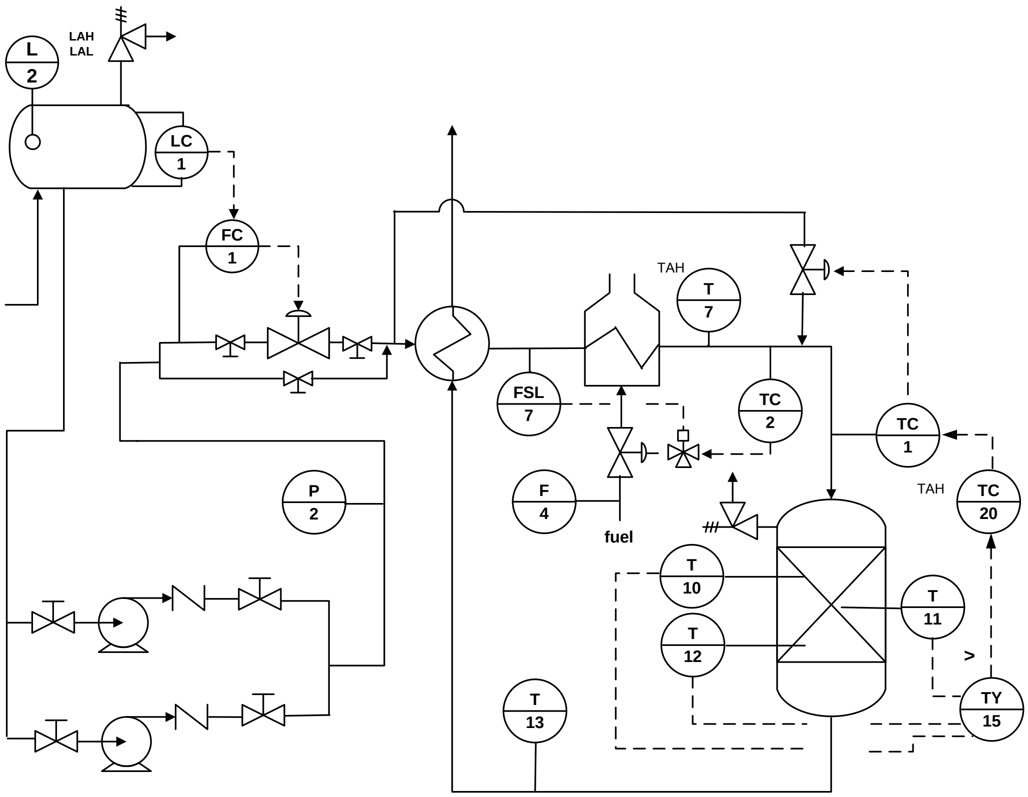
Operability in Process Design: Achieving Safe, Profitable, and Robust Process Operations

Chapter 4. Reliability



Thomas Marlin

RELIABILITY release 1.1 on April, 2014

This material is provided to promote education in the general field of "process operability" via the Internet site www.pc-education.mcmaster.ca . It is one of the chapters of an integrated presentation of selected operability topics. The author would like to hear from readers on how they are using this material. In addition, he would appreciate suggestions for improvements and extensions. He can be contacted at marlint@mcmaster.ca .

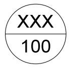
Acknowledgements

- Everyone who posts materials with the Creative Commons license
- H. P. Barringer for permission to use a figure on pump reliability and for his advocating for reliability in design and operations

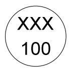
Disclaimer

Table of Contents

Symbols



CONTROL ROOM BOARD
MOUNTED INSTRUMENT

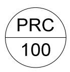


LOCAL BOARD MOUNTED
INSTRUMENT

MEASURED VARIABLE:
L: LEVEL
P: PRESSURE
A: ANALYZER
F: FLOW
T: TEMPERATURE

FUNCTIONS:
I: INDICATOR
C: CONTROLLER
A: ALARM
(H =HIGH, L=LOW)

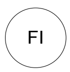
EXAMPLES:



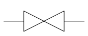
PRESSURE RECORDER
CONTROLLER: I.D. NUMBER 100,
MOUNTED IN CENTRAL CONTROL
ROOM.

TAH

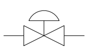
TEMPERATURE ALARM:
ACTIVATED AT HIGH
TEMPERATURE.



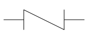
LOCAL FLOW INDICATOR



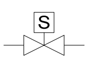
VALVE



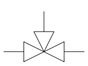
DIAPHRAGM VALVE:
CONTROLLED BY AIR LINE



CHECK (ONE-WAY)
VALVE

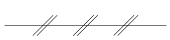


SOLENOID VALVE
CONTROLLED BY
ELECTRICAL SIGNAL



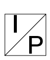
THREE-WAY VALVE

SPRING LOADED
SAFETY VALVE

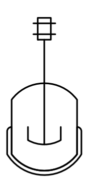


AIR LINE

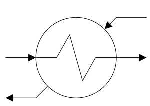
ELECTRICAL SIGNAL



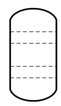
ELECTRICAL (CURRENT) TO
PNEUMATIC SIGNAL
CONVERTER



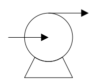
STIRRED TANK



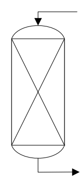
SHELL AND TUBE HEAT
EXCHANGER



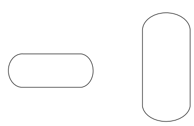
TRAYED COLUMN



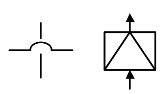
CENTRIFUGAL PUMP



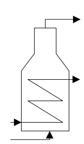
PACKED TOWER OR
PROCESS VESSEL (SUCH
AS A REACTOR).



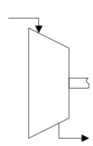
GENERIC TOWER OR
PROCESS VESSEL (SUCH
AS A REACTOR).



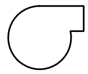
RUPTURE DISK,
BURST DIAPHRAGM

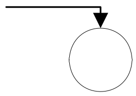


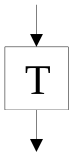
FIRED HEATER
(FURNACE)



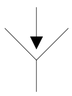
AXIAL
COMPRESSOR

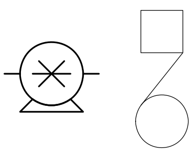

CENTRIFUGAL
FAN

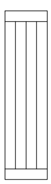

HEADER (STEAM OR
CONDENSATE)

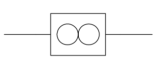

STEAM TRAP

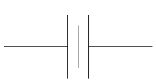

MOTOR

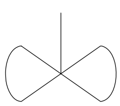

DRAIN TO SEWER

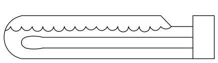

POSITIVE
DISPLACEMENT
PUMP

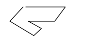

CONDENSER


TURBINE FLOW
METER

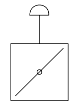

ORIFICE PLATE

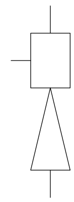

IMPELLER

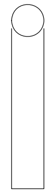

VAPORIZER
OR
REBOILER

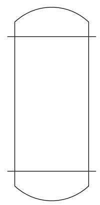

FILTER AND DRAIN

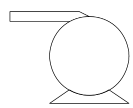

CYCLONE

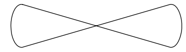

DAMPER
OR
BUTTERFLY VALVE

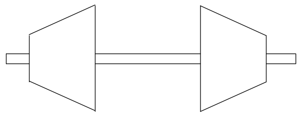

STEAM
EJECTOR


FLARE STACK


SHELL AND TUBE
HEAT EXCHANGER


FAN
OR
BLOWER

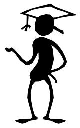

FAN


TURBINE USED TO
PROVIDE WORK
TO DRIVE
COMPRESSOR

Nomenclature

BPCS	Basic process control system
C_I	Installed cost
C_P	Purchase price
CW	Cooling water
F(t)	Failure probability density function
F(t)	Probability of failure
F_{BM}	Bare module factor
F_{in}	Volumetric flow into inventory
F_{out}	Volumetric flow out of inventory
GTCC	Gas turbine combined cycle heat recovery
K_C	Proportional gain in PID controller
K_P	Process gain
HAZOP	Hazards and operability
HAZROP	Hazards, reliability and operability
LCC	Life cycle cost
MTBF	Mean time between failures
MTTR	Mean time to failure
MTTR	Mean time to repair
MTOW	Mean time of waiting
n_f	Number of items failed
n_0	Initial number of items in failure test
n_s	Number of items not failed
OEE	Overall equipment effectiveness
PID	Proportional-integral-derivative controller
P()	Probability
PM	Preventative maintenance
PT&I	Predictive testing and inspection
R(t)	Reliability
RBD	Reliability block diagram
RCM	Reliability centered maintenance
SIS	Safety instrumented systems (safety control systems)
T	Period of plant operation, mission time
T_I	Integral time in PID controller
T_D	Derivative time in PID controller
V	Volume
Greek symbols	
α	Ratio of tank hold-up time to (MTTF + MTOW) for upstream process
$\lambda(t)$	Failure rate
ρ	Density

Chapter4. Reliability



4.0 To the Student

We expect reliable products. How would we like to have our automobile break down on a remote, snowy road and be unable to call for assistance because of a fault in our cell phone? As a result, most people will avoid products that have a track record of poor reliability.

Reliability influences profitability and safety. We would not fly an airplane that had a record of poor reliability. Not surprisingly, reliable performance is also important in the safety of manufacturing and process plants. A schematic of the relationship between faults and their effects on reliability and safety is given in Figure 4.1. Key topics of reliability are addressed in this chapter, while industrial safety is covered comprehensively in Chapter 5.

Since process reliability affects profitability, production capacity, product quality and other important factors in process performance, this chapter emphasizes important aspects of reliability. Designing a reliable plant requires that the process structure and equipment be selected to reduce the likelihood of breakdowns and the economic consequences of those (few) breakdowns that occur.

Given the importance of reliability, one would expect that reliability would be addressed in many core courses. Regrettably, this is not the case in nearly all chemical engineering curricula. Therefore, this chapter will fill the gap and provide basic knowledge required for process design. If you work in process design or plant operations, you will undoubtedly need to enhance your capability beyond the materials in this chapter, but you will have a head start from this material.

Reliability is a critical aspect to be achieved by all process plants via thorough analysis and appropriate process design and operation.

4.1 Introduction

Although we all have a general understanding of the term, we will start with a definition of reliability (US DOD, 1981).

Reliability: The probability that an item can perform its intended function for a specified interval under stated conditions.

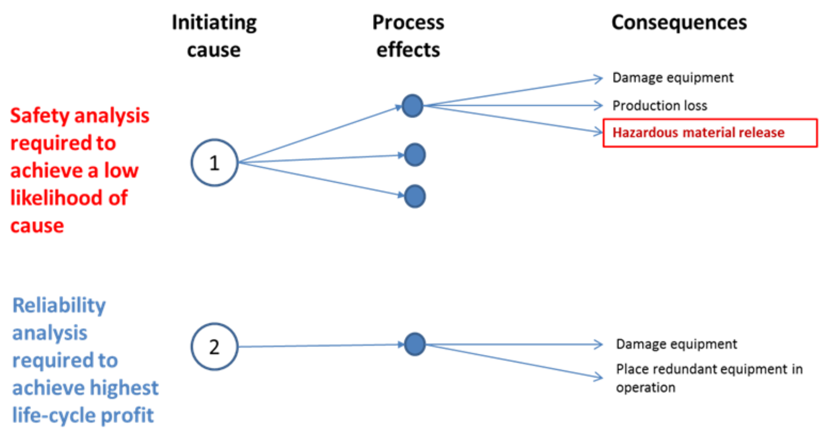


Figure 4.1. Schematic of safety and reliability in design and operations. Some process faults lead to potential hazards and require safety analysis. Some process faults result in economic loss but no hazards and require reliability analysis.

Since we are dealing with a probability, a process system cannot be categorized simply as "reliable" or "unreliable". Essentially no system is one hundred percent reliable; we must accept that some, albeit small, likelihood of failure exists for even highly reliable systems.

The definition also includes a caveat that the system must operate under "stated conditions". Therefore, we must be thorough in defining the conditions under which equipment must perform its intended function. For example, is it required to perform a function when electrical power has failed or during a fire?

Finally the "intended function" of a process system has many meanings. We might be overly optimistic and define the "intended function" to include maximum yields, energy efficiency and production rate; if so, no process system would be highly reliable. Let's consider the following degradations in plant performance.

- Catalyst decay can prevent a process plant from achieving the desired yield of valuable product
- Compressor vibration at high speeds can reduce the maximum production rate in a process plant
- Fouling of a heat exchanger can reduce the maximum reboiler duty in a distillation tower reboiler

These degrading conditions are undesirable, but they are also typical of the day-to-day challenges encountered in plant operations. As a result, the standard definition of reliability should be expanded to account for many conditions in which some, but not all, process capability has been lost. Therefore, reliability is not "black or white"; it has shades of grey. We will design a plant that might recover to its full capability after some faults, but achieve only partial capability to achieve the desired production rate or product yields after different equipment faults.

How do engineers decide the best investment in equipment to improve reliability? The natural method is economics! (Recall that safety-related design is provided in Chapter 5, where an entirely different criterion is provided.) Too little investment will lead to excessive economic loss due to low reliability, and to high an investment will not lead to an acceptable incremental improvement in plant profit. We invest the amount that will yield at least the minimum rate of return (MARR), using principles of time-value of money.

In this chapter, you will learn to do the following.

- Define reliability metrics and communicate these effectively
- Understand the effects of process structure on reliability
- Achieve reliability through (i) process design, (ii) operations and (iii) inventory.
- Understand the basic four elements of a process maintenance program
- Integrate reliability into engineering economic decision-making

4.2 Discussion of Reliability Issues

Before beginning the coverage of reliability calculations and design features, we will engage in a brief, qualitative discussion of reliability, covering causes, consequences, and responses.

4.2.1 Causes - Factors affecting reliability

Many factors affect plant reliability. When designing a plant, engineers must consider all of these factors and make many decisions to eliminate or ameliorate significant factors. Some of the most important factors affecting reliability are briefly introduced in the following.

- **Materials of construction –** Engineers select materials of construction for equipment that yield acceptable strength, corrosion resistance, and interaction with process materials. At times, multiple materials may be required, such as when a steel vessel is lined with glass or plastic to obtain strength and corrosion resistance.
- **Process conditions –** Each process equipment, e.g., pump, valve, heat exchanger, and so forth, functions well for a limited range of process conditions, and outside of the specified conditions, the equipment functions with reduced reliability. For example, a globe valve body functions well for clean fluids, but it is subject to plugging when used with slurries.

    - **Extreme process conditions during normal operations –** Sometimes, process economics require operating some equipment near its physical limits. For example, in olefins-producing plants, pyrolysis chemical reactions occur in pipes through which hydrocarbon feed flows. The temperatures required for desired conversions are extremely high, approaching the maximum limits of the steel alloy metals. While such operating conditions are within the safe operating window, equipment performance and reliability is reduced due to long-term degradation.

  - **Extreme process conditions during excursions** – When few, small disturbances occur the process can be maintained within its normal operating window. However, larger disturbances occur that could lead to equipment damage and low plant reliability. In cases where damage can occur, process controls should be employed to prevent the damage; control responses should alter conditions to prevent damage and maintain operation, if possible. If not possible, the controls should safely shutdown the effected equipment. We recognize that shutting down equipment involves an economic penalty for lost production time, but product can be started again, without the cost and long delay required for repairing damaged equipment.

- **Equipment faults** –Even the best designed and manufactured equipment can experience faults. The plant design should include features to reduce the effects of faults for the equipment most likely to fail. In most process plants, the least reliable equipment are rotating mechanical equipment (pumps, compressors, turbines, motors, etc.), electronic equipment (sensors, transmission, etc.), and final control elements (valves, motors speeds, etc.).
- **Personnel error** – Operating personnel are well trained and have years of experience before assuming supervisory positions. However, humans make errors due to understanding, miscommunication, and momentary inattention. Many mistakes can be corrected quickly without undue hazard or cost. However, we must ensure that plant designs prevent excessive damage or economic loss as a result of an error.
- **Severe External Disturbances** – Infrequently, external factors like weather can influence the plant. These "acts of God" (hurricane, tornado, flood, earthquake, etc.) can damage equipment and cause release of materials to the environment. The process design should match the types of external disturbances likely for the site of the plant.
- **Deliberate acts** – Regrettably, misguided people occasionally decide to damage property and might even attempt to injure others. These acts can vary from minor vandalism to extreme terrorism. These potential sources of damage will not be addressed in this chapter. (For an introduction, see Abrahamson and Sepeda (2009).)

Example 4.1 External Disturbances – The extent of analysis of and preparation for extreme (and highly unlikely) external disturbances should be matched to the consequences of the effects. Since an accident in a nuclear power plant could have enormous negative consequences, one analysis considers an airplane accident in which a large commercial jet crashes into a commercial nuclear power plant.

A commercial nuclear reactor in the USA is enclosed in a containment vessel to protect for external disturbances and to contain releases from the reactor. As a result of the terrorist attack of Sept 11, 2001, much of the critical infrastructure in the US is being reviewed for adequately protecting the community from effects of events not originally considered during design. Two opinions regarding the external disturbance in this example are provided for the reader in Illumin (2014) and Nuclear Energy Institute (2002). The lesson for the reader is that "unlikely" events can become important and that even unlikely events must be considered for high-consequence scenarios.

4.2.2 Consequences of faults due to low reliability

Failures can lead to consequences of varying degrees of severity. The following list gives a range of likely consequences in a process plant, from the most serious to the least.

- **Hazards to people in the plant and community –** Release of hazardous materials and explosions are consequences that could lead to death and injury. These are very serious and must be "prevented". Since these events cannot be completely prevented in most cases, we strive for a probability or likelihood that is very low. Methods for analyzing these situations and designing safety barriers are presented in Chapter 5.
- **Damage to equipment –** Although process equipment is designed to avoid damage under typical conditions, the equipment can be damaged under extreme conditions. To the extent possible, the plant design should avoid these extreme conditions and prevent damage if these conditions are approached.
- **Loss of production –** A failure can result in plant shutdown, with complete loss of production.
- **Off-specification Materials –** A failure can result in a major disturbance to plant operating conditions, so that material being processed cannot be sold as product. In some cases, the material can be re-processed at a later time; however, in other cases (e.g., polymer reactions) the material may have to be disposed of at a high cost.
- **Reduced process performance –** Often, reduced process performance results in economic loss. Recall that the full capital cost has been invested, and the complete operating cost is expended. Thus, the loss of yield, higher fuel consumption, or lower production rate substantially reduces the profitability of the project.
- **Insignificant consequence –** For small degradations in equipment performance, process variables can be modified using the capacity and flexibility included in the design. The cost for such modifications can be very small.

4.2.3 Responses to faults

In evaluating the proper designs for each potential cause, the engineer must match the cost of the design with the likely cost of failures. While each failure has its own unique effect on plant operation, it is useful to group failure severities into a few categories in this discussion, because these groupings enable us to discuss the effects.

Before discussing the severity, we should understand an important aspect of plant operations. Continuous plants startup in excellent condition, with all equipment operating "as new". The plants operate for many months (up to several years); during this time, minor maintenance is possible, but major repairs are not possible. A full plant shutdown, termed a "turnaround", is planned many months in advance so that skilled personnel and spare parts are available. The turnaround is a short period of intense effort to maintain the plant. Because of the cost for lost production, the turnaround is executed in the minimum time, and the plant is returned to production. Plant shutdowns between planned turnarounds are avoided if possible. However, unplanned maintenance shutdowns are required for severe failures.

- **Do nothing, no significant effect –** Minor changes in behavior during plant operation are expected. As addressed in chapters on Operating Window and Flexibility, plant designs provide the ability to respond to expected, minor changes without significantly affecting the performance of the plant. For example, a heat exchanger is expected to foul over months, and the lower heat transfer coefficient can be compensated by a higher flow rate of cooling water to achieve the same rate of heat transfer.
- **Do nothing, effect tolerated at lower plant performance –** Over time, equipment performance can degrade in a manner that reduces plant performance but does not introduce a hazard. In these situations, the engineer must decide whether the cost of an extra shutdown is warranted. In many situations, the plant will continue in operation, albeit at lower performance. For example, a compressor might experience excessive vibration at high speeds. In response, the plant production rate could be reduced, so that the continuous operation can be continued.
- **Repair during operation –** There is a significant economic advantage for repairing equipment while maintaining plant operation. In some cases, such repair is possible, but only when provided through extra investment at the plant design phase. The extra investment providing the capability for repairs is made based on economics; historical data indicates the equipment most likely to fail, which dictates where the investment would be appropriate.
- **Replacement during operation –** This situation is very similar to the previous situation. With proper design, some equipment can be replaced without requiring a plant shutdown. Again, this investment is appropriate from equipment that is prone to frequent failures.
- **Shutdown required for repair or replacement –** In some cases, the failure requires a shutdown for repair. Certainly, failures leading to hazardous conditions require an immediate shutdown. In non-hazardous situations, continued operation can result in such large economic loss that the cost of an extra shutdown is justified by the increased profitability after the plant is restarted.

At the design stage, the engineer must decide on the appropriate investment in equipment to provide initial reliability and the additional investment to enable personnel to repair or replace selected equipment while the plant remains in operation. During plant operation, the engineer must evaluate the plant performance and determine what equipment requires repair or replacement. This analysis is performed using the principles of engineering economics that all engineering students learn in university. The special formulation for this “life cycle analysis” is presented in Section 4.8 of this chapter.

Example 4.2 Economic analysis – In this example, we will consider instrumentation, which is one of the plant components that affect reliability. Estimate the cost of instrumentation, and determine whether the detailed reliability analysis is worth the effort.

The cost of the instrumentation in a typical chemical process plant can be evaluated using cost estimation correlations. The purchase cost of each item of capital equipment is estimated from correlations; we will use the symbol C_P for this purchase price. The installed costs of the equipment are estimated as a factor multiplied by the purchase cost. This factor is called the Bare Module Factor (F_{BM}), and the factor accounts for all

materials and labor to install the equipment. Thus, the cost of the installed equipment (C_I) is given in the following expression.

$$C_I = C_P * F_{BM}$$

Although the correct value of the Bare Module Factor depends on the specific equipment, we will use typical values for this evaluation. The factor is a composite that includes many costs; labor, insulation, piping, support structure, electrical, and instrumentation. As a rough estimate, the bare module factor has a value of about 3.5, and the contribution of instrumentation is about 0.08. The fraction of the total cost that provides the field instrumentation can be determined in the following expression.

$$\text{Fraction of cost for instrumentation} = (C_P * 0.08)/(C_P * 3.5) = .02$$

The cost of field instrumentation is about two percent of the plant cost, which is very small. We don't design in detail for the project economic evaluation; we use the bare module factor. So, is detailed design for reliability for instrumentation (or other components) worth the effort in the detailed design?

The answer is a resounding YES! Naturally, the cost of the equipment is important, but the performance of the plant is crucial for achieving profitable economic returns. Typically, the base case economic analysis is based on about 360 days/year of operation with low (or no) cost for repairing failed equipment. Lower reliability caused by low reliability plant equipment will reduce the days of operation and add substantial additional annual cost for equipment repair; the result will be much lower profitability.

Therefore, careful design of complex plant systems involves all equipment affecting reliability (potential failures and operation degradation) regardless of the (possibly low) purchase and installation cost of the equipment.

(Note that this analysis has used "typical" cost factors. For any proper cost estimation for economic analysis the factors should be determined from appropriate data bases. For example, the bare module factor can vary from 0.10 (for large tanks) to over 4.0.)

Now that we have introduced the qualitative issues regarding process reliability, the next section covers reliability terminology and basic modeling methods. These reliability measures and predictions will provide principles for process design.

4.3 Reliability Measures and Modeling

This section builds understanding of reliability through introducing reliability measures that are used in the process industries. These measures give a clearer understanding of the desired reliability performance. In addition, methods for modeling reliability are presented. These methods with examples give us an understanding of the effect of process design structures on reliability.

4.3.1 Reliability measures

Reliability: We will begin with reliability, which was defined in words in Section 4.1. This definition yields the following expression for reliability.

$$P(T > t) = R(t) \tag{4.1}$$

with $R(t)$ = reliability, probability of no failure, with values 0-1
$P()$ probability of occurrence
T = time of mission (time of plant operation)

Since a system either functions or does not function, the probability of failure is the following

$$R(t) + F(t) = 1 \tag{4.2}$$

with $F(t)$= probability of failure

One can think about an experiment in which the reliability and failure rate are determined experimentally. We could start with a large number of items and measure all items to determine which have failed. The reliability would be given by the following.

$$R(t) = \frac{n_s(t)}{n_s(t) + n_f(t)} = \frac{n_0(t) - n_f(t)}{n_0(t)} = 1 - \frac{n_f(t)}{n_0(t)} \tag{4.3}$$

We observe from expression (4.3) that an item's reliability is always non-negative and decreases monotonically with time. Reliability equals 1.0 at zero time and equals 0.0 at infinite time. Differentiating (4.3) gives the following.

$$\frac{dR}{dt} = -\frac{1}{n_0}\frac{dn_f(t)}{dt} = -f(t) \tag{4.4}$$

with $n_s(t)$ = number of items that had not failed (survived) by time t
$n_f(t)$ = number of items that failed by time t
$n_0(t)$ = initial number of items
$f(t)$ = instantaneous probability of failure, i.e., the probability density function

Failure Rate: The failure rate is the number of failures per unit of time at a specific lifetime divided by the number of surviving items at that time. This rate can be expressed in the following equations.

$$\lambda(t) = \frac{1}{n_0(t) - n_f(t)}\frac{dn_f(t)}{dt} = \frac{n_0(t)}{n_0(t) - n_f(t)}\frac{d(n_f(t)/n_0(t))}{dt} \tag{4.5}$$

$$\lambda(t) = -\frac{1}{R(t)}\frac{dR(t)}{dt} \tag{4.6}$$

The relationship between the reliability and failure rate can be determined by integrating equation (4.6) to give the following.

$$R(t) = \exp\left[-\int_0^t \lambda(t)dt\right] \tag{4.7}$$

For the case with constant failure rate (independent of time, $\lambda(t) = \lambda$), reliability is expressed as follows.

Constant failure rate:

$$R(t) = e^{-\lambda t} \tag{4.8}$$

Let's look at the failure rate function. The classical explanation of failure rates begins with the "bathtub curve" shown in Figure 4.2. The failure rate is separated into three segments.

- An initial "break-in" segment, sometimes referred to as infant mortality segment. These early failures can be due to causes such as manufacturing faults, incorrect selection of components, and installation mistakes. When a process plant is being constructed, equipment is placed in operation individually before the plant is started up; this approach is meant to locate failures during the break-in period so that they can be repaired.
- A long segment with constant failure rate, which is often called the chance failure period or the useful life. Interestingly, a complex, multi-item system which requires all components to function for success can be modeled as a single item with a constant failure rate (Lees, 1996, page 7-45).
- A final "wear-out" segment. Essentially all items will fail due to wear, aging, corrosion, erosion, and so forth, so that an increasing failure rates at very long times seems reasonable. The wear-out phase can be (nearly) eliminated by the practices of (1) inspection and replacement of worn items and (2) routinely replacing items after a period of operation before wear-out is known to occur.

While the bathtub curve is intuitively clear, it does not always represent the failure behavior of industrial equipment or complex systems. The results from three studies shown in Figure 4.3 indicate that <u>few equipment fail as described by the bathtub curve</u> and that most have a prolonged period with a constant failure rate, perhaps with an initial period with changing failure rate. This conclusion supports some of the analysis using constant failure rates given here and will be the basis for some maintenance policies presented in a later section.

Determining the failure rates of items in a process plant is a primary task of reliability engineers, and techniques for this analysis are available in the literature. In this chapter, our goal is to introduce principles and designs that are generally applicable for most failure rates, so we will limit our analysis to systems with constant failure rate.

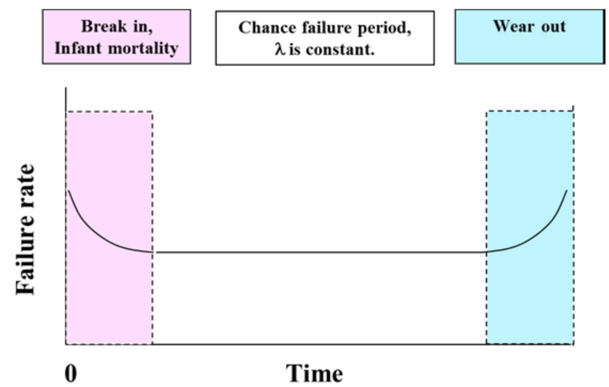


Figure 4.2. Bathtub curve failure rate distribution with time.

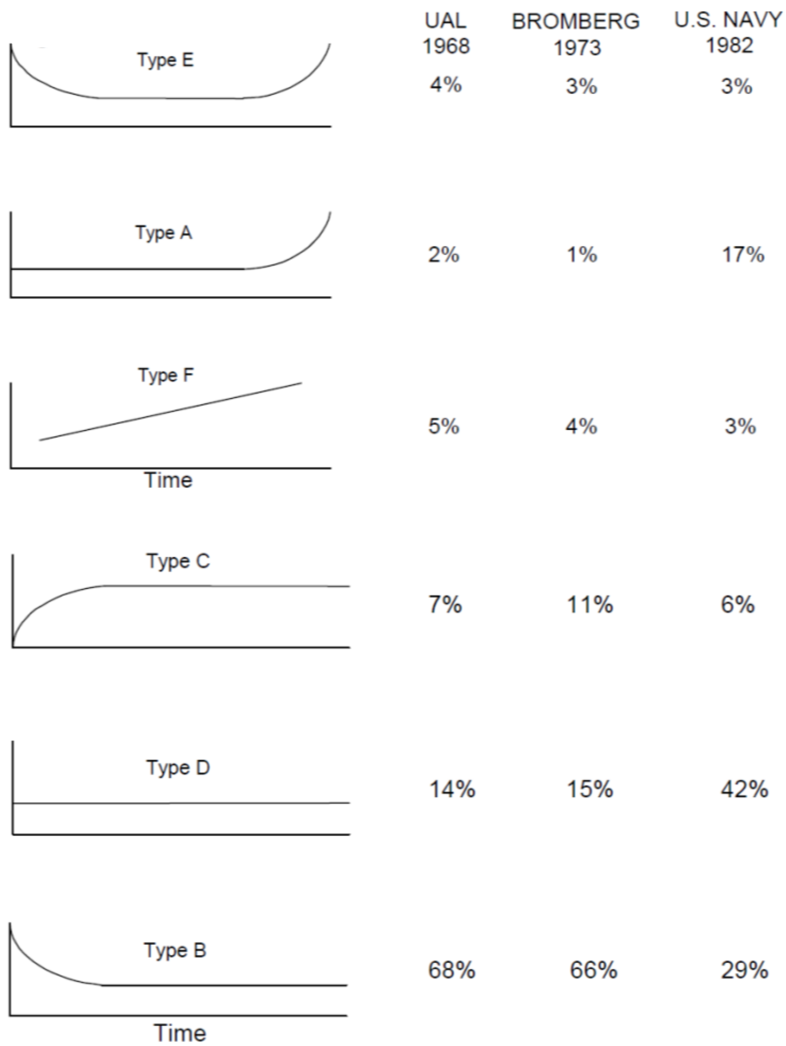


Figure 4.3. Various patterns of failure rates vs. time with percentages of each pattern experienced by each industry. (from NASA, 2000)

In the remainder of the chapter, we will limit consideration to items with constant failure rates. However, engineering practice should match the time-dependence of the failure rate to empirical experience with the equipment.

Example 4.3. Failure data - Determine the typical failure rate of a one-way valve, also termed a check valve. A check valve is designed to allow flow in the desired direction in a pipe and prevent flow in the reverse direction.

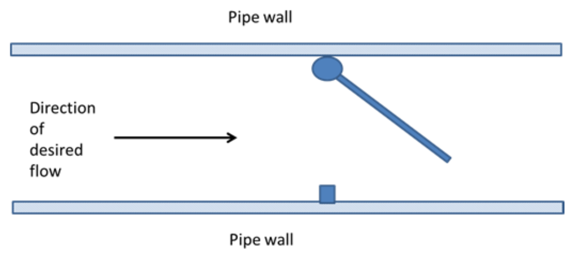


Figure 4.4. Schematic of swing-type one-way, check valve.

The purpose of this question is to highlight an important issue with failure data. Most equipment can experience several different failures that can have substantially different consequences. Therefore, engineers need data for every important failure. The following data is reported by Lees (1996).

- **Failure to open** — **$1x10^{-4}$ failure/demand**
- **Internal leak (reverse flow, serious)** — **$3x10^{-7}$ failure/hour**
- **Rupture** — **$1x10^{-8}$ failure/hour**

The failure to open represents situations in which the flow is normally zero and occasionally flow is required. Internal leak represents the situation in which the flow stops and reverse flow could occur. Note that this one-way valve never provides a tight closure, so that a small flow is expected; this failure data is for a large (undesirable) reverse flow. The rupture is for a loss of containment, in which liquid escapes the pipe.

When performing reliability analysis, the engineer must ensure that data used applies to the failures and consequences relevant to the analysis.

Mean times: Often, average times of operation between faults are used to characterize system reliability. The most common terms are explained in the following.

- **Mean time to failure** (*MTTF*): The average time between a device being placed in operation and its first failure.
- **Mean time between failures** (*MTBF*): This measure includes time to repair or replace and time to wait.
- **Mean time of waiting** (*MTOW*): Wait time can be due to many causes, such as administrative processing, time for personnel to arrive, and time for spare parts delivery. In addition, time to regain plant operation, i.e., startup the plant, must be included in wait time.

The following relationship follows from the definitions.

$$MTBF = MTTF + MTOW \tag{4.9}$$

The mean time to a failure is related to the reliability and failure rate as demonstrated in the following analysis that evaluates the first moment (mean) of the probability of failure.

$$MTTF = \int_0^\infty t\, f(t) dt = -\int_0^\infty t \frac{dR}{dt}\, dt \tag{4.10}$$

Integrating by parts and noting that the reliability at infinite time is zero yields the following.

$$MTTF = \int_0^\infty R(t) dt = \int_0^\infty exp\left[-\int_0^t \lambda(t) dt\right] dt \tag{4.11}$$

For the case of constant failure rate,

Constant failure rate:

$$MTTF = \int_0^\infty e^{-\lambda t} dt = {}^{1}/_{\lambda} \tag{4.12}$$

Plant performance measures: The process industries are keenly interested in the measuring plant performance, so that deviations from peak performance can be identified and corrected quickly. The most common performance measure is availability that is defined in the following.

Availability is the percentage of time that the system is in condition for successful operation. (Modarres, 1993). The total time should be taken as the expected plant operation time, which excludes expected downtime for causes such as weekends, scheduled maintenance, time when no demand exists, etc. (In some instances, the term **service factor** is used synonymously in place of availability.)

For a repairable system with a constant failure rate, the availability can be evaluated using the following expression.

Constant failure rate:

$$Availability = \frac{MTTF}{MTTF + MTTR + MTOW} \tag{4.13}$$

Clearly, plant availability has a significant impact on profitability. Any time the plant is (completely) unavailable, no revenue can be generated, although the capital cost and fixed operating expenses are not reduced.

As discussed above (Section 4.2.2), a "failure" can have various degrees of consequences. Therefore, many plants cannot be correctly categorized as being in one of only two states, operable or inoperable. A common approach to considering partial loss of process capacity is to evaluate the Overall Equipment Effectiveness (OEE), which is calculated as shown in the following expression.

$$OEE = Availability * Performance * Quality \tag{4.14}$$

The term "Performance" is perhaps a misnomer, as it relates to only production rate in this definition. It is the percentage of the expected (no fault) production rate actually achieved. The "Quality" is the percentage of the product that satisfies specifications. The OEE characterizes plant performance better than Availability.

However, even OEE is inadequate for multi-product plants with variable-quality products. Some reasons that EEO is inadequate are given in the following.

- Many chemical plants have multiple products, so that there is no single "production rate". A partial fault in one part of the plant can be partially compensated by increasing product(s) that do not require the unit with the partial fault.
- Products that do not satisfy the quality specification have various dispositions, for example, they could be recycled, sold at lower value, used for fuel, or discarded with no value (and perhaps a processing cost).
- Lost performance for the three key terms are not equivalent in their consequences; however, the measure apportions equal importance to all three. For example, (.90)(.99)(.81) = (.81)(.90)(.99).
- Again, "availability" depends on the seriousness of a fault, with some faults requiring a total shutdown, while others having minor impact on production or profitability.
- Safety concerns are not explicitly addressed. A single near-miss of a major accident is far more important that many minor economic losses.

The performance of a process plant is too complex to summarize in a single numerical measure. However, performance measures like Availability and EEO are in use, and they can be employed as rough, easily calculated indicators of unit performance that can be supported by subsequent, detailed analysis.

Engineers need to have the attitude that the measure(s) can highlight potential problems (or success) but do not alone guarantee complete insight into plant performance.

Example 4.4. Time to Failure - A system of power generation plants, the "grid", must provide the power demanded by the consumers; if the grid fails, everyone knows immediately! Therefore, they must be designed for reliable performance. What is the mean time to failure and to repair for sample equipment?

Sample reliability data is reported on power plant equipment by the U.S. Department of Energy, in DOE (1999). Values for a couple of the entries are given in the following.

System	MTBF (h)	MTTR (h)	Availability
Boiler (planned major maintenance overhaul)	12514	608.5	0.9536
Feed-water pump	4949	12.11	0.9976
Condenser tube leaks	8588	9.5	0.9989

As expected, a major maintenance task, which can involve replacing riser tubes inside the boiler, takes the most time. Mechanical rotating equipment also has a lower availability than piping in heat exchangers.

4.3.2 Reliability prediction

A process plant is composed of a multitude of individual components, such as vessels, heat exchangers, pumps, motors, valves, sensors, and many more. Certainly, low failure rates for every component is desirable, but the performance of the integrated system of paramount importance regardless of the individual components. Plant design employs an understanding of the effects of some basic process structures to achieve the desired overall reliability. The reliability of a few common structures will be evaluated in this section, and these reliability results will be applied in subsequent designs in this (and later) chapters.

We will investigate structures with multiple units.

Unless specifically stated otherwise, the failure rates in each unit will be considered constant with time, and each unit's failures will be independent of other units' failures.

This situation occurs often; a valve failure may have no relationship to the failure of a pressure vessel or a temperature sensor. However, "common cause" failures are possible. For example, the loss of steam supply could cause failures in a reboiler, steam-driven turbine, and heat exchanger. Therefore, reliability analysis must include the integrated process and utility systems that provide steam, electricity, compressed air, and so forth.

Series: The most common process structure is series, where a number of units are arranged in sequence. All of the units must function properly for the series structure to function. A series system is shown in the block diagram in Figure 4.5, which depicts the causal relationship between failures; it does not imply the direction of material flow, as would be the case for a process flow diagram. For independent failures in each unit, the reliability of the series is the product of the individual reliabilities.

$$R_{series} = R_1 R_2 R_3 \ldots. = \prod_{i=1}^{N} R_i \tag{4.15}$$

with R_{series} = the reliability of the series system
R_i = the reliability of the i^{th} unit
N = the number of units in the series

Since the unit reliabilities are less than one, the series reliability must be lower than the reliability of each of its component units. The reliabilities of series systems with equal individual unit reliabilities are shown in Figure 4.5.

The mean time to failure for a series system is given in the following.

$$MTTF_{series} = \frac{1}{\lambda_{series}} = \frac{1}{\sum_{i=1}^{N} \lambda_i} \quad (4.16)$$

The MTTF for the series system is less than the MTTF for each of its component units.

From both equations (4.25) and (4.16), we note that the reliability and MTTF are adversely affected by a large number of elements in series and even one series element with low reliability.

Therefore, we expect the need for uniformly high-reliable components in series structures.

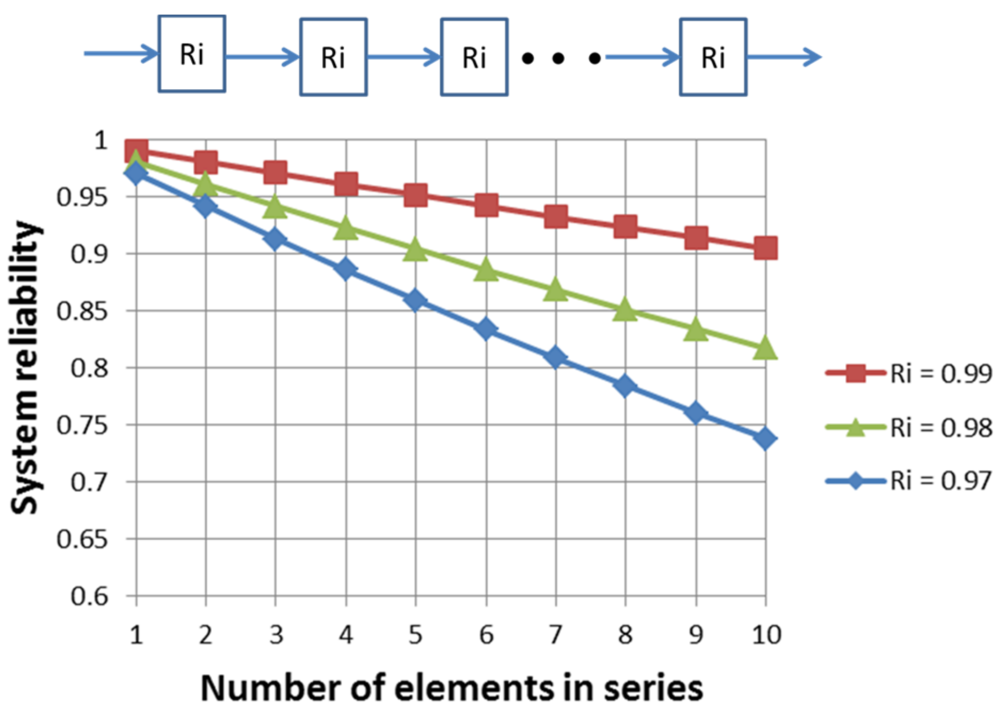


Figure 4.5. Example of reliability of a series of elements with equal element reliability. Each element has reliability Ri.

Example 4.5 Lusser's Law – When was the importance of the series structure on reliability first recognized?

The general conclusion stated above was "discovered" by an engineer named Lusser when developing the V1 weapon for Nazi Germany during World War II. The weapon was not initially successful because of the large number of parts that needed to function for the proper operation of the weapon, as shown in Figure 4.5. Lusser is acknowledged to have recognized this principle and required improvements in the manufacture of all components in the weapon. While he advanced the practice of engineering, his "success" resulted in increased death and destruction in civilian areas during the war. The principle of high component reliability in series systems is sometimes referred to as "Lusser's Law" (Wikipedia, 2014).

Example 4.6 Many series components – A process system requires many components to function simultaneously for the system to operate successfully. These components include process equipment (pumps, valves, etc.), control equipment (sensors, signal transmission, computers, etc.), utilities (steam, compressed air, fuel, etc.), and power equipment (power supplies, motors, etc.). Consider a system with thirty reliable components, each with a reliability of 0.99, and one component with a reliability of 0.95. What is the reliability of the system?

Often, the engineer will make an approximation that a series system has reliability nearly the same as the lowest reliability in a series system. Certainly, a series system must have a reliability value no higher than its lowest component. If all other components have a high reliability, is the proposed approximation reasonable? The calculation below gives the result for the example.

$$\mathbf{R_{system} = (0.95)(0.99)^{30} = (.95)(.74) = 0.70}$$

As we see, the system reliability (0.70) is much lower than its "weakest link" (0.95). When many moderate to high reliability components must all function, yielding a series reliability system, the overall system might not function with acceptable reliability.

Parallel: Another common process structure is parallel, where a number of units are included in the system and the system will function when one or more of the units functions properly. A parallel system is shown in the block diagram in Figure 4.6, which depicts the causal relationship between failures; it does not imply the direction of material flow, as would be the case for a process flow diagram. For independent failures in each unit, the probability of failure of the parallel system is the product of the individual probability of failures.

$$F_{parallel} = F_1 F_2 F_3 \ldots\ldots = \prod_{i=1}^{N} F_i \tag{4.17}$$

with $F_{parallel}$ = the probability of failure of the parallel system

F_i = the probability of failure of the i^{th} unit

N = the number of units in the system

Using the relationship in Equation (4.2), the reliability of the parallel system can be determined.

$$R_{parallel} = 1 - F_{parallel} = 1 - \prod_{i=1}^{N}(1 - R_i) \tag{4.18}$$

The mean time to failure for a parallel system with N identical elements (having MTTF) is given in the following equation. (For the derivation of this equation, see Moderras, 1993.)

Identical parallel units:

$$MTTF_{parallel} = MTTF\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots.. + \frac{1}{N}\right) \tag{4.19}$$

The reliabilities of parallel systems with equal individual unit reliabilities are shown in Figure 4.6. We note from equation (4.19) that the incremental improvement of the system MTTF decreases as the number of elements increases. Often, the installed cost of each element is independent of the number of elements, and the cost of a failure is independent of the design. As a result, an optimum number of parallel units exists and can be determined using reliability and economic data.

We expect a parallel structure to have an optimal number of elements where the benefit of an additional element just equals the cost of adding the element.

Example 4.7. Parallel pumps – The operation of plant boilers is critical for reliable supply of heat and power to a plant. Boiler feed water pumps must function properly for the operation of the boilers, and we require that the system have a mean time to failure of greater than six years. If each pump has a MTTF of 3.5 years, what is the minimum number of pumps in a parallel structure required to achieve the desired system reliability?

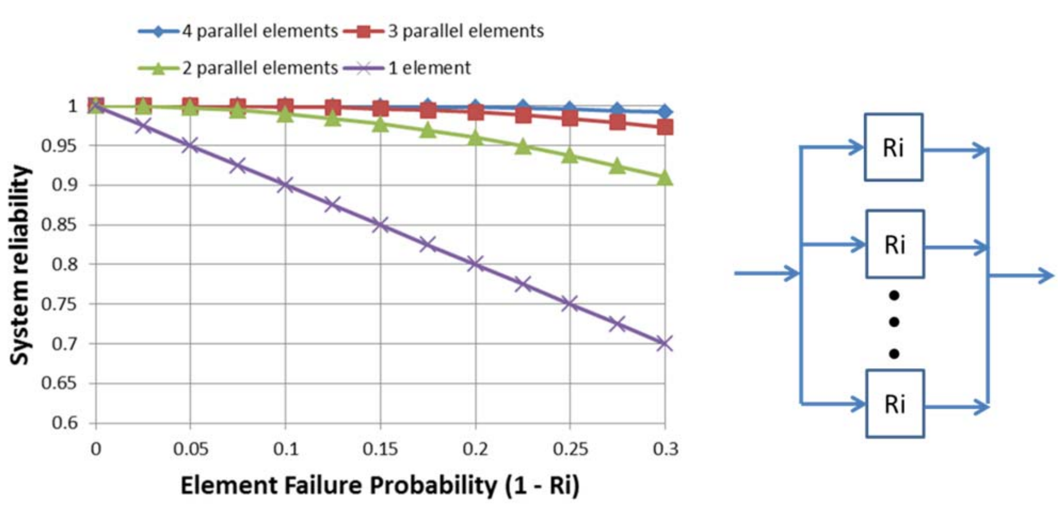


Figure 4.6. Example of reliability of parallel elements with equal element reliability.

We will apply equation (4.19) to determine the parallel system reliability for various numbers of parallel structures. The results are given in the following.

Number of pumps	System MTTF (years)
1	3.5
2	5.3
3	6.4

This solution requires that three pumps be operating continuously, with each pump having the ability to provide the entire water flow rate. Therefore, under normal operations each pump will operate at about one third of its maximum capacity. Can you think of any reasons why this might not be the best solution? (Hint: See Example 4.12.)

Complex "mixed parallel-series" structures: Not surprisingly, process equipment configurations yield reliability structures more complex than simple series and parallel structures. Often, these equipment configurations are selected to provide desired reliability performance. Here, we will consider systems consisting of only series and parallel sub-systems, and we will demonstrate the method for reducing a complex block diagram so that reliability can be determined. The general approach is to locate sub-structures that are entirely series or parallel and to apply the previous formula to evaluate the reliability of the sub-structure. This approach can be applied iteratively until the overall reliability has been evaluated.

Example 4.8. Lets' determine the reliability of the three structures shown in the block diagram in Figure 4.7. We will consider the situation in which every element has the same reliability of 0.90, so that we can determine the effect of the structure on the system reliability.

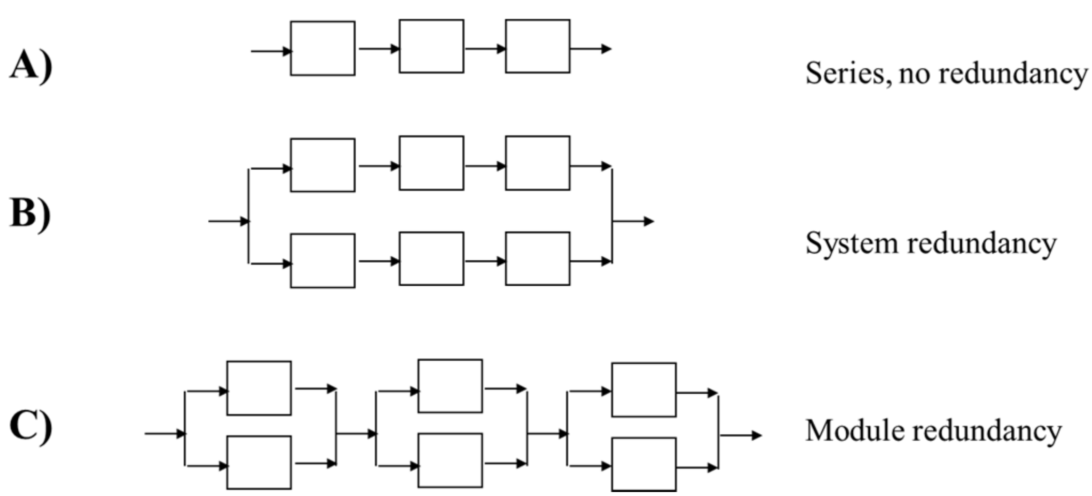


Figure 4.7. The block diagrams for three systems considered in Example 4.8. Each system functions if at least one path with functioning elements exists.

A. This is a series system, and its reliability can be evaluated by applying equation (4.15). The result is determined as shown in the following.

$$R_{series} = R_1 R_2 R_3 = (0.90)^3 = 0.729$$

B. This is a system with "system-level" redundancy, i.e., the entire system is duplicated. The system functions properly is either one of the two redundant systems is fully functional. The first step is to reduce each of the individual series systems to a single element, noting that the top and bottom series have the same structure.

$$R_{top\ series} = R_1 R_2 R_3 = (0.90)^3 = 0.729$$

Then, the reduced structure is a two-element parallel system that can be evaluated as shown in the following.

$$R_{system\ redundant} = 1 - F \quad = 1 - \prod_{i=1}^{N}(1 - R_i) = 1 - (1 - 0.729)^2 = 0.927$$

C. This is a system with "module-level" redundancy, i.e., every module or element system is duplicated. The system functions properly when at least one of the parallel elements in each module functions. The first step is to reduce each of the individual parallel modules systems to a single element.

$$R_{parallel\ module} = 1 - F \quad = 1 - \prod_{i=1}^{N}(1 - R_i) = 1 - (1 - 0.90)^2 = 0.99$$

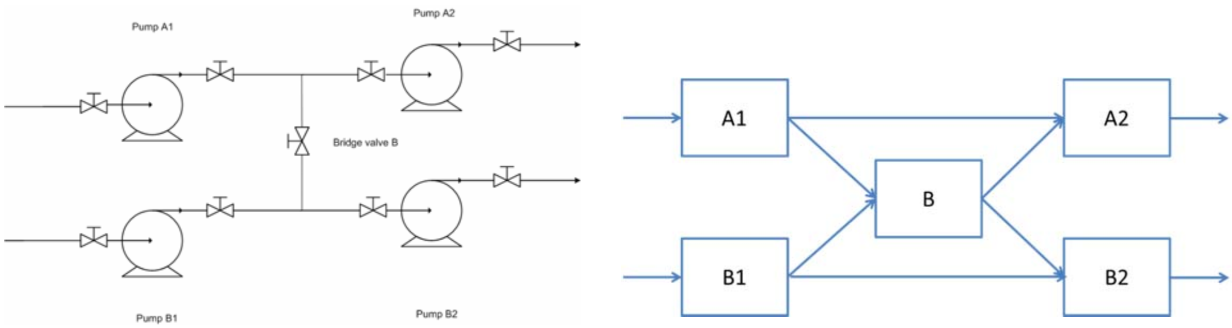
Then, the resulting series of reduced modules can be evaluated as a series.

$$R_{module\ redundant} = R_1 R_2 R_3 = (0.99)^3 = 0.97$$

Naturally, both systems with redundancy are more reliable than the series system in (A). Also, we observe that module redundancy provides much higher reliability than an equivalent system redundancy.

Complex structures with a bridge: Some complex structures cannot be reduced to a "mixed series-parallel" system. One of these is a structure with a bridge, such as the physical system in Figure 4.8a, which shows two series pumps with a bridge between the suctions of the second stages. This bridge is often referred to as a "crossover" or "jump-over". We will consider the situation in which the system functions when the fluid can flow through two operating pumps in series; we implicitly assume that one series configuration can pump the maximum desired capacity, if needed.

To evaluate the reliability (Dhillon, 2005), we first develop the block diagram of the system in Figure 4.8b. We will consider two scenarios that cover all possible outcomes. First,



a. Process schematic b. Reliability Block Diagram

Figure 4.8. Process bridge system.

the scenario considered occurs when the bridge functions. In this case, the system functions when at least one of the first parallel pumps and at least one of the second parallel pumps functions.

$$\underbrace{(R_B)}_{\text{Probability of bridge functioning}} \; \underbrace{[1-(1-R_{A1})(1-R_{B1})][1-(1-R_{A2})(1-R_{B2})]}_{\text{Probability of two parallel systems functioning (required when bridge functions)}} \tag{4.20}$$

Second, we consider the scenario in which the bridge has failed, which gives the following reliability.

$$\underbrace{(1-R_B)}_{\text{Probability of bridge not functioning}} \; \underbrace{[1-(1-R_{A1}R_{A2})(1-R_{B1}R_{B2})]}_{\text{Probability of remaining series-parallel system functioning (required when bridge fails)}} \tag{4.21}$$

The total reliability is the sum of these individual reliabilities.

$$\begin{aligned} R_{\text{Bridge system}} = {} & (1-R_B)\;[1-(1-R_{A1}R_{A2})(1-R_{B1}R_{B2})] + \\ & (R_B)\;[1-(1-R_{A1})(1-R_{B1})][1-(1-R_{A2})(1-R_{B2})] \end{aligned} \tag{4.22}$$

Example 4.9. Determine the reliability for the pump system in Figure 4.8 for two designs, (a) with and (b) without the crossover. The operating period is one year or 8760 hours.

For this problem, the reliabilities of each pump can be taken to be 0.75 (MTTF of 3.5 years) and the reliability of the crossover valve is taken as 0.999 (MTTF of 114 years) (Block and Geitner, 1999).

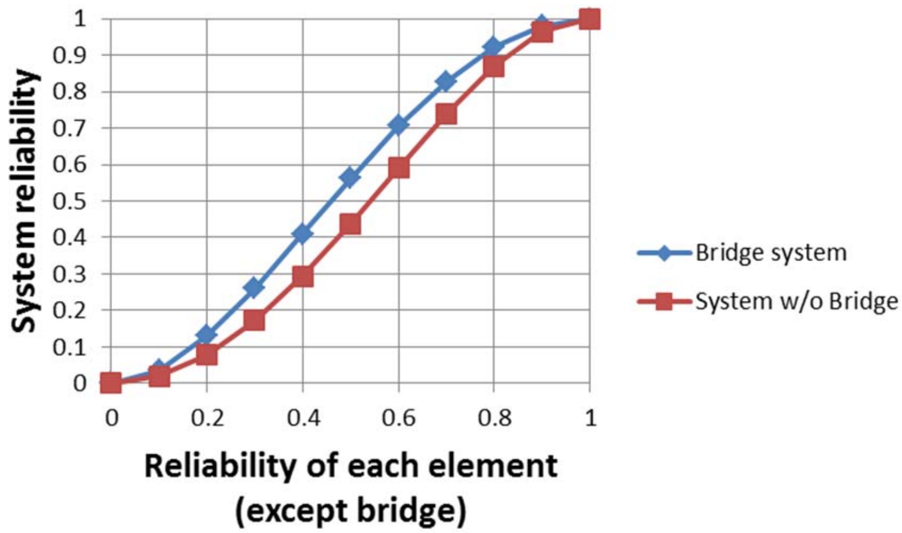


Figure 4.9. Reliability of the system in Figure 4.8b with and without a bridge element. All elements have the same reliability except for the bridge which has the reliability of 0.999.

a. We note that the reliability without the bridge is given by the expression for the failed bridge, i.e., equation (4.22), without the (1-R_B) term. The results are given in the following.

$$R_{No\ bridge} = [1-(1-R_{A1}R_{A2})(1-R_{B1}R_{B2})] = 0.81$$

b. The reliability for the system with the bridge in calculated using equation (4.22) to yield the following value.

$$R_{Bridge\ system} = (1-R_B)\ [1-(1-R_{A1}R_{A2})(1-R_{B1}R_{B2})] + (R_B)\ [1-(1-R_{A1})(1-R_{B1})][1-(1-R_{A2})(1-R_{B2})] = 0.88$$

We see that the crossover significantly increases the reliability for the system in Figure 4.8. For a broader comparison, the reliability of the same system structure with varying element reliabilities is shown in Figure 4.9. We observe that the bridge can significantly increase system reliability, especially when the individual elements have low reliability.

The key advantage of the bridge system is that the bridge can convey the resource (process fluid, steam, fuel, electricity, etc.) between many units; there is no fixed structure of the bridge limited to backing up a single other unit.

Complex "standby" structures: Often, some equipment is in service and carries the full load for the process, while other equipment is not in operation, but is available to replace failed equipment. Some device is required to sense a failure and activate the next available replacement. A two-element standby system reliability block diagram is shown in Figure 4.10. Naturally, engineers provide standby units when the single element has a lower than acceptable

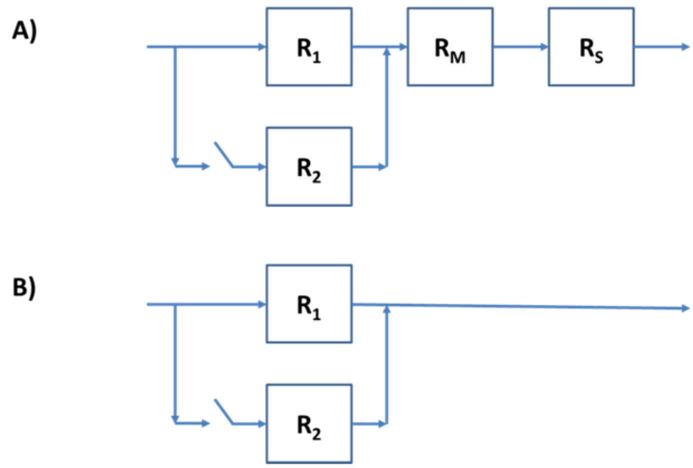


Figure 4.10. Reliability block diagrams for standby systems. (A) including measurement (M) and switching (S) equipment and (B) assuming perfect performance of measurement and switch.

reliability and the cost of the standby is not excessive. Standby structures are common in the process industries, and a few examples are given in the following.

- A pump with standby backup(s) that are not in continuous operation
- An electrical power supply with backup
- A microprocessor in a process control system with a backup microprocessor
- A process plant boiler system will have spare boiler(s) in standby
- Electrical utility power generation grids have gas turbines that can startup rapidly

The reliability of the standby system depends on the reliability of the process elements, the sensing and switching equipment. Here, we will consider the situation in which the sensing and switching are perfect, each element has the same, constant reliability, failures are independent and each standby element enters service "as good as new". The reliability and mean time to failure for the standby system are given by the following expressions (Dhillon, 2005).

Identical standby units:

$$R_{standby} = e^{-\lambda t}\sum_{i=0}^{N-1}\frac{(\lambda t)^i}{i!} = e^{-\lambda t}\left(1+\lambda t+\frac{(\lambda t)^2}{2}+\cdots+\frac{(\lambda t)^{N-1}}{(N-1)!}\right) \tag{4.23}$$

Identical standby units:

$$MTTF_{standby} = \left(\frac{N}{\lambda}\right) \tag{4.24}$$

with λ = element failure rate
N = number of standby units

These expressions demonstrate the significant increase in reliability and MTTF through standby units. However, the engineer must determine if the sensing, switching and standby startup can be achieved fast enough to prevent a process failure. For example, combustion involving air and fuel flows cannot accommodate a loss of flow for even a few seconds. (For the combustion process, the flame would extinguish, and a resumption of flow would introduce fuel into a hot vessel without a flame, which would be very dangerous.) In this situation upon the failure of a compressor or pump, the startup of a standby unit would require too much time. Since a standby is not possible, the combustion process should be automatically shut down (using a safety instrumented system) when a loss of flow is identified. In many situations, the response does not have to be immediate and a standby system can be very effective.

Naturally, standby equipment can still improve plant performance, since it can replace faulty equipment, even when a disturbance will occur upon the occurrence of a fault. We often use the term "**hot standby**" for equipment that can be placed in operation quickly enough to prevent a disturbance (e.g., a shutdown for switching) and "**cold standby**" for equipment that requires significant time for switching (usually causing some loss of plant performance).

Complex "k out of N" structures: Sometimes, one equipment cannot provide sufficient capacity for the process, so that several are required to function simultaneously. Here, we consider a system requiring "k" elements to be in operation and a total of "N" elements available. Either all of the units are functioning, or some units are in standby and can be started with 100% sensing and switching reliability without delay. Some typical applications of this structure in process plants are given in the following.

- Multiple boiler feed water pumps, where more than one is required to be in operation
- Multiple cells in a cooling tower, where more than one is required to be in operation
- Multiple safety valves on a vessel, where more than one valve must open to fully relieve a high pressure

The expression for the reliability and MTTF for this structure is given in the following (Dhillon, 2005).

Identical k out of N units:

$$R_{k/N} = \sum_{i=k}^{N} \binom{N}{i} R^i (1-R)^{N-i} \tag{4.25}$$

with $\binom{N}{i} = \frac{N!}{(N-i)!i!}$

Identical k out of N units:

$$MTTF_{k/N} = \frac{1}{\lambda} \sum_{i=k}^{N} \frac{1}{i} \tag{4.26}$$

Sample results for a three-element system are given in Figure 4.11. The parallel (1 out of 3) system has the highest reliability, because only one element is required to function. The "2 out of 3" structure has the mid-value of reliability, and the "3 out of 3" or series system has the lowest reliability. Naturally, the reliability of "k out of N" systems can be increased by increasing the total number of elements (N), but this step increases investment and maintenance costs.

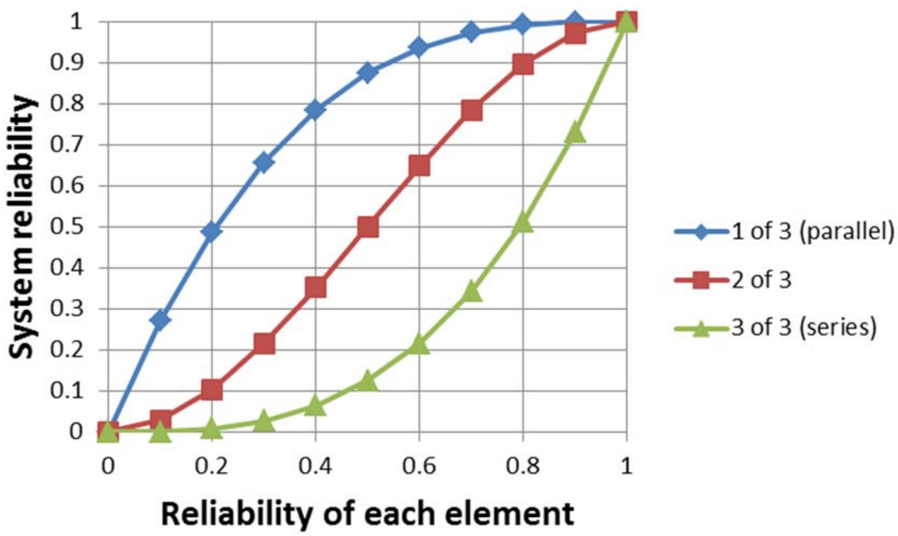


Figure 4.11. Comparison of several three-element systems.

An additional advantage for the parallel and all complex structures is the existence of spare equipment. In addition to the advantage of spare equipment, equipment can be out of service for maintenance. Therefore, no production time or capacity is lost as a result of planned maintenance in complex systems. This maintenance will result in a lower failure rate and longer MTTF for each element in the plant structure.

In this section, various measures of reliability and the effects of various plant structures on reliability have been introduced. The meaning of the terminology is important since it is used in the process industries. In addition, the various complex structures (and others) are applied widely. While the detailed reliability calculations are not often performed by the general (non-specialist) engineer, the understanding of the advantages of each structure is important.

Next, these principles are extended to applications for the process industries. Naturally, every process requires excellent design, operation and maintenance for highly reliable performance. However, to simplify the presentation, these topics are discussed in individual sections on design, operations, inventory, and maintenance.

4.4 Reliability through Plant Design

Good design is critical for achieving reliable plant operation. Major design decisions involve high costs for equipment and process structures that can contribute to high (or low) reliability. After the design has been completed, changes to improve reliability are extremely costly, so there is an economic imperative to "getting it right the first time". There is no checklist for all process plants that ensures high reliability, but there are similar issues and approaches that can be applied to many processes that these are addressed in this section.

4.4.1 Reliability through equipment specification

Equipment must be selected to match the requirements of the process. Certainly, one important aspect is the material of construction, which must be appropriate for the entire range of process environment (composition, pressure, temperature, etc.) experienced during normal and abnormal operation. Some key properties are discussed briefly in the following.

Materials of Construction – The engineer must select the materials for all equipment in the plant.

- Mechanical properties – Equipment must have the strength to not fail at the process pressure, resist wear from flows, not be affected by fluctuating pressures, and so forth. These features should be achieved at the typical process pressures while in contact with potentially reactive process materials.
- Chemical reactivity – Naturally, the equipment materials should be resistant to chemical reactions with the process materials. Corrosion is a cause of longer-term equipment degradation and sudden, catastrophic failure.

Since this topic is covered comprehensively in references, it will not be addressed in detail here, other than to note that proper material selection is required for successful design. Guidance on selecting appropriate materials is available in, for example, Towler and Sinnott (2008) and Peters et. al. (2003).

Example 4.10. Material Selection – In this example, we consider the process shown in Figure 4.12 that removes minerals from city water so that it can be used in a boiler without depositing minerals that would scale the boiler vessel. The schematic is simplified and concentrates on the first stage, the Cation resin reactors. One of the resin reactors has sufficient capacity for the water flow rate, and the second reactor can be regenerated with acid. The piping and manual (block) valves provide for operation of either reactor while the other is being regenerated. We recognize that the resin reactors normally process water, but they also handle strong acid during regeneration. Therefore, we specify that the Cation vessels and associated piping be constructed of material resistant to the acid, perhaps stainless steel or coated carbon steel. Is this adequate?

Before answering this question, you should decide the positions of the manual valves (open or closed) for R-100 in operation and R-101 being regenerated.

The manual valve positions are given in the following

v102	**open**	**v120**	**open**
v104	**open**	**v122**	**closed**
v106	**closed**	**v124**	**open**
v108	**closed**	**v126**	**closed**
v110	**open**		

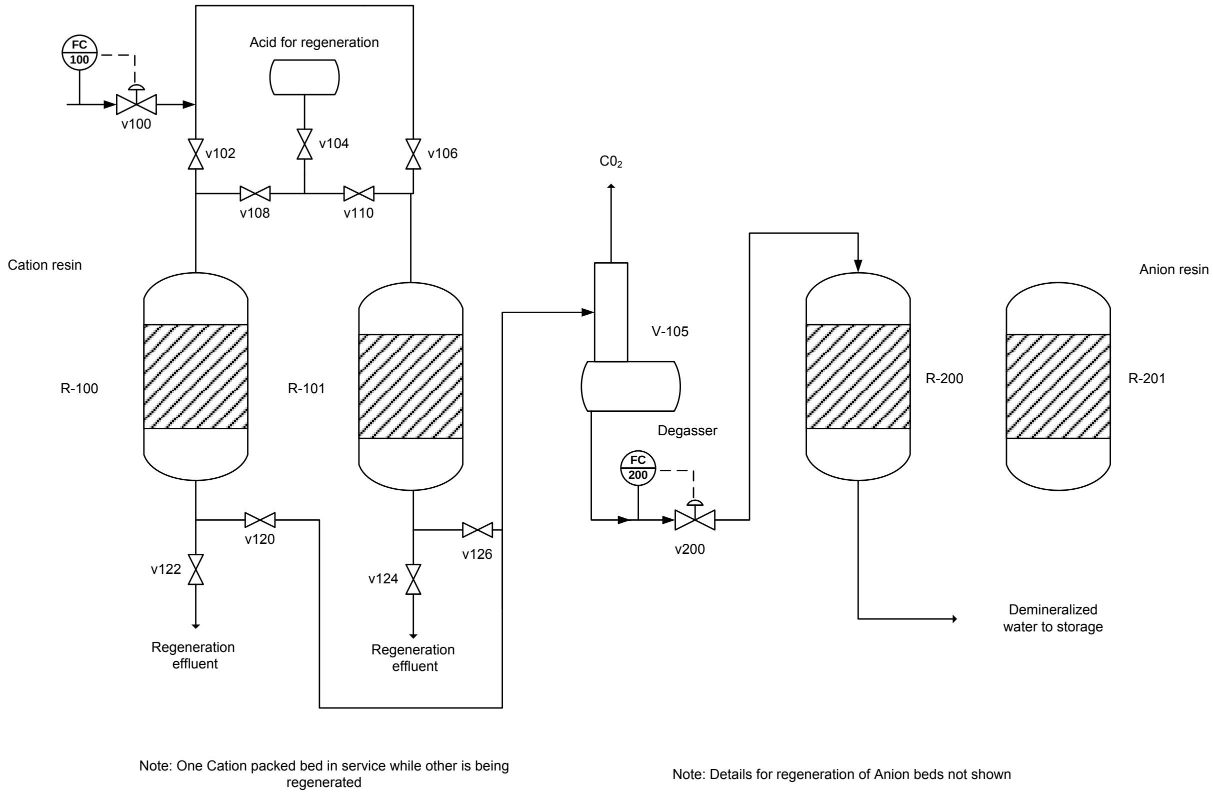


Figure 4.12. Simplified schematic of a demineralization process for boiler feed water.

This approach would provide reliable operation if the plant is operated properly. However, the manual operation of the valves must be correct every time that the Cation reactors are changed from operation to regeneration. If an operator fails to open/close the manual valves correctly, the regeneration acid will flow to the degasser and the Anion reactors. In this situation, the downstream equipment constructed of carbon steel will be severely damaged! Over many regenerations during years of operation, the accident is very likely to occur, and the accident will result in severe equipment damage, high maintenance costs and low plant availability.

Many design modifications are possible to increase the reliability of the process.

- **Construct all equipment of acid-resistant materials, which could be very expensive**
- **Automate the valve operation that would be activated by an operator's command**
- **Install an on-stream pH sensor on the stream entering the degasser with an alarm for high pH**
- **Provide an automatic control that would close all valves allowing flow to the degasser when the pH sensor indicates a high pH. This would be termed a safety-instrumented system (SIS) or interlock system.**

This example demonstrates two important considerations when specifying materials of construction.

First, the engineer must consider not only typical conditions (here, water flowing through the Anion reactors) but also planned atypical conditions (here, acid regeneration). Second, the engineer must also consider abnormal conditions that have a high or moderate likelihood of occurring in the design (here, incorrect manual valve positions that are adjusted frequently).

Match equipment to process conditions – Process equipment functions properly over a range of conditions, so that the engineer must be certain that this range accommodates the expected process conditions experienced during plant operation. It is important that the engineer consider conditions deviating from the base case design, due to new feed compositions, changes in reactor conversions, disturbances and equipment faults. Judgment is required in defining this range; a guideline is that the range must include conditions from which the process should recover and return to normal operation. Also, extreme conditions should not cause excessive damage to equipment or hazards to personnel.

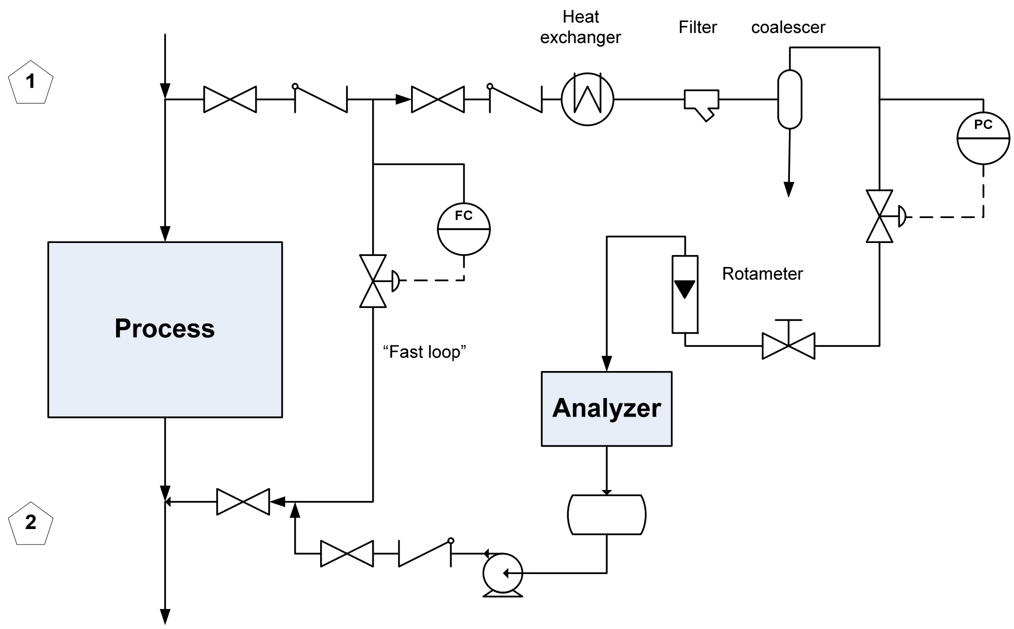
Example 4.11 Analyzer sample system – Often, a complex chemical analysis for quality control requires a sample of the fluid being extracted from the process. The material must be prepared for the chemical analysis and protected from disturbances from undesired components, which might be present infrequently as a result of a process disturbance. Design a sample system for an online analyzer.

Some of the characteristics required for a sample system are described in the following.

- **Dynamics – Some analyzer cannot be located near the sample point because they must be located in complex and expensive shelters that are shared with several other analyzers. Therefore, a "fast loop" is included in the design to reduce transportation delay. The fast loop should have a high flow rate, with only a small sample from the fast loop used for analysis. The fast stream should be returned to the process because the large amount of material should not be wasted.**
- **Flow- The flow rate should be controlled**
- **Pressure - The pressure of the stream should be controlled to prevent a surge in the process pressure from affecting the sensitive analyzer.**
- **Separation - The fluid should be processed to separate material that could damage the sensor or affect the analysis. Typical means of separation include a phase separation to remove an undesired liquid phase, e.g. water, or vapor. Naturally, this separation must not influence the components to be measured by the analyzer.**
- **Temperature - If necessary, the sample stream temperature can be modified with a heat exchanger.**

A typical sample system design is given in Figure 4.13.

The experienced reliability of onstream sensors varies greatly from company to company. One of the factors in achieving high reliability is a well-designed sample system.



Note: Locations of points 1 and 2 in the process must be selected to provide the required pressure drop.
For example, location 1 could be a pump outlet, and location 2 could be the suction of the same pump.

Figure 4.13. Typical on-stream analyzer sample system.

Example 4.12. Sizing pumps – Engineers recognize that uncertainty exists in predicted operating conditions when designing plants. Generally, engineers favor "oversizing" equipment to account for uncertainty. Is this an appropriate strategy?

There is a common misconception that overdesign is always better. Let's consider the selection of a pump capacity. A survey of opportunities for improved motor energy efficiency included motors used as pump drivers (DOE, 1998). The results shown in Figure 4.14 indicate that the greatest improvements exist in the category of "Reduce or Control Pump Speed", which indicates that many pumps are oversized.

The DOE study concentrated on the important aspect of energy efficiency, but the oversized pumps also result in degraded plant reliability. A schematic showing the effects of pump operating region on pump reliability is given in Figure 4.15. At low flow rates, i.e., low compared with the pump best operating region, pump reliability is much lower; therefore, oversizing a pump is not a "safe" approach for equipment selection. At high flow rates, the reliability is also low. There is a "sweet spot" where the pump is highly efficient and highly reliable. Plant design should seek to maximize the time near this best operating point. Note that if the flow rate varies greatly during plant operation, reliable designs can include parallel pumps with different capacities or a single variable-speed pump driver.

Equipment Group/Efficiency Measure	Range of Savings (Percent of System Energy)
Process System Design	
Reduce Overall System Requirements	
•Equalize flow over production cycle using holding tanks.	10%–20%: depends on variation in flow.
•Eliminate bypass loops and other unnecessary flows.	10%–20%: depends on initial system design.
•Increase piping diameter to reduce friction.	5%–20%: depends on initial system design.
•Reduce "safety margins" in design system capacity.	5%–10%
•Reduce system effects due to piping bends.	
Match Pump Size to Load	
•Install parallel systems for highly variable loads.	10%-30%: depends on initial system design.
Reduce or Control Pump Speed	
•Reduce speed for fixed loads: trim impeller, lower gear ratios.	5%–40%: depends on initial system design.
•Replace throttling valves with speed controls to meet variable loads.	5%–50%: depends on initial system design.
Component Purchase	
•Replace typical pump with most efficient model.	1%–2%
•Replace belt drives with direct coupling.	About 1%
•Replace typical motor with most efficient model.	1%–3%
Operation and Maintenance	
•Replace worn impellers, especially in caustic or semi-solid applications.	1%–5%

Figure 4.14. Potential energy savings for pumping (from DOE (1998), pg. 18.)

This analysis leads to a common expression concerning rotating equipment, here applied to pumps, "Pumps don't die; engineers kill them."

The lesson learned from this example is to design the "right-sized" equipment and consider the effects of efficiency and reliability when sizing equipment.

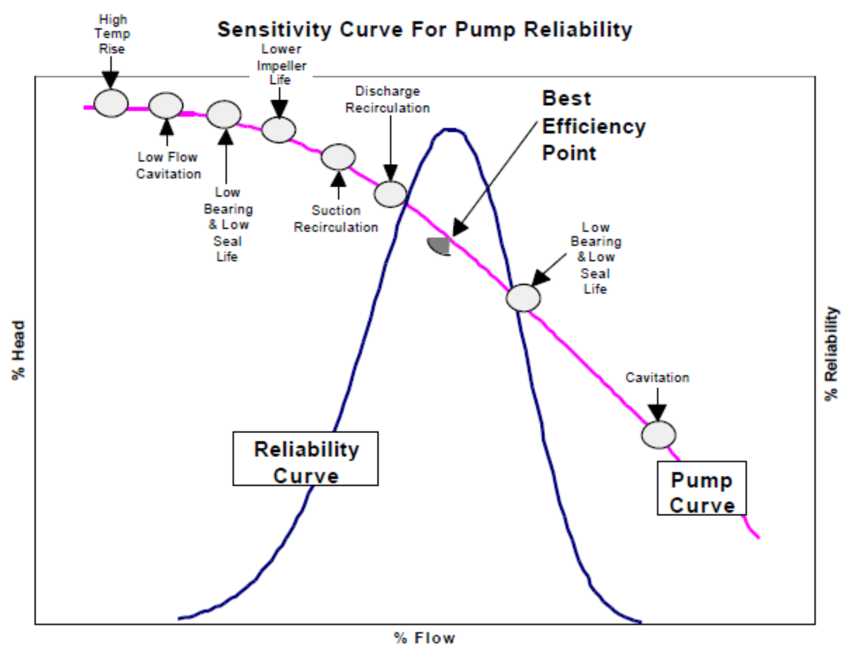


Figure 4.15. Schematic showing the effects of pump sizing on performance and reliability. (from Barringer and Weber (1996))

4.4.2 Reliability through equipment isolation and repair

Even with the best design and operation, equipment fails and must be repaired or replaced. Since a process shutdown is costly, the process should be designed to enable maintenance without shut down for the equipment most likely to fail, i.e., the "weakest links" in the reliability chain. A few of the more common designs are introduced in the following.

- **Control valves –** The stem positions of control valves are continuously moving. As a result, the seal between the stem and valve body wears, and ultimately, the valve leaks. Also, if the seal is too firm, excessive friction could prevent precise stem position response to a change in control signal. Usually, a valve's performance degrades slowly, so that there is time to plan and schedule maintenance. The design in Figure 4.16 is typical for control valves required for normal process operation; this design contains several manually operated valves. Typically, the isolation valves are fully opened and the by-pass valve is closed. When maintenance is performed on the control valve, the isolation valves are closed, and the by-pass valve is opened enough to allow the desired flow rate to pass through the system.

  Caution: Safety-related valves manipulated by automatic shutdown (SIS) systems should not have a bypass. If they had bypasses, the safety barrier could be defeated, leaving the process susceptible to a hazardous condition.

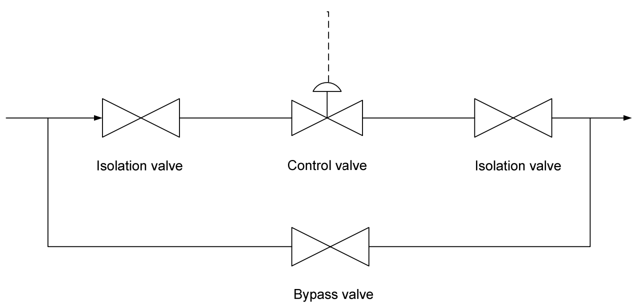


Figure 4.16. Design of a control valve with isolation and bypass manual valves.

- **Heat exchangers –** Heat exchanger performance can degrade due to fouling that reduces the overall heat transfer coefficient; as a result, occasional maintenance to mechanically and chemically clean the surfaces is required. Also, exchangers can develop leaks that must be repaired. Often, the design shown in Figure 4.17 is employed to provide flexibility for maintenance. Isolation and by-pass valves allow the flows to be stopped without stopping plant operation. Naturally, the heat transfer is lost, so the design must consider additional adjustments such as

  (1) replacing the heat transfer with a spare exchanger,
  (2) increasing duties in other heat exchangers in a series of exchangers, or
  (3) reducing production rate so that a desired exit temperature can be achieved.

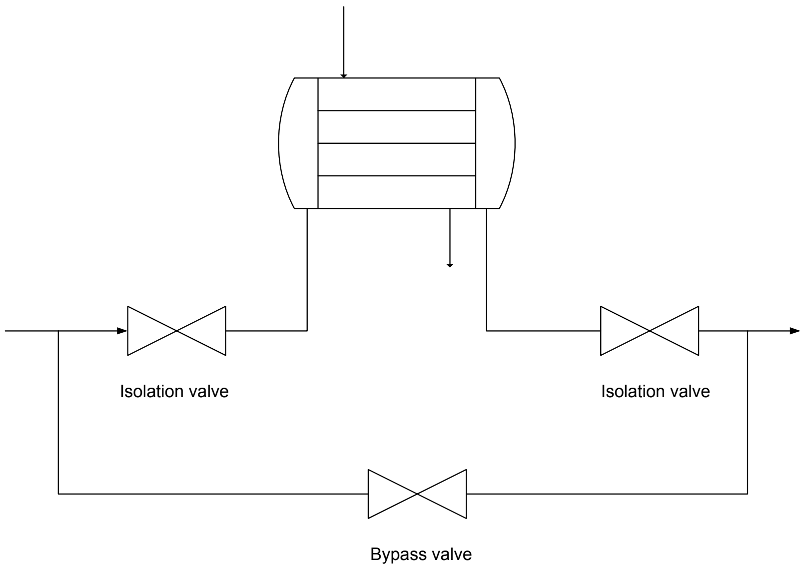


Figure 4.17. Shell and tube heat exchanger with isolation on the tube side.

- **Pumps –** Rotating equipment has a relatively high failure rate because of the components of seals, motor, and coupling. Therefore, parallel pumps are often provided in process plants. A typical design is shown in Figure 4.18. Either (or both) pumps can be in operation, and a single pump can be isolated for repair or replacement. Note that the one-way valves exist to prevent a large backflow when a pump fails; these one-way valves do not provide a "leak-proof" seal, so manual block vales are always provided in series to provide isolation.

  Distillation with two reboilers – Generally, fouling occurs at a slow rate and equipment can be maintained adequately during the annual (or semi-annual) plant shutdown for maintenance. However, there are situations in which the rate of fouling is high, and equipment cannot operate properly for an extended period of time. In such unique cases, the design needs to provide redundant equipment, so that the fouled equipment can be

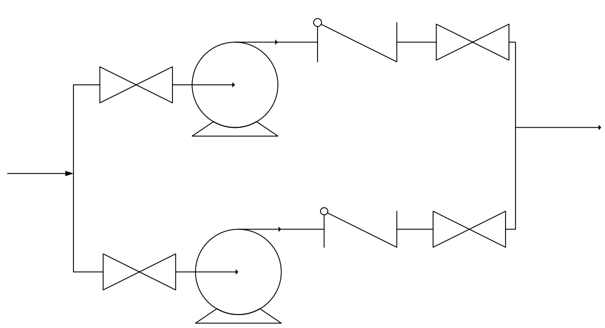


Figure 4.18. Centrifugal pump design with redundancy and isolation

taken out of service and restored to full capacity. An example is a distillation tower in which fouling occurs rapidly in the reboiler. As shown in Figure 4.19, two reboilers would be provided to enable the tower to remain in continuous operation for a year or longer in spite of the short (months) time between exchanger cleaning.

- **Physical layout** – The physical configuration of all equipment must provide space for people and equipment to perform maintenance and repair tasks. The physical layout is facilitated by three-dimensional design software. A good example of equipment needing space is a shell and tube heat exchanger. When fouling has reached an unacceptable amount, the heat exchanger has to be "opened" and people need access to the inner and outer tube surfaces. Therefore, the bundle of tubes must be extracted from the shell. Since a tube bundle is typically 5 to 8 meters long and can be longer (Mukherjee (1998)), a long open space is required to extract the tubes from the shell. In addition, space for machinery to support and move the tube bundle is required. A picture of a tube bundle is shown in Figure 4.20.

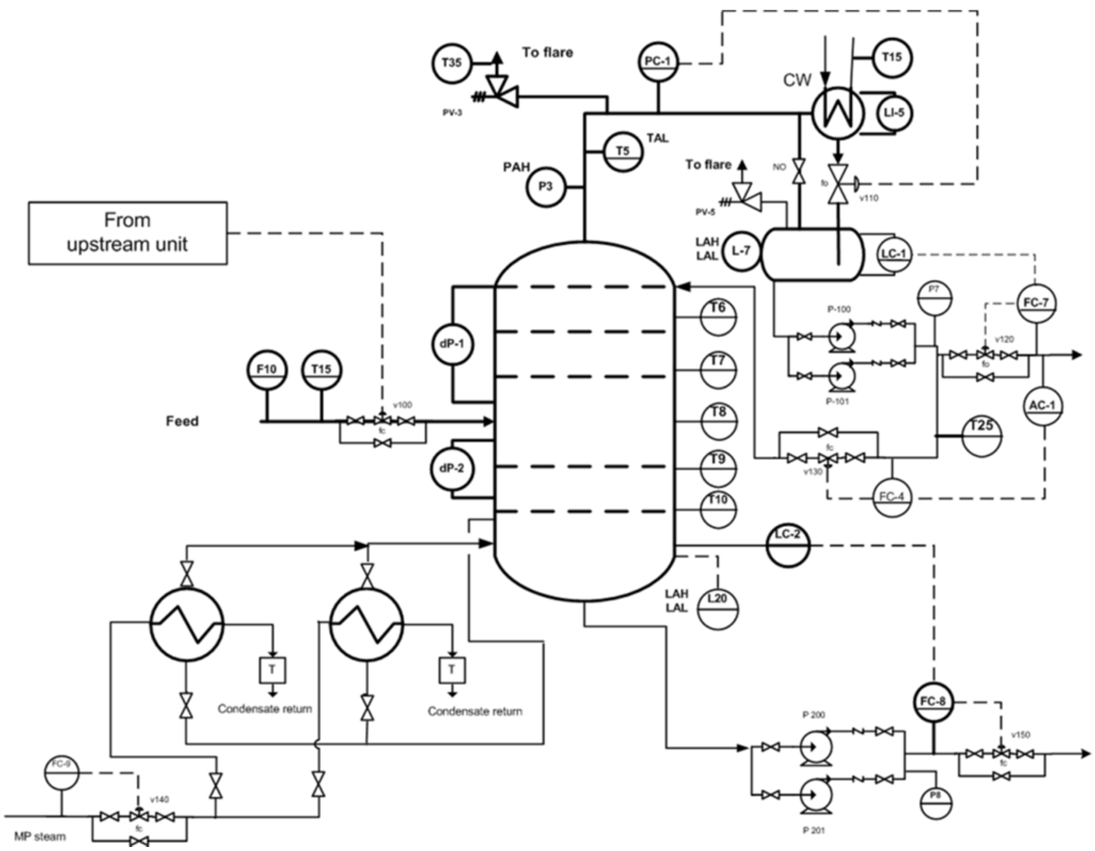


Figure 4.19. Distillation tower with two reboilers to enable cleaning exchanger without requiring shutdown.

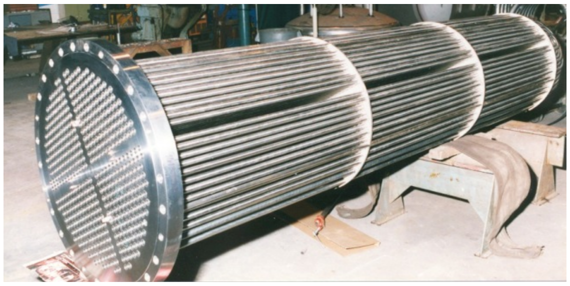


Figure 4.20. Picture of a heat exchanger tube bundle. (SolidsWiki, 2014)

Naturally, we desire to maintain production while some equipment is being repaired or replaced. In the case of by-passing a valve or a pump, a spare is obviously required. Spare equipment is required for other by-passed equipment, such as is a distillation reboiler or condenser. Time is required to replace a failed element, and the full plant production rate can be achieved with a spare of the same capacity as the original equipment.

In some cases, spare equipment is not essential. Some equipment, such as heat exchangers, can be taken out of operation while the plant continues making on-specification products, although production rate might have to be reduced while the equipment is repaired or replaced. It these cases, the decisions to whether include spare equipment or higher capacity equipment to compensate depend on economics.

- **Heat exchanger** - By-passing a heat exchanger reduces the heat transferred to/from a process stream. In some cases, other heat transfer can be adjusted to achieve full production: while in other cases, the production rate must be reduced. As an example, a preheat exchanger network is shown in Figure 4.21; this network recovers process heat to reduce the amount of fuel consumed in the fired heater at the end of the network. One (or more) of the preheat exchangers can be taken out of service, and the preheat network can continue in operation. Whether the production rate (in this case, the flow rate of crude oil) could be maintained at its maximum value would depend on the ability of the fired heater to replace the duty taken out of service.

It is important to recognize that these design decisions are based on economics. As a result, expensive equipment is not duplicated. For example, redundant pumps are common, while redundant compressors are very uncommon. If some expensive equipment has a low reliability, the economic analysis of a potential project must include the lost production and repair costs associated with the anticipated failures in operation.

In this section, we have seen options for increasing reliability through plant design. This theme is continued in the next section, where the effect of process structures on reliability is presented.

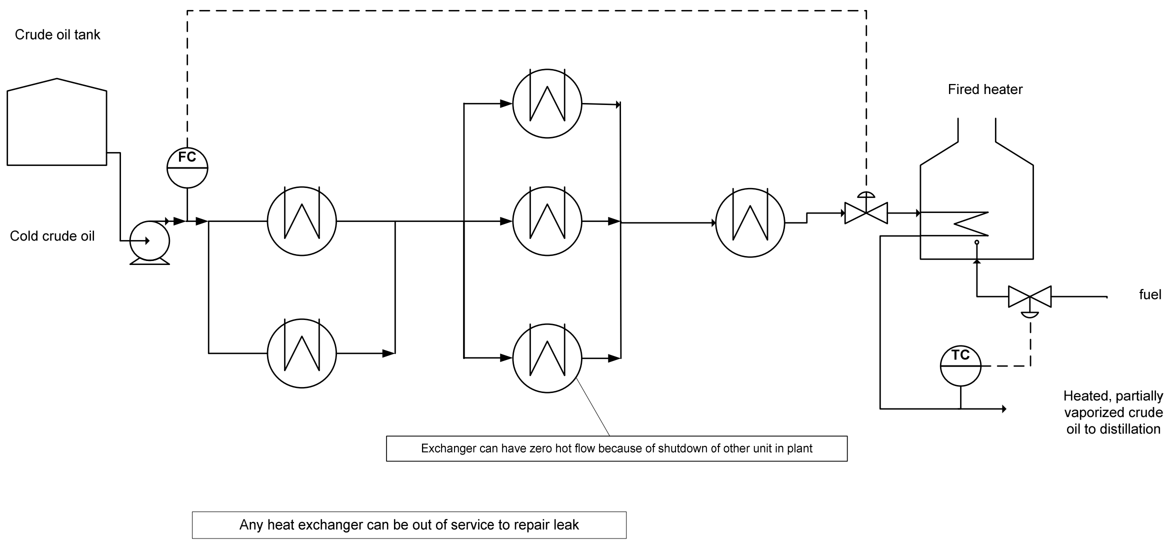


Figure 4.21. Crude oil preheat exchangers and fired heater. (Bypasses on heat exchangers not shown to simplify drawing.)

4.4.3 Reliability through process structure

The important influences of process structure on reliability have already been presented in Section 4.3. In this section, process designs are presented that capitalize on the properties of favorable structures. Where the approach involves additional equipment, the engineer must balance the improved reliability against the increased cost of equipment. Naturally, the economics favor spare equipment for the lower-cost, lower-reliability equipment; the economic analysis method is presented in Section 4.8 on life-cycle analysis.

Redundancy and diversity – The advantage of a redundant, parallel structure is much higher reliability than any of its constituent elements. Diversity involves equipment with different failure root causes. Thus, a design with redundancy and diversity has a much lower likelihood of all parallel equipment failing simultaneously.

Example 4.13. Level measurement – Important process variables are often measured using duplicate (redundant) sensors. To reduce the likelihood of common cause failures, the sensors can be selected to employ different physical principles. How would you select sensors for level in a vessel with a range of one meter?

Large deviations in level can cause several consequences; for high level, a consequence would be liquid flowing to a downstream process that was designed for vapor; for low level, a consequence would be lack of liquid to a pump and vapor flowing to a process designed for liquid. Many methods are available for measuring level, and this solution will use two of the most common, pressure difference and float, which are described in the following.

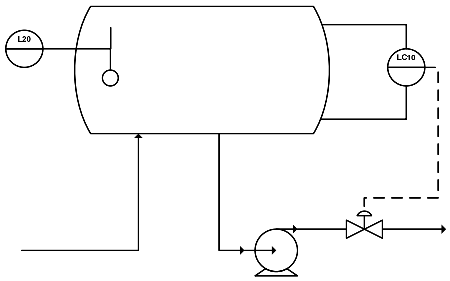


Figure 4.22. Level measurement showing redundancy and diversity.

Sensor type	Sensor principle	Common failure
Pressure difference	**The differential pressure between two locations (taps) is proportional to the product of the liquid height multiplied by its density. This relationship is independent of moderate changes in the vessel pressure**	**The density is not measured and is assumed known and constant. A density change introduces an error between the actual and measured values.**
Level float	**A small empty vessel floats on the liquid interface. The position of the float indicates the liquid level.**	**The float behavior can be influenced by viscous, "sticky" fluid. Also, the float can become corroded and fill with the process liquid.**

The redundant sensors are influenced by different failures, a feature that decreases the likelihood of common-cause failures and increases reliability. In typical designs, the differential pressure sensor is used for control, and the float sensor is used for an alarm. An example of level measurement is shown in Figure 4.22.

Example 4.14. Power to machines - The supply of power to machinery is critical to successful plant operation. The two major sources of power are steam turbines and electrical motors. How can redundancy and diversity principles be applied for pump drivers?

Consider the situation in which steam is the preferred source of power, which would be the case if excess steam from the high-pressure source were available. In this situation, a steam turbine would be provided to power the pump. However, a steam disturbance – perhaps the failure of several boilers simultaneously – could result in a deficiency of steam in the plant. In this situation, the primary pump could be stopped and the secondary pump power by an electrical motor could be started. This design enables the plant to continue operation while a steam deficiency is corrected, which might take significant time. The pump design is shown in Figure 4.23.

Network distribution – Utilities provide important services that are critical for proper operation of an integrated plant. Examples of utilities that are required in the plant include steam, fuel, hydrogen, oxygen, nitrogen, and so forth. For these utility systems, the flow rates to each consumer are adjusted to satisfy product rate requirements, and the utility system must satisfy demands from production equipment. In many designs, multiple sources supply multiple

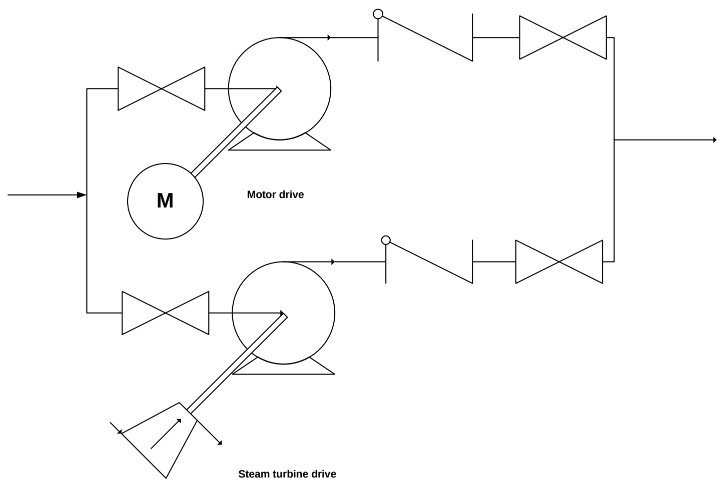


Figure 4.23. Redundant pumps with diversity in power sources.

consumers. To provide high reliability, all sources supply to a distribution network from which all consumers are supplied. This is a special (extreme) example of the bridge structure introduced in Section 4.3.

A steam system is an important example of a utility network. An example is given in Figure 4.24. The system has several pressure levels, termed headers, at conditions needed by various steam consumers for power and heat transfer. Since this is a utility for the plant, the work required by the turbines and the steam consumers and suppliers change continually and cannot be adjusted to aid in operating the steam system: the steam system must satisfy the plant requirements.

The design includes several adjustable variables to enable the steam system to satisfy plant requirements. First, steam is generated at the highest pressure via adjusting the flow rates of fuel to the boilers. Second, turbines T1 and T2 can satisfy their power requirements with steam flows to either a lower steam level or to condensation, and the ratio of these flows can be adjusted to balance steam supply to and consumption in each of the medium and low pressure headers. Third, steam can flow from a high-pressure header to a lower pressure header through adjustable “letdown” pipes labeled 3, 11, and 13. The use of letdowns is to be avoided because of inefficiencies; however, letdowns are needed to ensure that adequate steam can reach all consumers.

The advantage of this design is the shared sources for all consumers, so that consumers do not rely on a single source. While a single source can fail, other sources can increase their production to supply all consumers, as long as the remaining sources have sufficient capacity. The steam system in Figure 4.24 has the following advantages.

- Independent, redundant sources of fuel for the boilers
- Several parallel boilers for redundancy in case of a boiler failure

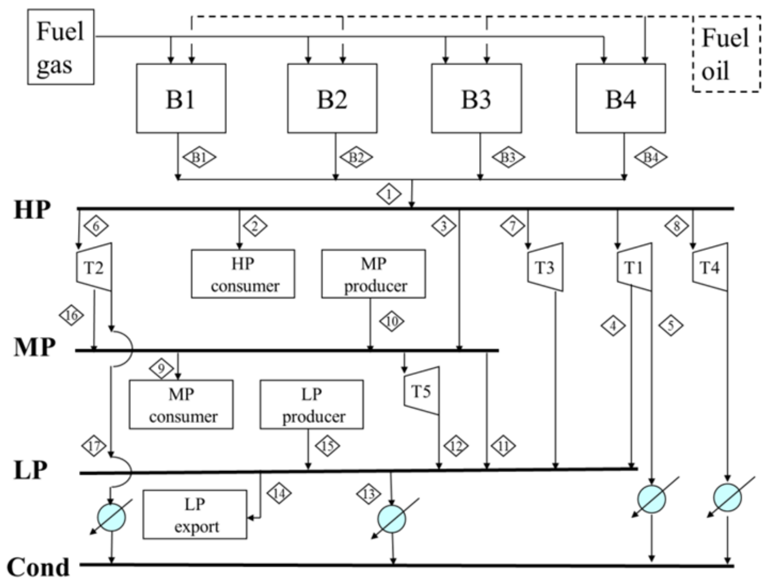


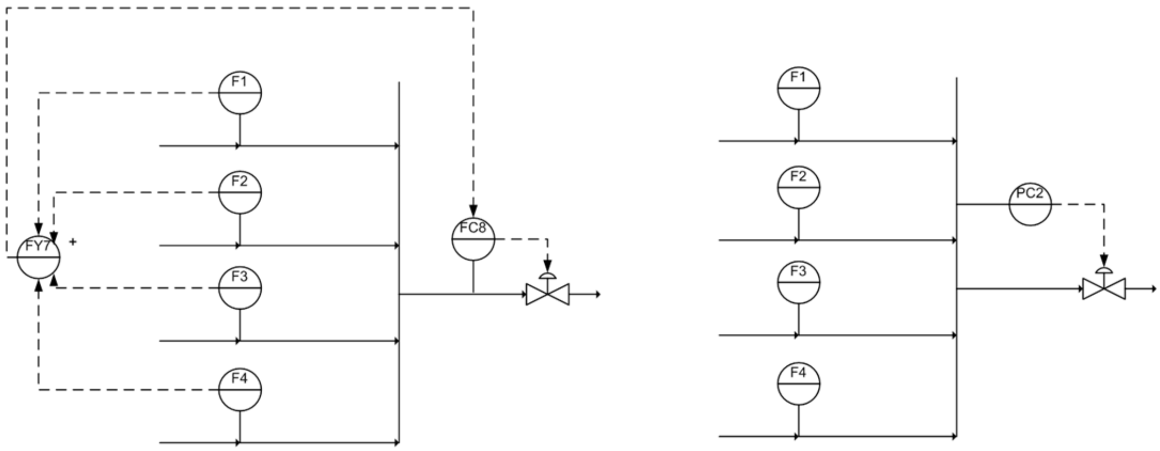
Figure 4.24. Typical steam system in a process plant.

- Adjustable turbine steam extraction and condensation
- Steam letdowns to balance supply and demand, if needed
- All steam from the boilers is "pooled" in the high pressure header that can provide steam to high pressure and lower pressure headers
- A control system is provided to ensure that all plant needs are satisfied by adjusting the boilers steam, the turbine extraction/condensation flows, and steam letdown flows.

The new engineer might find these systems complex, but they operate very reliably and provide the correct amount of steam quickly as the process demands change.

As noted, the proper operation of these networks depends on a process control system that balances the utility steam generation and consumption in each header pipe as both change continuously. The design principle is shown in Figure 4.25a. The approach of equating the generation flows with the independent consumer flows is theoretically correct but impractical. Since the all flow measurements are corrupted by errors, balancing the measurements would not balance the actual flow rates, and with the flows imbalanced, the header pressure would drift. A simpler and practical approach is to control the pressure in the header (pipe), as shown in Figure 4.25b. When the pressure is constant, the flow rates in and out are equal.

Standby of spare equipment – Parallel units provide a higher reliability than an equivalent single unit. In many designs, one unit is in operation and one (or more) parallel unit is in "standby", because of the high cost of maintaining the spare unit in operation for a long time when not needed. Naturally, one important issue is the reliability of the decision making that recognizes the need for starting the standby equipment. Another major issue for standby units is their ability to respond rapidly when needed. Two examples will elucidate these issues and possible designs.



a. Incorrect method because of measurement errors b. Correct method

Figure 4.25. Methods for balancing flows in and out of a pipe.

- **Standby placed in operation via automatic control** - Pressure control is important for maintaining efficient process performance, protecting equipment from damage, and achieving safe operation. The system in Figure 4.26a achieves pressure control under normal operation by adjusting the vapor flow entering the unit, because the flow leaving the unit is set by an upstream controller. When the pressure control valve is fully opened, the controller PC1 is no longer able to regulate the pressure, and a different, standby manipulated variable is required. The design in Figure 4.26b uses a split-range control design to automatically adjust the usual valve (fuel A) or the standby valve (v101) via one feedback PID controller. The design in Figure 4.26c uses two controllers; since two feedback controllers cannot be applied to the same variable with the same set point values, the standby controller has a slightly higher set point. Only when the pressure is above the set point of PC3 (and well above the set point of PC2) does PC3 open the standby valve (fuel B). Both designs successfully implement the standby strategy; the design in Figure 4.26c has a higher reliability because is utilizes an independent pressure sensor, transmitter and controller.

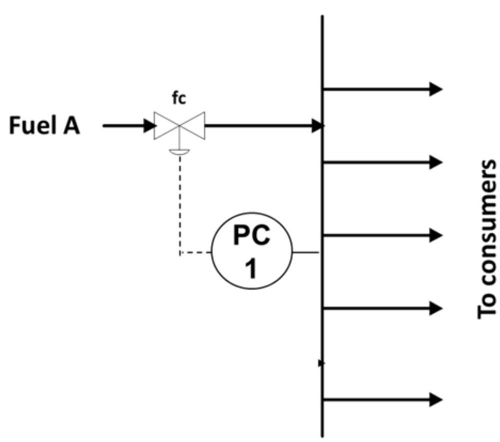


Figure 4.26a. Typical pressure control using one adjustable flow.

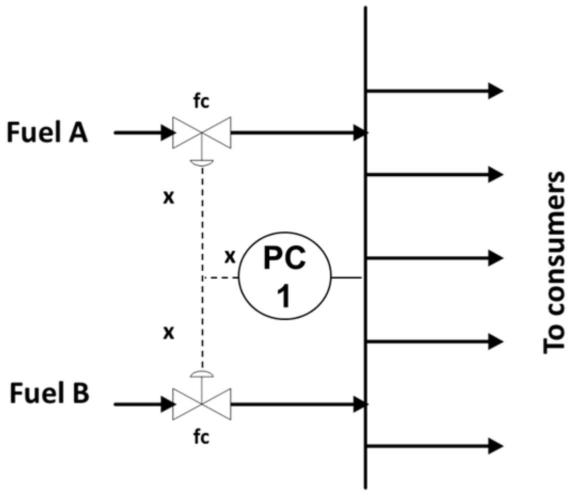


Figure 4.26b. Pressure control with standby valve adjusted by single split-range controller.

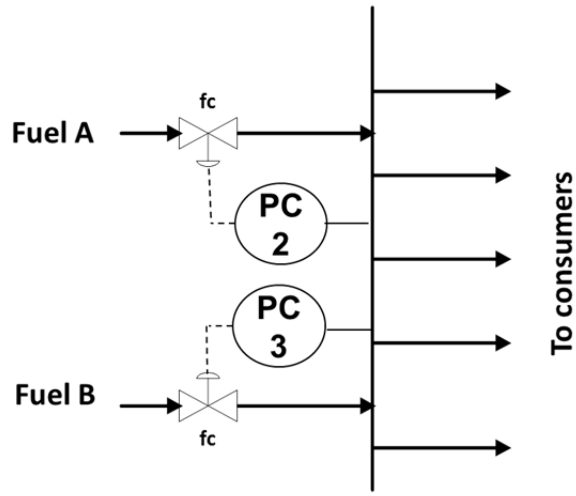


Figure 4.26c. Pressure control with standby valve adjusted by standby controller.

- **Cold/warm/hot standby** – The responsiveness of a standby system depends on the ability of the manipulated process to react to a command. In general, the cost of maintaining the standby process increases as the time to respond is decreased. Let's consider a typical process plant steam generation system in Figure 4.27, where a number of boilers are provided to generate steam. The demand of steam varies continually and can change rapidly as process units change operation. Also, the average value of the steam demand changes with key variables like production rate and weather (season). Since balancing the steam generation and demand is critical for good plant operation, the pressure in the high-pressure header (distribution pipe) is controlled by adjusting fuel to the boilers that are in operation. There are three possibilities for a standby boiler.

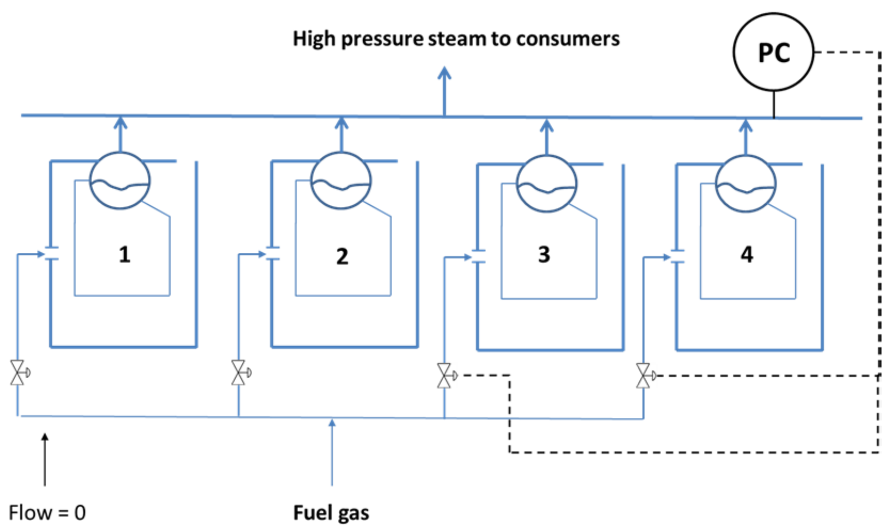


Figure 4.27. Boiler system with two (3 and 4) boilers adjusted automatically, one boiler (2) in hot standby, and one boiler (1) in cold standby.

- **Hot standby –** The boiler has a significant amount of fuel being combusted, the water in the boiler is circulating, and a significant amount of steam is being produced. This boiler can be produce steam in a few minutes. The hot standby boiler can be linked to the header pressure controller to automate the recovery.

- **Warm standby –** The boiler has a low rate of fuel being combusted to warm the water in the boiler drum and tubes. The fuel can be increased slowly to bring this boiler into operation within roughly one hour. Plant operating personnel will be required to adjust the standby boilers operation until it can be connected to the pressure control.

- **Cold standby –** This boiler is at ambient temperature, and no fuel is being combusted. The equipment must be heated slowly, and several hours will be required to place the boiler into operation. Bringing a cold boiler in service requires considerable time of the plant operating personnel.

The choice of standby depends upon the cost for lost steam production when one of the operating boilers experiences a fault and shuts down. In many process plants, the cost is high because part of the plant would have to been shut down. Therefore, a structure is required that provides nearly immediate compensation for a boiler failure. For example, rather than having two boilers at 90% of their capacity, the plant can be operated with three boilers at 60% of their capacity. In this parallel process structure, the desired steam production can be achieved very quickly upon the failure of one boiler.

However, if the boilers generate steam for heating buildings the cost for reducing steam production for a short time is not high, and the standby boiler can be operated in warm standby mode. The desired steam generation rate can be resumed within about one hour, which would not severely affect building heating. While some boilers might be in cold standby, having all standby boilers in the cold mode would be unusual because of the long time required to activate a cold boiler.

Standby systems are very similar to parallel systems. In a standby system, the redundant equipment is not in continuous operation; in a parallel system, the redundant equipment is in operation. The advantages and disadvantages of the standby system are summarized in the following.

- **Advantages** of standby compared with parallel
  - There is less wear on the redundant equipment, which would lengthen its life and improve its reliability
  - The equipment in operation can be designed to operate at its peak performance
- **Disadvantages** of standby compared with parallel
  - The measurement and switching equipment must be reliable and decreases the reliability of standby system
  - The standby system should reach full capacity rapidly, which might not be possible in all cases

Recycle systems to prevent total plant shutdown – When equipment is taken out of operation for unplanned repair or replacement, plant personnel must decide the correct policy for the remainder of the plant. If the repair of the failed equipment will require a long time, the remainder of the plant may have to be shut down. If the repair of the failed equipment can be completed in a short time, there are advantages for maintaining the remainder of the equipment in operation, namely, safety (many accidents occur during startup and shutdowns), extended equipment life (heating and cooling equipment introduces stress that lowers life), and production (quick recovery after repairs have been completed). Note that the advantage comes from reducing the MTTR, since "repair" includes the time to restore the full plant to operation.

We seek to maintain equipment in operation that is not directly affected by the fault. One approach is to introduce recycle, with the recycle used only when required to maintain the process near normal operation during repairs. The concept is shown in the schematic in Figure 4.28. When process unit 4 fails and must be taken out of service, the recycle on materials enables processes 1 to 3 to remain at near-normal operating conditions.

Recycle is used to reduce the adverse effects of an equipment failure when the following criteria are satisfied.

- Storage of materials is not possible or available
- Shutdown and startup of equipment requires a long time compared with the time to repair the failed process.
- The units can be operated safely in recycle without damage or production of large quantities of useless process materials (intermediate products)

Note that an alternative approach for maintaining operation involves diverting intermediate products to storage, which is addressed in Section 4.6.

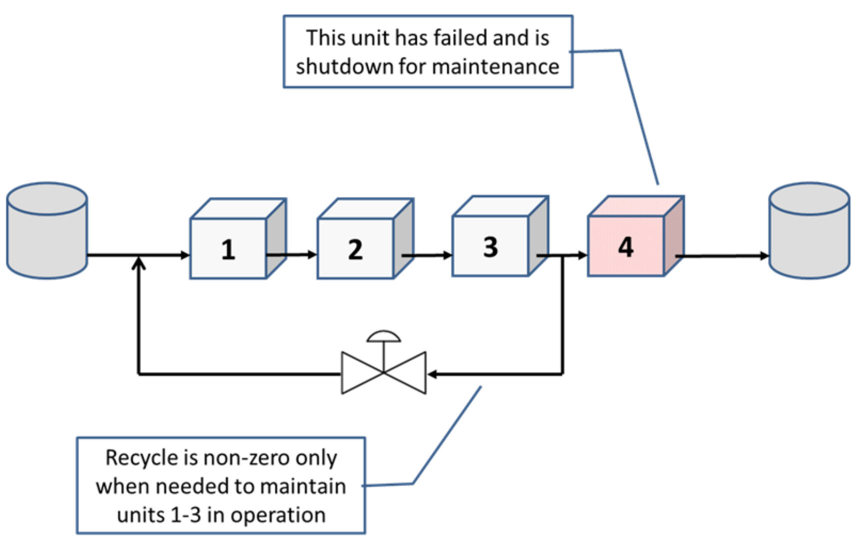


Figure 4.28. Schematic of recycle used to maintain some equipment in operation during a partial shutdown

Naturally, reliable plant performance requires more than purchasing and installing the proper equipment. This equipment must be operated in a manner that increases reliability. This section introduced design decisions that improved reliability. The next section addresses proper operation procedures.

Example 4.15 – Redundant pumps – A plant has decided that redundant pumps are appropriate for a plant design; the basic design is given in Figure 4.18 with electric motors powering both pumps. Present options for the operation of the redundant pumps.

The options are given in the following, with the first three being standby designs and the fourth being parallel redundancy.

Option	Startup second pump	Isolation valves	advantages	disadvantages
Local manual	Manual action located at pump to start standby	manual	Low cost	Long time required to start backup
Remote manual	Manual operation in control center to start standby	Remote operated valves activated from control center	Faster startup	Higher cost
Automatic startup	Automatic based on low pressure measured at outlet of pumps	Always open (one-way valves prevent recirculation)	Very fast startup	Higher cost Not instantaneous startup
Both in operation	Both in operation at all times	Always open (one-way valves prevent recirculation)	No loss of flow upon failure of one pump, but very short drop	Higher energy Potential loss of reliability for operating away from best efficiency point on each pump (See Example 4.12) Both pumps experiencing wear all of the time.

4.5 Reliability through Plant Operations

Plant operations can have a strong impact on plant reliability. The basic approach in proper operations is to avoid conditions that unduly lower the reliability of the plant equipment. We include the modifier "unduly" because severe normal operating conditions often reduce the reliability of equipment, but these conditions are required for profitable production. Examples include heat exchanger fouling and catalyst deactivation that occur slowly during normal process operations. To ensure reliable operation, the engineer must select the appropriate operating conditions that provide safe operation and a proper balance of profit and slow equipment degradation. In addition, the engineer must define policies and implement automatic process control to avoid excursions from the defined acceptable range of operating conditions into regions that reduce reliability. This section begins with a presentation of operating policies for reliability; then, it proceeds to cover automatic process control for reliability.

4.5.1 Operating policy for reliability

By “operating policies”, we mean strategies devised by engineers that achieve all safety, production rate and product quality goals in a profitable manner and in addition, lead to high reliability.

- **Even wear** – We have seen the value of parallel process structures for high reliability. For example, the common design with two parallel pumps when only one is needed. In these situations, the engineer must decide which of the parallel equipment are placed in service. Generally, the decision is to operate the pumps so that they operate the same percentage of the time each year. This ensures that the spare pump has been functioning well recently, which increases the likelihood that it will function if the primary pump fails.
- **Manage inventories** – Material inventories can strongly affect the reliability of a process plant by enabling some units to operate while one unit is being repaired. This important topic involves both design and operations issues, which are both addressed in the next section in this chapter.
- **Operations that balance short-term and long-term effects** – Many operations decisions are challenging to make correctly because the overall plant performance involves short-term and long-term effects. The best operating policy must find the proper balance, which is usually evaluated using economic analysis because the time-value of money accounts for advantages (profits) and disadvantages (losses) occurring at different times. Here, we will discuss typical decisions in process plants and the important factors influencing the proper decisions. In a later section in this chapter, the “life-cycle” economic analysis will be explained, and this economic formulation would be appropriate for quantitatively evaluating these decisions.

Example 4.16. - The best steam superheat temperature. In electrical power generation plants generating steam, the saturated high-pressure steam is further heated, i.e., superheated, to increase the efficiency of the power cycle. How is the superheated steam temperature selected?

In general, a higher the temperature yields higher plant efficiency. However, the allowable steam temperature is limited by turbine blade materials. If the superheated steam temperature entering the turbine is too high, the turbine blades will experience long-term damage that will result in failures, and a blade failure will damage the equipment, could injure plant personnel, and result in a long time for repair. Therefore, the strategy is generally to operate near the maximum without violating the maximum. Some plant data is shown in Figure 4.29 for an industrial, coal-fired power plant (Longman, 1988). The initial data (first 12 days) was about as high as the steam temperature could achieve with very limited constraint violations. The second one-day region showed the effect of raising the average temperature; the number of constraint violations, here indicated as alarms, increased dramatically. Even though the turbine efficiency was higher, the second region of operation was deemed to be unacceptable because the reliability of the turbine would be

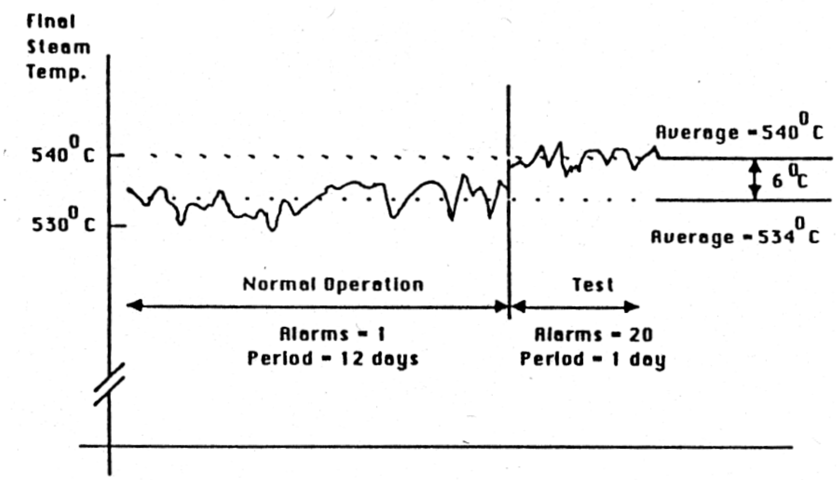


Figure 4.29. Trend plot of superheated steam temperature inlet to turbine (Longman, 1988).

adversely affected. Based on this analysis, the plant must operate in the initial region, unless reduced steam temperature variability through process control can allow an increase in average temperature without concurrently increasing violations.

Example 4.17 The cost of change – Electrical utility companies must balance generation with power demand. As the demand changes, it becomes necessary to start and shutdown individual generating units. What is the effect of this "cycling" on the reliability of the equipment?

Cycling equipment operated at high temperatures and pressures can significantly affect equipment and reduce its reliability. Combined cycle gas turbine (GTCC) power plants are faster than drum boiler plants to start up, so they are generally the units that are adjusted more frequently by power companies to manage the grid. The GTCC plant includes a gas turbine, usually firing natural gas, and a heat recovery section that generates steam. Power is generated by both the gas turbine and steam turbine(s). A schematic of a GTCC plant is shown in Figure 4.30.

The utility needs to balance the cost of startup/shutdown with the cost of maintaining a unit in operation at a low efficiency between periods of use. Maintaining the unit at low power generation (and lower efficiency) results in higher fuel costs. Each startup/shutdown degrades the equipment and results in lower reliability, as demonstrated by a study of twenty years operation of many GTCC power plants (EPRI, 2004) that demonstrates a substantially lower reliability for plants that cycle when compared with plants that have a more constant base load. However, the lower reliability is not immediately apparent, which leads an underestimation of the effects of cycling. Often, companies estimate the cost of lower reliability, due to increased repairs and hours of plant operation, to be 100 to 200 \$/cycle (Lefton et. al., 2006; Lefton et. al., 2012). However, a thorough analysis of historical data indicates a cost of approximately \$6800/cycle for shutdown/startup of the heat recovery section (Camp and Vandergriff, 2004) and over twice that cost for the entire unit (Lefton et. al., 20012). Clearly, this high cost of cycling should lead to fewer shutdown/startup cycles, if the proper economic values are used.

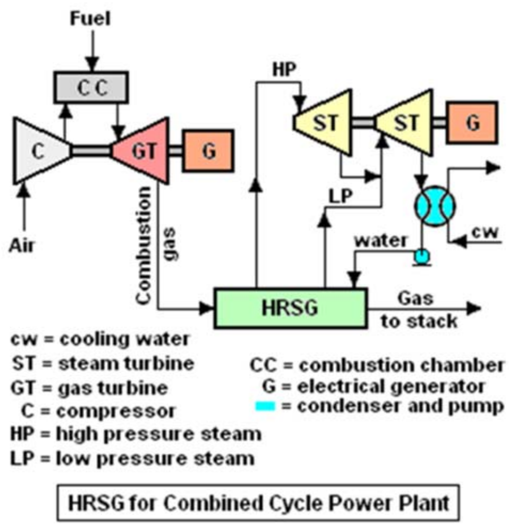


Figure 4.30. Schematic of a gas turbine combined cycle power plant (Beychok, 2009).

4.5.2 Process automation for reliability

As previously explained, preventing excursions into undesirable regions of operating conditions improves reliability by preventing equipment damage and production of off-specification materials. In the previous section, operating policies were discussed. These policies could the considered to be plans that will be achieved in the best conditions, for example, no disturbances, no equipment faults, and no human error. In this section, we will consider automation approaches to provide much greater assurance of remaining in an acceptable operating window when challenges occur. We must recognize that we cannot eliminate the possibility of excursions to undesirable conditions, but we can substantially reduce the likelihood and increase the average reliability.

Generally, we achieve high reliability by a "systems approach" that does not rely on one feature (or layer) of the design to provide an adequate barrier from the undesired conditions. Plant designs include several layers of protection that provide "strength in reserve". Only when all layers fail can the process reach the undesired condition. Since the protective layers are designed to be independent, the probability of all failing should be low and the reliability should be high.

Layers of protection - An example of the typical layers of protection are given in Figure 4.31 and are discussed briefly in the following.

- **BPCS** – The basic process control system (BPCS) is implemented with highly reliable computing and instrumentation equipment to enforce operating policies through feedback control principles. All engineers have some background in process control and appreciate the importance of the rapid, dependable responses of the feedback system to disturbances. Further details on process control for operability are provided in Chapter 6.

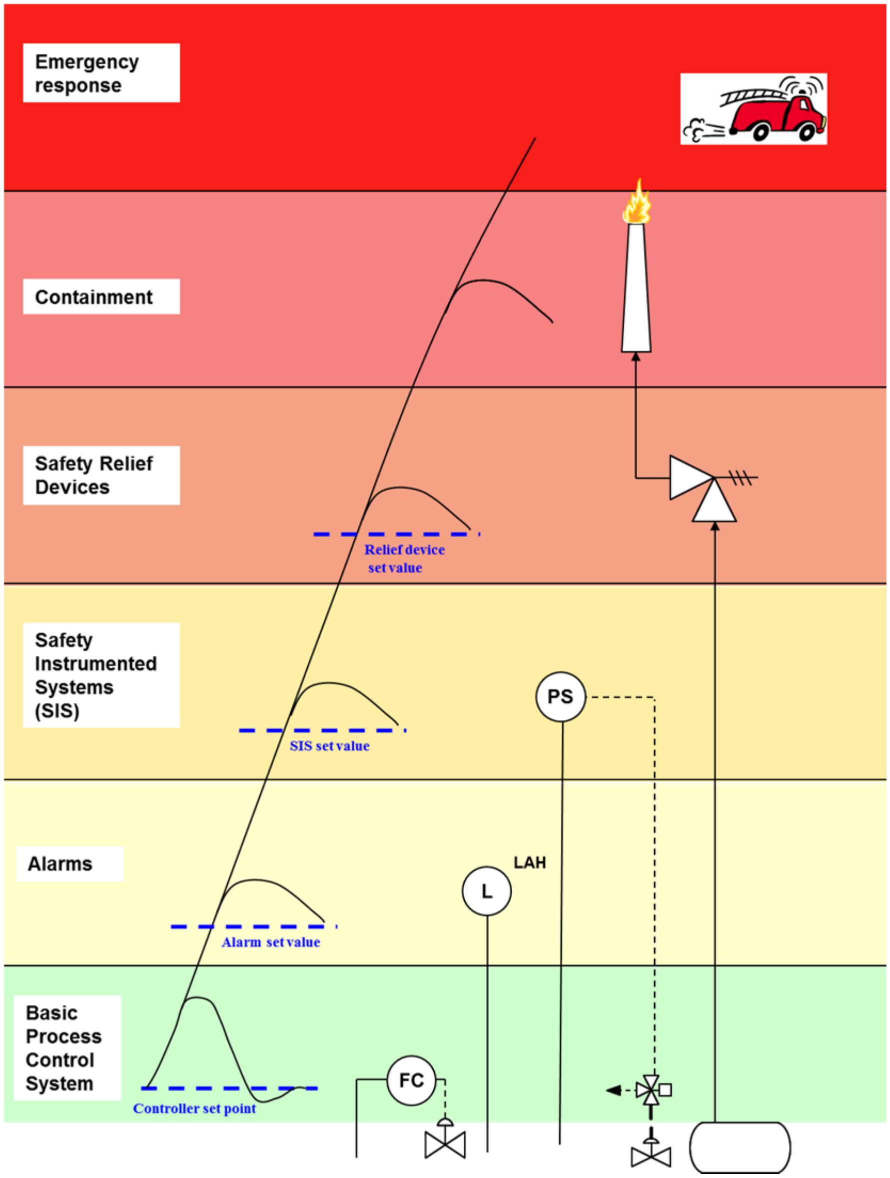


Figure 4.31. Schematic of the layers of control for safety and reliability.

- **Alarms**- Some operating conditions are not immediately dangerous or costly, but when they occur, the plant operating personnel should monitor the situation closely, diagnose potential causes, and be ready to intervene, if required. Therefore, process plants have many alarms that serve to highlight problematic situations. No actions are automated by alarms; people must monitor, decide and act.
- **SIS** – When a condition is recognized that can cause hazards or severe economic loss (e.g., damage to equipment) extreme actions may be required. These actions are referred to as safety instrumented systems (SIS). A typical action is to shut down some equipment, which stops plant production. Naturally, this action is costly, but the cost of the action is lower than the damage likely if the action is not taken. These actions must

be implemented rapidly and in a specific manner; therefore, SIS designs involve automatic control through computing and instrumentation.

- **Pressure relief –** Any vessel that could be closed, through deliberate or inadvertent actions, must have pressure relief. Usually, relief prevents high pressures, but it can also prevent low pressures that could damage a vessel. Thus, a design must prevent pressure deviations from a safe range accounted for in the equipment specification and manufacture. The typical approach is a relief valve (or burst diaphragm) that opens a path for flow when the safe pressure range has been violated. These devices are "self actuating", i.e., no computing or external power are required for automatic, rapid operation.

These protection layers are also applied to prevent hazardous conditions from occurring. To prevent excessive duplication in this learning material, details on these layers of protection are provided in Chapter 5 on Safety. However, a few examples of applications for reliability are presented here.

Example 4.18. Compressor surge – Compressors are important, expensive equipment used in process plants for gas flow and refrigeration systems. A typical relationship between the flow through the compressor and the pressure rise across the compressor (head) is shown in Figure 4.32. We note that the allowable region of operation lies to the right of the dashed line marked as "Surge Boundary". To the left of the line, a compressor experiences unstable flow that can result in reverse flow that seriously damages the blades; therefore, operation in this region designated by surge is to be absolutely avoided. The specific details for any compressor are defined in the figure (or "map") provided by the manufacturer of the compressor. How is operation in the surge region avoided?

Automatic process control is employed to avoid operation in the surge region because of the rapid damage done by reverse flow. The most basic form of anti-surge protection is a minimum flow controller shown in Figure 4.32 as FC that has the minimum acceptable flow rate (plus some safety margin) as its step point. When the feed flow rate to the compressor decreases below the minimum flow rate required to prevent surge, the surge flow controller (FC) immediately determines that its measurement is below its set point. In response, the feedback controller opens the recycle valve sufficiently to maintain the flow through the compressor above the surge value. More reliable protection and higher energy efficiency are possible with more advanced approaches, e.g., White and Kurz (2006) and Staroselsky and Ladin (1979).

Example 4.19. Boiler level – A circulation drum boiler contains a reservoir of water in a drum, and the water circulates by natural convection through many tubes where heat exchange occurs and the water is partially vaporized. A schematic of a boiler is given in Figure 4.33. A continuous flow of water through the tubes is essential; if the water flow were to stop, the tube metal temperature would quickly rise, and the tubes would be damaged. What features are required to prevent damage due to no water circulation?

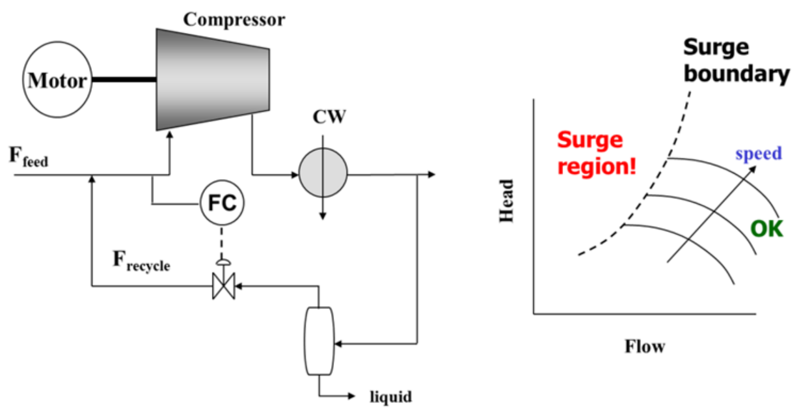


Figure 4.32. Compressor process and flow-head map. Surge is prevented by the anti-surge, minimum flow controller **FC**.

To ensure water flow, the reservoir in the drum must not be depleted. Therefore, a basic process control system (BPCS) controls the drum level by adjusting the flow of water to the drum. In addition, an alarm is included to warn the operating personnel when the level reaches a low threshold value. A third layer for reliability involves the Safety Instrumented System (SIS) that stops the fuel combustion (the fuel flow by closing two valves) when the level measurement indicates an unacceptably low level. Finally, a safety valve is installed on the steam line leaving the drum to prevent excessive pressures, i.e., pressures above the equipment pressure rating. We see that this simple process requires all four layer of protection to achieve acceptable reliability (and safety). Each of the four layers relies on independent equipment to improve the ability to respond to a disturbance.

- **Life-extending control** – Generally, engineers seek to design and implement control systems that introduce rapid corrections to minimize the deviation of the controlled variable from its set point. However, we should always consider the behavior of all variables when determining the best dynamic response for the equipment. For some equipment high rates of change can result in damage that can accumulate over months or years and lead to equipment failure. A few examples are presented in the following.

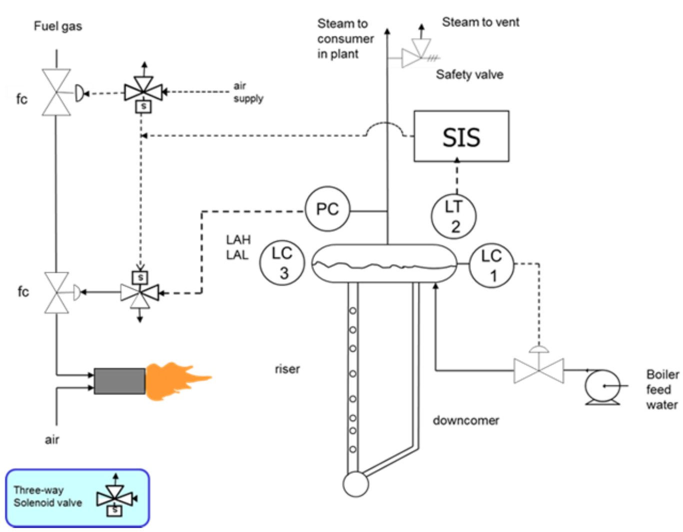


Figure 4.33. Boiler drum with four layers of protection for reliability (and safety)

- Unnecessary high-frequency **f**uel fluctuations to combustion processes that lead to stresses in equipment that shorten equipment life
- Unnecessary high-frequency distillation reboiler heating-medium flow fluctuations that cause pressure fluctuations that result in tray damage
- Unnecessary high-frequency speed fluctuations in rotating equipment (variable speed pumps and compressors)

Often, good performance requires a balance between variances in the controlled and manipulated variables. Often, this requirement is achieved by proper tuning of conventional PID controllers. An example that compares PID tunings for life-extending control of a process fired heater is presented in Appendix A.

Some advanced Life-extending control approaches require novel control algorithms, e.g., Li et. al. (2006), that moderate high stress conditions in real-time. The methods include models of the process and the potential damage caused by manipulated variable fluctuation and an algorithm to balance the behaviors of controlled and manipulated variables.

Therefore process control should be implemented in a manner that balances the need to remain close to the set point with the need to operate equipment for long times without damage.

Finally, this section (4.5) addressed reliability through good process operation via operating policies and automation. We must recognize that excellent operation relies on the right equipment with required capacity and flexibility being included in the design. Good operations complements good design, but good operations cannot compensate for poor design. In the same manner, a good design cannot ensure reliability; it must be complemented by good plant operations.

4.6 Reliability through Plant Inventory

An essential aspect of reliable plant performance is the management of material flow rates and inventories. Naturally, the continuous flows through the plant must be maintained within acceptable limits for all equipment. A lower limit defines the "turn-down" for the equipment; the turn-down limit varies greatly for various process equipment; typically, it is around 70 percent of design flow for more complex units. The maximum flow rate is usually slightly above the design flow because of the safety factors included in equipment sizing; however, greater maximum flows can be achieved if anticipated during the equipment design.

In addition, material is stored in feed, product, and intermediate inventories, and these inventories should never be empty – to enable flows out to continue – nor be completely full – to prevent spillage that could cause hazards and environmental damage. Here, we will concentrate on liquid inventories; however, the insights and methods apply as well to gases and solids.

Inventories allow for imbalance between flows in and out for a limited period of time by accumulating the difference in the storage vessel. This imbalance can affect the reliability of integrated process units in a plant. The reliability topic addressing plant inventory spans both design and operations. Therefore, it is presented here as a separate section. Before addressing reliability, we begin with a short discourse on principles of process inventory.

4.6.1 Principles of process inventory

Inventories are located throughout a process plant, and the following gives examples of process inventories.

- Feed and product tanks
- Intermediate tanks
- Distillation trays
- Distillation condenser & reflux drum
- Distillation bottoms accumulation & reboiler
- Fired heater, fluid in pipes
- Heat exchanger: shell and tube sides
- Chemical reactor: stirred tank, tubular, packed bed, fluidized, and so forth
- Pumps and piping
- Vapor compression refrigeration: liquid refrigerant
- Fuel storage

Note that most process inventories are not addressed in a steady-state flowsheet of a continuous process, because the size of the inventory does not affect the steady-state behavior of the plant. One exception is the volume of a chemical reactor that is specifically accounted for because of its effect on reactor performance in the steady-state. The storage inventories influence dynamic behaviors that are very important, in fact essential, for good plant performance, but these behaviors are not captured by the steady-state model.

Therefore, engineers must use methods and calculations beyond steady-state flowsheeting to determine the location and capacity of inventories.

During plant design, the engineer must be aware of the advantages and disadvantages of process inventories. Some of the common advantages and disadvantages of inventories located in plants are summarized in Tables 4.1 and 4.2, respectively. Inventories accommodate periodic delivery of raw materials and dispatch of products, enable smooth flows throughout the plant, and provide residence time for chemical reactions. These advantages are important, so that process inventories are essential for the successful operation of nearly all process plants.

Table 4.1. Reasons for Inventories in Process Plants

Reason for inventory	Process examples
Required for process performance	• Provide continuous flow of liquid to pumps • Residence time for chemical reactors • Provide environment to achieve vapor-liquid equilibrium, e.g., liquid on each tray of distillation column • Store materials between series batch-batch and batch-continuous plant structures
Mixing to reduce effects of stream property variation	• Feed drum to distillation tower or chemical reactor
Flow rate modulation	• Control level by adjusting one flow using averaging level control (See Chapter 6) • For large storage vessels, set both flows in and out constant for long periods of time, allowing inventory to vary
Allow periodic feed delivery and product dispatch	• Feed inventory used to segregate different feed materials and to allow periodic delivery with constant feed rate to plant • Product inventory used to segregate different product materials and to allow periodic dispatch to customers with constant production rate from plant
Isolate different materials for multi-product, flexible manufacturing	• Store intermediate products for subsequent processing in downstream equipment, with isolation of materials required for different final products
Capture materials during unusual operation	• Store material that is off-specification made during startup, shut down, or upsets for recycle to process • Store materials for processing to benign components and release to the environment
Increase reliability	• Maintain partial plant operation when one unit in shutdown, either intentionally or unintentionally • Continue plant operation when raw materials delivery or product dispatch does not meet schedule

Table 4.2 Negative Aspects of Inventory

Negative aspect	Process examples
Hazards	• Combustible materials, e.g., crude oil, gasoline, • Toxic materials • Pressure vessels
Product quality degradation	• Over time, e.g., food, pharmaceuticals, even liquid fuels
Space in plant	• Space can be very costly in some locations
Capital cost	• Vessel and piping costs • Additional costs for inert blanking and other special needs
Working capital cost	• Stored materials are work-in-progress and handled as working capital
Operating costs	• Heating or refrigeration is required for storage at temperatures different from ambient temperature
Slow plant dynamics	• Longer time to change product quality when switching operations

The disadvantages are equally important. Large inventories of hazardous material have led to catastrophic accidents, such as Bhopal (Lees, 1996; Mitchell, 1996) and Seveso (Mitchell, 1996). As a result, current design guidelines require limited inventories of hazardous materials (AIChE, 1993). In addition, costs for inventory can be high. For example, an installed 50,000 barrel (~ 8000 cubic meters) crude oil storage tank would cost about 1.0 ± 20 M$ (Loh et. al., 2002; Matches, 2014), and with the cost of crude at $100 per barrel, the cost of working capital for the stored oil would be 5 M$. A petroleum refinery would have many such feed storage tanks!

Therefore, the engineer must find a balance of advantages and disadvantages by locating and sizing the inventories appropriately.

Before addressing the inventory design, we will quickly review the dynamic behavior of inventory processes. By applying an overall material balance, the dynamic model for a single inventory can be derived as shown in the following.

$$\textit{Accumulation of mass} = \textit{mass flow in} - \textit{mass flow out} \tag{4.27}$$

$$(\rho V \Delta t)_{t+\Delta t} - (\rho V \Delta t)_t = \rho F_{in} \Delta t - \rho F_{out} \Delta t$$

with

- F = volumetric flow rate
- V = volume in material in inventory
- t = time
- ρ = density of material in inventory

Assume for simplicity that density (ρ) is constant, and divide by Δt, and take the limit as $\Delta t \to \infty$. The result is the following dynamic model of the inventory.

$$\frac{dV}{dt} = F_{in} - F_{out} \tag{4.28}$$

In essentially all industrial designs, the flows in and out of the inventory are not influenced by the volume (or mass) of the material in the inventory, so that F_{in} and F_{out} are independent of V. Therefore, the amount of material in the inventory changes unless the flows in and out are exactly equal, as shown in Figure 4.34. Thus, most industrial inventories are unstable process systems, which require careful management by plant personnel or automatic control, as discussed in Chapter 6.

With this basic understanding of the advantages and disadvantages of inventories and the dynamic behavior of inventories, we are well prepared to consider how inventories affect reliability and how we can improve reliability via inventories.

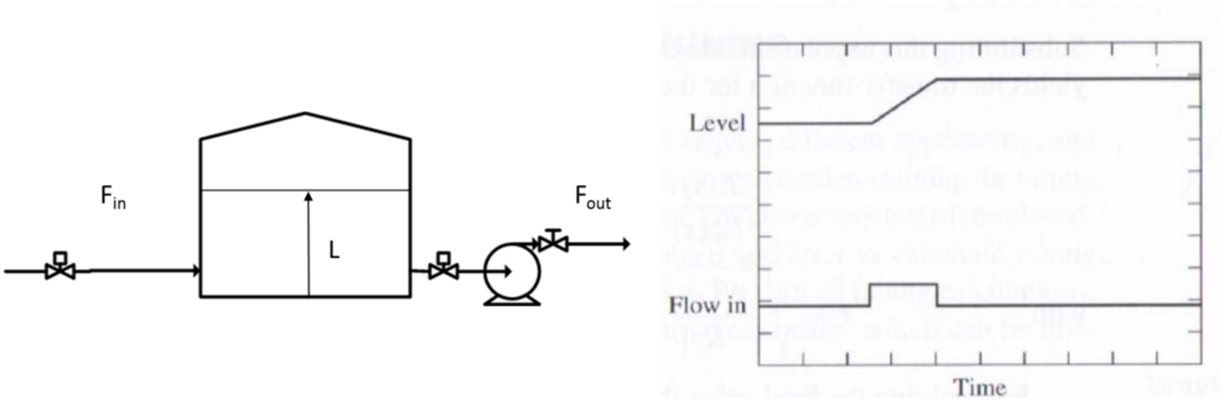


Figure 4.34. Non-self-regulatory inventory dynamics with constant flow out and initial condition of equal flows in and out (Marlin, 2000)

4.6.2 Inventory for production management: Feed and product inventory

Nearly all production facilities have storage of raw materials and finished products. In both cases, the periodic nature of the material transportation to and from the plant requires that storage be provided. For example, raw materials can be delivered by truck, railroad car, ship, or pipeline, depending on the quantities involved, distances traversed, geographical location, and the physical properties of the material. Usually, deliveries arrive periodically, e.g., every few days. In some cases, raw materials are delivered continuously by pipeline. However, disturbances in equipment can cause delivery interruptions that could cause abrupt plant shutdowns. Therefore, a reliable design includes some inventory to enable the plant to run while the continuous-feed system is repaired.

In a similar manner to feed delivery, product is periodically dispatched to customers and/or marketing centers. An example is a found in a petroleum refinery that produces gasoline, among other finished products. Gasoline is blended from numerous intermediate products resulting from distillation separation of crude oil and subsequent reactions to improve properties in fuels products. A schematic of the gasoline blending system is given in Figure 4.35. Each intermediate product is stored in an individual tank to provide flexibility in adjusting component ratios for any specific batch of gasoline product. The gasoline must satisfy numerous quality specifications, such as octane, vapor pressure, percent vaporized at specified conditions aromatics, ethanol percentage, and so forth. The product can be collected in a product tank, from which it can be shipped to customers, or it can be sent directly into a pipeline for transportation to customers. Note that the pipeline is shared among many companies, so that the product dispatch is periodic with this approach. Storage of intermediate components is required for other refinery products, like diesel, lubricating oil, and so forth. Clearly, a large number of storage tanks are required to achieve continuous plant production with periodic dispatch of many unique products.

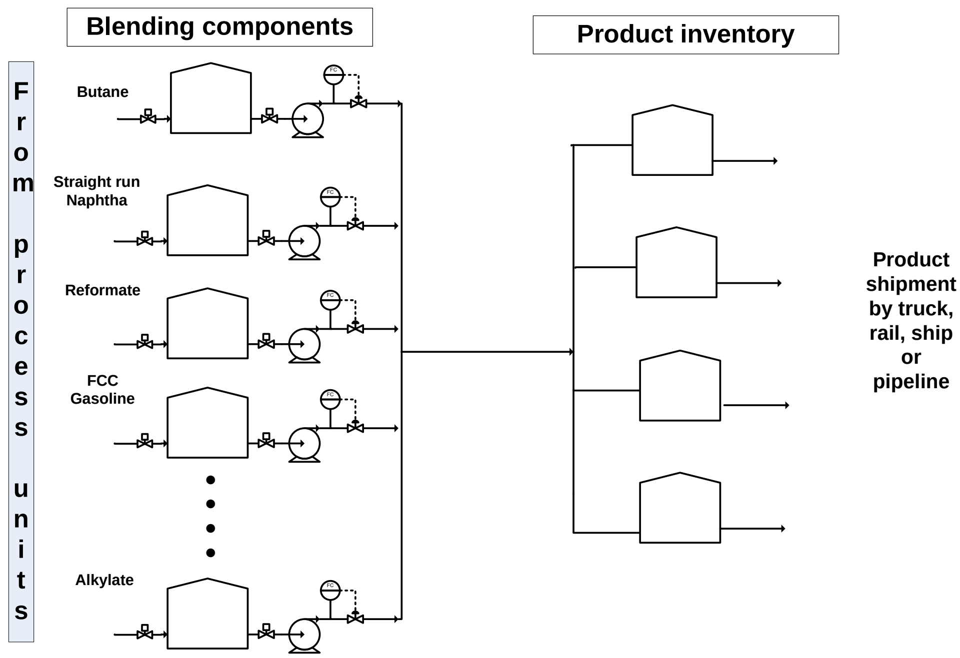


Figure 4.35. Simplified schematic of gasoline blending structure in petroleum refinery

In some plants, the product is usually dispatched continuously. Examples include ethylene production and oxygen supply. In both of these cases, the product is transported through pipelines to customers. However, disruptions can occur in plant production rate and/or customer demand, including the demand falling to zero for a short time. When these disruptions can be corrected in a short time (minutes to hours), the effects of the disruption can be minimized by (1) continuing supply to customer when the upstream plant is not in operation and (2) continuing the upstream plant in operation when the demand is low in the downstream customer. Therefore, the design includes storage between the two plants, and this inventory can be used to modulate disruptions when an imbalance occurs between instantaneous production and dispatch rates. In the cases noted above, the product is a gas, so that storage in its original form would be very costly. Usually, the gas is liquefied before storage, stored as a liquid, and vaporized when used to supply the customer. Clearly, the liquefaction dramatically increases the capital and operating costs of storage, so that only minimum storage is justified.

4.6.3 Inventory for production management: Intermediate inventory

Most process plants include intermediate storage beyond the relatively small inventory that is available in individual process units, e.g., distillation reflux drums. Again, this intermediate inventory provides storage when a temporary imbalance exists between the production rates in contiguous process units. This imbalance can occur due to planned or unplanned production disruptions.

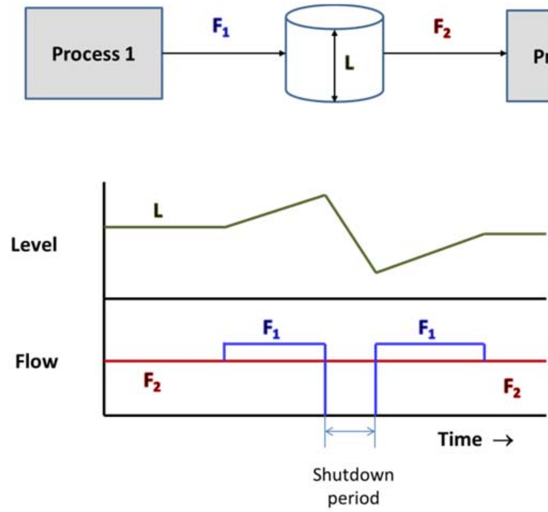


Figure 4.36. Level and flow behavior for a planned shutdown of Process 1 with Process 2 in continuous operation.

Planned production disruptions – Large continuous process plants often implement maintenance shutdowns in a staged manner, in which only part of the plant is shutdown at one time. This reduces the demand for skilled personnel and construction equipment and enables the tasks to be completed in a short time with less risk of delays. The remainder of the plant can remain in operation and most products can be provided to customers, perhaps at a reduced rate. A typical strategy for intermediate inventory management is shown in Figure 4.6 for a planned production disruption.

Example 4.20. Integrating discontinuous and continuous processes – A process plant consists of discrete-operating units, batch reactors and continuously operating separation units. How can this be accomplished?

An example batch-continuous plant is shown in Figure 4.37. The batch reactors operate as discontinuous processes, with time for loading raw materials, batch reaction, and discharging products. The reactor operations can be scheduled so that only one reactor is discharging products at a time. Inventory can be located between the discontinuous and continuous parts of the plant to store flow fluctuations from the reactors and provide a smooth, continuous flow to the separations units.

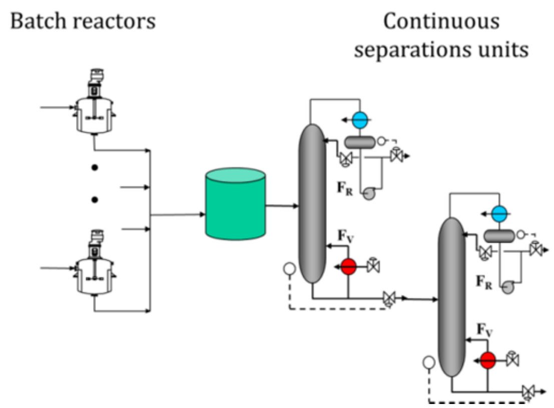


Figure 4.37. Inventory between discontinuous and continuous processing units.

Unplanned production disruptions – Process equipment is complex, and although proper design should lead to long periods of operation, breakdowns occur that require immediate repair. Some process equipment is more likely to experience breakdowns because of their inherent characteristics. For example, rotating equipment, such as compressors, turbines and pumps, has much lower reliability that pipes and vessels. These generalizations enhanced by relevant experience with specific units (bioreactors, filter presses, etc.) enable engineers to establish plant sections that are likely to operate with higher and lower reliability. When these categories are known, the plant design can be enhanced to increase overall plant performance by adding intermediate inventory.

Before discussing the location and sizing of the inventory, we need to consider the production rate and equipment capacity. Typically, each process unit will have a maximum capacity. For a series process with all elements having equal reliability, a good design will have equal maximum capacity for each unit. This design approach enables the plant to achieve its desired maximum production with minimum capital investment. However, the capacity of a unit should be increased if it is expected to experience frequent breakdowns that require unit shutdowns and maintenance. During the maintenance shutdown for the unit, the other units in the series would have to be shut down unless adequate inventory were provided in the design. With the capacity and inventory modifications, the unreliable unit can achieve the same average production rate as the more reliable units.

A similar situation can occur when the plant operates at lower than its maximum capacity. Naturally, we desire to produce at or near to the design maximum to increase operating revenues. However, the markets for all products vary, and process plants can experience long periods during which the production rate is lower than the maximum plant capacity. In this situation, a unit breakdown and repair can be accommodated with intermediate storage for a series of units with equal maximum capacity.

Dynamic responses for the two situations are shown in Figures 4.38. When the plant is operating below its maximum capacity and a unit has a breakdown in Figure 4.38a, the plant can continue its operation and achieve its desired (average) production rate. When the designated low-reliability unit in Figure 4.38b (P1) experiences a breakdown while the plant is operating at its maximum production rate, the plant cannot achieve its desired average production rate, and the cost for a failure is very high.

Now that we understand the value of intermediate inventory, we will investigate the proper inventory location, flow pattern, sizing and operations strategy.

- **Location –** Intermediate inventory is located in streams that connect an unreliable unit to other units in the plant. If the unreliable unit is the first in a series, it needs a downstream intermediate inventory, and if it is the last unit, it needs an upstream intermediate inventory.

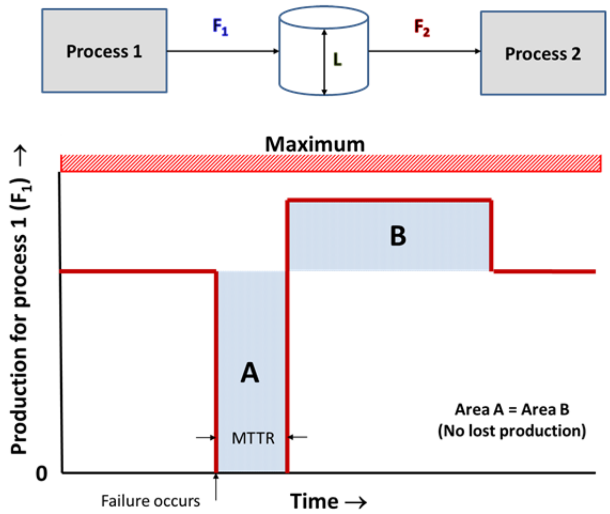


Figure 4.38 a. Design and unit capacity that results in no production loss for failure in Process 1.

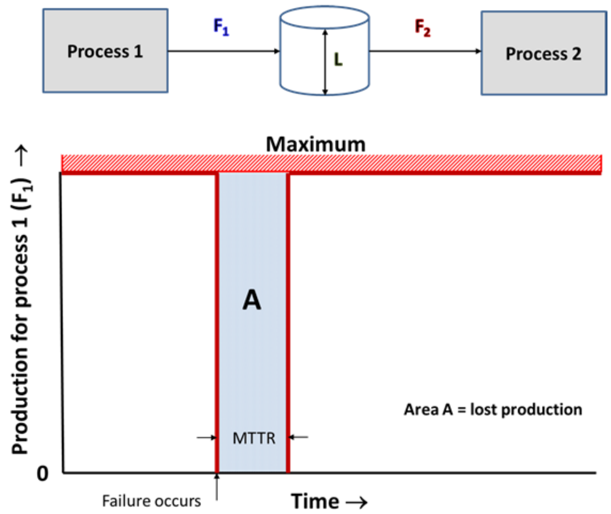
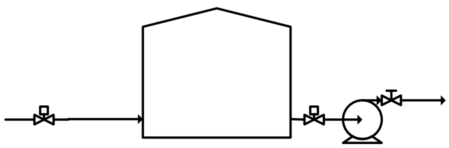


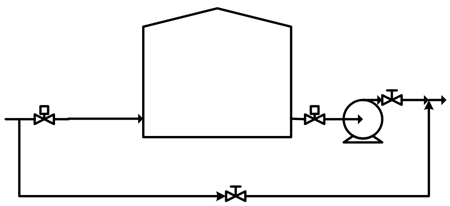
Figure 4.38b. Design and unit capacity that results in production loss for failure in Process 1.

- **Flow pattern** – The process flow can either (1) always pass into and out of the storage vessel or (2) have the option of by-passing the vessel. These two alternate designs are shown in Figure 4.39. An advantage for the flow-through design is the mixing of stream properties which can reduce variability to downstream processes. We should note that storage vessels can be very large, so that mechanical mixing is not possible; therefore, the properties out of the tank are difficult to predict. A disadvantage for allowing material to partially mix in the vessel is the difficulty in matching the best operating conditions to the properties of the material being processed in downstream units. The spill tank allows improved property tracking in the process stream because the partially processed material progresses through the plant in a predictable manner.

- **Sizing** – The amount of inventory determines the time period during which the flow imbalance can be sustained without changing the flows to the inventory (the production to/from other units) and without violating level limits (draining or overflowing the storage vessel.). This time should be sufficient to enable plant personnel to complete repairs and place the unit into operation. The time to repair is not a single value because



A



B

Figure 4.39. Flow connections to inventory. (A) flow-through and (B) “spill tank” option for flow-through or by-pass.

the causes of the breakdowns can different, along with other vagaries in the repair process. If the inventory were sized to provide time for the MTTR plus MTOW, the entire plant would have to shut down for fifty percent of the breakdowns. Therefore, the engineer needs to know the distribution of the time to repair (plus waiting) and select an appropriate time that will accommodate the majority of repair times. Thus, a tradeoff exists between lost production and the sum of negative aspects of inventory in Table 4.2.

- **Operations strategy** – The final key decision is the strategy for the inventory during “normal operations”, i.e., between breakdowns. The proper strategy provides the most time for repairing the most likely (or most crucial) breakdowns before other units are affected. A summary of strategies is given in Table 4.3.

The operating strategies and design approaches just presented are based on assumptions that warrant discussion. First, no automatic level control is present, so that all adjustments in flows are managed by people. This assumption is typically valid because these storage tanks are large to provide time for repairs. Second, breakdowns are assumed to be “far apart” in time, so that the inventory can be completely restored before the next breakdown occurs. Again, this is usually valid; if it were not valid, changes in equipment design or materials would be implemented to reduce the breakdown frequency. Third and finally, plant personnel can reduce non-zero production rate into/from inventory if real-time information indicates that the repair would take longer than time available at current rate.

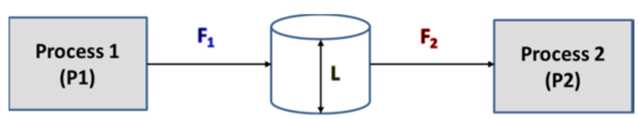


Table 4.3. Strategies for intermediate inventory.
(See figure above)

Production capacity		Reliability		Other factors and comments	Maintain Level between breakdowns
P2	**P1**	**P2**	**P1**		
higher	lower	lower	higher		low
lower	higher	lower	higher	Improper design*	low
lower	higher	higher	lower		high
higher	lower	higher	lower	Improper design*	high
equal	equal	equal	equal		50
equal	equal	equal	equal	Hazard or high cost for lack of feed to P2*	high
equal	equal	equal	equal	Hazard or high cost for lack of feed to P1*	low

* Loss of average production rate due to breakdowns

Example 4.21 Effect of tank on reliability – We are designing two series processes. The upstream process (P1) has a low reliability of 0.15, and the downstream process (P2) has a much higher reliability of 0.95. The upstream process has a much larger maximum processing rate than the average production rate. Since the upstream process has such a low reliability, we are looking to increase the total system reliability by placing a tank between the two processes.

The time to repair the first process has an exponential distribution and a mean repair time of T_R. Determine the effect on system reliability of tank holdup time as a ratio to the mean repair time.

Reliability of P1	=	R_1	=	0.15
Reliability of P2	=	R_2	=	0.95
Mean repair time	=	T_{R1}		
Holdup time	=	$\alpha(T_{R1})$	=	Volume/flow rate

First, we calculate the reliability without the tank, which is a simple series process with two elements.

$$\mathbf{R_{w/o\ tank} = R_1 * R_2 = (0.15)*(0.95) = 0.143}$$

The reliability of the series of P1 and the tank can be established by recognizing that a failure of P1 only affects the flow out of the tank if the time to repair is longer than the holdup time in the tank. When the time to repair is shorter than the holdup time, the flow from the tank can remain unchanged, so that the downstream process is unaffected and the series process remains in operation. Because process 1 has a large capacity, its processing rate can be temporarily increased above its average value to build the tank inventory to the desired high value.

If the repair time were constant and known exactly, a good design would have the tank size giving a holdup time slightly above the Process 1 repair time. However, the repair time varies. A typical repair time distribution is an exponential distribution. This situation can be expressed as the following (Cason, 1972).

$$\begin{aligned} \mathbf{R_{P1\text{-}tank}} = \;& \mathbf{(1 - \text{failure rate of P1-Tank series})} \\ & \mathbf{(1 - F_1 * \exp(-\alpha T_{R1}/T_{R1}))} \\ & \mathbf{(1 - F_1 * \exp(-\alpha))} \end{aligned}$$

The reliability of the series process with the tank is the product of the $R_{P1\text{-}Tank}$ and P_2.

$$\mathbf{R_{with\ tank} = (1 - F_1 * \exp(-\alpha))\, R_2}$$

The results of this expression for various values of the tank size as a ratio of the repair time (α) is given in Figure 4.40. As expected, the larger the tank holdup, the higher the system reliability. The proper design depends on the relative costs of flow stoppage and the inventory, as well as safety and environmental concerns, if any.

The analysis in this solution is valid for systems conforming to the following conditions.

- **No common-cause failures**
- **Constant failure rate**
- **Failures are separated by sufficient time to enable P1 exit flow to restore the tank level to its high inventory**

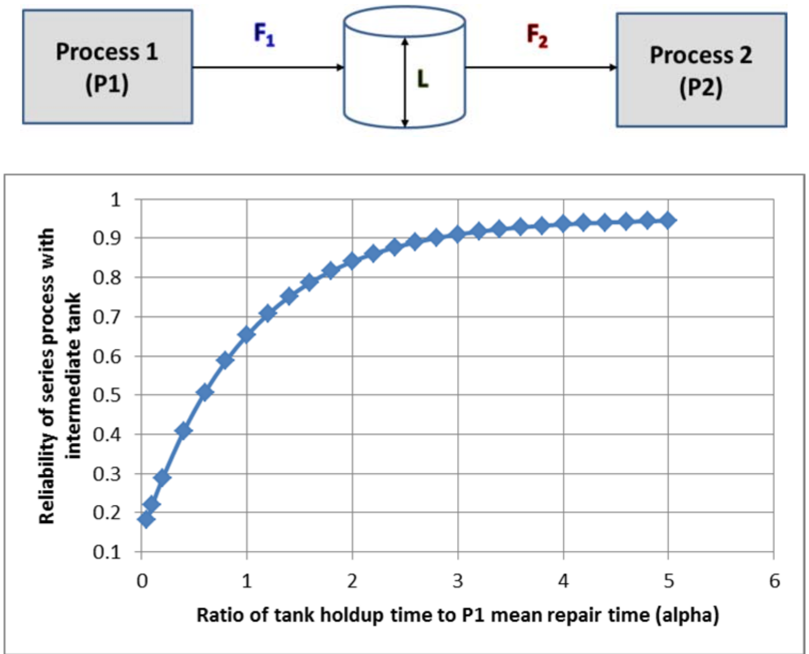


Figure 4.40. Reliability of series processes with intermediate tank from Example 4.21.

In conclusion, inventories can have major positive and negative effects on process performance. Regarding reliability, inventories can dramatically increase overall process reliability and average production rate, especially when one unit in the plant has a much lower reliability than all other units. However, engineers must always be cognizant of the negative aspects of inventories. Generally, we observe the following guideline.

Provide only the minimum inventory required to achieve desired plant performance.

Even when observing this guideline, the inventories can be large, as indicated by Figure 4.41. The figure shows, “a large liquid terminal facility on the north east side of Houston's Ship Channel, exclusively used for crude and fuel oil. The facility has three tanker docks, and over sixty large tanks, cumulatively capable of storing more than 10 million barrels (1.6 million cubic meters) of oil (LUDB, 2014)”. At a crude oil value of $100 per barrel, the inventory of working capital would have a value of one billion dollars!

Figure 4.41. Picture of Houston Ship Channel oil terminal (LUDB, 2014; Creative Commons share alike 3.0)

4.7 Reliability through Maintenance

Everyone has experience with physical systems whose reliability improves with maintenance. For example, an automobile will function reliably for an initial period without maintenance, but it will surely breakdown without maintenance after several years of operation. The same is true for process equipment.

The question is not whether to provide maintenance, but rather how to invest in maintenance in an economically appropriate manner that provides increased reliability commensurate with the maintenance costs. This chapter provides an introduction to maintenance in process plants.

4.7.1 General maintenance approaches

Over several centuries of manufacturing practice, many approaches to maintenance have been developed. A generally accepted history of the development in maintenance shows a trend from reactive toward predictive maintenance as shown in Figure 4.42; similar figures with slightly differing dates and entries appear throughout the literature, e.g., Moubray (1997) and MaintenanceResources (2014). In this section, we introduce the four major categories of maintenance that encompass today's most maintenance activities. Naturally, the engineer is faced with the challenge of matching the maintenance category with equipment in a plant; therefore, the next section introduces Reliability-Centered Maintenance (RCM) that provides criteria for applying the approaches based on the needs of the entire plant system.

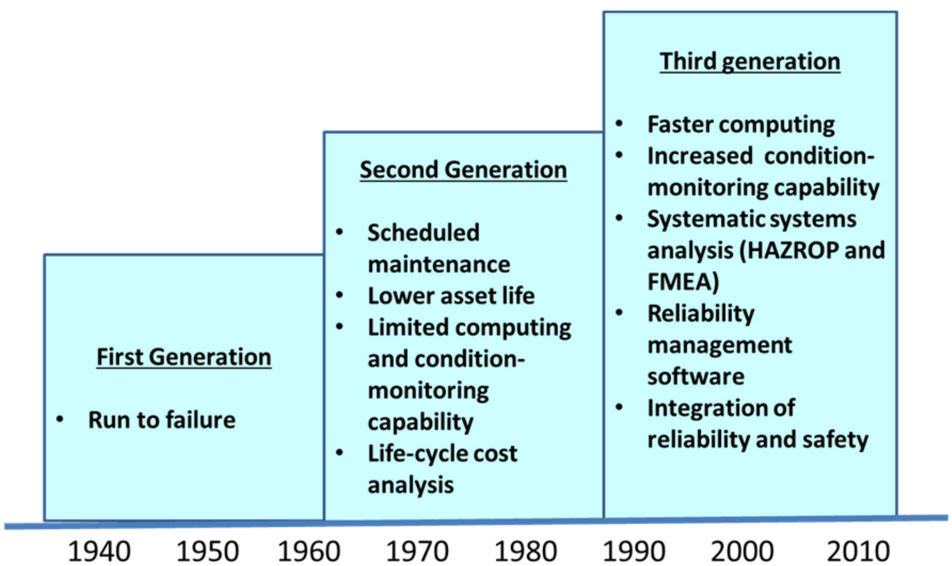


Figure 4.42. General historical trend of maintenance practice in industry.

We begin with a brief explanation of the four maintenance categories, with their most commonly used terminology first, followed by alternative terms in parentheses.

- **Reactive maintenance** (**Run-to-Fail**) **–** This approach involves no maintenance activities until the equipment fails to perform its tasks properly, i.e., until it fails. Then, the equipment is repaired or replaced, as appropriate. After maintenance, the equipment is returned to service and no further actions are taken until it again fails.
- **Preventive maintenance (PM) –** This approach involves planned maintenance that is performed on a periodic basis, with the period measured as time, total production processed, number of cycles (start and stop cycles), number of batches, and so forth. This maintenance is performed without reference to the current condition of the equipment. Some parts may be replaced as a component of this maintenance.
- **Predictive maintenance (Predictive testing and inspection, PT&I) –** This approach involves measurements and analysis that determines the performance of the equipment, i.e., condition monitoring. Maintenance is only performed when the current condition indicates that it is required. The difference from reactive maintenance is that this approach seeks to determine incipient failures before the performance of the equipment affects the key aspects of safety, product quality or production rate.
- **Proactive maintenance –** This approach seeks to prevent future failures through root-cause analysis of past behavior that determines the underlying causes of those failures. Actions are performed to reduce the likelihood of future failures through equipment redesign, modification, or directed maintenance.

Each of these approaches has advantages and disadvantages, as summarized in Table 4.4.

4.7.2 Reliability-Centered Maintenance (RCM)

In response to this myriad of methods and complex reliability experience, engineers have developed a widely applied method for maintenance selection termed Reliability-Centered Maintenance (RCM). The concepts and application of RCM are not new; the basic approach was documented by F. Stanley Nowlan and Howard F. Heap nearly four decades ago (Nowlan and Heap, 1978). Initial RCM implementations appear to have been more widely applied in the aeronautical, defense, nuclear power, automotive, and aerospace industries, but application in the process industries is now widespread.

Specific RCM objectives as stated by Nowlan and Heap are to (NASA, 2000):

- achieve the inherent safety and reliability levels of the equipment
- restore the equipment to these inherent levels after deterioration has occurred
- obtain the information necessary for design improvement of those items where their inherent reliability proves inadequate.
- accomplish these goals at a minimum total cost, including maintenance costs, support costs, and economic consequences of operational failures.

Table 4.4 Advantages and Disadvantages of Four Maintenance Approaches

Approach	Advantages	Disadvantages	Appropriate Application
Reactive	• Lowest personnel cost • Least technically demanding	• Potential safety hazards • High economic losses for damaged equipment • High economic loss for production interruptions • High peak labor demands with long periods of low demand	• Equipment that is not critical for production and/or safety • Low cost equipment replacement • Redundant equipment design to accommodate individual failures
Preventive	• Even demand for personnel • Can increase MTTF • Many equipment have components that wear and need replacement	• Can introduce failures through errors during unneeded maintenance actions • Labor intensive, some maintenance likely not required • Does not eliminate major failures	• Equipment that is critical for production and/or safety • Equipment or components that wear rapidly and require repair or replacement • Required by best practice or law (e.g., boiler inspection)
Predictive	• Lengthens average equipment life • Maintenance that prevents breakdowns, increasing safety and profitability	• Cost for sensors and support software • Requires more technical sophistication	• Equipment that is critical for production and/or safety • Random failure patterns • Diagnosis possible through increased monitoring
Proactive	• Lower failure rate • Prevents breakdowns, increasing safety and profitability • Reduce maintenance costs	• Requires through root-cause analysis of breakdowns and near-misses • May require costly modification to existing equipment	• Equipment that is critical for production and/or safety • Equipment whose repair and replacement is costly

RCM analysis identifies the important function of equipment and considers the likelihood and consequence of failures when designing the plant. The engineer must decide on appropriate design features that (1) reduce the probability of failure, (2) identify incipient failures and prevent them from fully developing and/or (3) reducing the failure consequence. Naturally, highly likely failures with serious consequences require more investment than highly unlikely with minimal consequences. The RCM analysis is shown schematically in Figure 4.43. Clearly, a maintenance program in a complex plant will apply all four maintenance approaches matched to the specific needs each plant equipment or system.

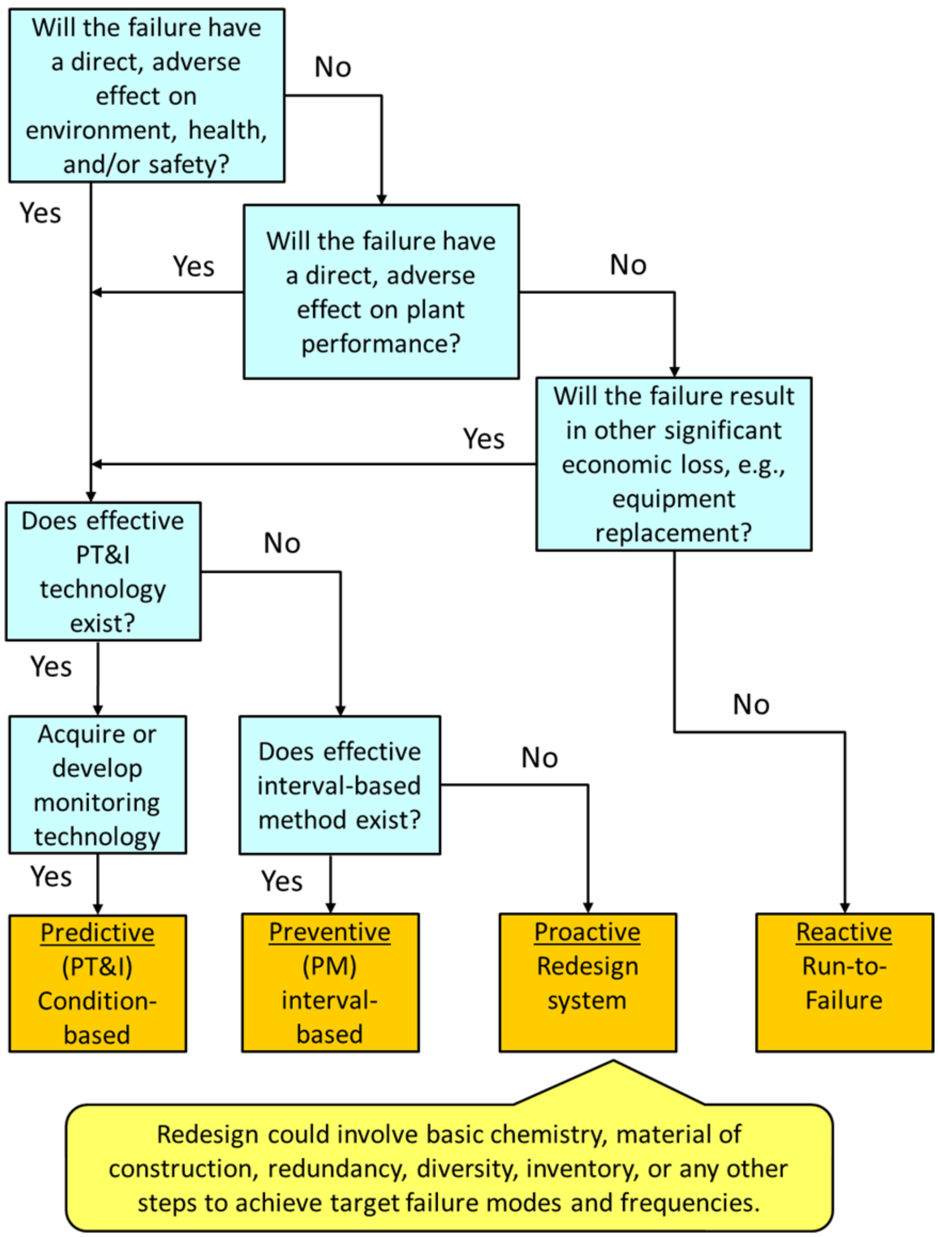


Figure 4.43. Maintenance selection flowchart (adapted from NASA, 2000)

Typical distributions of the maintenance effort over the four approaches are given in Table 4.5. The data for 2000 is not in agreement with the viewpoint depicted in Figure 4.42; the data indicates a slower adoption of the more advanced methods. However, the data after RCM implementation shows the trend toward application of improved maintenance approaches, i.e., predictive maintenance increases as reactive maintenance decreases.

Table 4.5. Summary of Maintenance Practice (DOE, 2010)

Maintenance approach	Survey of industrial practice in 2000 (percent)	Average maintenance distribution after RCM (percent)
Reactive	55	<10
Preventive	31	25 to 35
Predictive	12	45 to 55
Other	2	(not reported)

4.7.3 Preventive maintenance for age-related failures

Preventive maintenance is appropriate for equipment that experiences specific failure behavior, namely "age-related". Age-related failures result in the behavior shown in Figure 4.44, which has a very low failure rate for a period of time from startup and a higher failure rate around a reasonably well-known failure time. The period with a very low failure rate is termed the "useful life" of the equipment, and the causes of failures are caused by some form of "wearout". This type of behavior often occurs when the equipment comes in contact with corrosive process materials that cause fatigue, corrosion, oxidation, and so forth (Moubray, 1997).

For equipment with behavior characterized in Figure 4.44, a corrective action can be taken periodically to return the equipment to or close to new condition. Naturally, the corrective period should be less that the wear-out time, and should not be too frequent to reduce the costs of maintenance and the negative effects of inadvertent errors during maintenance. The restorative actions could involve either (1) repair, i.e., actions to return the original equipment to new conditions, or (2) replacement, i.e., removing the equipment currently in practice with new equipment.

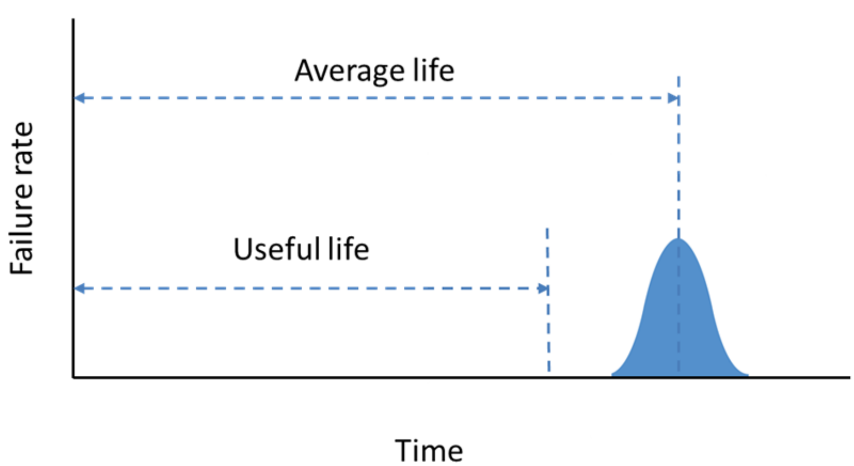


Figure 4.44. Failure behavior of equipment appropriate for preventive maintenance.

Preventive maintenance is recommended when the following conditions are satisfied.

- An identifiable age exists beyond which the likelihood of failure increases significantly. This behavior occurs in Figure 4.3 for systems A and E (and to a lesser extent, F)
- Most of the equipment performs properly until this age, i.e., very few premature failures occur
- The corrective action returns to equipment to “like new” operation with the same useful life
- The cost of maintenance is less than following the “run to failure” approach. We recognize the advantages of preventive maintenance that allows actions to be well prepared and scheduled for times when the production-related cost is low or zero.

Finally, we emphasize the key aspect in selecting preventive maintenance, which is the failure behavior that includes a long period of very low failure rate followed by an increasing failure rate after a well-defined wear-out time. If all of the conditions above are not satisfied, preventive maintenance is not appropriate.

4.7.4 Predictive maintenance for random failures

Predictive maintenance is appropriate for equipment that experiences specific failure behavior, namely “not age-related” or random. For the equipment, failures are independent of the time of operation from startup. Typical failure rate plots for this equipment are shown in Figure 4.3 systems C, D and B. Note that the data in Figure 4.3 indicate that majority of equipment belongs to these categories, which experience long periods of nearly constant failure rates with no wear-out period.

Another schematic of failure behavior is shown in Figure 4.45. Equipment can experience a long period of good performance. When a failure begins, the failure might not be detectable; however, at some point, the failure can be identified with measurements. At a later time (point P), the failure has progressed to the point at which the process performance has been substantially affected and the fault can be detected. Finally at point F, the equipment has failed completely to perform its function.

Predictive maintenance should be performed frequently enough to avoid the failure progressing to the point F. Often (but not always), a process fault begins gradually and continues to worsen until it significantly influences process performance, requiring immediate action. Plant performance can be substantially improved by recognizing incipient faults, so that moderate corrective actions can be implemented. The P-F window for predictive maintenance is shown in Figure 4.45, which is between the first time the failure can be detected (with a high degree of certainty) and the equipment fails to perform its function.

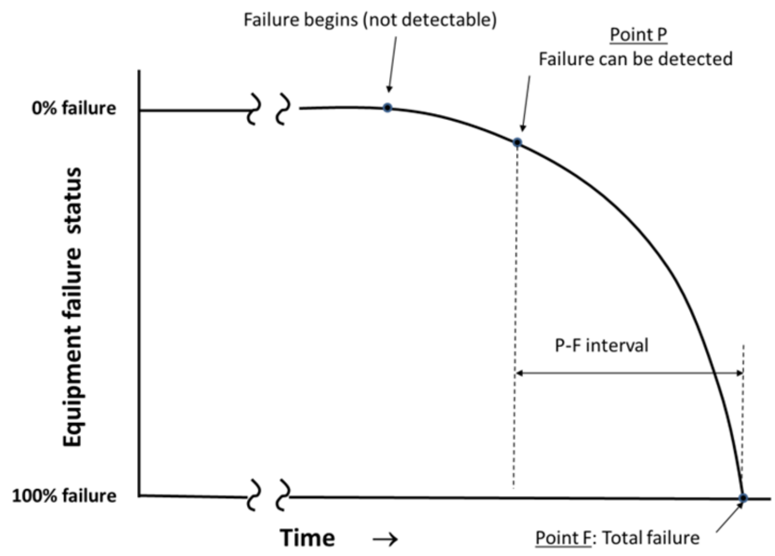


Figure 4.45. A typical P-F plot for equipment using terminology from Moubray (1997). Note that the "F point" might occur before total equipment failure if equipment fails to satisfy process requires for a partial failure.

Since shutting down equipment for inspection can be very costly, much of this monitoring is performed while the equipment is in normal operation, which is often termed "on-condition monitoring". This monitoring can be a combination of measurements, including laboratory analyses (chemical analysis), human senses (hearing and touch), real-time sensors of process conditions (pressure, temperature, etc.), and real-time sensors of equipment conditions (vibration and corrosion). Examples of predictive maintenance measurements are given in Table 4.6, and a thorough discussion of each of these applications is provided in DOE (2010).

The decision whether to implement a predictive maintenance application is guided by the following conditions.

- A failure condition monitoring measurement(s) must exist
- The P-F period must not vary too much
- The selected monitoring period must be shorter than the P-F window.
- The monitoring period must provide sufficient time for corrective actions after the fault has been identified. See Figure 4.46.
- The monitoring period must prevent too much process performance degradation. (The process performance could become too poor before a 100% equipment failure, in which case, point F must be moved to the left in Figure 4.46.)
- The monitoring period should be selected to minimize total cost (of maintenance and failure). Thus, a very short maintenance period is avoided.

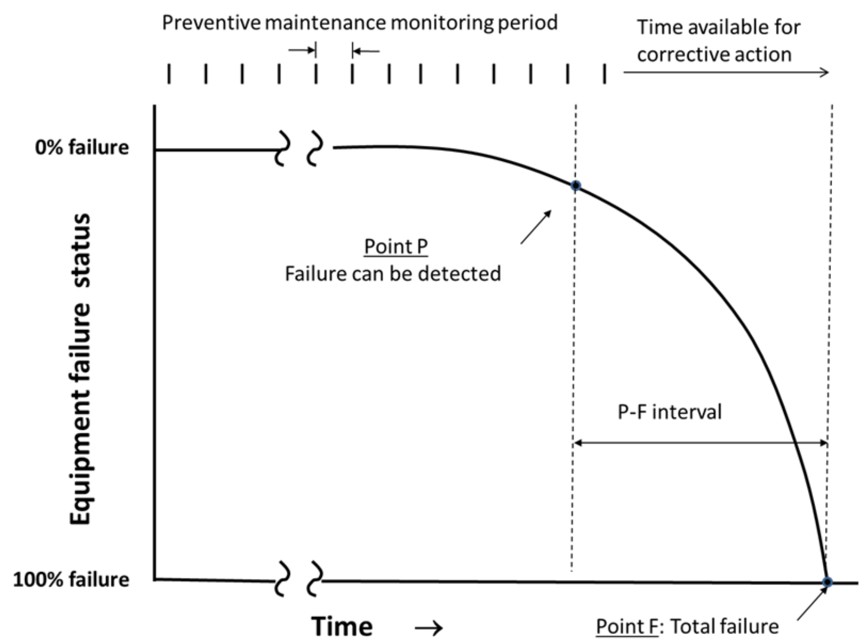


Figure 4.46. Schematic of predictive maintenance monitoring period.

Table 4.6. Typical Variables for Reliability monitoring and diagnosis. (DOE, 2010)

Technologies	Applications	Pumps	Electric Motors	Diesel Generators	Condensers	Heavy Equipment/ Cranes	Circuit Breakers	Valves	Heat Exchangers	Electrical Systems	Transformers	Tanks, Piping
Vibration Monitoring/Analysis		X	X	X		X						
Lubricant, Fuel Analysis		X	X	X		X					X	
Wear Particle Analysis		X	X	X		X						
Bearing, Temperature/Analysis		X	X	X		X						
Performance Monitoring		X	X	X	X				X		X	
Ultrasonic Noise Detection		X	X	X	X			X	X		X	
Ultrasonic Flow		X			X			X	X			
Infrared Thermography		X	X	X	X	X	X	X	X	X	X	
Non-destructive Testing (Thickness)					X				X			X
Visual Inspection		X	X	X	X	X	X	X	X	X	X	X
Insulation Resistance			X	X			X			X	X	
Motor Current Signature Analysis			X									
Motor Circuit Analysis			X				X			X		
Polarization Index			X	X						X		
Electrical Monitoring										X	X	

Many predictive monitoring and diagnosis applications are based on knowledge of process technology, as demonstrated in the following examples.

- **Distillation tray temperatures –** A novice engineer might conclude that monitoring multiple tray temperatures is not valuable. After all, the equipment will not be damaged by temperatures in the range experienced in the tower. However, monitoring is valuable because the temperature of each tray is related to the composition of the boiling liquid on the tray. Therefore, the temperature profile gives information on the composition profile. Usually, several tray temperatures above and below the feed tray are measured. For example, if two adjacent temperatures, which are typically different by 7 °C, are nearly equal, the monitoring system should indicate an issue that requires diagnosis. Perhaps, the trays have been damaged and liquid is by-passing the trays between the two sensors, resulting in similar compositions on the trays with temperature sensors.
- **Reactor temperature profiles –** Chemical reactors filled with granular catalyst can be used for reactions with significant heat of reaction, either exothermic or endothermic. For these reactors, the temperature profile might be expected to continuously increase (exothermic) or decrease (endothermic). However, flow patterns are not always uniform in a reactor, which can lead to points of low flow rate and higher extent of reaction. Often, the temperature profiles will show hot (or cold) spots in the reactor that indicate non-uniform flow. Note that there is no guarantee that a limited number of temperature sensors will respond to a local temperature variation.
- **Heat exchangers –** Many heat exchangers suffer from a decrease in overall heat transfer coefficient due to fouling. This decrease occurs gradually, typically over months. The engineer can monitor the performance of many heat exchangers in a plant and schedule maintenance when least disruptive to the overall plant operation. Monitoring requires measurements of flow rates and temperatures to enable the heat transfer coefficient to be calculated.

Further discussions on maintenance are available in DOE (2010) for boilers, chillers, cooling towers, steam traps, and building heating, ventilation, and air conditioning (HVAC), and many additional monitoring examples are described in Moubray (1997).

Predictive maintenance is based on knowledge of failure sources and the inclusion of sensors that enable early detection of incipient faults.

Example 4.22. Automobile maintenance – Provide examples of maintenance in each of the four categories for a personal automobile.

Some examples are given in the following table.

Reactive (Run-to-failure)	**Items that do not affect safety or efficient operation can be in this category.** • **Interior lights** • **Power windows** • **CD player**
Preventive	**These items are performed periodically, without checking the condition.** • **Change the oil** • **Change cooling fluid** • **Rotate tires**
Predictive (Condition-based)	**The items require real-time measurement and analysis. The following are examples for the Toyota 2011 described in the Prius Owner's Manual (Toyota, 2011).** • **Low oil pressure while engine running** • **Low tire air pressure** • **High temperature** • **Low brake fluid**
Proactive	**These items are implemented by the automobile manufacturer. The examples below are reported for the Toyota 2010 Prius (Safecar, 2014) and can be corrected at a dealer.** • **Transistors that could overheat and cause a power decrease** • **Brake fluid leak affecting stopping distance** • **Calibrate passenger seat sensor affecting the passenger airbag** • **ABS braking** • **Missing label for maximum load in vehicle**

4.8 Life Cycle Cost Economic Analysis (LCC)

The best decisions for investment process equipment and maintenance is determined by economic analysis generally referred to as life cycle cost analysis (LCC). (Recall that designs for safety use other methods described in Chapter 5 to ensure that hazards have a very low likelihood of occurrence.) The principles of this economic analysis follows standard principles covered in engineering curricula; therefore, this presentation emphasizes only the unique features that consider effects of reliability.

The structure of economic analysis typically involves the steps in Table 4.7. Naturally, the analysis is not a simple, linear process. Engineers need to iterate as they evaluate the cost and performance effects of various design decisions. For a review of engineering economic analysis, see Blank and Tarquin (2012).

Table 4.7. Basic Components of Engineering Economic Analysis

Technical analysis
- Design basis and goals
- Technology selection
- Plant structure selection
- Flowsheet material and energy balances
- Materials of construction
- Equipment selection and sizing

Cost estimation
- Purchase cost of equipment
- Installation cost of equipment
- Engineering cost
- Startup cost
- Personnel cost
- Marketing and corporate overhead costs
- Feed material costs
- Fuel, electricity and other materials
- Product sales quantity and price

Profitability analysis
- Evaluate annual cash flows before tax
- Determine the after tax cash flows
- Determine the interest (discount) rate for the company
- Select the appropriate profitability measure, usually net cash flow (NPV)
- Calculate the profitability for the base case
- Sensitivity analysis

Decision analysis
- Risk and uncertainty analysis
- Cash flow analysis
- Select the best alternative(s)

Life-cycle cost analysis emphasizes the importance of considering all relevant costs during the project, especially the tradeoff between investment and reliability. This approach seeks to overcome the mistake of evaluating an investment based solely on the initial equipment cost. The approach is often depicted by the ship-iceberg analogy shown in Figure 4.47, indicating the dangers of not considering all costs (and revenues) throughout the life of the project. Some of the key decisions affecting plant reliability, and costs associated with reliability, are given in Table 4.8.

The key characteristic to LCC is full evaluation of investments and costs influencing reliability. Here, we will concentrate on four key economic factors; fault frequency, cost of a fault on equipment, cost of production loss, and accurate accounting for equipment investment.

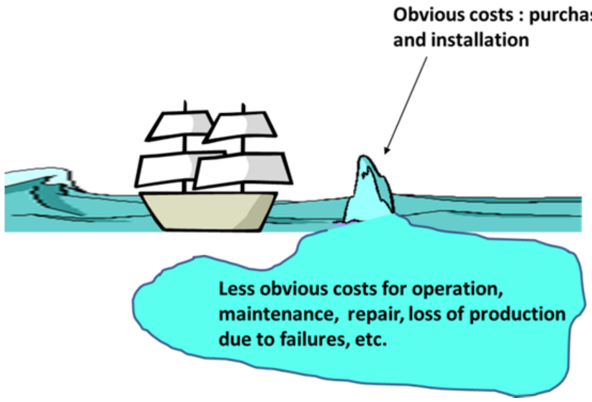


Figure 4.47. Depiction of the relative magnitudes of initial investment (visible part of iceberg) and total life-cycle costs (the entire iceberg). (modified from Kawauchi and Rausand, 1999)

One important factor is the frequency of faults occurring with the plant structure and equipment. Many companies have data bases with equipment performance, which include the effects of their purchase, installation and maintenance practices. Naturally, this data is preferred where it exists. However, published reliability data is available and can be used where company data is not available. Some sources of publically available reliability data are given in the following.

- AIChE (1989) Guidelines for Process Equipment Reliability Data with Data Tables, AIChE, New York, 1989. Data for a wide array of process equipment from the Center for Chemical Process Safety.. (http://www.aiche.org/ccps/publications/books/guidelines-process-equipment-reliability-data-data-tables)
- Block and Gietner (1999) Simplified data for numerous process equipment
- Bickell (2011) Simplified data for equipment in nuclear power and process plants (http://www.esrt-llc.com/Component%20Reliability_files.htm)

Table 4.8. Key design decisions that affect reliability and Life Cycle Cost

Decision	Effects on reliability
Equipment selection	- fault frequency - process performance (energy, yield, etc.) - equipment life (replacement cost) - cost of a fault (isolation and repair, inventory, prevent major damage, etc.)
Spare parts	- mean time to wait (MTTW) during repair
Maintenance	- fault frequency: ability to predict and prevent fault
Operating conditions	- fault frequency and performance degradation: operation near limits can reduce longer-term performance and equipment life

- HSE (2012) Data for materials storage and transfer with references for additional information. Data provided for various failures types. (http://www.hse.gov.uk/landuseplanning/failure-rates.pdf
- Lees (1996) Data in Appendix 14 covers numerous process equipment, but it is dated
- DNV GL (2014). OREDA data handbooks, containing extensive data on oil and gas production including offshore, can be purchased at the following site. (http://www.oreda.com/handbook.html)
- Akhmedjanov, F. (2001) *Reliability Databases: State-of-the-Art and Perspectives*. A report on available reliability data bases. (http://orbit.dtu.dk/fedora/objects/orbit:91234/datastreams/file_7728815/content)
- DOE (1999) *Market-based Advanced Coal Power Systems, Final Report*, Appendix D May 1999. Data for equipment in power generation plants. (http://www1.fe.doe.gov/programs/powersystems/publications/MarketBasedPowerSystems/appd.pdf)
- EPRI, (1992) *A Database of Common-Cause Events for Risk and Reliability Applications*, Electric Power Research Institute, June 1, 1992. Guidance on modeling common cause failures and data for equipment for power generation. (http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=TR-100382)

A second key factor is the cost of a fault associated with returning the equipment to operation. Some of these costs are summarized in the following.

- Repairing damage to equipment
- Use of spare parts that must be replaced
- Personnel time
- Off-specification materials that must be recycled or processed for disposal
- Loss of containment leading to spills to the environment

A third key factor is the cost of a production loss caused by faults. Several scenarios exist based on the plant design and market conditions.

- **No production loss –** Many designs can eliminate the effects on production of a fault. For example, redundant equipment with immediate (or very fast) switching can assume the function of failed equipment. Naturally, this is why plant designs contain so much redundant equipment, especially for lower cost equipment. In this scenario, the cost for production loss is zero.
- **Immediate production loss that can be compensated –** When production in a unit must be stopped, the overall cost of the immediate loss depends on whether the production can be recovered at a later time by a short-term increase in production. This recovery is possible in two situations; (1) the failed unit has greater capacity than the remainder of the plant or (2) the plant production is lower than its maximum capacity because of low market demand. In both of these scenarios, the production must be averaged by inventory in the plant or in the customer's storage facility for the compensation to be successful. If immediate production is essential, as would be the case for supplying oxygen or electricity to a customer, the compensation would not be possible. In scenarios where compensation is possible, production can be managed as shown in Figure 4.38a to satisfy the average demand. In these scenarios, the production costs for a fault can be

zero or can be small, associated with efficiency effects of operating at higher production rates for a short time.

- **Immediate production loss that cannot be compensated –** When the product must be supplied immediately and no inventory exists, a loss in production cannot be compensated. In these situations, production can be managed as shown in Figure 4.38b. In this scenario, the cost for production loss is high, essentially the product of the total production decrease multiplied by the incremental profit per unit of sales. Other losses could be incurred due to contract terms and perhaps, loss of future sales due to unreliable deliveries to customers.

A fourth key factor is full accounting of costs associated with design for reliability. As we have seen, these designs can include (1) redundant equipment, (2) diverse equipment, (3) inventories, (4) complex bridge and network process structures, and (5) a hierarchy of control designs to lower the frequency of faults. Naturally, the design modifications involve increased costs over a "lean, less reliable" design, so that the engineer must consider all of these costs in LCC.

- Cost of equipment purchase and installation
- Engineering costs for design, procurement and installation
- Documentation
- Spare parts
- Personnel training
- Other design modifications to provide maintainability, e.g., by-pass around exchangers, valves, etc.
- Effects on operating efficiency, if any. These could include pump efficiency, pressure drop in a piping circuit, etc.

There is a general impression that these costs are either not considered or considerably underestimated in common practice (Barringer and Weber, 1996). For example, adding a diverse instrument requires training, documentation and spare parts because the instrument might not be in use elsewhere in the plant. Also, documentation and drawings for modifications can be costly.

It is important to note that LCC demands thorough analysis of all costs (purchase, operations, etc.) and benefits (higher production, lower equipment damage) for each design option. LCC favors neither high nor low investment for reliability. It requires a fair and complete analysis of the profitability over the project's life. Further discussion of LCC can be found at Abbe (2013).

Example 4.23. Standby pumps – A process requires a single 100 HP pump. If the pump fails, not hazards occur. However, the equipment must be repaired. Also, if no redundant pump is available, the process must be shut down during repairs, so that production is lost. Standby pump(s) can be installed that can startup immediately to continue plant production if the standby has not failed. Data is provided below. Determine the number of standby pumps, from zero to four, based on economic analysis.

Pump information				
Pump is 100 hp centrifugal, carbon steel				
Reliability includes pump, shaft and coupling; it does not include motor				
Economic analysis based on equivalent annual cost				
Discount (interest) rate = i =			0.12	(%/100)
Project life =			10	yr
Economic data				
pump installed cost	50000		$/pump	
annualized pump cost	8849.208208		$/yr-pump	
Additional engineering	3500		$/additional pump	
Annualized Additional engineering	619.4445746		$/yr-additional pump	
Preventive maintenance	1600		$/yr-pump	
cost repair pump after failure	3400		$/failure	
Process cost for failure	100000			
(Note: Power cost is not affected by number of standby pumps because standby pumps are idle, until needed.)				
Reliability data (constant failure rate)				
MTBF for one pump =	3.4		yr	
failure/yr = 1/MTBF system	0.294117647		yr^(-1)	

The analysis involves evaluating the total annualized cost of operation, which includes costs for installed equipment, maintenance, repair, and lost production. As the number of standby pumps increases, capital and maintenance costs increase but the number of failures per year decreases. Therefore, the cost of repair and production loss decreases. The economic analysis considers the time value of money, which is based on the interest rate of 12% given above. All economic values are converted to equivalent annualized cost (Blank and Tarquin, 2012). The results are given in the following table.

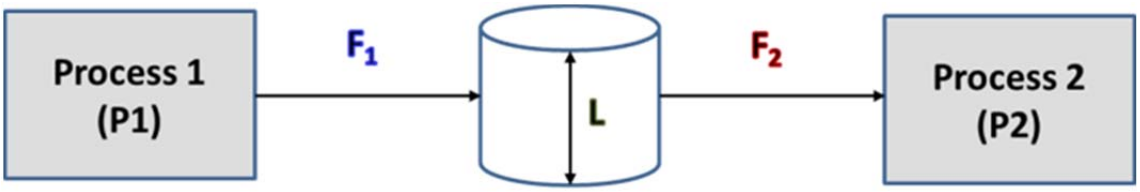
Number of pumps	System MTBF (yr)	Failure rate (1/yr)	A. Cost of equipment	B. Prev. maintenance	C. Cost of failure	Total cost ($/yr)
n	MTBF*n	1/(System MTBF)	Pump cost * n + Additional eng * (n-1)	Unit PM cost * n	(Repair + Process)/(System MTBF)	Sum of A, B, and C
1	3.4	0.294117647	8849.208208	1600	30411.76471	40860.97291
2	6.8	0.147058824	18317.86099	3200	15205.88235	36723.74334
3	10.2	0.098039216	27786.51377	4800	10137.2549	42723.76868
4	13.6	0.073529412	37255.16656	6400	7602.941176	51258.10773

The total annualized cost is minimum for the two-pump design, i.e., one standby pump. Although the reliability increases with additional standby pumps, the cost of additional investment is not recovered by the reduced costs resulting from lower failure rate. This result is typical for process applications, where one standby pump is typical.

Example 4.24. Lowest-cost intermediate tank - The series analyzed in Example 4.21 consisted of two processes separated by a tank. Process 1 has a low reliability, but a high maximum production rate, so that it can make-up lost production due shutdowns for repair. The repair time for Process 1 has an exponential distribution. Process 2 has a higher reliability. The reliability of the entire system was determined in Example 4.21. In this example, the task is to determine the lowest cost design.

An economic optimum is expected because increasing the inventory size decreases the likelihood of having to shut down Process 2 – and shut-down costs - but increases the capital cost of the tank. Also, the effect of increasing inventory size decreases as the inventory increases, as shown in Example 4.21.

Some required data for the analysis is given in the following.



Inflation factor (2014/1998)	1.5		CECI used to determine costs for 2014			
Project life =	15	y			R1=	0.15
interest rate =	0.15	(15%)	before tax		R2 =	0.95
Plant flow rate =	100	m^3/h				
Cost per hour =	2,000	$/h	for shutdown Process 2		F1 =	0.85
MTTR + MTOW =	5	h	for Process 1			
MTTR + MTOW =	25	h	for Process 2			
hours/year =	8600	h	other time planned shutdown			

The analysis involves a straightforward application of engineering economics principles. We note that a Process 1 shutdown does not require a total system shutdown unless the Process 1 repair time is greater than the tank holdup time. Since the Process 1 repair time varies, changing the holdup time influences the total system performance. If Process 2 must be shut down, twenty five hours are required to restart the process. We will take 8600 hours for a year, with the remainder of the time (160 hours) taken by planned shutdown time for maintenance.

The calculations for the solution are presented in the following table. A plot of the annualized cost versus the tank inventory is given in Figure 4.48. The lowest cost occurs around a tank size of 1000 m^3.

This analysis is simplified to limit space.

- The analysis is based on before-tax cost to simplify the presentation; after tax analysis would follow the same methodology.
- Other costs for land, maintenance, working capital and so forth for the tank are not included.
- All good economic studies include sensitivity analysis of every result.
- Non-economic factors such as safety and hazard analysis for the inventory size are not included in the analysis.

Inventory volume (m^3)	holdup time (h)	Alpha ***	Reliability total system	MTTF (h)	Annual Failures (/y)	Shutdown time (h/y)	Shutdown cost ($/y)	Installed inventory cost (1998) * ($)	Installed cost (2014) ** ($)	Annualized cost of inventory ($/y)	Total cost SD + Inventory ($/y)
0	0	0	0.1425	4413.847971	1.937439636	48.43599091	96871.98182	0	0	0	96872
150	1.5	0.3	0.35178929	8231.847893	1.041559698	26.03899246	52077.98492	130000	195000	33348.32527	85426
300	3	0.6	0.5068346	12655.05098	0.678230712	16.9557678	33911.53559	182000	273000	46687.65537	80599
600	6	1.2	0.70678567	24781.87571	0.346678078	8.666951957	17333.90391	225000	337500	57718.25527	75052
900	9	1.8	0.81652115	42426.71613	0.202583094	5.064577351	10129.1547	245000	367500	62848.76685	72978
1200	12	2.4	0.87674525	65379.94644	0.131488526	3.28721315	6574.4263	260000	390000	66696.65053	73271
1500	15	3	0.90979694	90972.70958	0.094507873	2.36269683	4725.393661	290000	435000	74392.4179	79118
2000	20	4	0.93521012	128388.7809	0.066971005	1.674275132	3348.550265	350000	525000	89783.95264	93133
2400	24	4.8	0.94335448	147479.5713	0.058303278	1.457581945	2915.16389	390000	585000	100044.9758	102960

* Inventory cost from Loh, Lyon and White (2002)
** Inflation based on Chemical Engineering Cost Index
*** Alpha = (vol/flow)/(MTTR+MTOW), dimensionless

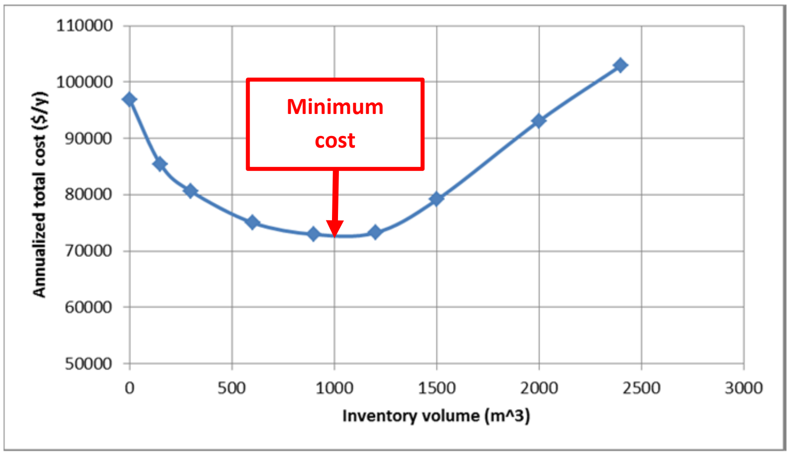


Figure 4.48. Relationship between total cost and inventory volume from Example 4.24.

4.9 Managing design for reliability

Throughout the history of chemical engineering practice, the application of reliability principles has been implicit in the design analysis. Common designs have been developed over years based on insights and experience in operating plants. While reliability has been a consideration in all designs, a systematic analysis of alternatives and a consistent decision analysis have not typically been applied.

Over the last decades, reliability analysis has been improved by applying a systematic analysis method that ensures each equipment and its effects on the entire process system are evaluated. The analysis method discussed here is an extension of the HAZOP method that is fully explained in Chapter 5. An abbreviated table showing the results of a HAZOP analysis is given in Table 4.9. The HAZOP team's attention is focused on a specific node (location) in the process, and they analyze possible safety issues by considering a list of parameters (process variables) and guidewords (deviations from normal) at the node. The team identifies all possible causes for the guideword and consequences for each cause. Then, they propose possible actions to eliminate or reduce the likelihood of the event and the consequence if it should occur. The HAZOP method provides a systematic, albeit time-consuming, method for safety analysis. It is widely applied in engineering practice. Much more detail on HAZOP is given in Chapter 5.

Table 4.9 A typical HAZOP form *

<table>
<tr><td colspan="3">Company: XYZ Polymer Limited</td><td colspan="3">Facility: Hamilton Works</td></tr>
<tr><td colspan="3">Design Intent: Raise circulating oil stream temperature flowing at 100 m^3/h from 250 to 400 °C</td><td colspan="3">HAZOP Team Members:</td></tr>
<tr><td colspan="3">Drawing: Figure 5.20</td><td colspan="2"></td><td>Date: Jan 2, 2011</td></tr>
<tr><td colspan="6">1.0 Node: Pipe after feed pump before entering heater</td></tr>
<tr><td colspan="6">Parameter: Flow</td></tr>
<tr><td>ID. No.</td><td>Guideword / Deviation</td><td>Causes</td><td>Consequences</td><td>Safeguards/ checks</td><td>Actions</td></tr>
<tr><td>1.1</td><td>No Flow</td><td>a. pump motor failure</td><td>a. Fluid in pipe being overheated

pipe metal overheated and damaged

Pipe bursting and releasing oil into the firebox (in contact with flame)

Shutdown and loss of production</td><td>a. Reliable power supply to motor

low flow alarm</td><td>a. feed flow sensor and SIS on low flow
• Close fuel valves
• Open air valve
• Alarm with SIS
• Manual reset
• Short delay to guard against noise
• Manual activation of SIS possible
• Open stack damper

Low flow alarm using controller sensor</td></tr>
<tr><td></td><td></td><td>b. coupling failure</td><td>b. Hazard from metal pieces at high velocity</td><td></td><td>b. Install guard over coupling</td></tr>
<tr><td></td><td></td><td>c. feed valve closure</td><td>See (a) above</td><td>c. Flow controller, valve fail open</td><td>See (a) above</td></tr>
</table>

* This table is part of Table 5.6 in Chapter 5.

A similar process has been proposed for reliability and maintainability based on Failure mode and effects analysis (FMEA) (see, for example, Pride, 2014). However, when the safety and reliability studies are performed independently considerable duplication occurs and potential synergies are lost. Therefore, the two studies can be combined into what is now referred to as HAZROP – Hazard, Reliability and Operability – analysis (Hendershot et. al., 1998; Post and Hendershot, 2002). The integration of the two studies is facilitated by their many similarities, as summarized in the following.

- **Team orientation** – A multi-disciplinary team is required because of the wide knowledge base required to perform the study; no one engineer can successfully complete the study. Also, the study is led by a facilitator who is trained in managing these studies.
- **Facilities studied** – Naturally, the safety and reliability issues involve the same plant facilities. Neither study predetermines the important parts of the plant.
- **Management** – Both studies require thorough analysis of results, specific follow-up actions, and management to ensure that the work is completed.

The following advantages can be realized by integrating the studies.

- **Lower cost –**Although the combined study requires more time than either individual study, the combined study takes less time than performing two independent studies.
- **Skilled team –** The combined team includes people with a strong understanding of the integrated plant and of the mechanical equipment in the plant.
- **Improved results –** Practitioners report that the improved team gives improved results. Specifically, the emphasis on reliability results in fewer production losses.
- **Timing –** Practitioners note that the HAZOP is typically performed during design but that the RCM study is typically performed on operating plant. By performing both during design, problems are identified and fixed early, leading to smoother and shorter plant startups.
- **Hidden failures –** Both safety and reliability studies seek to identify "hidden failures", which are not directly observable until a fault occurs. An example of a hidden failure is a safety valve that is stuck closed, perhaps due to corrosion. The valve is normally closed and should open when the pressure exceeds a high limit; the failure to open represents a failure in the protection system that would certainly exacerbate the undesirable situation. Reliability studies concentrate on equipment and may lead to the better recognition of hidden failures.

To integrate the two studies into one HAZROP, the procedures must be modified. Primarily, additional guidewords are needed to consider reliability and maintenance issues.

The major issue with performing a thorough reliability study is the cost, mainly the time of skilled engineers and technicians. However, successful reliability centered maintenance (RCM) requires this study. In addition, safety studies are generally required by law. The integration of these two studies in a HAZROP involves more effort than either study alone. However, the HAZROP is reported to require much less effort than two independent studies (Post and Hendershot, 2002).

4.10 Conclusion

The best single word to describe the content and importance of this chapter is "lifecycle". While the word was used to modify the economic analysis, it really applies to the entire design and operation philosophy encompassing reliability. The life-cycle viewpoint includes all factors from "cradle to grave" for a process.

When concentrating on reliability, we emphasize the effects of design and operation on the performance of equipment, especially their failures. Reliability investments reduce the costs of failures, damage to equipment, maintenance and repair personnel, reprocessing work-in-progress materials, and lost production and sales. Therefore, a balance of investment of costs and revenues should be achieved by a good project, and the proper balance can be determined using Life Cycle Cost (LCC) analysis.

Reliability engineering is based on knowledge of component failure rates, e.g., pumps, motors, sensors, valves, pipes and so forth. The reliability of interconnections of equipment components can be predicted using various methods; here, Reliability Block Diagrams (RBD) are introduced, and more general simulation methods are available.

Reliability is influenced by plant design and operations. A wide variety of approaches have been introduced, and even these methods are not comprehensive. The chemical engineer must master these methods to understand best practices in plant design, because of the wide application of methods such as isolation for repair and replacement, redundancy, control to prevent excursions leading to damage, material inventories, and many more.

Maintenance has historically not received its due attention in process plants, but attitudes are changing. The current best practice, reliability-centered maintenance (RCM), matches maintenance approaches (and costs) appropriately to events based on consequences.

As explained in this chapter, the coverage of reliability is limited to scenarios where failures affect profit but not safety or serious environmental damage. Design for safety is based on achieving an acceptably low likelihood of hazardous conditions, not by an economic tradeoff. Naturally, no distinct boundary exists between reliability and safety, and the analysis techniques and design modifications to achieve acceptable performance are similar. In addition, analysis methods of failure and design modifications for improvement are quite similar. As a result, design and operation for reliability and safety are closely coupled and often the same personnel are involved in both topics. Therefore, this chapter, in addition to providing valuable engineering insights and methods for reliability, gives a useful introduction to the next chapter on safety.

References

Abbe, P. (2013) Lifecycle Costs for Capital Equipment In the CPI, *Chemical Engineering*, July 2013, 36-43

Abrahamson, D. and A. Sepeda (2009) Managing Security Risks, *Chemical Engineering Progress* , 105, 7, 41-47

Blank, L. and A. Tarquin (2012) *Engineering Economy, 7th Edition*, McGraw-Hill, New York

Barringer, H.P. and D. Weber, Life Cycle Cost Tutorial, Fifth International Conference on Process Plant Reliability, Houston, Texas, October 2-4, 1996 (http://www.barringer1.com/pdf/lcctutorial.pdf)

Cason, R. (1972) Estimate the Downtime Your Improvements will Save, Hydrocarbon Processing, January 1972, 73-76

CCPS (1993A) *Guidelines for Engineering Design for Process Safety*, American Institute of Chemical Engineers, New York

Block, H. and F. Geitner (1999) Use Equipment Failure Statistics Properly, *Hydrocarbon Processing*, January 1999, 49-53.

Camp, G. and D. Vandergriff (2004) What does it cost to cycle a heat-recovery steam generator?, *Combined Cycle Journal*, Feb 11, 2004, 18-20

Dhillon, B. (2005) *Reliability, Quality and Safety for Engineers*, CRC Press, Boca Raton, FL.

DOE (1998) United States Industrial Electric Motor Systems Market Opportunities Assessment, Dec. 1998 (https://www1.eere.energy.gov/manufacturing/tech_assistance/pdfs/mtrmkt.pdf)

DOE (1999) Market-Based Advanced Coal Power Systems, Appendix D, May 1999 (http://www1.fe.doe.gov/programs/powersystems/publications/MarketBasedPowerSystems/Market-Based_Advanced_Coal_Power_Systems.html)

DOE (2010), *Operations and Maintenance (O&M) Best Practices Guide*: Release 3.0, US Department of Energy, August 2010 (http://energy.gov/eere/femp/articles/operations-and-maintenance-best-practices-guide)

Hendershot et. al. (1998) Putting the "OP" back in HAZOP, MAINTECH South '98 Conference and Exhibition, Houston, Texas, December 2-3, 1998

Post, R. and D. Hendershot (2002) Synergistic Design Approach to Safety and Reliability Yields Great Benefits, *CEP*, 98, 1, 60-67

Illumin (2014) vol. 15, 1, Feb. 2014 (http://illumin.usc.edu/printer/110/is-safeguarding-america39s-nuclear-power-plants-impossible/)

Johnman, P., K.Hitz, E. Fyvie, H. Morris, D. Gosden, and B. Taber, Eraring Power Station Control Study, in Marlin, Thomas, John Perkins, Geoff Barton, and Mike Brisk (1988) *Advanced Process Control Applications, Warren Centre Industrial Case Studies of Opportunities and Benefits*, ISA, Research Triangle Park. (Copyright transferred to editors in 1995).

Kawauchi, Y. and M. Rausand (1999) *Life Cycle Cost (LCC) Analysis of Oil and Chemical Industries*, Norwegian Institute of Science and Technology, Report 99007, June 22, 1999. (http://frigg.ivt.ntnu.no/ross/reports/lcc.pdf)

Lees, F. (1996) *Loss Prevention in the Process Industries*, Volumes 1-3, Butterworth-Heinemann, Oxford

Lefton, S., P. Besuner, and D. Agan (2006) The Real Cost of On/Off Cycling, *Modern Power Systems*, Oct. 2006, 11-13

Lefton S., Nikhil Kumar, Doug Hilleman, Dwight Agan (2012) The Increased Cost of Cycling Operations at Combined Cycle Power Plants, Presented at the International Conference on Cycling Plant Charlotte, North Carolina November 2012 (http://www.investorvillage.com/uploads/14974/files/cycleCCplant.pdf)

Li, D., H.J. Marquez, T. Chen and R.K. Gooden (2006) Optimal Life-extending Control of a Boiler System, *IEE Proc.-Control Theory Appl.*, Vol. 153, No. 3, 364-370.

Loh, H., J. Lyons, and C. White (2002) Process Equipment Cost Estimation Final Report, DOE/NETL-2002/1169, January 2002, page 55

LUDB (2014) Creative Commons share alike 3.0 (http://clui.org/ludb/site/houston-fuel-oil-terminal)

Madhuranthakam, C.R., A. Elkamel and, H. Budman (2008) Optimal tuning of PID controllers for FOPTD, SOPTD and SOPTD with lead processes, *Chemical Engineering and Processing* 47 251–264

MaintenanceResources (2014) (http://www.maintenanceresources.com/referencelibrary/ezine/chemclean.htm)

Marlin, T. (2000) *Process Control*, *Designing Processes and Control Systems for Dynamic Performance*, McGraw-Hill, New York

Matches (2014) http://matche.com/EquipCost/

Mitchell, J. (1996) The long road to recovery: Community responses to industrial disaster, United Nations University Press, New York. (http://archive.unu.edu/unupress/unupbooks/uu21le/uu21le00.htm)

Modarres, M. (1993) *What Every Engineer should know about Reliability and Risk*, Marcel Dekker, New York.
Mukherjee, R. (1998) Effectively Design Shell-and-Tube Heat Exchangers, *CEP*, Feb. 1998, 21-37
Moubray, J. (1997) *Reliability Centered Maintenance*, Industrial Press, Oxford, 1997
National Aeronautics and Space Administration (NASA) (2000) Reliability Centered Maintenance Guide For Facilities And Collateral Equipment, February, 2000. (http://www.hq.nasa.gov/office/codej/codejx/Assets/Docs/RCMGuideMar2000.pdf)
Nowlan, F. and H. Heap (1978) Reliability-Centered Maintenance, U.S. Department of Commerce, Report AD-A066-579, December 29, 1978. (http://reliabilityweb.com/ee-assets/my-uploads/docs/2010/Reliability_Centered_Maintenance_by_Nowlan_and_Heap.pdf)
Nuclear Energy Institute (2002) (http://www.nei.org/News-Media/Media-Room/News-Releases/Analysis-of-Nuclear-Power-Plants-Shows-Aircraft-Cr)
Peters, M., K. Timmerhaus, and R. West (2003) *Plant Design and Economics for Chemical Engineers, 5th Edition*, McGraw-Hill, New York.
Pride, A. (2014) Reliability-Centered Maintenance, *Whole Building Design Guide* , National Institute of Building Sciences, (http://www.wbdg.org/resources/rcm.php#top)
Safecar, 2014 U.S. Department of Transportation (http://www-odi.nhtsa.dot.gov/owners/SearchSafetyIssues)
SolidsWiki (2014) http://www.solidswiki.com/index.php?title=Tube_Heat_Exchangers
Staroselsky, N. and L. Ladin, Improved Surge Control for Centrifugal Compressors, *Chemical Engineering*, May 21, 1979, 175-184
Towler, G. and R. Sinnott (2008) *Chemical Engineering Design; Principles, Practice, and Economics of Plant and Process Design*, Butterworth-Heinemann, Burlington, MA
Toyota (2011) Prius 2011 Owner's Manual, ToyotaMotorCompany
US DOD (1981) *Definition of Terms for Reliability and Maintainability*, MIL-STD-721C, June 12, 1981 (http://www.everyspec.com/MIL-STD/MIL-STD-0700-0799/MIL-STD-721C_1040/)
White, R. and R. Kurz (2006) Surge Avoidance for Compressor Systems, Proceedings of the 35th Turbomachinery Symposium, Texas A&M University Turbomachinery Laboratory , pg 123 (http://turbolab.tamu.edu/proc/turboproc/T35/)
Wikipedia, (2014) http://en.wikipedia.org/wiki/V-1_flying_bomb

Additional Resources

The following Internet sites provide useful information on reliability principles and applications to process equipment. Investigate the information in links variously referred to as tutorials, whitepapers and references.

- http://www.barringer1.com/
- http://www.reliableplant.com
- www.Reliabilityweb.com
- http://www.mutualconsultants.co.uk
- http://www.lifetime-reliability.com
- http://www.maintenanceresources.com
- http://www.theriac.org/

Test Your Learning

4.1. The goal of absolutely zero faults cannot be attained. In response, two competing viewpoints have developed. One viewpoint is "Normal Accident Theory" that views complex systems as inherently prone to faults that cannot be anticipated or prevented. The other viewpoint is "Highly Reliability Organizations" that views complex systems as manageable and concludes that well designed and operated system can perform their functions with an acceptably low risk, even if faults are inevitable. Review these two ideas and apply them to a process design that you have completed or are currently developing. As an introduction to the literature, see the following review paper and references therein; Leveson et. al. (2009) Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems, *Organization Studies,* 30 (02&03), 227–249.

4.2 A method for evaluating proposed designs for Reliability was proposed in the following article: Thompson, G., J. Geomine, and J. Williams (1998), A method of plant design evaluation featuring maintainability and reliability, *Proc Instn Mech Engrs* , Vol. 212 Part E, 71-80. Critically evaluate the method, identify good features, limitations and errors (if any), and the level of completeness of the design required for this analysis. Propose the types of plants that would be appropriate candidates for this method of analysis, e.g., continuous, batch, discrete piece manufacturing, etc.

4.2 The reliability of two systems, parallel and standby, are not predicted to be equal, although they appear to be very similar. Explain the difference between the reliability equations reported in the chapter.

4.3 A report is available on the Internet by Walt Boyes with the title and URL given below. Evaluate this article identifying strengths and shortcomings.

CONTROL Special Report: Ten Steps to Avoid Unnecessary Plant Shutdowns
(https://drupal.org/files/issues/Controls_Maintenance_Report.pdf)

4.4 The data on failures rates in Figure 4.3 show that a very small percentage of the systems studied experience wear-out failures that would have higher rates at longer times. Discuss why real industrial systems might experience this behavior, in contradiction to the bathtub curve.

4.5 A sample steam system is shown in Figure 4.24. Design a multiloop feedback control system for the steam system that satisfies the following the control objectives.

- Regulate the pressure of each steam header (pipe at each pressure level) near the desired valve.
- Provide the desired work for each steam turbine that is determined (and varies with) the plant production requirements.
- Minimize the "letdown" steam flow rates. Letdowns allow steam to flow directly from one header to another without work to the process.
- Respond to the variability in steam flows from the steam generators and to the steam consumers that are determined by plant production requirements.

The control system does not have to provide details for control of boiler drum level, steam superheater, and other details of the boiler control.

4.6 The concept of compressor surge is explained in the chapter, and simplified anti-surge controller is shown in Figure 4.32.

a. Describe how you would determine the set point for the anti-surge flow controller.
b. Discuss how the set point could be calculated in real-time to improve the energy efficiency of the compressor while achieving anti-surge control.
c. Discuss special requirements for the flow sensor, digital controller and control valve.
d. Investigate anti-surge control and select a design that will perform better than the design in Figure 4.32. If appropriate, your new design can be implemented in parallel with the design in Figure 4.32.

4.7 The design in Figure 4Q.7 provides level control for the tank. The flow rate through the process experiences wide variation with a low frequency; a histogram of the flow rate shows that it spends nearly equal time at all values between 25% and 115% of the Best Efficiency Point (BEP) of the centrifugal pump. Suggest modifications that will provide acceptable reliability and low life-cycle costs. Discuss advantages and disadvantages of the design.

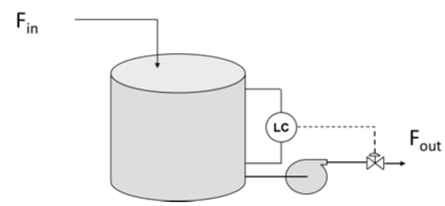


Figure 4Q.7

4.8 A continuously operating process experiences variability in liquid raw material feed delivery while desiring to maintain a constant feed rate oo 75 m^3/h to the process. For each of the delivery variations given below, determine the proper raw material inventory storage size.

a. The raw material is delivered in batches exactly every seven days.
b. The raw material is delivered continuously by pipeline, but the pipeline flow varies according to the following expression.

Raw material flow to storage in m^3/h = $F_{in} = 75 + A \sin(\omega t)$

with
- A = amplitude of the delivery variation
- t = time in hours
- ω = frequency of delivery variation in radians/h
- P = the period in hours (Recall that the $P = 2\pi/\omega$)

c. The raw material is delivered in batches of 12600 m^3 with the delivery time distributed according to a normal distribution with a mean of seven days and a standard deviation of one day.

4.9 A heat exchanger network is shown in Figure 4.21. A good practice is to periodically calculate the heat transfer coefficients for every exchanger to determine fouling, which will enable engineers to schedule appropriate maintenance, i.e., removal from service of an exchanger for cleaning.

a. Define the calculations required to evaluate the heat transfer coefficients
b. Design the sensors required for this heat exchanger performance monitoring task.
c. Determine checks on the measurement that you would recommend before performing the calculations

4.10 Select a chemical process from a previous or current course. Answer the following questions for the process.

a. Discuss whether Availability would be a good Key Performance Indicator (KPI).
b. Discuss whether Overall Equipment Effectiveness would be a good Key Performance Indicator (KPI).
c. Determine variables calculated from process data that would provide useful information on plant performance and that you would recommend as good Key Performance Indicators (KPIs).

4.11

a. For a single feedback control loop, determine the equipment required for the control loop to function.
b. Is this a series, parallel or other structure?
c. Investigate the failure rate for each element in the control loop.
d. Estimate the MTTF for the control loop

4.12 Since boilers are so critical to the successful operation of a process plant, key equipment are provided with backup. Assume that the plant requires two parallel pumps to function for successful operation. Determine the MTTF for the following structures. You may use the individual equipment MTTF from Block and Geitner (1999) as 3.5 years.

a. Two pumps
b. Three pumps
c. Four pumps
d. Five pumps

4.13 You have designed a process including a distillation tower separating propane overhead from butane and pentane bottoms. The tower bottoms in operating at 1.7 MPa and 110 °C. You have to specify a centrifugal pump for the bottoms stream. Should it conform to ANSI or API pump specifications? (Hint: looks like it is time to investigate these terms using the Internet.)

4.14 Cooling water is used extensively in process plants for temperatures above about 20 °C. Cooling water is low cost and generally reliable. However, the performance of cooling water systems degrades over time.

a. Sketch a typical industrial cooling water closed circuit, showing all major equipment and streams.

b. Identify major causes of performance degradation over time, and for each cause, recommend equipment design, operations and/or maintenance actions to reduce the rate of degradation or ameliorate the effects.

4.15 We achieve desired process performance by adjusting valves. Control valves are adjusted continually by process controllers. For reliable performance, the valve opening should closely follow the command sent by the controller.

a. Describe typical poor control valve performance.

b. Describe design guidelines that would contribute to good control valve performance.

4.16 Fuel gas consists mainly of methane and can contain ethane and heavier hydrocarbons as well as hydrogen. Many process plants generate fuel gas components as by-products that can be used as fuel in the plant. In some plants, a large number of units can generate and consume fuel gas. The operations of the producing and consuming units are not coordinated, can change rapidly, and the cost of failing to provide the fuel demanded by the consuming units is high – some units would have to be shut down. Proper operation of the fuel gas system is critical for reliable operation of the integrated plant.

A fuel gas distribution system is sketched in Figure Q4.16. We note that this system is similar to steam supply, in which any consumer can be supplied by any producer; this improves the reliability of the system. Some additional information is given in the following table. Note that the fuel gas to only one consumer can be manipulated by the fuel gas control system; this one can be manipulated because the consumer has an alternative source of fuel oil that can be adjusted to satisfy the consumer’s total fuel needs.

Flow	Manipulated by the fuel gas control system	Dynamics	Range (% of total fuel gas flow rate required to operate the plant)	Cost
Producing (P)	no	fast	0-100%	n/a
Consuming (C)	only one flow	fast	0-20%	very low
Generation	yes		0-100%	medium
Purchase	yes		0-100%	low
Disposal	yes		0-100%	high

a. Complete the missing information in the “Dynamics” column.

b. Determine the failure position for each of the numbered valves, v1to v5.

c. Determine the best steady-state behavior of the system. To accomplish this task, determine the best economic behavior of all flows as the system varies from no producing (P=0, C>>0) to large producing (P>>C). Plot the position of each control valve as a function of the value of the variable (P-C) as this variable goes from a very large-magnitude negative number to a large positive number.

d. Design a control system to (i) control the system gas pipe pressure, (ii) provide all fuel gas required by the plant consumers, and (iii) minimize the total cost of fuel consumed. You may add sensors and control valves but not change the piping.

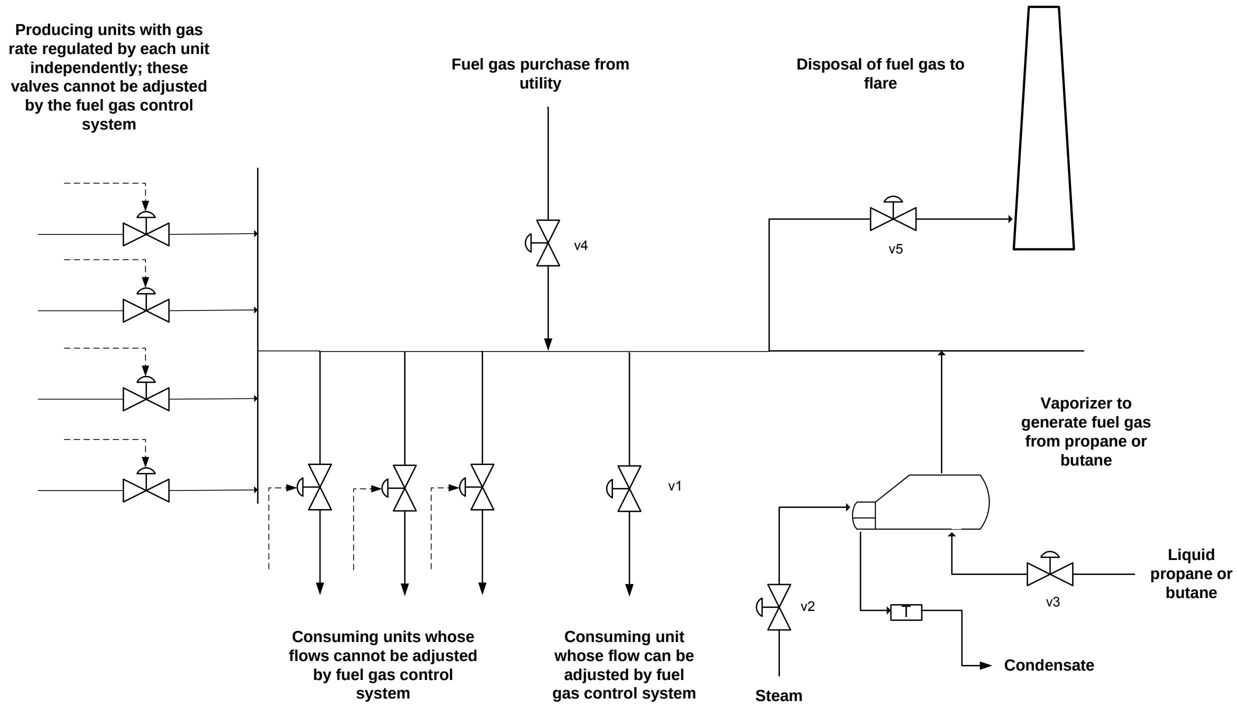


Figure Q4.16. Process plant fuel gas system for question 4.16. (Details like by-pass lines and safety relief are not shown to simplify the drawing.)

4.17

a Each of the elements (boxes) in Figure Q4.17a has a reliability of 0.99. The overall system functions if at least one path through the system involves functioning elements.

Determine the overall reliability of the system.

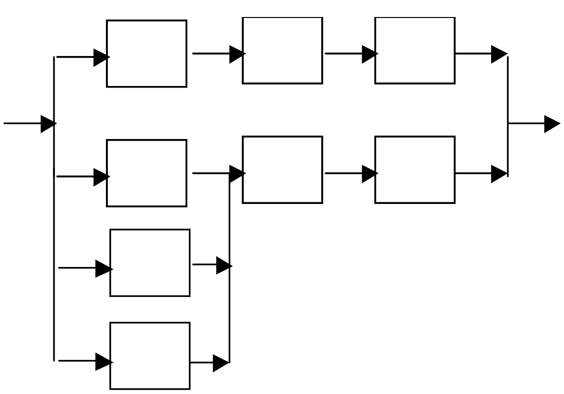


Figure Q4.17a.

b. Each of the elements (boxes) in the Figure 4.17b has a reliability of 0.98. All elements must function for the recycle system to operate. Determine the overall reliability of the system.

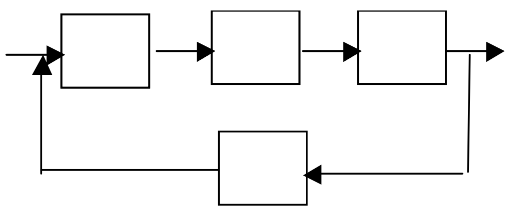
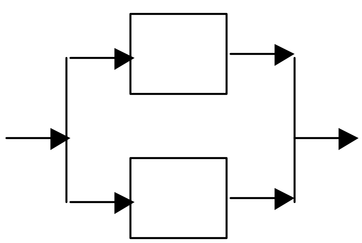


Figure Q4.17b

c. We have used the following expression for the reliability of the parallel system. Prove that the expression is correct. State key assumptions that are required for your solution to be valid.



$$R_{Parallel} = 1 - (1 - R_1)(1 - R_2)$$

4.18 Several inventory systems are depicted in Figures Q4.19 a-f. Derive the equation representing the material balance for each inventory, and based on your model, determine whether the system self-regulatory or non-self-regulatory.

4.19 RCM consists of four categories of maintenance activities. Select a process plant and discuss examples of all four RCM categories. Some potential plants are given in the following.

Reverse osmosis Desalination
Waste water treatment process
City water purification process

4.20 Investigate Failure Mode and Effects Analysis (FMEA) and prepare a 20 minute lecture-discussion for you class. Include a short exercise for students to complete after your presentation; naturally, you need to prepare a solution to the exercise.

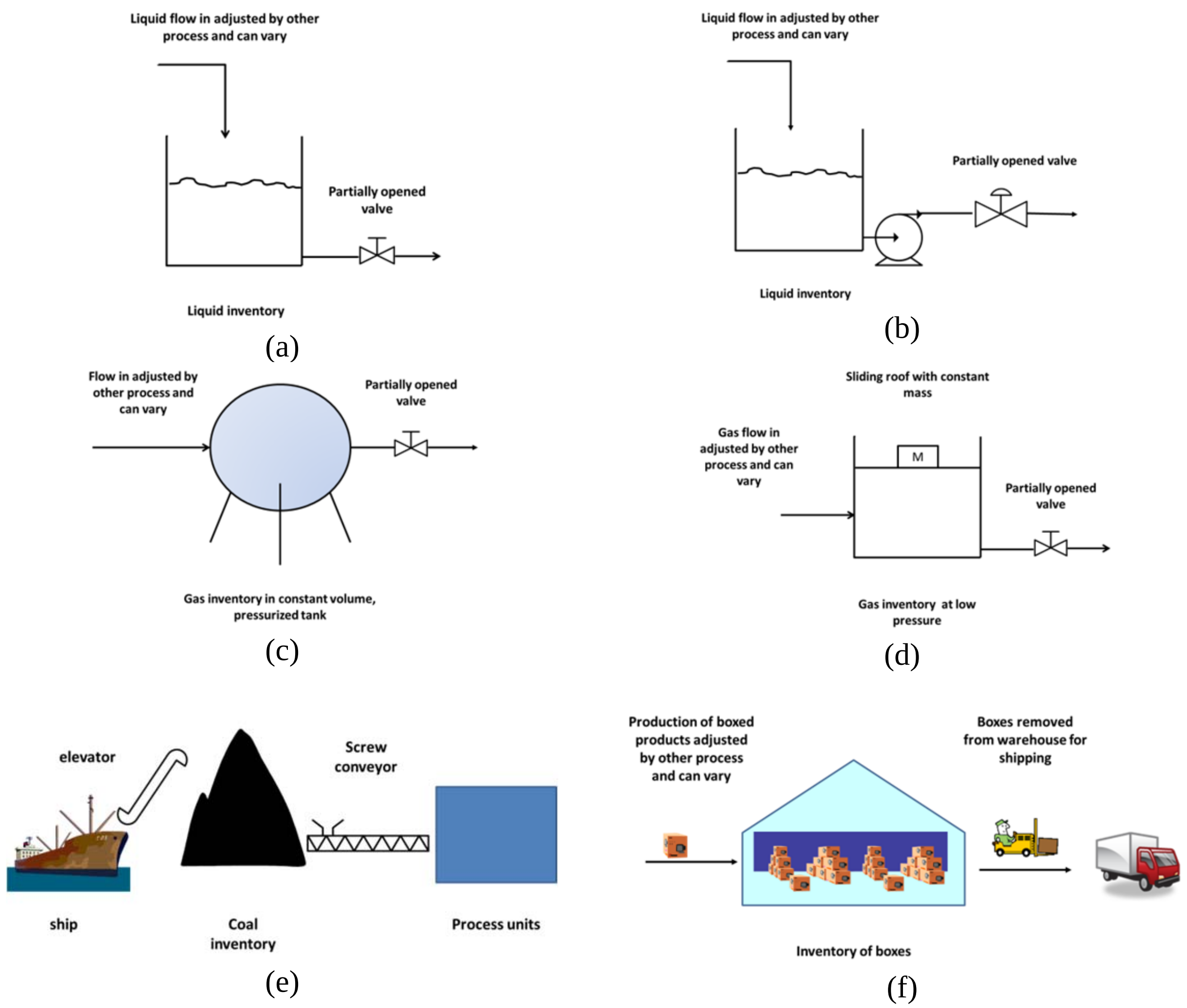


Figure Q4.19. Inventory systems for question 4.19.

Appendix A. Controller tuning for Life Extending Control

In this appendix, we consider a fired heater control example shown in Figure 4A.1 where the outlet temperature is controlled via feedback by adjusting the fuel flow rate. How can the engineer adjust controller parameters to adequately regulate the temperature without longer-term damage to the fired heater?

Some process dynamics and two sets of PID controller tuning are given in Table A4.1.

- One tuning (A) is based on tuning correlations that were recommended in the literature based on a study that considers only <u>controlled variable behavior</u> with perfect knowledge of the plant dynamics (Madhuranthakam et. al., 2008).
- The other tuning (B) is based on tuning that considers <u>controlled variable behavior, manipulated-variable behavior, disturbance source, measurement noise, and process uncertainty</u> (Marlin, 2000).

The dynamic responses for controllers using each of the two controller tunings in response to a set point change are shown in Figure 4A.1a and b. For Tuning A, the controlled variable returned to the set point more quickly. However, the fuel rate experienced a rapid and large transient; it exceeded its final value by a factor of about seven. This aggressive adjustment of the fuel causes thermal stress in the metal and brickwork in the firebox, and it would significantly reduce the time between expensive equipment maintenance and replacement. In contrast, Tuning B yields a much smoother transient, which is generally preferred for this equipment in spite of the somewhat slower response of the controlled variable.

Since the example in Figure A4.1 considers only one deterministic change, another scenario with a stochastic disturbance is evaluated. Three cases are shown in Figure A4.2; (a) no control, (b) Tuning A and (c) Tuning B. We see the dramatic difference in manipulated variable fluctuation between Tunings A and B. When we consider the continual controller actions over months and years, we recognize the importance of life-extending control using Tuning B. The more moderate feedback action results in a slightly higher variance of the controlled variable, which must be accepted when life-extending control is required.

Naturally, the feedback controller exists to maintain the controlled variable near its set point. Each process requires its own unique transient behavior to achieve the best overall performance considering short-term and long-term factors. The engineer is responsible for defining the proper tradeoff and achieving it.

The "takeaway" message is that the engineer must understand all performance goals for each process and tune the controllers according. The engineer must always consider the behavior of both the <u>controlled and manipulated</u> variables.

Table A4.1 Process and controller parameters

Process and controller parameters	Units	**A**. Tuning giving tight set point tracking without concern for equipment damage (Madhuranthakam et. al., 2008)	**B**. Tuning giving moderate valve adjustments to lengthen equipment life (Marlin, 2000)
Process gain	K/%open	3.5	
Process time constant	minute	2.1	
Process dead time	minute	0.23	
Controller gain (K_C)	% open/K	2.4	0.34
Controller integral time (T_I)	minute	3.2	0.58
Controller derivative time (T_D)	minute	0.07	0.0

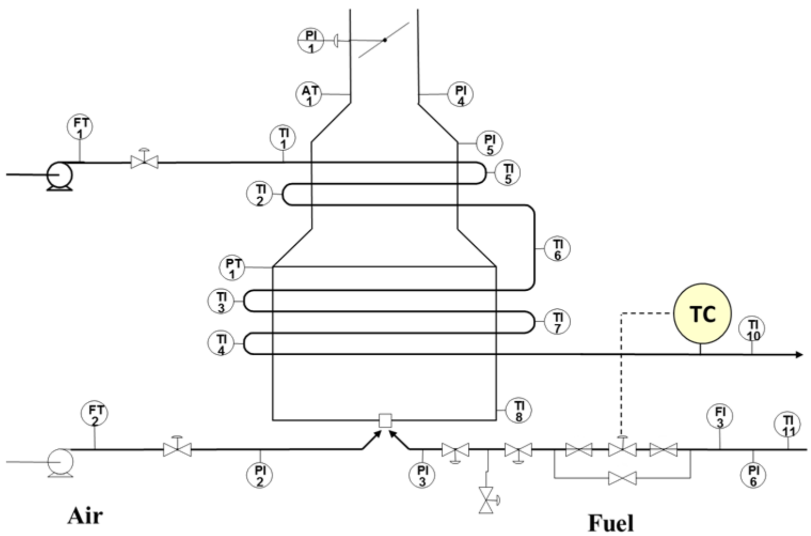


Figure A4.1. Fired heater with temperature control. (Other controllers and safety equipment are not shown.)

Figure A4.2a. Set point response for Tuning A

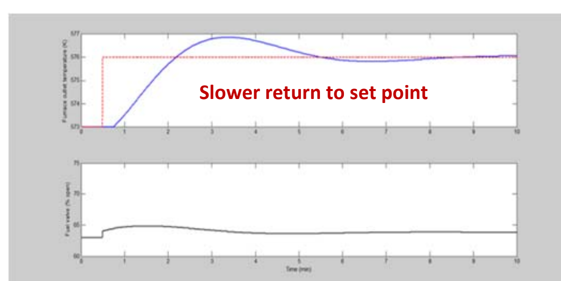
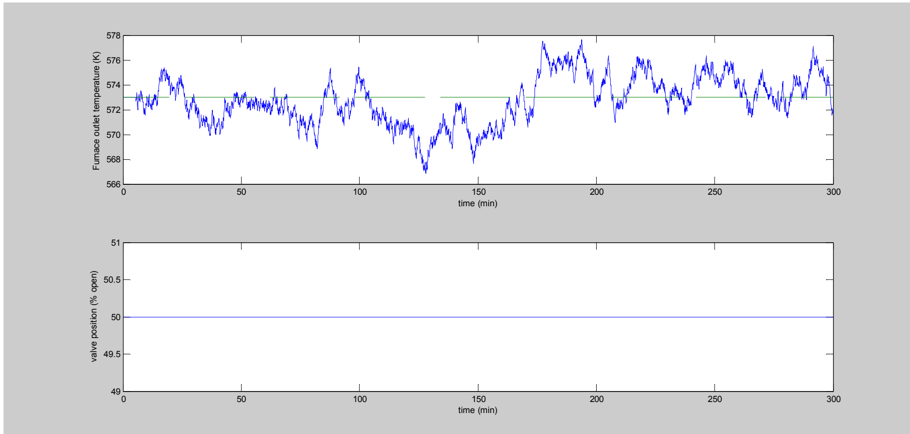
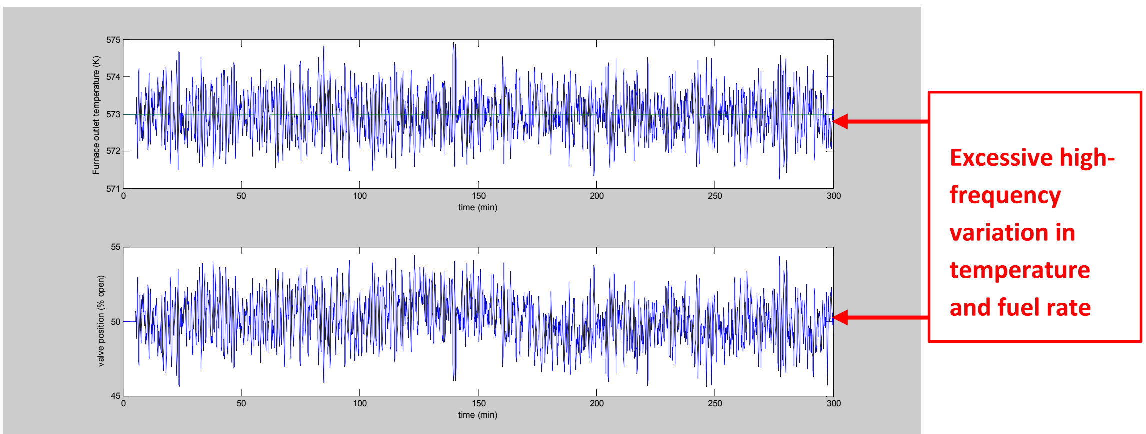


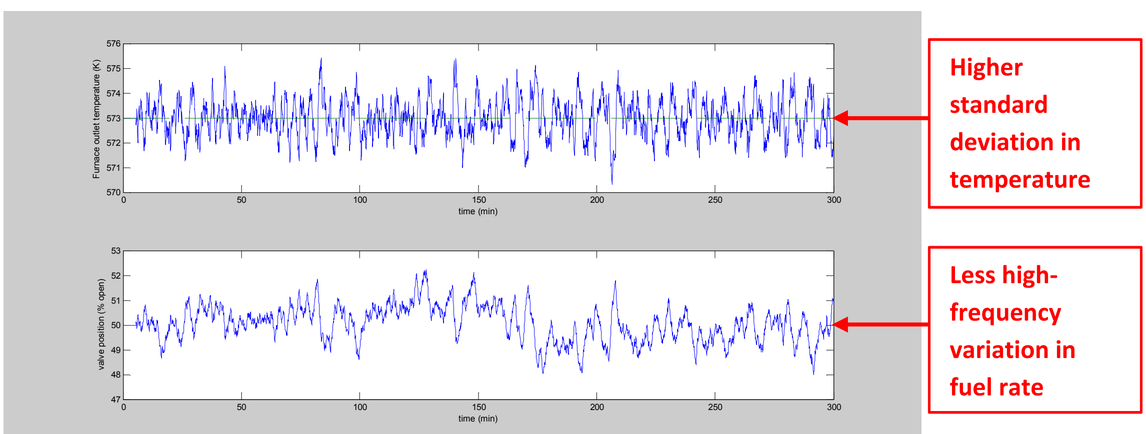
Figure A4.2b. Set point response for Tuning B



(a) No control, yielding a temperature variance of 1.95 K^2



(b) Tuning A yielding temperature variance of 0.59 K^2



(c) Tuning B yielding temperature variance of 0.76 K^2

Figure A4.3. Results of temperature control subject to stochastic disturbances for two controller tunings.