ELSEVIER

A Systems Approach to Managing the Complexities of Process Industries

Fabienne Salimi and Frederic Salimi

IChemE ADVANCING CHEMICAL ENGINEERING WORLDWIDE

A Systems Approach to Managing the Complexities of Process Industries

Fabienne Salimi
Process Safety Expert, ADEPP Academy
Frederic Salimi
Process Safety Expert, ADEPP Academy

ELSEVIER

Elsevier
Radarweg 29, PO Box 211, 1000 AE Amsterdam, Netherlands
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, United Kingdom
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-804213-7

For Information on all Elsevier publications
visit our website at https://www.elsevier.com/books-and-journals

Publisher: Joe Hayton
Acquisition Editor: Kostas Marinakis
Editorial Project Manager: Jennifer Pierce
Production Project Manager: Sruthi Satheesh
Designer: Mark Rogers

Typeset by MPS Limited, Chennai, India

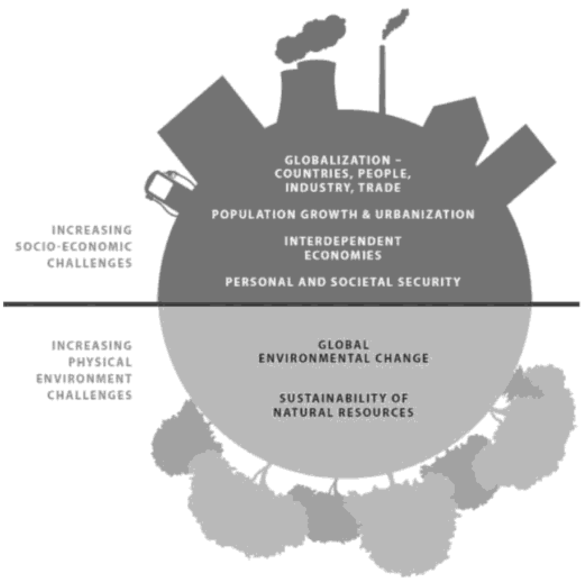
Contents

Acknowledgments

I was always amazed about the wonders that man-kind can do when they join their forces to turn a dream to a reality. When I was a child, I was thinking “What if” the brains of all people on the world are interconnected to make a huge brain? My friends and mentors smiled and did not take this question seriously.

Today, technology gives us the required tools to think more seriously about this question. The IIoT and augmented reality are already there and stimulate imagination of many of us.

As the health, safety, and environmental practitioners, we understand that the complex solutions engineered to meet fundamental human needs. They should be safe and not harm people and environment. But what does complexity mean in process industry and how can we manage it?



INCOSE Vision 2025 - Page 7.

Since 1994, the authors of this book have reflected on this question and developed a tool called ADEPP (Analysis & Dynamic Evaluation of Project Processes). We acknowledge the importance of technical and financial supports of the French innovation organizations in particular "Institute Français du Pétrole (IFP) in development of version 1 of ADEPP."

In 2014 the authors created a partnership with the following companies to develop the prototype of version 2 of ADEPP. We acknowledge their trust and importance in crystallization of the ideas that we express in this book:

- Hydraulic Analysis Ltd + Software Simulation Ltd (United Kingdom)
- VMG (Europe Branch in Spain)
- Antea (Italy)
- Human Focus (United Kingdom)
- EON Reality (France)

We also acknowledge the positive reception and constructive discussions with the following system engineering and complexity experts who inspired and encouraged us:

- Alan Hayman (System and Complexity Thinking Consultant)
- Frank Verschueren (Engineer Inspector for FOD WASO/Belgian fed government COMAH regulations)
- Matthew E. Weilert (Systems Thinking & Engineering Consultant)
- Gene Bellinger (Systems Thinking & Engineering visionary)
- Joss Colchester (director and developer of complexity academy, i.e.—an excellent source of high-quality system and complexity courses for the beginners)
- Mark Simpson (Product Manager at Siemens)

We acknowledge the usage of the valuable books and documents published by the following organizations for promotion of system engineering, system thinking, complexity thinking, quality and risk thinking, and IIoT:

- INCOSE (International Council on Systems Engineering)
- SEBoK (Systems Engineering Body of Knowledge)
- LNS Research
- Skybrary—Aviation Safety
- NASA (National Aeronautics and Space Administration)
- MIMSOA (Maintenance Information Management Open System Alliance)
- Health & Safety Executive (United Kingdom)
- Energy Institute
- IOGP (International Oil & Gas Producers)

Finally, we express our gratitude towards all those individuals and companies who directly or indirectly contributed in our education and professional understanding. May this book pay a humble tribute to their efforts.

Fabienne-Fariba Salimi & Frederic Salimi

Perspective

1.1 UNDERSTANDING A QUESTION IS HALF AN ANSWER!

"Management System" is a structured and documented set of interdependent practices, process, and procedures used by the managers and the workforce at every level in a company to plan, direct, and execute activities as shown in Fig. 1.1.

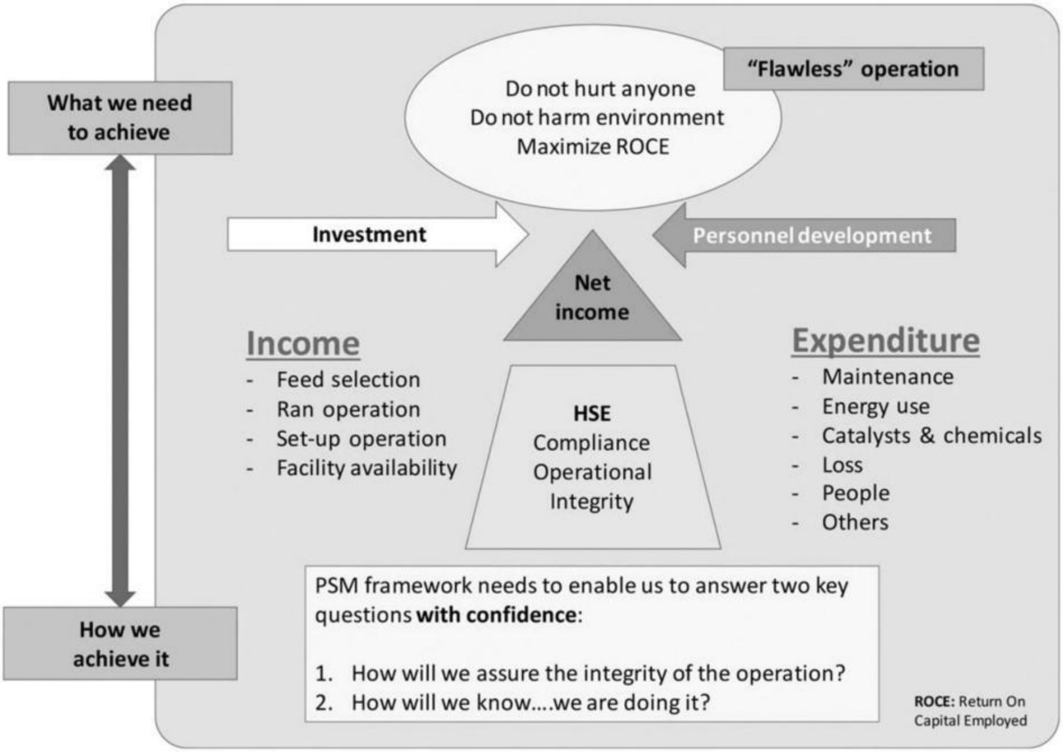


FIGURE 1.1

Process safety management in context. *Figure reproduced from webpage https://www.energyinst.org/technical/PSM published by the Energy Institute.*

A Systems Approach to Managing the Complexities of Process Industries.
DOI: http://dx.doi.org/10.1016/B978-0-12-804213-7.00001-3

Since, first days of quality management system in the late 60s, we have come a long way in improving quality, occupational health & safety, technical safety, and environmental management systems. For decades, these regulatory management systems were taken as the constraints to production and profitability of the businesses. This perception creates the conflicts and unsatisfactory results. In this regard the Energy Institute states:

> . . ., most well-run organisations can tell you how many incidents they had yesterday; however, our real challenge is to be able to answer the question "How likely am I to have an incident-free day tomorrow"?

Energy Institute continues,

> We have all seen the typical banner statements 'zero harm', 'flawless operation', 'target zero', 'incident free', 'nobody gets hurt'; but the two key questions for executives and managers at all levels are:
> 1. How will we assure the integrity of the operation?
> 2. How will we know we are doing it?
>
> All too often the first two words used to answer these questions are "*I think….*"; in reality, this means "*I dont' know*"! Recent events have shown that such answers are no longer acceptable and that, from top to bottom, organisations need to be able to answer these two key questions with absolute *confidence*.

Not only, the quality and health, safety, environment (HSE) practitioners but also the operational teams feel that the "management systems" do not work as they are advertised. But why is it so? And what can we do about it? The other side of the coin is that we often talk and analyses the failures, but we do not look at success very frequently. Why despite the flaws in the management systems, are the operations performed safely and reliably?

Socrates said that "*Understanding a question is half an answer*"!

To answer these questions, we need to understand the word "System" in "process safety management system" with the mind of a system engineer.

This book aims to raise the awareness of the HSEQ practitioners, managers and operational personnel in process manufacturing to the required system engineering skills. We will clarify how the relatively new ISO/IEC 15228 and ISA-95 (IEC/ISO 62264) standards are embedded in the operational excellence guidances and how they can smooth the journey of the process facilities toward the digital transformation. Then the most practical methods will be introduced to assess and manage the complexities of their day-to-day tasks, configuration management, and the strategic decision makings.

1.2 PROCESS SAFETY MANAGEMENT IN CONTEXT OF THE OPERATIONAL EXCELLENCE

Today the management systems philosophies are refined and go beyond inspection, focusing on the strategies that incorporate processes and people to the physical assets management to achieve the operational excellence.

Operational management system (OMS) is the consolidation of the company's knowledge and requirements into a single framework to manage assets and activities safely and responsibly. It includes the company's policies, standards, practices, procedures, and processes. This "corporate memory" is organized within the System's Elements and Expectations, which are designed to ensure the control measures are complete and robust.

The OMS framework applies to the all the management systems including:

- Production Operations Management,
- Reliability and Asset Integrity Management,
- Quality Operations Management,
- Inventory Operations Management, and
- Regulatory Compliance Management

Management system is a structured and documented set of interdependent practices, process, and procedures used by the managers and the workforce at every level in a company to plan, direct, and execute activities.

Operating covers, the design, implementation, and control of activities that convert resources into products and services to fulfill a company's business strategy. The word "operating" refers to the entire lifecycle of a company's activities and products. In this context, "operating" applies to every upstream or downstream company activity, from engineering to decommissioning, throughout the entire value chain and lifecycle of the business and its products.

In 2011, International Oil & Gas Producers issued the IOGP 510 which is a new Operating Management System Framework to help companies define and achieve performance goals and stakeholder benefits while managing the broad and significant range of risks inherent in the oil and gas industry. This guideline and its supplement IOGP 511 can be applied to the other process industry sectors such as hydrocarbon processing, chemical, pharmaceutical industries too. Fig. 1.2 illustrates the four fundamentals and ten elements of the OMS framework.

FIGURE 1.2
The OMS framework—four fundamentals underpin 10 elements. *From IOGP 510.*

IOGP 510 suggests a generic framework which offers an integrated approach and the flexibility to address some or all the wide range of risks, impacts or threats related to occupational health and safety; environmental and social responsibility; process safety, quality, and security. The degree of integration and the scope of an OMS will be determined by individual companies and will differ depending on their activities, organizational structure and management system maturity as shown in Fig. 1.3.

At the facility level the office should provide information about new customer orders, raw materials that have been ordered, specific customer demands for products, and so on. The shop floor will also have to send information to the office. For example, information about the status of orders, about the exact amounts of raw materials that were used in the production process and so on. Although they speak different languages, both levels should communicate with each other as shown in Fig. 1.4.

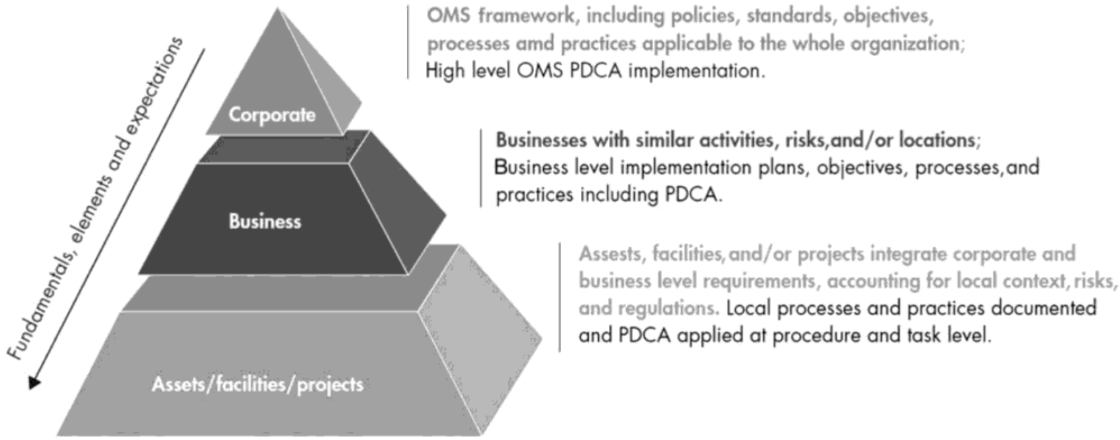


FIGURE 1.3
Hierarchy of the OMS implementation. *PDCA*, Plan, Do, Check, Act. *From IOGP 510.*

With the appearance of new technologies, it is getting easier to automate the exchange of information between the office and the shop floor. An automated interface between enterprise and control systems can lead to a lot of advantages. Relevant information becomes accessible at the right time and the right place to the right person. The company has access to the real-time information such as information about raw materials and end products, which enables optimum usage of storage capacity.

ISA-95 (IEC/ISO 62264) is an international standard which has been developed to address the problems encountered during the development of automated interfaces between enterprise and control systems. This standard applies to all industries, and in all sorts of processes, such as batch, continuous, repetitive, or discrete processes.

The Part 1 of the ISA-95 standard defines a functional hierarchy model. Each level provides specialized functions and has characteristic response times, as shown in Fig. 1.5.

Level 0 defines the actual physical processes.

Level 1 defines the activities involved in sensing and manipulating the physical processes. Level 1 typically operates on time frames of seconds and faster.

Level 2 defines the activities of monitoring and controlling the physical processes. Level 2 operates on time frames of hours, minutes, seconds, and subseconds.

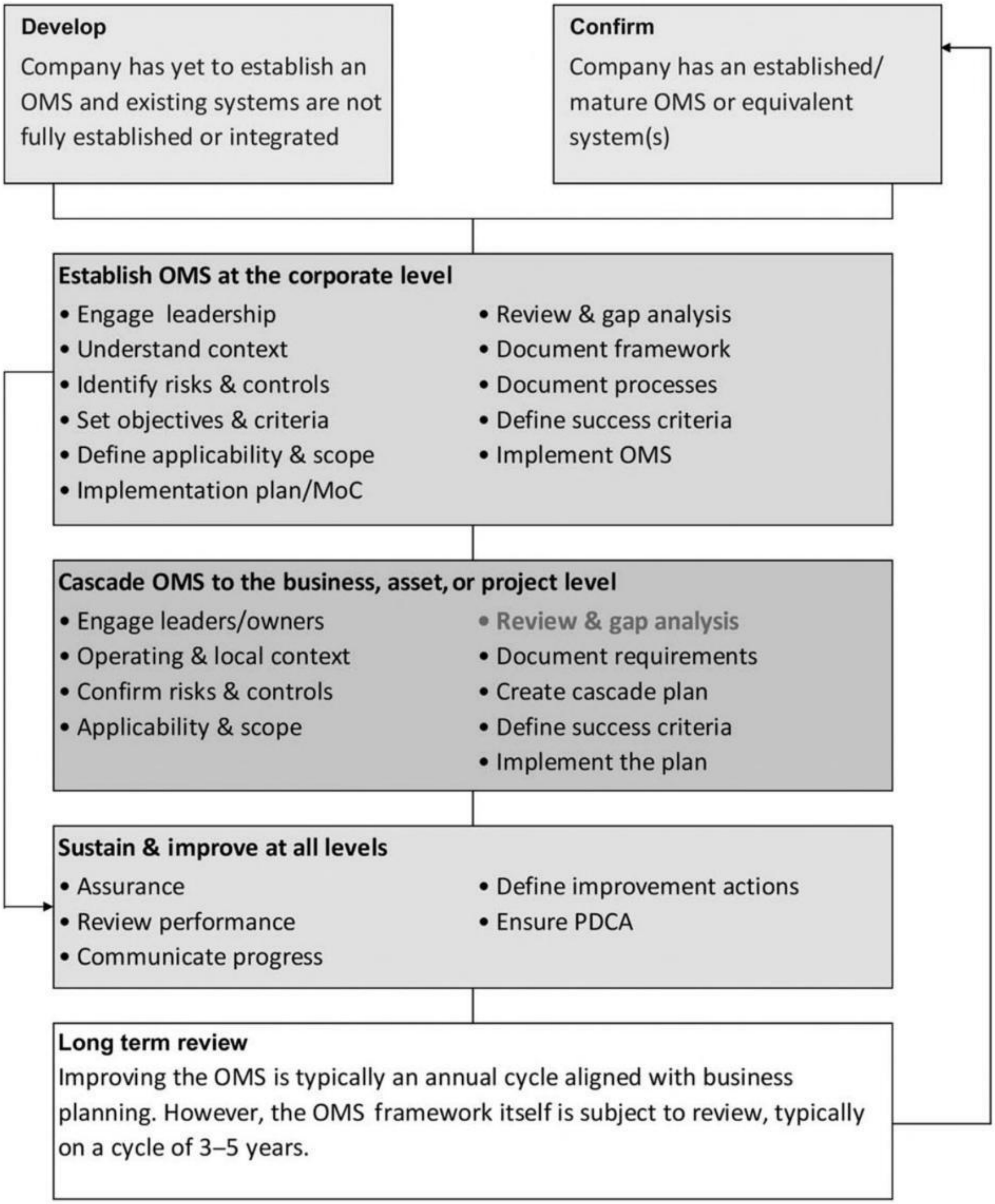


FIGURE 1.4

Establishing and sustaining an OMS flow chart. *From IOGP 510.*

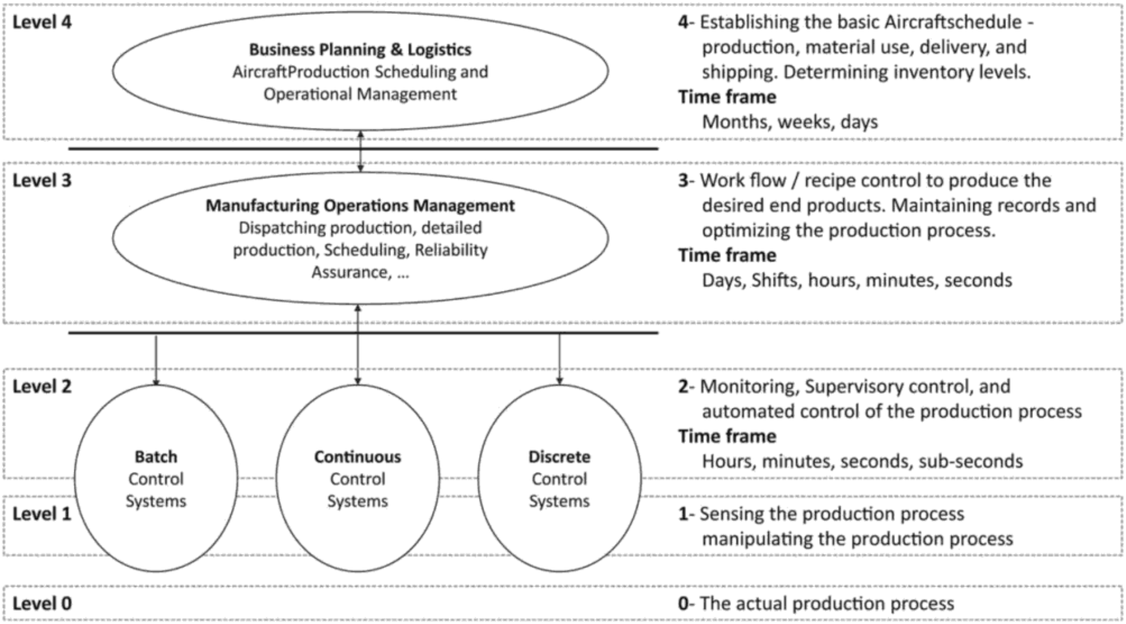


FIGURE 1.5
ISA-95 multilevel functional hierarchy of activities.

Level 3 defines the activities of workflow to produce the desired end products. It includes the activities of maintaining records and coordinating the processes. Level 3 typically operates on time frames of days, shifts, hours, minutes, and seconds.

Level 4 defines the business-related activities needed to manage a manufacturing organization. Manufacturing-related activities include establishing the basic plant schedule (such as material use, delivery, and shipping), determining inventory levels, and making sure that materials are delivered on time to the right place for production. Level 3 information is critical to Level 4 activities. Level 4 typically operates on time frames of months, weeks, and days.

The Level 5 can be added to capture Quality Governance and Planning and then added the value chain as quality management occurs across the lifecycle. Level 5 determines the strategy for Operational Excellence, Knowledge Retention, and Quality and Risk Management. This Level 0-5 framework is applicable to entire value chain as shown in Fig 1.6.

This framework is valuable because it provides a temporal perspective which includes both enterprise quality and functional quality. In a single

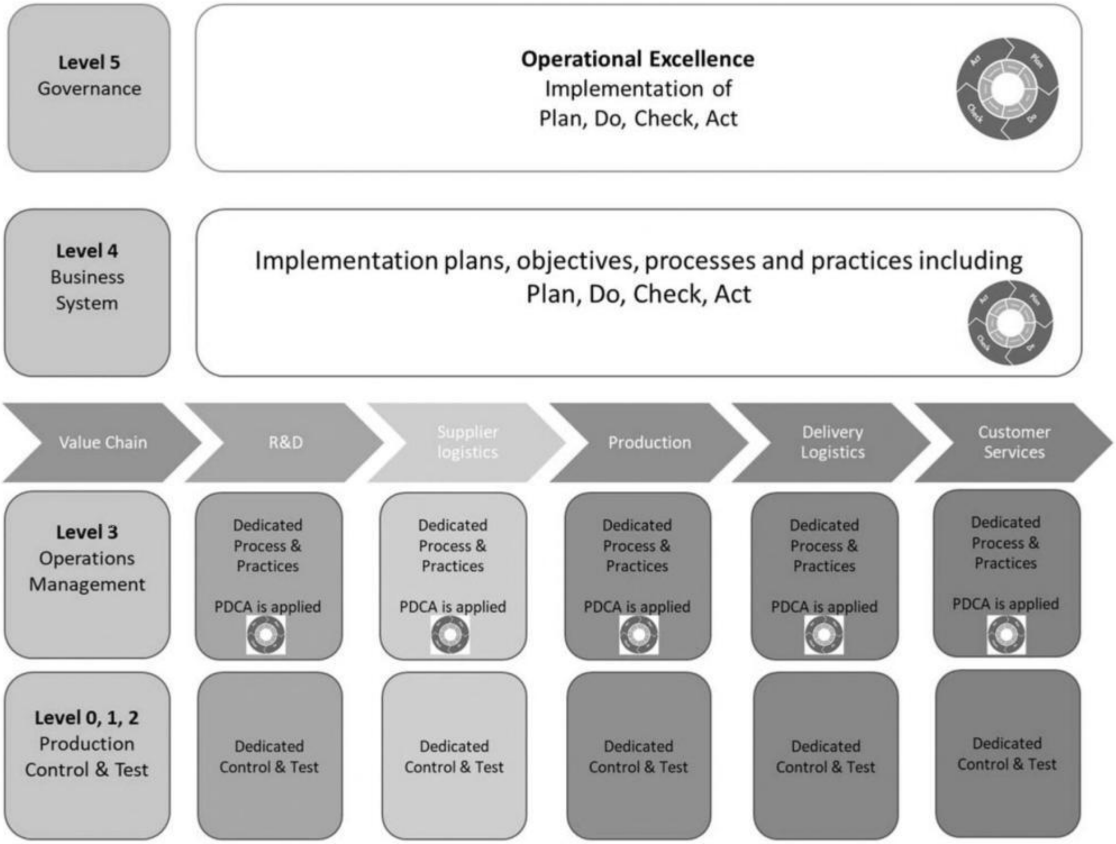


FIGURE 1.6
Adaptation of the ISA-95 framework to understand the total quality management system.

framework, it represents strategy and management down to operations and real-time asset performance. The connected devices and analytics capture the connection to Industrial Internet of Things (IIoT).

System engineering is the foundation of the operational excellence standards and guidelines. In the following sections, we highlight how the system engineering is applied in operating management systems of the process facilities.

1.3 REGULATORY COMPLIANCE MANAGEMENT SYSTEM

The broad footprint of management of regulatory compliance means that many areas of the enterprise can be significantly affected. Failures in

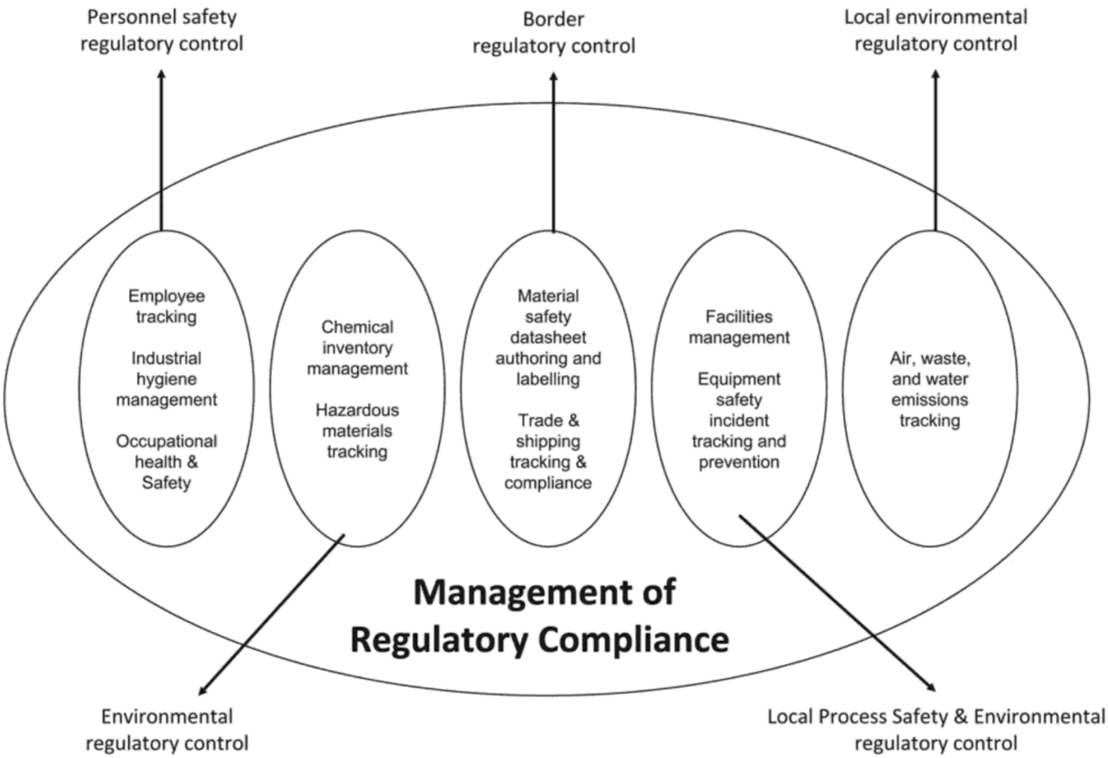


FIGURE 1.7
Functions in management of regulatory compliance.

regulatory compliance can stop production, force product recalls, and potentially cause safety problems. Where management of regulatory compliance activities involves the quality and safety of production, then the activities are in the scope of manufacturing operations. Fig. 1.7 breakdowns the most important regulatory compliances and the general activities associated with them.

Fig. 1.8 highlights the requirements of SEVESO III for process safety management (PSM) systems and Fig. 1.9 compares the structure of the quality management, environmental and occupational health & safety management systems.

The local or activity specific regulatory compliances should be considered case by case.

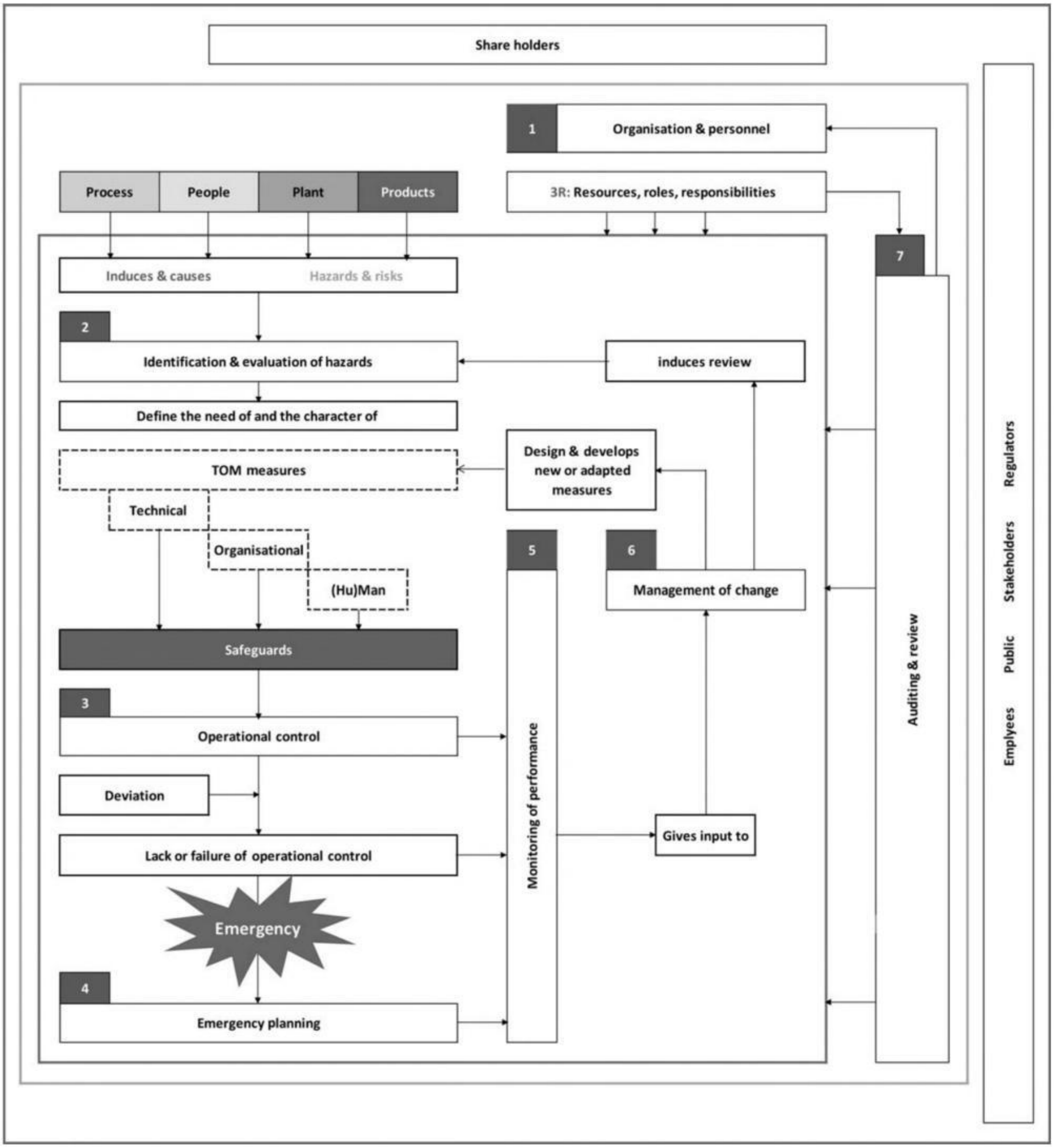


FIGURE 1.8
SEVESO III regulatory compliance framework.

ISO 9001		ISO 14001		OHSAS 18001	
0.1	Introduction		Introduction		Introduction
0.2	General				
0.3	Process approach				
0.4	Relationship with ISO 9004				
	Compatibility with other management systems				
1	Scope	1	Scope	1	Scope
1.1	General				
1.2	Application				
2	Normative reference	2	Normative references	2	Normative references
3	terms and definitions	3	Definitions	3	Definitions
4	Quality management system	4	Environmental management system requirements	4	OH&S management system requirements
4.1	General requirements	4.1	General requirements	4.1	General requirements
4.2	Documentation requirements (title only)				
4.2.1	General	4.4.4	Documentation	4.4.4	Documentation
4.2.2	Quality manual				
4.2.3	Control of documents	4.4.5	Control of documents	4.4.5	Control of documents
4.2.4	Control of records	4.5.4	Control of records	4.5.4	Control of records
5	Management responsibility (title only)	4.4.1	Structure and responsibility	4.4.1	Structure and responsibility
5.1	Management commitment	4.4.1	Structure and responsibility	4.4.1	Structure and responsibility
5.2	Customer focus	4.3.1	Environmental aspects	4.3.1	Hazard Identification, Risk Assessment & Determining controls.
		4.3.2	Legal and requirements	4.3.2	Legal and requirements
		4.6	Management Review	4.6	Management Review
5.3	Quality policy	4.2	Environmental policy	4.2	OH&S policy
5.4	Planning	4.3	Planning	4.3	Planning
5.4.1	Quality objectives	4.3.3	Objectives, targets and programme(s)	4.3.3	Objectives, targets and programme(s)
5.4.2	Quality management system planning	4.3.3	Objectives, targets and programme(s)	4.3.3	Objectives, targets and programme(s)
5.5	Responsibility authority and communication (title only)	-	-	-	-
5.5.1	Responsibility and authority	4.4.1	Resources, roles, responsibility and authority	4.4.1	Resources, roles, responsibility and authority
5.5.2	management representative	4.4.1	Resources, roles, responsibility and authority	4.4.1	Resources, roles, responsibility and authority
5.5.3	Internal communication	4.4.3	Communication	4.4.3	Communication, Participation and Consultation
5.6	Management review	4.6	Management review	4.6	Management review
5.6.1	General				
5.6.2	Review input				
5.6.3	Review output				

FIGURE 1.9

Comparison of the regulatory management systems.

When policies and procedures for management of regulatory compliance do not exist on a company-wide basis, then compliance control can be regarded as a manufacturing operations activity, for manufacturing compliance.

Management of incidents, deviations, corrective actions, and preventative actions is often associated with maintenance of regulatory compliance or with continuous improvement processes. These activities are also often performed in conjunction with other Manufacturing Operations Management (MOM) activities.

Incidents are the unexpected events related to maintaining plant operations, safety, regulatory compliance, or security. Incident management involves investigation to determine the root cause of the incident and may lead to preventive actions to prevent future incidents.

Incidents and response to them should be recorded as part of incident management system.

EXAMPLE 1: An unexpected release of a chemical into the environment may generate an incident, and the incident report may have to be sent to the appropriate regulatory agency.

EXAMPLE 2: An unexpected pump failure from a newly installed pump may generate an incident, and the incident response may be to investigate and potentially change the supplier.

Deviations are the measured differences between an observed value and an expected or normal value, or an anomaly from a documented standard or process. Deviation management involves the determination of the root cause of the deviation and may lead to corrective actions to remove the source of the deviation.

Deviations and response to them should be recorded.

Maintaining plant operations often requires that corrective actions, in response to an incident, deviation, or failure. Clear, appropriate, and implementable corrective actions should be identified at the conclusion of any investigation. Tracking and follow-up should be managed to ensure that the corrective actions are implemented and verified.

The root cause of the incident and the corrective actions should be recorded.

EXAMPLE 1: Corrective actions may include improving procedures, adding maintenance procedures for equipment, or implementing retest or revalidation procedures.

Preventative actions are managed in a similar fashion, to prevent possible future incidents or deviations.

EXAMPLE 2: Batch cycle times on a process cell may not meet the rated value, and this is identified as a deviation; then, a preventive action is created to reduce the batch cycle time.

Recommended actions are managed in a similar function. Recommended actions are predefined sets of actions to occur in the event of an incident or deviation.

1.4 COST OF NONCOMPLIANCE

Industrial facilities are created to satisfy human needs. Today, working in a safe workplace is a fundamental human right, and any business activities must be embedded in the current social, physical, cultural, and economic environment.

Management of the social responsibilities and liabilities post a major accident can be very complicated. The major disaster of Erika oil tanker in 1999 and BP Horizon in 2009 are the examples of these complex situations.

In many cases the complacency or haste of decision makers is the leading cause of the major accidents. Very often the cost of eliminating the technical causes is much less than the financial cost of the accident consequences. Table 1.1 summarizes the cost of nonquality of a few major accidents.

Table 1.1 Cost of Accident Versus Cost of Eliminating the Cause of Accident

Major Accident	Cause	Consequence
1986: Space Shuttle Challenger	Break down of an O-ring Cost of redesigning O-rings: a few hundred thousand dollars	Human: 7 fatalities Financial: 1 billion USD Environmental: Minor Reputation: Inestimable
2009: Toyota	Problematic floor mat and defective breaks leading to unintended acceleration	Human: 52 dead and 38 injured Financial: 5.5 billion USD Environmental: Minor Reputation: Inestimable
2010: BP Horizon	Weak Cement around well The cost of checking the cement: 188,00 USD Time: 10 hours	Human: 11 fatalities Financial: 10 billion USD Environmental: Inestimable Reputation: Inestimable—losing 1/3 of BP value in stock market forcing BP to sell some of its assets worldwide

The managers carry the responsibility for ensuring that the equipment is competitively priced and that its safety integrity is adequate in operation. They should apply a systematic approach to ensure that optimum solutions are implemented to consider the complexity of the system and balance the equilibrium between the cost and safety.

A Study on 319 major industrial accidents which were recorded per the UNEP-specified criteria concludes:

- Although the number of major industrial accidents is higher in *developed countries* than in *developing ones*, the number of deaths and injuries is considerably less. Very probably, this fact is the result of better enforcement of *safety regulatory legislation* in developed countries.
- Another effect of better enforcement of safety regulatory legislation is the fact that it seems that during the *last two decades*, the number of major industrial accidents *is decreasing in general*.

Fig. 1.10 demonstrates two other important facts:

1. Comparison between BP Horizon and Piper Alfa shows that:
   a. *Asset loss*: 100% damage of both BP Horizon and Piper Alfa offshore platforms

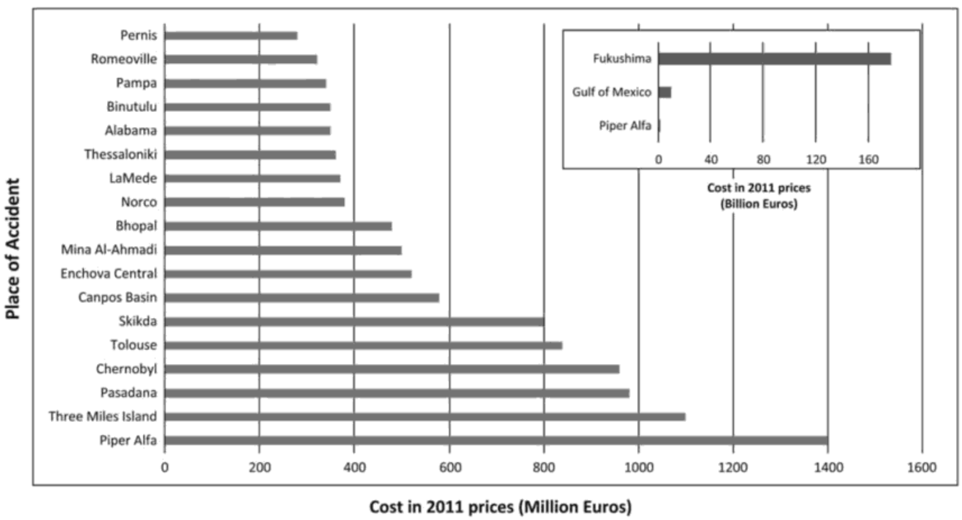


FIGURE 1.10
Cost of some the major accidents.

b. *Human loss*: BP Horizon (11 fatalities) versus Piper Alfa (167 fatalities)
c. *Environmental damage*: BP Horizon (inestimable) versus Pipe Alfa (relatively limited)

Safety case regulations and risk-based approach came into force after Pipe Alfa disaster. This comparison shows that the safety regulations have been effective in protecting lives of BP Horizon personnel. On the other hands, due to the application of the novel technology on much more challenging environmental conditions, the environmental damages of BP Horizon have been much more sever and affected the areas beyond the USA boarders up to the African coasts.

2. The Fukushima major accident demonstrates that when natural events combine with industrial accidents, the losses can be much more devastating. Climate changes cause the more sever natural extrems. Decision makers should bear in mind that the original design basis and safety factors of the ageing plants may not be sufficient to cope with the actual environmental conditions. The cost of the Fukushima accident is about 160 times more than Chernobyl.

Safety and quality are the two faces of a coin. If a defect or noncompliance in the process production leads to toxic and/or flammable materials, then a major accident occurs. Fig. 1.11 demonstrates how quality assurance cycle is related to the risk-based PSM. Without a robust quality management system an effective safety management system cannot be implemented.

Cost effectiveness is the outcome of a realistic and wise balance between opposite spending: the cost of the good quality (or the cost of conformance-immediately and exactly measured) and the cost of poor quality (or the cost of nonconformance-latent and unpredictable extent). As Fig. 1.12 shows the cost of good quality affects:

- Costs for investing in the prevention of nonconformance to requirements.
- Costs for appraising a product or service for conformance to requirements.

The cost of poor quality affects the internal and external costs resulting from failing to meet requirements.

Internal failure costs are costs that are caused by-products or services not conforming to requirements or customer/user needs and are found before delivery of products and services to external customers. They would have

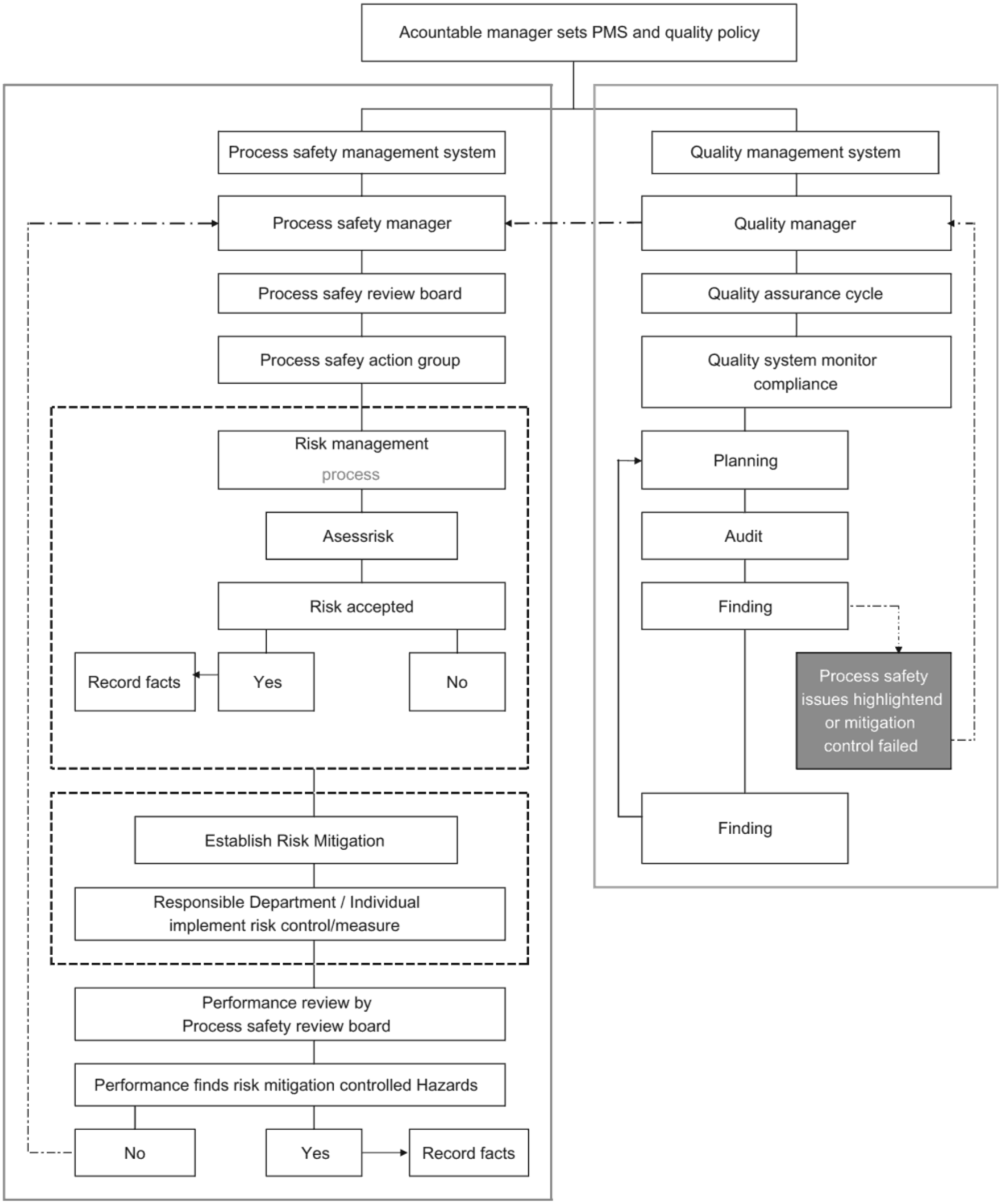


FIGURE 1.11

Integrated quality and process safety management systems. Inspired by: Safety management systems—guidance to organizations.

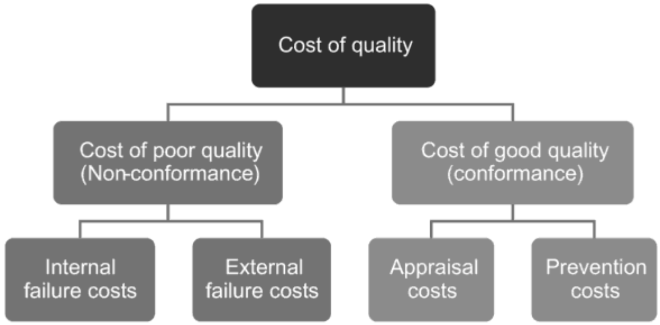


FIGURE 1.12
Cost of quality.

otherwise led to the customer not being satisfied. Deficiencies are caused both by errors in products and inefficiencies in processes.

External failure costs are costs that are caused by deficiencies found after delivery of products and services to external customers, which lead to customer dissatisfaction.

Prevention costs are costs of all activities that are designed to prevent poor quality from arising in products or services.

Appraisal costs are costs that occur because of the need to control products and services to ensure a high-quality level in all stages, conformance to quality standards and performance requirements.

The total quality costs are then the sum of these costs. They represent the difference between the actual cost of a product or service and the potential (reduced) cost given no substandard service or no defective products.

Many of the costs of quality are hidden and difficult to identify by formal measurement systems. The iceberg model is very often used to illustrate this matter: Only a minority of the costs of poor and good quality are obvious—appear above the surface of the water. But there is a huge potential for reducing costs under the water. Identifying and improving these costs will significantly reduce the costs of doing business.

A general study made by UK Health & Safety Executive into the cost of accidents showed that the costs of error rectification far exceeded those that would have been incurred if a systematic approach had been employed from the outset. Fig. 1.13 summarizes the typical insured and uninsured cost associated to an accident.

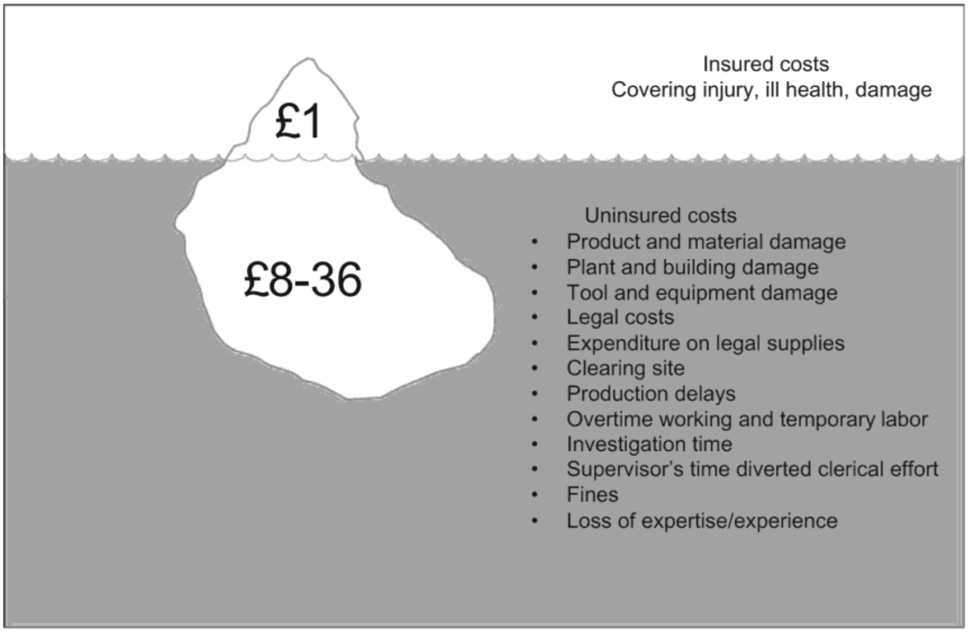


FIGURE 1.13
Iceberg model for the major accident costs. *From Out of control—Why control systems go wrong and how to prevent failure.*

1.5 PROCESS SAFETY VERSUS OCCUPATIONAL SAFETY

In Part 3-Section 10.6 of ISA-95 the typical health and safety activities listed as follows:

1. Handling, classification, packaging, and labeling of hazardous substances including safety data sheets.
2. *Disaster planning including emergency planning and response, and fire safety.*
3. Hazard communication in the form of warning signs, training, and advice.
4. Occupational health surveillance in the form of occupational exposure controls (including chemical, physical, biological agents, and noise).
5. Medical surveillance of personnel.
6. *Process safety in the form of machinery safety, lifting equipment, pressure systems, confined space entry/work permits/access control.*
7. *Management of functional safety.*

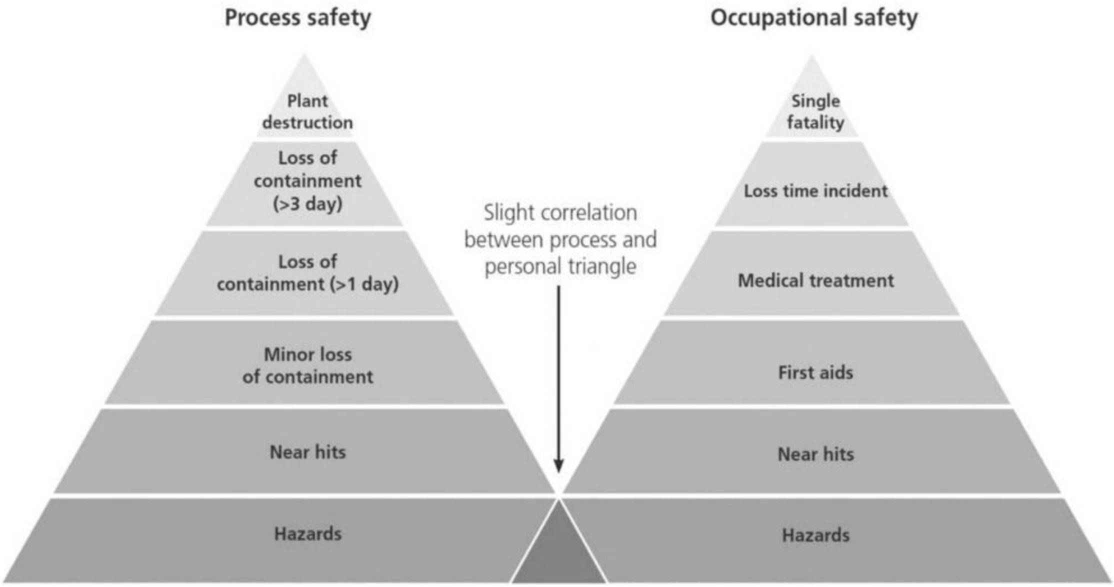


FIGURE 1.14
Process safety and occupational safety. *From Energy Institute-HUMAN FACTORS BRIEFING NOTE No. 20.*

8. Electrical safety.
9. Ergonomics including office work, manual handling of loads, and the like.
10. First aid.

This list mixes the material, occupational health & safety and process safety together. Many people are confused in the same way and ask the HSE practitioners "what is the need for PSM when our HSEMS is already in place?"

The likelihood and the extent of consequences of the occupational safety hazards differ significantly from the process safety hazards. In other words:

- *Occupational safety*—focuses on protecting the safety, health and welfare of people at work (sometimes is called "Personal safety").
- *Process safety*—focuses on the major accident hazards associated with releases of energy, chemicals, and other hazardous substances.

Process safety is a blend of engineering and management skills focused on preventing catastrophic accidents and near hits, particularly, structural collapse, explosions, fires, and damaging releases associated with a loss of containment of energy or dangerous substances such as chemicals and petroleum products. These engineering and management skills exceed those required for managing workplace safety as it impacts people, property and the environment. Fig. 1.14 compares the process safety and the occupational safety indicators.

1.6 PROCESS SAFETY INDICATORS

API 754 introduced a four-tier model for implementation of process safety key performance indicators (KPIs) in the process industry. The model is illustrated by the pyramid diagram in Fig. 1.15 that also shows the need for higher numbers of KPIs at the more leading levels.

The four tiers expressed as a triangle to emphasize that statistically larger data sets are available from the KPIs at the lower tiers. This approach mirrors the now-familiar personal accident triangle shown in Fig. 1.16 based on insurance claim work in 1931 by W. Heinrich and refined in 1969 for safety by Bird & Germain.

Tier 1 and Tier 2 (T1 and T2) are well-defined KPIs based on the recording of process safety events (PSEs) that involve loss of process containment (LOPC) that either exceed gas or liquid release thresholds or result in serious consequences such as injury or fire.

In contrast, Tiers 3 and 4 (T3 and T4) provide an intentionally broader concept, with the aim of encouraging companies to introduce a range of more leading KPIs that are typically defined locally at the facility or asset level, or in some instances across a business or company, to monitor the effectiveness of barriers that are specifically designed as risk controls at the operating level.

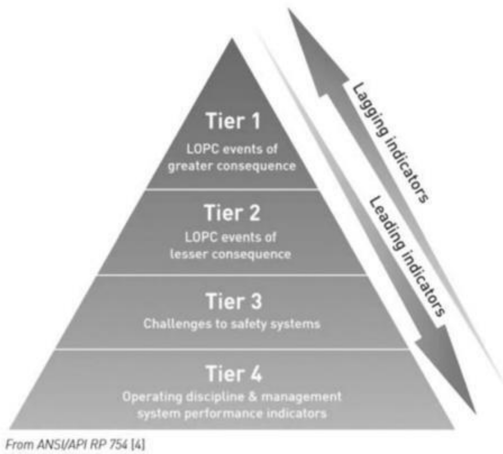


FIGURE 1.15
Process safety indicator pyramid per API 754.

FIGURE 1.16
Occupational safety indicator pyramid.

1.7 WHAT DO WE MANAGE, "SAFETY PROCESSES" OR "PROCESS SAFETY"?

"Process Safety" in "Process Safety Management" is another confusing term. "Process Safety" and "Safety Processes" cover very different scopes. The same confusion can occur in using the following terms:

- *Process manufacturing* is the branch of manufacturing that is associated with formulas and manufacturing recipes. It can be contrasted with discrete manufacturing, which is concerned with discrete units, bills of materials, and the assembly of components.
- *Manufacturing processes* are the steps through which raw materials are transformed into a final product. The manufacturing process begins with the creation of the materials from which the design is made. These materials are then modified through manufacturing processes to become the required part. Manufacturing processes can include treating (such as heat treating or coating), machining, or reshaping the material. The manufacturing process also includes tests and checks for quality assurance during or after the manufacturing and planning the production process before manufacturing.

The "*Process Safety* Management" as we know is, in fact, the "*Safety Processes* Management." The safety processes may or may not be relevant to the chemical engineering and unit operation processes. A process engineer may have no expertise in the activities such as the "permit to work (PTW)" or management of the subcontractors.

1.7.1 Process Safety Engineering

"Process Safety" engineering aims to reduce the risk of an undesirable process events such as the overpressure, overtemperature, overflow, vacuum, undertemperature, low level to as low as reasonably practicable. The safety measures beginning by inherently safer design to emergency response systems are in place to achieve this goal.

HAZard & OPeratability (HAZOP) studies identify the credible undesirable events.

Then, process safety engineers implement the required protection layers using the layer of protection analysis (LOPA) as follows:

1. Inherently safer design
2. Basic Process Control Systems
3. Critical Alarms in compliance with EEMMU 191 and ISA-84.0 guidelines
4. Safety Instrumented Systems (SIS)

   API 14C (ISO 10418) provides the prescriptive recommendation for primary and secondary protection of the conventional oil & gas equipment. API 14C has been developed for offshore facilities, but today it is applied for both onshore installation use this guideline too. We believe that with some customization for the reactors or specific equipment, the approach of API 14C is very useful for evaluation of the process safeguarding requirements of petrochemical and refineries processes too.

   None of the safety barriers is 100% effective. The required safety integrity level of the instrumented-based safety functions is determined and assured by application of the international standards of IEC 61508 and IEC61511.
5. Secondary process safeguards such as relief valves or dikes around the storage tanks are in place to minimize the risk when the primary instrumented-based process safeguards failed to protect the process against an undesirable process event. Fig. 1.17 illustrates how the protection layers reduce the initial risk of the tolerable risk.

Traditionally the requirements of the nonprocess emergency response systems including F&G detection, ESD, active and passive fire protection and EER systems were determined by the loss prevention engineers. The external specialist consultants perform the risk-based studies.

Today, process safety engineering is considered as a new discipline. The "process safety engineer" should cover both process and nonprocess hazard identification, risk assessment, and safety barrier management.

Bow-tie or Swiss cheese method is another common technique that the process safety engineers use to determine the safety critical elements (SCEs).

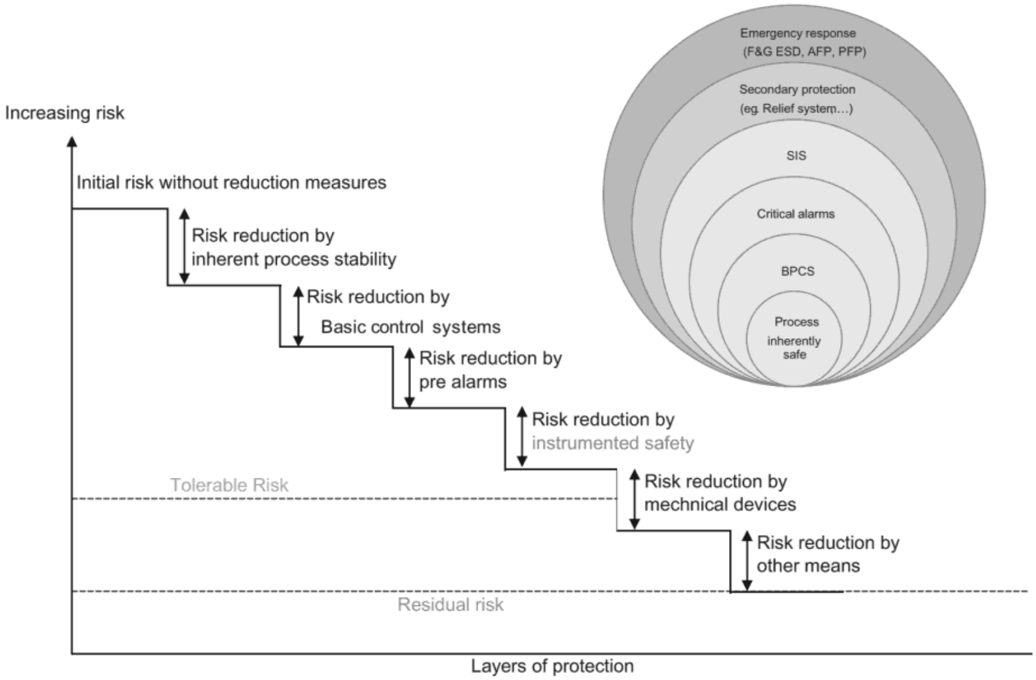


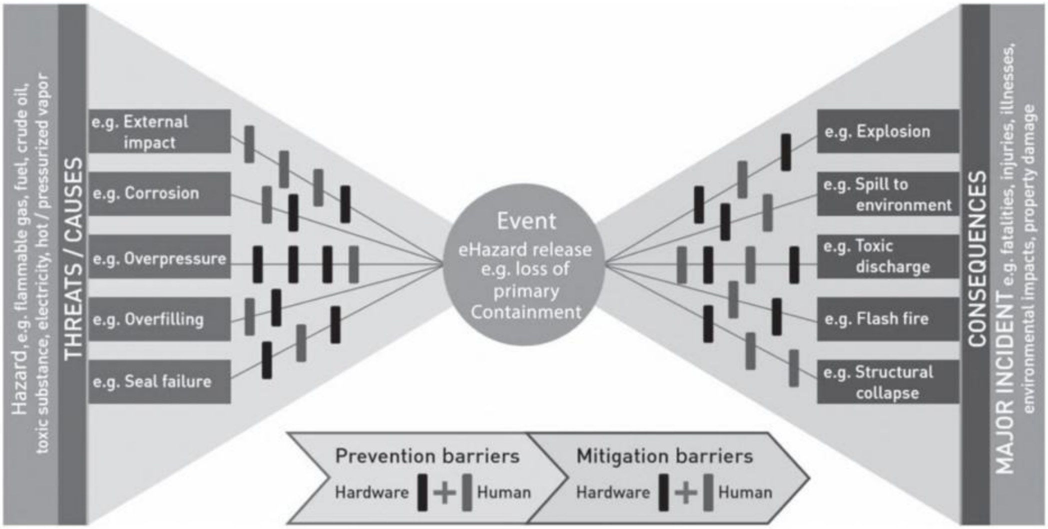
FIGURE 1.17
Layers of protection analysis (LOPA).

Barrier thinking is a useful concept to manage the safety barriers which could be the hardware or human intervention.

A barrier is defined as a functional grouping of safeguards, such as primary containment, process equipment, engineered systems, operational procedures, management system elements, or worker capabilities designed to prevent loss of process containment (LOPC) and other types of asset integrity or PSEs, and mitigate any potential consequences of such events. A set of barriers is also often referred to as a risk control system.

As illustrated in Fig. 1.18, barriers are put in place to manage the risk of a hazard being released resulting in an unintended event, such as LOPC, which could cause harmful consequences. A properly functioning barrier will either stop the event from happening (a prevention barrier) or reduce its consequences (a mitigation barrier).

Hardware barriers include the activities necessary to assure that they continue to meet the performance standards set at the design stage, while the asset's workforce provides human barriers that respond and act to manage the potential cause or threat of an event. The elements of the asset's management system then provide the necessary support processes to ensure the barriers are effective throughout the asset's life (Fig. 1.19).



Hardware barriers	Human barriers
Category 1: Structural integrity Category 2: Process containment Category 3: Ignition control Category 4: Detection systems Category 5: Protection systems–including deluge and firewater systems Category 6: Shutdown systems–including operational well isolation and drilling well control equipment Category 7: Emergency response Category 8: Life- saving equipment– including evacuation systems.	Category 1: Operating in accordance with procedures including: • Permit to work • Isolation of equipment • Overrides and inhibits of safety systems • Shift handover, etc. Category 2: Surveillance, operator rounds, and routine inspection Category 3: Authorization of temporary and mobile equipment Category 4: Acceptance of handover or restart of facilities or equipment Category 5: Response to process alarm and upset conditions (e.g. outside safe envelope) Category 6: Response to emergencies.

FIGURE 1.18

Example of bow-tie model. *(From: IOGP-456).*

For example:

- in a pressure vessel engineered with sufficient integrity and controls to prevent release of hydrocarbons, the definition of a hardware barrier includes the management of that barrier or the tasks and activities necessary to assure that it continues to meet the requirements of the performance standard. The management system includes a description of the maintenance and inspection process designed to support this.

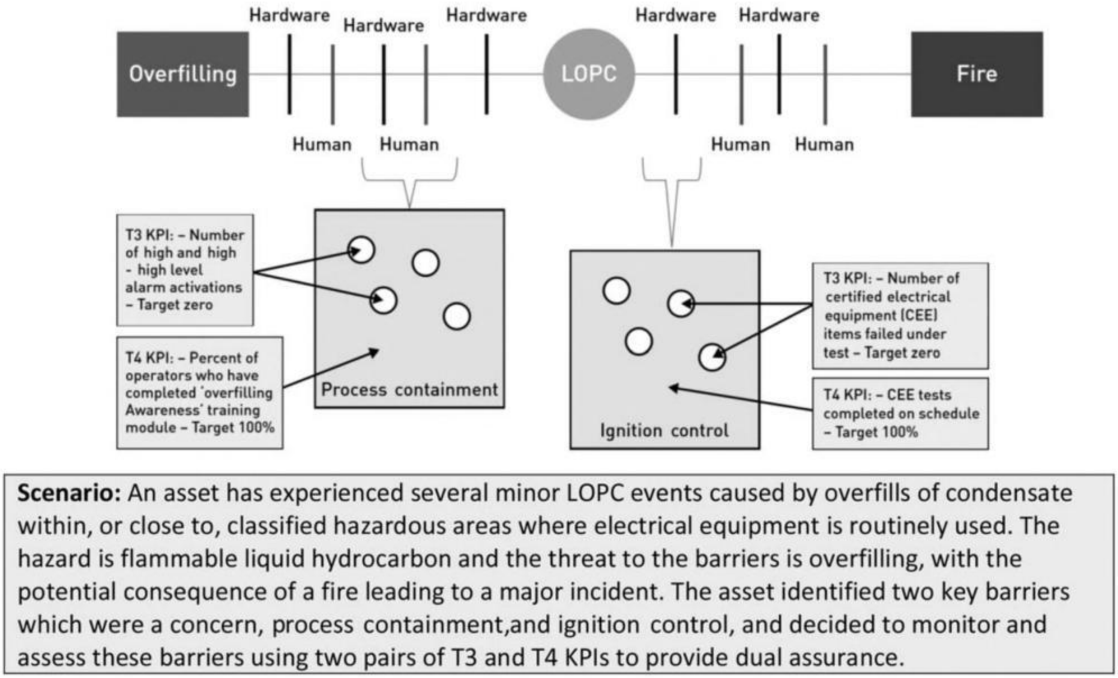


FIGURE 1.19
Selection of key barrier for application of dual assurance. *(From: IOGP-456).*

- an operator monitoring the filling of a tank can respond to an alarm by implementing a procedure to prevent an overfill. The effectiveness of this human barrier relies on the discipline and knowledge to operate the plant in accordance with the procedures. Failure to do so may be attributable to an underlying management system failure such as competency management, unclear procedures or under-resourcing.

The KPIs are in place to proactively track and identify the flaws in the safety barrier which are analogue to the "holes in the cheese" and then based on KPI reports the required actions should be taken to eliminate or minimize these defects. Two categories of KPIs can be distinguished. API 754, categorizes the process event KPIs in four categories. The first three categories measure outcomes (i.e., unintended events or effects) and the fourth category of KPIs measure inputs that sustain barriers. IOGP 556 calls this approach as "Dual Assurance."

1.7.2 Management of the Safety Processes

The ethical, legal, and financial imperatives motivate the organization to adopt a more holistic and systematic approach to assuring the integrity of their operations. Process Safety Management (PSM) is a risk-based framework which defines the key Safety Processes to be managed by organizations to assure the integrity of their operations.

Technical, maintenance, operational, human, and organizational factors are incorporated in the PSM framework.

PSM can be defined as

> *. . .a businesslike approach to safety. It is a systematic, explicit and comprehensive* process *for managing safety risks. As with all management systems, a* safety management system *provides for* goal setting, *planning, and measuring performance. A safety management system is woven into the fabric of an organisation. It becomes part of the culture, the way people do their jobs.*

For the purposes of defining PSM, safety can be defined as

> *. . . the reduction of risk to a level that is as low as is reasonably practicable (ALARP).*

The guideline of Center for Chemical Process Safety (CCPS) *for risk-based process safety (RBPS) provides a high level framework.* Fig. 1.20 illustrates the Energy Institute version of the CCPS PSM framework.

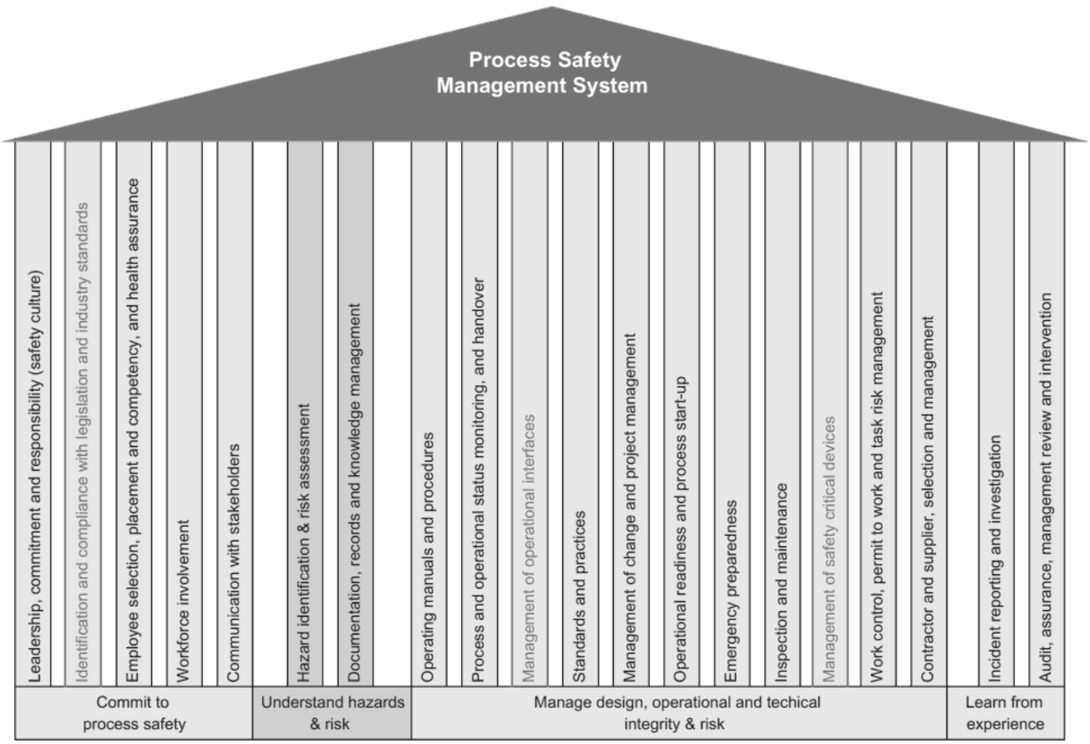


FIGURE 1.20

Energy institute process safety management elements.

Implementation of an effective PSM cannot be achieved if the impact of the other management systems is neglected. Fig. 1.21 illustrates the relationship between the PSM and the other management systems.

The word "process" in PSM does not refer to the chemical engineering processes or process safety engineering that we explained in the previous section. The focus of the PSM is on the "processes" as defined in the *Systems Engineering* standard entitled "ISO/IEC 15288—Guidance for System Lifecycle Processes." Therefore without having a good understanding of system engineering implementation of an effective PSM cannot be possible.

The processes can be used by organizations (for example functional organizations and projects) that play the role of acquirer, supplier (for example main contractor, subcontractor, service provider) or management to fulfill responsibilities about the system-of-interest.

A process is an integrated set of activities that transform inputs (for example a set of data such as requirements) into desired outputs (for example a set of data describing the desired solution).

Fig. 1.22 illustrates example inputs and outputs of a process for engineering a system. The inputs can be either converted to desired outputs or can enable

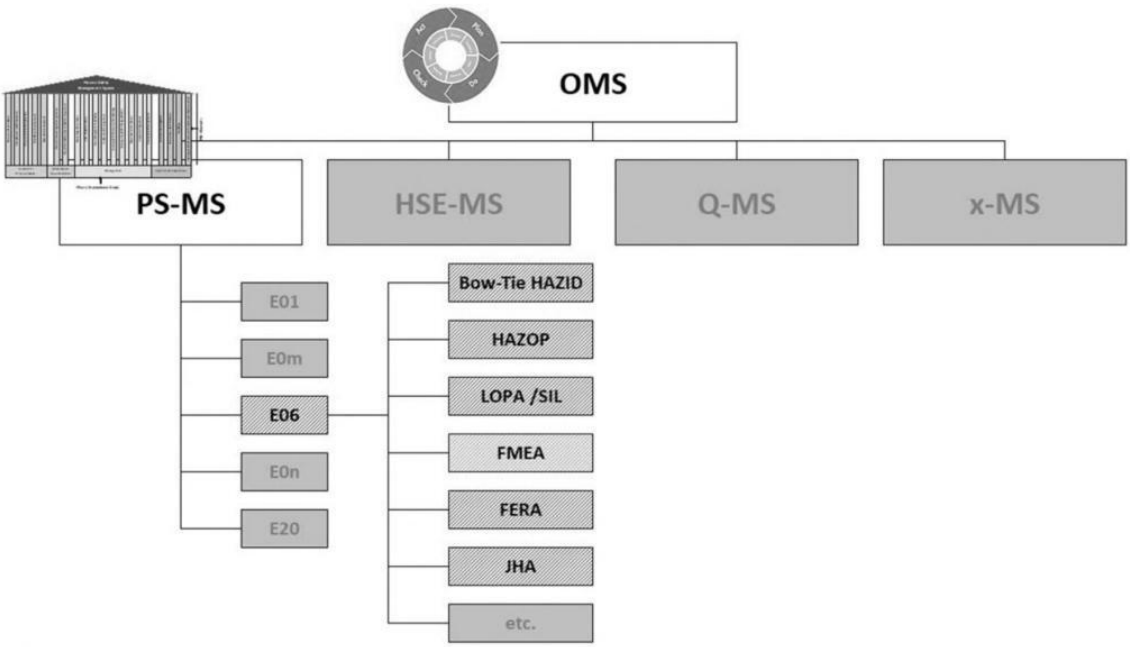


FIGURE 1.21
Operational Excellence Roadmap.

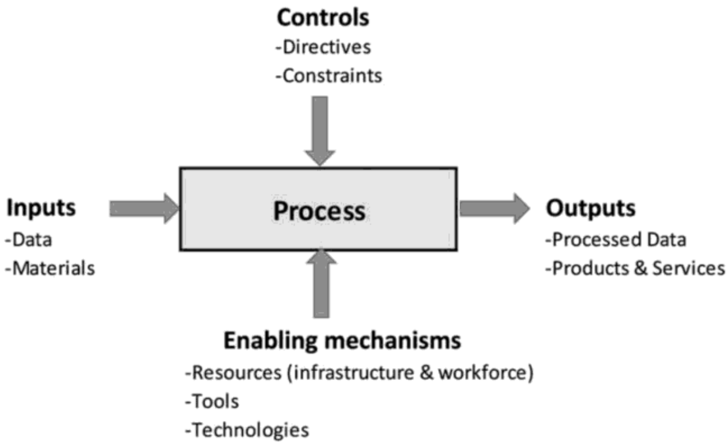


FIGURE 1.22
Example process inputs and outputs according to ISO/IEC 15288.

or control the conversion. Each set of these process inputs and outputs needs to be defined and managed.

Processes can be controlled by organizational or enterprise management directives and constraints and by governmental regulations and laws. Examples of such controls on a process include:

1. The project agreement.
2. The interfaces with other systems for which the project is responsible (see Fig. 1.23).
3. The applicable system lifecycle stage or stages.
4. The organization or enterprise that has project responsibility.

Each process can have a set of process enabling mechanisms as follows:

1. The workforce that performs the tasks related to the process.
2. Other resources required by the process such as facilities, equipment, and funds.
3. Tools (for example software and hardware, automated, manual) required for performing the process activities.
4. Technologies needed by persons performing the activities including methods, procedures, and techniques.

1.7.2.1 Lifecycle Processes

ISO/IEC 15288 describes four groups of system lifecycle processes—agreement, enterprise, project, and technical. Each process has a specific purpose, a set of expected outcomes and a set of activities.

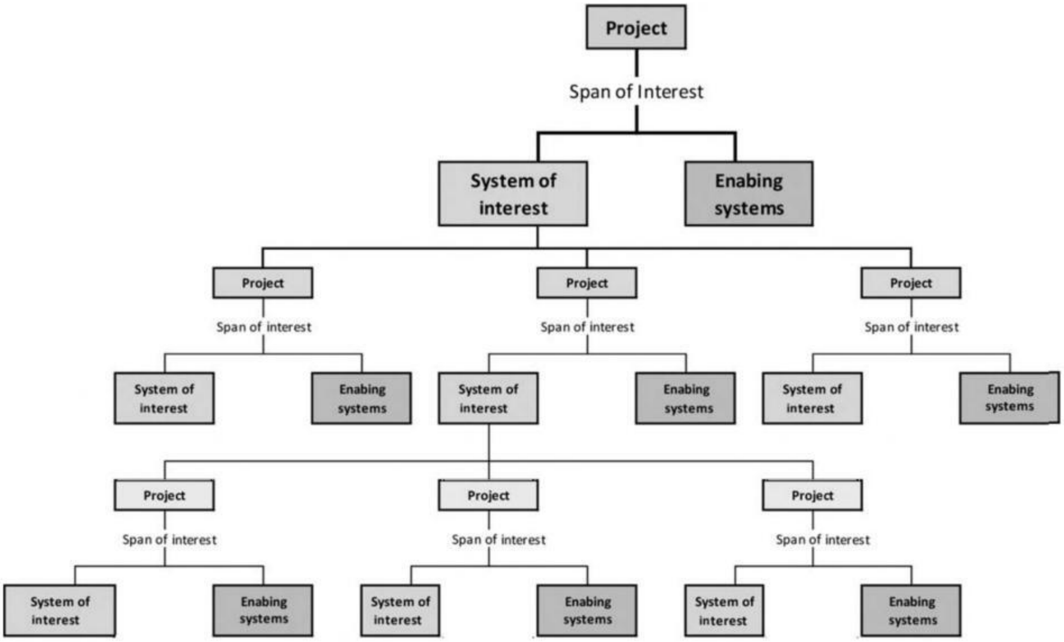


FIGURE 1.23
Hierarchy of projects.

1.7.2.2 Agreement Processes

The agreement processes are applicable for establishing the relationship and requirements between an acquirer and supplier. The agreement processes provide the basis for initiation of other project processes to enable arriving at an agreement to engineer, utilize, support, or retire a system and to acquire or supply related services.

The agreement processes can be used for several purposes such as listed below.

1. To form and ensure completion of an agreement between an acquirer and a supplier for work on a system at any level of the system structure.
2. To establish and carry out agreements to acquire a system or related enabling system services.
3. To obtain work efforts by consultants, subcontractors, functional organizations, projects, or individuals or teams within a project.
4. To provide the basis for closing an agreement after the system has been delivered or work has completed and payment made.

1.7.2.3 Enterprise Processes

Enterprise processes are for that part of the general management that is responsible for establishing and implementing projects related to the products and services of an organization. Thus the enterprise through these distinct processes provides the services that both constrain and enable the projects, directly or indirectly, to meet their requirements.

The enterprise processes are not necessarily the only processes used by an enterprise for governance of its business. For example enterprises also have processes for managing accounts receivable, accounts payable, payroll processing, and marketing. These processes are not within the scope of the International Standard.

For multiple projects involved in or interfacing with an enterprise, or for a teaming arrangement among external organizations, other enterprise processes can be appropriately established or the processes can be appropriately tailored.

To perform these processes, it is not intended that a new organizational unit or discipline within an enterprise be created. Identified and defined roles, responsibilities, and authorities may be assigned to individuals or existing committees or established organizational units. When necessary, however, a new enterprise unit can be formed.

The enterprise processes have specific objectives to fulfill such as listed below.

1. Provide the proper environment so that projects within the organization can accomplish their purpose and objectives.
2. Ensure that there is an orderly approach to starting, stopping, and redirecting projects.
3. Ensure that organizational policies and procedures are defined that set forth the processes of the International Standard and that are applicable to projects within the enterprise.
4. Ensure that appropriate methods and tools are selected and provided to projects so that they can complete process activities efficiently and effectively.
5. Ensure that projects have adequate resources for the project to meet cost, schedule, and performance requirements within acceptable risks and that human resources are appropriately trained for completing their responsibilities.
6. Ensure that project work products for delivery to customers are of a suitable quality.

1.7.2.4 Project Processes

The project processes should be used to manage technical process activities and to assure satisfaction of an agreement. Project processes are performed to establish and update plans, to assess progress against plans and system requirements, to control work efforts, to make required decisions, to manage risks and configurations and to capture, store, and disseminate information.

Outcomes from performing the project processes help in the accomplishment of the technical processes.

The project processes apply to engineering projects that are most often part of larger projects. When that is the case, the appropriate project processes are performed at each level of the system structure. These processes also apply when performing enterprise processes or carrying out the activities related to a lifecycle stage, including utilization, support, and retirement.

When several projects coexist within one enterprise, project processes should be defined to allow for the management of the resources and performance of the multiple projects.

1.7.2.5 Technical Processes

The technical processes are applicable across all lifecycle stages. The following technical processes should be performed to engineer a system.

1. Stakeholder requirements definition process.
2. Requirements analysis process.
3. Architectural design process.
4. Implementation process.
5. Integration process.
6. Verification process.
7. Transition process.
8. Validation process.

These processes should be performed to satisfy the entry or exit criteria of a system lifecycle stage or set of stages. For example, they may be used during early system lifecycle stages to create a feasible system concept, determine technology needs and establish future developmental costs, schedules, and risks. During mid-system lifecycle stages the technical processes may be used to define and realize a new system. During later system lifecycle stages they may be used on legacy systems to make technology refreshments or technology insertions, as well as to correct variations from expected performance during production, utilization, support, or retirement.

The other three technical processes (operations process, maintenance process, and disposal process) can be used during any system lifecycle to accomplish the objectives of a lifecycle stage and support the technical processes used for engineering a system. The operations process and the maintenance process can be performed, as applicable, to support a particular version of a system. The disposal process can be performed to deactivate legacy systems, to dispose of legacy systems and to safely dispose of unwanted by-products from system use.

1.7.3 Technical Process Model

Fig. 1.24 provides a model for the application of the technical processes. This model includes only the technical processes that are primarily used for engineering a *system-of-interest*. The operation process, support process, and disposal process are not shown in Fig. 1.24. These three processes should be used as appropriate to provide inputs to the stakeholder requirements definition process. The requirements could be in the form of acquirer requirements such as

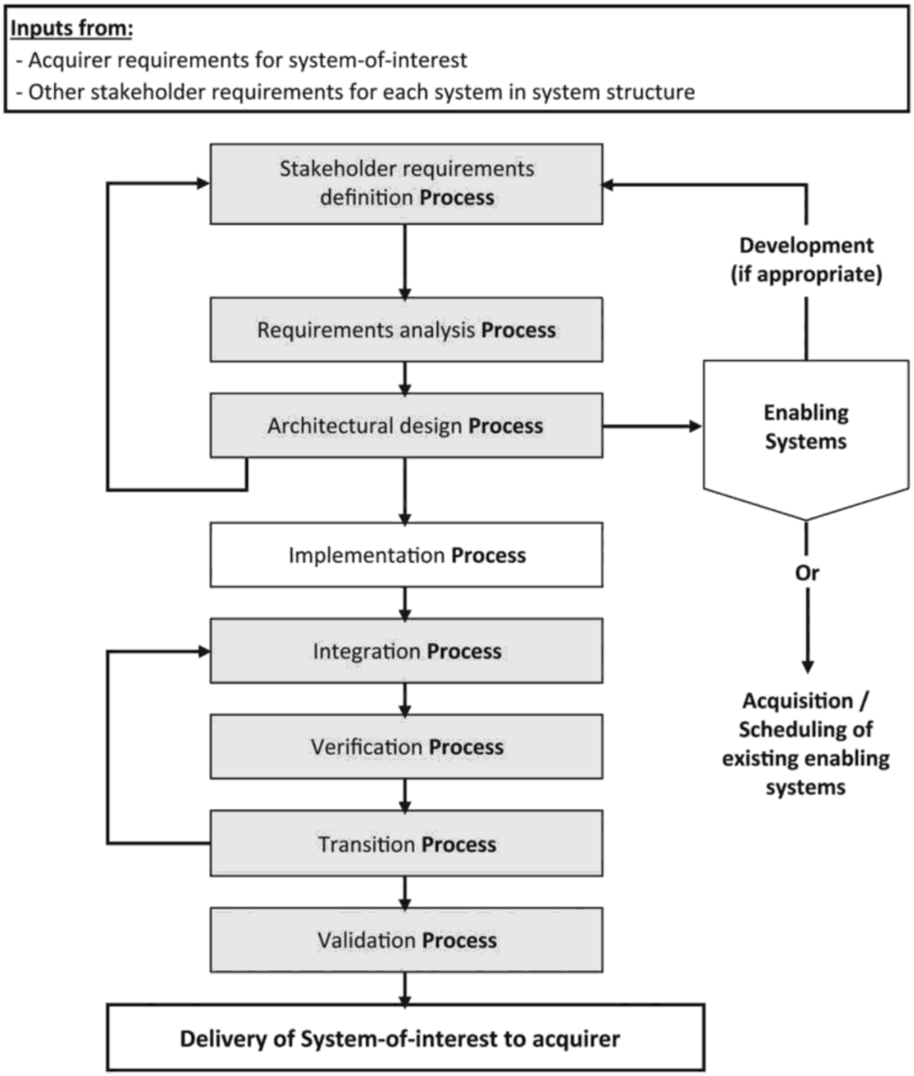


FIGURE 1.24
Application of technical processes to engineer a system-of-interest with the enabling systems.

operability, supportability, and disposability or in the form of other interested party requirements such as for enabling systems to provide related services.

The stakeholder requirements definition process, requirements analysis process, and architectural design process are used to design the solution for each system in the system structure. Application of these processes can be highly iterative to arrive at the desired design solution.

The implementation process, integration process, transition process, and validation process are used to realize the architectural design solution for each system in the system structure. These processes can be highly iterative too.

For each architectural design solution in the system structure the enabling system requirements related to the system should be identified. The enabling system requirements should be satisfied either by engineering the enabling systems that need to be developed or by acquisition or scheduling the existing and available enabling systems.

1.7.4 System Lifecycle Model

Within a lifecycle stage, processes are performed as required to achieve stated objectives. The progression of a system through its life is the result of actions managed and performed by people in one or more enterprises using the processes selected for a lifecycle stage.

ISO/IEC 15288 considers a six stages lifecycle model with the "enterprise view" and the "engineering view" as shown in Fig. 1.25.

The order of use of the lifecycle processes is influenced by multiple factors such as social responsibilities, world trade laws, organizational cultures,

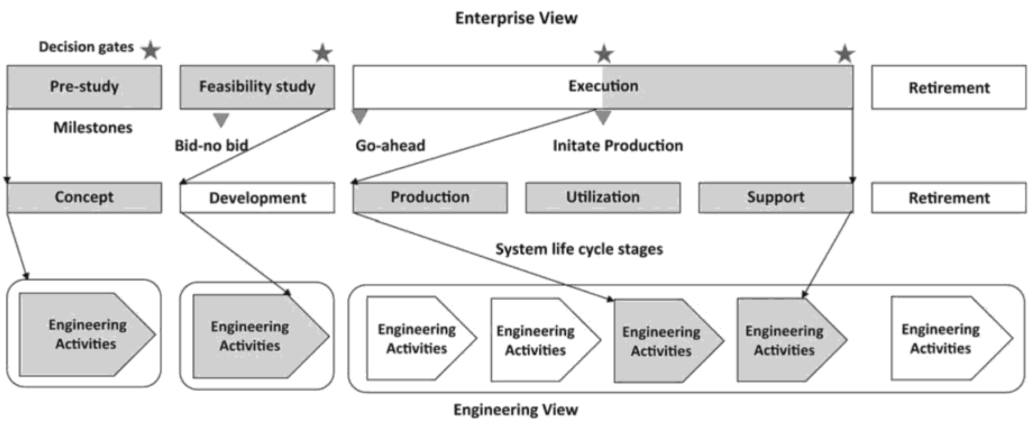


FIGURE 1.25
Enterprise and engineering views related to the representative system lifecycle model.

and technical considerations. Each of these factors can vary during the life of a system. A manager of a system lifecycle stage typically selects the appropriate set of lifecycle processes to meet the exit criteria and other stage objectives. For example, during any of the later lifecycle stages a manager can use the operation process, maintenance process, and disposal process to manage the system while it performs its required functions or is serviced to meet system requirements. During earlier lifecycle stages the same processes can be used to help managing the development of the system as well as affect the disposal of waste products or work products that are no longer needed.

To determine which processes to select and apply during a system lifecycle stage a manager is guided by the purpose and outcomes for each of the stages. The selection of the appropriate processes enables the system's progression through its lifecycle to be managed. The system lifecycle model of Fig. 1.25 can be considered as an illustration of an orderly passage associated with a system going from one stage of life to another. Both the enterprise and engineering views can be helpful in enabling this passage.

An enterprise (for example an automobile company or medical equipment supplier) or a domain group of an organization (for example a government defense agency or industry group) often has a unique view the system lifecycle to control the passage from one system lifecycle stage to the next. The enterprise view illustrated includes management-focused stages that are used to form both milestones and decision gates. The enterprise uses these milestones and gates as decision points where investment decisions can be made as to whether a system should be continued to the next stage or be modified, be canceled or retired or have the plans for the next stage revised before approval. These milestones and decision gates can be used by enterprises to contain the inherent uncertainties and risks associated with costs, schedule, and functionality when a system is created or utilized.

In order to meet the exit criteria of a decision gate a system has to be appropriately engineered and the appropriate work products need to be produced to provide decision-making information and required deliverables. Thus planned engineering activities need to take place during each system lifecycle stage to obtain the outcomes and meet the purpose of the stage or a set of stages.

The engineering view of Fig. 1.25 provides an example framework of engineering activities required to meet the criteria of management decision gates and related system lifecycle model milestones.

Engineering is involved with a system in the early lifecycle stages (concept and development) when it is being studied, defined, and created. Reengineering is involved in later stages (production, utilization, support, retirement) when unwanted and unexpected variations come about due to design errors or failures or new requirements are provided because of technology, competition, or threat system changes.

To engineer a feasible system solution during the concept stage a system structure needs to be sufficiently defined and evaluated. This should be done to assure that system requirements are met and that the costs and risks are understood for the feasible system concept selected. When a parts list is an exit criterion (for example required as part of a proposal or to prepare a creditable cost proposal), sufficiently detailed engineering should be done to ensure that the parts list is complete and that the costs and risks are understood.

To engineer a system solution during the development stage a system needs to be designed with appropriate detail from the system-of-interest level down through successive system levels until a system element can be made, bought, reused or implemented by software. Each system should be verified that it meets its specification requirements included in configuration descriptions from architectural design, and validated that it meets the acquirer and other interested party requirements. Each system elements need to be transitioned to the acquirer where can be assembled and integrated into a higher-level system that is verified, transitioned, and validated. This action continues through successive levels upward to realize the desired system-of-interest.

This approach whether applied to the concept stage or the development stage is typically called top down and bottom up engineering and describes one block of the engineering activities. The top down, bottom up approach is illustrated in Fig. 1.26 and is called the "Vee" diagram or model. This

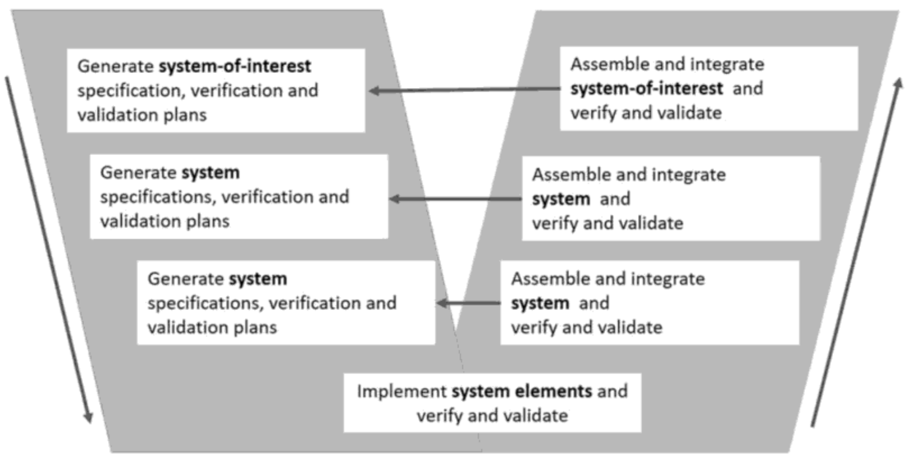


FIGURE 1.26
The engineering "Vee" model.

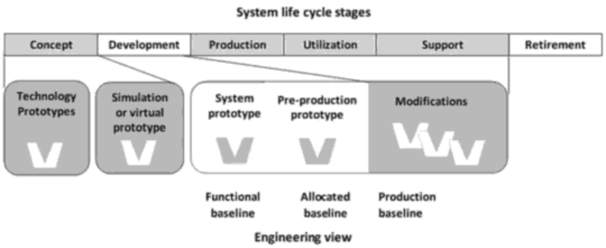


FIGURE 1.27
Engineering view with engineering "Vee" models.

figure reflects the work products and actions expected from the recursive application of the processes in Fig. 1.24 to define and realize the system structure.

Reengineering efforts to correct variations or failures and to meet changed requirements are typically initiated at a system level within the system structure and below the level of the system-of-interest. The same general engineering approach using the "Vee" model is appropriate. In this case, however, the system affected is the place in the system structure where the reengineering effort begins. The requirements for the change are analyzed as to how they could have an impact on interfacing and interacting systems and the performance of the system-of-interest. Then the stakeholder requirements definition process, requirements analysis process, and architectural design process are used downward through successive levels of system structure to define architectural solutions. After the system elements are implemented using the implementation process, the integration process, verification process, transition process, and validation process can be used upward through successive levels to the system-of-interest. This approach is often called middle-out engineering.

The engineering "Vee" model is used in each system lifecycle stages as appropriate to meet stage entry or exit criteria or to meet the enterprise view milestone or decision gate requirements as shown in Fig. 1.27.

1.7.5 Process Versus Procedure

The language of the 2000 revision to the ISO 9000 series significantly moves away from procedure to process and the new concept that the results an organization achieves are the product of the interaction between its processes and not its procedures.

Identifying and managing critical business processes is a vital factor in the effective management of successful organizations. This appears to be a fairly

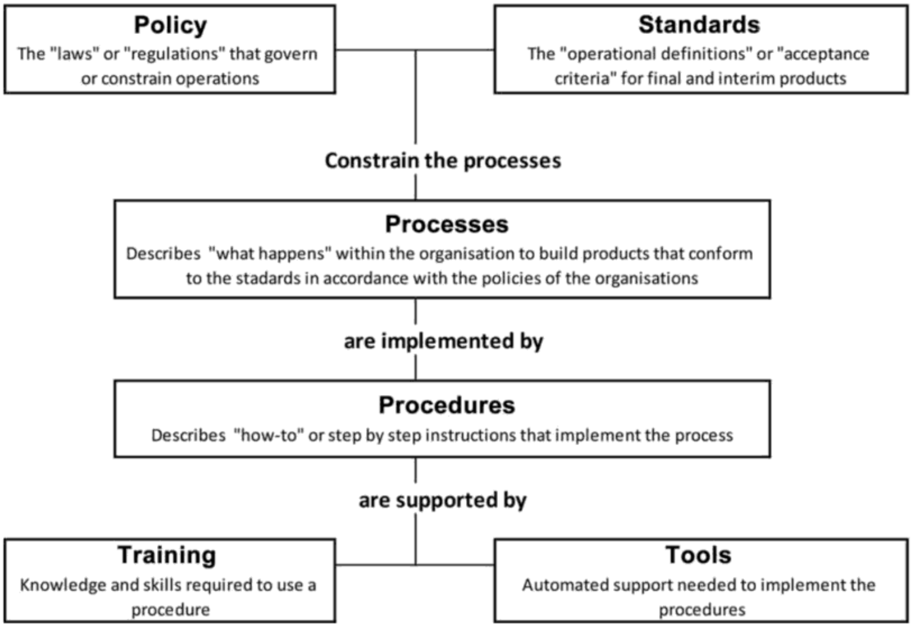


FIGURE 1.28
Process and procedure roles.

obvious statement. At the heart of the business excellence model there is a strong beat generated by the emphasis on process management. Within the context of quality management standards, and more specifically ISO 9000, "procedure" is a key word which has acquired a particular meaning over the years (Fig. 1.28).

1.7.5.1 Procedures

In its simplest form a procedure is a way in which one works to accomplish a task. It can therefore be a sequence of steps that include preparation, conduct, and completion of a task. Each step can be a sequence of activities and each activity can be a sequence of actions. The sequence of steps is critical to whether a statement or document is a procedure or something else. Specifications, contracts, and records are not procedures as they do not tell us how to do anything. These describe the outputs resulting from carrying out procedures or tasks, leaving us to decide any further actions necessary to use these outputs. The output will more than likely be used as inputs to other procedures.

We need procedures when the task we have to perform is complicated or when the task is routine and we want it to be performed consistently. Hence procedures are intended to make something happen in a certain way. If we are not concerned about how something is done and are interested only in the result we do not produce procedures but issue instructions such as "post the letter," "repair the spin drier" or "recruit another person." These are the work instructions as they intend us to do "quantitative" work without telling how to do it or the "qualitative" standard to which the work should be carried out. Instructions are not procedures unless they follow in a sequence and enable us to perform a task.

A set of self-assembly instructions is a procedure as it tells how to proceed to assemble the product. But the wording on the label telling us not to put hot objects on the surface is an instruction or a warning (a special type of instruction).

As procedures are normally used by people they are designed with a user in mind. The user is usually an individual or a group of individuals, although procedures can cover a sequence of steps each of which is performed by different individuals or groups. The perceptions of procedures vary considerably depending on the context in which they are created and used. Any sequence of steps, no matter how simple or complicated, can be expressed as a procedure that is intended to cause someone to act in a certain way to accomplish a task. The key is that the steps follow a sequence. A random collection of statements is not a procedure unless we rearrange these in a sequence that enables someone to proceed.

1.7.5.2 Processes

Processes produce results by converting, transforming, or simply using inputs to create outputs. An input could be material, information, people or a set of conditions and these are passed through a sequence of stages during which they are either used, transformed, or their status changed to emerge as an output with different characteristics. Hence, processes act upon inputs and are dormant until the input is received.

At each stage the transformation tasks may be procedural, but may also be mechanical, chemical, etc. Inherently processes do not normally recognize departmental or functional boundaries (but are often hindered by them) nor the boundaries between customers and suppliers.

Each process has an objective with both quantitative and qualitative measures of its outputs directly related to its objectives. The transformation or process stages are designed to ensure the combination of resources achieves the objectives—the desired outputs. Of course, this means that the process has to receive the right inputs to deliver the desired outputs. Also the correct resources should be applied at the right stages, in the correct quantities and in the right manner.

Table 1.2 Procedures Versus Processes

Procedures	Processes
Procedures are driven by completion of the task	Processes are driven by achievement of the desired outcome
Procedures are implemented	Processes are operated
Procedures steps are completed by different people in different departments with different objectives	Process stages are completed by different people with the same objectives—departments do not matter
Procedures are discontinuous	Processes flow to conclusion
Procedures focus on satisfying the rules	Processes focus on satisfying the user
Procedures define the sequence of steps to execute a task	Processes transform inputs into outputs through use of resources
Procedures are driven by humans	Processes are driven by physical forces some of which may be activated by humans
Procedures may be used to process information	Information is processed by use of a procedure
Procedures exist they are static	Processes behave they are dynamic
Procedures cause people to take actions and decisions	Processes cause things to happen

It is true that a process can be illustrated as a sequence of steps just as a procedure is illustrated, but the similarity ends there. Table 1.2 compares the key features of procedures and processes.

To make a transition away from managing procedures towards process management an organization must answer whether it has:

- clearly defined what its objectives are and how it will measure and review the success of achieving those objectives
- evaluated the impact of those objectives on the interested parties, the stakeholders
- designed the critical, end-to-end processes necessary to deliver the objectives
- assessed and provided the resources, skills, and competence to make the processes work

The change in language from procedure to process is not about perception or semantics. To remain competitive the processes should be designed to add value consistently.

1.7.6 Efficiency Versus Effectiveness

Productivity is determined by looking at the production obtained (effectiveness) versus the invested effort in order to achieve the result (efficiency); in other words, if we can achieve more with less effort, productivity increases (Fig. 1.29).

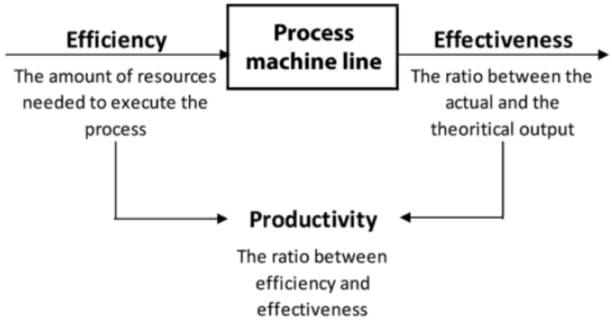


FIGURE 1.29
Productivity is the ratio between efficiency and effectiveness.

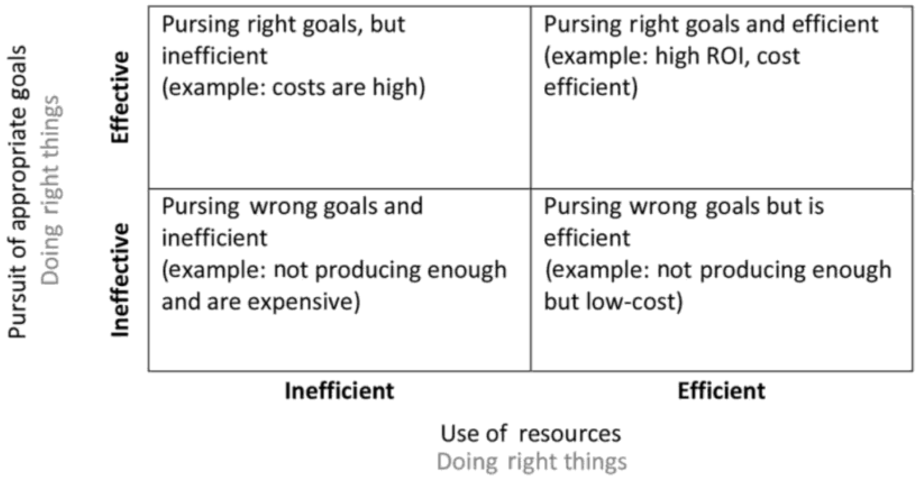


FIGURE 1.30
Effectiveness and efficiency matrix.

For example Amec Foster Wheeler reports that following implementation of their lean "More4Less" program, they achieved 30%–60% cost saving for modifications with accelerated delivery times of more than 50%.

Effectiveness and efficiency are two fundamental goals; all businesses over the world are pursuing, however, more often, there are lack of clarity upon their true means and how to achieve them accordingly (Fig. 1.30).

Business must ensure both efficiency and effectiveness, and with agility if they are to be successful. Efficiency is *doing things right* with minimum inputs and resources (do it right the first time) and effectiveness is *doing the right thing* by following the principles and leading in the right directions. Leaders focus on effectiveness, to ensure business having the vision and well-defined goals to reach it; while managers focus on efficiency, "efficiency" is the relationship between how much time (or labor) you expected or planned to expend, versus what the actual was. If you expend less time or labor than expected, you were efficient.

Companies often talk about employee effectiveness and efficiency when brainstorming ways to improve business. While they sound similar, effectiveness means something entirely different than efficiency. An effective employee produces at a high level, while an efficient employee produces quickly and intelligently. By combining effectiveness and efficiency a company produces better products faster and with fewer resources.

To improve effectiveness, companies must take the initiative to provide thorough performance reviews, detailing an employee's weakness through constructive criticism. Managers must make it a point to address effectiveness and explain how an employee's performance affects the company as a whole. To avoid a workplace full of ineffective employees, companies must hire high-performing employees by weeding out candidates at the recruiting level. Employees are often ineffective because they do not care about their work or because they do not possess the skills to contribute. By interviewing candidates, calling references and conducting tests, companies can bring on employees with skills better suited for performing at a high level.

Employees and managers are often inefficient because they either do not know how to be efficient or do not have the necessary tools to perform tasks efficiently. Ways to improve efficiency include meeting with managers and employees to outline ways to implement efficiency in the workplace and asking for opinions on what the workplace is missing. For example, a small business that lacks an employee email system prevents managers from communicating with employees efficiently.

Quality is doing the right thing right, the first time which means operation with zero backlog and wastage and highest customer satisfaction rate. Generally, you have to assure the effectiveness first, and then make the effect more efficient. Efficiency means a way to measure how good you are in what you are doing in terms of available resources.

Most of the organizations think of efficiency as the most beneficial (profitable) means of doing business. Distributing workloads and delegating is often necessary, but many business practices add complexity that inevitably leads to losses, through additional expenses, waiting, bureaucracy, etc. Often such unnecessary complexity becomes obstacle for businesses to achieve *agility to response* to the changes, or lack of flexibility to make alternative options to do the work. At higher mature level, agility is the ultimate goal for business to response to change with speed, and out-beat competitors with capacity.

Effectiveness is a product of *wisdom* which enlarges both the range of consequences considered in making a decision and the length of time over which the decision is believed to have possible consequences. By taking long- as well as shortrun consequences into account, wisdom prevents sacrificing the future for the present. For example, our technology enables us to keep terminally ill people alive at great cost. But is this the right thing to do in the long run? Is it wise? Might the same resources be better used elsewhere? Wisdom is required for the effective pursuit of ideals, and therefore is required of leadership. Leaders must also have a creative and recreative role in the pursuit of ideals, and these are esthetic functions.

1.8 PROCESS INDUSTRY VERSUS DISCRETE MANUFACTURING

All manufacturing processes can be broadly categorized into two groups: discrete parts assembly manufacturing and process industry manufacturing. Assembly manufacturing generally consists of the manufacture of individual parts and components and then welding, bolting, or otherwise fastening them together into a finished product. Examples include automobiles, aircraft, motorcycles, cell phones, computers, power tools, television sets, and hair dryers.

Process industries are characterized by processes including chemical reactions, mixing, blending, extrusion, sheet forming, slitting, baking, and annealing. Finished products can be in solid form packaged as rolls, spools, sheets, or tubes; or they can be in powder, pellet, or liquid form in containers ranging from bottles and buckets to tankcars and railcars. Examples include automotive and house paints, processed foods and beverages, paper goods, plastic packaging films, fibers, carpets, glass, and ceramics. The outputs may be sold as consumer products (e.g., food and beverages, cosmetics) but more often become ingredients or components for other manufacturing processes (Fig. 1.31).

Process industry and discrete parts assembly manufacturing operations are different and have different challenges. The differences are profound enough that the application of system engineering and other industrial engineering tools must be approached quite differently (Fig. 1.32).

The difference between assembly and process industries has often been characterized as discrete versus continuous processing, but that is a profound over simplification. While many of these processes are continuous (e.g., oil refining, manufacture of bulk chemicals), many are batch chemical (house paints, industrial lubricants) or what could be considered mechanical batching (e.g., rolls of paper, tubs of fiber) and become discrete later in the

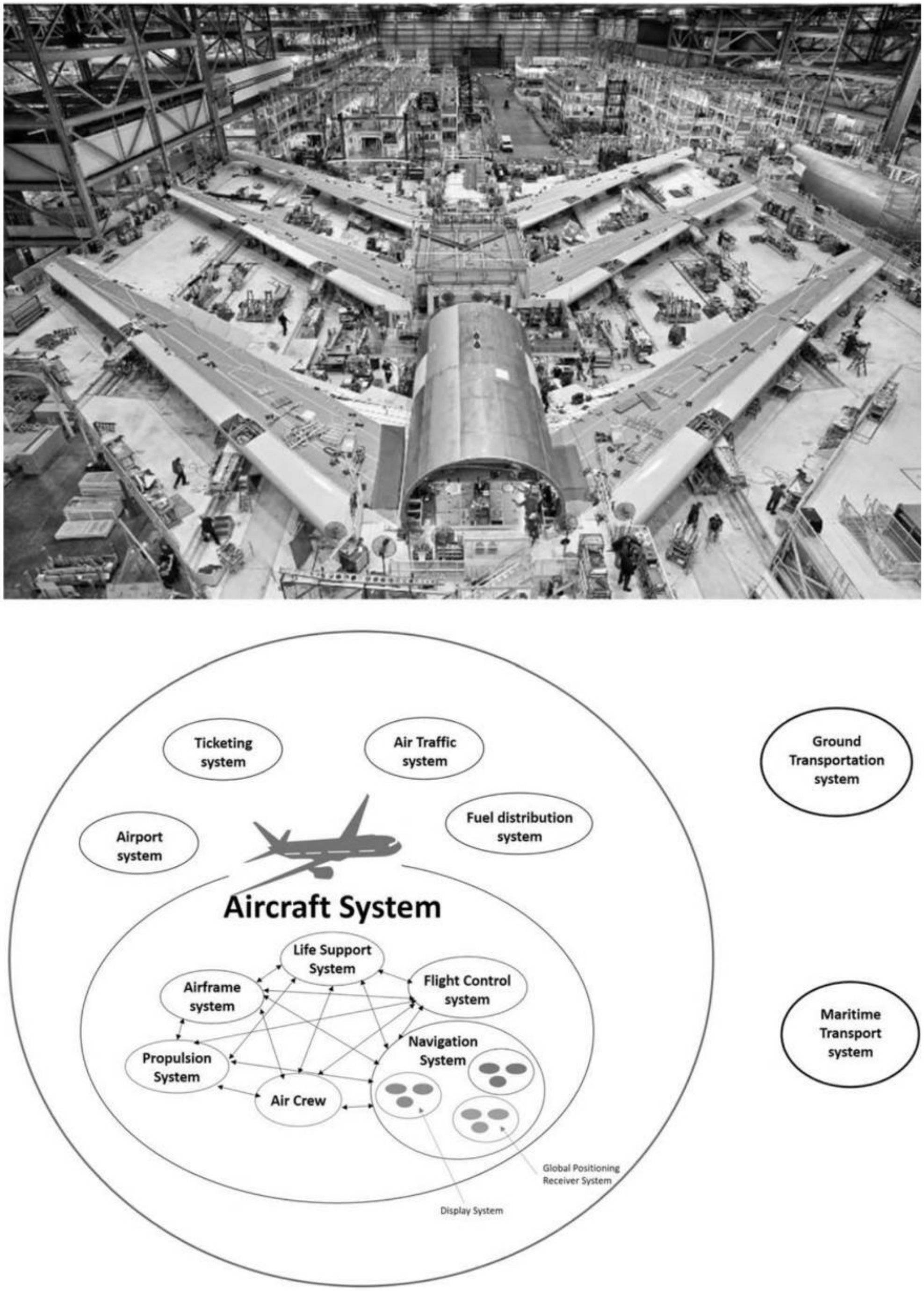


FIGURE 1.31
Air transport system. Example of "System of Systems" in Manufacturing industry.

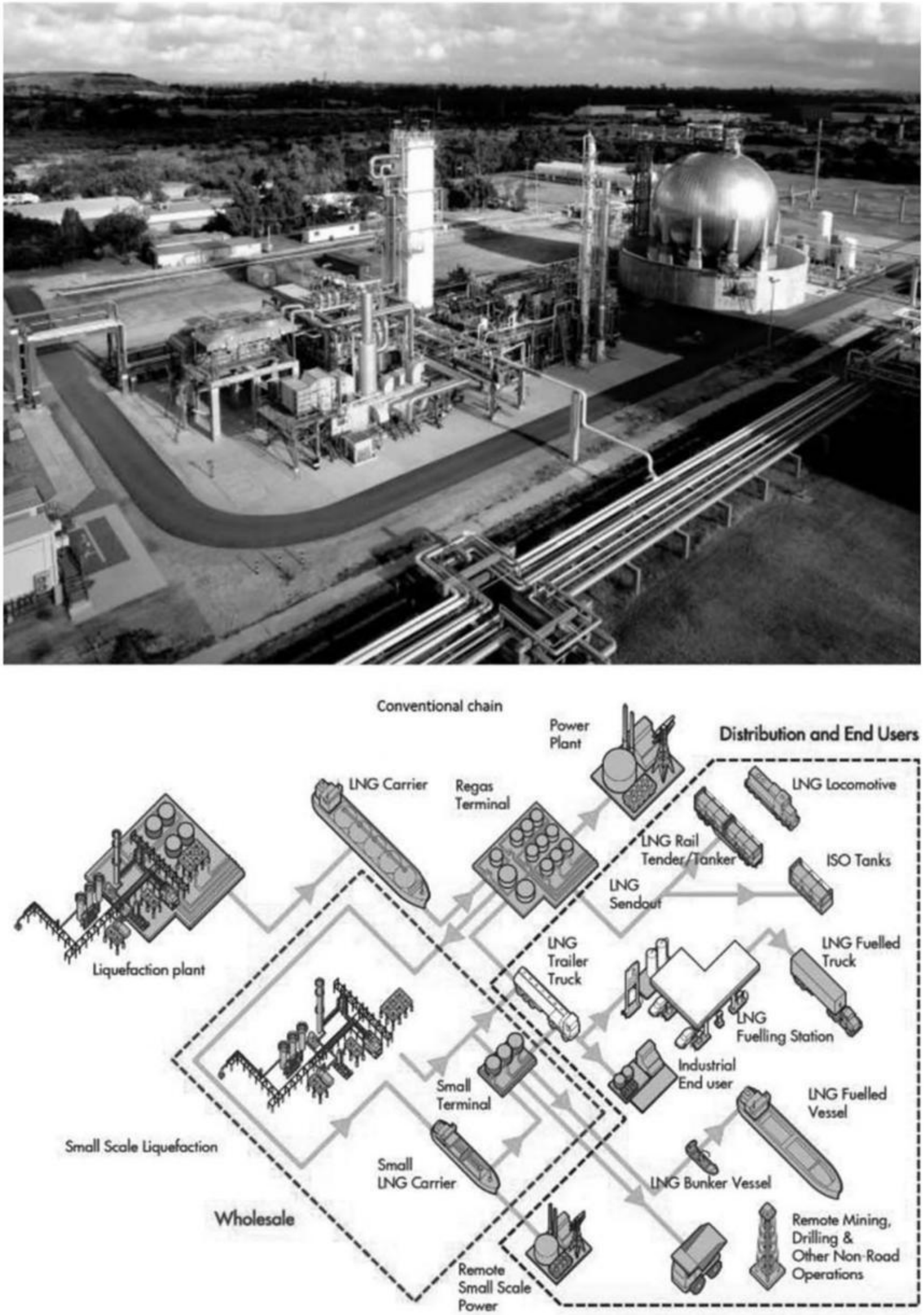


FIGURE 1.32
LNG production & distribution system. Example of the "System of Systems" in Process industry.

process (e.g., tubes of toothpaste, rolls of carpet, buckets of paint, jars of mayonnaise, boxes of cereal).

A better characterization of the difference would be that the number of different part types converges as material flows through an assembly operation, while the product variety increases as material flows through a process operation. Assembly manufacturing starts with a very large number of raw materials and ends with a small number of finished product stock keeping units (SKU), while process operations are the opposite; very few raw materials become highly differentiated as material flows through the process, ending with a large number of finished SKUs. Table 1.3 summarizes the contrast between discrete part assembly manufacturing and process industry.

1.9 APPLICATION OF SYSTEM ENGINEERING IN PROCESS INDUSTRY

Traditional systems engineering was seen as a branch of engineering in the classical sense, that is, as applied only to the *physical systems*, such as spacecraft and aircraft. More recently, systems engineering had evolved to take on a broader meaning especially when *humans* are seen as an essential component of a system. Fig. 1.33 illustrates how the human organizations are embedded in the aircraft and its enabling systems. The other systems are the "enabling systems".

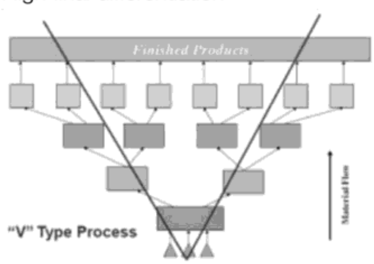
With the introduction of the international standard ISO/IEC 15288 in 2002 the systems engineering discipline was formally recognized as a preferred mechanism to establish an agreement for the creation of products and services to be traded between two enterprises—the acquirer and supplier.

ISO/IEC 15288 considers two specific kinds of systems: *systems-of-interest* and *enabling systems*. There is a relationship between these two kinds of systems. Each system-of-interest has its associated set of enabling systems needed for the system-of-interest to be created, utilized and retired from use during its lifecycle.

Consistent with the broader scope of systems engineering the Systems Engineering Body of Knowledge (SEBoK) has defined three types of systems engineering:

1. *Product systems engineering* is the traditional systems engineering focused on the design of physical systems consisting of hardware and software.
2. *Enterprise systems engineering* pertains to the view of enterprises, that is, organizations or combinations of organizations, as systems.

Table 1.3 Comparison Between Assembly Manufacturing and Process Industry Business Characteristic

Business Characteristic	Assembly Manufacturing	Process Industries
Examples	Automobiles, aircraft, cell phones, computers, power tools, industrial equipment, home appliances	Oil & gas, petrochemical, refineries, chemical, paints, paper & plastic sheet goods, food & beverages, fibers, yarns, carpets, metals & ceramics
Production	Parts or assemblies Bill of material (BOM)	Ingredients, formula, recipe (process bill of materials)
Repetitiveness	Unit	Bulk—ability to adjust batch sizes depending upon available inventory of ingredients/other materials
Parts	The assembly products can be broken down to the parts and reassemble using the repaired parts or new spare parts	In process manufacturing, after a product is produced it cannot then be broken down into its component parts
	An assembly line is a manufacturing process in which interchangeable parts are added to a product in a sequential manner to create an end product	An off-spec product may or may not be processed again
Process flow model	“A” processes Part variety convergence Many raw materials Little final differentiation 	“V” processes Material variety divergence Few raw materials High final differentiation 
Primary economic drivers	Labor productivity Inventory reduction	Asset productivity Inventory reduction Increased throughput Reduced yield losses
Primary rate limiting factor	Labor	Equipment
Tools/ techniques	Value stream mapping 5S Standard work Poka-yoke SMED One-piece flow Cellular manufacturing Production leveling Mixed model production Autonomation Synchronize flow to TAKT Pull systems	Supply chain mapping Value stream mapping 5S Standard Work Poka-yoke SMED Flow determined by equipment size Cellular manufacturing Product wheels Autonomation Synchronize flow to TAKT Pull systems

Continued

Table 1.3 Comparison Between Assembly Manufacturing and Process Industry Business Characteristic *Continued*

Business Characteristic	Assembly Manufacturing	Process Industries
Batch logic influenced by	Machine set-up time Transportation lot size	Batch size by: Vessel size Roll length and width Bale size campaign size by: Changeover time EOQ
Set-up issues	Time to replace, reset tooling	Time to clean out process vessels Time to reset, stabilize temperatures Time for pressures to equillibrate Time to get properties on aim after
Cellular manufacturing implementation	Group technology physical work cells	Group technology virtual cells
Production leveling techniques	Control market demand Mixed model production Heijunka[a]	Product wheels: Batch sequence optimization Batch length optimization Heijunka[a]

[a]*Heijunka (English: Production smoothing or leveling): Heijunka (hi-JUNE-kuh) is a Japanese word for leveling. It is part of the lean methodology of process improvement that helps organizations match unpredictable customer demand patterns and eliminate manufacturing waste by leveling the type and quantity of production output over a fixed period of time.*

3. *Service systems engineering* is about the engineering of service systems. A service system is conceived as serving another system. Most civil infrastructure systems are service systems.

In the process industry the notion of the "product systems engineering" can be ambiguous. The process plant is the final product in the project phase. The EPC contractors shall integrate the physical subsystems and assure the integrity of the overall plant system, as shown in Fig. 1.34.

An empty process plant like an aircraft is made of the dissociable parts and can be considered as a discrete assembly product.

Modularization of the production units reduces the cost of the EPC projects but adds the interfaces which increase the complexity of manufacturing and assembly of the process units.

The advances in technology enable us to realize the very high capacity plants in the tough environmental conditions. These projects are called *megaprojects* and need a significant infrascrture and supply chain configurations. They

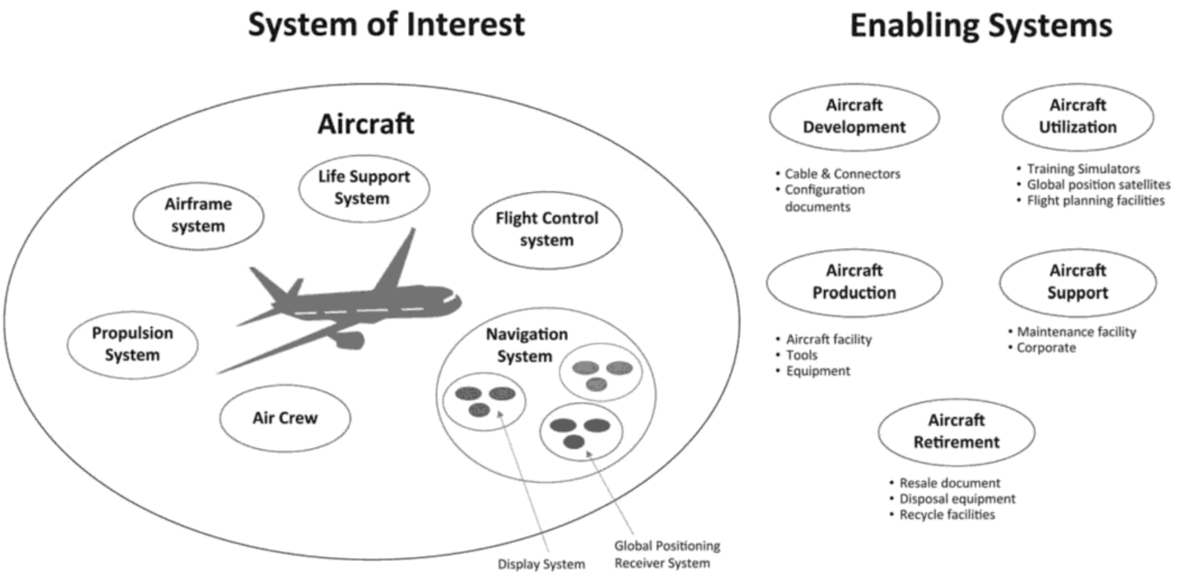


FIGURE 1.33
Example aircraft system-of-interest and its enabling systems. *From: ISO/IEC 15288 in 2002.*

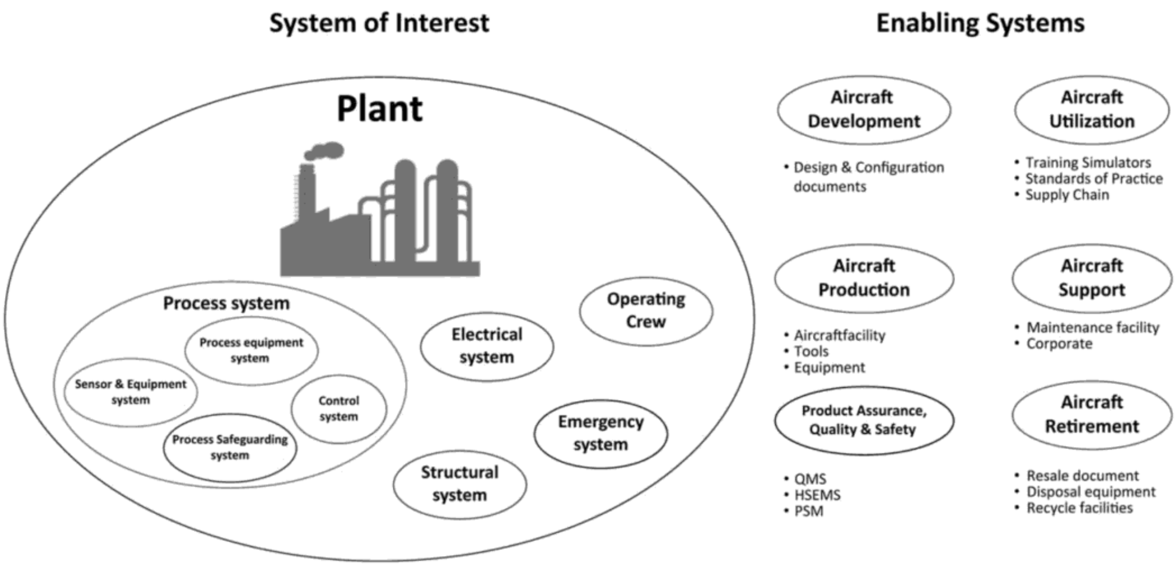


FIGURE 1.34
System-of-interest and its enabling systems for a process plant according to ISO/IEC 15288.

attract a lot of public attention because of substantial impacts on communities, environment, and budgets, and many of them costs more than US$1 billion. In theory the higher capacities mean the lower production costs, but it also means coping with much higher complexity during design and realization of the project.

Ernst & Young published a report in 2014, revealing that almost *two-thirds* (64%) of multibillion-dollar, technically and operationally demanding megaprojects continue to exceed budgets, with three-quarters *(73%)* missing project schedule deadlines. The report "Spotlight on megaprojects" examines the performance of 365 megaprojects and the impact on the oil and gas industry of these overruns (Fig. 1.35).

Modularization and megaprojects increase the need for understanding the complexity management techniques in the system engineering of the process manufacturing plants.

In conventional system engineering, after testing and iteration of the prototype, the new product is industrialized and produced in series (Fig. 1.36).

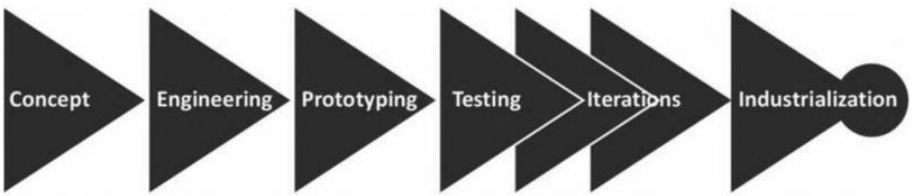


FIGURE 1.35
Lifecycle of a new discrete assembly product.

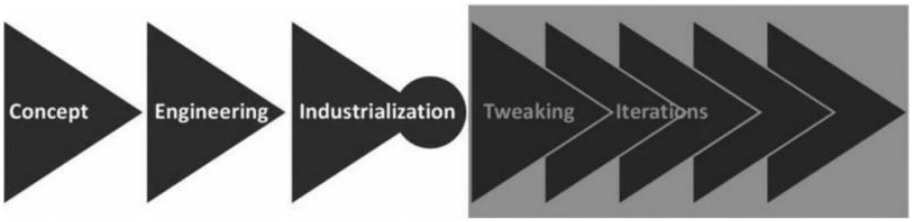


FIGURE 1.36
Lifecycle of a new process plant.

The process plants are the *unique products* because even for similar process licenses when the location, layout, and capacity change, the entire configuration of the facility changes. Therefore industrialization starts soon after the detailed design. Optimization of the plant is performed after industrialization by the "Tweaking and Iterations" of the industrialized process plant (Fig. 1.37).

The consequences of this approach are as follows:

- The costs are unpredictable:
  - Magnitude of deficiencies
  - Number of iterations
  - Standstill time (while upgrading)
- The final results will always be a compromise:
  - Final performance will depend on the initial philosophy of the concept/prototype
  - Depending on the additional costs or investments one is willing to make, the resulting performance will be "as good as it gets."
- The industrialized solution will most probably be conservative, with little innovations.

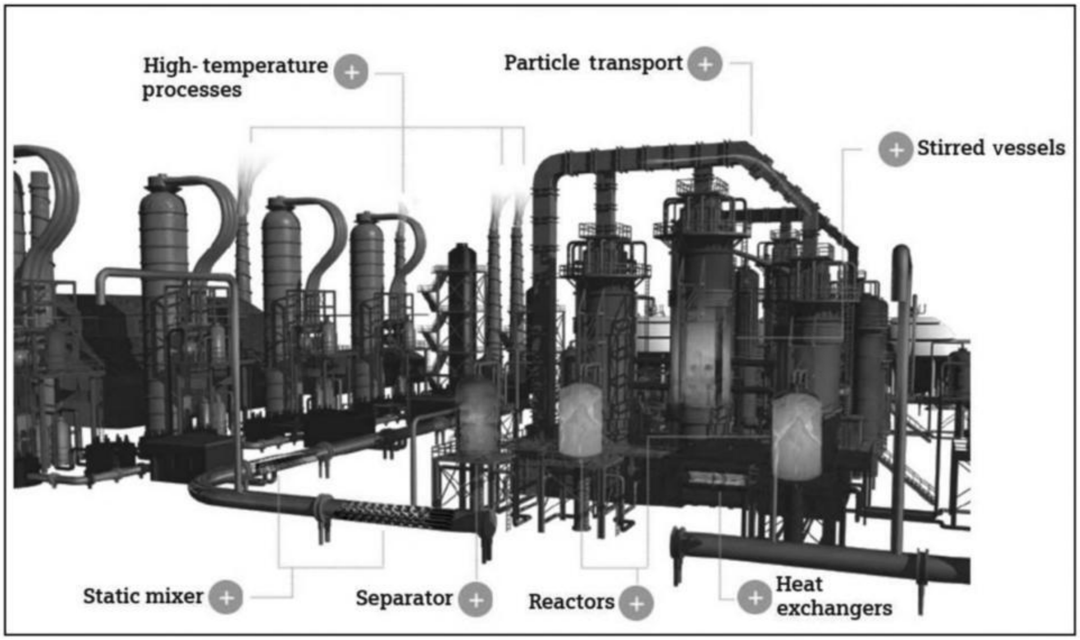


FIGURE 1.37
Virtual prototyping and CFD modeling enables the cost effective "Tweaking & Iteration."

Virtual prototyping and simulation is an effective solution to fulfill the requirements of the process plants for "Tweaking and Iterations" phases. With this approach:

- Concepts and solutions can be new, unknown, risky, and innovative:
  - Big failures are allowed in virtual prototypes
  - Designers can develop up to the limits, and learn from it
  - Crazy ideas are allowed (and might just work)
- The final design will be optimized:
  - Virtual iterations are fast and inexpensive
  - Visualizations (surface plots, flow trajectories, iso-surfaces) give more insight into a design then measurement ever will
  - Use of parameter optimization

Fig. 1.38 compares the virtual prototyping and simulation phases of the process plants with the physical prototyping of a new discrete assembly product. These features for the system engineering of the process manufacturing plants are not covered by ISO/IEC 15288.

"Structural," "electrical," and "emergency response" systems are essential to the integrity and safe functions of the process system. They can be considered as the independent systems, but their failure will lead to the safe or unsafe failures of the "process" functions. For example:

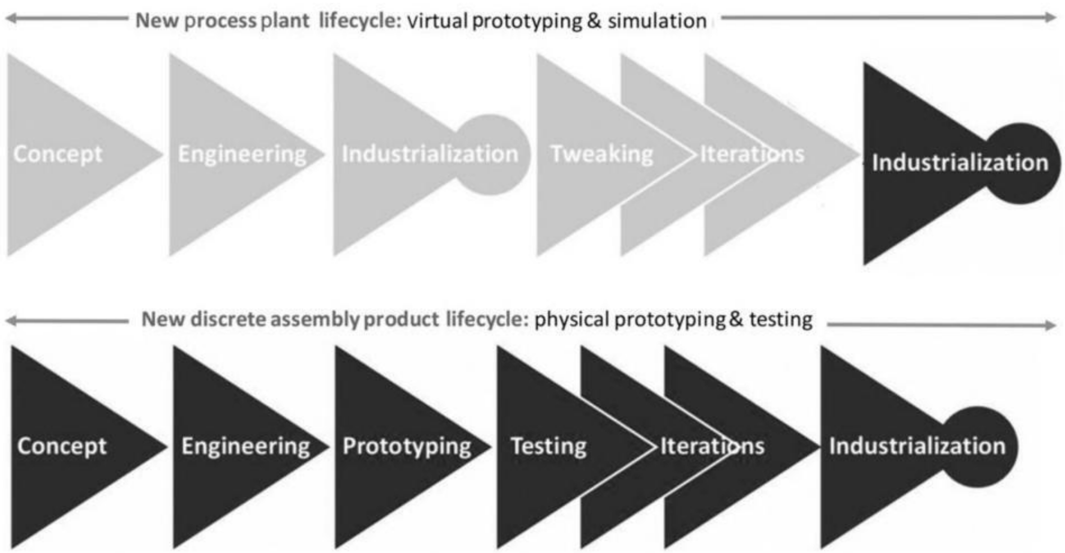


FIGURE 1.38
Comparison of the prototyping solutions of the process and discrete manufacturing plants.

- If the structure of the unit is buckling the pipework system will be under stress and hazardous materials may leak from the pipe flaws or loosen flanges.
- If the electrical system fails all the rotatory equipment will stop, and safe shutdown of the plant will be initiated.
- If there is a fire and emergency firefighting system fails to operate then the fire will escalate, and process equipment may totally be damaged.

The structural and process equipment systems interact continuously. For example, when a relief valve is opened, vessel structures are subjected to vibration, an emergency blowdown cause the cold stress in the equipment and associated pipework, or the land movements may cause the buckling and stress to the process equipment affecting the performance and safety of the unit operation.

Fig. 1.39 illustrates the effects of the internal and external environments on a process column and Fig. 1.40 illustrates the mechanical stress distribution on

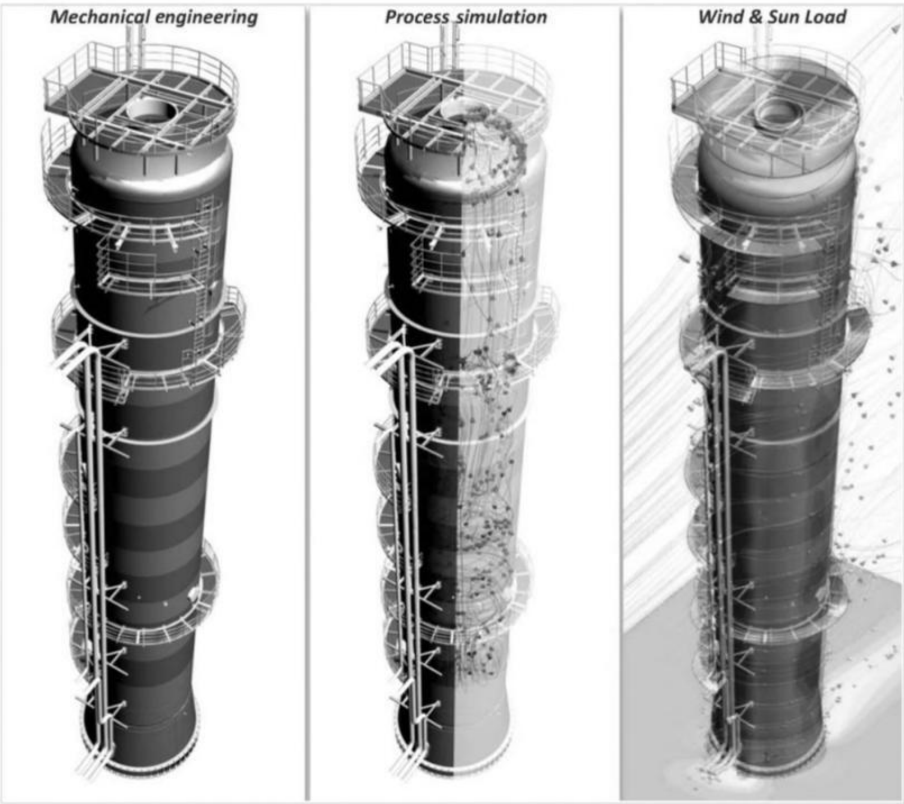
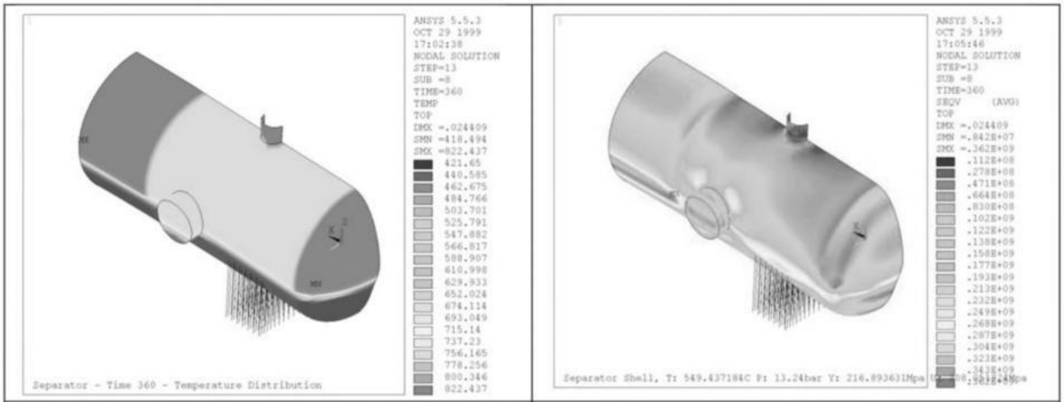


FIGURE 1.39
Internal process materials and natural environment interacts continuously with the mechanical and structural parts of process units.



Temperature distribution at 360 seconds	Von Mises equivalent stress at 360 seconds

FIGURE 1.40
Response of pressurized process vessels and equipment to fire attack.

the surface of a pressure vessel which is attacked by a fire. API 579 provides the guidance for the fitness for service study of these cases.

Fig. 1.41 illustrates the interaction of the process plant systems. Each of these systems has their own lifecycle processes. If there is any changes in the configuration of one of these systems, the effects of this change on the configuration and perforamce of the other systems should be verified to assure the integrity of the whole system.

A perfect plant without the materials in the process equipment serves to nothing. During operation the "process materials streams system" is our primary "system of interest." The other systems are the "enabling systems". The other systems such as process equipment and control systems are the enabling systems. In other words the process flow diagrams such as Fig. 1.42 illustrate how the process related system of interest and its enabling systems are configured.

"Materials in movement" in the process equipment systems are homogeneous and cannot be dissociated into the parts. Their state and conditions are the functions of the upstream and downstream process conditions, i.e., temperature, pressure, etc. Process conditions are controlled by the combination of the human intervention and control systems. If the process conditions exceed the design limits product can be irreversibly damaged.

Sometimes the material components or state phases are in the equilibrium, and the materials system shows the self-regulation characterstics against the process conditions changes. For example, to control a distillation column at least five control loops should be provided. If these control loops are optimized individually,

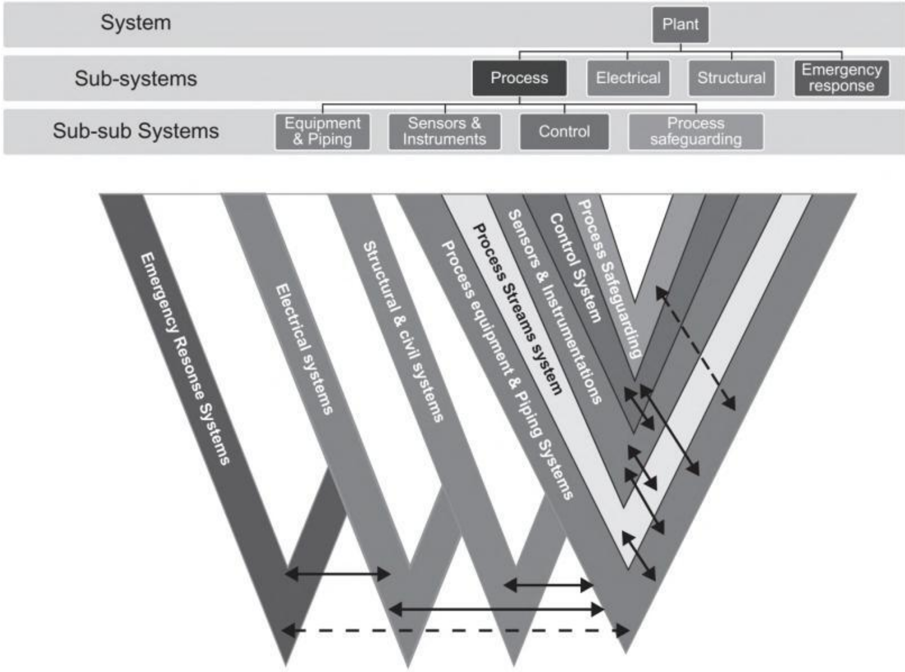


FIGURE 1.41
Process plant subsystems and "vee" diagrams.

it does not mean that the whole distillation column is optimized. Thermodynamic equilibrium creates the dependency between liquid and vapor phases. When one phase is subjected to change, the other phase changes too. This can have the positive or negative effect on the performance of the control system.

Process equipment system contains and provides the necessary conditions for the transformation of the raw materials into the final products. Sensors and control systems interact *continuously* with the process equipment and material systems. "Process safeguarding system" not only protects the "process equipment system" against the undesirable process events but also protects people and the environment against the major accident outcomes. Process safeguarding system like emergency response system is initiated *on demand*.

ISA-95 (IEC/ISO 62264) is an another international standard which has been developed about a decade ago to address the problems encountered during the development of automated interfaces between enterprise and control systems. This standard applies to all industries, and in all sorts of processes, such as batch, continuous, and repetitive or discrete processes.

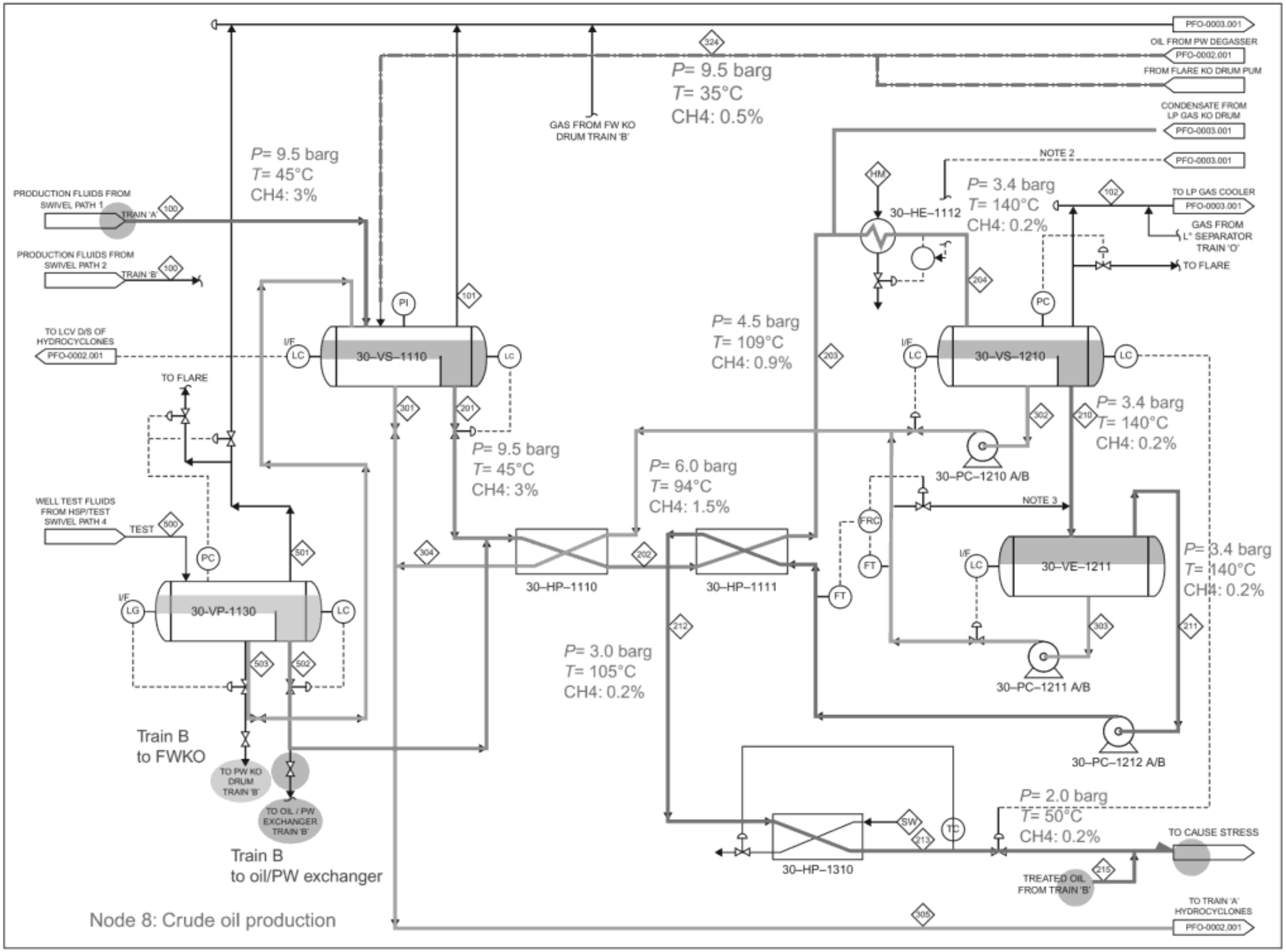


FIGURE 1.42

Transformation of the raw material to products is simulated with process simulators.

ISA-95 distinguishes between the "process equipment" and other "physical asset" systems. This concept has been illustrated in Figs. 1.43 and 1.44.

Physical asset is defined as a tangible, man-made object that has a specific function, normally within a broader system. ISO 55000, focus on the physical asset integrity management system. The management of physical assets and asset systems is inextricably linked to the other categories of assets. The critical interdependencies are illustrated in Fig. 1.45. Although human factors such as leadership, motivation, and culture are not directly addressed within the scope of ISO 55000, they are critical to the successful achievement of optimized and sustainable asset management and require due consideration. This is applicable to the organization's owners, managers, employees, contractors, and suppliers and is considered as the elements of PSM systems (see Fig. 1.20).

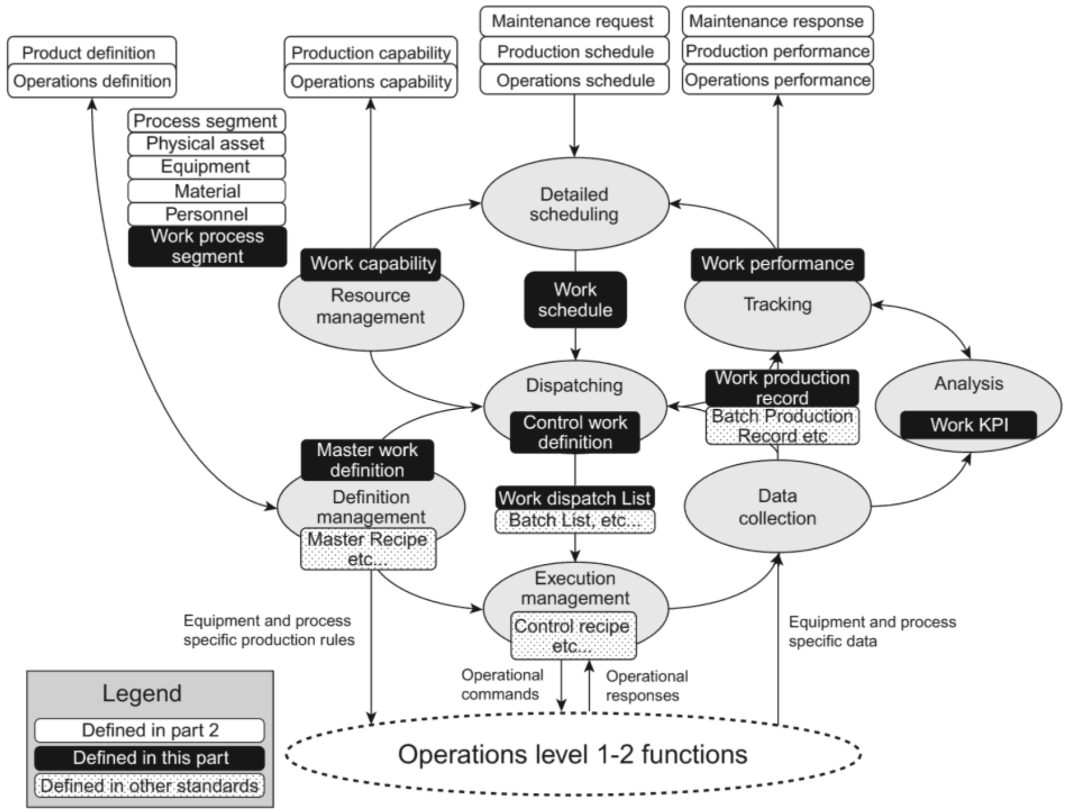


FIGURE 1.43
ISA-95 work information models for operations management.

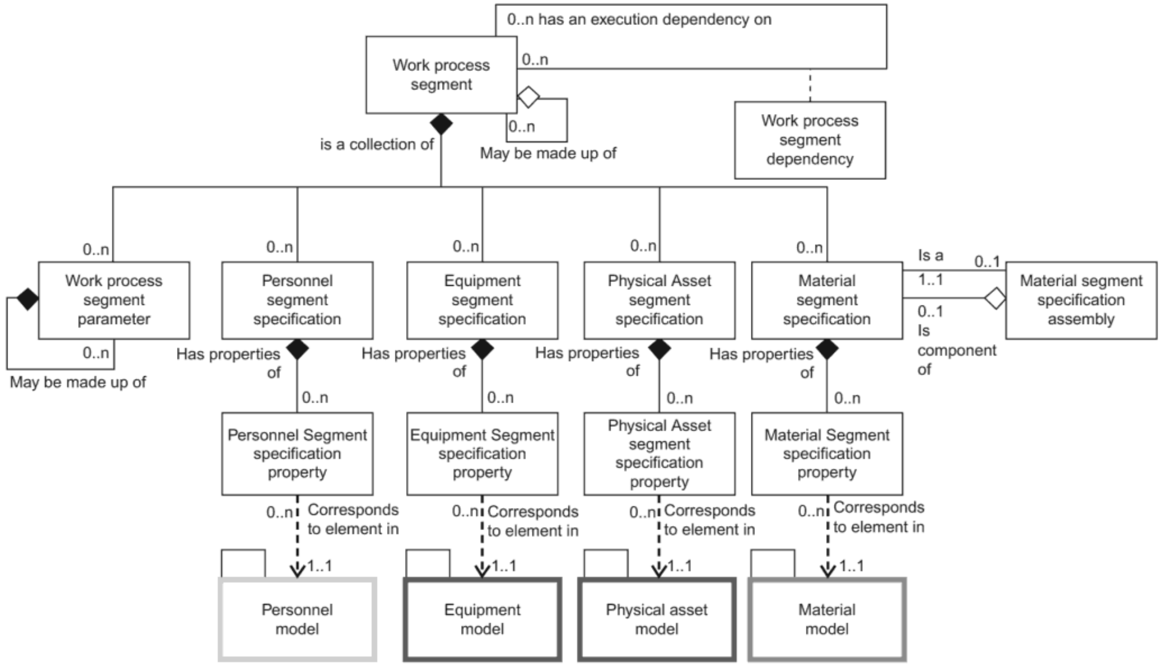


FIGURE 1.44
ISA-95 Work process segment model.

Some of the physical assets are SCEs. These elements shall comply with the regulatory requirements. Fig. 1.46 summarizes how the SCEs are identified and Fig. 1.47 categorizes the SCEs for the oil & gas facilities.

In the process industry the project managers play the "product system engineer" role during EPC phase.

During operation, process engineers play the role of "product system engineer." When the raw materials or capacity change, the process engineers should optimize process system for the new conditions. Process engineer should coordinate with the instrumentation and control engineers to assure the **performance** of the sensors and control enabling systems on one hand and coordinate with Maintenance engineers assure the **integrity** of the physical assets on the other hand.

Plant managers have a few or no degree of freedom to change the plant system. They have double role of "Enterprise System Engineering" at the plant level and "Service System Engineering" in supply chain context.

Quality and HSE assurance systems are among the enabling systems too. They deal with the regulatory requirements and obligations. Fig. 1.48 illustrates the types of the "Systems in Operational Environment."

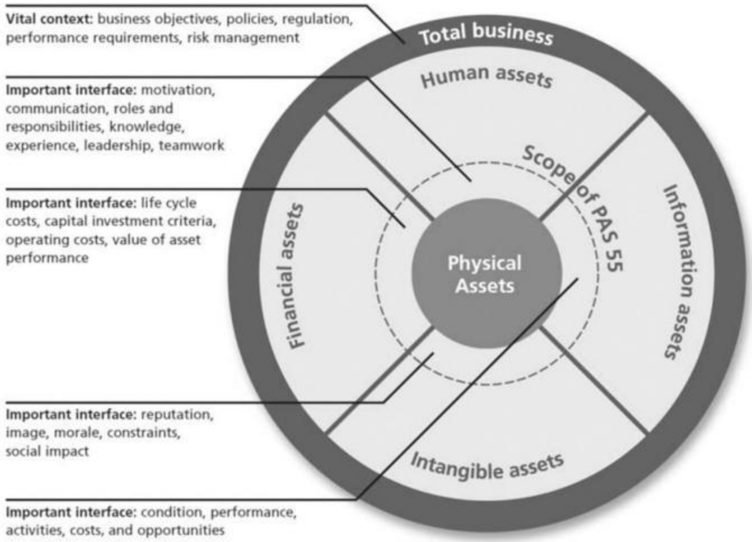


FIGURE 1.45

ISO 55000 Physical assets system in relation to the other categories of assets. *Reproduced with permission from BSI Standards limited (BSI).*

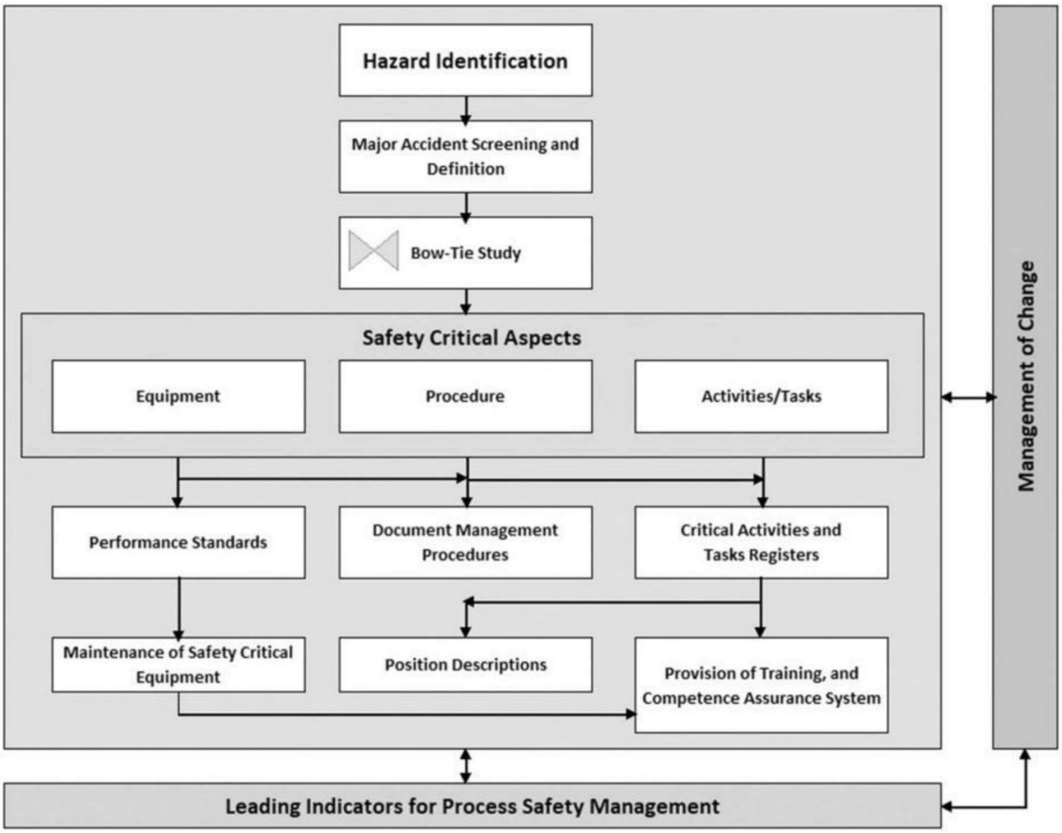


FIGURE 1.46

Safety critical system management. *From: Bow-Tie diagrams in downstream hazard identification and risk assessment.*

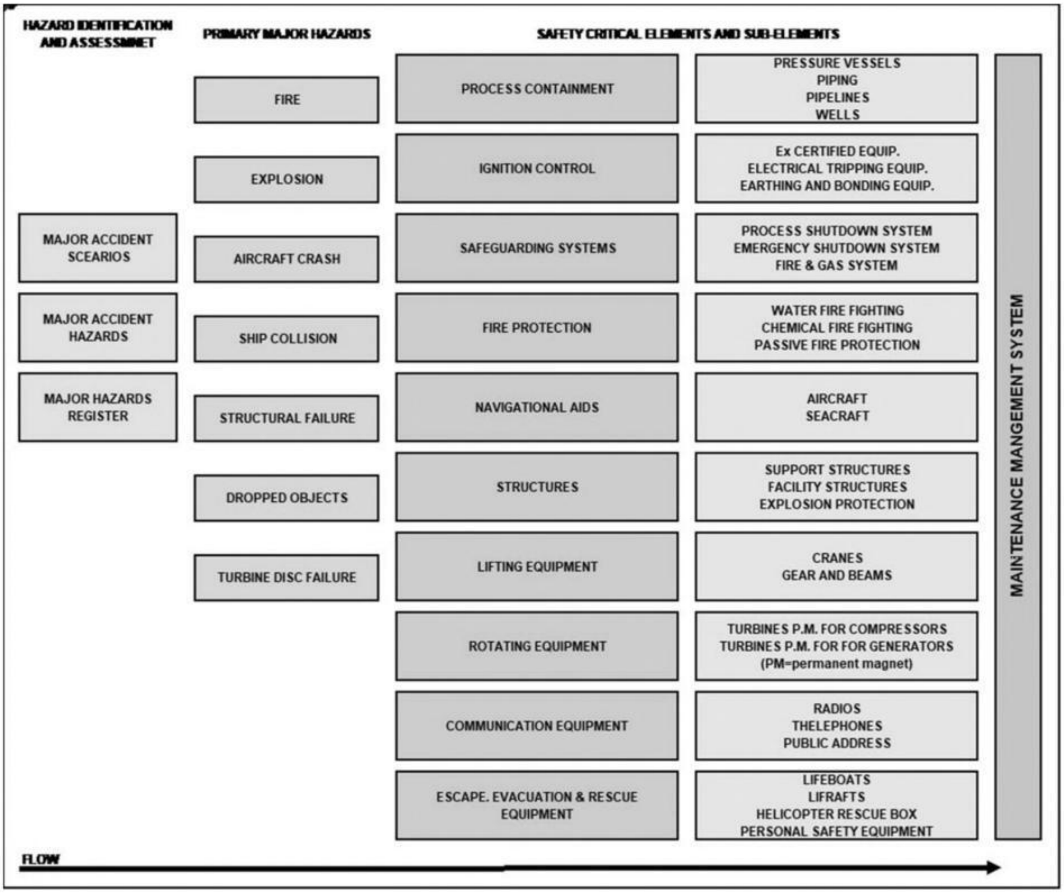


FIGURE 1.47

Safety critical elements for the offshore oil & gas facilities. *From: Energy Institute Guideline (ISBN 978 0 85293 462 3).*

Conclusion: To implement an effective "Process Safety Management System," we should understand that it is not a "Standalone Closed System" but one of the "Systems in Operational Environment" of the production plant which is our main "System of Interest."

1.10 ESSENTIAL SKILLS TO COPE WITH THE CYBER-PHYSICAL SYSTEMS

The 21st century is moving at a tremendous pace with technology taking us places, both personally and professionally, that most of us would not have envisioned 10 years ago. From a manufacturing perspective, these advances

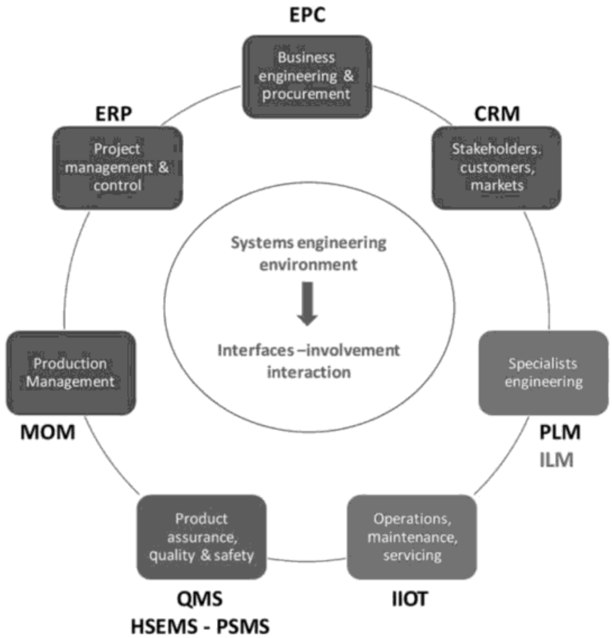


FIGURE 1.48
System engineering environment (Ref. Prof. H. Stoewer). *Inspired from: INCOSE Handbook-2006, Figure 4-1: context of systems engineering technical processes.*

are heralding another industrial revolution which has been named Industry 4.0. Fig. 1.49 summarizes the industrial revolution timeline.

Today, control systems can autonomously operate manufacturing equipment within clearly defined parameters. The transition to the cyber-physical system (CPS) is fluid because the lines between the virtual, digital, and real worlds are disappearing before our very eyes. A CPS responds to changes; it can digitally process tasks in a split second, and it can convert the inputs into commands.

The traditional manufacturing world is converging with the digital manufacturing world to enable organizations to digitally plan and project the entire lifecycle of products and production facilities. This approach offers tremendous benefits to the manufacturing processes, with significant cost benefits and robust growth.

The IIoT is everywhere now and connect millions of devices, machines, sensors, and systems throughout the world. The collaborative interfaces and successive break-up of the traditional automation pyramid and substitution with networked, decentralized, or partially self-organizing services are the great opportunities for improving the quality and safety management system frameworks. Fig. 1.50 lustrates the evolution of the traditional automation pyramid to the decentralized or partially self-organizing services.

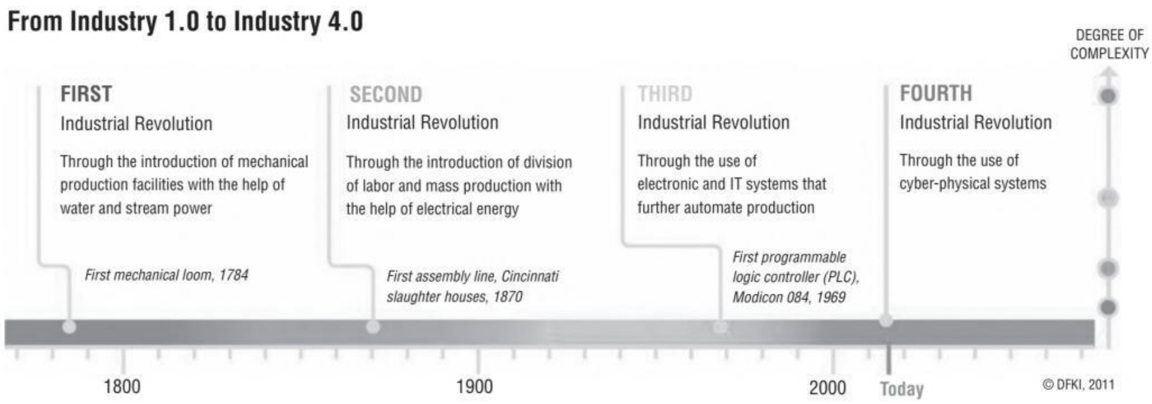


FIGURE 1.49
Industrial revolution timeline.

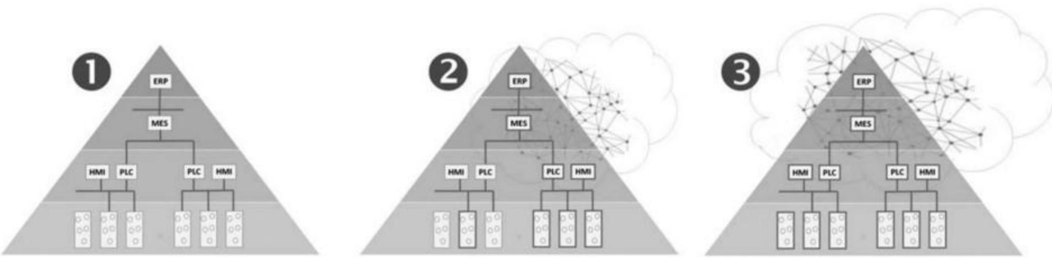


FIGURE 1.50
Evolution of the traditional automation pyramid to the decentralized or partially self-organizing services. *From: http://www.dlg.org/fileadmin/downloads/food/Expertenwissen/e_2015_5_Expertenwissen.pdf.*

A decentralized, self-organizing system can respond independently and adeptly to unexpected events. The result is the resilient factory—one that is error-tolerant, agile, and able to learn.

With these available advanced technologies, dream of the integrators for implementation of an effective and easy to use integrated management systems can become a reality. Integration of the management systems which can be achieved only if the following notions are fully understood and democratized throughout the organizations:

- *System engineering* is an *interdisciplinary* field of engineering that focuses on how to design and manage complex engineering systems over their *lifecycles*. Issues such as requirements engineering, reliability, logistics, coordination of different teams, testing and evaluation, maintainability, and many other disciplines necessary for successful system development, design, implementation, and ultimate decommission become more difficult when dealing with large or complex projects.

- *System thinking* is a way of thinking about, and a language for describing and understanding, the forces and interrelationships that shape the behavior of systems. This discipline helps us to see how to change systems more effectively and to act more in tune with the natural processes of the natural and economic world.
- *Complexity thinking*: Russell L. Ackoff quoted: "Problems that arise in organizations are almost always the product of interactions of parts, never the action of a single part. Complex problems do not have simple solutions. The search for simple –if not simpleminded– solutions to complex problems is a consequence of the inability to deal effectively with complexity."
- *Risk thinking*: Risk awareness is growing among quality and HSE managers. They recognize that risk is not limited to negative possibilities. Companies can also use risk-based thinking to pinpoint opportunities, which represent the positive side of risk. The "Plan-Do-Check-Act (PDCA) cycle" is the link between the operational excellence and risk management and can assure the effective process improvement.
- In the context of ISO 9001:2015, *risk-based thinking* replaces what was called the preventive action in the previous standard version. ISO's risk-based thinking requirements center on incorporating risk into decision-making, without exactly formalizing how to do it. Areas, where risk appears in the new standard requirements, include organizational context, leadership, planning, operation, performance evaluation, improvement.
- *Risk management* is the identification, assessment, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives) followed by coordinated and economical application of resources to minimize, monitor, control the probability, and impact of unfortunate events or to maximize the realization of opportunities. Risk management's objective is to assure uncertainty does not deflect the endeavor from the business goals.
- *Resilience engineering* is a new way of thinking about safety.

  The traditional view of safety (known as "Safety I") is to prevent things from going wrong. However, the new view ("Safety II") is that safety is the ability to succeed under varying conditions. Resilience engineering aims to increase the number of things that go right, rather than to reduce the number of things that go wrong.
- It is concerned with building systems that are resilient to change. By analyzing what goes right, resilience engineering attempts to understand normal performance, so that work can be made better and safer.

- Success has been ascribed to the ability of groups, individuals, and organizations to anticipate the changing shape of risk before damage occurs; failure is simply the temporary or permanent absence of that.
- IT, OT, ET integration: Technology now makes the integration of "Engineering," "Operational," and "Information" technologies possible. Successful integration enables the companies to break down barriers between horizontal and vertical lifecycle departments, phases of business, and chain values.
- *Big data management*: Collecting more and more data without processing them to knowledge present no value. Today's OMS captures more data than ever, allowing companies to leverage sophisticated reporting and business intelligence.

With these skills and using the right tools the user-friendly and easy to use workflows and applications can be designed. Then, all workforce of business can be involved and contribute in the design and application of the operational excellence.

The new versions of ISO 9001, ISO 14001, and ISO 45001 and ISA-95 provide the guidance to achieve this goal.

1.11 WHY DOES COMPLEXITY MATTER?

Enterprise systems are inherently complex, often involving many business processes, people, and organizations across a company. Given this built-in complexity, it is no surprise that failures abound; it is amazing these systems function at all. Fig. 1.51 illustrates the complexity of a production plant which is a "system of the systems" operated by the "team of the teams" with the "organisation of the organisations."

Systems engineering deals with work-processes, optimization methods, and risk management tools in such projects. It ensures that all possible aspects of a project or system are considered, and integrated into a whole.

Fig. 1.52 illustrates the system fundamentals and elements of the engineered systems. A process plant consists of many closed and open systems which interact with other systems in a shared environment affected by the behaviors, properties, and functions characterized by *emergence* and *complexity*.

An open system is defined by the interactions between system elements within a system boundary and by the interaction between system elements and other systems within an environment. Closed systems have no interactions with their surrounding environment.

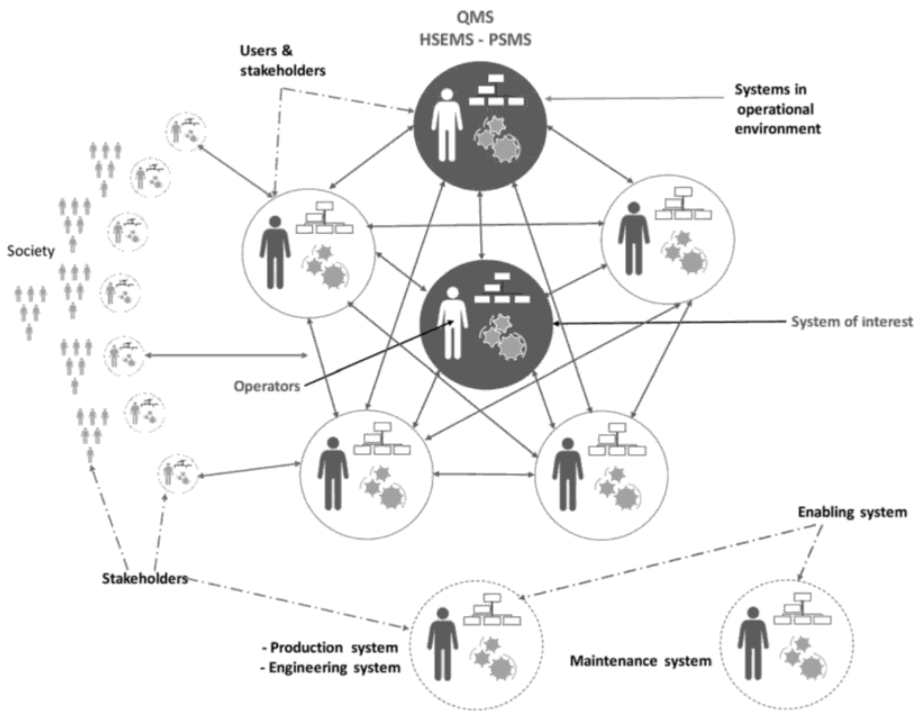


FIGURE 1.51
Requirements elicitation captures the needs of stakeholders, operators, and users across systems boundaries (INCOSE 2002).

Emergence is a consequence of the fundamental system concepts of *holism* and *interaction*. System wholes have behaviors and properties arising from the organization of their elements and their relationships, which only become apparent when the system is placed in different *environments*.

The stem of the word *complexity*, i.e., *Complex* is composed of the Latin words *com* (meaning: "together") and *plex* (meaning: woven). This concept is different from *Complicated* where *plic* (meaning: folded) refers to many layers. A *complex* system is thereby characterized by its interdependencies, where as a *complicated* system is characterized by its layers.

Neil Johnson states that "even among scientists, there is no unique definition of complexity — and the scientific notion has traditionally been conveyed using particular examples..." Ultimately he adopts the definition of "complexity science" as "*the study of the phenomena which emerge from a collection of interacting objects*."

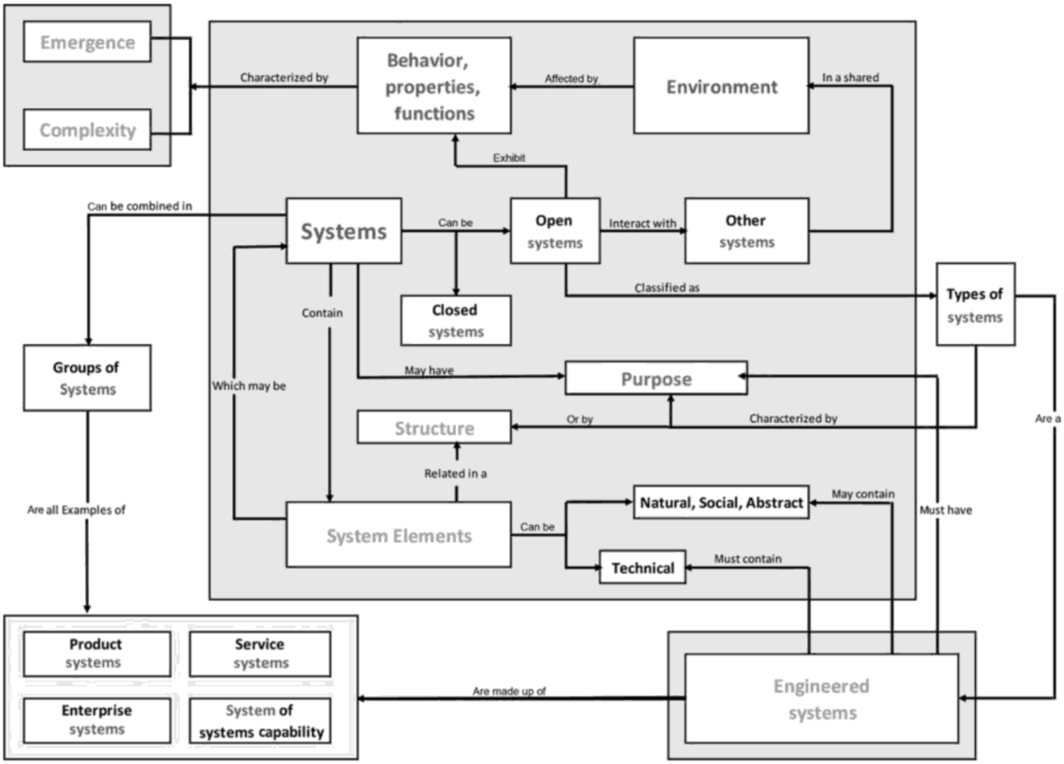


FIGURE 1.52

System fundamentals and engineered systems (SEBoK v.01).

Emergence and complexity concepts represent many of the challenges which drive the need for *systems thinking* and an appreciation of systems science in system engineering.

Russell L. Ackoff quoted: "Problems that arise in organisations are almost always the product of interactions of parts, never the action of a single part. Complex problems do not have simple solutions. The search for simple –if not simpleminded– solutions to complex problems is a consequence of the inability to deal effectively with complexity."

Complexity is an attribute of the *technical system* being developed but also of the problem space (including *people* and *organizations*), and the *environment*. Complexity is associated with the *number of parts, diversity, dynamism* and with *emergence*. It is a challenge to systems engineers not to *over-simplify* in pursuit of representations and capabilities that can be understood and controlled; the right level of complexity is essential.

Although the meaning of complexity varies from "confusion" to "measurable characteristics" of technical systems, it is most useful to systems engineers to identify characteristics that can be resolved and whose resolution will improve the development and operation of modern systems. Complex systems engineering requires both a shift in thinking and an expanded set of tools and techniques.

Discrete high-tech and hazardous manufacturing such as space, aeronautics, railway, and automotive projects define clearly their complexity assessment and management tools and techniques in the deliverables of their projects and operation.

Application of the complexity assessment and management are not explicit and straight forward in the process manufacturing such as oil & gas, petrochemical, and chemical industries. The nuclear industry is an exception and very often inspired the other process industry sectors. Also the manufacturers of the specialized packages such as compressors, gas turbines, and subsea equipment may apply the complexity science in design and operation of their products. However, these closed systems are only a few parts of the entire plant open system.

System engineering, system thinking, and complexity thinking skills are essential to design and operate an effective PSM system. To guarantee success, not only the HSE practitioners but also everybody in the managerial and operational teams should be trained for these skills and apply them in their day to days tasks and decision makings.

The Cynefine framework is a quick and easy technique for complexity assessment and management of a given context. It can be combined with any qualitative decision making or risk-based activity such as HAZID, HAZOP, JHA, PTW, MOC, etc.

Cynefin framework is divided into five domains: obvious (*simple*), complicated, complex, chaotic, and disorder. This framework strives to make sense of the prevailing environment. It distinguishes the decision-making models in two groups: "categorization models" and "sense-making models". In a categorization model the framework precedes the data. In a sense-making model the data precedes the framework.

Fig. 1.53 summarizes how Cynefin framework is applied for the complexity assessment of the self-determined learning processes. From this assessment, we understand that procedural "learn then work" is not effective if we intend to promote the creativity and innovation in a particular activity. On the other hand, giving the possibility of "working to learn" will increase the risk of failures and business interruptions. The company should make sure that everything is in place to be "safe to fail."

This book aims to raise the awareness process manufacturing personnel and consultants to the importance of the system engineering, system thinking,

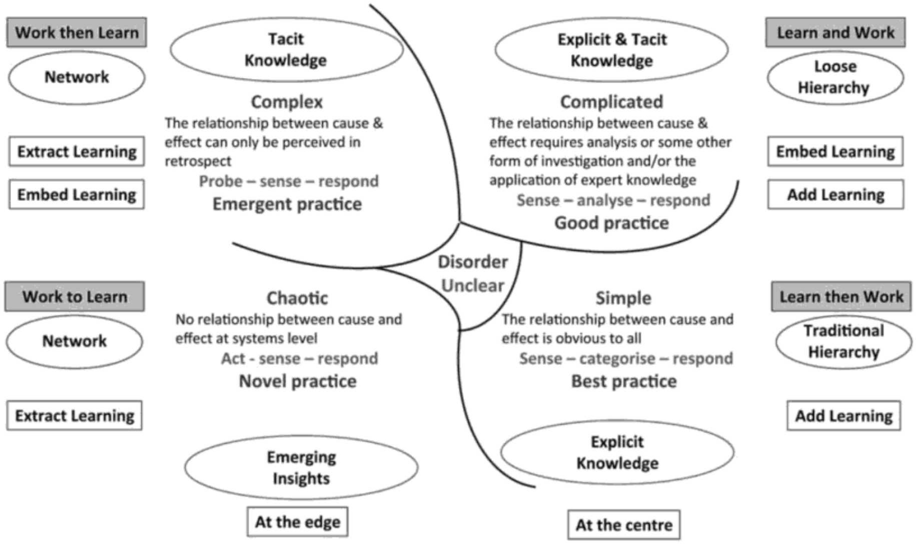


FIGURE 1.53
Cynefin framework for self-determined learning complexity level assessment. *From: http://colabria.com/heutagogy/.*

and complexity thinking in the implementation of their OMS. Without these skills a thorough risk assessment is not achievable. We will scrutinize the complexity issues associated with the PSM to provide the insights to the HSE practitioners to choose the optimal approach for implementation of PSM in their organization.

1.12 BARRIER THINKING & COMPLEXITY

As an example, let us assess the causes the relief valve (PRV) failure and the impact of this failure on a gas release incident (Fig. 1.7). In a thorough bow-tie, all the technical, organizational and human causes and safety barriers during the lifecycle of PRV should be considered.

None of the safety barriers is 100% effective. The reliability of a safety barrier can be increased by different techniques such as intrinsically safer systems, redundancy, shorter time of the test, etc. can be used to increase the integrity level of the individual safety barriers. The bow-ties of Fig. 1.54 illustrates the relationship of the preventive and mitigation measure for the individual top events such as “Gas Release,” “Overpressure,” “PRV failure,” “Design Failure,” etc.

In Fig. 1.55 we have considered only one of the safety barriers of in each bow-tie of Fig. 1.54 and related them to each other. We assumed that the barriers are 100% independent and neglected the common cause failures.

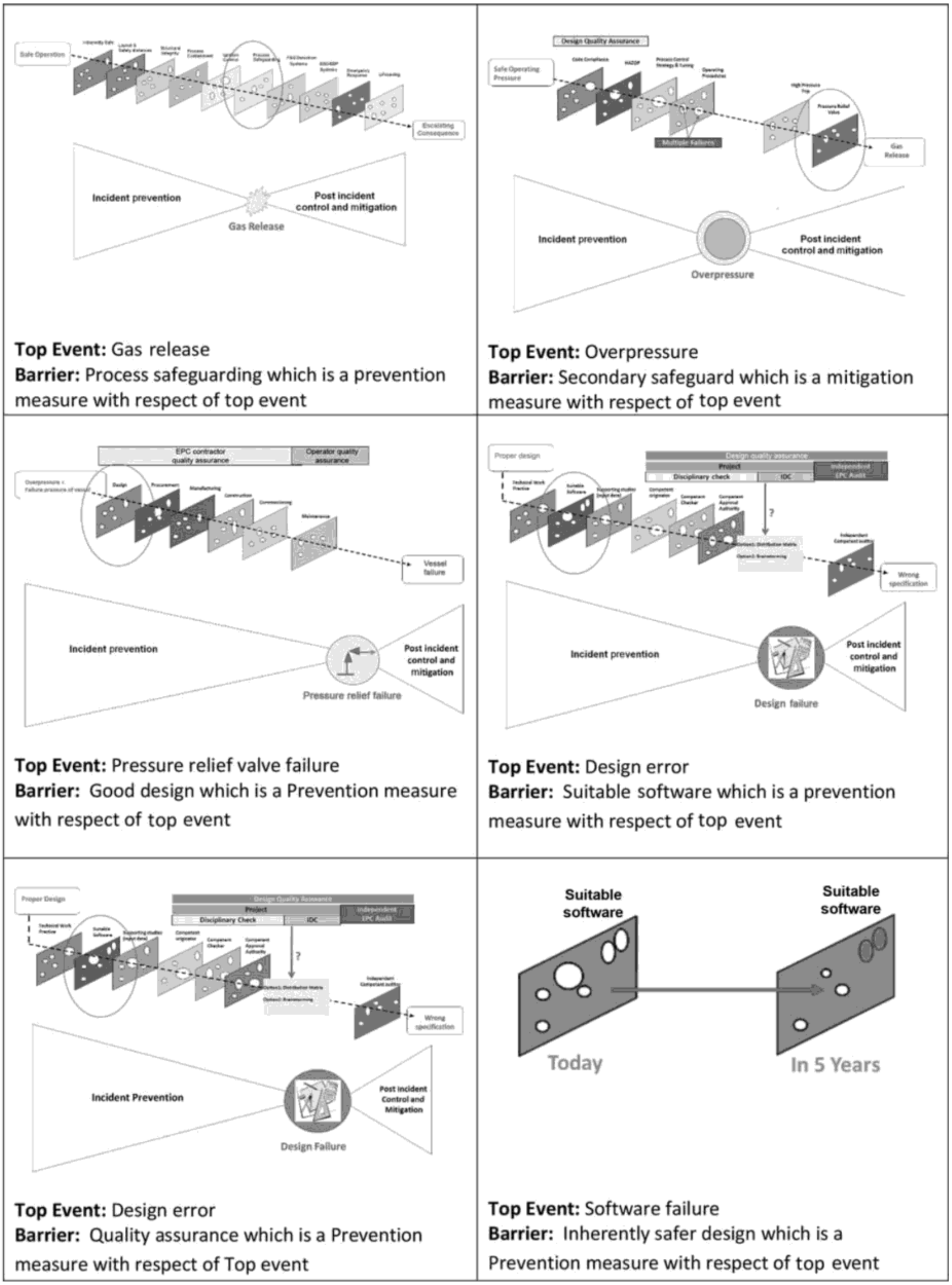


FIGURE 1.54
PRV bow-tie assessment.

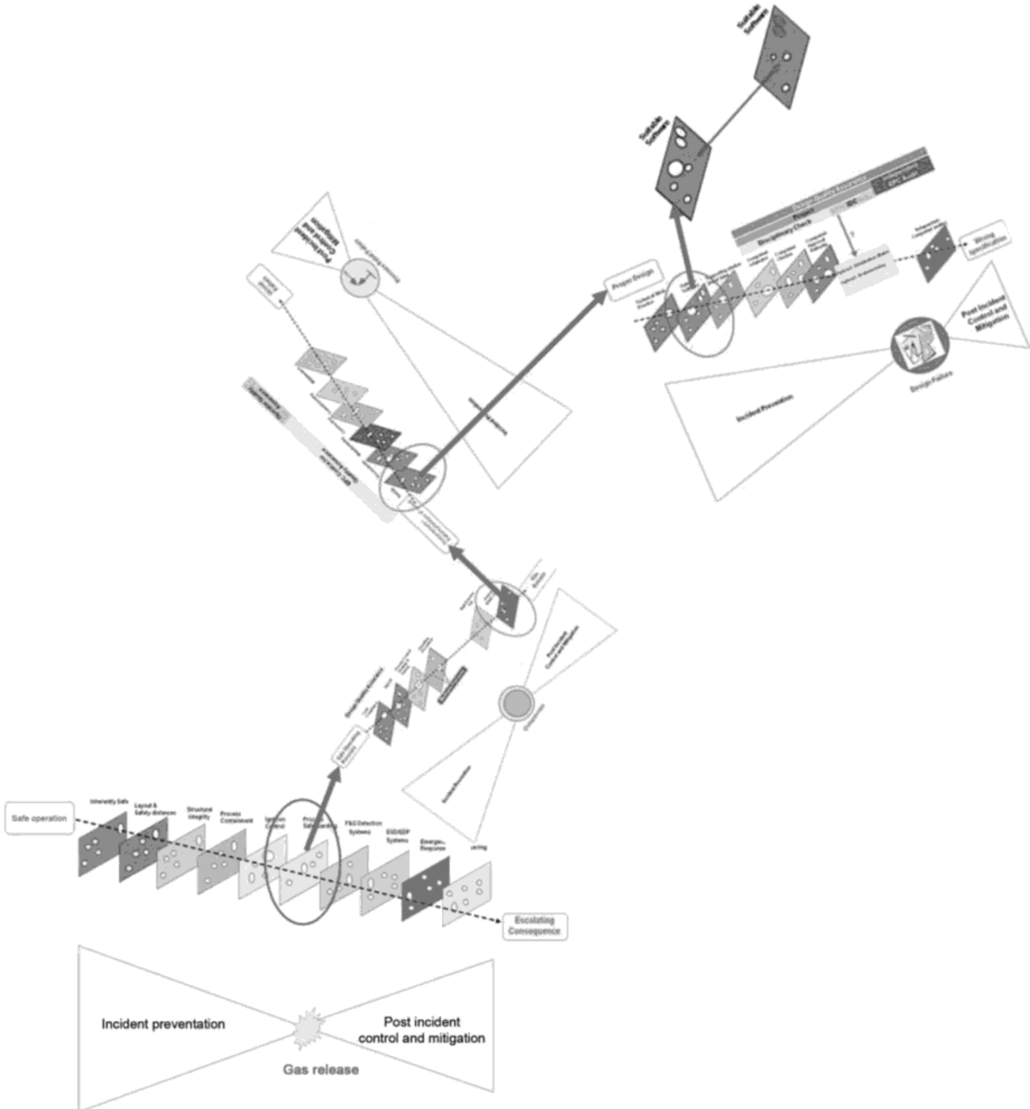


FIGURE 1.55
Combined bow-ties for PRV failure assessment.

For the real systems which all the barriers should be scrutinized to the sub-layers up to individual element, the combined bow-tie and Swiss cheese model can become complex very quickly (Fig. 1.55).

Considering all these facts take us to believe that a realistic bow-tie assessment looks more like a Croissant with interrelated *resilient*, random, and

FIGURE 1.56
The safety critical elements are not always independence. A croissant in its whole is much better representative the system of the safety critical elements in a real plant.

enclosed hollow spaces rather than the rigid sliced Swiss cheese with perfect and independent holes.

No matter how and the croissant is made or subjected to the shocks the croissant will be acceptable as far as the composition and texture of pastry substance, as well as the number and configuration of the holes, remain at defined range (Fig. 1.56).

In a real production facility the combination of technical, organizational and human factors assures the ability to perform in a resilient manner.

1.13 CHANGE MANAGEMENT & COMPLEXITY

The world that enterprise lives in it is anything but static. Technology and people change continuously and cause the constant moving of the things around all the time. Enterprise management system should continually cope with both shallow and deep conflicts between the designed features and the reality. ISO 10007 for configuration management aims to provide the guidance to minimize the risk of the gap between design requirements and the reality of the plant (Fig. 1.57).

The novel conditions are common, and things that we have not seen before do occur relatively frequently. Therefore lots of out of the box adapting and tailoring activities are required to make systems working.

In 2002 the McKinsey Quarterly study of 40 companies found that 58% of change initiatives failed to reach their goals. We need to understand how organizations work before we can effectively change them (Fig. 1.58).

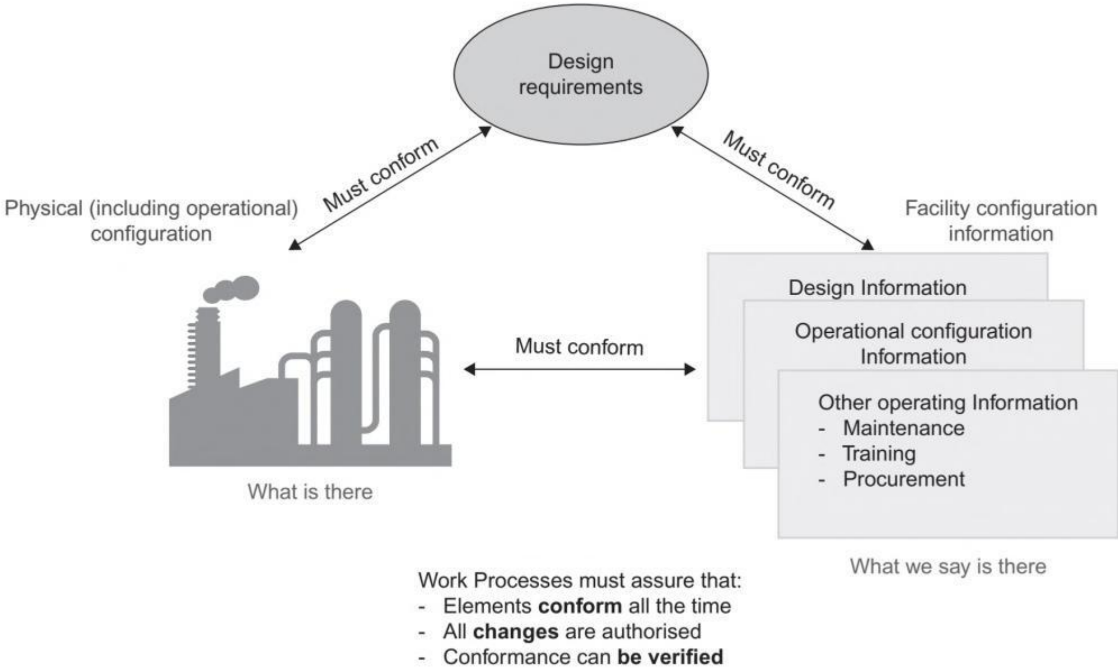


FIGURE 1.57

Relationship among design requirements, documentation, and physical configuration. *Inspired from: Configuration management in nuclear power plants.*

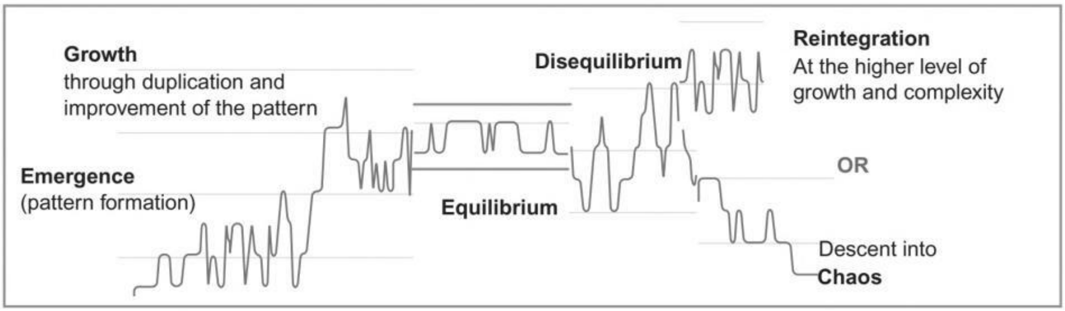


FIGURE 1.58

Change cycle. *Inspired from: complex adaptive systems theory-12613245196525-phpapp02.*

Change is only made possible by people who by their very nature are complex, unpredictable, dynamic, and resistant to engineering. Organizations depend on people. Therefore to improve operational systems we should understand the complexity of people individually and organization environment.

The definition of insanity is *"doing the same thing twice and expecting a different result,"* but this simple wisdom rule does not apply to the complex environment in which, *"doing the same thing twice* will *give a different result."*

Also, we always say that *"You can't fix what you can't measure"* but *"You* can *intervene in a complex environment, even though you* can't *measure it reliably."*

Complexity is an attribute of the *technical system* being developed but also of the problem space (including *people* and *organizations*), and the *environment*. Complexity is associated with *size, diversity, dynamism* and with *emergence*. It is a challenge to systems engineers not to *over-simplify* in pursuit of representations and capabilities that can be understood and controlled; the right level of complexity is essential.

OMS including the PSM are complex by their very nature. They encompass a great number of diverse and dynamic technical, organizational, and people simultaneously. Over simplification of the monitoring and control of them to the check list-based audits and gap analysis of the sample cases will lead unsatisfactory results and inappropriate prioritization and decision making.

1.14 COMPLEXITY AND DECISION MAKING AND COMPLEXITY

In the context of ISO 9001:2015, *risk-based thinking* replaces what was called the preventive action in the previous standard version. ISO's risk-based thinking requirements center on incorporating risk into decision-making, without exactly formalizing how to do it. Areas, where risk appears in the new standard requirements, include organizational context, leadership, planning, operation, performance evaluation, and improvement.

Fig. 1.59 from ISO 31000 illustrates the risk management steps. The trouble with the conventional risk assessment approach is that we do not just "find" causes; we tend to "create" them, and when none can be found, we use the "act of God" opt-out clause. This approach is a social process, which changes over time just as thinking and society change: from the end of the Second World War until the late 1970s, most accidents were perceived as a result of *technical failure*. The Three Mile Island accident (March 1979) saw the emphasis begin to shift from technical to *human failure*. With the challenger disaster in 1986 the cause identified was not solely technical or human but *organizational failure*.

There is a "cliff" between the ordered domains (including obvious and complicated) and chaos. Chaos may result from either deliberate unethical behavior or failure to recognize complicated or complex situations. In the latter cause, complacency may cause one to over-simplify and misinterpret a problem causing an already complicated situation to become chaotic. Once one falls into chaos, it is difficult to recover. Therefore decision maker should manage in the complicated and complex spaces to avoid the cliff (Fig. 1.60).

Complex and chaotic contexts unordered: "there is no immediate apparent relationship between cause and effect." A complex context as a place where "cause and effect are only obvious in hindsight, with unpredictable emergent outcomes."

Making decisions in a complex context calls for leaders to probe, sense, and respond in order to discover an emergent practice. Of these three actions the key to success in a complex context is effective probing. Probing is considered as conducting "safe-to-fail experiments" (not fail-safe experiments). If a solution does not work, leaders should get rid of it. If it succeeds, they should amplify it.

Table 1.4 summarize the Cynefin framework for decision making of the leaders. Consultants should help the leaders to determine the complexity level of their context and then set the effective strategy to achieve the required results.

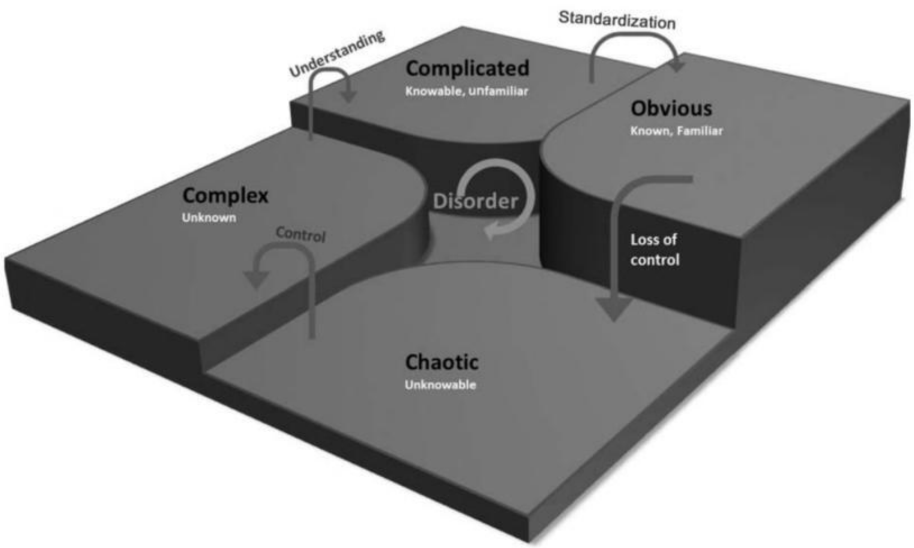


FIGURE 1.60
Cynefin frame work domain.

In our experience, it's possible to standardize at least one-third of all modules or submodules for even the most complex equipment. For some types of projects (e.g., those with little variation), it's possible to standardize up to two-thirds. The frequency of use, complexity, and nature of the module will determine the appropriate level of standardization; decisions must be driven by a clear business case on a module-by-module basis. At the same time, the benefits from modularization increase with the scale of a company's portfolio: the more units, the greater the impact on a company's bottom line.

There are a few smaller plants where complete plant-level standardization is possible—e.g., the standardized "monotower" unmanned platforms used for gas production in the North Sea. For a floating production, storage, and offloading vessel, the oil and gas processing module can use a standard design template, but it must be scaled to the oil and gas flow characteristics of the particular well. However, the power and compression module can be standardized because the same design and equipment can be reused on many vessels. For larger plants, such as offshore platforms or liquefied natural gas (LNG) plants, the focus moves to replicating modules that make up the plant, such as helicopter-landing pads on platforms or compressor trains in LNG plants.

While it is believed that modularization and standardization can provide major benefits to the oil and gas industries, two issues have proven to be stumbling blocks:

- First, companies must overcome the natural reflex among many project managers: to think that their projects are *unique* and therefore resistant to common approaches.
- Second, companies often fail to *convince* project-design engineers that standardization brings benefits that more than compensate for limited design choice.

Organization changes in four areas can help resolve these issues:

1. *In engineering and design activities*, companies that have successfully embraced modular standardization employ common design specifications and guidelines for each project type (e.g., refinery or production platform). Typically, such organizations have a library of modules built with cross-functional input (engineering, commercial, and procurement) and use design software that provides access to approved modules and equipment lists covered by supplier purchasing agreements.
2. *In project management*, these companies broaden stage-gate-review criteria to include plant- or module-design reuse, and to minimize design changes. Some companies are developing metrics to track reuse and accelerate adoption.

4.5.5 System Engineering Process Verification and Validation

SE practice dictates that criteria for validating that requirements are met are specified early in the project lifecycle and, where practical, at the same time as the requirements themselves are defined. Assurance (by verification) that the processes are being followed, and that the intention of each stage has been achieved in the subsequent stage of the lifecycle, is also important.

Processes are measured to ensure they are producing the expected results within time and cost constraints. There are a number of tools used for this purpose, including assessments, audits, and measuring process factors that provide leading indicators of performance.

Assessments are self-performed investigations designed to examine compliance against requirements, or to determine how well a process meets the intended objectives. Results identify areas for improvement. These are effective tools to discover where process designs or personnel are not performing as intended, and provide warning of potential noncompliance and other project issues.

Audits are performed by those independent of doing the work (e.g., by quality assurance staff, the procurer, or the regulator) for the purpose of checking process results against requirements. These audits are not controlled by the contractor but need to be included in their budgets. Like assessments, audits reveal process or implementation weaknesses or noncompliances that need to be addressed to ensure project success.

The most important approach to process verification is the measurement of factors contributing to success. Each process can be considered an equation where the final result is based on the contributing factors. These factors can be supplier quality, weather, specific construction methods, tooling arrangements, process controls, or other factors that influence output quality. Each process could have hundreds of such factors, but not all factors are important. Identifying these factors will require collecting data. Six sigma methods may be useful in assessing these factors. Once found, these factors will provide leading indicators useful to point to problems that can be addressed before they adversely affect quality.

It is important to also validate that we are achieving the results expected (or required) from the construction process. Evidence of requirements satisfaction tends to be associated with the measurement of how well the product of the project is meeting the defined quality, time and cost targets assuming an optimized construction process. The quality target for the product will be measured using established SE methods (e.g., analysis, inspection, demonstration, factory, and on-site testing).

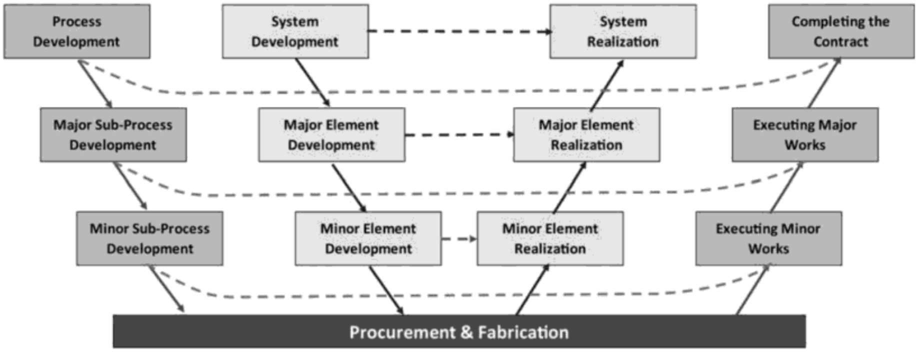


FIGURE 4.9
The modified "V" model.

For a megaproject many systems will be integrated on-site during the construction stage as the product system of the project is progressively built. It is important that all the systems are proved prior to integration (some off-site) and then again as part of the integrated system.

A recent approach to verification and validation that is particularly applicable to megaprojects is that of progressive assurance, as used on railway projects.

The modified "V" model in Fig. 4.9 shows the duplication of the legs to explicitly show the simultaneous development of the product and the process. The direction of the arrows indicates the idealized flow of information and/or material, in reality there will always be some corrective feedback between stages.

4.5.6 Defining and Allocating the Hand-over Responsibilities

A common model used within infrastructure projects is the "V" Model. A version updated by the Dutch Ministry of Public Works as illustrated in Fig. 4.10.

The situation today is that there is frequently a misunderstanding of the responsibilities within the model. Acquirers often underestimate their responsibilities vis-à-vis stakeholders and the interfaces with them at system level. The contractors are often thought to be doing a good job for the acquirer. On the other hand, contractors often have a poor understanding about the goals of the acquirer on a political and environmental level.

The hand-over responsibilities defined by the V-model are bidirectional. At each system level, the hand-over responsibilities are shifting from the acquirer to the contractor. The acquirer is always the main party related to system responsibilities. Within megaprojects the political and environmental impact can be very significant. The acquirer must ensure that the contract is

Index

Note: Page numbers followed by "*f*" and "*t*" refer to figures and tables, respectively.

F

G

H

I

J

K

L

M

P