators of danger and must be aware of what action to take in response to:

- Alarms
- Instruments indicating out of specification
- Leaks
- Flames
- Unexpected hot spots or cold spots
- Ice where no ice should be
- Vapor
- Loose equipment.

22.2 Safety Critical Equipment (SCE) and Systems (SCS)

Safety critical equipment or systems are items, the failure of which can endanger human life or cause significant damage. These systems are normally subject to statutory design and maintenance requirements. The engineering management of such systems is addressed by the topic of Systems Engineering[2] and by specific topics relating to high-risk industries.[3]

Safety critical systems require the application of techniques designed to assess and assure the safe operation of high-risk plant. These systems occur in plant operating at high or low temperatures and pressures, particularly where these contain flammable, toxic, or hazardous materials, such as are found in the oil and gas, chemical, and mineral processing industries. Inspection techniques apply to the

[2] ISO 15288 Systems Engineering—Systems Life Cycle Processes.

[3] IEC 61511-1 Functional safety, Safety Instrumented Systems.

pipes and pressure vessels, pumps, valves, compressors, hoses, and protective devices. The same principles apply to other safety-related structures such as lifting and fairground equipment. The design of systems for safety involves the use of items such as safety valves, redundant systems, back-up systems, and instrumentation to warn of or close down dangerous situations. The use of protective clothing and equipment and of safety procedures are also important in these applications.

The integrity of safety critical systems involves some features over and above those normally found for more general systems, although there is a considerable overlap. Some specific points are covered in this section, however, this is a very extensive subject and the intention is only to indicate the main concepts.

22.2.1 Safety Critical Examples

The following are some examples of safety critical equipment or systems:

- boilers, pressure vessels, and piping
- anything involving hazardous or toxic substances
- cranes, hoists, and elevating work platforms
- amusement devices
- lifts and escalators
- air conditioning units and cooling towers
- gas cylinders
- aviation systems
- railway systems
- nuclear industries
- storage tanks
- wells and wellhead equipment
- fire detection systems
- fire extinguishing systems
- instrumentation associated with safety.

22.2.2 Risk-Based Inspection

High-risk applications have substantial associated documentary and regulatory systems. Those for the oil and gas industry are developed by the American Petroleum Institute.[4] The term Risk-Based Inspection is used in describing the techniques which have been developed for addressing safety issues in these industries.

[4] API 580 and API 581 Risk Based Inspection.

A key document is API 581 which describes Risk-Based Inspection. The API standards provide methods for calculating operational limits for pressure vessels and pipes depending on the conditions, typically temperature, pressure, and fluid type, and the type of metal used. The technical factors considered include:

- Fatigue
- Overheating
- Thinning of pipes and vessels
- External damage
- Stress corrosion cracking
- Creep
- High-temperature hydrogen attack
- Brittle fracture
- Equipment linings failure.

22.2.3 Example—Distillation System

Figure 22.1 shows a piping and instrumentation diagram (P & ID) for a distillation system. This system illustrates many of the features of safety critical systems in that it involves liquids and gasses at high temperatures and pressures with an extensive set of instruments and control systems. It is not intended here to consider the working of this system in detail, but to use it as an example of a common type

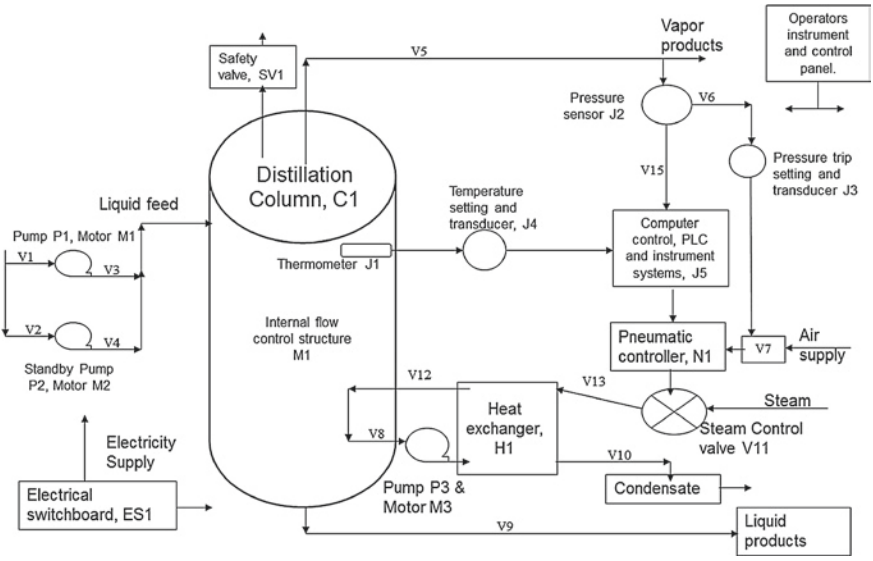

Fig. 22.1 Distillation system

of system that includes pressure vessels and piping, pumps, valves, instrumentation, sensors for pressure, temperature, level and flow and related controls.

22.2.4 Asset Integrity Management Plan (AIMP)

Systems such as the distillation system shown in Fig. 22.1 require an asset integrity management plan. An Asset Integrity Management Plan (AIMP) is a management plan specifically aimed at ensuring the integrity of safety critical equipment. It will include the following elements:

- Identification of Safety Critical Equipment (SCE) in the equipment register, to include tag number, nameplate data.
- Identification of Safety Instrumented Systems (SIS) and Safety Integrity Functions (SIF), which are systems or functions required to ensure safe operations and safe response to any departure from normal operating conditions.
- Analysis of Safety Critical Equipment (SCE), SIS, and SIF to determine the requirements for inspection and maintenance by activity and frequency.
- Development and application of integrity management and safety and operating plans.
- Development of detailed procedures for inspection and maintenance work including relevant test, performance or monitoring standards.
- Documentation of all procedures in the Asset Management Information System
- Management of these procedures through the Asset Management Information System.

22.2.5 Maintenance Specific to Safety Critical Equipment

Activities will typically include the following. The frequencies may be based on statutory requirements, reliability statistics, vendor recommendations, and best practice.

- Pressure Safety Valve (PSV) testing
- Functional tests (Emergency Shutdown (ESD) system, fire and gas detectors, etc.)
- Critical Function Testing of Safety Instrumented Systems (SIS)[5] and Safety Instrumented Functions (SIF)[6]
- Statutory vessel and piping inspections
- Instrument calibration

---

[5] IEC 61511.

[6] AS 1851 (Clause 1.11) and AS 4428 (Clause 4.2).

- Periodic running tests of standby equipment
- Mechanical and performance tests of any equipment (including fire pumps)
- Specify and apply testing and acceptance criteria for when repair is complete
- Reference vendor manuals that describe the maintenance and testing requirements for the maintenance procedures
- Maintenance activities must preserve the integrity of the safety systems.

22.2.6 Internal Corrosion Management

Internal corrosion presents significant risk to pressure equipment and pipelines particularly when corrosive substances are present. An internal corrosion control plan is developed for each facility to establish control and mitigation methods for managing corrosion, and also to monitor and assess the effectiveness of the corrosion management systems that have been implemented.

22.2.7 Protective Devices

Safety Critical Equipment often has protective devices, the functions of which need to be considered, such as:

- Fences
- Guards
- Fuses
- Circuit breakers
- Limit switches
- Safety valves
- Emergency stop buttons
- Overload cut outs
- Standby systems
- Smoke detectors
- Alarms
- Bursting discs
- Filters and filter by-passes
- Fire detection systems
- Fire water systems
- Gas alarms
- Governors
- Nonreturn valves
- Space alarms
- Sprinkler systems
- Tank vents

- Trips mechanical, electrical, other instrument
- Closed circuit television monitoring.

These have functions such as:

- Warn of danger
- Switch off or close down operation
- Relieve pressure
- Guard against foreign objects, e.g., hand in guillotine
- Provide standby service, e.g., emergency lighting.

22.2.8 Record Keeping[7]

Records of maintenance and function tests for safety critical equipment typically include the following information:

- Date of maintenance or function test
- Name of person who performed the maintenance or function test
- Serial number or other unique identifier of equipment (loop number, tag number etc.)
- Results of maintenance or function test
- Reference to work requests or work orders raised.

22.3 Layer of Protection Analysis (LOPA)[8,9,10]

A layer of protection is something that reduces risk by a significant factor. In Layer of Protection Analysis, layers are added until a desired level of safety is reached. As an example consider a pressure vessel such as the distillation column in Fig. 22.1. This could burst causing damage. To protect against this we have layers of protection as shown in Fig. 22.2.

The initial layer of protection (numbered 1 in Fig. 22.2) is provided by a gauge and a warning light on a control panel. An operator should respond to this warning by taking action to make the situation safe. If the operator does not act, an audible warning signal (numbered 2) sounds to attract the attention of the operator. This is the second layer of protection. If the operator still does not act, a safety valve opens (numbered 3), and if this does not work or does not reduce the pressure sufficiently, an automatic

[7] AS 1851 (Clause 1.15) and AS 4428 (Clause 3.2, 4.5).

[8] IEC 61508 series and IEC 61511 describe LOPA and SIL.

[9] CCPS/AIChE, Guidelines for Safe Automation of Chemical Processes, 1993, pp. 7–16.

[10] Angela E. Summers, Introduction to layer of protection analysis, Journal of Hazardous Materials.

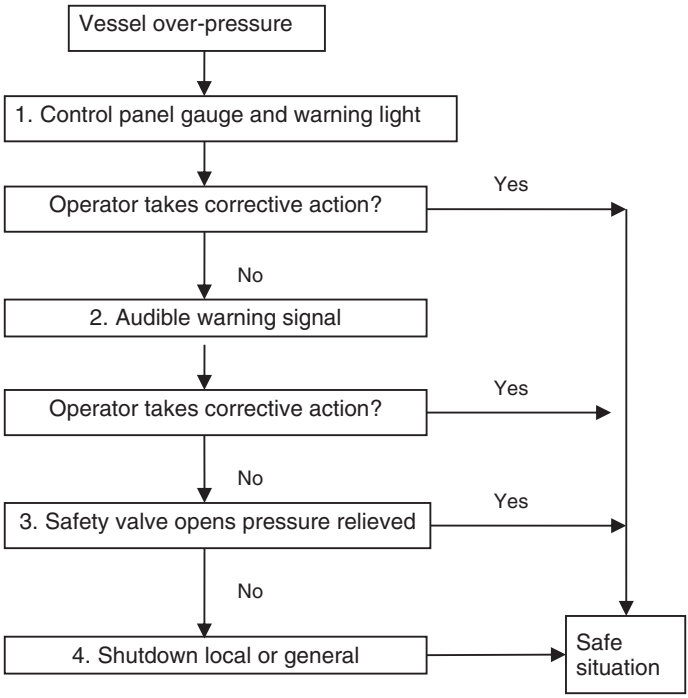

Fig. 22.2 Layers of protection

local or general shutdown (numbered 4) occurs. Thus in total there are four layers of protection protecting against potential damage caused by vessel overpressure.

22.4 Safety Integrity Level (SIL)

The Safety Integrity Level of a system is a measure of its relative safety as achieved by the application of Layers of Protection. Analytical techniques such as fault tree and event tree analysis may be applied in assessing a safety integrity level. Layers of protection may be added until the required safety integrity level is reached.

22.4.1 Design for Safe Operation

The following are some examples of techniques which can be applied in design for safe operation.

- Procedures and action to be taken in response to specific readings of instruments or signals, e.g., pressure, temperature
- Setting control trips

- Selection of automatic control and operation overrides
- Establishment of safety limits on plant characteristics, e.g., thinning of pipes
- Inspection practices and follow-up action
- Maintenance tasks and intervals
- Design of operation interlocks
- Design and operation of protection systems
- Automatic shutdown or restriction of plant operation based on Safety Instrumented Systems or Safety Integrated Functions
- Formulation of recovery methods
- Root cause analysis of trips and faults.

22.4.2 Facility Siting and Layout

Ref: OSHA (USA) CFR 1919.119. API RP-752. Consider process hazards, including fire, explosion, and toxicity, in relation to:

- Site workers;
- Location of control room;
- Occupants of buildings;
- Nearby residents; and
- Access to emergency facilities.

22.4.3 Fitness for Service Assessment

Fitness for service criteria are to be established and applied to assets. These will specify inspection and performance standards relating to such issues as the following. Reference should be made to industry standards where appropriate. For example, for the oil and gas industry, see API 579.

- Thickness of pipes and pressure vessels;
- Cracks, e.g., in structures, cranes;
- Misalignment;
- Vibration;
- Levels of corrosion or wear;
- Insulation resistance in transformers and other electrical equipment.

22.5 Repairs Requiring Engineering

If a particular repair is required but is not included in the existing maintenance manual, then engineering will be required to design the repair. Examples are: the extent of weld repairs for corrosion, the extent of what has to be replaced after

unusual events, e.g., fire or impact damage; the need of cutting away structures for access during equipment upgrades, a repair specification is required to cover the safe restoration of the affected structures.

A *repair specification* is a repair procedure which is authorized by a competent authority for a specific maintenance activity. The competent authority can be an individual, a company, or a group of qualified engineers. The data associated with a repair generally consists of drawings and analysis that show compliance to regulations. The key task is to make certain that the repair specification does not violate any of the assumptions made in the design of the repaired engineering system.

22.6 Terminology Summary

Cause and Effect Matrix (C & E)
Emergency Shutdown System (ESD)
Fire and Gas (F & G)
Layer of Protection Analysis (LOPA)
Piping and Instrumentation Diagram (P & ID)
Process Flow Diagram (PFD)
Process Shutdown System (PSD)
Process Safety (PS)
Pressure Safety Valve (PSV)
Safety Critical Equipment (SCE)
Safety Critical System (SCS)
Safety Integrity Function (SIF)
Safety Integrity Level (SIL)
Safety Instrumented Systems (SIS)

22.7 Exercises

22.7.1 Self-Assessment Quiz

1. Identify three or more essentials for safety management.
2. Identify three or more situations where permits to work are typically required.
3. Why are safety tags used?
4. What is Safety Critical Equipment (SCE).
5. What organization is particularly involved in creating standards applicable to the oil and gas industries?
6. What types of safety issues are addressed by Risk-Based Inspection?
7. Identify five or more types of protective device used in high-risk plant.
8. Define the concepts of Layer of Protection and Layer of Protection Analysis.
9. Under what circumstances is engineering input required for approving repairs and what is an engineering approved repair specification?

22.7.2 Self-Assessment Quiz Solutions

1. *Identify three or more essentials for safety management.*
   - An organizational capability that is competent to determine and apply the procedures necessary to meet the related safety standards.
   - Awareness of safety regulations.
   - Competency in applying safety procedures.
   - Training programs.
   - Documented records which identify the training and competencies achieved.
   - Reviews or audits of safety competencies required and achieved by staff members.
   - Contractor competency.
2. *Identify three or more situations where permits to work are typically required.*
   - Confined space
   - High level
   - Ground opening
   - Hot work
   - Permit to work (from operations).
3. *Why are safety tags used*?
   Tags are used to as a sign that equipment is out of service or under repair. Tags indicate that equipment is not to be switched on except by, or on the authority of, the person who placed the tag.
4. *What is Safety Critical Equipment* (*SCE*)?
   Safety critical equipment or systems are items, the failure of which can endanger human life or cause significant damage.
5. *What organization is particularly involved in creating standards applicable to the oil and gas industries*?
   The American Petroleum Institute (API).
6. *What types of safety issues are addressed by Risk-Based Inspection*?
   High-risk applications in the oil and gas industry involving equipment such as pressure vessels and pipes and factors such as temperature, pressure and fluid type, and the type of metal used. Potential failure modes include:
   - Fatigue
   - Overheating
   - Thinning of pipes and vessels
   - External damage
   - Stress corrosion cracking
   - Creep
   - High temperature hydrogen attack
   - Brittle fracture
   - Equipment linings failure.

7. *Identify five or more types of protective device used in high-risk plant*.
   Any five or more items listed in Sect. 22.2.7.

8. *Define the concepts of Layer of Protection and Layer of Protection Analysis*.
   A layer of protection is something that reduces risk by a significant factor. In Layer of Protection Analysis, layers are added until a desired level of safety is reached.

9. *Under what circumstances is engineering input required for approving repairs and what is an engineering approved repair specification*?
   If a particular repair is required but is not included in the existing maintenance manual, then engineering will be required to design the repair. A *repair specification* is a repair procedure which is authorized by a competent authority for a specific maintenance activity.