Exceptions: None.

Insight: Some of the most useful information comes from the operators who work in the plant every day. They may not fully understand the technical details, but their wealth of knowledge of the day-to-day problems and the dynamics of their plant can be invaluable to you. Building a strong relationship with the operators should be a top priority. If you watch their backs, they will watch yours.

Rule of Thumb: The more knowledge you master, the more valuable you become. Seek to know EVERYTHING, and never stop. Even experts in the automation field find themselves learning new things every day.

If we had to choose one trait above all others that places an engineer on the path to success, it would be a constant quest for knowledge.

Tip #19: Always Run Spare Wires and Plan for Expansion

Hunter Vegas (System Design)

Over my career I cannot think of a single time when I regretted running spare cables or oversizing field junction boxes. However, I can think of too many instances where I ran out of room and/or capacity much sooner than I had expected, and wished I had run MORE spares.

Concept: The incremental purchase cost of a 36 pair cable over a 24 pair cable is practically negligible when compared with the labor cost of running either cable. Install spare wire capacity whenever possible, or at least plan for future expansion when sizing junction boxes, cable trays, and control system I/O.

Details: During system design, always run spare cable, oversize the field junction boxes, and buy extra I/O cards. Ideally, the cost of this spare capacity can be worked into the project cost during the estimating phase so the money will be available when the project is approved. Even if the spare capacity was not included in the original budget, the additional cost of adding the extra capacity is usually low enough that it can be incorporated with no significant impact on the budget. If the project budget is so tight that larger cables or spare capacity cannot be installed, at least PLAN for future additions. Install slightly bigger field junction boxes and cable trays so that more cables can be added later. Oversize conduits, and leave a draw string in them so wires can be pulled in on future projects. Leave blank spaces in the I/O cabinets so I/O racks can be added later, or at least leave space in the room so I/O cabinets can be installed in a future project.

This concept is particularly true when running fiber optic cable. The labor to run a 6 fiber, 12 fiber, or 24 fiber cable is essentially the same and the material cost difference is low. Running a cable with less than 12 fibers is pointless, and if expansion is even slightly possible, run a 24 fiber cable.

Watch-Outs: Always ask about future expansion plans during the design phase of an automation project. By knowing how the ultimate system might appear, you can make minor design changes that will make future growth much less costly and difficult. If the system will double in size, you can lay out the I/O cabinets, power supplies, etc. in such a way that they can be easily upgraded in the future without burdening the current project significantly.

Exceptions: Occasionally an automation project involves a machine or a process that is so mature that future expansion is unlikely. This is not a common occurrence, but if this situation applies, clearly the cost of adding spare capacity would not be justified.

Insight: Project managers hate adding spare capacity after the project has been approved because they consider it "scope creep" and not part of the project. Plants adore spare capacity because it allows the execution of process improvement projects at a much reduced cost. In the long run, the company certainly saves money, but the project

For the manipulation of jacket temperature to control outlet temperature, the main process time constant (τ_p) is (positive feedback if heat of feed and reaction exceeds product of heat transfer coefficient and area):

$$\tau_p = (C_p{*}M_o)/[C_p{*}F_f + \Delta Q_r/\Delta T_o + U{*}A] \quad \text{(F-6g)}$$

For the manipulation of jacket temperature to control outlet temperature, the process gain (K_p) is:

$$K_p = (U{*}A)/[C_p{*}F_f + \Delta Q_r/\Delta T_o + U{*}A] \quad \text{(F-6h)}$$

For the manipulation of jacket temperature to control outlet temperature, the near integrator gain (K_i) is:

$$K_i = (U * A)/(C_p * M_o) \quad \text{(F-6i)}$$

For the manipulation of feed temperature to control outlet temperature, the process gain (K_p) is:

$$K_p = (C_p{*}F_f)/[C_p{*}F_f + \Delta Q_r/\Delta T_o + U{*}A] \quad \text{(F-6j)}$$

For the manipulation of feed flow to control outlet temperature, the process gain (K_p) is:

$$K_p = (C_p{*}T_f)/[C_p{*}F_f + \Delta Q_r/\Delta T_o + U{*}A] \quad \text{(F-6k)}$$

For manipulation of jacket temperature, the additional small secondary process time constant associated with the heat capacity and mass of the jacket wall is:

$$\tau_p = (C_w{*}M_w)/[U{*}A] \quad \text{(F-6l)}$$

Any change in the temperature at the heat transfer surfaces or the feed inlet must be dispersed and back mixed into the volume. This process deadtime (θ_p) is the turn over time that can be approximated as the liquid inventory divided by the summation of the feed flow rate (F_f), agitator pumping rate (F_a), recirculation flow rate (F_r), and vapor evolution rate or vapor bubble rate (F_v). Since this turn over time is computed in terms of volumetric flow rates, the liquid mass and the mass flow rates are divided by their respective densities as shown in Equation F-6m.

$$\theta_p = (M_o/\rho_o)/[(F_f + F_a + F_r)/\rho_o + F_v/\rho_v] \quad \text{(F-6m)}$$

If there is an injector (dip tube or sparger ring) volume, a change in composition at the nozzle must propagate by plug flow to the discharge points of the dip tube or sparger ring. The deadtime for a feed flow (F_1) is the injector volume (V_1) divided by the injection mass flow (F_1) divided by its respective density (ρ_1).

$$\theta_p = V_1/(F_1/\rho_1) \quad \text{(F-6n)}$$

Table 3-1. Analyzer Comparison

TYPES OF ANALYZERS / COMPONENTS TO MEASURE	ACID GASES	AIR	AMMONIA	ARGON	BENZENE	CARBON DIOXIDE	CARBON MONOXIDE	CATALYST RESIDUE	CHLORINE	COLOR	COMBUSTIBLE GAS	CONDUCTIVITY	DENSITY	ETHYLENE	FREON	HYDROCARBONS	HYDROGEN GAS	MERCURY	METALS	NITRIC OXIDE	NITROUS OXIDE	NITROGEN GAS	NITROGEN DIOXIDE	NITROGEN OXIDES (NOx)	OXYGEN GAS	ORP	OPACITY	ORGANIC COMPOUNDS	OZONE	pH	PROPANE	SPECIFIC GRAVITY (GAS)	SPECIFIC GRAVITY (LIQUID)	SULPHUR DIOXIDE	SULPHUR OXIDES (SOx)	VISCOSITY	WATER VAPOR (Moisture)
AMPEROMETRIC									Y								Y																	Y			
CAPILLARY TUBE																																				Y	
CATALYTIC			Y								Y			Y		Y									Y											
CHEMILUMINESCENCE			Y			Y																	Y	Y					Y					Y			
CONDUCTIVITY												Y											Y														
ELECTROCHEMICAL			Y			Y			Y														Y		Y												
FLAME IONIZATION DETECTOR					Y		Y				Y			Y	Y	Y											Y										
FOURIER TRANSFORM INFRARED			Y	Y	Y	Y	Y							Y	Y	Y							Y														
GAS CHROMATOGRAPH		Y	Y	Y	Y	Y	Y		Y					Y	Y	Y	Y						Y														
INFRARED ABSORPTION			Y		Y	Y	Y							Y	Y	Y							Y														
MASS SPECTROMETER		Y	Y		Y	Y	Y		Y					Y	Y	Y	Y						Y														
NON-DISPERSIVE INFRARED			Y		Y	Y	Y				Y			Y	Y	Y							Y														
PAPER TAPE					Y				Y														Y														
PARAMAGNETIC			Y		Y																																
pH																																					
POLAROGRAPHIC			Y			Y	Y		Y								Y						Y														
RADIATION ABSORPTION													Y																								
ROTATING DISK VISCOMETER																																				Y	
THERMAL CONDUCTIVITY DETECTOR			Y	Y		Y	Y		Y								Y						Y														
ULTRAVIOLET			Y		Y				Y	Y							Y						Y	Y					Y					Y			
VIBRATING U-TUBE													Y					Y																			
X-RAY FLUORESCENCE								Y										Y	Y																		
ZIRCONIA OXIDE										Y																Y											

Legend : Acceptable = Y Commonly used = Y

Maintenance (Shops and Support) Department

Maintenance department personnel have responsibility for planning and controlling maintenance programs. They inspect, lubricate, and repair equipment. Their mission is to provide quality maintenance service and activities through efficient and effective systems and technologies that enable production facilities to manufacture at the lowest cost. They keep equipment histories, especially with regard to standards and traceability. They keep track of spare parts inventories, spare parts needs, and extra machinery lists. They prepare maintenance procedures and training courses. They suggest and manage training of operating personnel on equipment so a high proficiency of operation is possible.

The maintenance organization responds to the needs of the operating organization within the guidelines established by that organization (down time and frequency) with the type of maintenance required to deliver the forecast. Maintenance group personnel determine the "how" and the "who" for the maintenance function.

Operations and Maintenance Cooperative Efforts

Some maintenance functions require the operating group to cooperate with the maintenance department to determine the equipment to be included in any maintenance program. The group must justify new equipment to be purchased based upon equipment history, costs, and level of quality to match customers' needs. This cooperative group must determine what needs to be done and where maintenance will be performed.

Some organizations must keep statistics and cost data on the maintenance of equipment. This data may be a part of the history file kept by the maintenance department, or it may be a separate function kept by a support group (such as the accounting department). Information and statistics are kept for both the operating group and the maintenance department. Purchase costs, frequency of repair, repair costs, and other statistical data become a part of the crunch cost data. This type of information allows for continuous improvement of equipment and procedures.

Maintenance Management Organization

There are maintenance organizations and then there are other maintenance organizations. Is there a specific formula for the right organization? Perhaps not.

Department members should have the skills and stature to earn the respect of those with whom they work. Trades people need to be able to demonstrate that they have the skills to meet the demands of the plant.

A good rule of thumb for determining the size of the maintenance department is an operating dollar value equal to 2% of the replacement value of the facility. A high tech rule of thumb is one person full time for each one to two million dollars of automatic control systems investment.

Many companies have adopted a team approach to maintenance management in which various department members are assigned to specific teams (shown in the star organization chart of Figure 5-2 as function points). Each function point becomes a team with a specific mission. Team members represent specific duties or areas such as operations, personnel, planning, workplace, and coordination.

Regular meeting times are established, and team members share concerns at these meetings. This is thought to be a more effective way to solve problems and provide a more efficient department with much more involvement in the decision-making process. Each department member has input in managing the department.

Department Supervisor

The position of department supervisor requires a very dynamic and versatile individual. First, this individual must be extremely knowledgeable of the plant and plant processes. Ten to twenty years experience is a requirement for first- or second-line maintenance supervision. Plant knowledge generally comes from

years of experience in a variety of different assignments. Background should be engineering or technology with good people skills, organizational abilities, etc. In the past it was generally thought that a skilled trades person with good people skills could advance to this position. Modern thinking favors the engineering base because of the rapidly advancing technologies and complexity of the modern plant and processes. An instrumentation and control background seems to prepare a person well for this position.

The department supervisor has traditionally held a position of leadership within the department, but traditional roles are changing. In addition to the leadership function, the role of resource person has been added to the position. A resource person within an organization may be called upon from the bottom up as well as from the top down and is the spokesperson for the department. He or she is also easily identified with the department.

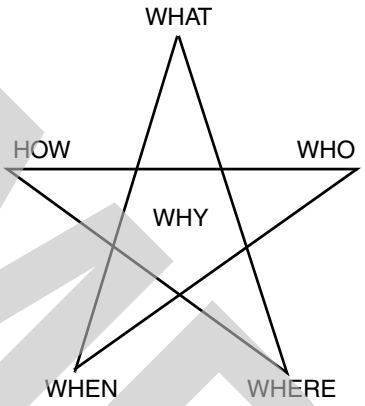

Figure 5-2. Team Functions.

Basic Requirements for a Maintenance Department

It is very important that all equipment be properly identified and critical instrumentation be backed up by up-to-date history files.

Planned Maintenance Program

A planned maintenance program should include the following important component programs: predictive maintenance, preventive maintenance, repair, corrective maintenance, and protective programs. A total program requires using each, based on data from the history file, cost reports, and critical applications. The following are definitions of important components of a planned maintenance program:

Planned maintenance — Each equipment piece is identified and its maintenance defined.

Repairs maintenance — Equipment fails and the required maintenance is performed.

Preventive maintenance — Equipment maintenance is scheduled prior to failure on an estimate of the life of the equipment.

Contents

Exercises

1.1 International safety standards require that operating companies follow the SIS safety life cycle specifically as outlined in the respective standard.

A. True

B. False

1.2 The SIS safety-life-cycle process can:

A. Reduce SIS costs

B. Increase process safety

C. Help insure that regulations are met

D. Provide an example of "good engineering practices"

E. All the above

1.3 Why should a company pay attention to IEC 61508 and IEC 61511?

A. It is legally required in some countries

B. It can save money on safety systems

C. Owners/operators often require compliance

D. A combination of answers A, B, and C

1.4 According to the SIS safety life cycle in IEC 61511, when should a process hazards analysis be conducted?

A. After the project scope is defined and the piping and instrumentation drawings (P&ID) are complete

B. Immediately before specifying the overall safety requirements

C. Immediately before verifying that the SIF will achieve the required risk reduction

D. Both A and B are correct

1.5 In the SIS safety life cycle, an SRS is done:

A. After defining the project scope

B. After the hazard and risk analysis phase

C. Throughout the phases of the life cycle

D. After overall safety validation

References

1. IEC 61508:2010, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems* (Geneva 20 – Switzerland: IEC [International Electrotechnical Commission]).
2. IEC 61511:2016, *Application of Safety Instrumented Systems for the Process Industries*, 2nd ed. (Geneva 20 – Switzerland: IEC [International Electrotechnical Commission]).
3. *Programmable Electronic Systems in Safety Related Applications – Part 1: An Introductory Guide* (Sheffield, UK: Health and Safety Executive, 1987).
4. *Programmable Electronic Systems in Safety Related Applications – Part 2: General Technical Guidelines* (Sheffield, UK: Health and Safety Executive, 1987).
5. DIN V VDE 0801, *Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben* (1990).
6. DIN V VDE 0801 A1, *Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben*, Änderung A1 (1994).
7. ISA-84.01, Application of Safety Instrumented Systems for the Process Industries (Research Triangle Park, NC: ISA [International Society of Automation], 1996).
8. IEC 61511:2003, *Application of Safety Instrumented Systems for the Process Industries* (Geneva 20 – Switzerland: IEC [International Electrotechnical Commission]).
9. ISA-84.00.01-2004 (IEC 61511 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector* (Research Triangle Park, NC: ISA [International Society of Automation]).
10. *Out of Control: Why Control Systems go Wrong and How to Prevent Failure*, (Sheffield, UK: Health and Safety Executive, 1995).
11. U.S. EPA (Environmental Protection Agency) and OSHA (Occupational Safety and Health Administration), *EPA/OSHA Joint Chemical Accident Investigation Report: Recurring causes of recent chemical accidents* (2000).
12. E. W. Scharpf, H. W. Thomas, and T. Stauffer, *Practical Safety Integrity Level Selection – Risk Analysis per the IEC 61511 Safety Lifecycle* (PA: Sellersville, exida, 2016).

3 Failure

A failure occurs when a device does not perform its intended function. For SISs, the definition of intended function is usually clear and should be properly recorded in the SRS. Each SIF in an SIS must

- perform its protection function;
- not falsely shutdown the process; and
- perform ancillary functions such as communications and diagnostics.

Nonperformance of any of these functions is a failure and must be considered in any probabilistic failure analysis.

Stress-Strength

The stress-strength concept of reliability is useful in understanding failures. In this concept, a failure will occur when some form of *stress* exceeds the associated *strength* of a device [1, 2]. Mechanical engineers adhere to this concept when selecting the size and type of material to be used for structural components. The mechanical engineer deals with a stress delivered by a physical force. The associated mechanical strength is determined by the component's ability to resist the force without becoming weakened or damaged.

In the safety and reliability analysis of the mechanical and electrical devices used in safety systems, many types of stress are present including chemical corrosion, electrical voltage/current transients, radio-frequency emission,

Table 3-1. Recommended Environmental Stress Levels for Control Room
Copyright exida, used with permission

Specification Type	Minimum Recommended Range				Recommended Test Specification
Operating Temperature	-10 C	to	60 C		IEC 60068-2-2 Test Bb
Operating Temperature Change	0.5 C/min				IEC 60068-2-14 Tests Nb
Storage Temperature	-40 C	to	85 C		IEC 60068-2-1 Tests Ab, Ad
Storage Temperature Change	10 C/min				IEC 60068-2-14 Tests Na
Operating Humidity	5%	to	95%	non-cond.	IEC 60068-2-3,Ca
Storage Humidity	0%	to	100%	cond.	IEC 60068-2-30, Dd
Vibration	10 Hz	to	150 Hz	2 g	IEC 60068-2-6, Fc
Mechanical Shock	15 g	for	11 msec.		IEC 60068-2-27, Ea
Corrosive Resistance	G3				ANSI/ISA-71.04
Electrostatic Discharge Immunity	6 kV		contact		IEC 61000-4-2
Electrostatic Discharge Immunity	8 kV		air		IEC 61000-4-2
Radiated E-Field Immunity	80 MHz	to	1000 MHz	20 V/m	IEC 61000-4-3
Radiated E-Field Immunity	1.4 GHz	to	2 GHz	6 V/m	IEC 61000-4-3
Radiated E-Field Immunity	2 GHz	to	2.7 GHz	3 V/m	IEC 61000-4-3
Magnetic Field	30 A/m				IEC 61000-4-8
Signal Line Burst Immunity (EFT)	2 kV				IEC 61000-4-4
Signal Line Surge Immunity (EFT)	2 kV				IEC 61000-4-5
Signal Line Conducted RF Immunity	150 kHz	to	80 MHz	10 V	IEC 61000-4-6
Signal Line Conducted RF Common Mode Immunity	15 Hz	to	150 Hz	10V	IEC 61000-4-16
Signal Line Conducted RF Common Mode Immunity	150 Hz	to	1.5 kHz	1 V	IEC 61000-4-16
Signal Line Conducted RF Common Mode Immunity	1.5 kHz	to	150 kHz	10 V	IEC 61000-4-16
AC/DC Power Line Burst Immunity	4 kV				IEC 61000-4-4
AC/DC Power Conducted RF Immunity	150 kHz	to	80 MHz	10 V	IEC 61000-4-6
AC Power Line Surge Immunity	2 kV		line to line		IEC 61000-4-5
AC Power Line Surge Immunity	4 kV		line to ground		IEC 61000-4-5
AC Power Conducted Common Mode RF Immunity	15 Hz	to	150 Hz	10V	IEC 61000-4-16
AC Power Conducted Common Mode RF Immunity	150 Hz	to	1.5 kHz	1 V	IEC 61000-4-16
AC Power Conducted Common Mode RF Immunity	1.5 kHz	to	150 kHz	10 V	IEC 61000-4-16
AC Power Voltage Dip Immunity	0.5 period		30% reduction		IEC 61000-4-11
AC Power Voltage Interruption	250 periods		95% reduction		IEC 61000-4-11
DC Power Line Surge Immunity	1 kV		line to line		IEC 61000-4-5
DC Power Line Surge Immunity	2 kV		line to ground		IEC 61000-4-5
DC Power Voltage Dip Immunity	10 msec.		60% reduction		IEC 61000-4-29
DC Power Voltage Interruption	30 msec.		100% reduction		IEC 61000-4-29
Functional Earth Burst Immunity	2 kV				IEC 61000-4-4
Functional Earth Conducted Common Mode RF Immunity	15 Hz	to	150 Hz	10V	IEC 61000-4-16
Functional Earth Conducted Common Mode RF Immunity	150 Hz	to	1.5 kHz	1 V	IEC 61000-4-16
Functional Earth Conducted Common Mode RF Immunity	1.5 kHz	to	150 kHz	10 V	IEC 61000-4-16
Radiated Emission, E-Field	30MHz	to	1000 MHz	30dB (μV/m) at 30m	EN55011
Conducted Emission	0.5 MHz	to	30 MHz	60dB (μV/m) at 30m	EN55011

4 Basic Reliability Engineering

Introduction

Several common metrics are used within the field of reliability engineering. The primary ones include reliability, unreliability, availability, unavailability, and MTTF (mean time to failure). This chapter develops these metrics assuming a single failure mode.

When different failure modes are considered (as they are when performing SIF verification), additional metrics are needed. These comprise a set of metrics that are defined in Chapter 6. The set includes probability of failing safely (PFS), probability of failure on demand (PFD), average probability of failure on demand (PFD_{avg}), mean time between failure spurious ($MTTF^{SPURIOUS}$), and mean time to failure dangerous ($MTTF^{D}$).

Successful Operation—No Repair

Probability of Success

Probability of success is often defined as the "probability that a system will perform its intended function when needed and when operated within its specified limits." The last phrase—*when operated within its specified limits*—informs the equipment user that the published failure rates apply only when the system is not abused, or otherwise operated outside its specified limits.

Example 4-2

Problem: A device has a constant failure rate of 5,000 FITS during its useful life. What is the MTTF?

Solution: 5,000 FITS equals 0.000005 failures per hour. The MTTF equals 1/0.000005 = 200,000 hours. In years, this equals 200,000/8,760 = 22.83.

Example 4-3

Problem: A pressure transmitter has an MTTF of 250 years. What is the failure rate in failures per year and FITS?

Solution: The failure rate per year equals 1/*MTTF* = 1/250 = 0.004 failures per year. To convert to FITS, which equals 10^{-9} failures per hour,

$$0.004/8{,}760 \textit{ hours per year} = 4.57 \bullet 10^{-7} \textit{ failures per hour} = 457 \textit{ FITS}.$$

Example 4-4

Problem: A pressure transmitter has an MTTF of 250 years. What is the reliability for a mission time of 5 years?

Solution: The reliability equals $e^{(-(1/250) \bullet 5)} = 0.98$

A Useful Approximation

Mathematically it can be demonstrated that certain functions can be written as a series of other functions. For all values of x, it can be shown that:

$$e^x = 1 + x + x^2/2! + x^3/3! + x^4/4! + \ldots \quad (4\text{-}7)$$

For a sufficiently small value of x, the exponential can be approximated with:

$$e^x = 1 + x$$

Substituting $-\lambda t$ for x:

$$e^{-\lambda t} = 1 - \lambda t$$

This is because $\int_0^{TI} A \bullet B$ is not equal to $\int_0^{TI} A \bullet \int_0^{TI} B$

If the PF_{avg} is used as the input from each component basic event, the PF_{avg} obtained by multiplying the gate inputs would be:

$$(\lambda TI/2) \bullet (\lambda TI/2) = (\lambda)^2 \bullet (TI)^2/4$$

The correct approach for an AND gate is to multiply the gate input probabilities first. This results in:

$$(\lambda TI) \bullet (\lambda TI) = (\lambda)^2 \bullet (TI)^2$$

Integrating this to obtain an average results in:

$$PF_{avg} = \frac{1}{TI}\int_0^{TI} \lambda^2 t^2 dt = (\lambda)^2 \bullet (TI)^2/3$$

Calculating the PF_{avg} before the gate input calculation results in an optimistic error, making the mistake even worse because this could lead to unsafe designs.

Time-Dependent Fault Tree Solutions

Time-dependent probabilities can also be calculated using a fault tree. A common method for accomplishing this is to set up a spreadsheet with fault tree input probabilities calculated for a small-time increment. The probability combinations are solved for each time increment, resulting in a time-dependent output. Table 5-1 shows the failure rates for two valves from the fault tree in Figure 5-16.

Table 5-1. Failure Rates for Two Valves

From Example 5-9	Failure Rate	Failure Rate Units
Main Valve	3,000	FITS
Secondary Valve	2,000	FITS

Table 5-2 shows the time-dependent spreadsheet solution. The left column provides time in hours. Columns from left to right calculate the probability of failure for each device in the model, one main valve and four secondary valves. The right column calculates the output of the fault tree for the time interval indicated in the left column.

It is important to know if a valve will open or close on trip. Table 6-4 shows an example failure mode classification based on a close-to-trip configuration.

Table 6-4. Final Element Failure Mode Categories

Instrument Failure Mode	SIF Failure Mode
Solenoid plunger stuck	Fail-Danger
Solenoid coil burnout	Fail-Safe
Actuator shaft failure	Fail-Danger*
Actuator seal failure	Fail-Safe
Actuator spring failure	Fail-Danger
Actuator structure failure - air	Fail-Safe
Actuator structure failure - binding	Fail-Danger*
Valve shaft failure	Fail-Danger*
Valve external seal failure	No Effect
Valve internal seal damage	Fail-Danger*
Valve ball stuck in position	Fail-Danger*
	* unpredictable - assume worst case

Note that the listings above are not intended to be comprehensive or representative of all component types, nor of all possible failure modes for the devices represented.

SIF Modeling of Failure Modes

When evaluating SIF safety integrity, an engineer must examine more than the probability of successful operation. The relevant failure modes of the system must be individually calculated. The normal metrics of reliability, availability, and MTTF only suggest a measure of success. Additional metrics to measure safety integrity include probability of failure on demand (PFD), average probability of failure on demand (PFD_{avg}), risk reduction factor (RRF), and mean time to fail dangerously ($MTTF^{D}$). Other related terms are probability of failing safely (PFS) and mean time to fail spurious ($MTTF^{SPURIOUS}$).

PFS/PFD

There is a probability that a SIF will fail and cause a spurious/false trip of the process. This is called *probability of failing safely* (PFS). There is also a probability that a SIF will fail such that it cannot respond to a potentially dangerous condition. This is called *probability of failure on demand* (PFD).

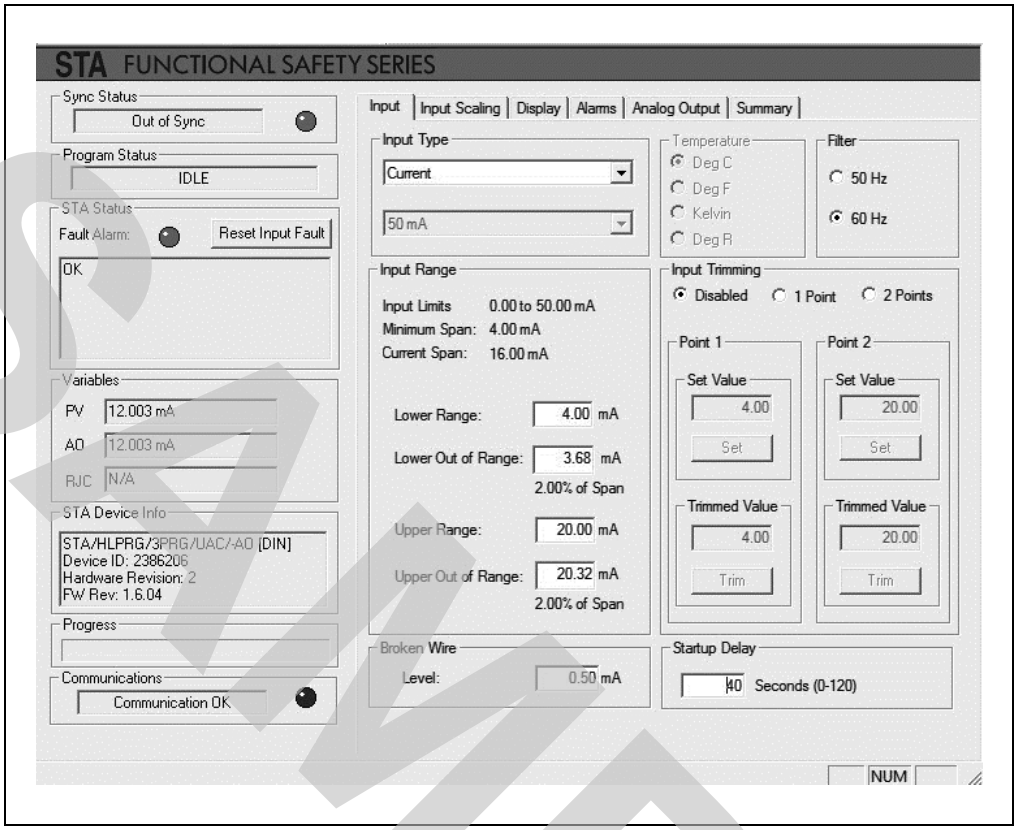

Figure 10-3. Logic Solver Input Configuration to Detect Current Levels and Indicate Internal Failure in Transmitters
Source: Copyright Moore Industries International, Inc.; reprinted with permission

The NAMUR-defined ranges are not considered standard by all sensor manufacturers, because some devices cannot support HART at 3.6 mA. In addition, fire and gas sensors with external power commonly use a 1 mA or a 2 mA current level to indicate an internally-detected fault. For these cases, the logic solver must be able to read those current levels, and to be programmed to interpret those levels as a diagnostic fault. This should be accomplished with a filter or timer to ensure that a transitioning current level does not cause a false trip.

When diagnostic annunciation is performed correctly, the probabilistic modeling can give credit for the automatic detection. The safety is improved and false trips can be avoided.

Figure 10-16. Moore Industries International STZ Temperature Transmitter in Different Packages
Source: Copyright Moore Industries International; reprinted with permission

Figure 10-17. Honeywell Smartline STT850 Temperature Transmitter
Source: Copyright Honeywell; reprinted with permission

tion, a realistic PFD_{avg} calculation reveals the design limitations. Equipment designed and certified as IEC 61508–compliant provides much better performance. Case 3 utilizes a United Electric Series One pressure switch. This is a Type B device with a relay output that can directly drive the ASCO 8314 3/2 direct-acting solenoid valve of the certified final element. The United Electric switch also has automatic diagnostics that are annunciated through a fault detection relay output. In this example, we assume that the relay is connected to an alarm in the repair center to indicate a requirement for service. Table 13-5 presents device failure rate data and other assumed parameters for SIL 1 Case 3. Table 13-6 summarizes the results of the SIL verification based on safety integrity evaluation, architectural constraints, and PFD_{avg} constraints.

Table 13-5. SIL 1 Case 3, Certified Switch: Failure Rate Data and Associated Parameters

Failure Rates (1/hr)						
		SD	SU	DD	DU	
Sensors						
	United Electric Series One 2SLP, relay	1.71E-6	7.6E-8	1.7E-6	8.0E-8	[3]
Logic Solver						
	Built into UE device	-	-	-		
Final Element						
	ASCO 8314 3/2 Direct-Acting Solenoid Valve	-	1.0E-7	-	9.7E-8	[3]
	Bray 98, Spring-Return Rack-and-Pinion Actuator	-	1.75E-7	-	4.27E-7	[3]
	Virgo P Series Ball Valve				5.63E-7	[3]
Mission Time (MT)						
The SIF equipment is expected to operate for 15 years before replacement and/or refurbishment and restoration in as-new condition.						
Proof Test Interval (TI)						
Sensors	3 years					
Logic Solver	N/A					
Final Element	3 years					
Proof Test Coverage (C_{PT})						
Sensors	99%					[4]
Logic Solver	N/A					[4]
Final Element	70%					[4]
Mean Time to Restore (MRT_{DD})						
Sensors	48 hours					
Logic Solver	N/A no diagnosed failures					
Final Element	N/A no diagnosed failures					

3.5 Answer: B. The failure is counted in the failure rate analysis, but the report indicates a systematic improvement is required in the device's proof test procedure.

3.6 Answer: B. The failure is counted in the failure rate analysis, but the report indicates that a systematic improvement is required to reduce the false trip rate by reconfiguring the PLC to recognize out-of-range current signals as a diagnostic indication.

Chapter 4: Basic Reliability Engineering

4.1 Answer: $F(1\ year) = 1 - 0.95 = 0.05$

4.2 Answer: $U = 1 - e^{(-0.015 \bullet 5)} = 0.072$

$U\ (approximation) = 0.015 \bullet 5 = 0.075$

4.3
Lambda = 0.015 f/y
MTTF = 66.7 years
MTTR = 24 hours
MTTR = 24/8,760 = 0.00274 years

From Equation (4-14)
SS Unavailability = MTTR / (MTTF + MTTR)
= 4.10778E-5

4.4
Lambda = 0.015 f/y
TI = 1 year
PF_{avg} = 0.015 • 1/2 = 0.0075 (perfect inspection)

4.5
Lambda = 0.06 f/y
TI = 1 year
C_{PT} = 0.6
LT = 10 years
PF_{avg} = 0.6 • 0.06 • 1/2 + (1-0.6) • 0.06 • 10/2
= 0.138

4.6 Answer: B. An estimate of probability can be made by dividing the number of failures by the number of trials, that is,

probability of failure = 5 / 112 = 0.044643

(Note: There is a level of uncertainty in this number due to the small number of trails. While this uncertainty can be calculated, doing so lies beyond the scope of this chapter.)

Symbols

Many mathematical symbols are used throughout this book. Some symbols are used only for the discussion of a particular topic; these symbols are therefore defined in that discussion and are not listed here. Some symbols may have multiple meanings that depend on the context; additional meanings are provided as needed for clarity in the appropriate sections of this book. Chapter 2 discusses the graphical symbols used in control system documentation. Chapter 15 uses a unique set of symbols that are defined at the beginning of that chapter.

The following symbols are used throughout this book:

b	=	bias value (manual reset) on proportional-only controller output
e	=	error (deviation between the set point and process variable)[1]
E	=	when capitalized, refers to (Laplace) transform of error
K	=	steady-state gain of first-order lag
K_C	=	controller gain (noninteractive and interactive control algorithms)
K_D	=	derivative gain (independent gains control algorithm)
K_I	=	integral gain (independent gains control algorithm)
K_P	=	proportional gain (independent gains control algorithm)
K_p	=	process gain (change in process variable/change in controller output)
m	=	manipulated variable, controller output
M	=	when capitalized, refers to (Laplace) transform of manipulated variable
PB	=	proportional band
PI	=	control algorithm with proportional and integral modes
PID	=	control algorithm with proportional, integral, and derivative modes
PV	=	process variable (see also symbol x)
SP	=	set point (see also symbol x_{SP})

1. The symbol e can also be used as the basis of natural logarithms, for example, when expressing the Laplace transform of dead time.

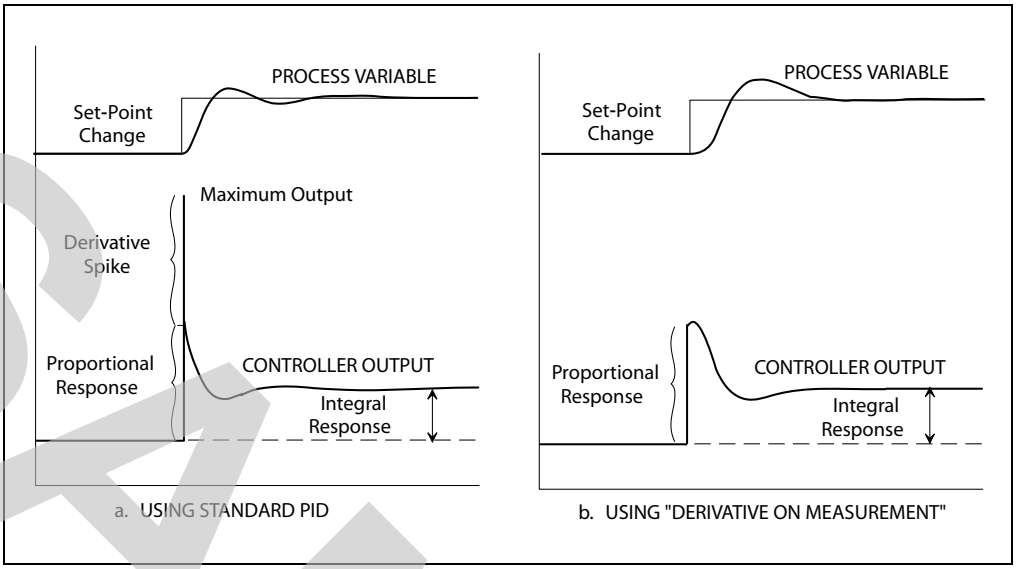

Figure 5-1. Response of Process Variable and Controller Output to a Set-Point Change

by making the derivative unit responsive to the measurement only, rather than to the error. Doing so will avoid the derivative spike caused by a set-point change. A block diagram of this configuration option is shown in Figure 5-2; the response to a set-point change is shown in Figure 5-1b. This modification is represented by the following equation:

$$m = K_C\left(e + \frac{1}{T_I}\int e\,dt - T_D\frac{dx}{dt}\right) \tag{5-2}$$

Note that the sign of the derivative contribution to the controller output has been changed from "+" to "–" in Figure 5-2. Since the derivative contribution must always act to oppose the direction of motion of the measurement, the derivative contribution must be negative on a load increase for a reverse-acting controller. If Figure 5-2 depicted a direct-acting controller, the sign of the derivative contribution would be changed to "+" and the signs at the summation point for the set point and measurement would be reversed. (Each figure in this chapter uses a reverse-acting controller as the basis of illustration.)

Suppose two controllers are mounted side by side, one with the standard form of the PID, and the other identical except for using derivative mode on measurement rather than on error. If the controllers were controlling identical processes and they were identically tuned, the response to a load upset would

three modes. In a manufacturer's library of software algorithms, a separate algorithm (integral-only) is normally provided that has the following form:

$$m = K\int e dt \tag{5-5}$$

The gain term may be expressed in several different ways, such as K, K_I, or $1/T_I$. In addition, some manufacturers may provide an integral-plus-derivative algorithm, in which case it may be converted into an integral-only algorithm simply by setting the derivative tuning parameter to zero.

Interactive or Noninteractive Controller

Which came first, the chicken or the egg? Commercially available analog controllers, using pneumatic mechanisms that achieved the general objectives of proportional, integral, and derivative control, were developed before a mathematical relationship for the ideal PID controller (Equations 4-5 and 5-1) had been formulated. When the working mechanisms were subsequently analyzed mathematically, they did not meet the "ideal" form. Instead, they could be described by the block diagram of Figure 5-9 and by the following equation, written in Laplace notation:[1]

$$M(s) = \hat{K}_C\left(\frac{(1+\hat{T}_I s)(1+\hat{T}_D s)}{\hat{T}_I}\right)E(s) \tag{5-6}$$

(The "^" over the symbols indicates the entered value for the tuning parameters.)

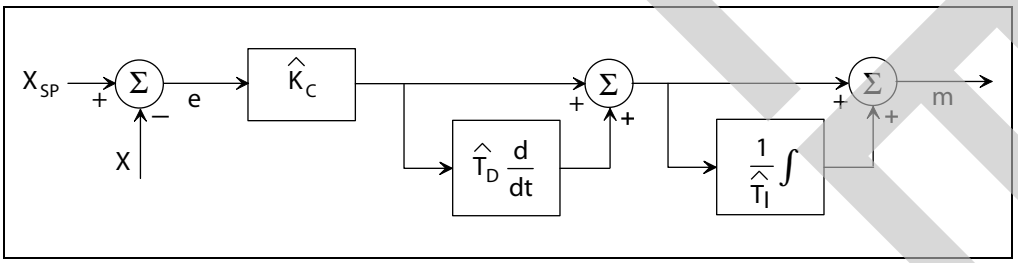

Figure 5-9. Block Diagram of an Interactive Controller with All Modes on Error

1. A further refinement of the mathematical description of commercially available analog controllers adds the effect of a filter to suppress measurement noise. This is discussed in the topic "Internal Filter" later in this chapter.

In Table 6-9, $\Delta F_{out-max}$ represents the maximum change in outflow resulting from a step change in inflow. The *outflow arrest time*, T_{aF}, represents the time from the occurrence of the disturbance until the maximum deviation of outflow from its value prior to the disturbance. The maximum rate of change of outflow is given because it is this quantity, rather than the size of the outflow change itself, that represents the maximum disturbance to a downstream process unit.

Table 6-9. Predicted Behavior of Outflow for Step Inflow Change

Behavior Attribute	Underdamped $\zeta < 1$		Critically Damped $\zeta = 1$
	Rigorous	Simplified	
Maximum Outflow Change $\Delta F_{out-max}$	$\left(1 + e^{-2\zeta f(\zeta)}\right)\Delta F_{in}$	Same as ←	$\left(1+e^{-2}\right)\Delta F_{in}$ (e = 2.71828)
Arrest Time T_{aF}	$T_I \times \frac{1}{\zeta\sqrt{1-\zeta^2}} \tan^{-1}\left(\frac{\sqrt{1-\zeta^2}}{\zeta}\right)$	$\frac{f(\zeta)}{\zeta} \times T_I$	T_I
Max Rate of Outflow Change	$\Delta F_{in} \frac{2\zeta}{T_I} e^{-\zeta f(\zeta)}$		$\Delta F_{in} \frac{2}{T_I} e^{-1}$
Note: In the table above, $f(\zeta) = \frac{1}{\sqrt{1-\zeta^2}} \tan^{-\frac{\sqrt{1-\zeta^2}}{\zeta}}$			

Working Relations for Liquid Level Control Tuning Parameters—Ideal Model

The relations given in Tables 6-7, 6-8, and 6-9 show the development of this tuning technique, but they are not very useful as working relations because of the amount of computation required. For three specific decay ratios, Tables 6-10 and 6-11 present working relations. The three decay ratios chosen are:

- Critically damped
- One-quarter decay
- One-twentieth decay

Liquid-Level-Control Tuning Example 1

Suppose you have a tank with the following specifications:

Tank diameter	5.0 feet
Distance between level transmitter taps	8.0 feet
Maximum outflow (upper end of outflow transmitter measuring span)	250 gpm

Calculate the tank holdup time:

$$\text{Surge volume} = \frac{\pi}{4} \times 5^2 \times 8 = 157.1 \text{ ft}^3$$

$$\text{Surge quantity} = Q = 157.1 \text{ ft}^3 \times 7.48 \frac{\text{gal}}{\text{ft}^3} = 1175.1 \text{ gal}$$

$$\text{Holdup time} = T_L = \frac{1175.1 \text{ gal}}{250 \text{ gpm}} = 4.7 \text{ min}$$

Also, suppose that you anticipate a worst-case disturbance would be a step inflow change of 10%. In the event of this disturbance, you want the level to deviate no more than 5% (about 5 inches). You would like the system to settle out rapidly, so you choose a 0.05 decay ratio.

ΔF_{in} = 10%

ΔL_{max} = 5%

With this data, use Table 6-10 to calculate tuning parameters:

$$K_C = \frac{0.50}{\left(\frac{5\%}{10\%}\right)} = 1.0$$

$$T_I = \frac{0.74 \times 4.7}{1.0} = 3.48 \text{ min/repeat}$$

We can use Table 6-11 to predict other properties of the response:

Overshoot ratio	OR = 0.34
Level arrest time	T_{al} = 2.88 × 3.48 = 10.02 minutes
Period	P = 8.09 × 3.48 = 28.2 minutes

The period may seem excessive, but because of the fast settling behavior selected, the maximum deviation during the second half-cycle will be about 1.1 inches, during the third half-cycle about 0.25 inches, and so on.

Maximum outflow	= 1.55 × 15% = 15.5% (peak value)
Outflow arrest time	= 2.88 × 3.48 = 9.9 minutes (time to peak value)
Maximum rate of change of outflow	= 0.35 × 10%/3.48 = 1% per minute

End of Liquid-Level-Control Tuning Example 1

Real-World Considerations

In Example 1, we determined tuning parameters for the level controller by considering only step changes in the set point or inflow. The only requirement that was imposed was to specify the ratio of maximum-level-change to inflow-step-change:

$$\left(\frac{\Delta L_{max}}{\Delta F_{in}}\right)$$

No consideration was made of the effect of a set-point change or of a disturbance to the tank outflow. Furthermore, only step changes in the set point and disturbances were considered. No consideration was given to the possibility of sinusoidal disturbances. For a sinusoidal input flow, the level and, consequently, the outflow will also vary sinusoidally at the same frequency as the input flow.

Example 1 also assumed that the control loop could be represented by an ideal model. In this section, we consider real-world conditions that could be encountered.

Sinusoidal Disturbance

Consider two cases of a dynamic system (e.g., a tank and level control system (responding to) some form of input function. In the first case, the input is a step, either a change in a set point or a disturbance. If the dynamic system is underdamped, the output will be a decaying signal at the *damped frequency* of the system. The damped frequency, ω, is related to the damping factor, ζ, and the *undamped natural frequency*, ω_n, of the system using Equation 6-30, which is repeated here:

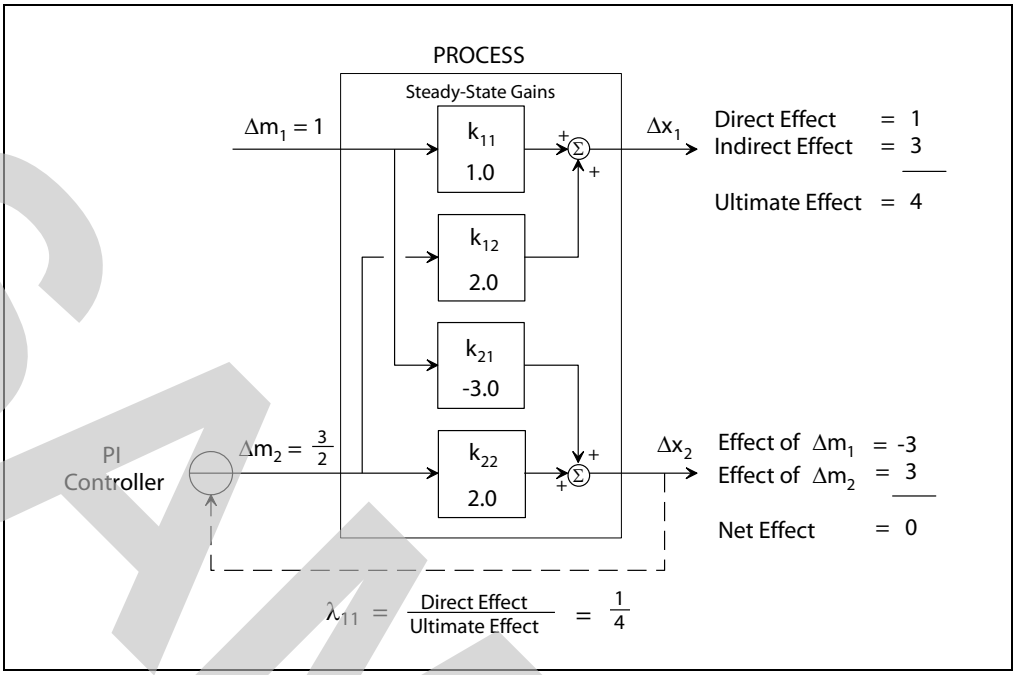

Figure 13-3. Example of Determination of One Relative Gain Element

Assume that a change is made to valve #1. Consider this as a change of 1 unit, that is, $\Delta m_1 = 1$. The *direct effect* on measurement #1 will be a change of 1 unit.[1]

$$\begin{aligned}\Delta x_{I(\text{direct})} &= k_{11} \times \Delta m_I \\ &= 1 \times 1 \\ &= 1\end{aligned}$$

If the PI controller between measurement #2 and input #2 is in Manual, then:

$$\text{process gain with the other loop in Manual} = \frac{\Delta x_{I(\text{direct})}}{\Delta m_1} = k_{11} \qquad (13\text{-}5)$$

The change in m_1 also changes measurement #2 by –3 units. That is:

$$\begin{aligned}\Delta x_2 &= k_{21} \times \Delta m_1 \\ &= -3 \times 1 \\ &= -3\end{aligned}$$

1. We will see later that the size of the step change cancels out, so its size is immaterial.