This book was written to replace *Safety Instrumented Systems Verification: Practical Probabilistic Calculations* by Harry Cheddie, PE, CFSE, and William M. Goble, PE, CFSE, 2005. The chapter sequence in the earlier book was partly maintained. A new book was needed, however, as a great deal of research has been completed in the field of SIF verification in the last 12 years. Far more field failure data is available, and the results of the field failure data studies have been included in recent updates of SIF verification methods and engineering tools. The performance-based approach with quantitative design verification is now far more realistic and continues to allow designers the ability to optimize and innovate.

The book covers the fundamental concepts from the field of reliability engineering, but does not get into the theory and development of those concepts. Other books cover those topics well; the intention in this book is to keep things practical.

The book does cover recent advances in SIF verification modeling and strives to provide far more realistic approaches to this task.
Iwan van Beurden, CFSE

Iwan van Beurden is the Chief Technology Officer, Director of Product Development at exida. He supports exida’s end user services, exida’s manufacturer services, and exida certification activities. He has more than 20 years of professional experience in the functional safety field. van Beurden is responsible for the development, maintenance, and certification of the exSILentia® integrated safety life cycle tool and associated products. van Beurden performs IEC 61508 development support, IEC 61511 life cycle services, functional safety assessments, and a variety of reliability analyses. He is an active member of the ISA84 committee and teaches exida and ISA training classes.

van Beurden is a Certified Functional Safety Expert (CFSE) and a senior member of ISA. He has published various papers and magazine articles. He holds a MS degree from Eindhoven University of Technology in Eindhoven, the Netherlands, where he majored in reliability engineering and graduated cum laude.
William M. Goble, PhD, PE, CFSE

William M. Goble is Managing Director and Cofounder of exida, a company that engages in research, training, product certification, and system consulting for safety-critical and high-availability systems. He has developed probabilistic analysis methods for functional safety that are widely used today. He has more than 40 years of experience in control systems, including product development, marketing, training, and functional safety certification.

Goble received a BS in electrical engineering from Penn State University, an MS in electrical engineering from Villanova University, and a PhD in reliability engineering from Eindhoven University of Technology. He is a registered professional engineer in the State of Pennsylvania and a Certified Functional Safety Expert (CFSE). He is an ISA Fellow. He has written hundreds of technical articles and several best-selling books on functional safety.
# Contents

About the Book ................................................................. ix
About the Authors ............................................................. xi

## Chapter 1. The SIS Safety Life Cycle .............................................. 1
  - Introduction ................................................................. 1
  - Functional Safety .......................................................... 2
    - Functional Safety Standards ......................................... 2
  - SIS Safety Life Cycle ....................................................... 6
    - Analysis Phase ......................................................... 9
    - Realization Phase ..................................................... 11
    - Operation Phase ..................................................... 12
  - Benefits of the SIS Safety Life Cycle ................................ 14
  - SIS Safety Life-Cycle Adoption ....................................... 15
  - Exercises ................................................................. 17
  - References ............................................................... 19

## Chapter 2. Safety Instrumented Systems ...................................... 21
  - Safety Instrumented Systems .......................................... 21
  - BPCS versus SIS .......................................................... 22
  - Safety Instrumented Function ......................................... 25
    - Equipment Used in a Safety Instrumented Function .......... 27
  - Exercises ................................................................. 28
  - References ............................................................... 30

## Chapter 3. Failure ............................................................. 31
  - Stress-Strength .......................................................... 31
  - Stress .................................................................... 32
Chapter 4. Basic Reliability Engineering. ........................................45
    Introduction. .................................................................45
    Successful Operation—No Repair ....................................45
        Probability of Success ..............................................45
        Reliability ...............................................................46
        Unreliability ............................................................47
        Mean Time to Failure (MTTF) ....................................48
        Constant Failure Rate ..............................................50
    Successful Operation—Repairable Systems .......................53
        Mean Time to Restore (MTTR) ..................................53
        Mean Time between Failures (MTBF) .........................55
        Availability ............................................................55
        Unavailability ..........................................................56
        Steady-State Availability .......................................56
        Average Unavailability with Periodic Inspection and Testing .......57
    Exercises .........................................................................62
    References .......................................................................64

Chapter 5. System Reliability Engineering ..........................65
    Introduction. .................................................................65
    System Model Building ..................................................66
    Reliability Block Diagrams ............................................66
        Series System ............................................................67
        Parallel System ...........................................................69
    Fault Trees .......................................................................71
        Fault Tree Symbols ....................................................71
        Comparison of the Reliability Block Diagram and the Fault Tree .73
        Fault Tree Solution Techniques ....................................73
        Fault Tree Common Mistakes .....................................77
        Fault Tree Average Probability Calculation ..................78
        Time-Dependent Fault Tree Solutions ............................82
    Markov Models ...............................................................84
        Comparison of Fault Trees and Markov Models ..................85
        Markov Solution Techniques ........................................86
    Realistic Safety Instrumented System Modeling ..................90
    Exercises .......................................................................90
    References .....................................................................93
Chapter 6. Equipment Failure Modes ................................................. 95
  Introduction ........................................................................... 95
  Equipment Failure Modes ...................................................... 95
    Fail-Safe ........................................................................... 96
    Fail-Danger ........................................................................ 96
    Annunciation ....................................................................... 97
    No Effect ........................................................................... 97
    Detected/Undetected .......................................................... 97
    Examples ........................................................................... 98
  SIF Modeling of Failure Modes ............................................. 100
    PFS/PFD ........................................................................... 100
    PFDavg ............................................................................ 101
  Exercises ............................................................................. 101
  References ............................................................................ 102

Chapter 7. Obtaining Failure Rate Data ...................................... 103
  Introduction ........................................................................... 103
  Failure Rate Estimation ........................................................ 103
    Manufacturer’s Field Return Data ....................................... 104
    Industry Database Consortiums .......................................... 107
    Site-Specific/Company Data-Collection Systems .................... 108
  Failure Rate Prediction .......................................................... 111
    B10 Cycle Testing ............................................................... 111
  Failure Modes Effects and Diagnostic Analysis (FMEDA) ....... 112
  Calibrated FMEDA—Combining Estimation and Prediction ...... 114
  Manual Proof Test Coverage ............................................... 115
  A Comparison of Failure Rates .............................................. 118
  Exercises ............................................................................. 121
  References ............................................................................ 122

Chapter 8. SIF Design and Verification Process ......................... 125
  Conceptual Design ............................................................... 125
  Modes of Operation .............................................................. 127
    Continuous Mode ............................................................. 128
    High-Demand Mode ......................................................... 128
    Low-Demand Mode .......................................................... 129
  Safety Requirements Specification (SRS) ............................. 130
  Equipment Selection ............................................................. 132
    Application Suitability ...................................................... 134
    Safety Integrity Evaluation ............................................... 135
  Architecture Constraints—Redundant Elements .................... 140
    Why Architecture Constraints? ......................................... 141
    Architecture Constraints from IEC 61511 ............................ 142
    Architecture Constraints from IEC 61508 ............................ 142
    Probability of Dangerous Failure Analysis ......................... 149
Chapter 9. SIF Probabilistic Verification ............................................. 155

Probabilistic Analysis ................................................................. 155
SIF Identification ........................................................................ 155
Continuous/High-Demand Mode Probabilistic Verification ............ 157
  Continuous-Demand Mode ....................................................... 157
  High-Demand Mode ............................................................... 157
Low-Demand Probabilistic-Verification Variables ......................... 162
  Failure Rates ........................................................................ 163
  Mission Time (MT) ............................................................... 164
  Proof Test Interval (TI) .......................................................... 164
  Proof Test Coverage Factor .................................................... 165
  Mean Time to Restore (MTTR) ................................................. 165
  Proof Test Duration (PTD) ....................................................... 170
  Probability of Initial Failure (PIF) ........................................... 171
  Site Safety Index (SSI) ............................................................ 172
  Redundancy—Common Cause ................................................ 173
  Probability of Failure on Demand Calculation ........................... 174
Probabilistic Calculation Tools .................................................... 176
Verification Reports ..................................................................... 176
Exercises .................................................................................... 177
References .................................................................................. 179

Chapter 10. SIS Sensors ................................................................. 181

Introduction ................................................................................ 181
Equipment Selection ................................................................. 181
Diagnostic Annunciation ............................................................ 182
  Logic Solver Configuration .................................................... 182
Probabilistic Modeling of Sensors ................................................ 185
Sensor Proof Test Strategies ....................................................... 195
  Multiple Proof Test Methods ................................................. 195
  Staggered Proof Testing ........................................................ 197
Sensor Redundant Designs ........................................................ 197
  Sensor Common-Cause Defense ............................................ 197
Pressure ..................................................................................... 199
Temperature ............................................................................. 202
Level ......................................................................................... 204
Flow ......................................................................................... 208
Toxic Gas/Flame Detectors ......................................................... 210
Burner Flame Detectors ............................................................ 212
Specialty Safety Sensors .......................................................... 212
Exercises .................................................................................... 213
References .................................................................................. 214
## Chapter 11. Logic Solvers

- Introduction .................................................................................................................. 217
- Equipment Selection .................................................................................................... 217
  - Cybersecurity ............................................................................................................... 218
- Relays/Pneumatic Logic ................................................................................................. 220
  - Smart Logic Modules .................................................................................................. 221
- Programmable Logic Controllers (PLCs) ...................................................................... 222
- Safety Programmable Logic Controllers ...................................................................... 222
  - Special Purpose Safety Controllers .......................................................................... 224
- Probabilistic Modeling of the PLC ................................................................................ 226
  - Failure Rate Data for PLC ......................................................................................... 227
  - Probabilistic Modeling of an Advanced Safety PLC ..................................................... 230
- Safety PLC Proof Testing .............................................................................................. 230
- Exercises ....................................................................................................................... 231
- References ..................................................................................................................... 231

## Chapter 12. Final Elements

- Introduction .................................................................................................................... 235
- De-energize-to-Trip Design ......................................................................................... 235
- Equipment Selection .................................................................................................... 236
  - Application Suitability ............................................................................................... 237
  - Safety Integrity .......................................................................................................... 237
- Final Element Interface Devices .................................................................................. 238
  - Solenoid Valves .......................................................................................................... 238
  - Quick Exhaust Valves (QEVs) ................................................................................... 243
  - Volume Booster Valves .............................................................................................. 245
- Actuators ....................................................................................................................... 246
  - Diaphragm Actuators .................................................................................................. 247
  - Piston Actuators ......................................................................................................... 248
  - Scotch Yoke Actuators .............................................................................................. 248
  - Rack-and-Pinion Actuators ....................................................................................... 250
  - Motor-Driven Actuators ............................................................................................ 250
  - Actuator Failure Modes ............................................................................................. 251
- Valves ............................................................................................................................ 251
  - Globe Valve ................................................................................................................ 252
  - Wedge Gate Valve ...................................................................................................... 254
  - Plug Valve .................................................................................................................. 254
  - Ball Valve ................................................................................................................... 256
  - Butterfly Valve .......................................................................................................... 258
  - Valve Failure Modes .................................................................................................. 259
- Integrated Final Element .............................................................................................. 260
- Probabilistic Modeling of Final Elements .................................................................... 261
  - Tight Shutoff Requirements ....................................................................................... 262
  - Close-to-Trip versus Open-to-Trip ............................................................................. 262
  - Service Category ........................................................................................................ 262
Introduction

The safety instrumented system (SIS) safety life cycle can be simply defined as an engineering process with design, analysis, and testing steps to ensure that SISs are effective in the key mission of:

- Risk reduction
- Optimal life-cycle cost of each system

The activities associated with the SIS safety life cycle start when the conceptual design of the facilities is complete, and stop when the facilities are completely decommissioned. The key activities associated with the SIS safety life cycle are analyzing risks and the need for risk reduction; establishing performance requirements for all safety functions in a system; implementing the system based on required performance criteria; and ensuring that the system is always operated and maintained correctly.

When the SIS safety life cycle is used with an existing system, the first step is to review and update the process hazard analysis and safety integrity level (SIL) selection. Given that information, the “as installed design” is documented and verified via analysis to determine if the design meets the verification requirements of current standards. Often it is discovered that the design is stronger than needed. In that case, there are opportunities to reduce ongo-
ing maintenance costs by increasing the proof test interval. The same general
design process is used with the objectives of:

- Risk reduction
- Ongoing optimal life-cycle cost going forward of each system

Functional Safety

Commission (IEC), IEC 61508, defines safety as \textit{freedom from unacceptable}
\textit{risk}. This is a good definition because it does not include “the elimination of
risk.” Functional safety has been defined in IEC 61508 as “part of the overall
safety relating to the equipment under control (EUC) and the EUC control
system which depends on the correct functioning of the electrical/electronic/
programmable electronic (E/E/PE) safety-related systems and other risk
reduction measures.” Functional safety has a similar definition in IEC 61511
[2], which states “part of the overall safety relating to the process and the
BPCS (basic process control system) which depends on the correct functioning
of the SIS and other protection layers.” The phrase “correct functioning of the
SIS” is key. A high level of functional safety means that an SIS will work cor-
rectly and with a high probability of successful operation. This success is
achieved with the selection of high-quality equipment that is well suited for
the intended purpose, and supported by a complete, high-quality operations
and maintenance program.

Functional safety is therefore the key objective in SIS design. To achieve the
right level of functional safety, several issues must be considered that may not
be part of the normal design process for automation systems. These issues are
provided as requirements in international standards.

Functional Safety Standards

For as long as automated systems have existed, engineers have designed auto-
matic protection into them. Engineers often have specifically designed many
of these automatic protection systems with pneumatic logic or electrical relays
because these components tended to fail in a de-energized mode. Systems
were designed to be safe when the automation de-energized. They were, in
other words, designed to “fail safe.”

As the logic became more complicated, systems expanded to include large
panels packed with relays and timers. It was, perhaps, natural for some engi-
neers to convert this logic to a new “solid-state” design when these compo-
nents became available in the late 1960s. Figure 1–1 illustrates an early solid-
state module designed to implement “burner logic” using diode transistor 
logic (DTL), an early form of simple integrated circuit logic. Unfortunately, 
there was little consideration of the component failure modes of these designs. 
The simple DTL systems had a much higher probability of dangerous failure 
than conventional pneumatic and relay-based systems.

When the first programmable electronic equipment, called programmable logic 
controllers (PLC), were created as an alternative to relay logic, many engineers 
immediately believed these new devices would be perfect for automatic pro-
tection applications. The functionality of these electronic devices, they felt, 
encompassed all that would be needed, and more. However, some engineers 
realized that the failure characteristics of solid-state/programmable electronic 
equipment might be quite different from traditional equipment. Other engi-
neers were well aware of the “crash rate” and unpredictable failure modes of 
software systems at the time.
In fact, some government regulators banned the programmable electronic equipment for use in automatic protection functions. Others began working with industry experts to establish guidelines for using electronic equipment in “emergency shutdown” applications. Eventually, international standards committees were formed and standards covering the design and usage of equipment in SISs were published.


Many members of these national safety standards efforts became members of an international committee that eventually wrote IEC 61508. This standard began in the mid-1980s when the IEC Advisory Committee of Safety (IEC ACOS) set up a task force to consider standardization issues raised by using programmable electronic systems (PESs). Work began within IEC SC 65A/Working Group 10 on a standard for PES used in safety-related systems. This group merged with Working Group 9, in which a standard on software safety was in progress. The combined group treated safety as a system issue. The first parts of IEC 61508 were published in 1998, with the release of the final parts of the first edition in 2000.

IEC 61508 is a basic safety publication of the IEC. As such, it is an “umbrella” document that covers multiple industries and applications. A primary objective of the standard is to help individual industries develop supplemental standards tailored specifically to those industries based on the original IEC 61508 standard. A secondary goal of the standard is to enable the development of E/E/PE safety-related systems where specific application sector standards do not already exist. IEC 61511 [8] is an industry-specific standard for the process industries that is based on IEC 61508. ISA-84.00.01-2004 (IEC 61511 Mod) [9] was released as the U.S. version of IEC 61511 in September 2004. Note that it is identical to IEC 61511 in every detail, except it also includes a grandfather clause taken from the Occupational Safety and Health Administration (OSHA) publication OSHA 29CFR 1910.119.

One clear goal of the committee was to create an engineering standard that would improve safety via the use of automation systems. Therefore, it was
essential to understand what had gone wrong in the past. A study [10] performed by the HSE in the United Kingdom revealed that many of the failures of automation systems to provide protection were caused by activities before and after the system had been designed. Figure 1-2 illustrates their results.

![Figure 1-2. Control System Accident Causes](image)

A significant percentage of the problems were caused by poor specification, that is, functionality that was missing or incorrect. How can a control system designer create an automatic protection function when that designer does not know its performance requirements? Many problems also occurred during installation, commissioning, operations, and maintenance.

In 2000, the U.S. Environmental Protection Agency (EPA) and OSHA investigated recent accidents at chemical facilities and refineries [11]. When all the incidents were compared, some common themes were identified:

- **Inadequate hazard review or process hazards analysis** – In almost every accident, Process Hazards Analysis (PHA) was found to be lacking. This relates to identifying the hazards and properly specifying the SIS based on the risk reduction required to mitigate hazardous events.

- **Installation of pollution control equipment** – They felt that this was also a reflection of inadequate hazards analysis and inadequate management of change procedures when adding new equipment that was not part of the original design. This item was listed separately due to the large number of these incidents.
• **Use of inappropriate or poorly designed equipment** – In several accidents, the equipment used for a task was inappropriate. Better design performance was required.

• **Warnings went unheeded** – They indicated that most incidents were often preceded by a series of smaller accidents, near misses, or accident precursors. Operations and maintenance procedures must include analysis, root cause investigation, and corrective action.

To a great extent, the EPA/OSHA findings support the results of the HSE study. They also emphasize that the key issues were identification of hazards and proper specification of the SIS taking the hazards into consideration. Both studies made it clear that focusing on programmable equipment and software design was insufficient. A life-cycle approach was needed. One of the fundamental concepts that has emerged from the functional safety standards is use of the SIS *safety life cycle*.

### SIS Safety Life Cycle

The SIS safety life cycle is an engineering process that contains all the steps needed to achieve high levels of functional safety during the conception, design, operation, and maintenance of instrumentation systems. Its objective is clear: an automation system designed in accordance with these requirements will predictably reduce risk in an industrial process. Figure 1-3 depicts a simple version of the safety life cycle.

The SIS safety life cycle begins with the conceptual design of a process and ends only after the SIS is decommissioned. The key idea here is that safety must be considered from the very inception of the conceptual process design, and must be maintained during all design, operation, and maintenance activities. The SIS safety life cycle has three phases, generally called *analysis* (scope and hazard review portion of projects), *realization* (design portion of projects), and *operation* (actual operation including maintenance and proof testing).

Figure 1-4 illustrates the SIS safety life cycle from the IEC 61508 standard. While this drawing shows additional details of the SIS safety life cycle, the three distinct phases are still clearly present. The IEC 61508 SIS safety life cycle indicates that most of the analysis phase activities constitute a logical sequence. After hazard and risk analysis are performed, safety requirements for the system are established. Some safety requirements are met by what IEC 61508 calls “external risk reduction facilities,” including changes in process
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,
mechanical vibration/shock, temperature, humidity, human error, gamma radiation, and other variables.

A given device is designed to resist a specified level of stress. Standards have been written to characterize expected stress levels in an industrial environment, together with the recommended associated test method (see Table 3-1). Designers’ products often meet or exceed these stress levels. The selection of various design parameters and protection components dictates the initial strength of a product. If the manufacturing process identically duplicates each product, each device’s strength will meet its intended design. Defects in raw materials and errors in the manufacturing process will reduce strength from unit to unit in an apparently random way.

**Stress**
Stress changes with time and is influenced by many independent parameters. Each of these independent parameters affects the stress level in a manner that could be modeled by a probability distribution. Given a large number of independent stress parameters, the central limit theorem would indicate a normal probability density function for stress. The normal distribution that characterizes stress is defined by both its mean and its standard deviation.

**Strength**
Because actual strength differs from unit to unit as a result of manufacturing errors and material defects, strength in a collection of manufactured products can also be modeled by a normal probability distribution. In addition, strength tends to decrease with operating time as a result of wear, chemical corrosion, and material aging. Some strength factors also decrease depending on applied stress levels.

Figure 3-1 illustrates the stress-strength concept. The horizontal axis represents the level of stress or strength. The curve labeled “Stress” is formed by integrating the normal distribution for stress from $x$ to infinity, where $x$ is any point representing stress on the horizontal axis. Therefore, the curve labeled “Stress” represents the probability that the stress is greater than the value of the stress variable on the horizontal axis.
### Table 3-1. Recommended Environmental Stress Levels for Control Room

*Copyright exida, used with permission*

<table>
<thead>
<tr>
<th>Specification Type</th>
<th>Minimum Recommended Range</th>
<th>Recommended Test Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Temperature</td>
<td>-10°C to 60°C</td>
<td>IEC 60068-2-2 Test Bb</td>
</tr>
<tr>
<td>Operating Temperature Change</td>
<td>0.5°C/min</td>
<td>IEC 60068-2-14 Tests Nb</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-40°C to 85°C</td>
<td>IEC 60068-2-1 Tests Ab, Ad</td>
</tr>
<tr>
<td>Storage Temperature Change</td>
<td>10°C/min</td>
<td>IEC 60068-2-14 Tests Na</td>
</tr>
<tr>
<td>Operating Humidity</td>
<td>5% to 95%</td>
<td>IEC 60068-2-3, Ca</td>
</tr>
<tr>
<td>Storage Humidity</td>
<td>0% to 100%</td>
<td>IEC 60068-2-30, Dd</td>
</tr>
<tr>
<td>Vibration</td>
<td>10 Hz to 150 Hz</td>
<td>IEC 60068-2-6, Fc</td>
</tr>
<tr>
<td>Mechanical Shock</td>
<td>15 g for 11 msec.</td>
<td>IEC 60068-2-27, Ea</td>
</tr>
<tr>
<td>Corrosive Resistance</td>
<td>G3</td>
<td>ANSI/ISA-71.04</td>
</tr>
<tr>
<td>Electrostatic Discharge Immunity</td>
<td>6 kV contact</td>
<td>IEC 61000-4-2</td>
</tr>
<tr>
<td>Electrostatic Discharge Immunity</td>
<td>8 kV air</td>
<td>IEC 61000-4-2</td>
</tr>
<tr>
<td>Radiated E-Field Immunity</td>
<td>80 MHz to 1000 MHz</td>
<td>IEC 61000-4-3</td>
</tr>
<tr>
<td>Radiated E-Field Immunity</td>
<td>1.4 GHz to 2 GHz</td>
<td>IEC 61000-4-3</td>
</tr>
<tr>
<td>Radiated E-Field Immunity</td>
<td>2 GHz to 2.7 GHz</td>
<td>IEC 61000-4-3</td>
</tr>
<tr>
<td>Magnetic Field</td>
<td>30 A/m</td>
<td>IEC 61000-4-8</td>
</tr>
<tr>
<td>Signal Line Burst Immunity (EFT)</td>
<td>2 kV</td>
<td>IEC 61000-4-4</td>
</tr>
<tr>
<td>Signal Line Surge Immunity (EFT)</td>
<td>2 kV</td>
<td>IEC 61000-4-5</td>
</tr>
<tr>
<td>Signal Line Conducted RF Immunity</td>
<td>150 kHz to 80 MHz</td>
<td>IEC 61000-4-6</td>
</tr>
<tr>
<td>Signal Line Conducted RF Common Mode Immunity</td>
<td>15 Hz to 150 Hz</td>
<td>IEC 61000-4-16</td>
</tr>
<tr>
<td>Signal Line Conducted RF Common Mode Immunity</td>
<td>150 Hz to 1.5 kHz</td>
<td>IEC 61000-4-16</td>
</tr>
<tr>
<td>Signal Line Conducted RF Common Mode Immunity</td>
<td>1.5 kHz to 150 kHz</td>
<td>IEC 61000-4-16</td>
</tr>
<tr>
<td>AC/DC Power Line Burst Immunity</td>
<td>4 kV</td>
<td>IEC 61000-4-4</td>
</tr>
<tr>
<td>AC/DC Power Conducted RF Immunity</td>
<td>150 kHz to 80 MHz</td>
<td>IEC 61000-4-6</td>
</tr>
<tr>
<td>AC Power Line Surge Immunity</td>
<td>2 kV line to line</td>
<td>IEC 61000-4-5</td>
</tr>
<tr>
<td>AC Power Line Surge Immunity</td>
<td>4 kV line to ground</td>
<td>IEC 61000-4-5</td>
</tr>
<tr>
<td>AC Power Conducted Common Mode RF Immunity</td>
<td>15 Hz to 150 Hz</td>
<td>IEC 61000-4-16</td>
</tr>
<tr>
<td>AC Power Conducted Common Mode RF Immunity</td>
<td>150 Hz to 1.5 kHz</td>
<td>IEC 61000-4-16</td>
</tr>
<tr>
<td>AC Power Conducted Common Mode RF Immunity</td>
<td>1.5 kHz to 150 kHz</td>
<td>IEC 61000-4-16</td>
</tr>
<tr>
<td>AC Power Voltage Dip Immunity</td>
<td>0.5 period 30% reduction</td>
<td>IEC 61000-4-11</td>
</tr>
<tr>
<td>DC Power Line Surge Immunity</td>
<td>1 kV line to line</td>
<td>IEC 61000-4-5</td>
</tr>
<tr>
<td>DC Power Line Surge Immunity</td>
<td>2 kV line to ground</td>
<td>IEC 61000-4-5</td>
</tr>
<tr>
<td>DC Power Voltage Dip Immunity</td>
<td>10 msec. 60% reduction</td>
<td>IEC 61000-4-29</td>
</tr>
<tr>
<td>DC Power Voltage Interruption</td>
<td>30 msec. 100% reduction</td>
<td>IEC 61000-4-29</td>
</tr>
<tr>
<td>Functional Earth Burst Immunity</td>
<td>2 kV</td>
<td>IEC 61000-4-4</td>
</tr>
<tr>
<td>Functional Earth Conducted Common Mode RF Immunity</td>
<td>15 Hz to 150 Hz</td>
<td>IEC 61000-4-16</td>
</tr>
<tr>
<td>Functional Earth Conducted Common Mode RF Immunity</td>
<td>150 Hz to 1.5 kHz</td>
<td>IEC 61000-4-16</td>
</tr>
<tr>
<td>Functional Earth Conducted Common Mode RF Immunity</td>
<td>1.5 kHz to 150 kHz</td>
<td>IEC 61000-4-16</td>
</tr>
<tr>
<td>Radiated Emission, E-Field</td>
<td>30MHz to 1000 MHz</td>
<td>EN55011</td>
</tr>
<tr>
<td>Conducted Emission</td>
<td>0.5 MHz to 30 MHz</td>
<td>EN55011</td>
</tr>
</tbody>
</table>
Similarly, the curve labeled “Strength” is formed by integrating the normal distribution for strength from 0 to \( y \), where \( y \) is any point representing strength on the horizontal axis. Therefore, the curve labeled “Strength” represents the probability that the strength is less than the value of the strength variable on the horizontal axis.

The dark area in Figures 3-1, 3-2, and 3-3 represents the probability where stress is greater than strength. This dark area is proportional to the failure rate. The stress-strength concept allows us to visualize this: as the strength is increased by moving the strength curve to the right, as depicted in Figure 3-2, the dark area is reduced and the failure rate is lowered. If the stress curve is moved to the left (Figure 3-3), the dark area is also reduced and the failure rate lowered.

The key concept to remember is that failure rates are lower when strength is increased and/or stress is reduced.

Figure 3-1. Stress versus Strength Probability Plot
Failure Rate

Instantaneous failure rate is a commonly used measurement of reliability that calculates the number of failures per unit time from a quantity of components exposed to failure.

\[ \lambda(t) = \frac{\text{Failures per Unit Time}}{\text{Quantity Exposed}} \]  

Typically, a failure rate is represented by the lowercase Greek letter lambda (\( \lambda \)). A failure rate is presented in units of inverse time. As Figure 3-4 illus-
Introduction

An engineer’s first design priority is successful operation. Great effort is made to ensure all equipment works for the life of the system. That priority makes sense in most systems because the failure mode is not relevant. In SISs, however, the failure mode is very important. It makes a difference if the system experiences a failure that causes a false trip versus a failure that prevents automatic protection.

Actual instrument failures can be classified as *fail-safe, fail-danger, or other failure mode*. This chapter defines these failure modes in the context of an individual instrumentation device. Note that sometimes the application must be understood before these classifications can be made. Also note that the SIF may or may not fail when one device has failed. A redundant architecture may compensate for device failures. Because the redundancy is modeled at the system level, not the device level, all failure mode definitions assume a single-channel architecture (1oo1).

Equipment Failure Modes

Automation devices can fail in different ways. We call these *failure modes*. In the next sections, these failure modes are defined using the acronyms SIF and SIS. The reader is reminded that a SIF is an instrumented *function* that
provides protection against a particular hazard. An SIS is an instrumented system that implements one or more SIFs.

**Fail-Safe**

Most practitioners define the term *fail-safe* as follows:

*In a nonredundant configuration (1oo1), a failure that causes a “false or spurious” trip of a SIF unless that trip is prevented by a redundant element in the architecture of the SIS.*

Many formal definitions of fail-safe have been attempted, including defining it as “a failure that causes the system to go to a safe state or increases the probability of going to a safe state.” This definition is not useful at the device level, because it groups together two (or more) failure modes when each may have a substantially different impact on safety and reliability. This book uses the practical definition in italic text (above).

**Fail-Danger**

Many practitioners define the term *fail-danger* as follows:

*In a nonredundant configuration (1oo1), a failure that prevents a SIF from performing its automatic protection function.*

Variations of this definition exist in standards. IEC 61508:2010 [1] provides a definition stating fail-danger is a “failure that

a. prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or

b. decreases the probability that the safety function operates correctly when required.”

The IEC 61508:2010 definition also combines two failure modes that, when separated, have significant impacts on the result. For example, the second part (b) of the preceding definition would include the open circuit failure of a transient suppression diode on the input of a PLC. This failure would decrease protection of the input circuit against electrical transients, and would increase the failure rate of the input circuit. However, the safety function would continue to operate successfully. Another example would be a component used only in an automatic diagnostic circuit. Failure of this component category would reduce diagnostic coverage, although the safety function would continue to operate.
Combining multiple failure modes into a single definition causes confusion and results in unrealistic modeling. This result is recognized by practitioners [2] who focus only on the first part (a) of the IEC 61508 definition. Likewise, this book focuses on the first part of the IEC definition and uses the fail-danger definition in italic text. When significant, the second part of the IEC 61508 definition is modeled separately. One major portion of that definition component is called an *annunciation* failure.

**Annunciation**

At exida, reliability engineers recognized that certain failures within equipment used in a SIF prevent the automatic diagnostics from operating correctly [3]. When reliability models are built, the automatic diagnostic failures can be modeled to show exactly how those failures impact the probability of failure. When these diagnostics stop working, the probability of dangerous failure or false trip increases. While these effects may be insignificant, their extent will remain unknown unless they are modeled.

Thus, an *annunciation failure* is defined as “a failure that prevents automatic diagnostics from detecting or annunciating that a failure has occurred inside the equipment.” Note that the failure may be within the equipment that fails, or inside an external piece of equipment designed for automatic diagnostic purposes.

**No Effect**

Some equipment failures have no effect on the SIF, nor do they cause a false trip or prevent automatic diagnostics from working. While some equipment functionality is impaired, that functionality is not needed for safety purposes. These failures are simply called *no effect* failures. Typically, they are not used in any reliability model intended to obtain probability of a false trip or of a fail-danger.

**Detected/Undetected**

Failure modes can be further classified as *detected* or *undetected*, a distinction defined by whether they are detected by automatic diagnostics. In this book, this classification is made at the instrument level, and the specific diagnostics are automatically performed somewhere in the SIS.
Examples
Consider a two-wire pressure transmitter. This device will provide a 4–20 mA electrical current signal in proportion to the pressure input. Detailed failure modes, effects, and diagnostic analysis (FMEDA) of several of these devices reveal a number of failure modes including: frozen output, current to upper limit, current to lower limit, diagnostic failure, communications failure, and drifting/erratic output. When the application is known, these failures can be classified into failure mode categories.

If a single transmitter (no redundancy) were connected to an analog trip amplifier set to trip when the current goes up (high trip), the instrument failure modes could be classified as shown in Table 6-1.

If the same single transmitter (no redundancy) were connected to an analog trip amplifier set to trip when the current goes down (low trip), the instrument failure modes could be classified as shown in Table 6-2. Notice the key difference between these examples: the classification of the output failure to upper and lower limit.

Table 6-1. Transmitter High-Trip Failure Mode Categories

<table>
<thead>
<tr>
<th>Instrument Failure Mode</th>
<th>SIF Failure Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frozen output</td>
<td>Fail-Danger</td>
</tr>
<tr>
<td>Output to upper limit</td>
<td>Fail-Safe</td>
</tr>
<tr>
<td>Output to lower limit</td>
<td>Fail-Danger</td>
</tr>
<tr>
<td>Drifting/erratic output</td>
<td>Fail-Danger</td>
</tr>
<tr>
<td>Diagnostic failure</td>
<td>Annunciation</td>
</tr>
<tr>
<td>Communication failure</td>
<td>No Effect</td>
</tr>
</tbody>
</table>

Table 6-2. Transmitter Low-Trip Failure Mode Categories

<table>
<thead>
<tr>
<th>Instrument Failure Mode</th>
<th>SIF Failure Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frozen output</td>
<td>Fail-Danger</td>
</tr>
<tr>
<td>Output to upper limit</td>
<td>Fail-Danger</td>
</tr>
<tr>
<td>Output to lower limit</td>
<td>Fail-Safe</td>
</tr>
<tr>
<td>Drifting/erratic output</td>
<td>Fail-Danger</td>
</tr>
<tr>
<td>Diagnostic failure</td>
<td>Annunciation</td>
</tr>
<tr>
<td>Communication failure</td>
<td>No Effect</td>
</tr>
</tbody>
</table>
For the high-trip scenario in Table 6-1, the output-to-upper-limit failure is considered fail-safe because the process value signal goes above the trip point. For the low trip scenario in Table 6-2, the same output-to-upper-limit failure is considered fail-danger, because it represents a process value that recedes from the trip point, and thus can no longer accurately indicate the process value. The same logic applies to the output-to-lower-limit failure mode, except that the fail-safe and fail-danger classifications are reversed compared to the output to upper limit failure mode.

Consider possible failure modes of a PLC with digital input and output, both in a de-energize-to-trip (logic 0) design. The PLC failure modes can be categorized relative to the safety function, as Table 6-3 illustrates.

<table>
<thead>
<tr>
<th>Instrument Failure Mode</th>
<th>SIF Failure Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input stuck high</td>
<td>Fail-Danger</td>
</tr>
<tr>
<td>Input stuck low</td>
<td>Fail-Safe</td>
</tr>
<tr>
<td>Input circuit oscillates</td>
<td>Fail-Danger*</td>
</tr>
<tr>
<td>Output stuck high</td>
<td>Fail-Danger</td>
</tr>
<tr>
<td>Output stuck low</td>
<td>Fail-Safe</td>
</tr>
<tr>
<td>Improper CPU execution</td>
<td>50% Fail-Safe</td>
</tr>
<tr>
<td></td>
<td>50% Fail-Danger</td>
</tr>
<tr>
<td>Memory transient failure</td>
<td>50% Fail-Safe</td>
</tr>
<tr>
<td>Memory permanent failure</td>
<td>50% Fail-Danger</td>
</tr>
<tr>
<td>Power supply low (out of tolerance)</td>
<td>Fail-Danger*</td>
</tr>
<tr>
<td>Power supply high (out of tolerance)</td>
<td>Fail-Danger*</td>
</tr>
<tr>
<td>Power supply zero</td>
<td>Fail-Safe</td>
</tr>
<tr>
<td>Diagnostic timer failure</td>
<td>Annunciation</td>
</tr>
<tr>
<td>Loss of communication link</td>
<td>No Effect</td>
</tr>
<tr>
<td>Display panel failed</td>
<td>No Effect</td>
</tr>
</tbody>
</table>

* unpredictable - assume worst case

Final element components will also fail, and again the specific failure modes of the components can be classified into relevant failure modes, depending on the application.
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

<table>
<thead>
<tr>
<th>Instrument Failure Mode</th>
<th>SIF Failure Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solenoid plunger stuck</td>
<td>Fail-Danger</td>
</tr>
<tr>
<td>Solenoid coil burnout</td>
<td>Fail-Safe</td>
</tr>
<tr>
<td>Actuator shaft failure</td>
<td>Fail-Danger*</td>
</tr>
<tr>
<td>Actuator seal failure</td>
<td>Fail-Safe</td>
</tr>
<tr>
<td>Actuator spring failure</td>
<td>Fail-Danger</td>
</tr>
<tr>
<td>Actuator structure failure - air</td>
<td>Fail-Safe</td>
</tr>
<tr>
<td>Actuator structure failure - binding</td>
<td>Fail-Danger*</td>
</tr>
<tr>
<td>Valve shaft failure</td>
<td>Fail-Danger*</td>
</tr>
<tr>
<td>Valve external seal failure</td>
<td>No Effect</td>
</tr>
<tr>
<td>Valve internal seal damage</td>
<td>Fail-Danger*</td>
</tr>
<tr>
<td>Valve ball stuck in position</td>
<td>Fail-Danger*</td>
</tr>
</tbody>
</table>

* 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).
Chapter 6 – Equipment Failure Modes

PFD\textsubscript{avg}

PFD average (PFD\textsubscript{avg}) is a term used to describe the average probability of failure on demand. PFD varies as a function of the equipment operating time interval. It will not reach a steady-state value if any periodic inspection, test, and repair is performed. Therefore, the average value of PFD over a period of time can be a useful metric, if it assumed that the potentially dangerous condition (hazard) is independent from equipment failures in the SIF.

The assumption of independence between hazards and SIF failures seems very realistic in applications where dangerous conditions do not occur frequently (i.e., occurrence is no more than once per year). When hazards and equipment failures are independent, it is realized that a hazard may occur at any time. Therefore, international standards have specified that PFD\textsubscript{avg} is an appropriate metric for measuring the effectiveness of a SIF.

PFD\textsubscript{avg} is defined as “the arithmetic mean over a specified time interval.” For situations in which a SIF is periodically inspected and tested, the proof test interval is the correct time period. Therefore:

\[
PFD_{avg}(TI) = \frac{1}{TI} \int_{0}^{TI} (PFD)(t)dt
\]  

(6-1)

This definition is used to obtain numerical results in several of the system modeling techniques. In a discrete-time Markov model using numerical solution techniques, a direct average of the time-dependent numerical values will provide the most accurate answer. When analytical equations for PFD\textsubscript{avg} are obtained using a fault tree, Equation 6-1 can be used to obtain equations for PFD\textsubscript{avg}.

Exercises

6.1 A solenoid valve is energized in normal process operation. It is de-energized when a dangerous condition is detected and vents air from a pneumatic actuator. If the solenoid coil fails short circuit and burns out, the solenoid valve will de-energize. How should this failure mode be classified?

6.2 A valve is designed to close on trip in a SIF. If this valve had a failure where internal seals were damaged and could not completely stop flow, how would this failure be classified?
6.3 A ball valve without an actuator cannot fail in such a way that it causes a false trip. What is the safe failure rate for the ball valve?

6.4 A flame detector used in burner management application falsely sees a flame when there is none. How would that failure mode be classified?

6.5 A gas detector used in a flammable gas shutdown function falsely indicates the presence of flammable gas. How would that failure mode be classified?

6.6 A safety PLC communicates shutdown status to the operator via a communication link. If this link fails to communicate, how would that failure mode be classified?

6.7 A SIF has a remote actuated valve energized and open. The valve must close when a demand is detected. The valve is fitted to a piston-type pneumatic actuator that has an O-ring seal around the piston. This seal degrades with time, becoming sticky. If left in position for a long time period, it will cause the actuator to stick in place. How would this failure mode be classified?

References


Obtaining Failure Rate Data

Introduction

In the early years of the functional safety standards, industry failure databases, as well as books available to the public, provided some approximate failure data information. Even with approximate data, the probabilistic method began to show designers how they could achieve higher levels of safety by eliminating weak links and optimize costs by choosing designs that matched risk. Nonetheless, realistic failure rate and failure mode data for SIF equipment failures are required to achieve the best SIF design optimization.

Reliability engineers have known for decades that realistic data must ultimately come from one source: expert-vetted, quality field-failure data for devices operating in a similar application. Perhaps that is why IEC 61511:2016 [1], Clause 11.9.3 states, “The reliability data used when quantifying the effect of random failures shall be credible, traceable, documented, justified, and shall be based on field feedback from similar devices used in a similar operating environment.” This strong language reinforces what reliability engineers have long understood.

Failure Rate Estimation

Statistical analysis techniques can be used to estimate failure rates from field failure reports. The failure rate estimates can be accurate, but the analyst must have a good understanding of the following: equipment operation; procedures for data collection that provide insight as to the quality of data; the key
environmental variables impacting failure rates; how the equipment is used at the system level (e.g., continuous operation, low-demand service, high-demand cyclic service, and so on); and how the failure data will be used by system designers. The three most common sources of field failure reports are:

- Manufacturer’s field return data
- Industry database consortiums
- Site-specific/company data-collection systems

Each of these sources has its advantages and disadvantages.

**Manufacturer’s Field Return Data**

Manufacturer’s field return data can be used for upper- and lower-bound failure rate calculations. Although this approach results in a wide failure rate range rather than a single failure rate number, the acquired information can still be useful. Because there are several variables that are seldom known by the manufacturer, including the percentage of failed units that are returned and the actual operating hours, this wide range is likely the best that can be accomplished. These variables usually must be based on assumptions. Although shipping records are often used to estimate operating hours, the total operating population must be estimated based on upper- and lower-limit assumptions.

When assumptions are made optimistically, very low failure rates result. Because low failure rates potentially result in dangerous designs, such assumptions are inappropriate for use in SIF design. When the assumptions are sufficiently pessimistic, an assumed upper-bound failure rate can be calculated.
Example 7-1

Problem: In the last 10 years, the manufacturer of a pneumatic spring-return actuator has reported four product returns due to failure. Manufacturer shipping records are shown in Table 7-1. What is the estimated number of operating hours? What is the estimated failure rate?

Table 7-1: Example Shipping Records and Operating Hour Estimates

<table>
<thead>
<tr>
<th>Year</th>
<th>Units Shipped</th>
<th>Operating Hours - No Delay</th>
<th>Operating Hours - 6 month delay</th>
<th>Operating Hours 6 Mo., 10% spares</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12665</td>
<td>120318</td>
<td>113985</td>
<td>102587</td>
</tr>
<tr>
<td>2</td>
<td>18665</td>
<td>158653</td>
<td>149320</td>
<td>134388</td>
</tr>
<tr>
<td>3</td>
<td>26765</td>
<td>200738</td>
<td>187355</td>
<td>168620</td>
</tr>
<tr>
<td>4</td>
<td>32886</td>
<td>213759</td>
<td>197316</td>
<td>177584</td>
</tr>
<tr>
<td>5</td>
<td>44690</td>
<td>245795</td>
<td>223450</td>
<td>201105</td>
</tr>
<tr>
<td>6</td>
<td>54665</td>
<td>147987</td>
<td>131544</td>
<td>118390</td>
</tr>
<tr>
<td>7</td>
<td>65328</td>
<td>156415</td>
<td>134070</td>
<td>120663</td>
</tr>
<tr>
<td>8</td>
<td>68775</td>
<td>136663</td>
<td>109330</td>
<td>98397</td>
</tr>
<tr>
<td>9</td>
<td>69336</td>
<td>97992</td>
<td>65328</td>
<td>58795</td>
</tr>
<tr>
<td>10</td>
<td>71284</td>
<td>34388</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1512706</td>
<td>1311698</td>
<td>1180528</td>
</tr>
</tbody>
</table>

Solution: The shipping records are provided on a yearly basis. Without more detailed information, it is assumed that shipments were uniform throughout the year. The actuator will be operated continuously once installed and commissioned. An assumption must be made for the number of spares shipped and the time interval between the ship date and commission date.

Table 7-1 shows three calculations of field unit operating hours based on different assumptions. If no delay between the shipment date and operation is assumed and no spares were shipped, unit operating hours are estimated to be 1,512,706. If a 6-month delay between shipment and operation is assumed and no spares were shipped, unit operating hours are estimated to be 1,311,698. If the 6-month assumption is combined with another assumption that 10% of the shipments were for spare parts, unit operating hours are 1,180,528.
Example 7-1 continued

For the lower-range failure rate calculation, the optimistic estimate of 1,512,706 unit operating hours and four failures reported is used. If an optimistic estimate that 90% of the actual field failures are returned to the manufacturer is made, the actual number of failures is five. A point estimate of the failure rate is 5 failures/1,512,706 operating hours equals 3.305 \times 10^{-6} failures per hour, or 3,305 FITS. Using a one-sided 90% confidence factor in a chi-square distribution for confidence interval, the lower range number is 5.71 \times 10^{-6} failures per hour, or 5,710 FITS. (Appendix A discusses confidence interval calculation.)

For the upper-range failure rate calculation, the lower estimate of 1,180,528 unit operating hours and four failures reported is used. It is further assumed that only 30% of the actual field failures are returned to the manufacturer. The number of estimated actual field failures for this assumption is 14. The point estimate of the failure rate is 14 failures/1,180,528 operating hours equals 1.186 \times 10^{-5} failures per hour, or 11,860 FITS. Using a one-sided 90% confidence factor in a chi-square distribution for a confidence interval, the upper bound failure rate is 1.656 \times 10^{-5} failures per hour, or 16,560 FITS.

A quite plausible range for the example failure rate, calculated based on confidence intervals, is estimated to be between 5,710 FITS and 16,560 FITS. While this is a large span, the numbers are still useful as a comparison against failure rate predictions.

The example highlights the significance of the *percentage returned* variable. Guidance on estimating this number comes from the cost of the device and the customer support policies of the manufacturer. User surveys have indicated the number is rarely above 90%, and could be as low as 5%.

When estimating the number of operating hours, it is also important to consider warranty periods. A conservative approach would assume that the product is only returned during the warranty period. Therefore, only operational hours from that period are counted.

Some manufacturers have a power-on hours counter built into their devices. When this functionality is available, the actual field operating hours for each device are precisely known, eliminating one variable. For various reasons, this feature is recommended for all electrically-powered equipment for all manufacturers, including improved analysis of field failure data.

Manufacturer field return data can also be quite valuable when the manufacturer identifies root causes of the failures. Root cause analysis information is
SIF Probabilistic Verification

Probabilistic Analysis

Probability of failure has been a performance metric for comparing and evaluating engineering designs since the 1950s. First used in military applications, the entire field of reliability engineering was developed to provide these metrics. The concept of using the probability calculation process as a performance metric for an SIS was proposed in ISA84 committee meetings in the early 1990s, and published in the first functional safety standard, ISA-84.01, in 1996 [1]. Since then, the method has become a commonly-found tool in the safety engineer’s design tool bag.

SIF Identification

The first step in the probability calculation process is to properly identify the specific equipment required for each SIF. All equipment associated with a particular SIF must be classified into primary (equipment needed to provide the required protection against the identified hazard) and auxiliary (equipment that provides other functionality, but is not required to protect against the identified hazard). This classification is important because only primary equipment is required to protect against the hazard, and must be included in the probability of failure analysis. It is a common mistake to assume that all equipment is required. Making this assumption results in probabilistic verification calculations that are quite pessimistic, and which may result in extra, redundant equipment and/or excess cost. The classification of equipment into
primary versus auxiliary can be documented in the cause-and-effect diagram, and should be noted in the SRS. Other design representations are used as well.

Example 9-1

Problem: A SIL 3 SIF is identified in an SRS. If a low liquid level (LT-2025) is detected in a separation unit, the separation unit outlet valve (VI-2003) must be closed to protect downstream equipment from high pressure “blow-by,” which is the identified hazard. To minimize process disruption, the separation unit inlet valve (VI-2002) must also be closed, a pump (MC-1005) turned off to prevent pump damage, and the inlet valve (VI-3001) for another process unit closed. A SIL 3-rated PLC is used as the logic solver. A hand switch (HS-2000) has been added only to meet local regulatory requirements. What equipment is classified as primary versus auxiliary?

Solution: For each piece of equipment related to the SIF, one must ask if that equipment is necessary to protect against the specified hazard. In this SIF, the hand switch (HS-2000) has been added only to meet local regulatory requirements, and is not part of the automatic protection; thus, it is classified as auxiliary. Since pump overload would not impact the blow-by hazard, the pump control (MC-1005) is classified as an auxiliary part of this SIF. The inlet valve (VI-3001) for the other downstream unit does not have to close to protect against this hazard; thus, it too is classified as auxiliary.

A process unit calculation has confirmed that the hazard would be prevented if only the separation unit downstream valve (VI-2003) closes. Although the necessity for the separation unit inlet valve (VI-2002) closure is debatable, a process calculation has shown that closure of the separation unit inlet valve alone is also sufficient to prevent the resulting pressure in the downstream unit from becoming hazardous. One might select only the downstream valve (VI-2003) for the safety function. However, selecting both valves (VI-2002 and VI-2003) in a 1oo2 configuration will likely be needed to meet SIL 3; thus, both valves are included in the SIF. The SIF primary equipment consists of the SIL 3-rated PLC, the LT-2025 level sensor, the VI-2002 inlet valve, and the VI-2003 outlet valve. This equipment is denoted in the cause-and-effect diagram (Figure 9-1) with an “X.” Other equipment is auxiliary, and is denoted in the cause-and-effect diagram with an “A.” This information must be documented in the SRS.
Continuous/High-Demand Mode Probabilistic Verification

Continuous-Demand Mode

In continuous-demand mode, a demand is always present or occurs frequently. Manual proof testing is certainly not useful for improving safety in a single channel (non-redundant) system. Even automatic diagnostics take too much time to execute, and are not fast enough to reduce the probability of dangerous failure in a single-channel system. Thus, failure rates detected by automatic diagnostics (classified as dangerous detected), as well as those not detected by automatic diagnostics (classified as dangerous undetected), are both counted in the PFH calculation. Consequently, the PFH must be calculated based on all dangerous failures. Equation 9-1 is used for non-redundant systems.

\[
PFH = \lambda_{DD} + \lambda_{DU} = \lambda_D
\] (9-1)

High-Demand Mode

In high-demand applications, automatic diagnostics may lower the probability of dangerous failure if the diagnostics are running fast enough compared to the demand rate, and the system is programmed to initiate transition to the safe state upon a diagnosed failure. IEC 61508:2010 defines the term diagnostic

![Figure 9-1. Example Cause-and-Effect Matrix](image-url)
test interval (DTI) as the “interval between online tests to detect faults in a safety-related system that has a specified diagnostic coverage.” Most agree that if the diagnostics are run 100 times or more within the average demand interval—that is, if \( DI \geq 100 \times DTI \)—then full diagnostic credit can be given. In a nonredundant system, if the automatic diagnostics run at a slower rate, partial diagnostic credit (PDC) can be given (see Equation 9-2) [2].

\[
PDC = \lambda (\frac{\lambda_{Diag}}{\lambda_{Demand}}) \left( 1 - \exp\left[-\frac{\lambda_{Demand}}{\lambda_{Diag}}\right] \right) \tag{9-2}
\]

where

\[
\lambda_{Diag} = \text{the automatic diagnostic rate} = \frac{1}{DTI}
\]
\[
\lambda_{Demand} = \text{the demand rate} = \frac{1}{DI}
\]

Note that when the statement is made, \( DI = n \times DTI \), \( \frac{\lambda_{Diag}}{\lambda_{Demand}} = n \).

Figure 9-2 demonstrates how PDC increases as the ratio of automatic diagnostic rate to demand rate increases. Table 9-1 displays a sample of PDC values.

![Figure 9-2. Partial Diagnostic Credit per Ratio of Automatic Diagnostic Rate to Demand Rate](image)
For nonredundant systems, the PFH for high-demand is calculated using Equation 9-3.

\[ \text{PFH} = (1 - PDC) \lambda_{DD} + \lambda_{DU} \]  

For both continuous- and high-demand modes, the calculated PFH value is compared to the continuous/high-demand target frequency of dangerous failures from IEC 61511 to determine the SIL achieved by the design (Table 9-2).

### Table 9-1. PDC Values for Select \( \frac{\lambda_{Diag}}{\lambda_{Demand}} \) Ratios

<table>
<thead>
<tr>
<th>( \frac{\lambda_{Diag}}{\lambda_{Demand}} )</th>
<th>PDC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>78% Credit</td>
</tr>
<tr>
<td>10</td>
<td>95% Credit</td>
</tr>
<tr>
<td>100</td>
<td>99% Credit</td>
</tr>
</tbody>
</table>

### Table 9-2. Continuous/High Demand Mode Dangerous Probability Limits per SIL

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Target Frequency of Dangerous Failures per Hour (Continuous Mode of Operation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 4</td>
<td>&gt;=10^{-9} to &lt;10^{-8}</td>
</tr>
<tr>
<td>SIL 3</td>
<td>&gt;=10^{-8} to &lt;10^{-7}</td>
</tr>
<tr>
<td>SIL 2</td>
<td>&gt;=10^{-7} to &lt;10^{-6}</td>
</tr>
<tr>
<td>SIL 1</td>
<td>&gt;=10^{-6} to &lt;10^{-5}</td>
</tr>
</tbody>
</table>
Example 9-2

**Problem:** A set of nonredundant (HFT = 0) safety equipment is used to implement a SIF with a demand expected every 50 milliseconds. Once a demand occurs, it takes 100 milliseconds for an incident to occur. (Therefore, the process safety time is 100 milliseconds.) The safety manual for each device has been reviewed. The longest diagnostic time interval is 1 second. After a failure is detected, the SIF equipment set requires 20 milliseconds to shut down the process. The following failure rate data are obtained for the equipment set by adding the failure rates of all device categories:

\[ \lambda_{DD} = 8.5 \times 10^{-6} \text{ failures per hour} \]

\[ \lambda_{DU} = 0.5 \times 10^{-6} \text{ failures per hour} \]

Based on PFH requirements, what SIL level is achieved by this design?

**Solution:** All dangerous failures will cause an incident within 150 milliseconds. The failure detection and response time of 520 milliseconds is not fast enough to bring the process to a safe state. Thus, \( \lambda_{DD} \) and \( \lambda_{DU} \) are added together to obtain the total dangerous failure rate, \( \lambda_D \). Because automatic diagnostics are not fast enough to be given credit for reducing PFH, this SIF is classified as *continuous-demand*. Using Equation 9-1, the PFH equals \( \lambda_D \) and is \( 9 \times 10^{-6} \) failures per hour, which meets the requirements for SIL 1 per Table 9-2.

Example 9-3

**Problem:** A set of nonredundant (1oo1, HFT = 0) safety equipment is used to implement a SIF. The DTI is 100 milliseconds. The system is programmed to take the process to a safe state when a diagnostic indicates an internal failure. The response time of the SIF to achieve a safe state is 50 milliseconds. The process safety time is 2 seconds. An average demand interval is 1 minute. The following failure rate data are obtained for the equipment set by adding the failure rates of all component categories:

\[ \lambda_{DD} = 8.5 \times 10^{-6} \text{ failures per hour} \]

\[ \lambda_{DU} = 0.5 \times 10^{-6} \text{ failures per hour} \]

Based on PFH requirements, what SIL level is achieved by this design?

**Solution:** \( DI = 1 \) minute and \( DTI = 100 \) milliseconds. \( DI = 600 \times DTI \). This SIF is operating in high-demand mode and will receive full diagnostic credit. DTI plus the SIF response time equals 150 milliseconds, which is well within the process safety time of 2 seconds.
Consequently, dangerous detected failures are likely to be converted to safe failures. The remaining dangerous failure rate is simply $\lambda_{DU} = 0.5 \cdot 10^{-6}$ failures per hour, and PFH is also $0.5 \cdot 10^{-6}$ failure per hour, which meets the requirements for SIL 2 per Table 9-2.

**Example 9-4**

**Problem:** A set of nonredundant (1oo1, HFT = 0) safety equipment is used to implement a SIF. The DTI is 100 milliseconds. The system is programmed to take the process to a safe state when a diagnostic indicates an internal failure. The SIF response time to achieve a safe state is 50 milliseconds. The process safety time is 500 milliseconds. An average demand interval is 1 second. The following failure rate data are obtained for the equipment set by adding the failure rates of all component categories:

- $\lambda_{DD} = 8.5 \cdot 10^{-6}$ failures per hour
- $\lambda_{DU} = 0.5 \cdot 10^{-6}$ failures per hour

Based on the PFH requirements, what SIL level is achieved by this design?

**Solution:** $DI = 1$ second and $DTI = 100$ milliseconds. $DI = 10 \times DTI$. This SIF is operating in high-demand mode and will receive partial diagnostic credit. DTI plus the SIF response time equals 150 milliseconds, which is within the process safety time of 500 milliseconds. Consequently, a portion of dangerous detected failures are likely to be converted to safe failures. Since the ratio of diagnostic rate to demand rate is 10, Equation 9-2 (and Table 9-1) give a credit for the diagnostics:

$$PDC \approx \left( \frac{\lambda_{Diag}}{\lambda_{Demand}} \right) \left( 1 - \exp \left( -\frac{\lambda_{Demand}}{\lambda_{Diag}} \right) \right)$$

$$= 10 \cdot (1 - \exp [-0.1]) = 0.9516$$

Equation 9-3 is used to calculate the PFH:

$$PFH = (1 - 0.95) \cdot \lambda_{DD} + \lambda_{DU}$$

$$= (0.05 \cdot 8.5 \cdot 10^{-6}) + 0.5 \cdot 10^{-6}$$

$$= 0.925 \cdot 10^{-6}$$

This meets the requirements for SIL 2 per Table 9-2.
Introduction

The sensors in an SIS measure the process variable conditions that indicate a potential hazard. Thus, several design issues are important. The design must:

- Select equipment suitable for the measurement application
- Select equipment with sufficient safety integrity and published realistic failure rate data
- Properly utilize the automatic diagnostic annunciation signal
- Consider and plan for manual proof testing
- Include any necessary redundancy required for safety and availability

Equipment Selection

The first and most important consideration when selecting sensors for safety applications is that they accurately and reliably measure the process variable. Another key consideration is that any process-wetted materials must be compatible with the process chemicals. Usually these are the same process variables used for control. For a safety application, successful operation in a similar process control application is a good indicator of process compatibility.
As described in Chapter 8, as with all equipment used in a SIF, a sensor device must also be justified based on safety integrity. Fortunately, the industry has evolved to the point where many different sensors have been IEC 61508 certified by an accredited certification body. Because the number of manufacturers and technologies is quite large, few engineers now spend time creating a prior use safety integrity justification. The IEC 61508 certification process is a rigorous, accredited third-party measure of safety integrity. These safety-certified devices are a special class of products with advanced automatic diagnostics that can detect many internal failures. A current list of valid IEC 61508-certified devices is maintained at www.sael-online.com.

**Diagnostic Annunciation**

The advantages of advanced automatic diagnostics in a sensor device depend on a failure detection-signal reaching the logic solver. The logic solver must be configured to either vote the sensor failure signal to trip, or annunciate the failure to the plant repair team, so that the failure can be quickly repaired and correct operation restored. Without annunciation and effective repair, the diagnostics are ineffective, and cannot be given credit in a SIF probability analysis.

Many sensors that use a 4–20 milliamp (mA) analog current to signal the process variable also use the current level to signal an internal failure detected by the sensor’s automatic diagnostics. One common set of current values used for this purpose is based on the NAMUR NE-43 recommendation [1], as Figure 10-1 illustrates.

![Figure 10-1. Current Levels Used to Indicate Internal Failure](image)

**Logic Solver Configuration**

It is essential that the logic solver connected to these sensors be programmed to detect a current less than 3.6 mA, or greater than 21 mA. A decision is then made to interpret this signal as a trip indication, or not. In nonredundant 1oo1
and redundant 1oo2 sensor architectures, most engineers elect not to trip, but instead announce a failure alarm to the maintenance team. This is done to avoid a false trip when the sensor fails, and PFD is not impacted significantly if restore times are less than 1 week.

For a 2oo3 redundant sensor architecture, the logic solver may or may not be configured to vote to trip, since the redundancy would avoid a false trip. In both cases, however, a failure alarm is sent to the maintenance team.

Depending on the logic solver, a one- or two-scan delay may also be needed to avoid a false trip as the analog signal transitions from its normal current level to the failure indication current level. Many logic solvers have preconfigured input blocks with all appropriate logic already defined and tested. Figure 10-2 illustrates input channel parameters that can be set in the Emerson DeltaV SIS with Electronic Marshalling safety PLC to enable the NAMUR failure detection. The “over-range” and “under-range” can also be used if values other than NAMUR are needed.

Figure 10-2. Logic Solver Input Parameter Settings from the DeltaV SIS Safety PLC
Source: Copyright Emerson Process Management: reprinted with permission

The configuration screen in Figure 10-3 depicts the approach used in the Moore Industries STA. Here input limits are entered as parameters. When the input current goes outside of limits, a fault relay output from the module is activated.
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.
Introduction

In every SIF, the logic solver provides the intelligence for performing the required application logic, as well as many other functions such as filtering, averaging, comparison, and calculations. Several types of technologies have been used over the years, including relays, pneumatic logic, solid-state logic, smart relays, programmable logic controllers (PLCs), and safety PLCs.

Equipment Selection

The logic solver is a critical piece of equipment in any SIF. As with all devices in a SIF, IEC 61511:2016 defines the requirements for the selection of logic solvers. The fundamental issues include:

- Verification that the device includes all required functionality for the application
- Verification that the device meets or exceeds the required operating environment
- Verification that the device has sufficient safety integrity for the SIL level of the application through IEC 61508 certification or prior use justification

The logic solver segment of the industry has matured to the point where many different logic solver products from many different manufacturers are
certified in accordance with IEC 61508. Given the criticality of the logic solver, virtually every SIF being designed or upgraded uses a device certified per IEC 61508 by an accredited certification body. The website www.sael-online.com maintains a current list of IEC 61508 certified devices.

Cybersecurity

Many logic solvers contain communication ports, and some have direct Ethernet/Modbus connections. Cybersecurity hacking has become a credible threat [1, 2, 3] to controls, alarms, and SIS. Several industry groups have responded to this threat by creating cybersecurity technical reports (ISA-TR84.00.09 [4]) and standards for systems (IEC 62443-3-3 [5]), integrators and maintenance providers (IEC 62443-2-4 [6]), and devices (IEC 62443-4-1 [7] and IEC 62443-4-2 [8]).

The IEC 62443-3-3 standard contains requirements for industrial automation and control systems, many of which are currently are being assessed and certified [9] to this standard. IEC 62443-3-3 covers seven foundational requirements (FR) and requirement enhancements that are mapped into four security levels (SL). The foundation requirement categories are:

- FR1 – identification and authentication control
- FR2 – use control
- FR3 – system integrity
- FR4 – data confidentiality
- FR5 – restricted data flow
- FR6 – timely response to events
- FR7 – resource availability

A Security Program is defined in the IEC 62443-2-4 standard. The standard describes the security services provided by those who perform systems integration. These security services include implementing all security requirements of the device manufacturers and security maintenance, including patch management, equipment changes and upgrades, and change management. There are additional requirements for personnel competency and integrity, as well as many requirements for procedures that implement specific protection at the systems level.
Many experts feel that cybersecurity can be significantly improved when the devices are hardened by design. The IEC 62443-4-1 standard details the device-development process, especially the software process. Many software design and implementation techniques can fortify the software against cyber-attack. These defense mechanisms can be added as modifications are made to the software. Manufacturers who meet the IEC 62443-4-1 standard must implement software process improvements and establish an update procedure to track emerging cyber threats.

The IEC 62443-4-2 standard lists specific requirements for devices, which are derived from the overall system requirements of IEC 62443-3-3 for each SL. These requirements include identification and authentication of all users, including humans and other devices; enforcement of usage privileges; protection against modification (malicious code, system integrity); data confidentiality; data flow limitations; security event response (audit logs, unauthorized communications); and device availability (robustness against denial of service attacks).

Logic solver manufacturers are working to meet and exceed these requirements. Several controllers have been certified per these standards [9]. Table 11-1 lists a few of the available cybersecurity certifications.

<table>
<thead>
<tr>
<th>Classification</th>
<th>Program Name</th>
<th>Source</th>
<th>Based On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Test</td>
<td>Achilles Communication</td>
<td>Wurldtech (GE)</td>
<td>Company Specification</td>
</tr>
<tr>
<td></td>
<td>Certification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eSTTS</td>
<td>exida</td>
<td>Company Specification</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IEC 62443-4-1</td>
<td></td>
</tr>
<tr>
<td>Product Evaluation</td>
<td>EDSA</td>
<td>ISA Security Compliance</td>
<td>ISCI Specification</td>
</tr>
<tr>
<td></td>
<td>Institute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eSDC</td>
<td>exida</td>
<td>IEC 62443-4-1, -4-2</td>
<td></td>
</tr>
<tr>
<td>System Evaluation</td>
<td>SSA</td>
<td>ISA Security Compliance</td>
<td>ISCI Specification</td>
</tr>
<tr>
<td></td>
<td>Institute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eSSC</td>
<td>exida</td>
<td>IEC 62443-2-4, -3-3, -4-1</td>
<td></td>
</tr>
<tr>
<td>Product</td>
<td>Institute</td>
<td>62443-4-1</td>
<td></td>
</tr>
<tr>
<td>eSDP</td>
<td>exida</td>
<td>IEC 62443-4-1</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>Certification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eESSP</td>
<td>exida</td>
<td>IEC 62443-2-4</td>
<td></td>
</tr>
</tbody>
</table>
Introduction

Many devices have been used as final elements in a SIF [1]. These include annunciation devices (such as horns, flashing lights, or sirens) in functions designed for consequence reduction. Some SIF designs require only simple devices like relays, motor contactors, and solenoid valves as the final element. In machine control applications, the final element may be a motor controller, or a device as complex as a clutch-brake assembly for rapidly removing kinetic energy.

In the process industries, the most common final element is a remote actuated valve. This assembly usually consists of a pneumatic/hydraulic control assembly, an actuator, and a valve (Figure 12-1). The control assembly may be relatively simple, such as a 3/2 solenoid, or more complex, such as a smart partial-valve stroke box or a complex electro-pneumatic assembly with solenoids, test switches, pneumatic booster relays, flow regulators, vent protectors, and quick exhaust valves.

De-energize-to-Trip Design

*De-energize-to-trip* (DTT) is a fundamental principle used in safety design that leads most engineers to think immediately of switching off the electricity. However, DTT refers to more than electricity. The de-energized condition in many final element devices is the lack of air or hydraulic pressure. Thus, a DTT design will move the final element devices to the safe state (valve opened...
or closed) on lack of air or hydraulic energy. This is the common approach for pneumatic designs.

In some designs, especially hydraulic designs, it is necessary to supply energy to achieve the safe state. These are energize-to-trip (ETT) designs. In such designs, it is necessary to use accumulators or other energy storage devices to provide the energy needed for a trip.

**Equipment Selection**

Like other devices used in a SIF, the products used in a final element must be justified for safety critical service by a combination of application suitability analysis and safety integrity analysis. There are many manufacturers of final element devices, however, not all of them have had their devices IEC 61508 certified. Fortunately, many manufacturers, especially those with reputations for high-quality design and manufacture, have received IEC 61508 certification for their products. In these cases, safety integrity justification is made much easier.

The application suitability evaluation and justification requires great attention to detail, since many operational problems are caused by the severe operating conditions and the final element’s process-wetted environment. All final element devices must be evaluated, keeping in mind the fact that these devices may remain in one position without movement for a long period of time. Of course, application suitability includes specific process needs for tight shutoff or closure speed.
Application Suitability

Recall from Chapter 8 the key issues for application suitability evaluation and justification. Normally, as applied to final elements, these key issues are:

1. The device must perform all required functions. In the case of a remote actuated valve, the functions might include:
   - Tight shutoff characteristics
   - Maximum response speed

2. The device must be rated for the anticipated operating environment and process chemistry where it will be installed. Thus,
   - Final element devices must withstand the environment, including corrosive atmospheres, high temperatures, and high pressures.
   - Valve construction materials must be checked against the process chemistry. (Note: In certain applications, standards exist that define proper materials [2].)

3. The implementation must be in accordance with the device safety manuals.

Safety Integrity

As with all safety devices, safety integrity evaluation and justification can be accomplished through one of the following:

- Documented prior use analysis and justification
- Third-party IEC 61508 certification

There are perhaps more manufacturers for final element devices than any other device types, and a significant number have obtained IEC 61508 certification for their products. All categories of final element devices are available, and a good selection of those are functional safety-certified devices. Most have systematic capability SC 3 for SIL 3 applications.

Some caution must be taken, however. It has been discovered that some manufacturers use sales channels that have forged certificates [3]. Always check the validity of any certificate by comparing a certificate provided by the manufacturer with the listing on the CB website. If the certificate is not listed or shown, contact the CB for confirmation. One example CB listing site is www.sael-online.com.
Figure 12-16 illustrates a Flowserve Limitorque MXa motor-driven actuator that offers up to 19,000 lb-in torque for the MX-140. Automatic PVST is available within this device, a feature that should be used to improve safety. Some engineers do not enable this feature because they are concerned that PVST will cause a false trip. With the motor-driven actuator, however, the risk of a false trip caused by the PVST is virtually nil.

**Actuator Failure Modes**

When the seals or even a cylinder body leaks in a DTT design, air pressure is lost and a safe failure results. The seals can also bind, causing a dangerous failure. An actuator spring failure is a dangerous failure. Force transfer components can bind, resulting in a dangerous failure as well. As with other devices, the design details and the application affect the failure rates. Table 12-2 and Appendix C provide generic failure rate data.

**Valves**

There are a range of issues to consider with the selection of valves. A valve for SIS service is different from a control valve. The control valve is often selected based on issues, such as cycle life and number of repetitive operations, while an SIS valve may remain motionless for years. In some cases, a control valve
may be protected from certain failure issues seen in the SIS valve because the regular movement of the control valve protects it from failure modes, such as media packing, polymerization, or corrosion binding. The SIS valve is more likely to experience such failure modes because it is stationary for long periods of time.

All valves must meet temperature and pressure requirements. Different valve designs can withstand higher levels of temperature and pressure. Tight shut-off requirements are essential in some applications. All performance must continue to specification during the useful life of the valve. Any performance deterioration must be considered up front and proper design margins used.

Valve seals are available in elastomer, polytetrafluoroethylene (PTFE), metal, or combinations of these materials. PTFE is a synthetic best known under the brand name of Teflon®.

**Globe Valve**

Globe valves have evolved into the most common choice for control applications. However, there are times when a control valve can be used in a SIF. If the control system was not claimed as an independent layer of protection and/or if control system failure is not the initiating event of the hazard being considered, then the control valve can be utilized as part of a SIF. A 3/2 solenoid valve is added to the final element control circuit to interrupt the modulating pressure to a globe valve. When the pressure is vented by the 3/2 solenoid valve, the control valve moves to its de-energized position.

Figure 12-17 illustrates globe valve construction based on the Fisher easy-e ET valve. Inlet flow comes from the left. The plug seal in the middle is raised and lowered by a linear actuator to restrict flow. (In this illustration, the outlet port is on the right.) Different seal materials are available to allow different shutoff characteristics and temperature ratings.

Globe valves can provide tight shutoff performance and can shut quickly. One disadvantage of a globe valve in a SIF application might be the restriction caused by the valve’s flow path. If the valve is already in place, however, that should not be a problem. Some globe valves have been designed specifically for On-Off operation and have less restriction. Many globe valves have been IEC 61508 certified. The devices are available in several sizes with a wide range of performance. Figure 12-18 illustrates a Fisher globe valve with diaphragm actuator.
**Figure 12-17. Globe Valve Construction**
*Source: Copyright Fisher Controls International, Inc.*

**Figure 12-18. Fisher Valve with Actuator**
*Source: Copyright Fisher Controls International, Inc.*
**Wedge Gate Valve**

The gate valve is a linear valve with a closure member (sometimes called an *obturator*) that slides in a parallel direction across the seat face. When this valve is open, there is little resistance to flow, and thus it is primarily used for On-Off isolation applications. The most common version of the gate valve is the *wedge gate valve*, so named because the closure member is wedge-shaped. It is tapered at an angle that matches the seat angle as shown in Figure 12-19. When pushed into the seat, the wedge provides an extra sealing mechanism.

![Figure 12-19. Wedge Gate Valve Construction](source: Copyright Velan, Inc.)

As with other valve types, there are many manufacturers that offer IEC 61508-certificated devices. Figure 12-20 illustrates a Velan Pressure Seal Gate Valve.

**Plug Valve**

A plug valve is a rotary valve with 90° rotation. The closure member, called a *plug*, is cylindrical or conical shaped. This valve allows straight through flow with minimal restriction because the valve port matches the seat port. The seal is achieved by a sleeve shaped to match the plug (Figure 12-21). Figure 12-22 illustrates a Flowserve Durco TSG4 severe service plug valve.
Figure 12-20. Velan Pressure Seal Gate Valve
Source: Copyright Velan, Inc.

Figure 12-21. Durco Plug Valve Cutaway
Source: Copyright Flowserve Corporation
Ball Valve

A ball valve is a version of a plug valve typically having a spherical closure member. There are two designs, each uses a different method to align and support the ball. These designs are called **trunnion mount** and **floating**. Ball valves are available in large sizes and can withstand high temperatures and pressures. Figure 12-23 is a cutaway drawing of a ball valve.

Floating and trunnion ball valves allow a smooth flow transition from connecting pipe through the ball’s bore for isolation or control of slurry, liquids, or gas. A hole in the middle of the ball provides nearly restriction-free flow through the valve. Two seals are present on either side of the ball. Seals are available in metal, plastic (typically PTFE), or elastomer. Breakaway torque requirements vary with the seal type.

Figure 12-24 illustrates a MOGAS C-Series ball valve. MOGAS products are suitable for extreme temperatures up to 1,650°F, and pressures up to 43,000 psig (2,965 barr g).
Figure 12-23. Cutaway Drawing of a Ball Valve  
Source: Copyright MOGAS Industries, Inc.

Figure 12-24. MOGAS C Series Ball Valve  
Source: Copyright MOGAS Industries, Inc.
Butterfly Valve

The butterfly valve was originally developed as a damper in an inexpensive (i.e., less metal) closure valve [4]. It is a rotary device with 90° rotation. The closure member is a disk. Originally the seals were elastomers, which limited the temperature and pressure ratings while allowing tight shutoff. Following these early designs, butterfly valves have been developed with much higher temperature and pressure ratings. PTFE seals and metal seals are now practical. When the valve is open, the disk remains in the path of the flow; thus, there is some restriction.

There are three types of butterfly valves: the resilient butterfly valve, the high-performance butterfly valve, and the triple offset butterfly valve. Figure 12-25 illustrates a schematic of the disk and seal for the three types.

The diagram on the left of Figure 12-25 illustrates a resilient butterfly valve disk. The seal of the resilient butterfly valve must be made from a flexible material. Consequently, friction occurs when the disk is near closure or when opening the valve. This friction was reduced with the double offset valve design (called high performance) depicted in the middle of Figure 12-25. Friction between the disk and the seal occurs much later in the rotation as a cam action occurs. This has allowed less flexible seals like PTFE and, in some designs, metal seals.
The drawing on the right of Figure 12-25 depicts a triple offset butterfly valve disk and seal. In addition to the double offset used in the middle schematic, a conical shape was added to the disk-seal interface. The disk rotates with virtually no friction. A tight seal is obtained when the disk makes contact with the seal. Metal and PTFE seals are common. Because the disk assembly is larger, the triple offset butterfly does have more restriction than the others. Because there is virtually no friction, torque must be maintained on the valve stem to achieve a seal.

Figure 12-26 illustrates a Virgo TriTork triple offset valve.

Valve Failure Modes

When a valve is considered alone as a component, it has virtually no safe failures. Even if the shaft is broken between a valve and its actuator, it is practically impossible for the valve to close on its own and cause a false trip.

A common dangerous-failure mode in a valve is binding (failure to move to a safe position). Binding may occur between the closure member and the seat, or between the stem and the stem bore. The sensitivity of binding between the
actuator failure modes 251
actuators 246
analysis 6, 9
annunciation 97
   failure 97
   undetected 187
application suitability 134
   evaluation 237
architecture constraints 140–142
architectures 383–384
availability 46, 55
b10 cycle testing 111
b10 point 111
ball valve 256
basic process control system (BPCS) 22
bathtub curve 36, 340
binding 259, 270
bins 350
blow-by 204
boundary 300
burner flame detectors 212
butterfly valve 258
bypassing 338

censored data 350
chemical industry 320
clean service 262, 381
close-to-trip 262
complementary 366
conditional probability 371
confidence interval 354
constant failure rate 50
continuous mode 128
continuous-demand 127, 129, 157, 160
current 221
cybersecurity 218
cycle testing 111
dangerous 112, 399
   detected 115, 157
   dangerous undetected 157
   failure rates 379–381
data analysis 343
data verification 223
data-collection systems 108
decommissioning 345
de-energize-to-trip 26, 235
demand 58
design safety requirements specification 127
detected 97, 185
diagnostic annunciation 182
diagnostic test interval 157
diaphragm actuators 247
direct-acting 238
diversity 198

end of life 36, 340
energize-to-trip 236
equipment failure modes 95
equipment selection 132, 181, 236
estimator 354
event data collection 341
expected value 48, 53
fail-danger 95–96, 185
fail-dangerous 113, 242, 244–245
fail-safe 95–96, 113, 185, 242, 244–245
failure mode 95
failure rate 35, 38, 118, 163
data 227, 263, 377
estimation 103
prediction 111
failures per million hours 37
failures per year 37
fault injection 223
fault tree 71, 73, 77, 85
analysis 71
AND gates 74
approximation 76
average probability calculation 78
OR gates 75
final element proof testing 267
FIT 37
fixed programming language 221
flame detectors 210
flow measurement 208
FMEDA 112–114
freedom from unacceptable risk 2
frequency of occurrence 363
function 95
functional safety 2
process auditing 344
globe valve 252
hardware fault tolerance 142
hardware issues 309
hazard 101
high performance 258
high-demand 127
mode 128-129, 157
high-performance butterfly valve 258
histogram 351
IEC 61508 125
2010 96
certification 139
equation 386
IEC 61511
2016 336
imperfect periodic restoration 60
independent 367
infant mortality 36
input circuit 227
input module 227
installation and commissioning (i & c) 332
intersection 365
interval estimation 354
level 204
switches 204
transmitters 204
logic solver 217, 278
configuration 182
low-demand 127, 129-130, 162
probabilistic-verification variables 162
main header high pressure SIF 315
main processor 227
management of change (MOC) policies and procedures 345
manufacturer’s field return data 104
Markov model 84–85
Markov solution techniques 86
mean 353
mean detection time (MDT) 166
mean repair time (MRT) 167
mean time between failures (MTBF) 55
mean time to failure (MTTF) 48
mean time to restore (MTTR) 53, 165
median 353
middle 353
millivolt inputs 221
mission time (MT) 46, 164
modes of operation 127
motor-driven actuators 250
multiple proof test methods 195
mutually exclusive events 366
network modeling 65
network models 66
no effect 97
obturator 254
ohms 221
oil and gas production 311
one out of one 384
open-to-trip 262
operation 6, 12
operation and maintenance requirements 336
optimal life-cycle cost 1
output circuit 227
output module 227
parallel system 69
percentage returned 106
perfect periodic restoration 57
perform the safety function 140
personnel competency 336
PFD_avg 101
pilot-operated 238
piston actuators 248
plug 254
valve 254
pneumatic logic 220
point estimate 354
point estimation 354
poppet valve 238
pressure 199
primary 155–156
probabilistic
  analysis 155
  calculation tools 176
  modeling of an advanced safety PLC 230
  modeling of the plc 226
probabilities 86, 356, 363
probability
  density function 351
  multiplication 367
  of dangerous failure analysis 149
  of failing safely (PFS) 100
  of failure on demand (PFD) 100
  of failure on demand calculation 174
  of initial failure (PIF) 171
  of success 45
  summation 368
program flow control 223
programmable logic controllers (PLC) 3, 222
proof test
  coverage factor 165
  design 338
  duration (PTD) 170
  interval (TI) 164, 192
  procedures 339
proof testing 337
QEV failure modes 244
quick exhaust valves (QEVs) 243
rack 250
rack-and-pinion actuators 250
random failures 38
random variables 349
redundancy 173
relays 220
reliability 46, 53
  reliability block diagram (RBD) 66, 73
repair procedures 340
resilient butterfly valve 258
resistance temperature detector (RTD) 221
restoration to operation 338
restore time 53
risk reduction 1
risk reduction factor (RRF) 10
route 1h 143
route 2h 147
runaway reaction protection SIF 321
safe 399
safe failure fraction (SFF) 143
safety controllers 224
safety instrumented function 25
safety instrumented systems 21
safety integrity 237
  evaluation 135, 137, 324
  level (SIL) 10
safety PLC 222
  proof testing 230
safety relays 220
safety requirements specification (SRS) 130
safety sensors 212
safety-related system 21
sample space 364
Scotch yoke actuators 248
security program 218
sensor 278
  common-cause defense 197
  proof test strategies 195
  redundant designs 197
series 141
series system 67
severe service 262, 381
SIF 275
  final elements 278
  identification 155
  logic solver 278
  modeling 100
  PFD_avg calculation 283, 286, 289, 293, 297, 300, 305, 308, 320, 325
sensor 278
SIL 1 architectures 280, 289
SIL 2 architectures 289
SIL 3 architecture 301
SIL
  capability 310
  verification 316
  verification process 276
  verification tools 326
SIS
  modeling 90
  safety life cycle 6, 14
  safety life-cycle adoption 15
site safety index (SSI) 172, 329
smart logic modules 221
software criticality analysis 222
solenoid valves 238
specific hazardous event 27
spool valves 238
spool-fails-to-move 270
spurious 185
SSI
  level 0 335
  level 1 334
  level 2 334
  level 3 333
  level 4 331
staggered proof testing 197
standard deviation 353
statistical analysis 350
statistical estimation 354
stay in place 250
steady-state availability 56
strength 31-32
stress 31-32
system 96
  model building 66
systematic 110
  capability 135
  failures 38

temperature 202
theorem of total probability 373
thermocouple 221
tight shutoff 262
time lag 111
time-dependent fault tree solutions 82
top event 72
toxic gas 210
training 336
trip amplifiers 220
triple offset butterfly valve 258
trunnion mount 256
type A 143
type B 143–144

unavailability 56
undetected 97, 185
union 365
unreliability 47
useful life 36, 341

valve failure modes 259
valves 251
venn diagrams 363
verification reports 176
voltage 221

volume booster valve failure modes 245
volume booster valves 245

wear 37
wear-out 37
  region 36
wedge gate valve 254
wellhead process equipment 314