Chapter 6

Fire Protection System Performance Success Probability

Chapter Contents

6.1	Introduction	6–1
6.2	Response Effectiveness	6–18
6.3	On-Line Availability	6–39
6.4	Operational Reliability Evaluation Logic	6–45
6.5	Operational Reliability Quantification	6–67
6.6	Redundancy and Inadvertent Operation	6–98
6.7	Manual Intervention	6–104
6.8	Performance-Integrity-Based Reliability Levels	6–114
6.9	Discussion	6–119
6.10	References	6–123

Visit us online at
www.fireriskforum.com

FIRE PROTECTION SYSTEM PERFORMANCE SUCCESS PROBABILITY

6

6.1 INTRODUCTION

Quantifying fire protection system (FPS) performance is Step 6 in the risk-informed, performance-based fire protection process. FPS performance represents one of the dominant factors in the reduction of potential risk levels. This chapter introduces methods to quantify the conditional probability of FPS performance success following a defined initiating event scenario and functional performance requirements.

As presented in Fig. 6.1, Steps 3, 4, and 5 provide the scenario, initiating event, and exposure profile input for evaluating FPS performance. FPS performance success probability depends on the system's response effectiveness, availability, and operational reliability. Each of these performance measures will be addressed in this chapter.

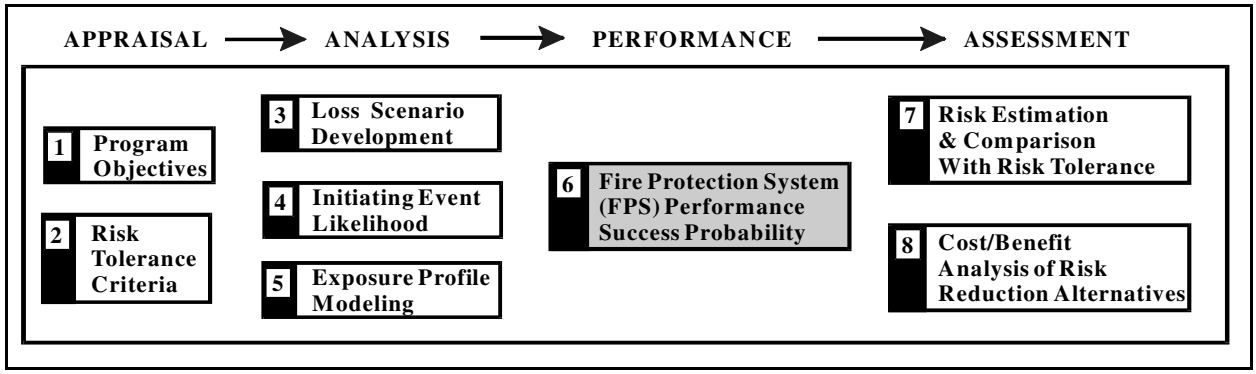


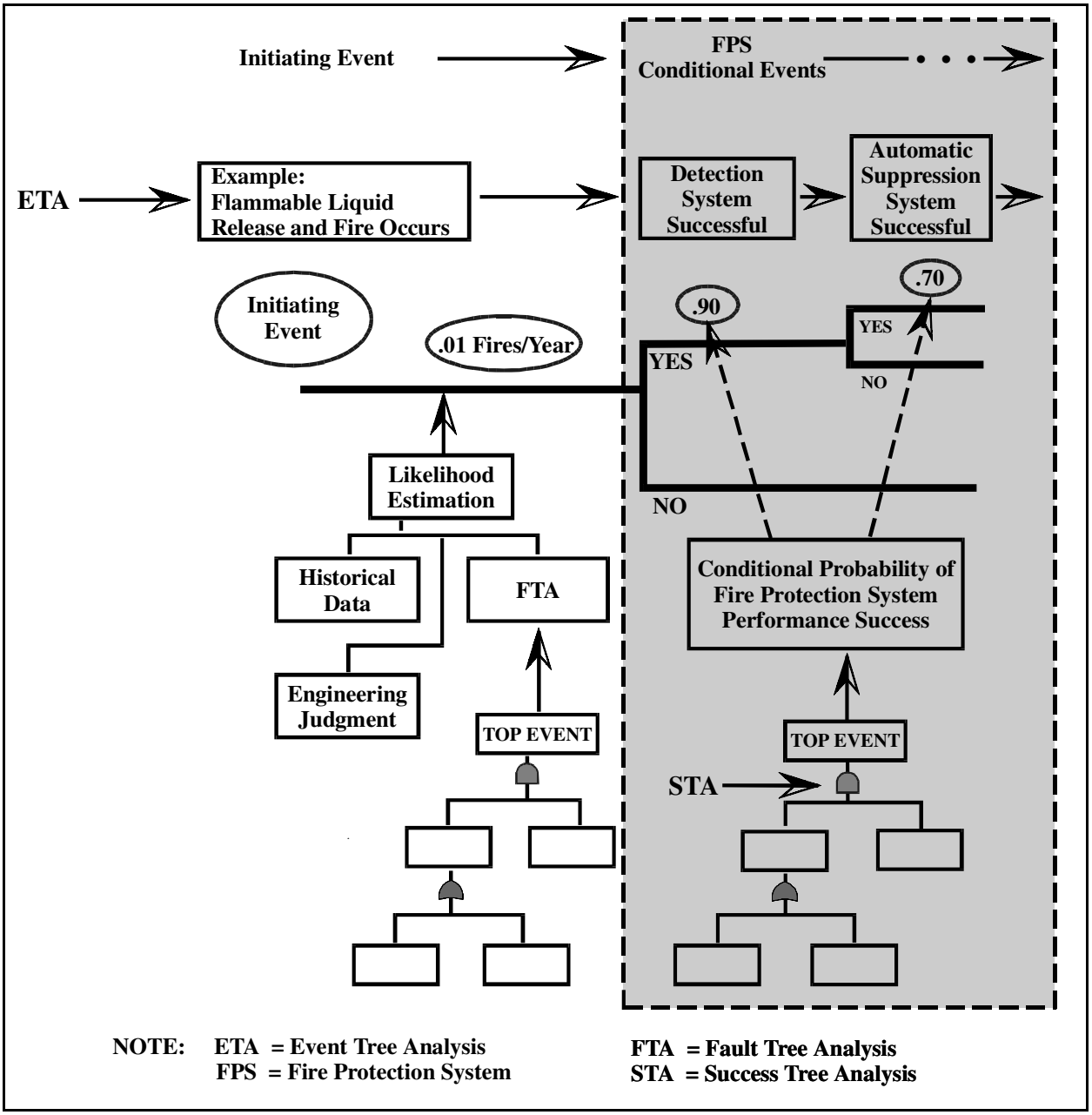
Fig. 6.1: Risk-Informed, Performance-Based Fire Protection Steps

Figure 6.2 presents the general event tree risk modeling framework, highlighting the area covered in this chapter, which is the quantification of conditional FPS events following the occurrence of a prior event. For example, what is the expected performance success probability of a detection system following the release and ignition of a flammable liquid? Or, what is the expected performance success probability of an automatic sprinkler system if the emergency control system does not shut down the release of flammable fuel?

Illustrated in Fig. 6.2 are the following important points:

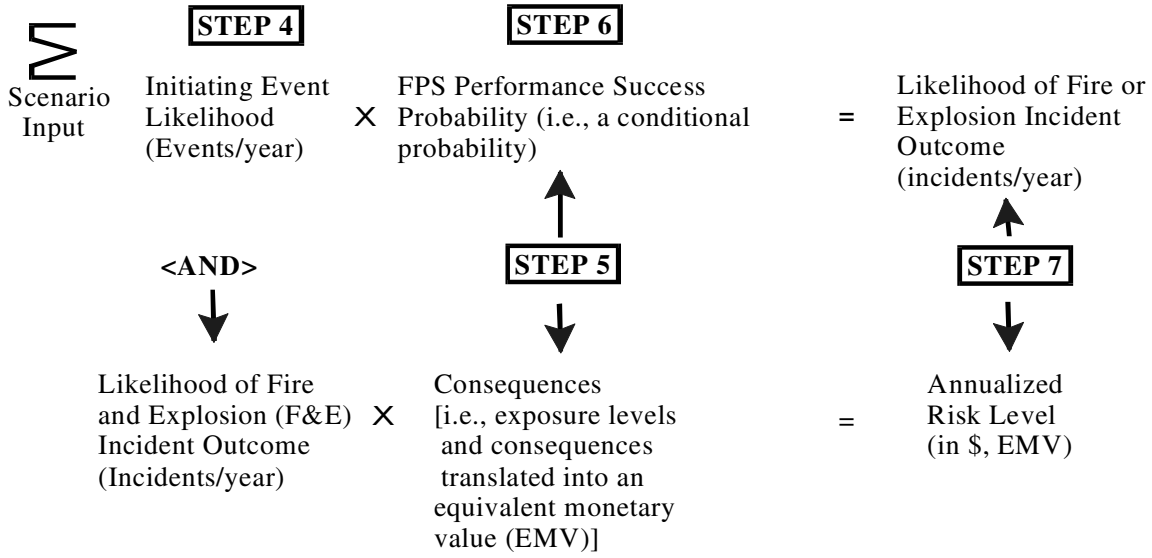
- Event tree analysis (ETA) is the probability modeling method used to incorporate FPS performance success probability in the calculation of fire risk.
- The evaluation requires scenario-specific input. That is, the performance success probability is solely related to the defined scenario inputs and performance requirements.
- Success tree analysis (STA) is the primary modeling logic applied in the determination of the probability of FPS performance success.

Fig. 6.2: General Fire Risk Modeling Framework Highlighting FPS Conditional Events



Risk Estimation Refresher

FPS performance success probability, Step 6, is a key factor in determining potential fire risk levels, as shown in the following equation:



Step 4: Initiating Event Likelihood: Provides the quantification of initiating fire events using a structured analysis approach that includes historical data, fault tree analysis (FTA), and engineering judgement.

Step 5: Exposure Profile Modeling: Provides an exposure profile of the fire or explosion source intensity versus time (at the target), which is a primary input for evaluating FPS performance and consequential outcomes.

Step 6: Fire Protection Performance Success Probability: Based on the input from Steps 4 and 5, the conditional probability (a number between 0 and 1) of the FPS is estimated based on performance measures that include the response effectiveness, availability, and operational reliability.

Step 7: Risk Estimation and Comparison: The annualized risk level is the product of Steps 4, 5, and 6. The annualized risk is usually expressed as an EMV to allow cost/benefit analysis of risk reduction alternatives (Step 8) if the risk tolerance criteria is exceeded.

6.1.1 The Performance Concept

Today there are an increasing number of "equivalent," "alternative," or "performance-based" FPS design options in building and fire codes. These options are in lieu of strict prescriptive codes, which may not be applicable, feasible, or cost-effective.

The risk-informed, performance-based approach allows us to develop and evaluate alternative FPS options to meet our risk reduction goals and risk tolerance limits and to comply with performance-based codes and objectives. Table 6.1 provides a simple example of the basic differences in stating performance goals between prescriptive, performance, and risk-informed performance-based approaches. The first difference among approaches is in establishing performance objectives and criteria, which must begin with a statement, usually expressed qualitatively for prescriptive approaches and quantitatively for performance-based approaches.

Prescriptive codes provide specific requirements that must be applied over a wide range of applications. They are generally straightforward; however, in many building and industrial applications, the feasibility, cost-effectiveness, and actual risk reduction benefit can be questionable. Many codes have incorporated or are in the process of developing performance-based code alternatives.

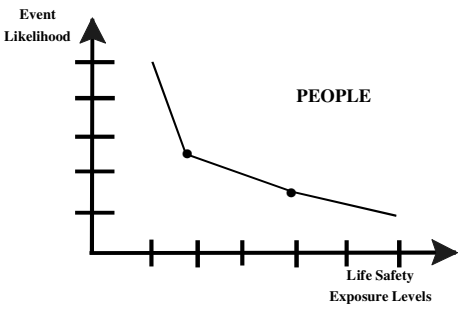
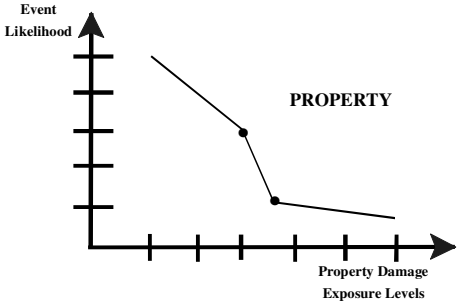
Performance-based codes generally provide:[1]

1. Qualitative fire safety performance goals and objectives (requirements are usually related to fire initiation, means of escape, fire growth and spread, structural stability).
2. Deterministic performance criteria; for example, life safety limits might include:
   Conductive heat: Temperature of the gas layer $\leq 65°C$
   Smoke obscurity: Visibility in the smoke layer should not fall below 2m
   Toxicity: $CO \leq 1400$ ppm
   $HCN \leq 80$ ppm
   $0_2 \geq 12\%$
   $Co_2 \leq 5\%$
   Radiant Heat: ≤ 2.5 kw/m^2 in egress paths
3. Verification methods which may include fire safety engineering design guides and tools such as acceptable computer fire models are usually referenced.

The risk-informed, performance-based approach provides:

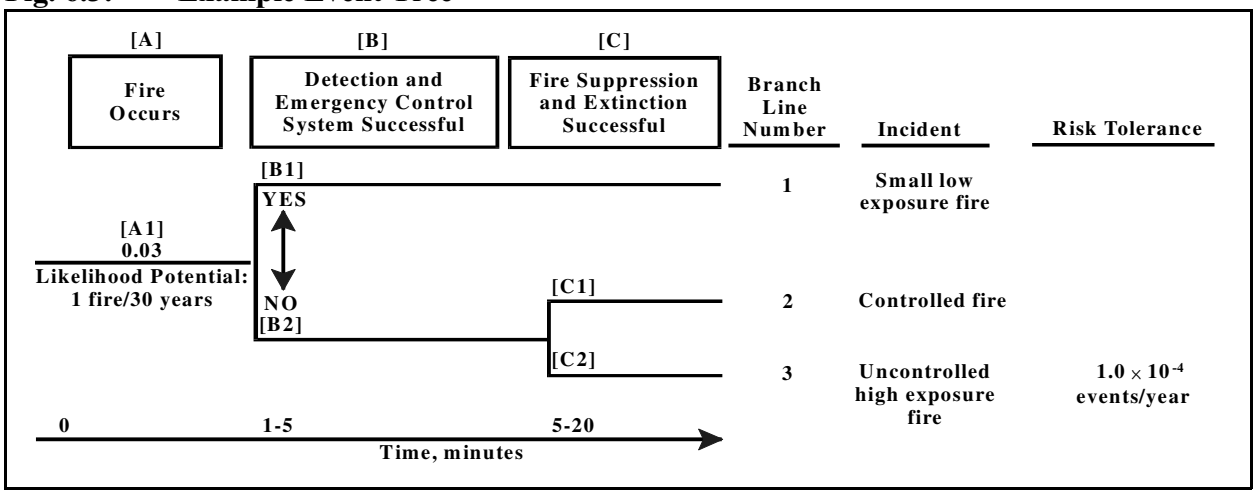
1. Quantitative fire safety performance goals and objectives in terms of a *risk tolerance profile*. The risk tolerance profile is an indication of tolerable fire event likelihoods versus various exposure trends such as life safety, property damage, and business interruption (see Table 6.1).
2. Probabilistic performance criteria in terms of the conditional probability of FPS success given a defined scenario, time-line, target threshold damage limits, and risk tolerance limits.
3. A method to verify the risk and safety levels of existing or proposed fire protection design options in a quantitative fashion.

Table 6.1: Approach For Stating Performance Goals

APPROACH	EXAMPLE PERFORMANCE GOALS	REMARKS
Prescriptive	Provide a 2-hr rated fire barrier wall between occupancy A and occupancy B	• Straightforward, easy to comply with. Verification provided with use of listed or approved design and materials • Is it warranted, feasible, cost-effective? • How much does it actually reduce the risk to people and property?
Performance	Provide an engineered fire safety system to a) prevent fire propagation between occupancy A and occupancy B b) minimize the life safety threat to occupants	• Verification usually involves use of fire safety engineering tools such as computer fire models, heat transfer analysis, etc. • Performance criteria is established in terms of temperature, heat flux, toxic combustion products, and smoke concentration limits for a design-basis fire • Generally does not incorporate event likelihoods, risk levels, or cost/benefit analysis
Risk-Informed, Performance-Based	Provide fire prevention and protection measures to meet the following risk tolerance profiles:  	• Verification involves use and integration of event and fault tree analysis, deterministic fire modeling, traditional fire protection methods, and decision analysis based on cost/benefit • U.S. building and fire codes do not currently incorporate risk profiles to evaluate acceptance of FPS design options. However, future use of risk-informed code equivalences and alternatives are expected.

As a short example of the risk-informed approach, let's assume our risk tolerance for an uncontrolled fire incident resulting in high exposure to people and property is 1.0×10^{-4} uncontrolled fire events/year (shown as branch line 3 in Fig. 6.3).

Fig. 6.3: Example Event Tree



From Fig. 6.3, the event tree calculation for branch line 3 in relationship to the risk tolerance limit is :

$[A1] \times [B2] \times [C2] \leq 1.0 \times 10^{-4}$ uncontrolled fire events/year

[A1] is already established at 0.03 fires/year. Now the question becomes: What is the required performance of [B] – Detection and Emergency Control and [C] – Fire Suppression and Extinction to meet the risk tolerance constraint of 1×10^{-4} uncontrolled fire events/year?

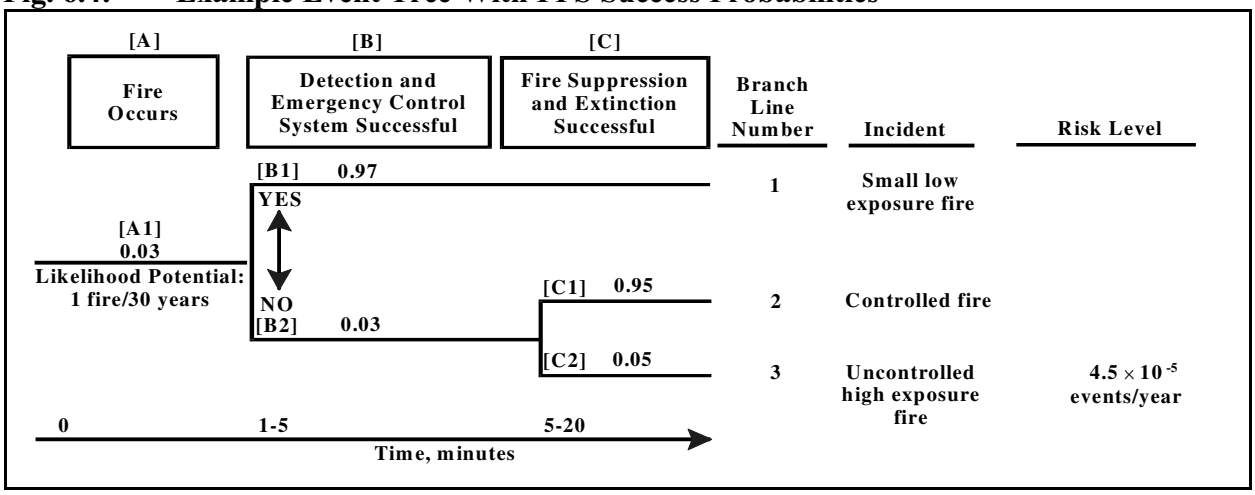
For this example, we will insert the following performance criteria, in terms of conditional probability of success, at: [B1] – 0.97
[C1] – 0.95

Figure 6.4 presents the example event tree with these probabilities added. From calculating through branch line 3, the resulting risk level is 4.5×10^{-5} uncontrolled fire events/year, which is less than the risk tolerance limit of 1.0×10^{-4} events/year.

The performance criteria for this example, based on a defined scenario and risk tolerance limit, can then be stated:

- Provide detection and emergency controls with a minimum performance level of 0.97 conditional probability of success.
- Provide fire suppression and extinction capabilities with a minimum performance level of 0.95 conditional probability of success.

Fig. 6.4: Example Event Tree With FPS Success Probabilities



With the risk-informed, performance-based approach, the fire safety designer can now start evaluating alternative fire detection and fire protection options that can perform at the specified performance levels and that are feasible and cost-effective.

Now the question becomes: How do we quantify the performance capabilities of existing detection and protection systems or the performance expectations of new proposed alternative detection and protection options?

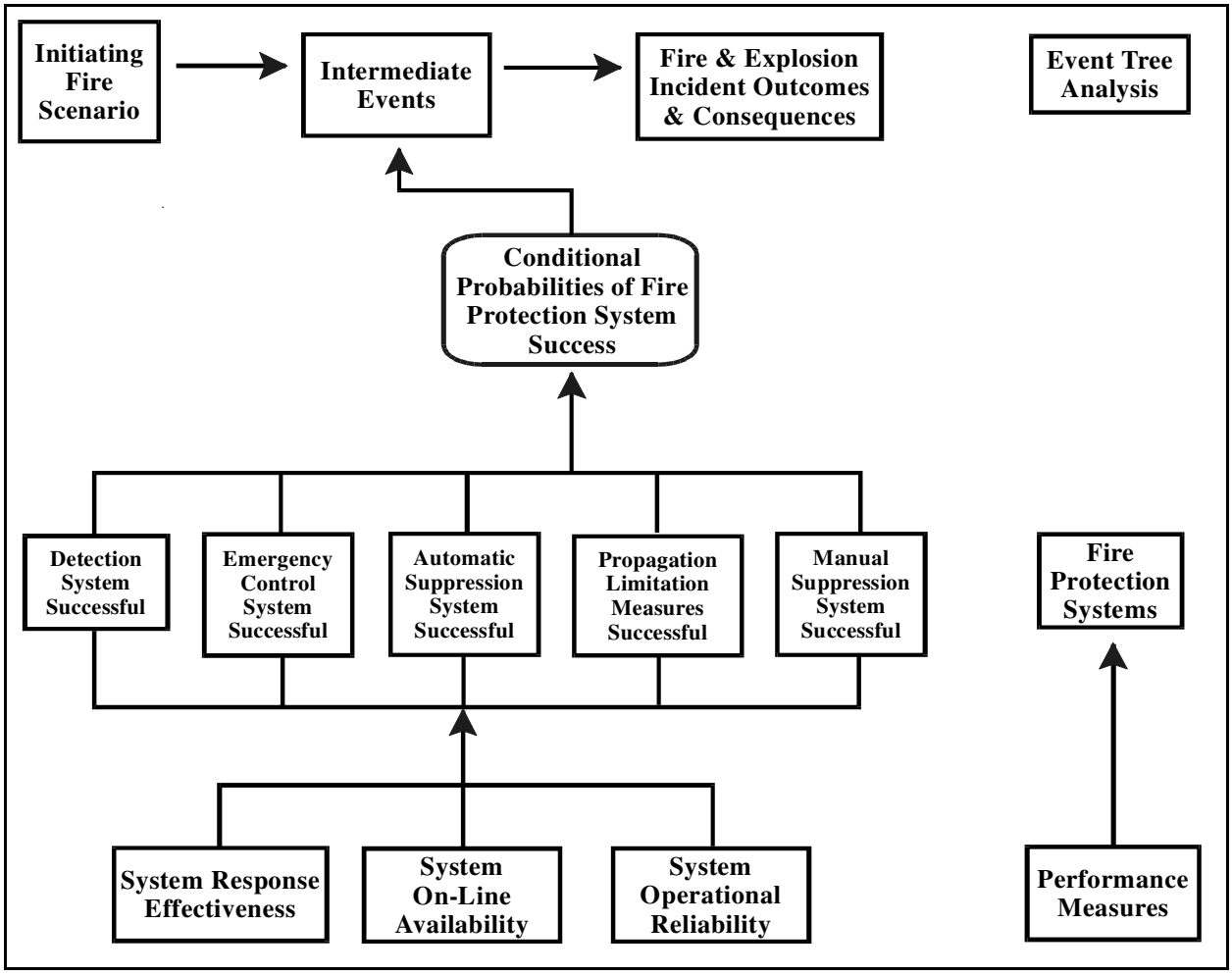
6.1.2 Performance Measures

Figure 6.5 presents a breakdown of some of the primary loss control systems that are being categorized as FPSs. This chapter does not attempt to address all loss control systems that may be encountered in fire risk-based evaluation but rather presents a consistent approach and methodology that can be used in a majority of situations to quantify performance success probability.

FPSs of primary interest in fire risk-based evaluations include:

- Detection systems
- Emergency control systems
- Automatic suppression systems
- Propagation limiting measures (i.e., fire barriers)
- Manual loss control intervention

Fig. 6.5: General Illustration-Fire Protection Systems Performance Input and Measures



A few items to note in Fig. 6.5:

- FPS performance input into ETA fire risk models is in terms of the conditional probability of success based on a defined initiating scenario
- The probability of success is quantified from the following performance measures:
  - System response effectiveness
  - System on-line availability
  - System operational reliability

Each of these performance measures will be described in this chapter.

Success Tree Analysis

Performance success is the probabilistic evaluation of the FPS to successfully perform when a defined fire or explosion demand (i.e., scenario input) is placed upon it. Performance success measures primarily include scenario-based response effectiveness, on-line availability, and operational reliability.

Performance success probability is a "conditional probability," meaning that it is a probabilistic estimate between 0 and 1, based on the occurrence of a preceding event, which is the scenario input and the functional performance requirements expected from the fire protection system.

Performance success tree analysis (STA) logic provides a "template" for the identification and systematic evaluation of primary performance measures that contribute to the quantification of the FPS performance success probability. The "template" provides a first-order decomposition pattern of contributing performance success mechanisms that can be used as a guide for further customization to fit specific scenarios, performance requirements, and FPS designs more accurately.

STA is well suited to model the ability of a FPS to perform successfully when a scenario-specific demand and functional requirements are placed upon it by providing:

- A systematic method to break down performance indicators for evaluation
- A format that provides selection and quantification of probabilities so that performance success can be probabilistically calculated
- A format to apply and integrate the results of deterministic fire models as support and justification for selected probabilities
- A method for evaluating performance improvements by using a computer spreadsheet so that what-if and sensitivity analysis can be conducted

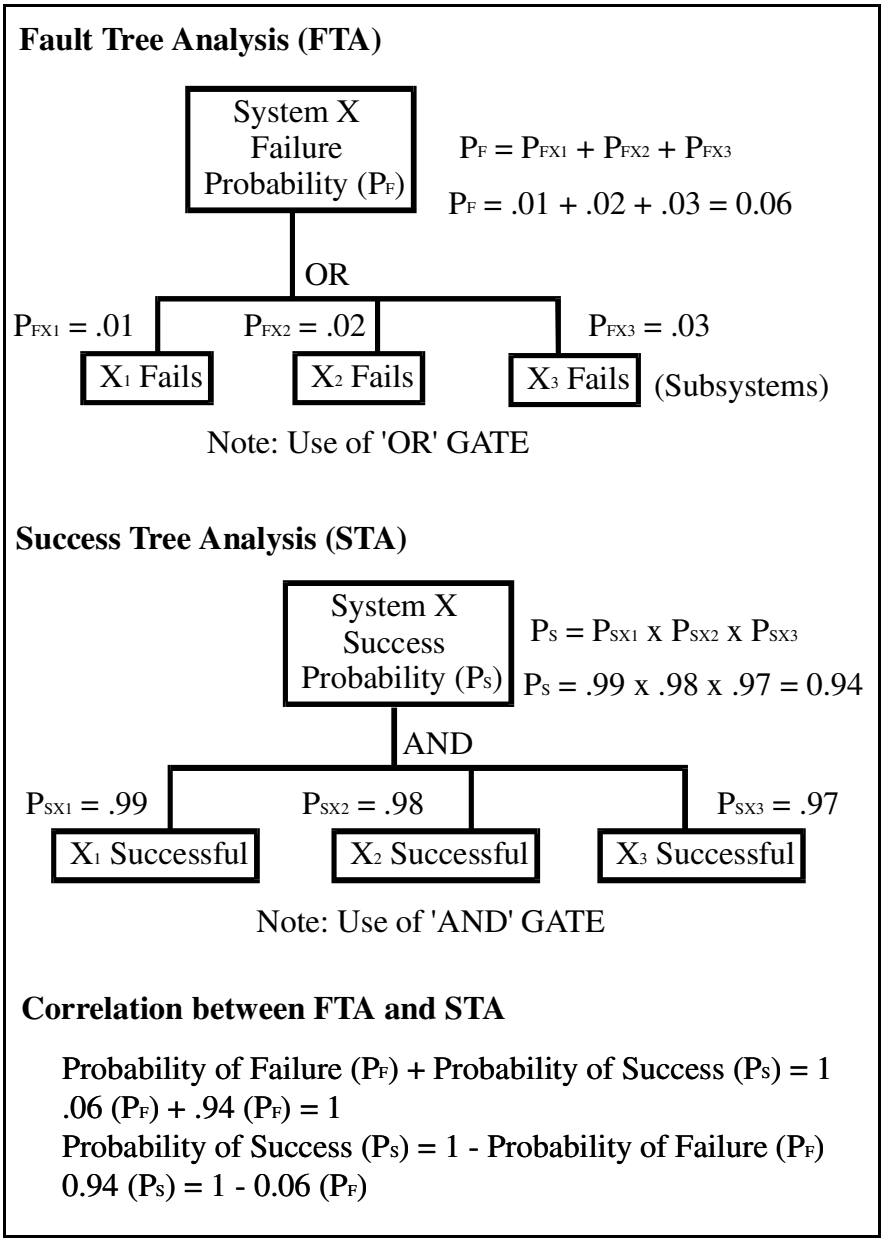
STA methodology is similar to FTA. An example of the relationship is illustrated in Fig. 6.6. In FTA, the top event is "system failure." In STA, the top event is "system success." As shown in Fig. 6.6, the correlation between FTA and STA is:

$$\text{Probability of Success } (P_S) = 1 - \text{Probability of Failure } (P_F)$$

As indicated on the bottom of Fig. 6.6, if the probability of failure (from FTA) is 0.06, then the probability of success (from STA) is 0.94.

For evaluating FPS performance, and from the event tree input standpoint, the success tree orientation is preferable. However, in some cases it is more efficient from a data collection and analysis approach to perform FTA using failure probability data and then to convert to STA orientation.

Fig. 6.6: Example of Fault Tree Analysis vs. Success Tree Analysis



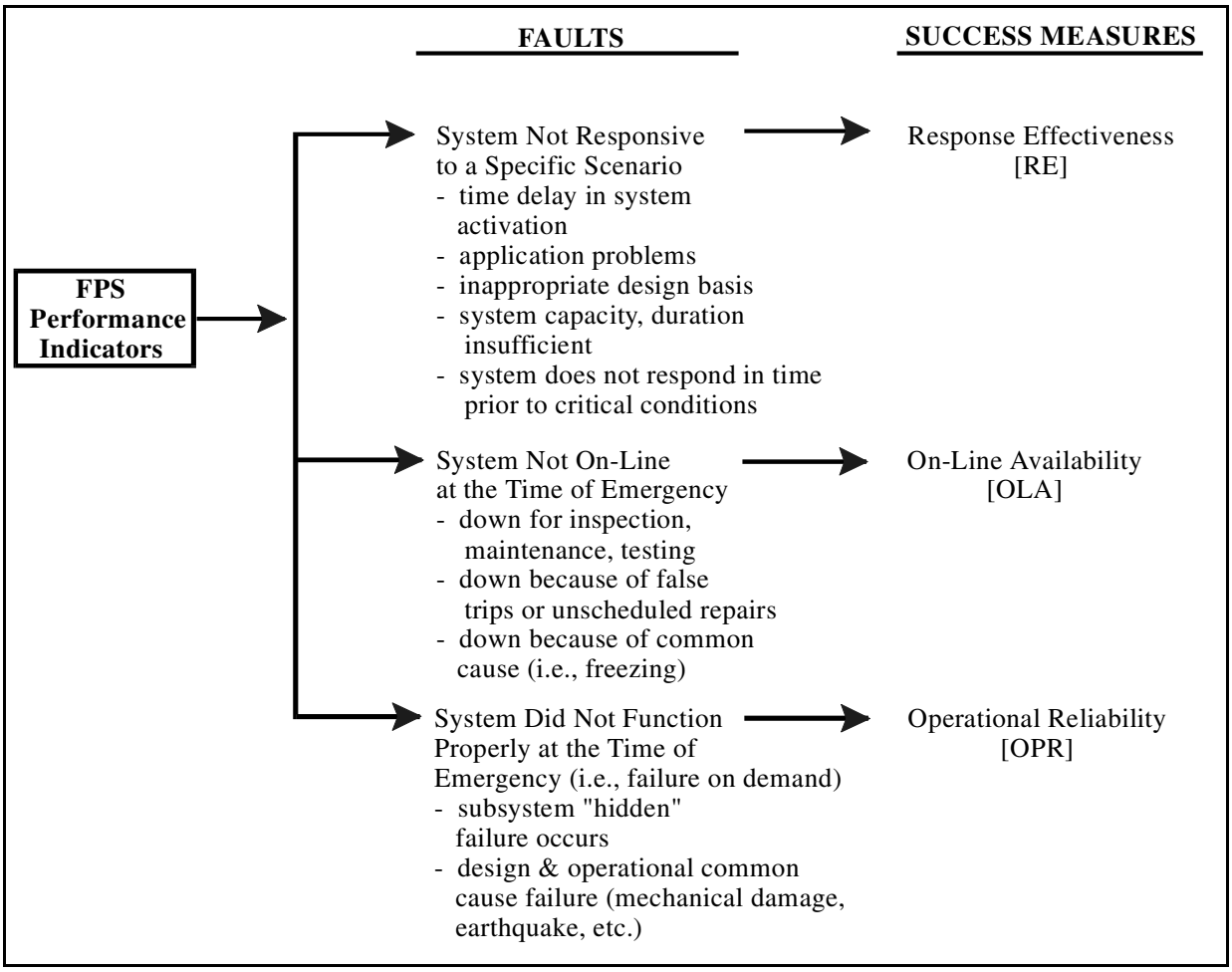
NOTE: An overview of FTA is provided in Chap. 4, Sect. 4.3, Fault Tree Analysis, and is not repeated in this chapter.

Developing performance STA logic involves:

- Identifying primary FPS performance measures
- Developing the success tree structure

For a defined FPS under a scenario-specific demand, performance success pathways can be evaluated in terms of performance measures and indicators developed from past system failure experience. Figure 6.7 provides an example of some primary success measures.

Fig. 6.7: Example of Primary FPS Success Measures

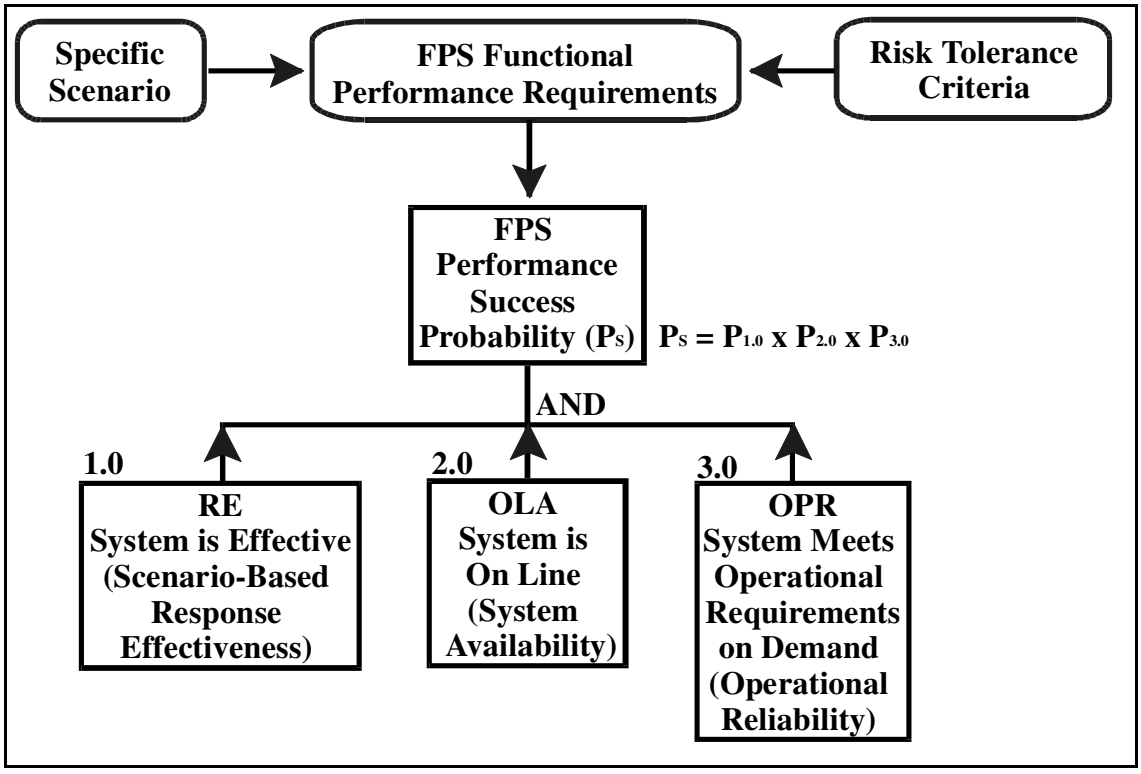


The performance success is the product of these three probabilistic measurement:

Primary Performance Measure	RE Response Effectiveness	OLA On-Line Availability	OPR Operational Reliability
FPS Performance Success Probability (P_S)	$P_S = P_{RE} \times P_{OLA} \times P_{OPR}$		

Figure 6.8 translates this performance equation into STA logic using "AND"gate logic.

Fig. 6.8: FPS Performance Success Tree Logic



As illustrated in Fig. 6.8, FPS performance success probability is based on the FPS functional performance requirements which are established by the:

- Specific scenario input
- Risk tolerance criteria (i.e., target threshold damage or value-exposed limits)

Once the performance requirements are established, quantification of the following performance measures can proceed:

- RE – Response Effectiveness
- OLA – On-Line Availability
- OPR – Operational Reliability

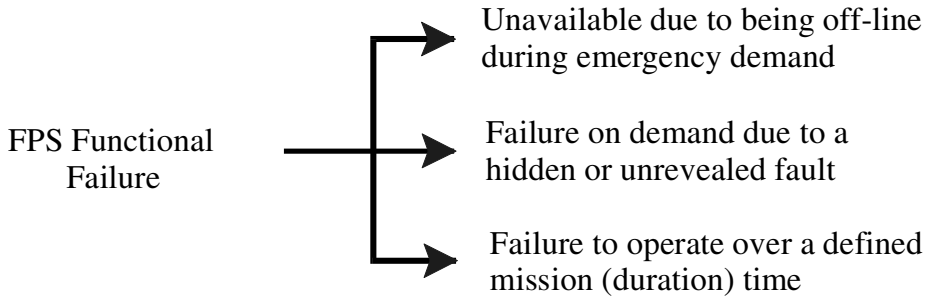
The first thing we want to evaluate is the effectiveness of the system to respond to a specific scenario demand. If the FPS system design application basis is not suitable for the scenario, or the system cannot respond in a time prior to critical conditions (i.e., damage limits exceeded), then the FPS performance success probability is zero.

The reliability aspect of the performance success is broken down into two components: on-line availability and operational reliability. As will be evident later on, dividing reliability into two parameters improves the FPS evaluation efficiency. Reliability can refer to an entire system or to subsystems or components within the system, and is expressed as a probability: Reliability = 1 - Functional Failure. Therefore, if an FPS functional failure probability is estimated at .001 (i.e., it may fail once out of a 1,000 demands), the system reliability is 0.999.

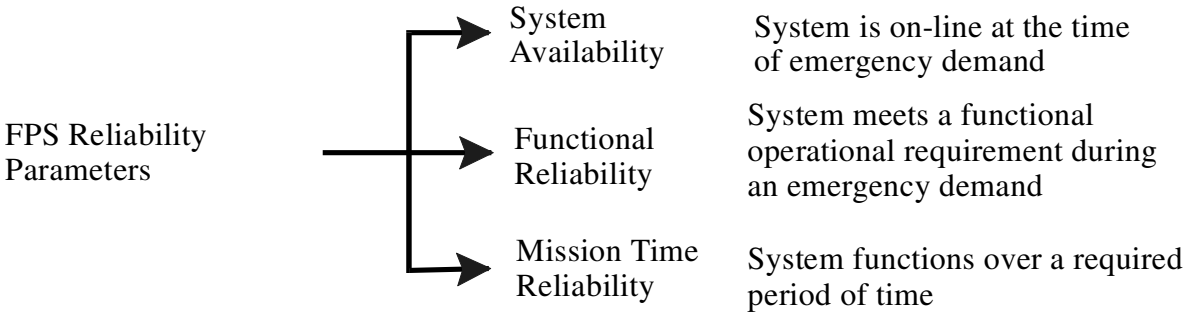
In general, terms for FPS systems:

Functional Failure = System fails to be on-line or operate in a manner based on its original design intent, when an emergency demand is placed upon it.

Functional failure can therefore be broken down into the following failure categories:



Performance success related to reliability parameters then involves:



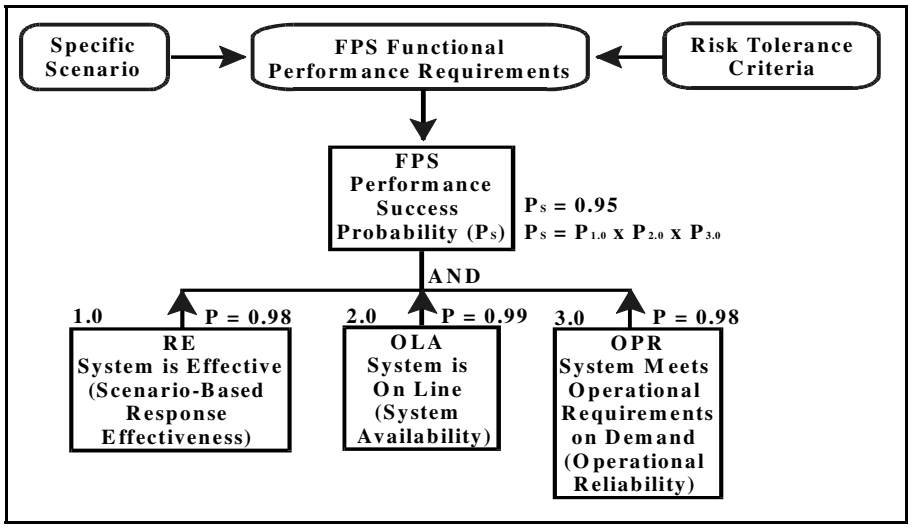
As will be described in the following sections, system availability is handled as a separate evaluation termed on-line availability. The mission time aspect of the reliability evaluation is also handled separately under the response effectiveness duration assessment. This approach allows operational reliability to be evaluated as a separate FPS performance measure, which in turn allows the failure-on-demand aspect of the reliability to be focused on.

At first, some analysts may think a 0.95 probability of FPS success for an existing system or for a performance criteria design goal is too low. However, if the design can meet the following probabilities (P):

$P_{RE} = 0.98$
$P_{OLA} = 0.99$
$P_{OPR} = 0.98$

then the resulting probability of FPS success (P_S) as shown in Fig. 6.9 is $P_S = P_{RE}$ (0.98) × P_{OLA} (0.99) x P_{ORP} (0.98) = 0.95.

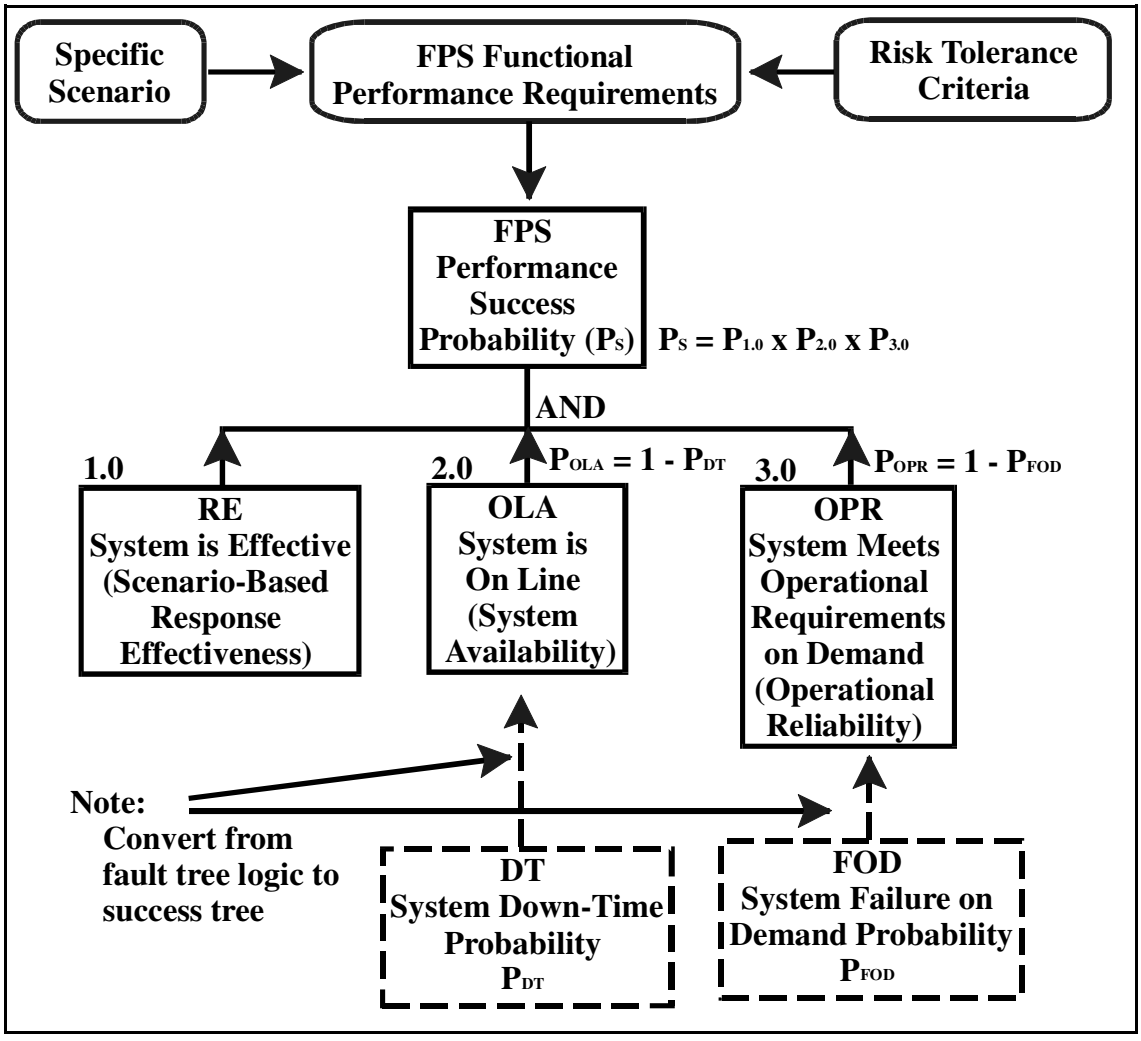
Fig. 6.9: FPS Performance Success Tree Logic



As previously stated, the logic presented in this chapter provides a template or framework that can be customized by the user to fit specific scenarios, performance requirements, and FPS designs more efficiently. The important thing is to identify the factors that significantly contribute to performance success.

The general logic followed in this chapter evaluates RE (Response Effectiveness) as a success tree and evaluates OLA (On-Line Availability) and OPR (Operational Reliability) as fault trees and then converts them to success tree orientation. As shown in Fig. 6.10, the notations used for the conversion are in dashed lines.

Fig. 6.10: The General FPS Performance Logic Tree Framework



6.1.3 Modeling Framework

Because of the importance in providing a credible and consistent method towards quantifying FPS performance success expectations, a systematic process is employed. The general modeling framework used for FPS performance evaluation involves the following:

1. Determine Performance STA Logic
    - Identify Primary FPS Performance Measures
    - Identify and Relate Performance Indicators
2. Quantify Probability of FPS Response Effectiveness (RE)
    - Evaluate Design Application Basis (DAB)
    - Evaluate System Response Time (SRT)
3. Quantify Probability of FPS On-Line Availability (OLA)
    - Evaluate System Being Off-Line Due to Inspection, Maintenance, Testing
    - Evaluate System Being Off-Line Due to Nuisance Trips
    - Assess System Being Off-Line Due to "OTHER" Conditions
4. Quantify Probability of FPS Operational Reliability (OPR)
    - Identify System and Subsystem Boundaries
    - Define Operational Requirements
    - Describe Design and Operation Integrity Factors
    - Estimate Failure-On-Demand Probabilities
5. Quantify Probability of FPS Performance Success
    - Combine Results from FPS Performance Steps 3, 4, 5 Into One FPS Performance Success Probability for Event Tree Input
    - Document Data Sources and Address Uncertainty Issues

The methodology and guidance described in this chapter provide an efficient approach towards the evaluation of FPS performance. These methods meet the intent and objectives of the fire protection community's view of performance-based approaches.

For example, the Society of Fire Protection Engineers (SFPE) has developed the following definition:

> ***Performance-Based Fire Protection Design:*** An engineering approach to fire protection design based on (1) agreed upon fire safety goals and objectives, (2) deterministic and/or probabilistic evaluation of fire scenarios, (3) the physical and chemical properties of fire and fire effluents, and (4) a quantitative assessment of design alternatives against fire safety goals and objectives.

The methodology introduced in this chapter, which centers around STA logic, can be used throughout the life cycle of FPS to evaluate and quantify performance success, given specific scenario conditions and risk tolerance criteria. This approach can be applied to:

- **Evaluation of Existing System**
  This quantifies expected performance success of existing FPS when subjected to specific scenarios and risk tolerance criteria.

- **Evaluation of New System Designs or Modifications**
  This quantifies expected performance success of design options or alternatives to meet scenario-based "Performance Design Targets." For example, if the targeted performance success probability for a specific scenario is .99 (i.e., successful 99 out of 100), then design alternatives are evaluated in terms of response effectiveness, projected on-line availability, and estimated operational reliability to meet this performance target.

  NOTE: Opportunities for improvements to meet performance targets and risk tolerance limits are addressed in Chap. 8, Cost/Benefit Analysis of Risk Reduction Alternatives.

Some Definitions

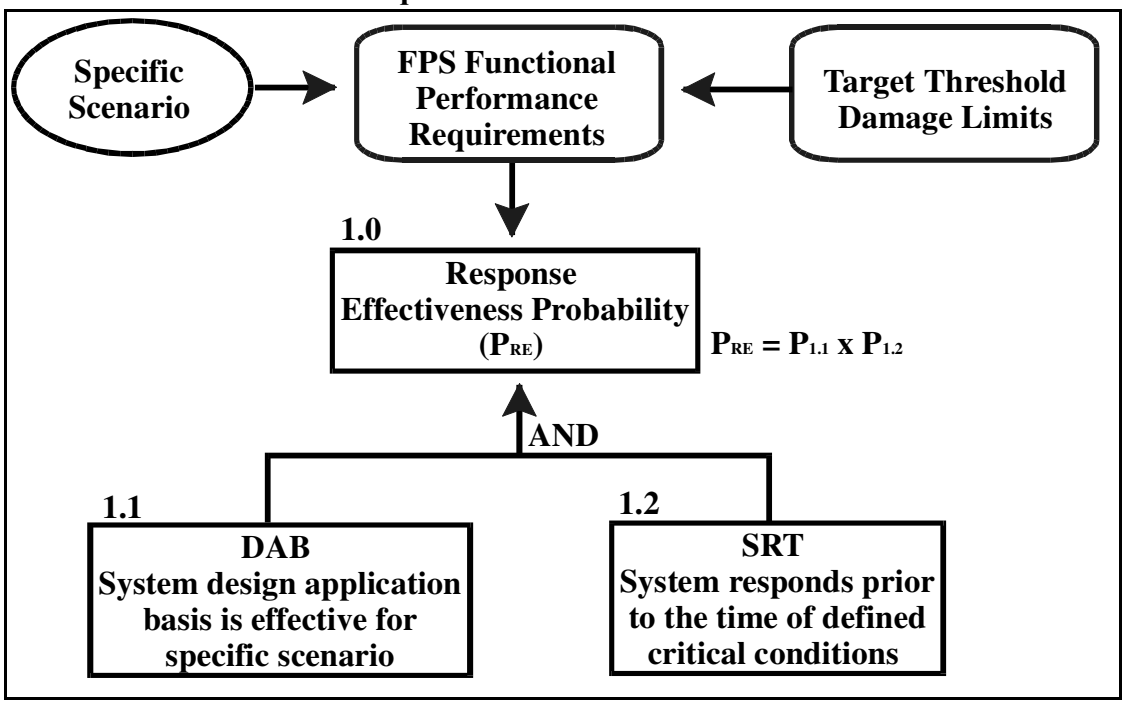
- **Conditional Probability:** Looking forward in evaluating sequential event (i.e., FPS performance success) probabilities (a number between 0 and 1) based on the occurrence of a preceding event.
- **Fire Protection Systems:** Equipment or procedures designed and implemented to prevent or control the propagation of defined fire or explosion scenarios. FPS can include detection systems, emergency control systems, suppression systems, fire barriers, etc.
- **On-Line Availability:** FPS on-line availability is the fraction of time per year the system is on-line and ready to operate at any given time.
- **Operational Reliability:** FPS operational reliability is the ability to operate on-demand and perform defined functional requirements.
- **Performance Success:** The probabilistic evaluation of FPS to successfully perform when a defined fire or explosion demand (i.e., scenario) is placed upon it. Performance success measures primarily include scenario-based response effectiveness, on-line availability, and operational reliability.
- **Response Effectiveness:** FPS response effectiveness is a measure of the scenario-specific design application basis (DAB) and the system response time (i.e., system responds prior to the time of defined critical conditions).
- **Success Tree Analysis (STA):** A method for the logical and systematic development of the performance measurement factors that contribute to the FPS performance success.

6.2 RESPONSE EFFECTIVENESS

FPS response effectiveness probability (P_{RE}) is based on functional performance requirements which, as illustrated in Fig. 6.11, depend on the:

- Target threshold damage limits
- Specific input scenario(s)

Fig. 6.11: FPS Response Effectiveness Probability as Related to Functional Performance Requirements and Success Measures



As illustrated in Fig. 6.11, the Response Effectiveness (RE) evaluation is quantified in terms of the following measures:

- DAB – Design Application Basis
- SRT – System Response Time

6.2.1 Design Application Basis

DAB evaluation involves:

- Identifying DAB success measures
- Probability selection based on functional performance requirements

Figure 6.12 provides a listing of the primary DAB success measures, based on past FPS design faults. These include:

- Suitability
- Capacity
- Duration

Fig. 6.12: Example General DAB Success Measures

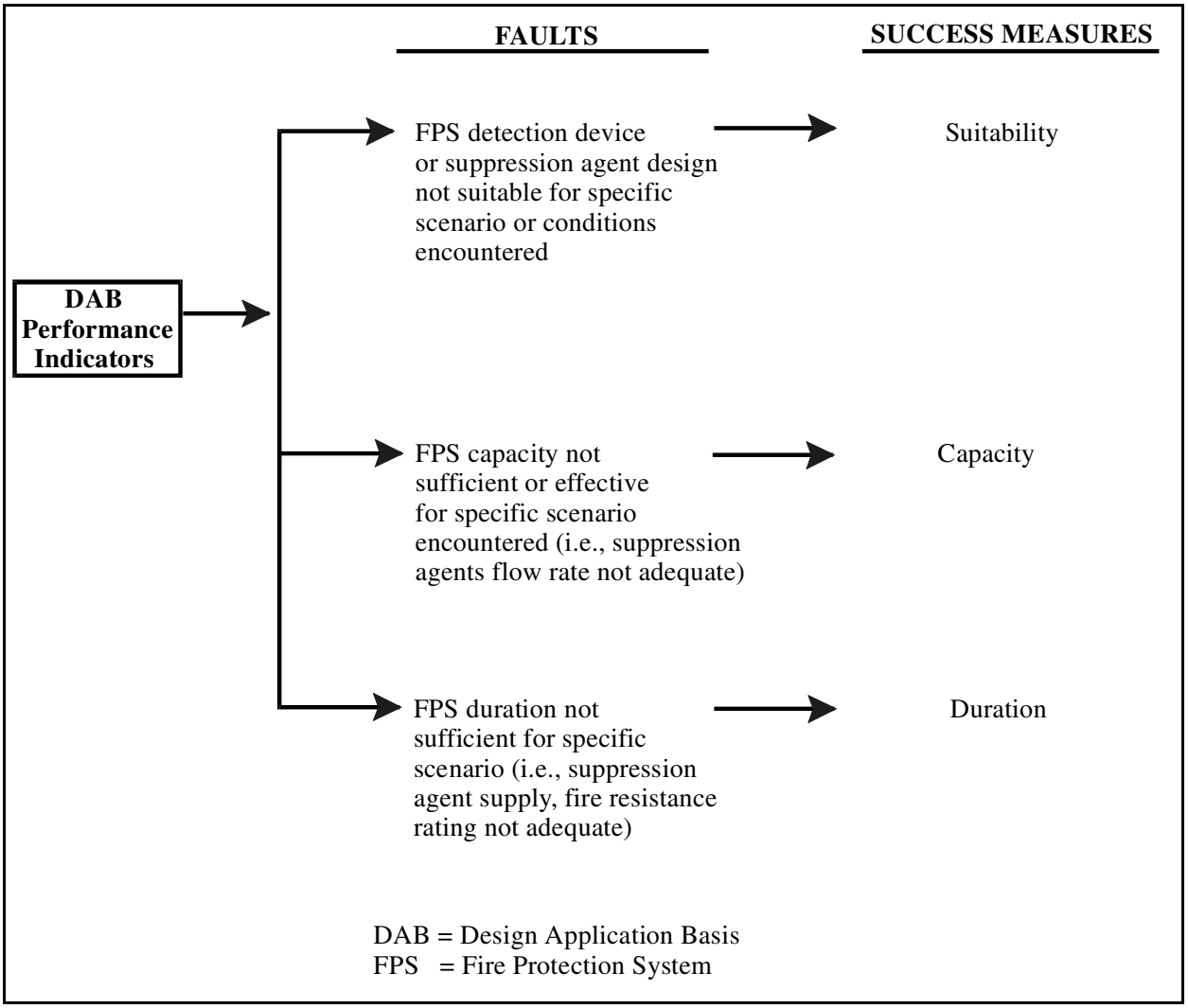
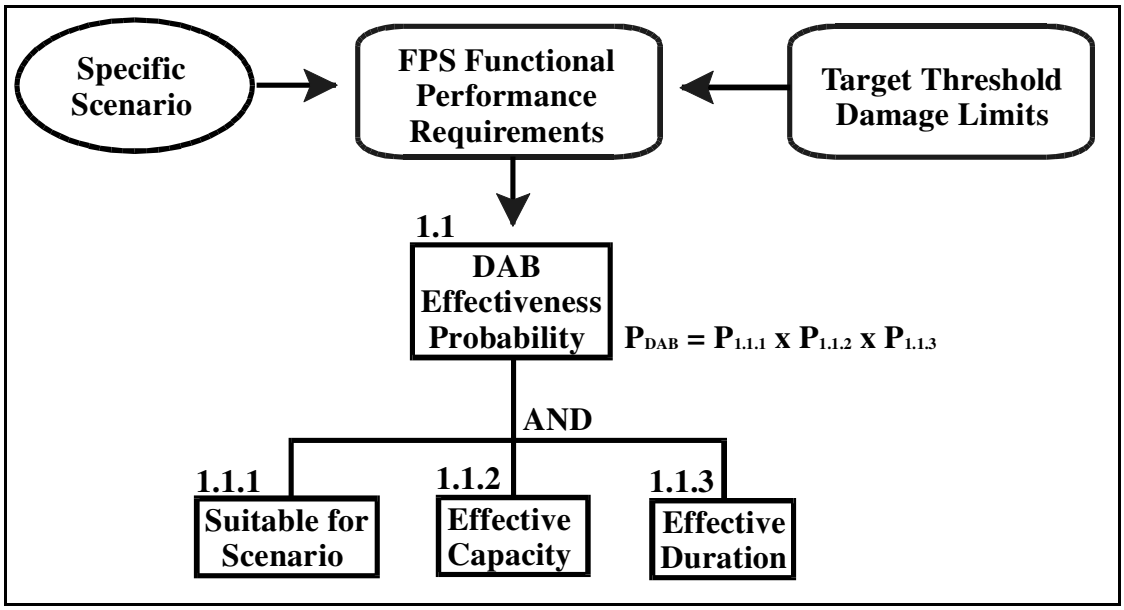


Figure 6.13 illustrates the general DAB success tree framework.

Fig. 6.13: General DAB Success Tree Framework



6.2.2 Suitability

FPS suitability must be evaluated in terms of the functional performance requirements. This evaluation requires knowledge of the specific scenario input and target threshold damage limits. Some suitability considerations include:

- Are the system detection and actuation devices suitable for this particular scenario?
- Do emergency control systems apply the correct intervention strategies?
- Is the suppression mechanism or agent suitable for this particular scenario?
- Will the suppression agent expose personnel or cause equipment damage?
- Are fire proofing or fire materials barriers suitable (i.e., heat, smoke resistance)?

"Suitable" means appropriate to a particular situation or condition. Experience is the primary dictator of suitability and can include the following information sources:

- Standards, industry practices
- Plant, industry specific experience
- Loss incident data
- Research and testing
- Engineering judgement (expert opinion)

It is important that at least one member of the risk assessment team have expertise in FPS capabilities and design, performance, and reliability features. The following references can lend support to DAB suitability issues.

Some Informational Sources

- *NFPA Fire Protection Handbook, 19th Edition*. Arthur E. Cote, Editor-in-Chief. Published by the National Fire Protection Association, Quincy, MA, 2002
- *NFPA Codes, Standards and Recommended Practices*. Published by the National Fire Protection Association, Quincy, MA. Web site: www.nfpa.org
- "FM Global Property Loss Prevention Data Sheets." Factory Mutual Insurance Company, Norwood, MA. Web Site: www.fmglobal.com
- "American Petroleum Institute (API) Guidelines Pertaining to Fire and Safety." Publication catalogue is available from API, Washington D.C.

Some other questions related to suitability include: Is the FPS under evaluation "appropriate" to the particular situation, conditions, scenario input, and functional performance requirements? Is the FPS suitable for the hazard involved, the limitation of damage, the impact on people, the limitation of production equipment down-time, the environmental concerns involved?

Detection Systems

Functional performance objectives of detection systems could include detection of:

- Smoke (aerosols)
- IR and UV radiant energy
- Thermal energy (heat, temperature rise)
- Gases (direct releases of flammable, toxic, or corrosive gases or products of fire combustion gases such as carbon monoxide (CO), hydrogen chloride (HCl), etc.)
- Pressure (pressure rise detectors such as those associated with explosion suppression systems)

With a detection system, in many cases, there is a suitability relationship between the specific scenario and response time. For example, if the specific scenario under risk study involved quick detection (i.e., detection within a certain time constraint) of a smoldering electrical cable fire, a heat detection system may not be a suitable application.

Emergency Control Systems

Functional objectives of emergency control systems (ECSs) could include:

- Emergency system shutdown of production equipment or utilities (i.e., electrical power, gas lines)
- Emergency system startup of safety systems

Emergency system shutdown could include:

- Shutdown of flammable liquid pumps
- Shutdown of production equipment
- Shutdown of ventilation systems
- Shutdown of electrical power

Emergency system operational mechanisms could include:

- Startup of ventilation on smoke removal systems
- Startup of gas depressurization systems
- Startup/activation of suppression systems

Also included under ECSs are emergency inerting systems, pressure relief devices, and passive systems such as flammable liquid diking, draining, and containment.

The suitability question is whether the existing ECS mechanisms or proposed ECS can meet the defined functional performance requirements. In most cases, the focus of ECS evaluation is on the operational reliability. However, ECS systems such as diking, drainage, or containment systems, gas blow-down emergency flare systems, ventilation systems, etc., must first be evaluated from a design application viewpoint.

Fire Suppression Systems

There are numerous types of fire suppression systems, all of which present application versus suitability issues. Table 6.2 lists some primary fire suppression systems.

Table 6.2: Some Primary Fire Protection Suppression Systems:

- Sprinklers
  - Wet System
  - Dry System
  - Pre-action
  - Deluge
- Water Spray Systems
- Foam-Water
  - Wet System
  - Dry System
  - Pre-action
  - Deluge
- Foam System
  - Low Expansion
  - Medium Expansion
  - High Expansion
- Water Mist
  - Low Pressure
  - High Pressure
- Carbon Dioxide
  - Low Pressure
  - High Pressure
  - Total Flooding
  - Local Application
- Clean Agents
  - FC-3-1-10
  - HBFC-2281
  - HCFC-124
  - HFC-125
  - HFC-227ea
  - HFC-23
  - HCFC Blend A
  - IG-541
- Halon
  - 1301
  - 1211
  - 2402
- Chemicals – Dry Chemical
  - Sodium bicarbonate
  - Potassium bicarbonate
  - Potassium chloride
  - Urea/potassium bicarbonate
  - Potassium carbonate
  - Monoammoniun phosphate

Each type of fire suppression system will have application effectiveness and response time constraints when related to performance requirements, which again are predicated upon the specific input scenario and risk tolerance criteria. Primary evaluation factors include:

- Fire suppressant agent control, suppression, extinguishment capability
- Exposure to operators and personnel in area
- Potential for damaging production equipment
- Potential production downtime/clean-up time following system activation
- Chances of inadvertent (false) operation
- Survivability (i.e., explosion overpressure effects, corrosive environments, physical damage)
- Special concerns, such as nuclear criticality versus water-based fire protection at facilities having nuclear materials or the effect of high pressure discharge or damage to sensitive electronic components, etc.

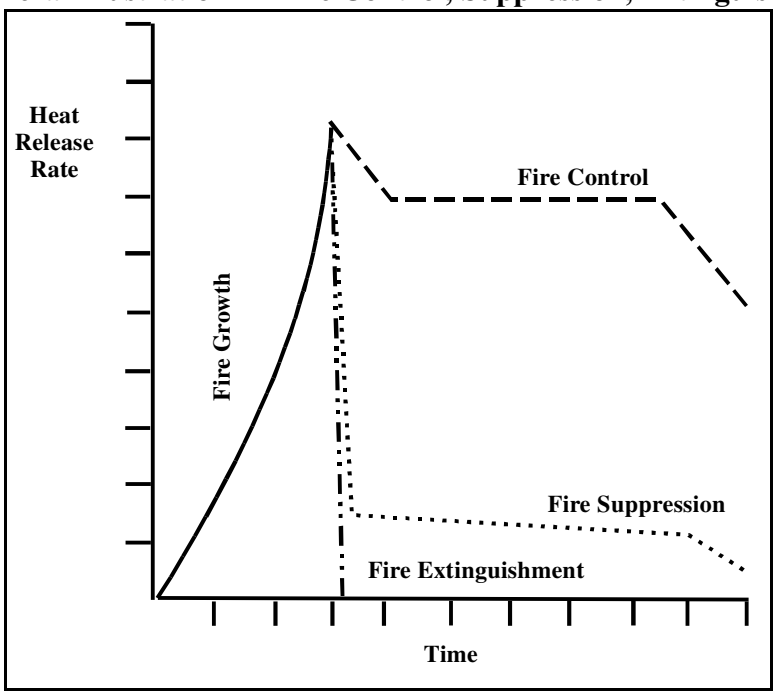
6.2.3 Capacity Effectiveness

Capacity can be generally defined as the maximum production, throughput, or output of an existing FPS or proposed design. Capacity issues are primarily related to suppression systems; however, detection system alarm audibility, ECSs such as drainage systems or gas blow-down systems would also be examined in terms of capacity.

In most cases, the probability associated with design capacity is fairly straightforward, based on engineering review. If, for example, the capacity effectiveness is associated with the flow rate or density of a water-based extinguishing system (i.e., sprinkler, water-spray, pumping system) then based on the functional requirements (i.e., need 0.25 GPM/3000 $ft.^2$ density), one can determine if this is available using water flow hydraulics modeling and analysis.

The most important issue here is to clearly define the functional capacity requirements. When doing a risk-informed evaluation we are interested in how all the FPSs perform in mitigating the initiating scenario in relation to our risk tolerance limit. That means in some cases, we may only need to have control or suppression and not immediate extinguishment. For example, for water-based fire suppression systems, we can achieve various levels of performance depending on the functional requirements, which might include control or suppression of extinguishment.

Fig. 6.14: General Illustration — Fire Control, Suppression, Extinguishment Levels



Some Definitions Related to Water-Based FPSs

Fire Control	–	Limiting the size of a fire by distributing water so as to decrease the heat release rate (HRR) and pre-wet adjacent combustibles while controlling ceiling gas temperatures to avoid structural damage.
Fire Suppression	–	Sharply reducing the HRR of a fire and preventing its regrowth by means of direct and sufficient application of water through the fire plume to the burning fuel surface.
Fire Extinguishment	–	Completely stopping the combustion process.

Assume an initiating event is defined as a flammable liquid release resulting in a pool fire. The flammable liquid has a low flash point (e.g., below expected water temperature of 80°F), a specific gravity <1 (liquid is lighter than water), and is nonmiscible with water (will not mix or be diluted with water). A DAB probability assessment for a sprinkler or water spray system may look like this:

SYSTEM	FUNCTION	REQUIREMENT	DAB PROBABILITY
Automatic Water Spray System 0.25 GPM/3000 ft^2	• Control	Keep ceiling temperature below 500°F for 45 – 60 min	> 0.90
	• Suppression	Reduce fire HRR to less than 50% within 10 min	0.60 – 0.70
	• Extinguishment	Extinguish fire within 15 – 20 min	0

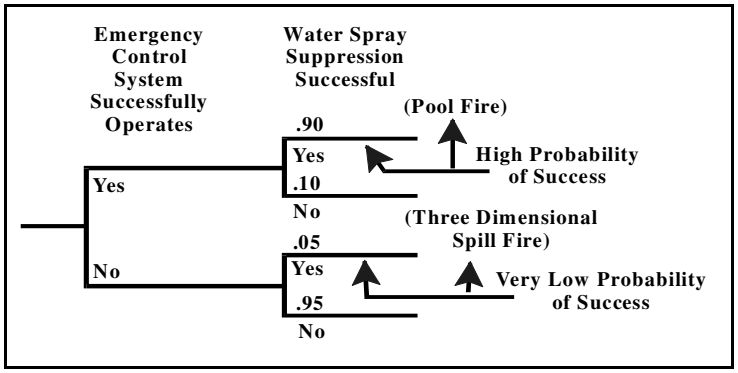
If the functional requirement for our example were extinguishment for this specific scenario, we would probably have to go with an alternative system such as a foam system to meet this requirement. If the scenario involved another fluid such as a 200°F flash point oil, then this same automatic water spray system would have an extinguishment success probability >0.90. Remember, the analysis is scenario-specific. In most cases, the probability of performance success would be based on engineering standards, experience, fire modeling efforts, and available research and test data.

When evaluating suppression agent capacity factors, some other issues might include:

- Potential obstructions to agent coverage
- Actual delivered density of agent (i.e., drop size/velocity concerns)
- Gas extinguishing agent or water mist concentration versus high challenge fires or enclosure tightness
- The preceding emergency control system actions/response/success

A primary factor to evaluate is what happens prior to the operation of the fire suppression system. If we have a flammable liquid release and the release is shut down by our emergency control system, then we have a two-dimensional pool fire. If the emergency control system fails, then we may have a running three-dimensional fire that may not be able to be controlled or suppressed no matter what the water spray density is (see Fig. 6.15). The benefit of doing ETA is that it evaluates the conditional performance success of the fire suppression system based on the preceding events such as detection and emergency control system success.

Fig. 6.15: Partial Event Tree Illustration



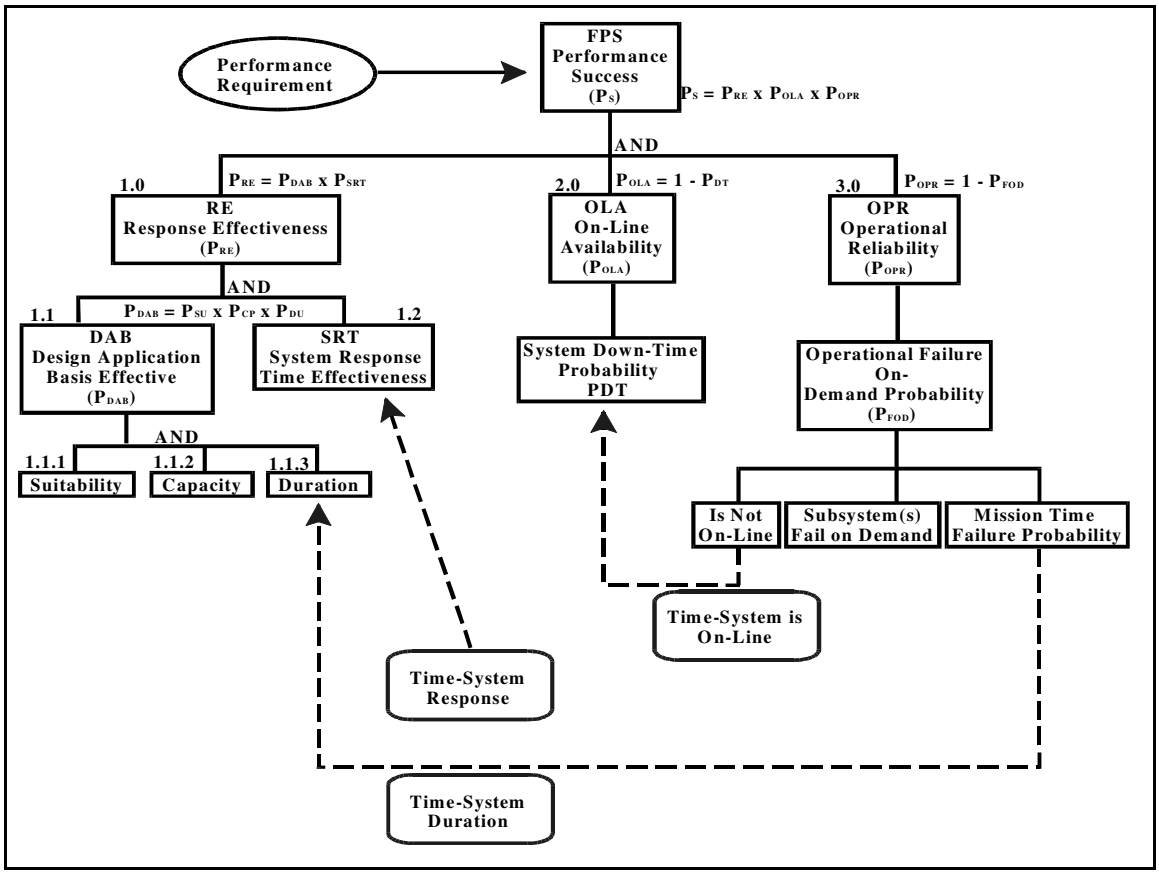
6.2.4 Duration

As a general definition, duration is the period of time that "something" lasts as determined by an existing or proposed design. This could be the adequacy of the suppression agent supply, the fire resistance rating of a fire barrier wall, etc. As with the capacity evaluation, duration effectiveness is evaluated based on functional performance requirements, not codes. In other words, codes could call for a 2-hr water supply or a 2-hr fire wall, while the performance requirement in our scenario-specific risk analysis could be 30 min, or the performance requirements could be greater than the code stipulated requirement.

Strongly related to duration is supply redundancy. However, in the DAB evaluation, we are interested in the total supply available for use versus performance requirements. The probability that multiple or redundant supplies are available at the time of a fire incident would be evaluated in the on-line availability and operational reliability assessment.

As stated in the beginning of this chapter, the duration or "mission time" may be a reliability performance measure involving the system functioning over a specified period of time under scenario-specific conditions. As illustrated in Fig. 6.16, in our methodology, the system mission or duration time aspect of operational reliability is handled under the response effectiveness DAB duration evaluation.

Fig. 6.16: FPS Performance Success Tree Framework — Highlighting Time Factors



The probability of design application effectiveness as related to duration, under scenario-specific conditions, would be based on engineering standards, experience, modeling efforts, or research and test data.

Another element that can be evaluated under the duration aspect of design effectiveness is "Survivability," which is the system's capability to withstand the effects of an incident prior to and during its operation. For example, the discharge nozzles and pipework of a waterspray system may be exposed to an overpressure due to an explosion preceding a fire for which the system is intended. In such cases, the exposed components must withstand the overpressures and the effects of the event itself until the system is fully operational and for the designed duration of system operation. Factors that affect survivability include strength of materials and the speed of actuation.

Typical features considered in survivability performance specification are: [2]

- Resistance to overpressure from explosion scenarios
- Resistance to cold shock from initial contact with spilled vaporizing liquids, such as from liquefied natural gas (LNG)
- Resistance to heat radiation or direct flame impingement prior to actuation of the system

If the initiating fire event was related to an external event scenario such as earthquake, then the FPS design effectiveness (i.e., sprinkler system earthquake bracing) under earthquake conditions would be evaluated as part of the design review.

6.2.5 Probability

Primary probability selection approaches for use in evaluating the Design Application Basis (DAB) segment of the System Response Effectiveness include experience, deterministic models, and engineering judgement.

1. *Experience*
   - Standards, industry practices
   - Plant, industry specific experience
   - Loss incident data
   - Research and testing
2. *Deterministic Modeling*

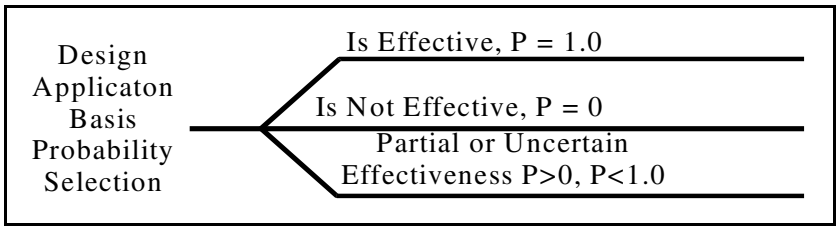
   Models to support DAB probability evaluations can include:
   - Hydraulic models
   - Heat transfer models
3. *Engineering Judgement*

   In the majority of cases based on items 1 and 2 above, we will be able to select the following probability (P) estimation:

   P = 1 DAB is effective

   P = 0 DAB is not effective

Fig. 6.17: Probability Selection



In some cases, there may be much uncertainty due to insufficient knowledge or experience and a large degree of engineering judgement must be applied. Engineering judgement usually involves reviewing what relevant information can be obtained from probability sources 1 and 2 and then applying expert opinion and team consensus. In some situations, further research and testing may be warranted if the potential risk far exceeds the cost of doing the tests.

The DAB analysis is very scenario-specific. Scenario screening and selection is addressed in Chap. 3.

6.2.6 System Response Time

System response time (SRT) evaluation involves:

- Identifying success tree indicators
- Relating scenarios to functional performance requirements
- Probability selection

Figure 6.18 provides an example of general SRT success measures.

Fig. 6.18: Example SRT Success Measures

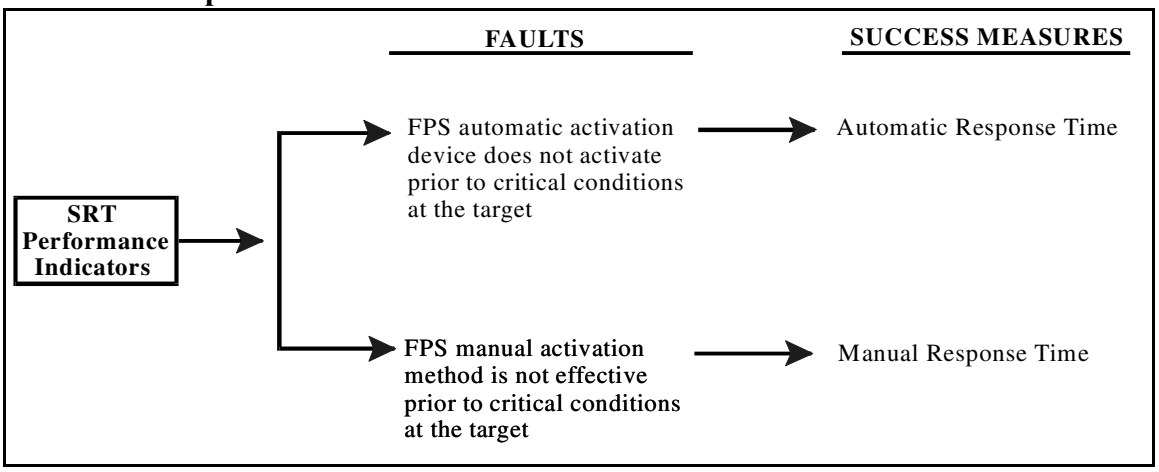
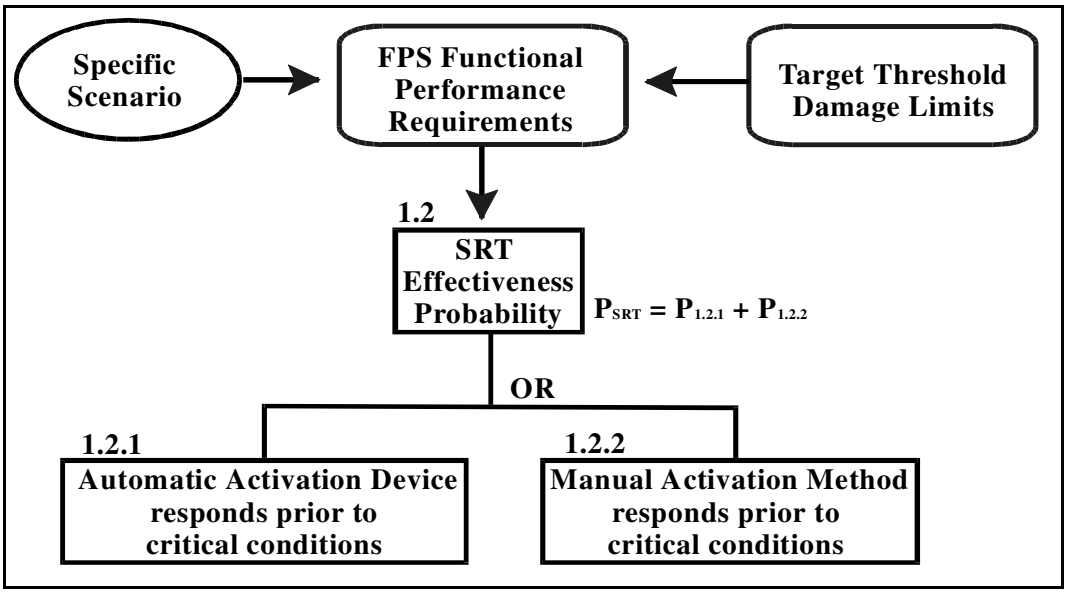


Figure 6.19 presents the SRT effectiveness probability related to functional performance requirements and success measures, which include both automatic and manual activation methods.

Fig. 6.19: System Response Time (SRT) Effectiveness Probability



Quantification of the FPS response time effectiveness is based upon the probability that the FPS responds prior to critical exposure conditions. Critical exposure time limits are established by the time line developed for the event tree fire risk model.

Remember, even though the FPS may meet the suitability, capacity, and duration measures, if the system does not respond (i.e., activate) prior to critical exposure conditions, then overall FPS effectiveness is severely compromised. Therefore, estimating an SRT probability is a very important factor in assessing FPS performance.

Refresher

In Sect. 5.2 of Chap. 5, Exposure Profile Modeling, establishing scenario-based critical target damage limiting conditions and event tree time line parameters were discussed. As a refresher, some tables from Chap. 5 are reproduced in this section as Tables 6.3 and 6.4. Table 6.3 provides an example time-related profile of loss of functional performance (of people, equipment, structures) versus thermal and nonthermal exposure. Table 6.4 is an example of establishing FPS response parameters to minimize the probability of exceeding the functional performance limits in Table 6.3. Note that the FPS systems in this example include a detection system, emergency control system, automatic fire suppression system, fire barrier system, and manual fire fighting equipment.

Figure 6.20 provides an example of a scenario-based exposure profile that graphically represents the data in Tables 6.3 and 6.4 versus potential thermal and nonthermal exposure intensity levels (note: modeling intensity levels are described in Chap. 5). This type of assessment provides the time line upon which to evaluate the probability of successful response time for existing or proposed FPS designs.

Table 6.3: Example Loss of Functional Performance versus Time, for Thermal and Nonthermal Exposures

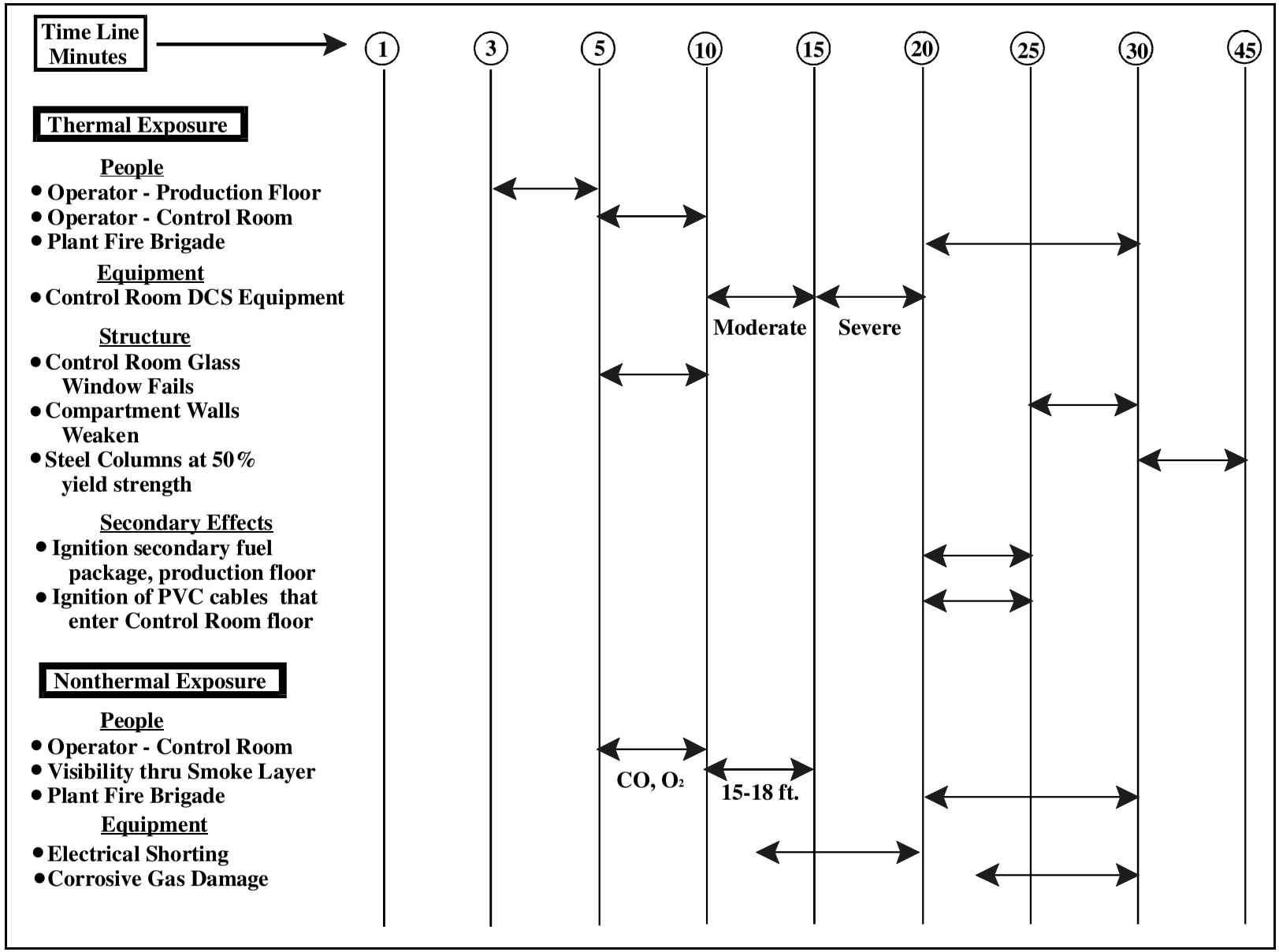


Table 6.4: Example Fire Protection System (FPS) Response Time Parameters

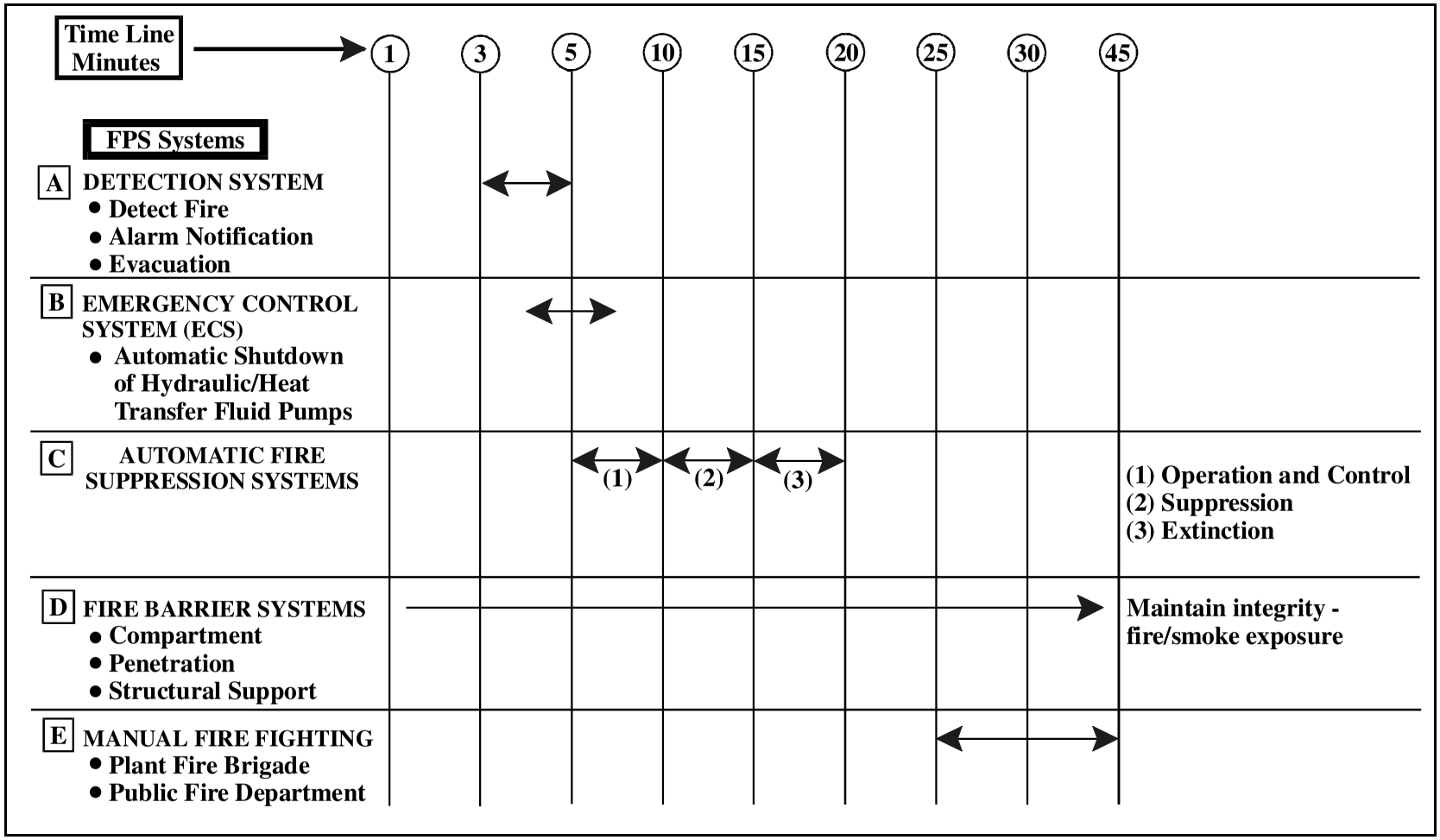
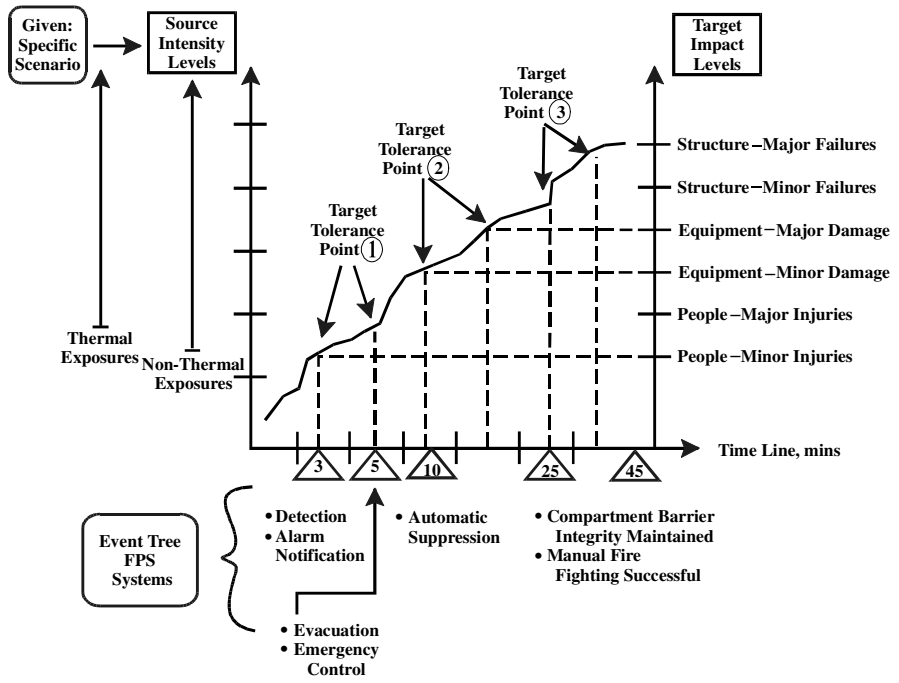


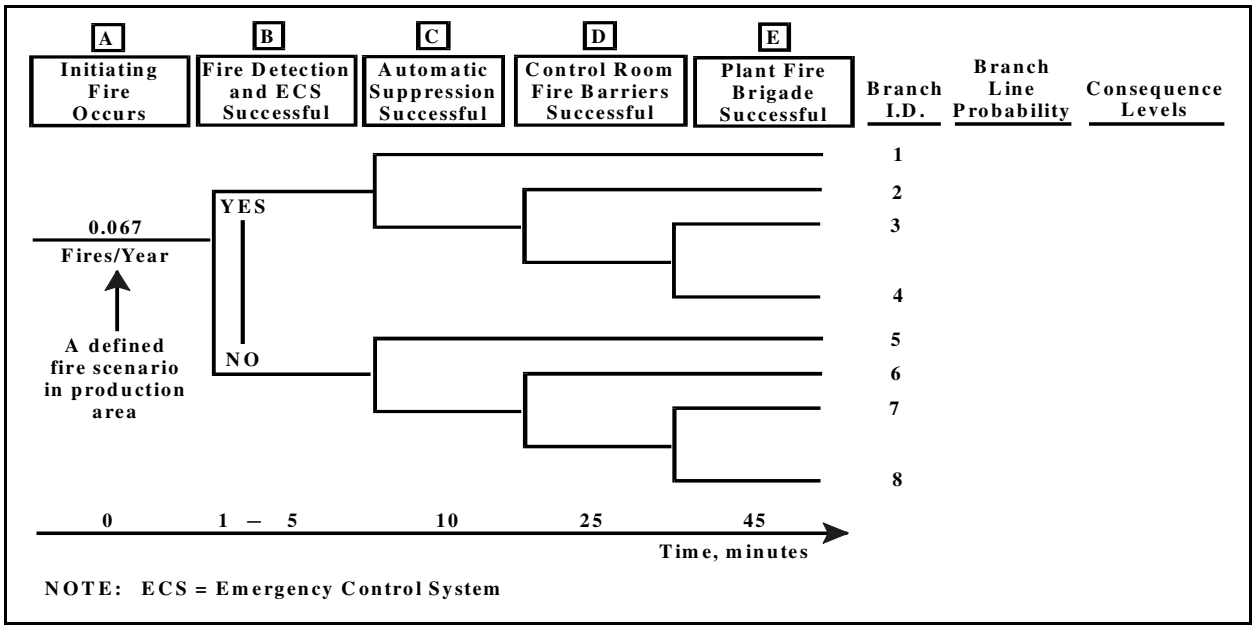
Fig. 6.20: Example Scenario-Based Exposure Profile Curve with Target Tolerance Points



TARGET TOLERANCE POINTS	ESTIMATED TIME LIMITS	TIME LINE FACTORS						
① People	3 – 5 min	Detection Time	+	Alarm Notification Time	+	Evacuation Time	≤	5 min
② Equipment	5 – 10 min	Detection Time	+	ECS Operation	+	Automatic Suppression	≤	10 min
③ Structure	25 – 45 min	Fire Brigade Notification Time	+	Fire Brigade Response Time	+	Manual Suppression / Extinguishment	≤	45 min

Figure 6.21 presents an example event tree time line based on Table 6.4 and Fig. 6.20.

Fig. 6.21: Example Event Tree Showing FPS Response Success Time Line Parameters



The purpose of this type of evaluation is to provide a probabilistic relationship between functional performance objectives and time limits for a specific scenario as shown in Table 6.5.

Table 6.5: Example Performance Objectives Versus Time Limits

	DETECTION	EMERGENCY CONTROL	AUTOMATIC SUPPRESSION	FIRE BARRIER	FIRE BRIGADE
Functional performance objectives	Detect heat and transmit alarm to control room for shutdown actions. Sound local alarms for employee evaluation	Following alarm, operators activate remote hydraulic oil shutdown, production equipment shutdown	Provide fire control and suppression of oil fire	Prohibit heat, smoke infiltration into control room	Automatic suppression system backup and final extinguishment
Time limits	1 – 3 min from fire initiation operate and transmit alarm	3 – 5 min from fire initiation, shut down hydraulic oil system	3 – 10 min; have successful suppression by sprinkler system	1 – 25 min; maintain control room barrier integrity	10 – 45 min; response and final extinguishment

6.2.7 FPS Response Time Evaluation Methods

Methods to evaluate FPS response time under scenario-specific conditions and performance requirements include:

1. Review manufacturer's data sheets, including product testing and approvals.
2. Conduct tests on automatic systems.
3. Perform drills to measure manual response.
4. Use deterministic models to estimate automatic detection and suppression activation response time (Chap. 5 addresses exposure profile modeling).
5. Apply engineering judgement and team consensus based on items 1 through 4 above.

Deterministic Modeling

In recent years, the response time of ceiling level heat detectors, fusible links on sprinkler heads, fusible links on roof-level smoke and heat vents, and spot-type smoke detectors have been modeled using the concept of time constant, τ, and response time index, RTI.[3, 4, 12, 13]

Estimated time constants for fixed temperature and rate-of-rise heat detectors have been developed based on the UL listing test procedures for these devices. These values, tabulated in Appendix B of NFPA 72, relate the listed spacings and temperature ratings of detectors to time constants allowing calculation of the RTI value.[3] The response characteristics of smoke detectors are not as well understood as those of heat detectors. They depend on smoke concentration, smoke particle size and optical properties. Some researchers have suggested that smoke detectors be treated as devices with time constants of 10 seconds, not as zero time constant devices, and with an effective actuation temperature rise, $T_d - T_o$, of 20°C (38°F). With these parameters, the response of smoke detectors can be estimated; however, there is much uncertainty in this method.

Presently, available fire models for calculating heat detector or sprinkler head activation time use the lumped mass heat transfer approach, with either the time constant, τ, or response time index, RTI, as the required input. Using a constant RTI value for determining detector or sprinkler head actuation time assumes that the time constant, τ, is always constant, which is incorrect because the time constant varies with the heat transfer coefficient, which in turn varies with the gas velocity past the detection device. To minimize calculation errors, some researchers are asking for tests that more accurately determine the heat transfer coefficient, h, τ and RTI for a wide range of gas velocities and detector geometries. An example might involve developing a test to find τ at three different velocities (slow, medium, and fast test fires) to provide representation of τ and RTI values associated with a detector type over a representative range of possible fire gas velocities. New methods need to be developed for evaluating smoke detector response.

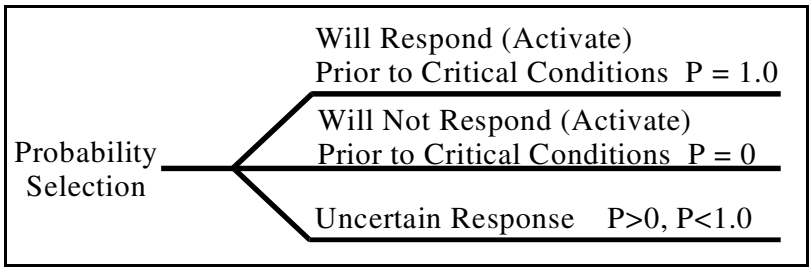
The concept of developing a thermal response coefficient (TRC) for heat detectors in lieu of using an estimated constant RTI based on detector head spacing is discussed in reference [4], which also provides a good discussion on the current state of smoke detector performance measures.

Computerized fire models contain many simplifying assumptions and approximations and users must be aware of the application limitations. In most cases, users will have to integrate engineering judgement into the interpretation of the results and use of the results to support probability of system response time estimates. Discussion of computerized fire models is provided in Chap. 5.

Conducting actual tests, if possible, of detection device actuation times provides an option to fire modeling. For example, using smoke generation devices, to test the response time of smoke detectors.

6.2.8 SRT Probability Selection

Following the review of results obtained from the evaluation methods discussed, the probability selection basis will fall within three categories.



In the majority of cases we will be able to select probability (P):

P=1.0 SRT Is Effective (responds prior to critical conditions)
P= 0 SRT Is Not Effective (does not respond prior to critical conditions)

However, in some cases there may be uncertainty due to insufficient knowledge, experience, modeling methods, and difficult to quantify factors.

Some factors that introduce uncertainty, especially in industrial facilities, include:

- Ventilation conditions
- Obstructions (between source fire pathway and location of detector or sprinkler head fusible link)
- Fire growth rate (smoldering versus flaming combustion)

One way to approach reduction of the uncertainty bandwidth is to expand the baseline modeling profile (input scenario, modeling assumption) by modeling some “what-if” modifications in the assumptions, such as the fire growth rate or ventilation rates, obstructions, or other factors. Figure 6.22 provides a simplistic illustration of some uncertainty factors.

Fig. 6.22: Some Uncertainty Factors

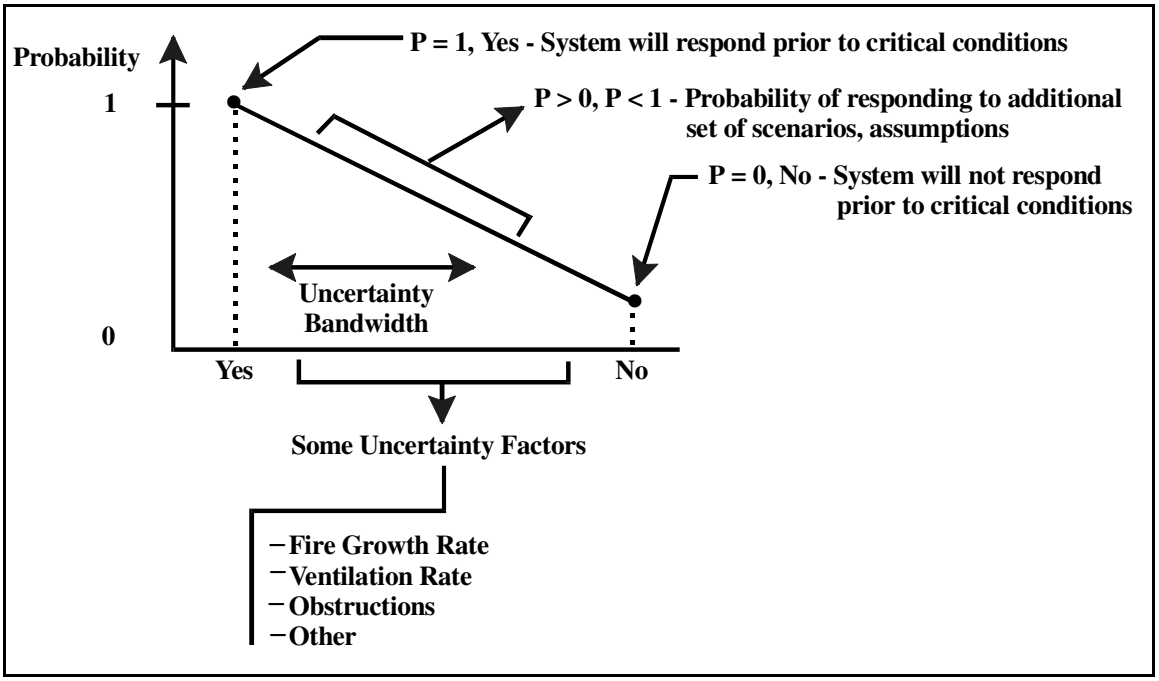


Table 6.6 provides an example of taking a baseline scenario (1A) and evaluating some modifications to the scenario (i.e., scenario 1B, 1C). The likelihood of these expanded scenarios are primarily engineering judgments based on some probable deviations that could occur in the modeling assumptions. Based on this evaluation, an accumulative probability of response time can be estimated.

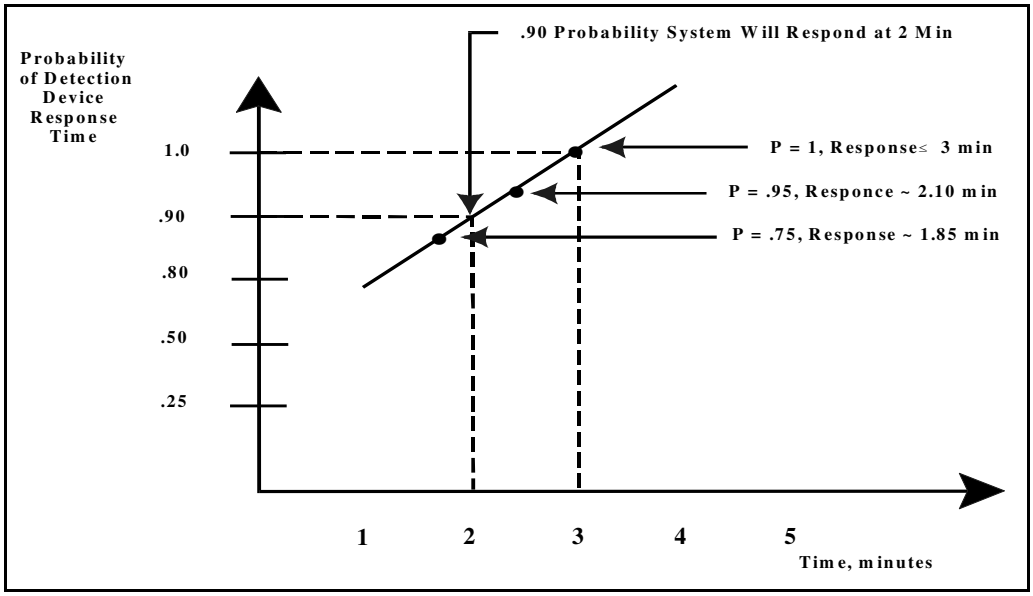
Table 6.6: Example Accumulative Probability of Response Time

FIRE SCENARIO	RESPONSE TIME (2)	RELATIVE SCENARIO LIKELIHOOD (3)	ACCUMULATIVE PROBABILITY
Scenario 1A - Baseline Scenario	1.85 min	.75	.75
Scenario 1B (1)	2.10 min	.20	.95
Scenario 1C (1)	3.00 min	.05	1.00
(1) Modification of baseline scenario	(2) Results of computerized modeling (i.e., fire model)	(3) Engineering judgement	

To allow a point probability estimate, the results of Table 6.6 can be plotted graphically, and by using linear regression or similar techniques, the probability of response at the estimated critical point can be estimated.

For example, as shown in Fig. 6.23, if our functional response time needed is 2 min, then the probability of this occurring is approximately 0.9, or 90% of the time. Again, SRT success probabilities are based on evaluation of specific scenarios and specific performance requirements.

Fig. 6.23: Example-Linear Regression Analysis of Response Time Probability



Explosion Suppression Systems

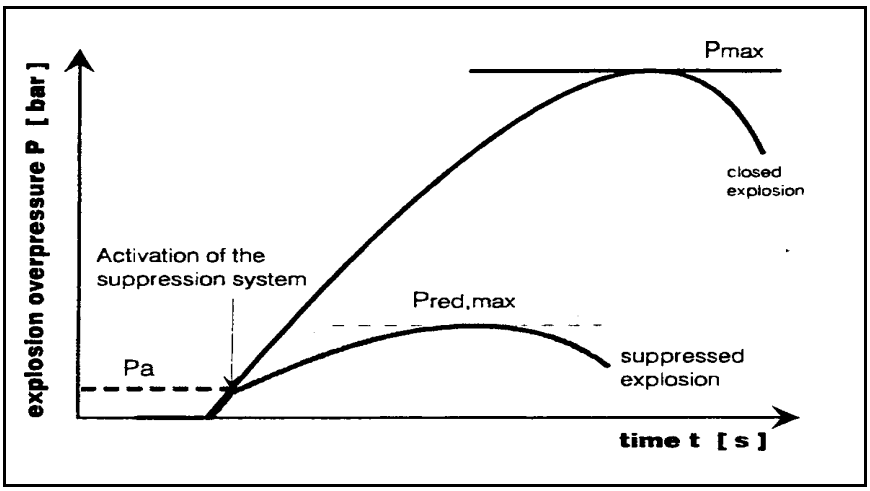
An explosion suppression system typically includes:

(1) Explosion sensor(s) or detector(s)
(2) High rate discharge explosion suppressor(s)
(3) Control and alarm equipment

The performance of these systems is evaluated in the same manner as FPS. The DAB (suppression agent suitability, capacity, duration), SRT (i.e., actuation time of optical sensors, pressure sensors, and discharge time of suppression agent prior to critical conditions) system availability, and operational reliability, are all factored in to the performance success probability.

The effectiveness of any explosion suppression system against an explosion is assessed by a determination of the suppressed (reduced) explosion pressure $P_{red,max}$ that prevents damage and provides a sufficient margin of safety as shown in Fig. 6.24.[5]

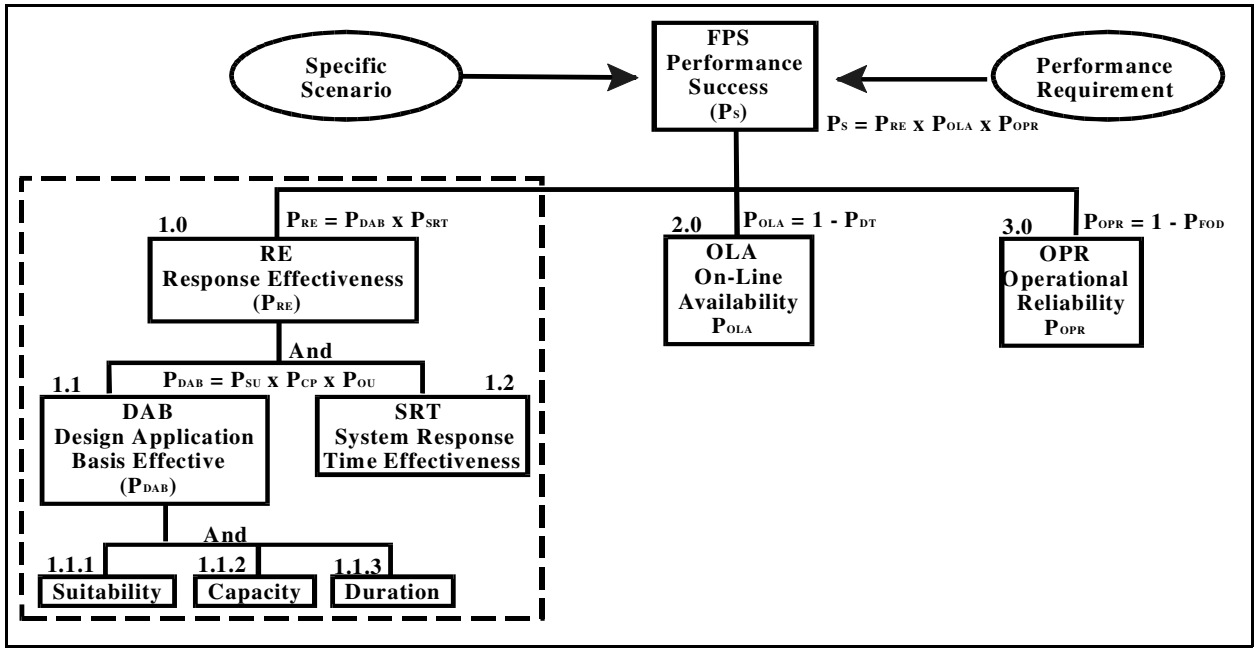
Fig. 6.24: Example of Pressure/Time Characteristic of an Unsuppressed and Suppressed Explosion



Summary

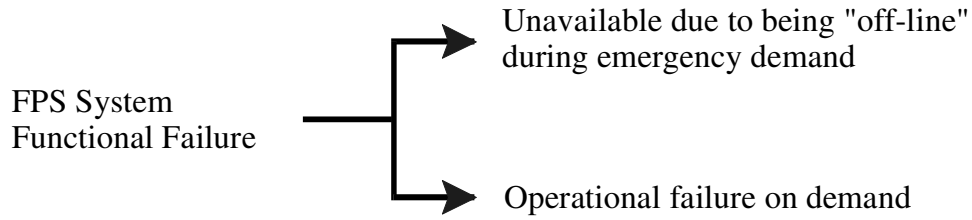
Figure 6.25 highlights the response effectiveness (RE) performance measure segment of FPS performance success. Evaluating the RE probability is the first evaluation conducted in FPS performance analysis, and in the majority of cases, it is the most important. As a first premise in the performance evaluation logic, the system must be properly designed to respond to the specific scenario and must respond within a time frame prior to critical exposure conditions.

Fig. 6.25: FPS Performance Success Tree Framework – Highlighting Response Effectiveness



6.3 ON-LINE AVAILABILITY

If the FPS is not on-line during an emergency demand, there is a failure. In our FPS performance evaluation methodology, FPS functional failure potential is broken down as follows:



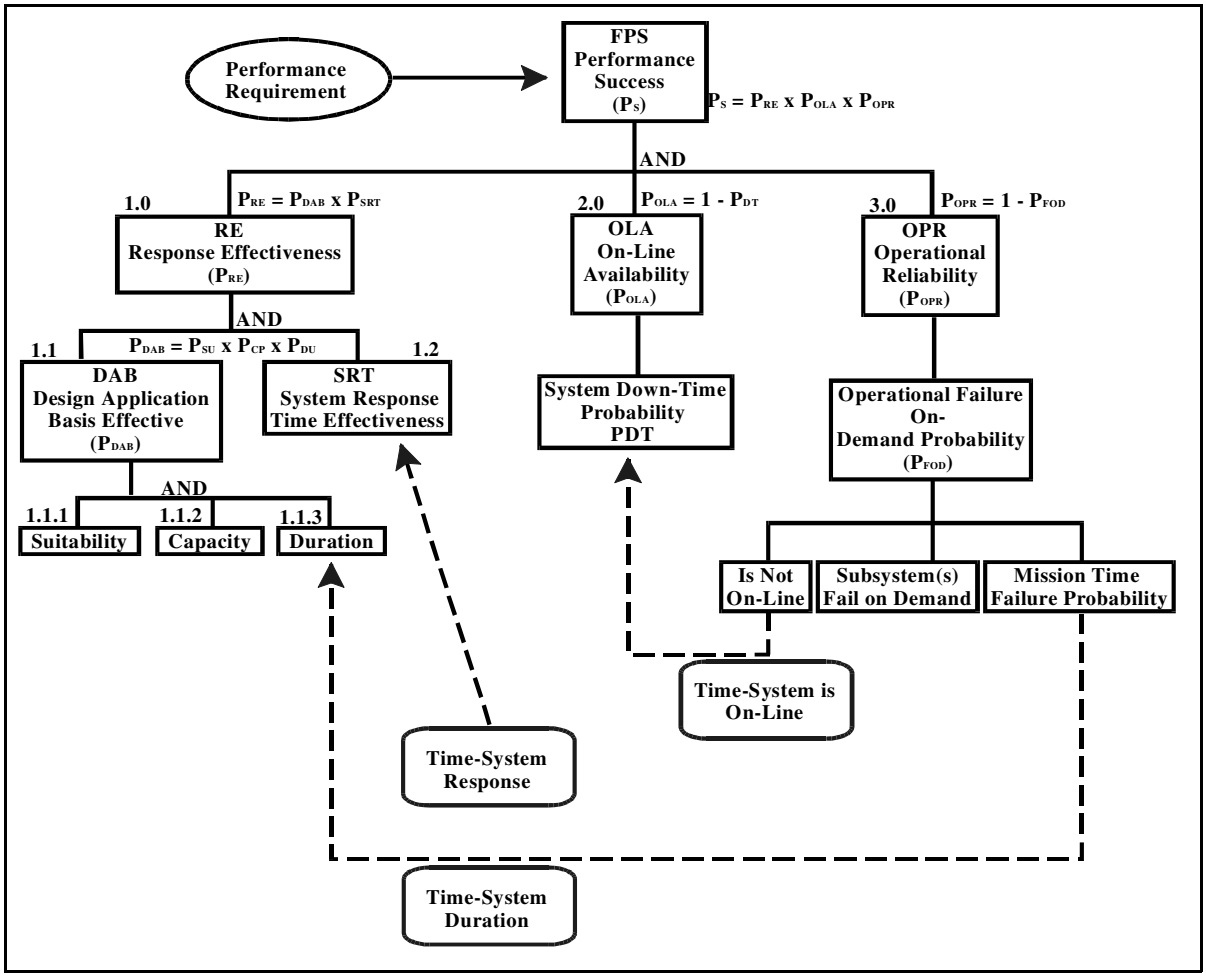
The major difference in this interpretation is that “Unavailability” is primary related to known or projected downtime potentials, while “Operational Failure-On-Demand” is primarily related to hidden or unrevealed failure-on-demand potentials, which are discussed in Sects. 6.4 and 6.5.

Figure 6.26 provides another illustration highlighting time relationships of the FPS performance success tree framework, . As presented in this figure, the operational failure of the system related to not being on-line is handled under the system downtime probability.

The benefit of examining on-line availability (OLA) as an individual reliability-based performance measure is:

- Existing Systems
  - Allows evaluation of down-time factors based on plant experience
  - Identifies downtime and availability factors related to inspection, maintenance, and testing (IMT) efforts, false system activation problems, and common cause problems such as freezing, flooding, etc.
- New System Designs or Modifications
  - Identifies opportunities to minimize potential downtime factors and to maximize availability based on design and recognition of common cause failure (CCF) potentials.
  - Identifies opportunities to minimize downtime potentials associated with IMT efforts

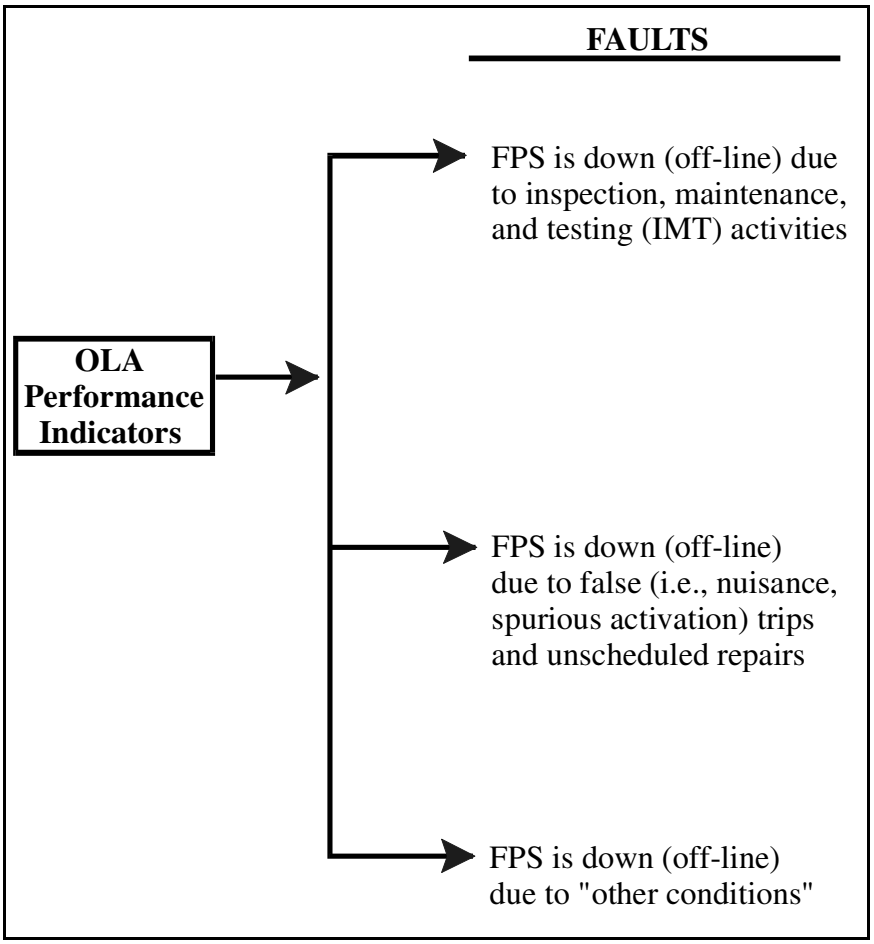
Fig. 6.26: FPS Performance Success Tree Framework — Highlighting Time



Performance Measures

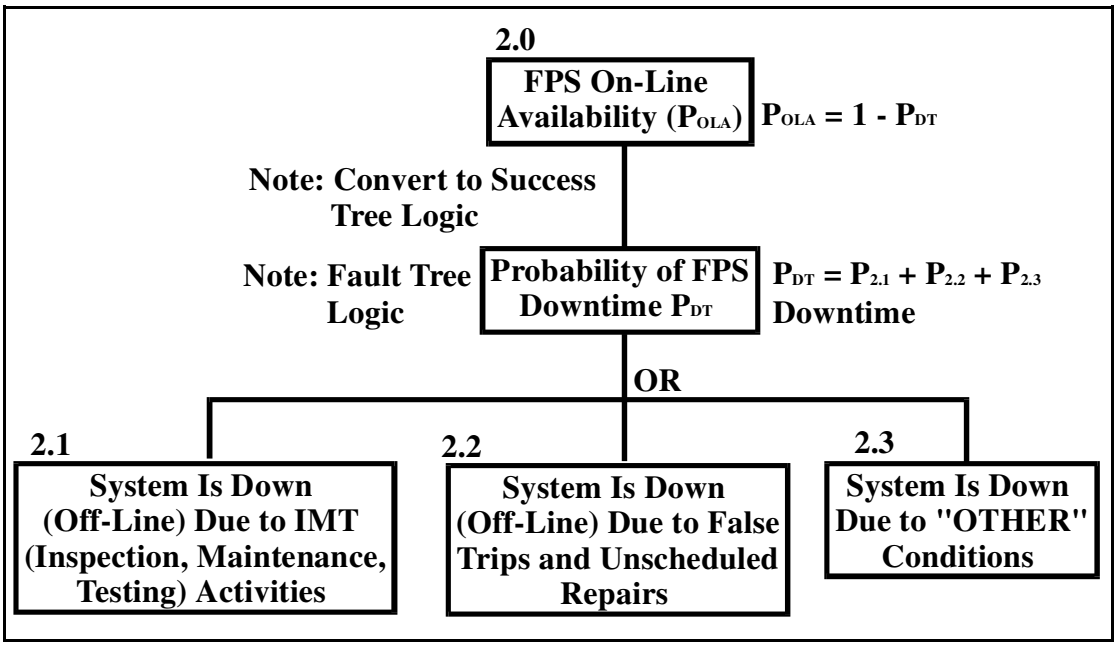
Figure 6.27 provides a listing of some primary OLA faults related to FPS downtime.

Fig. 6.27: OLA General Faults



Presented in Fig. 6.28 is the logic tree for OLA. As illustrated, a fault tree approach is used to evaluate the downtime probability (note "OR" Gate). This is then converted to success tree logic. The entire logic tree could be handled initially as a success tree, however, this conversion of using FTA and then converting is generally more efficient as information is usually conveyed in plant records as "downtime hour" not up-time or on-line hour.

Fig. 6.28: OLA General Fault and Success Tree Logic



6.3.1 Off-Line Due To Inspection, Maintenance, Proof Testing

The primary information sources on downtime associated with FPS system IMT activities are the plant's maintenance logs and records and interviews with plant maintenance personnel.

The estimates of this annual probability are derived from the historical or projected time (hours) when the FPS system is not available to perform its intended function, divided by the hours in a year. For example, if the system is taken off-line 80 hr per year for IMT efforts, then the annual probability of IMT unavailability is:

$$80\ hr/_{yr}\ \text{downtime} \ / \ 8{,}760\ hr/_{year} = 0.009$$

Interval unavailability due to IMT is given by

$$\text{Downtime}_{IMT}(0,T_I) = t_{TM} / T_I$$

where t_{TM} is the average duration of time the system is out of service for each periodic IMT and T_I is the interval of time between successive IMT efforts. Note: This unavailability does not include the unavailability due to system failure, which is addressed under operational reliability for hidden failure-on-demands.

It should be noted that IMT activities where systems are taken off-line present a negative effect under OLA evaluation. However, IMT efforts to discover hidden or unrevealed factors as part of the assessment of operational reliability is a very important factor. An optimized balance between the two needs to be considered when trying to achieve a maximum system performance success probability.

6.3.2 Off-Line Due To False Trips

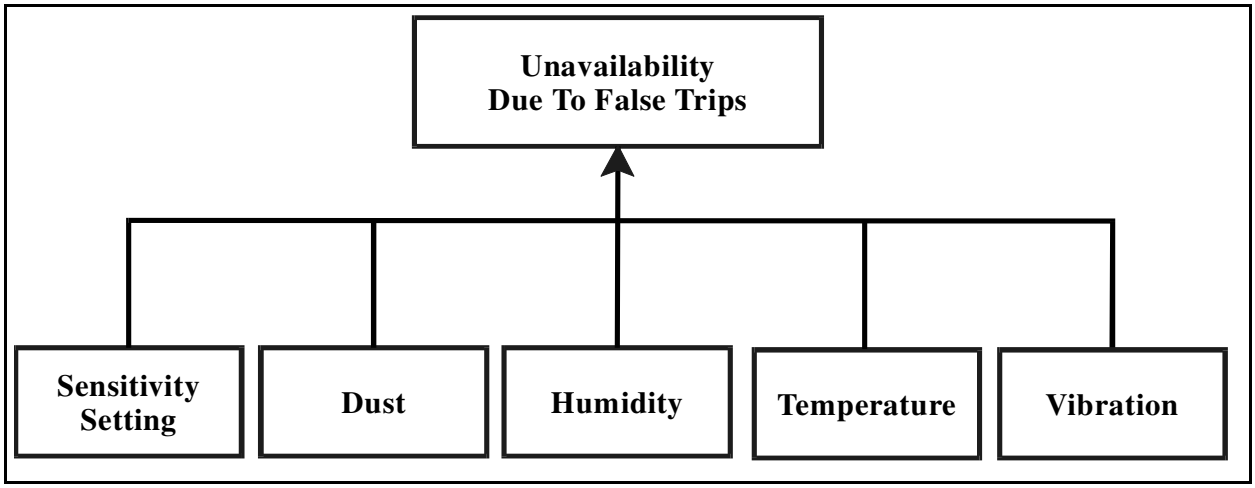
False trips or activations of FPSs, also termed nuisance or spurious trips, create a situation where the system is shut down and taken off-line so that cause can be investigated and repairs made if necessary.

The problems associated with false trips generally involve:

- The system is taken off-line and therefore is not available during a real fire emergency.
- When numerous false trips and alarms occur, occupants become complacent, responding slowly or sometimes ignoring alarms – a major problem in the event of a real fire.
- In many cases systems are bypassed and taken off-line for extended periods of time.

Most false trip problems are location and design related. For example, Fig. 6.29 lists some contributing false activation factors for detection systems.

Fig. 6.29: Some Factors Contributing to False Trips of Detection System



In many cases, facilities reduce detection-related false alarms by disconnecting or bypassing the alarm until the problem is resolved. While this reduces false trip errors, it increases the probability of having the detection system unavailable during a fire emergency.

Some other common causes of automatic fire detectors falsely activating include:

- Environmental effects (lightning)
- Insect induced
- Owner induced (lack of maintenance)
- User induced (accidental smoke generation or malicious actuation)
- Service induced (improper testing)

Good system design can prevent false activation of FPSs. The following provides two examples of what one corporate risk management office thought it had in terms of availability versus what it actually had at the plant site.

Upon obtaining design information for explosion prevention systems for six dust collection systems, along with the inspection and testing service agreement, the overall performance success appeared high. Based on the plant site survey, three of the six systems were bypassed and taken off-line because of four false activations of the systems over a three year period. The primary control panels were mounted adjacent to the dust collection systems, and it was evident that vibration was the primary contribution to the false alarms. This was a problem with the design and location of the control panel. Based on the site survey and downtime records from the plant, the system performance success probability, which initially appeared high, was rated very low. Correction recommendations focused on relocating the control panels to increase availability.

Another example involves the design and availability of flame detectors at truck loading racks for oil terminal facilities. Again, upon review of the design and service contract, the performance success of these flame detection systems, which were used to activate dry chemical protection systems, appeared high. However, upon site surveys, it was identified from plant records and interviews that at certain facilities, these flame detection systems were bypassed from automatic operation of the protection system. In a high lighting area at one facility, the flame detectors were bypassed an average of four months per year and therefore were unavailable. Corrective recommendations focused on the upgrade of the UV detectors to UV/IR detectors with a 15 second time delay.

Target availabilities for systems should be in the range of 0.99 to 0.999. The estimate of OLA annual probability is best derived from historical plant specific data extracted from operations and maintenance logs and records and interviews with plant personnel.

6.3.3 Off-Line Due To "Other" Conditions

From experience, it appears that adverse weather conditions (freezing, wind storms, flooding etc.) or unscheduled repairs from mechanical damage or vehicle damage represent a major portion of "other" conditions that render systems unavailable.

Adverse Weather Conditions

FPS unavailability from adverse weather conditions can cause a real problem to the overall performance success of a system. In many cases, this factor is not identified prior to fire incident occurrence.

For example in one project, based on plant records and interviews, it was identified at one plant that the control valves for a sprinkler protection system over the oil-fired burner system for a boiler were shut off for four months a year due to fear of freezing. The corporate safety director was unaware of this practice. The annual downtime probability on this system, which was a critical system from business interruption standpoint, was equated at

$$\frac{\text{4 months down}}{\text{12 months}} = \begin{array}{c}\text{0.33 annual probability of downtime} \\ \text{or} \\ \text{0.67 availability}\end{array}$$

As evident, this was a design and communication problem, which, in our methodology would severely affect overall system success probability.

Another example was discovered at a chemical plant. Due to flooding, water run-off, and drainage problems, the fire pump house was flooded three times over a five-year period. When the fire pump house was flooded, the controllers on the fire pumps were shut off, and the average time for clean-up and repair was 32 hr per incident. This equates to fractional downtime probability of 0.192 or an on-line availability of 0.81. Since the fire pumps presented a CCF to numerous deluge water spray systems at this plant, 0.81 on-line availability was not acceptable. Recommendations concerning water run-off channeling and drainage in the pump house area were made to improve this situation.

Unscheduled Repairs

Unscheduled FPS repairs following IMT efforts or external down-time caused by mechanical or vehicle damage can create an on-line availability problem. Having equipment spares, quick access to repair services, and contingency plans to expedite repair and replacement are very important.

For example, unscheduled repairs for components on fire barriers can represent an availability problem. Forklift damage to fire doors or fire barriers can be a recurring problem. From experience, I have reviewed many plans from a design standpoint where, at first glance, the performance success of the fire barrier walls would be rated high. However, after conducting a field survey, problems identified included damaged fire doors, painted fusible links on fire doors, doors wedged open and dampers tied open for ventilation reasons, unsealed cables penetrating the fire wall, etc. Based on engineering design review, field survey, and plant experience, an engineering judgment subjective probability is generally used to access “other” system down-time factors.

6.4 OPERATIONAL RELIABILITY EVALUATION LOGIC

FPS operational reliability (OPR) is the ability to operate on-demand and perform an operational requirement. OPR is not an on-line “availability” probability. For example, if a sprinkler system control valve is shut by scheduled authorized personnel to perform maintenance, repair, or proof testing, this is an unavailability factor. However, if the control valve partially fails or fully fails when placed in an emergency demand state due to a hidden or unrevealed failure, this is an operational failure-on-demand. Examples of other hidden failures might include: a gate valve drops causing partial or full obstruction to the sprinkler system water supply, or the valve is not fully opened following maintenance, repair, or testing, and this situation goes undetected until an emergency demand is placed upon it.

Quantifying the probability of FPS operational reliability involves the following steps:

1. Identifying performance success measures
2. Qualitative logic structuring
3. Quantification of failure-on-demand probabilities

This section focuses on items 1 and 2, which relate to qualitative logic structuring. Section 6.5 addresses failure-on-demand probabilities for quantification of OPR.

Figure 6.30 presents some of the primary faults and associated success measures related to FPS OPR.

Fig. 6.30: Example or General OPR Success Measures

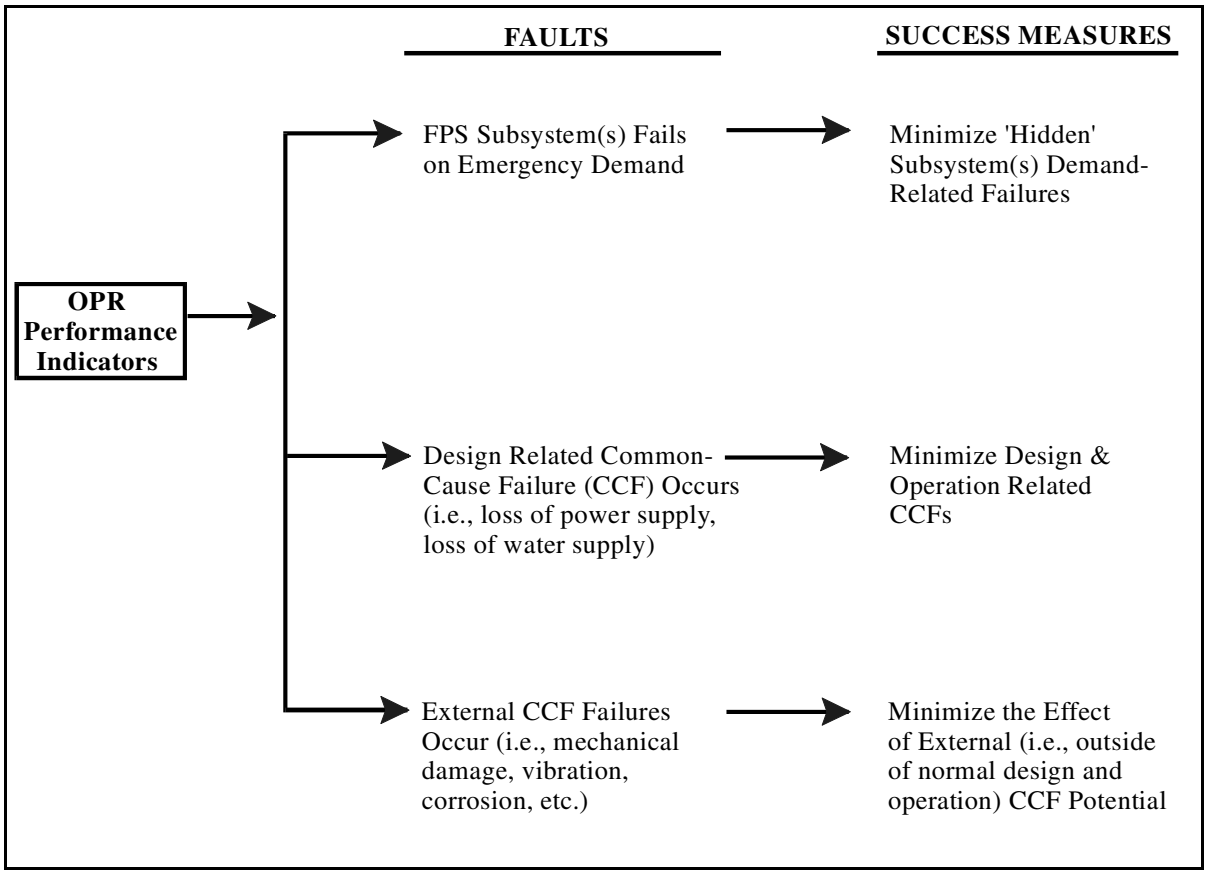
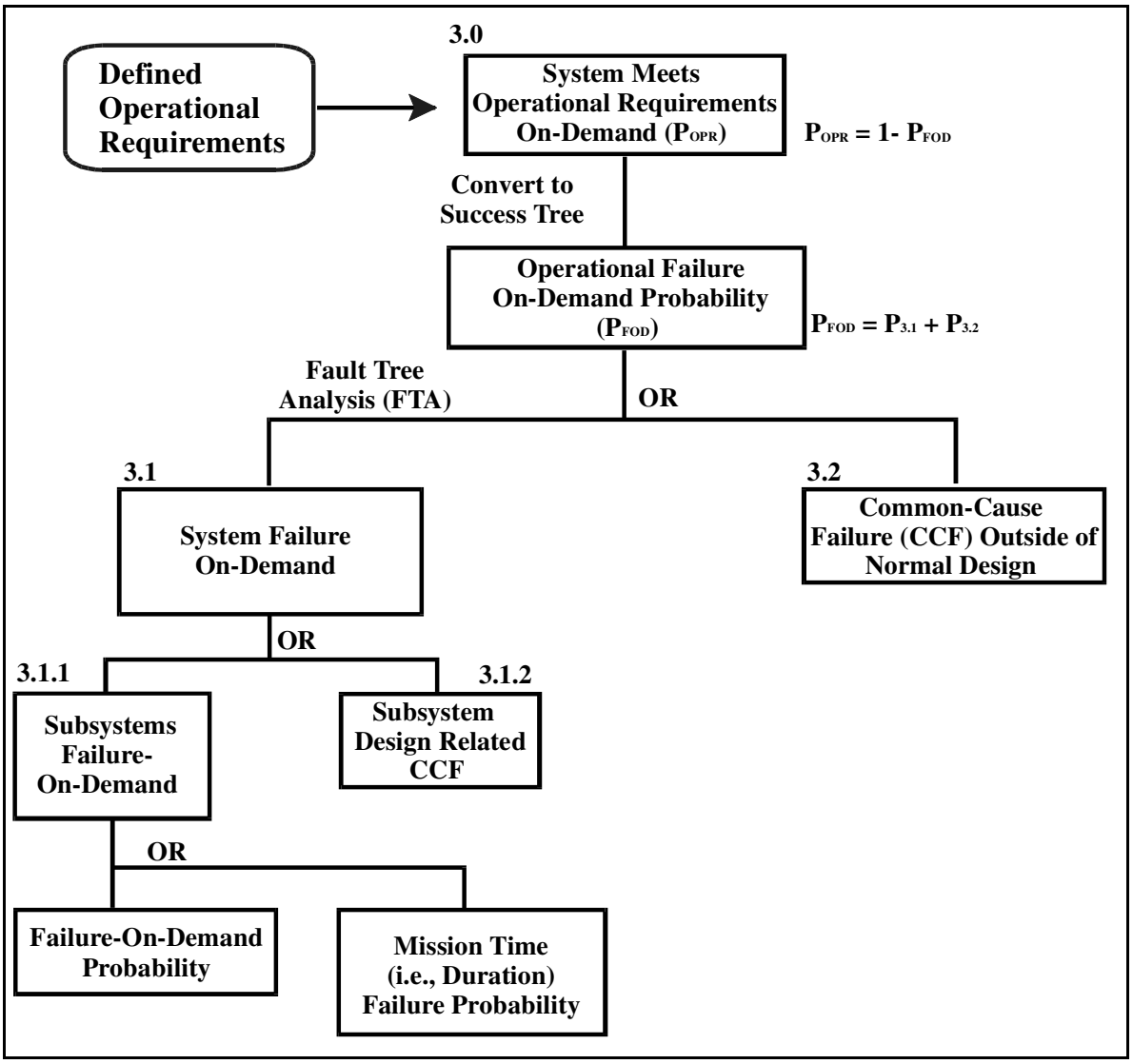


Figure 6.31 provides an illustration of the general OPR success tree framework. As noted in this figure, the system failure-on-demand probability (P_{FOD}) is evaluated using first-order fault tree analysis. The probability of successful operational reliability (P_{OPR}) (the top event) is then:

$$P_{OPR} = 1 - P_{FOD}$$

Fig. 6.31 Operational Reliability (OPR) Success Tree Framework



As presented in Fig. 6.31, subsystem failure (event 3.1.1) involves:

- Failure-on-demand probability (P_{FOD})
- Mission time (i.e., duration) failure probability

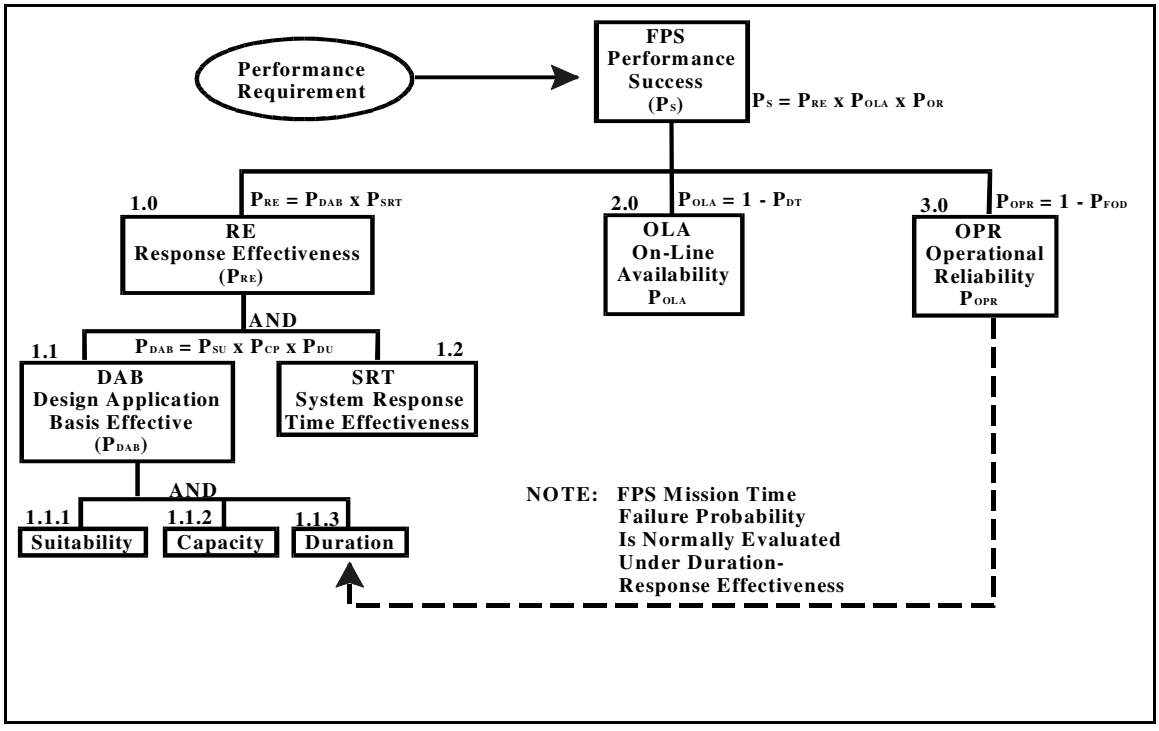
When evaluating FPS failure-on-demand probabilities, we are primarily interested in faults or failures that can be classified as hidden (concealed, undetected, unrevealed, etc.). Refer to item 4 in Table 6.7.

Table 6.7: Types of Failures

FPS Subsystem or Primary Component		
→	1. Fails Safe, Detected	Primarily from nuisance/false trips. Requires resetting, possible repairs.
→	2. Fails Safe, Undetected	In most cases, this would be identified by inspection and proof testing.
→	3. Fails Dangerous, Detected	Generally detected by on-line diagnostics (i.e., trouble signals) or visual inspections. Requires resetting, possible repairs.
→	4. Fails Dangerous, Undetected (i.e., Hidden)	Generally only identified when there is an emergency demand or by proof testing.

Mission or duration time is the period of time the FPS is required to respond under emergency (i.e., scenario-specific) conditions. This is the amount of time or duration the FPS must provide its defined function. As noted in Fig. 6.32, this time requirement is normally evaluated under duration-response effectiveness.

Fig. 6.32: FPS Performance Success Tree Framework – FPS Mission or Duration Time



6.4.1 Qualitative Logic Structuring

As previously stated, FPSs of primary interest in F&E risk-based evaluations include:

- Detection systems
- Emergency control systems (ECSs)
- Automatic suppression systems
- Propagation limiting measures (i.e., fire barriers)
- Manual loss control intervention

The framework for addressing DAB and OLA is very similar for numerous FPSs. The evaluation of the subsystem failures that need to be examined as part of OPR differs, however there can be a common method for addressing the evaluation structure.

Some logic structuring issues include:

- Apply a consistent "qualitative logic" methodology for FPS system and subsystem breakdown.
- Recognize and integrate manual intervention features if relevant to the evaluation (addressed in Sect. 6.6)
- Properly address operational requirements versus system redundancy features (overviewed in Sect. 6.7)
- Document assumptions.

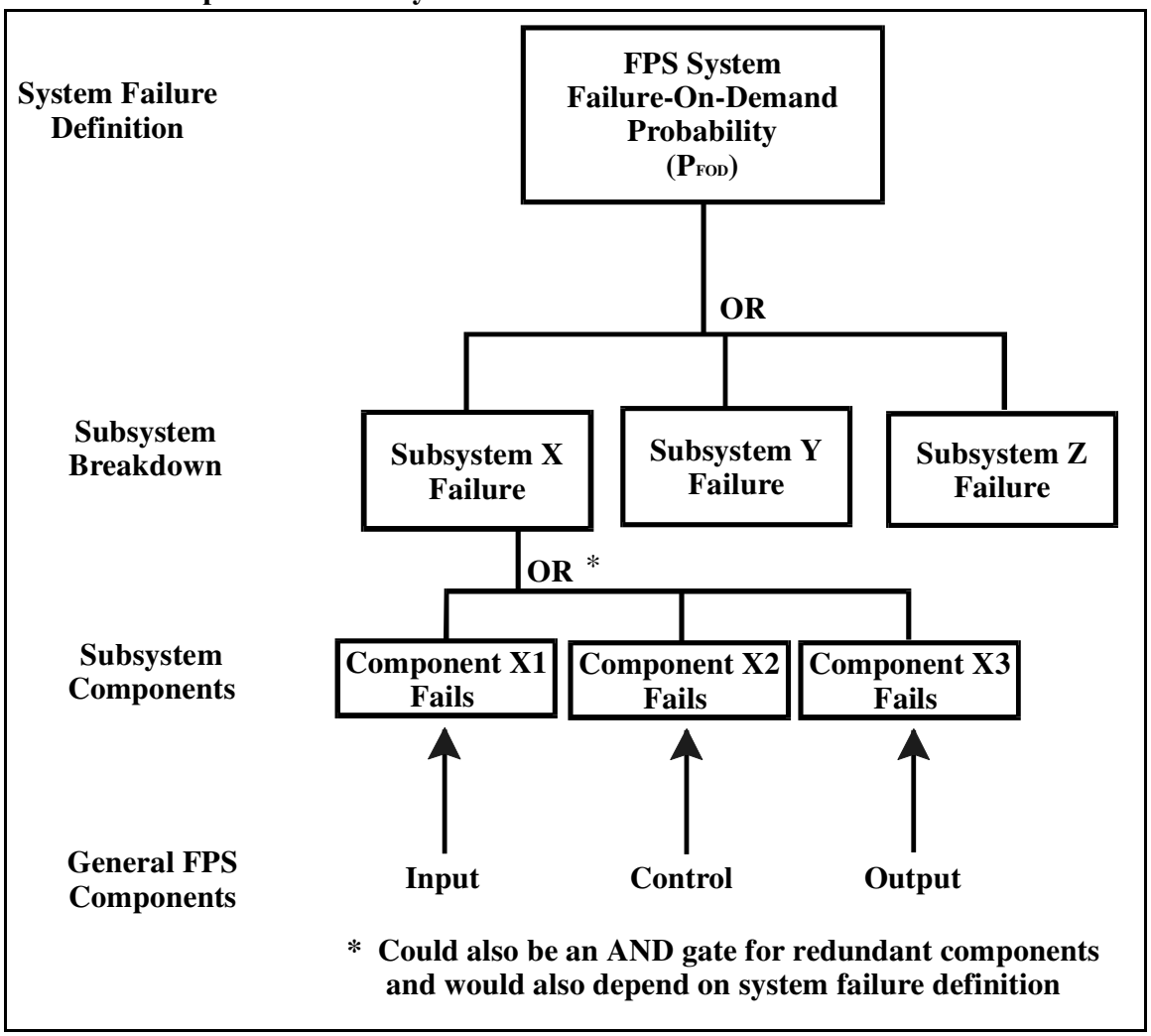
When evaluating OPR, we are initially concerned with a first-order review. That is, the probability of operational success of the subsystem elements and primary components that significantly contribute to the system level operational requirements.

Figure 6.33 provides an example of a first-order qualitative FTA breakdown:

- System level
- Subsystems
- Subsystem components

FTA is a widely used method for structuring and analyzing a system's reliability logic and for calculating the system's overall failure rate. The first and most important part of FTA development is to clearly define all the failure parameters associated with the top event, which is "system" failure. What exactly defines failure at the system level? For example; all the ten detectors in Zone A fail upon emergency demand; 20% of the water spray nozzles in Zone B fail upon emergency demand.

Fig. 6.33: Example of FPS Subsystem Breakdown



Input → Control → Output

In evaluating FPS failure-on-demand potential, one can subdivide the system/subsystem interface into an Input → Control → Output evaluation. Table 6.8 summarizes this for some systems.

Table 6.8: Example Input → Control → Output

SYSTEM	INPUT	CONTROL	OUTPUT
Detection System	Detection Devices	Control Panel	Alarms / Interlocks
Emergency Control System	Detection/Alarm Inputs	Control Unit(s) (PLC – Programmable Logic Controller)	Emergency Shutdown or Startup Interlocks
Fire Suppression Systems (i.e., a sprinkler or water spray system)	Water Supply • Tanks • Pumps	Water Distribution • Piping • Valves • Components	Water Flow at Nozzles • Piping • Sprinkler Heads/Water Spray Nozzles
Fire Barrier System	Barrier Components • Doors • Dampers • Penetrations	Barrier Integrity • Structural Components • Structural Stability of Wall	Fire Resistance • Tightness • Duration

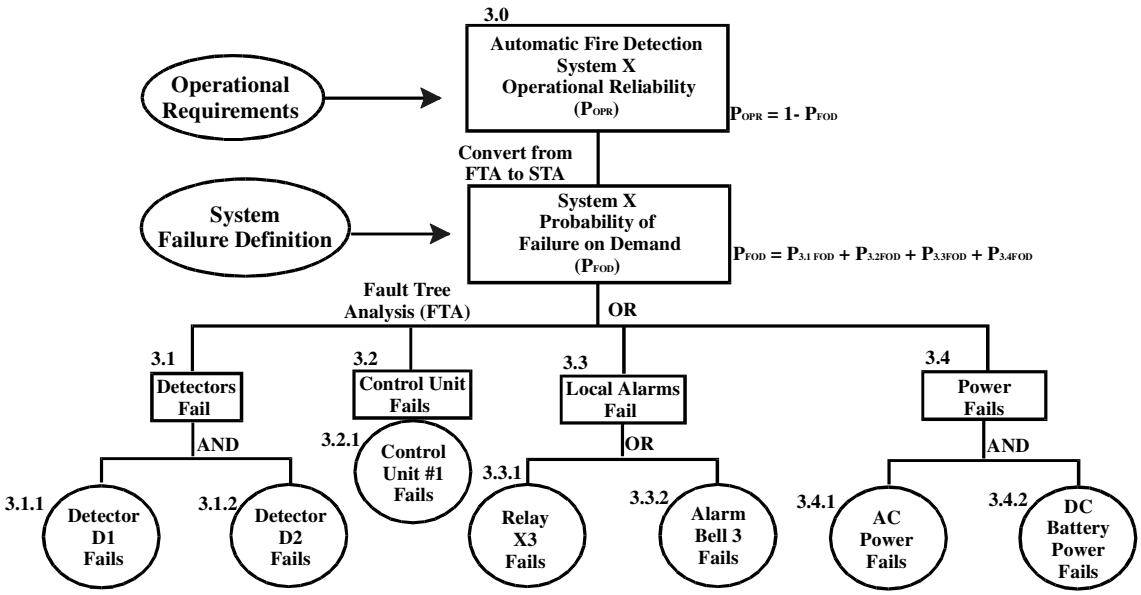
Automatic Detection Systems

For automatic detection systems, operational failure-on-demand potential is generally evaluated by breaking down the detection system into subsystems, such as:

- Detection device(s) (input)
- Control panel (control)
- Alarms, bells, horns (output)
- Power supply (CCF potential)

The functions and failure potentials of each subsystem should be identified as input into the fault tree structure and analysis. As an example, Fig. 6.34 provides a simplified breakdown of an automatic fire detection system with operational requirements (listed below the diagram).

Fig. 6.34: Example of General First-Order Detection System OPR Evaluation



System X Operational Requirement

Following the emergency demand (as specifically defined in the scenario input) a signal from a detection unit is delivered to the control panel, which relays the signal for local alarm notification and employee evacuation.

Note: The time response of the detector following the initiation of the emergency demand is evaluated in the "System Response Effectiveness" performance probability.

System X Success Logic

$P_{OPR} = 1 - P_{FOD}$

The system operational reliability (P_{OPR})

= 1 – Probability of system failure-on-demand (P_{FOD})

System X Failure Definition

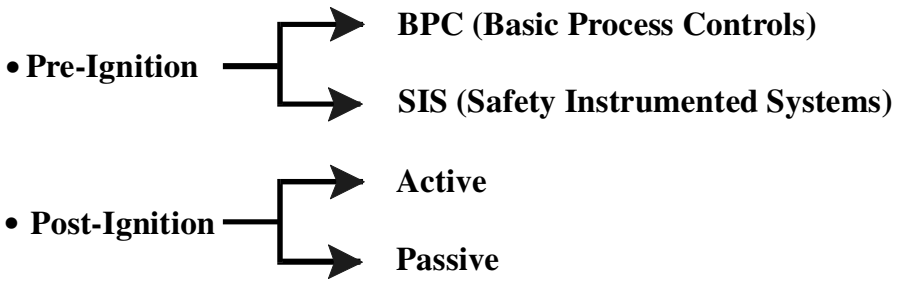
System X will fail on-demand (FOD) if any of the following occurs:

- Detector D1 AND D2 Fails (requires failure of two detectors)
- Control Unit #1 Fails
- Relay X3 OR Alarm Bell 3 Fails
- AC Power AND DC Battery Power Fails

A major assumption in FTA is that basic failure events are independent of one another. A basic event represents the failure of a subsystem component for which the component itself is responsible (note: the FTA system for a basic event, as shown in Fig. 6.34, is normally a circle). Therefore, it is important to check for component independence. For example in Fig. 6.34, Relay X3 (basic event 3.3.1) and DC battery power (basic event 3.4.2), depending on the design, could be physically located in the control panel and integrated into the control logic in such a manner that these failures would be evaluated in the overall control unit failure (basic event 3.2.1).

Emergency Control Systems (ECS)

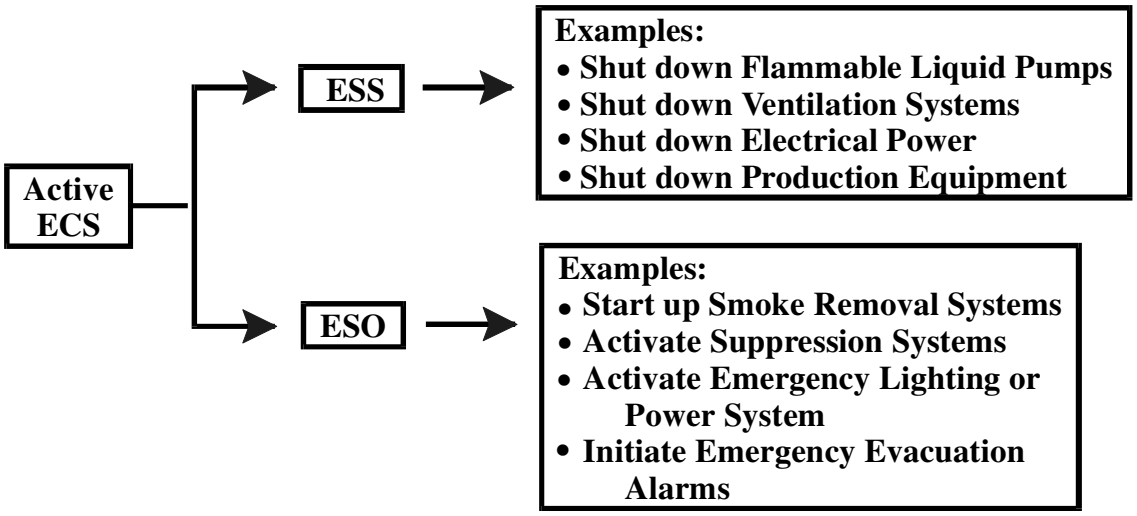
The probability of ECS performance success is evaluated in a very similar manner to detection systems. ECS can be placed into the following categories:



Pre-ignition ECS has been addressed in Chap. 4, Initiating Event Likelihood. This section addresses post-ignition ECS, which can include a number of different types of systems and functional requirements. Active systems are generally designed to shut down production related systems, equipment, or operations or to start up emergency systems or equipment following detection of a fire. Passive ECS can range from diking and drainage provisions to contain flammable liquid releases, certain types of explosion relief vents, aisle space between combustible storage to minimize fire spread, etc. The focus in this section is to overview active systems.

Active systems can be further defined in the following categories:

- ESS – Emergency System Shutdown
- ESO – Emergency System Operation



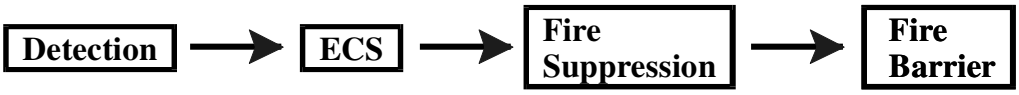
As related to fire detection interfaces inside production or process buildings, ECS functional requirements can include:

- Release of automatic door closers
- Stairwell or elevator shaft pressurization
- Smoke management or smoke control systems
- Initiation of automatic fire extinguishing equipment
- Emergency lighting control
- Unlocking of doors
- Emergency shut-off for gas and fuel supplies that may be hazardous

Presently, fire protection standards do not provide quantitative guidance towards the design of ECS to meet reliability-based performance levels. The best guidance on this subject is currently from the Instrument Society of America (ISA) in its document ISA TR 84. The methodology described in this document can be directly applied to fire protection related emergency shutdown and control systems. ISA provides design approaches for levels of design performance requirements versus reliability ranges considering failure rates, redundancy, and proof testing intervals.[14]

The methodology for approaching the evaluation of fire protection related emergency shutdown and control systems should parallel the guidelines developed by ISA (Instrument Society of America) for Safety Instrumented Systems (SIS).This is a very good reference that provides design guidance and methodologies such as reliability block diagrams, fault trees, Markov probability modeling, use of failure rate data, safety integrity measures, and prooftesting intervals. The reader is encouraged to obtain and review these documents. ISA's internet address is http://www.isa.org.

It is important to define the boundary conditions of the ECS along with the interfaces to other FPS systems. In the event tree analysis (ETA), each FPS generally represents an independent event sequence that is related by time and the specific functional requirement.



In many cases, the detection system and active ECSs are incorporated into one logic controller or there is a relay module connected from the fire alarm panel to an additional ECS control panel that initiates and controls the output functions.

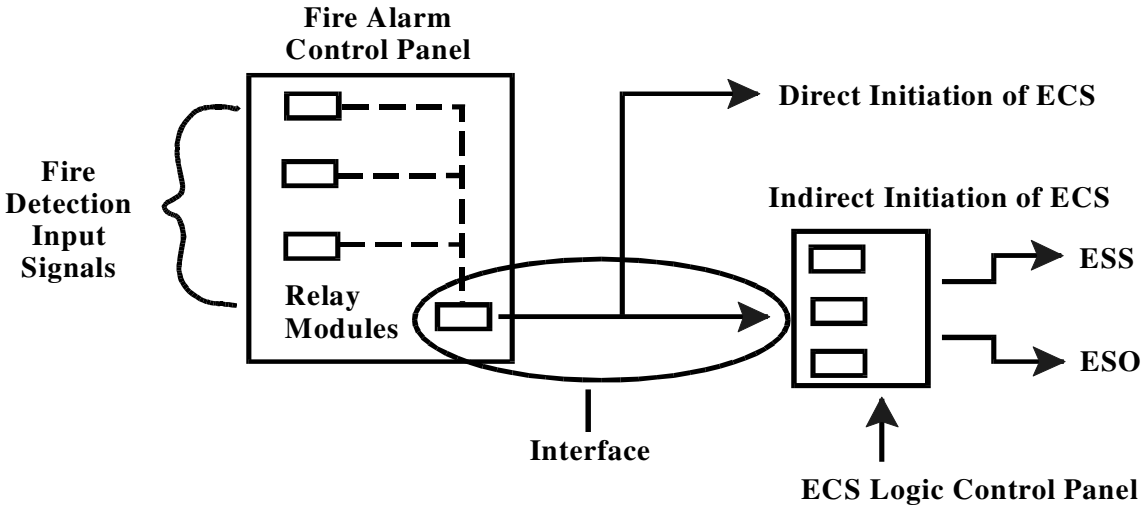


Figure 6.35 presents an example of an ECS performance evaluation framework.

Fig. 6.35: Example ECS Performance Evaluation Framework

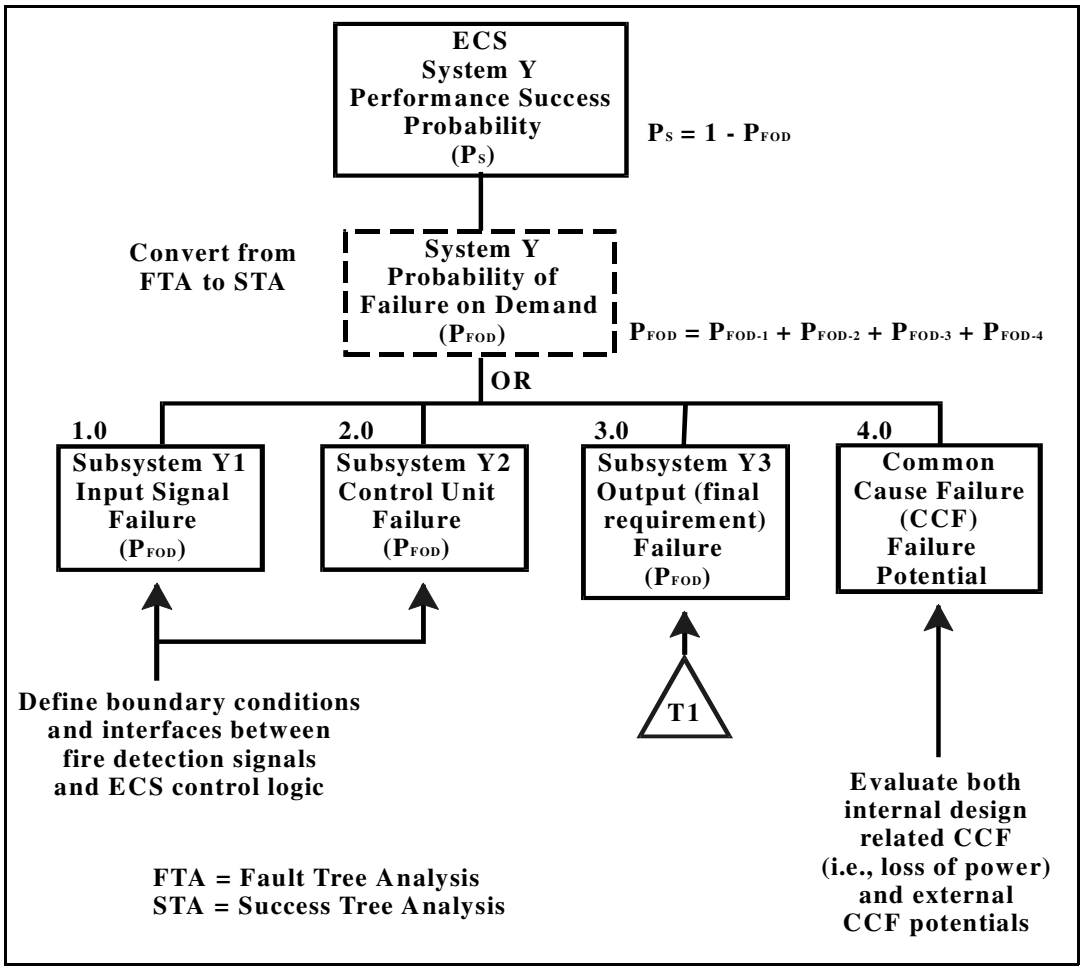
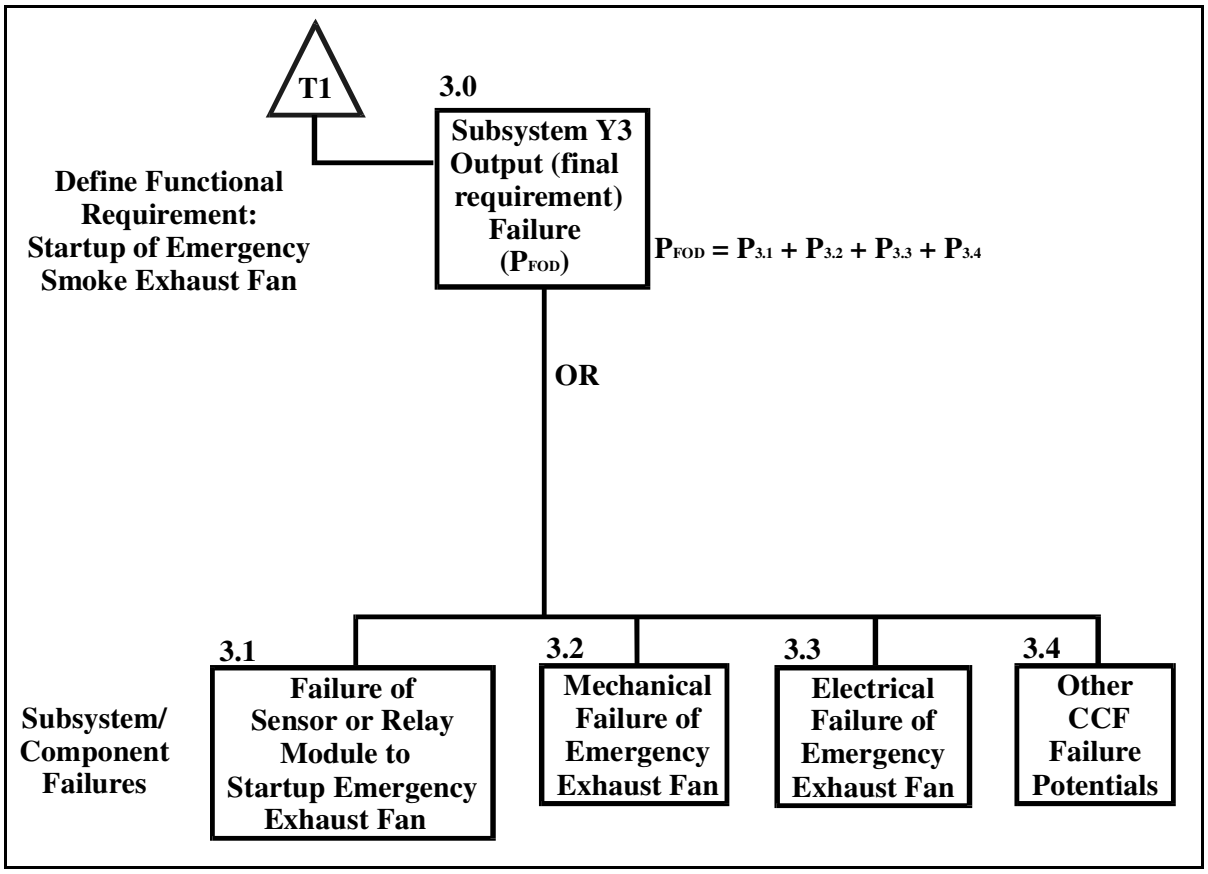


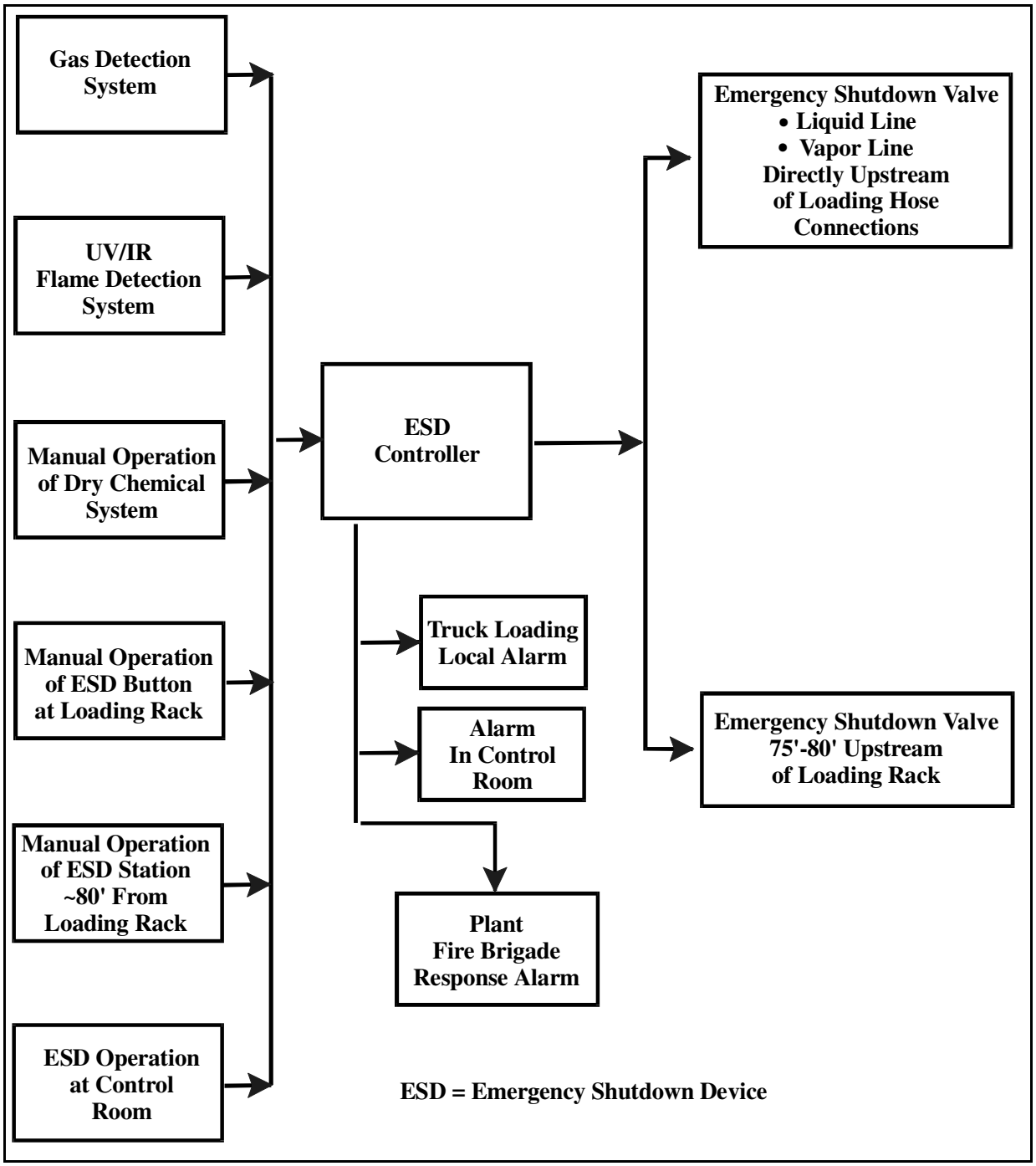
Figure 6.36 provides an example of a transfer function $\triangle_{T1}$, which is the output function of the ECS. The example in this figure is the startup of an emergency smoke exhaust fan.

Fig. 6.36: Example – Failure Evaluation of an Emergency Exhaust Fan



The structuring of ECS qualitative logic can take various forms during plant field surveys, design reviews, and interviews with plant operators. Figure 6.37 provides an example of a preliminary diagram for an ECS system of a flammable gas loading station. This diagram was later put into a fault tree format and quantitatively evaluated.

Fig. 6.37: ECS Framework Example – Emergency Shutdown System Logic Developed During Field Survey for a Liquefied Flammable Gas Loading Rack



Water-Based Fire Suppression Systems

Performance of water-based fire suppression systems is a primary consideration in mitigating fire propagation and damage. There are many types and configurations of systems. The focus here is to discuss a general framework for performance evaluation, which follows the information presented in preceding sections. The framework can also be used to evaluate other types of FPSs such as dry chemical, carbon dioxide, foam, etc.

As presented in Fig. 6.38, the framework for addressing fire suppression systems performance involves the evaluation of:

- RE – Response Effectiveness
- OLA – On-Line Availability
- OPR – Operational Reliability

The most detailed task is the evaluation of the OPR. The transfer gate $\triangle_{T1}$ is to provide detail on the operational reliability detail. Figure 6.39 illustrates the Input ➜ Control (Distribution) ➜ Output approach to the evaluation. Figure 6.40 is an example from transfer gate $\triangle_{T2}$, which provides some detail on the input subsystem contributing failure factors.

As evident, a full detailed assessment of OPR can be a major task. It is very important to identify the major contributing failures as a first step in the evaluation.

Fig. 6.38: Example Performance Evaluation Framework – Fire Suppression Systems

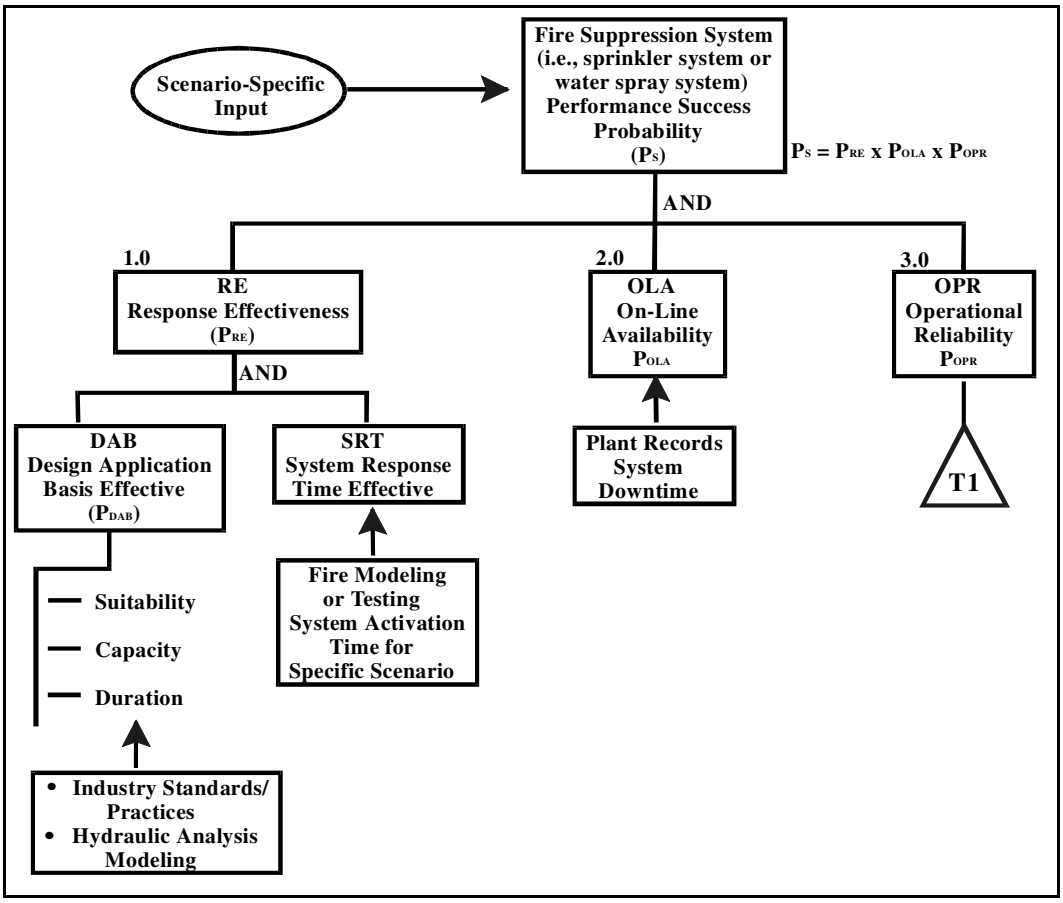


Fig. 6.39: Suppression System – OPR Evaluation Framework

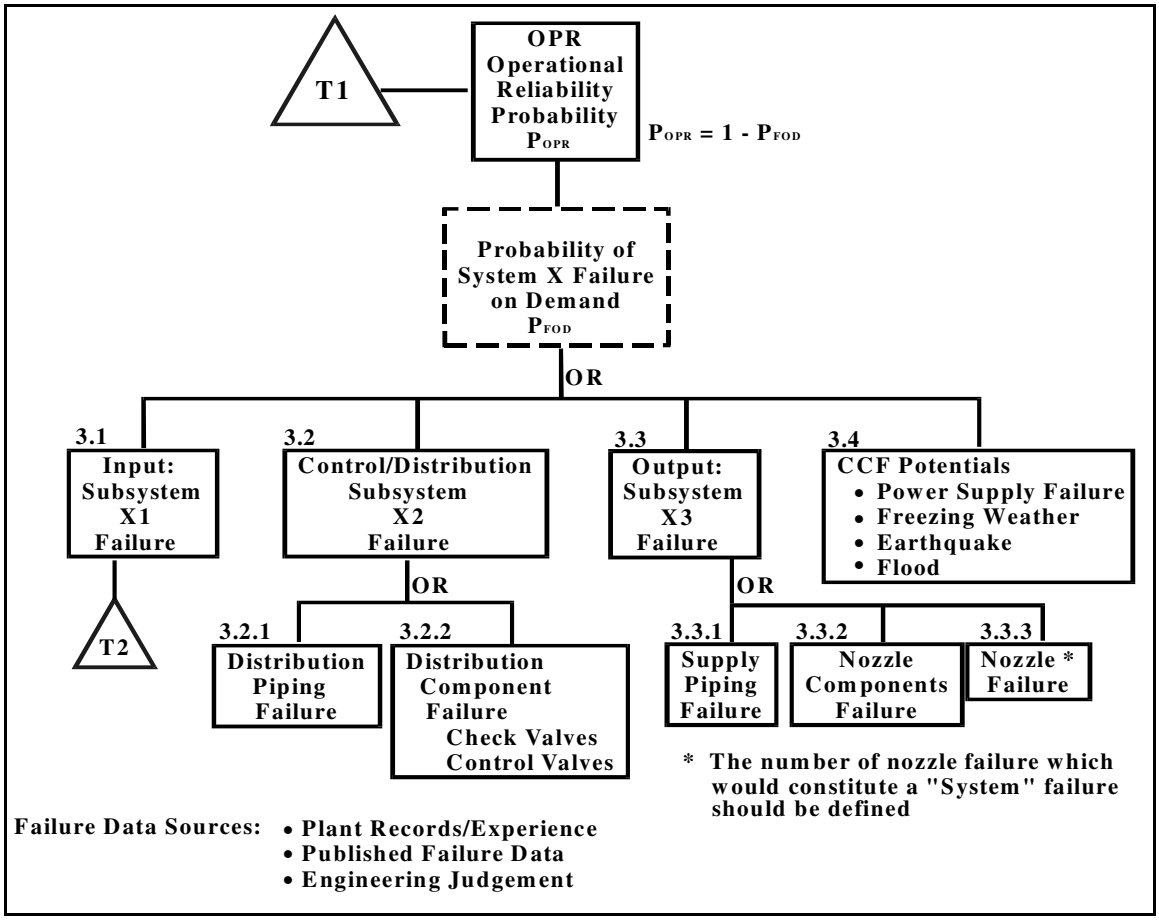
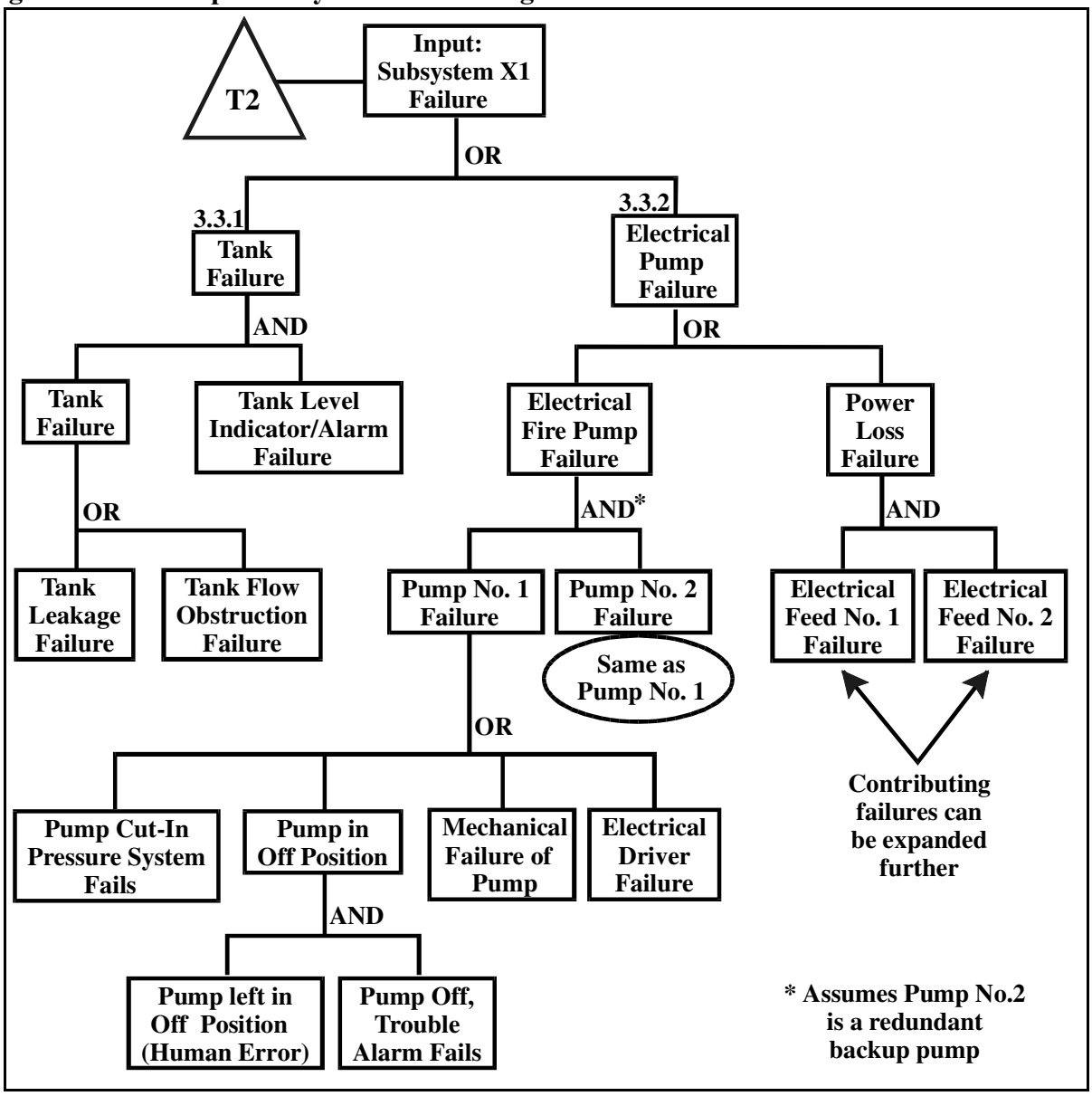


Fig. 6.40: Example Subsystem Failure Logic



Following the development of the qualitative logic tree structuring, it is very useful to set up a probability data source table, such as Table 6.9, to start compilation of failure data. Sources of failure data are described in Sect. 6.5.

Table 6.9: Example – Some Data Sources as Related to Fig. 6.40

FAILURES	PLANT RECORDS	MANURACTURED DATA	PUBLISHED FAILURE RATE DATA	ENGINEERING JUDGEMENT
• Tank failure	X			Design Review
• Level indicators	X	X	X	
• Pressure sensors (i.e., pump cut-in)	X	X	X	
• Controllers (i.e., pump controllers)	X	X	X	
• Trouble/supervision alarms (i.e., relays)	X		X	
• Pump failures	X	X	X	
• Electrical feed failures	X			Design Review
• Control valves	X		X	
• Check valves	X		X	
• Piping (tees/connections)	X		X	

Fire Barriers

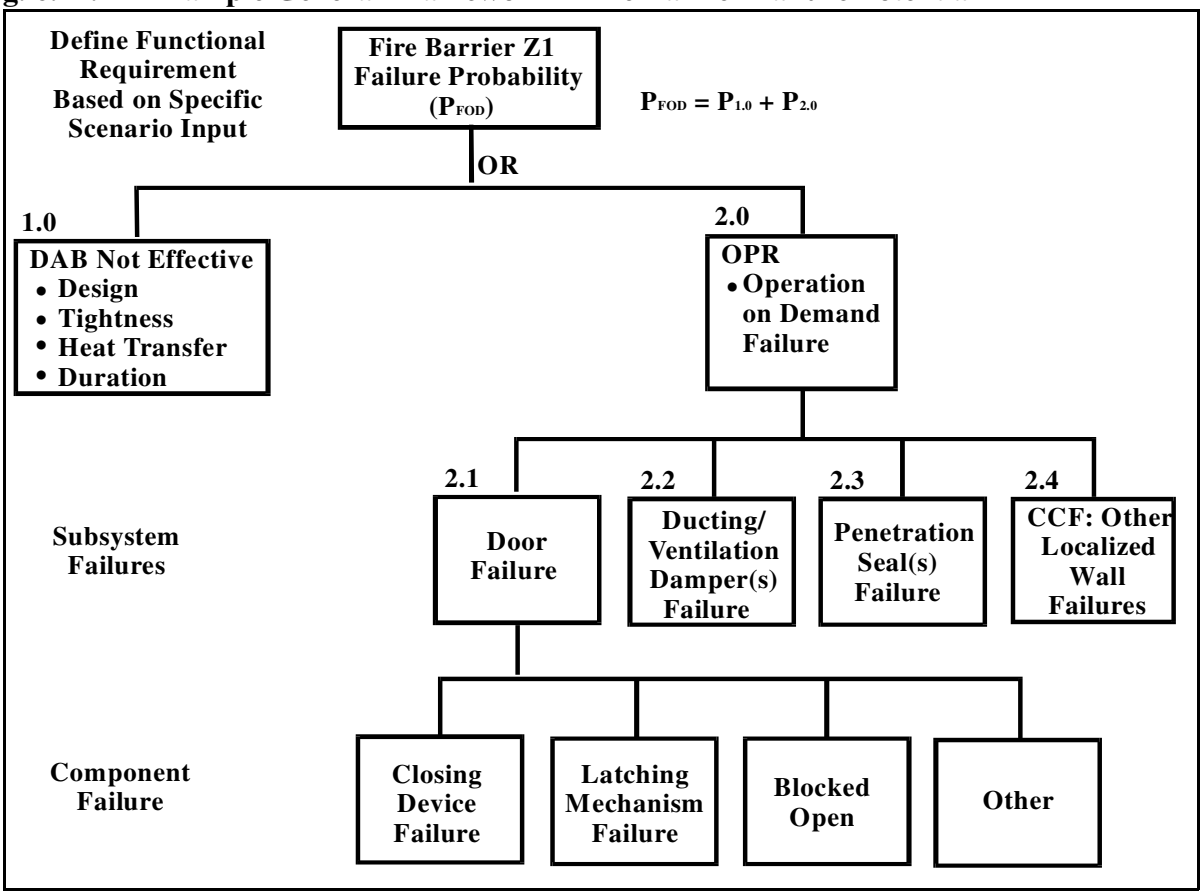
The effectiveness of a fire barrier in preventing the propagation of fire effects to adjacent compartments is determined by the physical performance of the barrier components and the heat transfer effects associated with transmission of fire and combustion products through the barrier.

All boundaries of a fire compartment credited as fire barriers, and their associated components need to be evaluated. These boundaries are walls, floors and ceilings. Barrier components may include doors, ventilation dampers, shutters, or penetration seals.

It is essential that the fire resistance of these components be evaluated, taking into account the scenario-specific severity of the fire in the area under consideration. In addition to the fire resistance aspect, other possibilities of the barrier failing need to be evaluated. They include: damper failures, doors left open, seal failures, or the existence of other unprotected openings. Particular attention may need to be given to those barrier components that require an active response to maintain fire barrier integrity (i.e., closing of a fire door via activation of a detection device).

Figure 6.41 provides an example of a general framework to evaluate fire barrier failure potential. Once the contributing failure logic has been developed, the functional requirements need to be reviewed as the probability of OPR success depends on "system" performance. For example, even though the wall itself may meet a fire and smoke resistance requirement, the openings (doors, ducts, conveyor, cable penetrations) may represent weak leaks that compromise the overall performance success.

Fig. 6.41: Example General Framework – Fire Barrier Failure Potential



Functional requirements of a fire barrier might include:

PERFORMANCE MEASURE	GENERAL REQUIREMENT	SCENARIO-SPECIFIC FUNCTIONAL REQUIREMENT
Fire resistance	Minimize heat transfer through barrier wall	Limit temperature on other side of barrier wall to XX temperature for 60 min
Barrier tightness	Minimize passage of smoke/ corrosive gases through barrier wall	Limit smoke/gas migration to other side of wall to YY concentration for 30 min

If the functional requirements of the fire barrier "system"are to limit corrosive products of combustion below a certain concentration, then the mass flow of smoke and combustion gases using fire modeling techniques can be evaluated and the time of closure of barrier wall components such as doors and dampers can be estimated. If the wall is equipped with high temperature fuse link door or damper closure devices, there may be a very low probability of meeting this functional requirement. With more and more automated production equipment and sensitive electronics being used in production buildings, smoke related damage issues can become a major concern.

Overall fire resistance and barrier performance can usually be based on engineering review and industry design standards and practices. However, this is not a review to meet a code requirement (i.e., a 2 or 3 hr wall code requirement) but an evaluation of fire resistance integrity-based on our specific scenario and defined functional performance requirements.

Fire models to evaluate the heat and temperature at the wall and wall components and heat transfer models to assess time-related barrier and barrier component stress can be applied in this evaluation to support success probabilities.

The following box provides some interesting information, indicating an approximate 15% failure rate on fire doors tested.

Information — Fire Doors

Reference: NFPA, Fire Technology, May 1992

Fire Doors: A Potential Weak Link in the Protection Chain

Diane L. Viera

Factory Mutual Engineering and Research

Norwood, Massachusetts

Of the fire doors tested through 1990, more than 15 percent failed to operate properly. During the testing FME&R engineers defined the causes of door failure. Failure mode categories include test difficulties and improper reset, inadequate maintenance, missing parts, door damage, occupancy-related concerns, defective parts, and improper installation. Table 1 shows the failure mode test results for the three doors that failed most frequently: rolling steel, horizontal sliding, and swinging.

Fire Door Failure Modes

Failure Mode	Rolling Steel (%)	Horizontal Sliding (%)	Swinging (%)
Test difficulties/improper reset	49	31	0
Inadequate maintenance	30	40	63
Missing parts	1	7	26
Damage	15	30	6
Occupancy-related	4	5	8
Defective parts	5	3	0
Improper installation	12	19	15
Unknown	6	5	2

Note: The total for each column is in excess of 100 percent because, in many cases, more than one failure cause was identified.

6.4.2 Operational Reliability (OPR) and Common Cause Failures (CCFs)

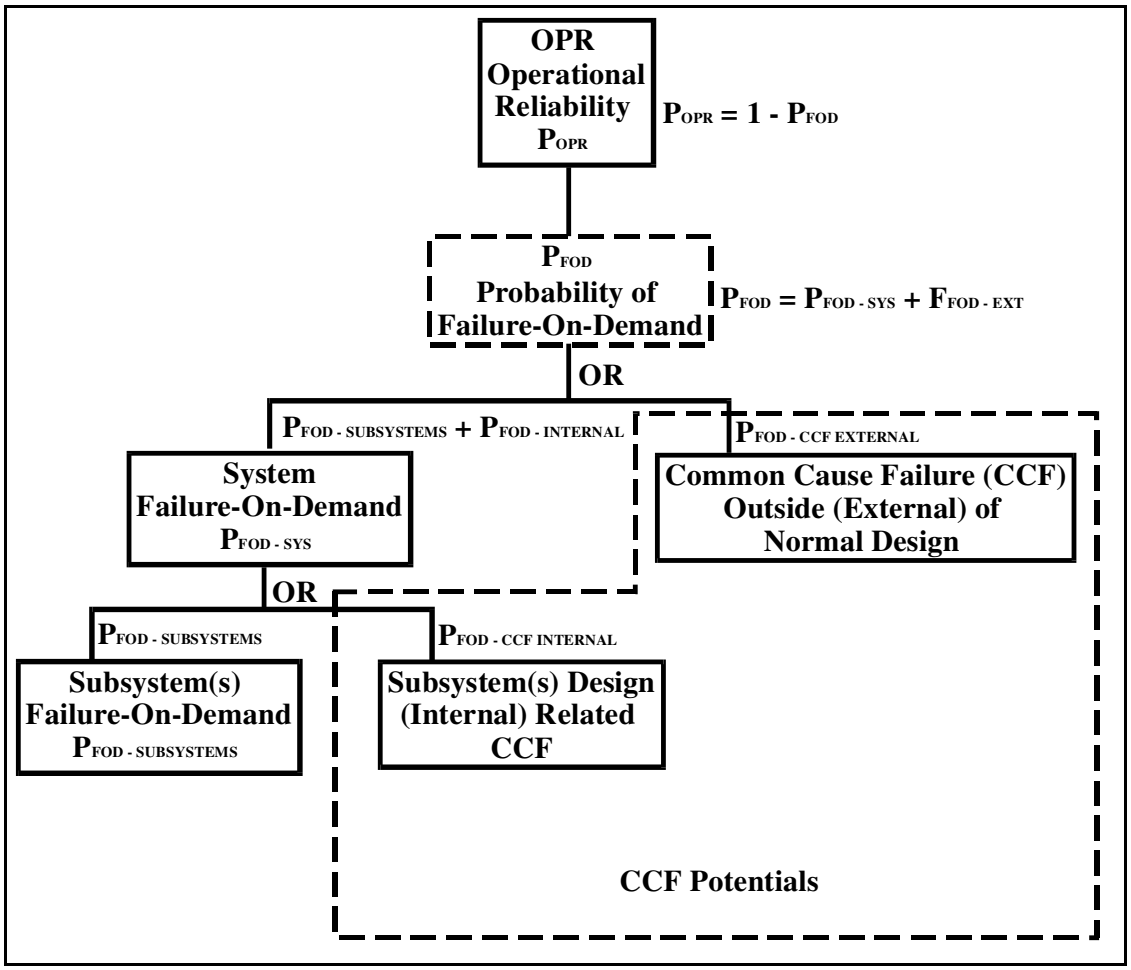
Identification and evaluation of CCFs are very important. Subsystem design related CCFs can include assessment of power supplies for detection and emergency shutdown devices, loss of water supplies for water-based suppression systems, etc. CCFs outside of normal design evaluation is subject to the definition of external events, which may or may not be integrated into the initial or proposed design, for example, earthquake design factors, freeze, flooding control factors, vehicle damage, etc. In establishing the qualitative logic structure, it is important to recognize CCF contributing factors and at this point qualitatively determine the potential affect on the overall OPR performance success.

In Fig. 6.42, CCFs are broken down into:

- Subsystem(s) design (internal) related
- CCF outside (external) of normal design

External CCF factors are addressed in Sect. 6.5

Fig. 6.42: Operational Reliability – Highlighting CCFs



Internal Design Related Failure Potential

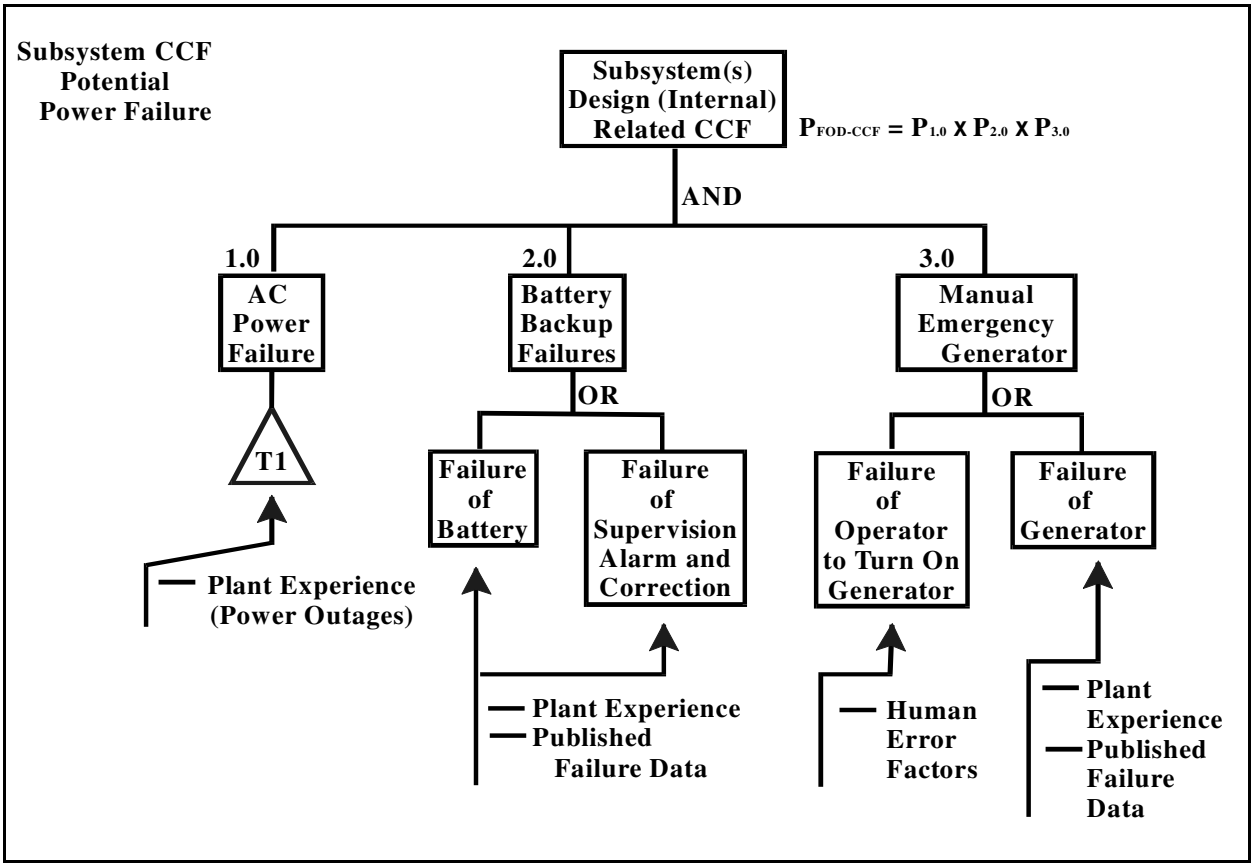
Internal CCFs affect numerous FPS subsystems and render the system inoperable to perform its intended function. Examples could include:

- Loss of the power supply to detection or emergency control subsystems
- Loss of the main water supplies for pumps that feed a water-based FPS

The scope of the risk evaluation and the complexity of the FPS usually dictates the level of detail needed to evaluate this. Most important up front is to structure a qualitative fault tree of the primary contributing factors.

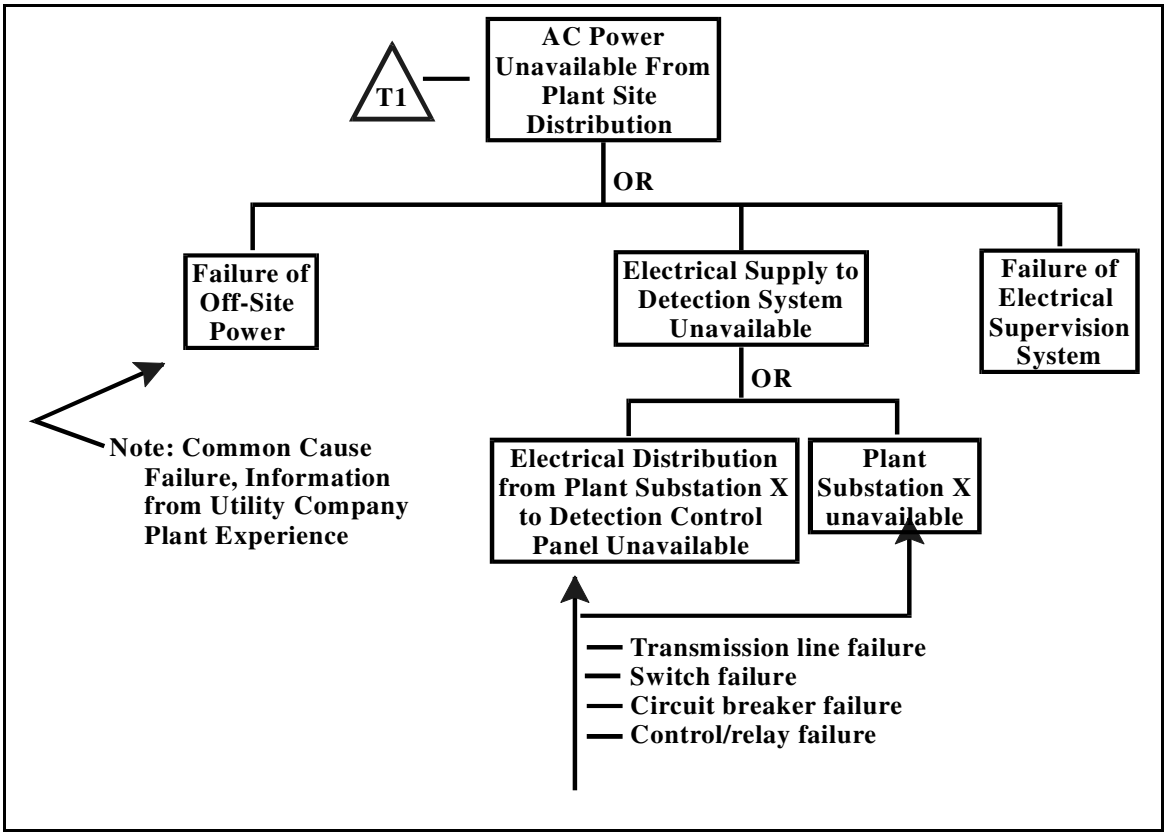
An example of a power supply CCF potential is given in Fig 6.43. Note the "AND" gate indicating the power supply redundancy. If the AC power fails, then there is battery backup. If AC and DC power fails, then there is an emergency generator that must be turned on manually (note – human factor error is discussed in next section). Some sources of failure data are listed below the fault tree.

Fig 6.43: Example Power Supply CCF



In most FPS designs, especially with power supply design, there is power redundancy and continuous supervision of incipient failures (i.e., low battery output) built into the design, thus a first-order failure evaluation can be conducted. However, in some instances, further CCF detail and analysis is needed, as presented in Fig 6.44.

Fig 6.44: Example of Further Detail – AC Power



OPR qualitative logic structuring provides:

- A consistent method for evaluating input → control → output subsystem interfaces
- Identification of failure modes and major contributing factors
- A logic tree template to aid probabilistic quantification

OPR quantification is discussed in Sect. 6.5.

6.5 OPERATIONAL RELIABILITY QUANTIFICATION

In risk-informed, performance-based fire protection studies, there are generally three ways to approach the quantification of FPS OPR:

1. Historical reliability data
2. Fault tree analysis (FTA)
3. Performance-integrity-based reliability levels

Credible historical reliability data (i.e., plant, industry, generic data) for the wide range of fire and explosion systems in use today is scarce. Usually the best one can do is to research and compile generic failure data for subsystem components and perform a first-order FTA. First-order FTA focuses on major contributing failures and primarily uses generic mean failure rates to develop failure on-demand probabilities (P_{FOD}) to estimate OPR (OPR = 1 - P_{FOD}).

This section focuses on the information needed to estimate P_{FOD}. An additional feature discussed in this section is the use of performance integrity measures (PIMs) to adjust generic failure rate data based on plant specific knowledge and engineering review.

The method of quantifying FPS OPR by performance-integrity-based reliability levels, which combines PIMS and engineering judgement is discussed in Sect. 6.8.

This section provides an introduction to reliability quantification using first-order fault tree logic. There are numerous good text books on reliability engineering that describe additional methods such as Markov Chains and, Stochastic Simulation (i.e., use of Monte Carlo Simulation). Some other references are listed in the box below.

Some References – Reliability Engineering

- Sutton, Ian S., *Process Reliability and Risk Management*, Von Nostrand Reinhold, New York, 1991
- Modarres, M., *What Every Engineer Should Know About Reliability and Risk Analysis*, Marcel Dekker, Inc., New York, 1993
- Smith, David J., *Reliability, Maintainability, and Risk: Practical Methods for Engineers*, Butterworth-Heinemar, New York, 1997

6.5.1 Probability Documentation Table

Documentation of probability data used in the first-order FTA should contain a listing of failure rates and probabilities and identification of data source(s) and references. If applicable, the method for adjusting failure rates should be documented. If expert opinion is used, names and experience of the experts and the method used to derive estimates should also be included.

The documentation table in Fig. 6.45 provides an example format that can be modified or expanded to meet specific needs. This example table provides a platform for discussing the primary documentation inputs covered in this section, which include:

- Description
- Mean failure rate
- Adjustment factor
- Number of failures required
- Probability of failure-on-demand (P_{FOD})
- Reference (failure data sources)

Description

The identification (ID) number relates the table item to the failure event in the fault tree. Under "mode of failure," we are primarily interested in faults or failures that can be classified as hidden, concealed, undetected, or unrevealed.

Mean Failure Rate

The value selected for the failure rate, whether in terms of the mean, median, or average must be listed.

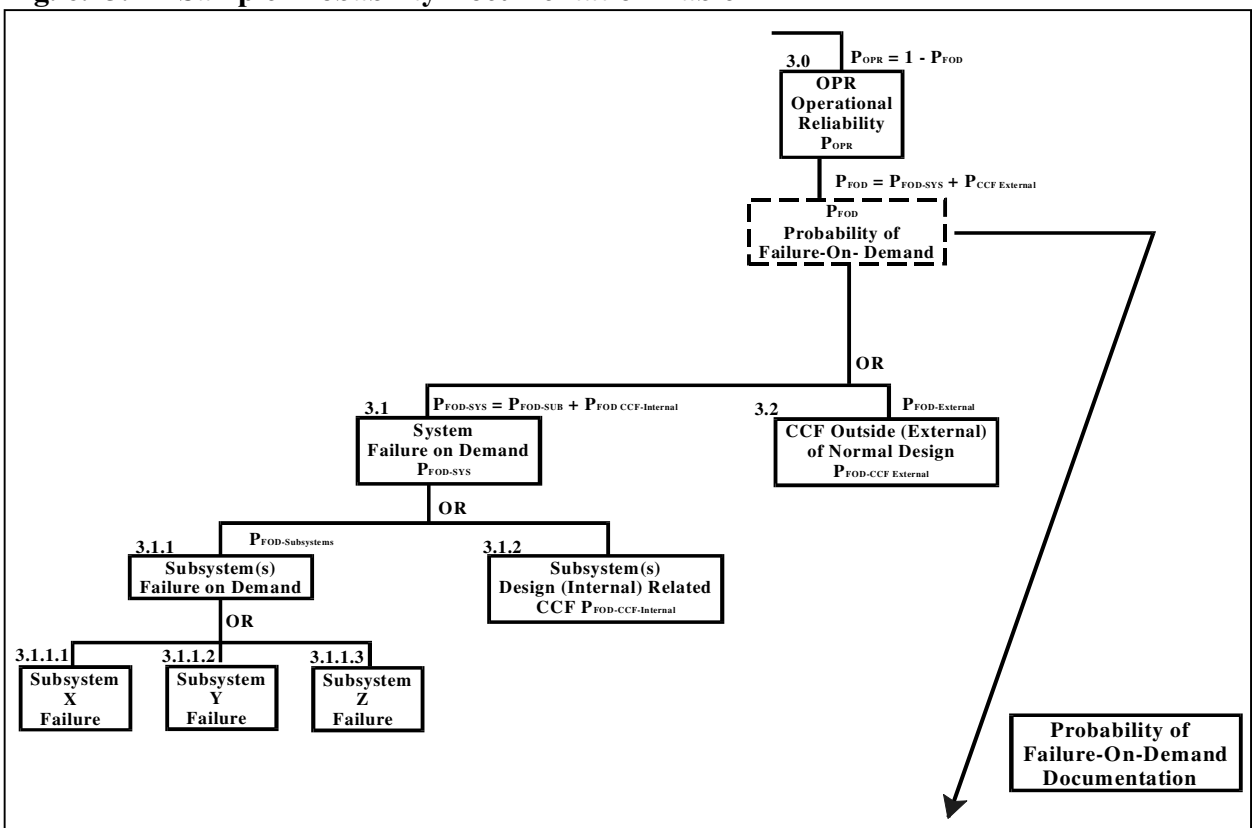
Some Definitions

Failure rate: The number of failures that occur divided by the total elapsed operating time during which the failures occur or the total number of demands, as applicable.

Mean Failure Rate: The measure of central tendency of a failure rate distribution, often referred to as its arithmetic average.

Failure probability: The probability — a value from zero to one — that a piece of equipment will fail on-demand (not to be confused with fractional dead time, which is an on-line availability factor) or will fail in a given time interval.

Fig. 6.45: Sample Probability Documentation Table



Example Probability Data Documentation Table

ID	DESCRIPTION • ID • MODES OF FAILURE	MEAN FAILURE RATE	ADJUSTMENT FACTOR	NO. OF COMPONENTS	FAILURE PROBABILITY P_{FOD}	REFERENCE
Description of events where failure probabilities are added		Failure rate or failure frequency	Adjustment of failure rate based on plant specific information, performance integrity measures, and engineering judgment	Number of components (i.e., check valves, control valves, etc.) or length of piping	Calculation of failure on-demand probability	Failure data sources used

Failure rates in the documentation table are given either as:

- Failures/D (Demand)
- Failures/HR (Time in Hours)

Failure rates can be obtained from plant data, manufacturer's data, and published data base sources and may be expressed in either terms of:

- Failures per time
- Failures per demand

$$\text{Time-Related Failure Rate} = \frac{\text{Total Number of Failures}}{\text{Total Operating Time Period}}$$

$$\text{Demand-Related Failure Rate} = \frac{\text{Total Number of Failures}}{\text{Total Number of Demands}}$$

On normally operating equipment, the demand is continuous and all failures can be considered a function of time. For FPS equipment considered emergency standby protection, the relative proportion of demand and time-related failures in combination with the frequency of demands and the type of maintenance and inspection program will have an impact on the total system failure rate. Details on how failures can occur are needed to fully understand the failure modes and to distinguish between time-related and demand-related failure rates.

Failures of continuously operating equipment are expressed as time-related failure rates. The time unit often used in failure rate data bases is h^{-1}, because very few items will fail more than once per hour. To convert from h^{-1} to yr^{-1}, the failure rate is multiplied by 8760 (i.e., 8760 hr per year). For example, a failure rate of 1 failure per 100,000 hr of continuous operation is equal to an annual failure rate of:

$$\frac{1 \text{ failure}}{100{,}000 \text{ hr}} \times \frac{8{,}760 \text{ hr}}{\text{year}} = \frac{.0876 \text{ failures}}{\text{year}}$$

If the system is in operation only 4,000 hr per year

$$\frac{1 \text{ failure}}{100{,}000 \text{ hr}} \times \frac{4{,}000 \text{ hr}}{\text{year}} = \frac{.04 \text{ failures}}{\text{year}}$$

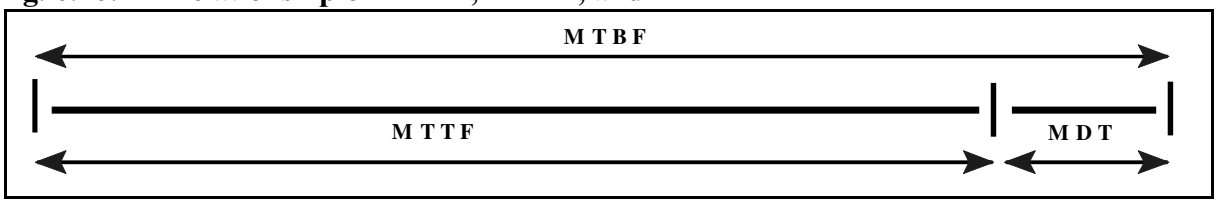
Those items that fail on-demand have a dimension less probability value. For example, if the demand-related failure rate is 40 failures per 1,000 demands, the failure probability is 0.04. As another example, the probability of operator error may be 0.25; this is a demand-related failure and it does not have units. It is extremely important to ensure that the correct units are assigned to a failure value so as to ensure unit consistency.

NOTE: Failure rate data sources are discussed in Sect. 6.5.3. and are also discussed in Chap. 4.

A commonly used measure of reliability is the mean time between failure (MTBF). The MTBF is equal to the mean time to failure (MTTF) plus the repair time. In many cases, the repair time is much less than the MTTF, so MTTF and MTBF are approximately equal. If the repair time is long, however, the two values may differ. [6]

Mean downtime (MDT) is the mean of times needed to restore an item to service. It includes not only repair time, but also other shutdown activities such as waiting for spare parts and moving an item to and from the workshop. The sum of MTTF and MDT is MTBF, as shown in Fig. 6.46. [6]

Fig. 6.46: Relationship of MTBF, MTTF, and MDT[6]



Overall Failure Rate, λ

Failure probability (P_f) can be modeled acceptably as a function of exposure interval (t) by the exponential, $P_F = 1\text{-}e^{-\lambda t}$. For brief exposure intervals ($t \leq 0.2$ MTBF), P_f can be approximated within 2% by λ (t), where

$$\lambda = \text{failure rate} = \frac{1}{\text{MTBF}}$$

Example: For subsystem X1, MTBF = 100,000 hr

$$\lambda = \frac{1}{100{,}000 \text{ hr}} = 1 \text{ X } 10^{-5} \text{ failure/hr}$$

Hours in service per year = 8760 hr

$P_F = 1 \text{ x } 10^{-5}$ failures/hr x 8760 hr = 0.0876 (annualized failure probability)

Failure probability (P_f); Reliability (R):

$P_F = 1\text{-}e^{-\lambda t}$
$R = 1\text{-}P_f$
$R = e^{-\lambda t}$

If the time interval of interest is 1 year, then:

$R = e^{-.0876\ (1)}$
$R = 0.91$

Same as:

$R = 1\text{-}P_{FOD}$
$R = 1\text{-}.0876$
$R = 0.91$

Table 6.10 provides an example of summarized failure data given in MTBF, for a liquefied natural gas (LNG) plant. [7]

Table 6.10: LNG Plant MTBF Data[7]

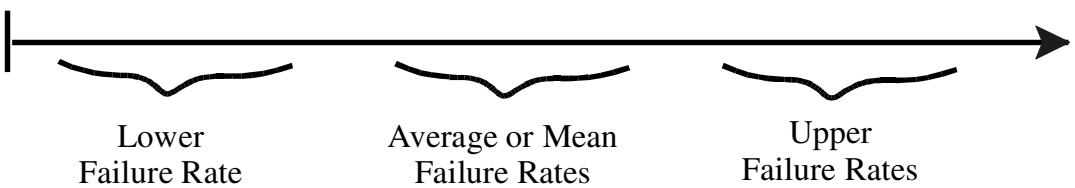
PLANT AREA	OPERATING HOURS	MAJOR FAILURES	MTBF (HOURS)
Gas pretreatment	675,000	25	27,000
Heat exchangers	2,837,000	16	177,000
Vaporizers	188,000	26	7,200
Cryogenic storage tanks	1,809,000	2	904,500
Cryogenic storage systems	1,809,000	4	452,000
Compressor systems	2,256,000	116	19,000
Cryogenic pumps	366,000	86	4,000
Cryogenic valves	6,278,000	4	1,569,000
Cryogenic piping	1,164,000,000*	2	582,000,000*
Process control systems	1,505,000	9	167,000
Human errors	4,779,000#	19	252,000#
Spills and leaks	1,626,000	11	148,000
Truck loading and unloading	1,156,000	0	>1,156,000
Fire protection systems	1,450,000**	24[n]	60,000**
fire water systems	1,450,000**	14	104,000**
dry chemical systems	1,423,000**	2	712,000**
gas systems	364,000**	2	182,000**
foam systems	88,000**	0	>88,000
Hazard detection systems	16,703,000	76[n]	220,000
gas detectors	16,703,000	44	380,000 (SD)
low temp. det.	2,631,000	2	1,315,000
flame det.	10,570,000	12	881,000
high temp. det.	8,418,000	0	>8,418,000

* Ft-hours # operator-hours ** in-service hours [n] normalized

From Gas Research Institute Report GRI-80/0093

6.5.2 Performance Integrity Measure (PIM) Failure Rate Adjustment

In evaluating failure rate data from plant specific records, published failure data, manufacturer's data, expert opinion, etc., we will develop in most cases a failure rate "bandwidth" or range:

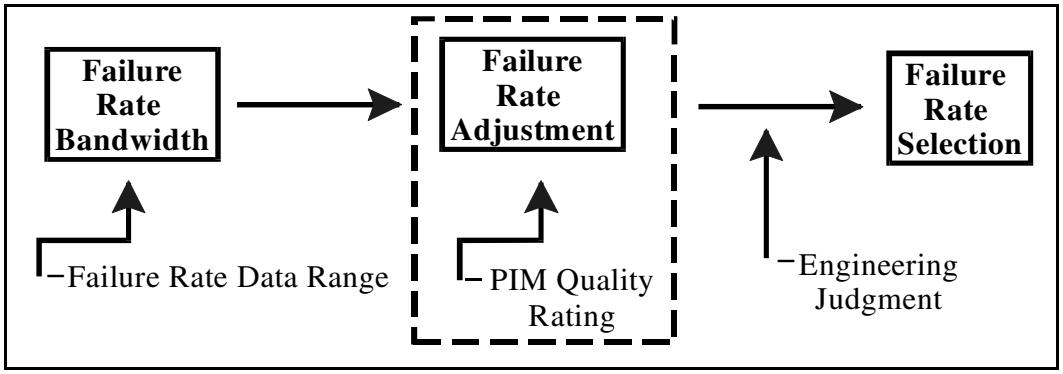


There are three basic methods for selecting equipment, component, and system failure rates for OPR evaluation:

1. Select the mean value.
2. Use engineering judgement and expert opinion to select a failure rate value within the bandwidth based on experience, plant specific knowledge, and subjective opinion.
3. Use a PIM quality grading approach to support the selection of failure rates and failure probabilities.

Method 3, which actually combines the first two methods and is intended to provide a less subjective and "consistent" approach towards failure rate selection, will be discussed in this section. Figure 6.47 presents a general illustration of the process.

Fig. 6.47: Failure Rate Adjustment via PIM Quality Rating



PIMs provide a set of descriptive measures that in turn provide qualitative and semi-quantitative grades of the quality of FPS reliability. The term primary is intended to indicate that the described set of measures account for greater than 95% of the expected reliability performance level.

Table 6.11 provides an example data sheet to qualitatively evaluate PIMs. As listed in this table, some primary evaluation measures include:

- Design standards
- Life cycle (age)
- Management of change (MOC) program
- Inspection and maintenance programs
- Proof testing program
- Operating environment (vibration, dust, corrosive, etc.)
- Physical damage exposure (i.e., mechanical damage from equipment, vehicles)
- Redundancy features
- Diagnostics (fault-detection capabilities)
- CCFs potentials

At the top of Table 6.11, the FPS system is described and the primary subsystems are listed. The following provides an overview of these performance measures.

Table 6.11 Example Data Sheet for Evaluating Performance Integrity Measures (PIMs)

SYSTEM: Automatic Heat Detection System 001, located over process KLM in Building XYZ.							Review By: Date:
PIM No.	Integrity Measures	SUBSYSTEMS					
		Detection Devices	Signaling Circuits/ Control Loop Wiring	Control Panel	Alarms	Power Supply	REMARKS
PIM-1	General Design Standards						
PIM-2	Life-Cycle (Age)						
PIM-3	Management of Change (MOC) Program						
PIM-4	Inspection & Maintenance Programs						
PIM-5	Proof Testing Program						
PIM-6	Operating Environment (Vibration, Corrosion)						
PIM-7	Redundancy Features						
PIM-8	Diagnostics (Fault-Detection Capabilities)						
PIM-9	Other (i.e., physical damage exposure)						

General Design Standards

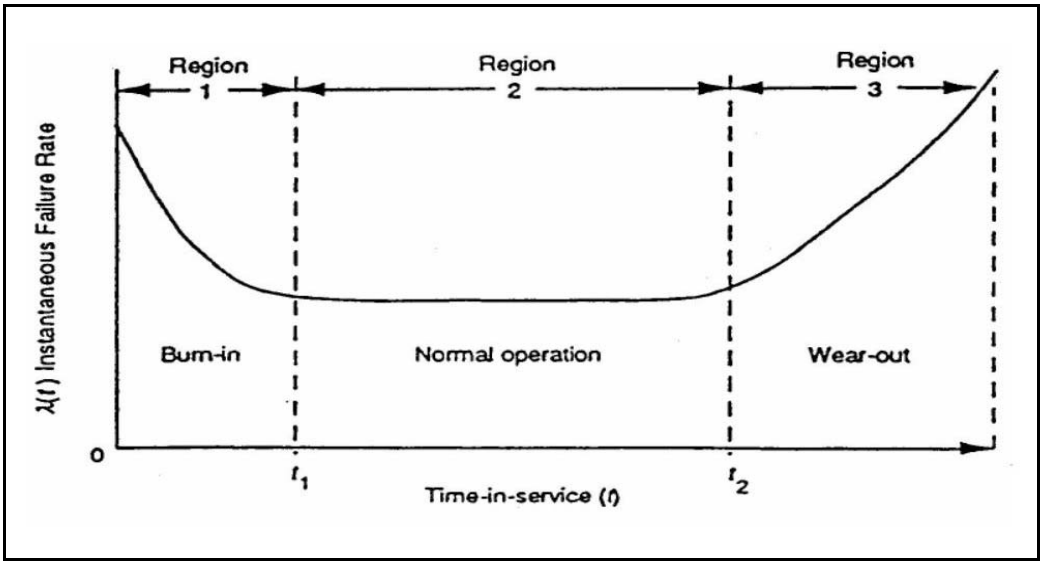
Most codes, standards, and industry guidelines are based on loss experience and are updated periodically to reflect failure experience and new technology. When using a generic failure rate data base, the years the data were compiled and the design standards applied during that time should be recognized. In general, the selection of a failure rate for a system or equipment designed to newer or current design standards should have a failure around the mean value or below. If the system or equipment under evaluation has an older design in comparison with the failure rate data compiled, the failure rate may be above the mean value.

Life-Cycle (Age)

Some failure rate data base sources only provide a mean failure rate or an average failure rate. This failure rate estimation, which is the exponential distribution or the negative exponential distribution, is characterized by its dependency on a single, independent variable, $\lambda(t)$, the failure rate under normal operation. In this approach, $\lambda(t)$ is assumed constant over time.

If the failure rate (i.e., failures per unit time) of a component does not change with the component's age, then the probability of component failure depends only on the time interval of interest. However, most components have a higher rate of failure when new and when approaching the end of their normal useful life span as shown in Fig. 6.48. The higher rate when new (region 1) can be related to fabrication, assembly, installation defects, or lack of acceptance testing. Components do not have infinite lifetimes and, at some point, wear out due to normal causes. This leads to the increase in failure rate as the component wears out (region 3). The quality of acceptance testing will minimize the potential higher failure rate during the initial stages of equipment installation. The quality of the maintenance, repair, and replacement program will modify the failure potential denoted as the "wear-out" region in Fig. 6.48.

Fig. 6.48: Equipment Failure Rate Bathtub Curve



Management of Change (MOC) Program

Modifications to FPSs over the life cycle need to be documented in a MOC program as changes and improvements will have an impact on the failure rate estimation. A written procedure should be in place to initiate, document, and review the change.

The MOC program should reflect modification:

- To the original design
- To inspection, maintenance, testing (IMT) procedures
- Based on new or amended design standards
- To fix control system software errors
- To correct systematic failures identified during testing
- As a result of experiencing a failure rate higher than desired

Inspection and Maintenance Programs

The quality of the inspection and maintenance program will have a major impact on the failure rate. It is important to note that many failures occur following maintenance operations. For example, the following general information has been reported on maintenance-induced failures:

- Air Force
  - 40% of failures are induced by previous maintenance (complex weapon systems)
- North American Electric Reliability Council
  - Approximately 50% of forced outages occur within three months of a planned maintenance outage or overhaul
- Chemical-Petrochemical Industry
  - Approximately 25 – 35% of process equipment failures involve maintenance induced errors.

It is important to recognize the potential for maintenance induced errors for FPSs. Only certified personnel should be allowed to work on complex FPSs, and proof testing to verify system restoration and operation should be conducted following maintenance functions.

Proof Testing

OPR is impacted by the frequency of proof testing as well as by the failure rate of the device itself. For FPSs, documenting the required test interval and test procedure associated with a required reliability and performance level is critical. The test procedure must prove the correct functioning of all parts of the FPS (i.e., input devices → control unit → output functions).

Proof testing is particularly important for detecting hidden failures, those that may not be revealed during normal operations.

Developing an FPS testing program should involve:

1. An understanding of which components are critical to meet OPR requirements. For critical components, an optimum proof testing interval should be established, and in some cases, redundancy should be considered. A critical spare parts program should be maintained, and a documented replacement program (i.e., based on critical component useful life) should be established.
2. An understanding of which components are not critical and where high frequency testing, redundancy, and maintaining a spares inventory provide no real risk reduction benefit.
3. Documented IMT procedures. The procedures should also list the qualifications and certifications needed by the people doing the testing.
4. Optimized test intervals based on the required OPR, plant experience, and manufacturer's experience and recommendations.
5. Monitoring and auditing of IMT programs to ensure that procedures and quality controls are being implemented. When plants downsize, FPS IMT programs are usually affected.

Recalling the discussion on the constant failure rate (λ) assumption, the failure probability (P_F) can be modeled as a function of the exposure interval (t) by the exponential formula:

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

$$\text{Reliability } (R) = 1\text{-}P_F$$

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

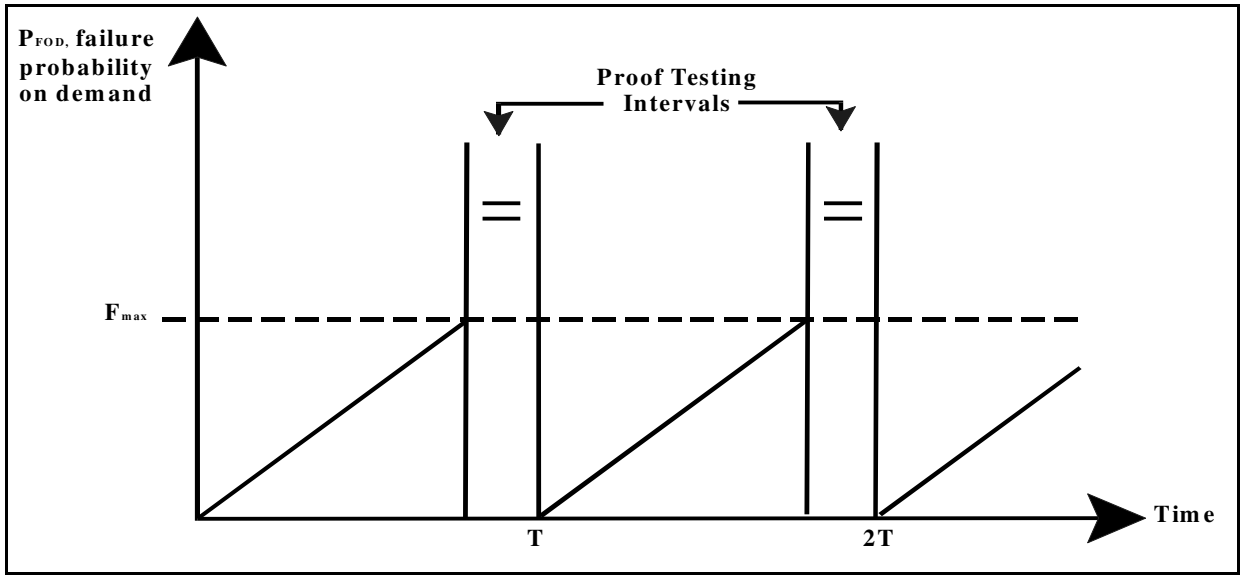
Table 6.12 provides an example of reliability levels versus failure rate and proof testing intervals for three cases. In case 1, even though monthly proof testing is done, the reliability is relatively low because of the high failure rate potential. Case 3 provides the highest reliability.

Table 6.12: Example of Reliability Levels Versus Failure Rate and Proof Testing

MTBF (hours)	ANNUALIZED FAILURE RATE: $\lambda = \frac{1}{\text{MTBF}}$	PROOF TESTING INTERVAL	TIME BETWEEN TESTS (t)	RELIABILITY (R) $R = e^{-\lambda t}$
Case 1: 2,000	λ = 0.0005 failures/hr or for 8,760 operating hours per year = 4.38 failures/yr	Tested every month, 12 tests per year	0.08 (1/12)	R = 0.70
Case 2: 45,000	λ = 0.000022 failures/hr or for 8.760 operating hour per year = 0.19 failures/yr (i.e., on the average, approx. 1 failure every 5 years)	Tested every 12 months, 1 test per year	1.00 (12/12)	R = 0.82
Case 3: 175,000	$\lambda = 5.7 \times 10^{-6}$ failures/hr or for 8.760 operating hours per year = 0.05 failures/yr (i.e., on the average, approx. 1 failure every 20 years)	Tested every 12 months, 1 test per year	1.00 (12/12)	R = 0.95

An FPS system or sub-system fault is termed hidden or *unrevealed* if that fault is not apparent unless the system is called upon to operate during an emergency or fails during proof testing. When the system is given a proof test, P_{FOD} may be taken to have been restored to zero, (i.e., $P_{FOD} = 0$). Hence, if there is a maximum permissible failure probability (F_{max}), we can specify the interval between tests *T* such that P_{FOD} does not exceed F_{max}. [11]

Fig. 6.49: Example – FPS System Failure Probability With Proof Testing (T)

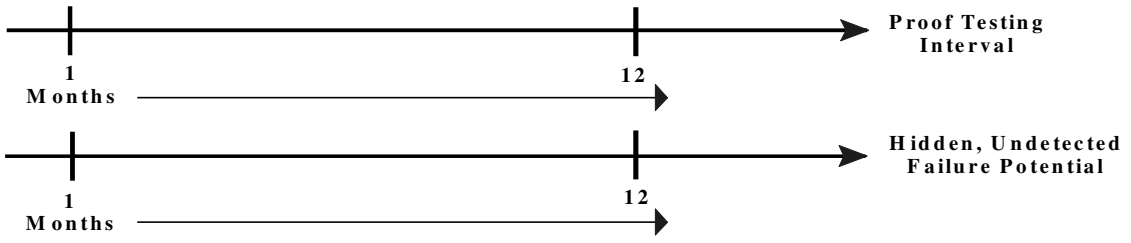


Calculation of failure to operate on-demand probability (P_{FOD}) involves computing the mean, or average, probability of failure for FPS subsystems or primary components whose failures would go undetected until tested or relied upon to function on-demand during an emergency. The average probability for component failure to operate on-demand can be calculated from the following equation:[11]

$$P_D = \frac{\lambda T}{2}$$

where λ is the failure rate in units of failures per hour and T is the system/subsystem/component test interval in hours.

For example, for a fire suppression system under emergency demand, the control valves could fail in the closed position. This failure would not be detected until the control valves were required to operate in the event of a fire or during an annual test.[11]



As an example, in Table 6.12, case 3 has an annual failure probability of 0.05 failures/year based on one proof test per year. If testing was increased to every six months or twice a year, then the failure probability (P_{FOD}) would be:

$$P_{FOD} = \frac{0.05}{2} = \frac{0.025 \text{ failures}}{\text{year}}$$

$$\text{Reliability} = 1.0 - P_{FOD}$$

$$= 1.0 - 0.025 = 0.975$$

With this evaluation of proof testing intervals, the overall risk reduction impact of increasing reliability from 0.95 to 0.975 versus the additional testing costs would have to be examined.

Operating Environment

The external environment to the system or equipment may have the potential of producing a failure. The environment may involve corrosion (i.e., corroded sprinkler heads) or vibration (vibration induced failure of detection devices, control panels, etc.), which can reduce reliability over the life of the equipment under evaluation.

The operating environment is very much related to CCF potential and should be examined for existing systems and proposed new designs.

Redundancy

System, subsystem, and equipment component redundancy will affect the estimation of the probability of failure-on-demand. Backup power supplies are a good example. Redundancy is addressed in Sect. 6.6.

Diagnostics (Fault Detection Capability)

Many FPSs have on-line diagnostic fault detection and self-testing capabilities. These can include supervision of system control valves, loss of primary power for detection and alarm systems, etc. Actuation of such supervisory (i.e., trouble alarms) fault detection systems provides a method of identifying faults that are fail-safe-detected or fail-dangerous-detected prior to having a hidden failure during an emergency fire situation. It is important to examine the design integrity and reliability aspects of these systems.

Performance Integrity Measure (PIM) Quality Scoring

Table 6.13 provides an example of a PIM quality grading sheet. The first column in Table 6.1.3 lists relevant PIMs and PIM Indicators. Indicators are graded A to F:

Grading: A = 4 – very high quality program
B = 3
C = 2
D = 1 – very low quality program
F = 0 – no program

The fire protection subsystems are graded based on engineering review and evaluation. The Importance (IMP, a type of weighting) is assigned to each PIM for the subsystem being evaluated. The importance in example Table 6.13 is based on:

IMP: 5 = very important
4
3
2
1 = very minor importance

Importance

Importance is a measure of the contributing influence of the performance indicators or potential operational failure contribution based on experience and historical data (plant specific, industry specific, or generic data). Importance supporting data and information usually come from:

- Historical data – reported failures
- Experience/judgement

For example:

Subsystem X1: Based on 70 reported failures, the relative influence of the contributing factors in terms of percentage (%) may look like this:

No	General Type	Relative %
10	Improper Design	14
5	Excessive Vibration	8
15	Electrical Malfunctions	21
10	Errors Following Maintenance	14
10	Aging/Corrosion problems	14
15	Lack of Inspection /Proof Testing	21
5	Misc. — Spurious Failures	8
70	Failures	100

Table 6.13: Example PIM Quality Grading Sheet

SYSTEM:		Heat Detection System 001, located over process KLM in Building XYZ				
Performance Integrity Measures (PIM)		SUBSYSTEMS: PIM INDICATORS	Detection Devices Grade / IMP	Control Unit Grade / IMP	Evacuation Alarms Grade / IMP	Power Supply Grade / IMP
PIM-1 General Design Standards	A	Designed per NFPA 72, Current Edition	A / 5	B / 5	A / 5	B / 5
	B	Designed per NFPA 72, Older Edition				
	C	Minor deviations from NFPA 72				
	D	Major deviations from NFPA 72				
	F	Not designed per NFPA 72				
PIM-2 Life-Cycle (Age)	A	Newer Equipment, formally acceptance tested	A / 5	A / 5	A / 5	A / 5
	B	Newer, Not formally accepted tested				
	C	At or slightly below ½ useful life				
	D	Above ½ useful life				
	F	At end of useful life				
PIM-3 Management of Change Program	A	Very Good Program	A / 4	A / 4	A / 4	A / 4
	B	Above Average, Good Program				
	C	Average, Minimal Program				
	D	Below Average, Poor Program				
	F	No Program				
PIM-4 Inspection/ Maintenance Programs	A	Very Good Program	C / 5	C / 5	C / 5	C / 5
	B	Above Average, Good Program				
	C	Average, Minimal Program				
	D	Below Average, Poor Program				
	F	No Program				
PIM-5 Proof Testing Program	A	Very Good Program	C / 5	C / 5	C / 5	C / 5
	B	Above Average, Good Program				
	C	Average, Minimal Program				
	D	Below Average, Poor Program				
	F	No Program				
PIM-6 External Environment (i.e., vibration)	A	No Vibration	A / 4	A / 4	A / 4	A / 4
	B	Negligible Vibration				
	C	Minor Vibration				
	D	Major Vibration				
	F	Excessive Vibration				
PIM-7 External Environment (i.e., corrosion)	A	No Corrosion	A / 3	A / 3	A / 3	A / 3
	B	Negligible Corrosion				
	C	Minor Corrosion				
	D	Major Corrosion				
	F	Excessive Corrosion				

Table 6.13: Example PIM Quality Grading Sheet, Cont.

SYSTEM: Heat Detection System 001, located over process KLM in Building XYZ

Performance Integrity Measures (PIMs)	SUBSYSTEMS: PIM INDICATORS	Detection Devices Grade / IMP	Control Unit Grade / IMP	Evacuation Alarms Grade / IMP	Power Supply Grade / IMP
PIM-8 Redundancy	A Very Reliable Redundancy B C ↓ D F No Redundancy	A / 5	B / 5	A / 5	B / 5
PIM-9 Diagnostics (Fault Detection)	A Very Good Diagnostics B C ↓ D F No Diagnostics	B / 5	C / 5	C / 5	C / 5
PIM Quality Ratings	* Quality Grade Point Average (GPA) →	3.39	3.15	3.27	3.02

Grading
A = 4
B = 3
C = 2
D = 1
F = 0

IMP = Importance
5 = Very Important
4 =
3 = ↓
2 =
1 = Very Minor

* Quality Grade Point Average (GPA) = $\sum_{PIMs}$ Grade X IMP / $\sum_{PIMs}$ IMP

Importance factors can be obtained from incident data. Incident data bases sometimes provide a relative (%) breakdown of fire and explosion cause and contributing loss factors, including factors contributing to the failure of the FPS. These relative breakdowns provide an importance or weighting for what are the significant performance integrity factors and input for engineering judgements and expert opinion.

Sources for past fire and explosion (F&E) loss incident data include:

- Fire protection and safety associations
- Industry associations
- Government agencies
- Research organizations
- Insurance companies
- Journals/technical papers
- Risk assessment reports

Fire incident data from such sources as the National Fire Protection Association (NFPA) and American Petroleum Institute (API) provide fire loss incident data for a number of processes, plants, and equipment. Federal and state agencies, such as the Department of Transportation (DOT) also collect a wide variety of accident data. A listing of incident data sources is provided in Chap.4.

Table 6.14 provides a relative breakdown of unsatisfactory sprinkler performance compiled by NFPA based on historical incident data.

Table 6.14: Groups of Leading Reasons for Unsatisfactory Sprinkler Performance

PROBLEM GROUP	PERCENTAGE OF CASES	PROBLEM	PERCENTAGE OF CASES
A. Failure to maintain operational status of system	53.4	A1. Water shut off A2 Inadequate maintenance A3. Obstruction to water distribution A4. System frozen	35.4 8.4 8.2 1.4
B. Failure to assure adequacy of system for complete coverage of current hazard	21.6	B.1 System not adequate for level of hazard in occupancy B2. System designed for partial protection only	13.5 8.1
C. Defects affecting but not involving sprinkler system	15.9	C1. Inadequate water supply C2. Faulty building construction	9.9 6.0
D. Inadequate performance by sprinkler system itself	5.6	D1. Antiquated system D2. Slow operation of sprinklers D3. Defective dry-pipe valve	2.1 1.8 1.7
E. Other	3.6	E1. Exposure fire E2. Other or unknown	1.7 1.9
Total	100.0		100.0

Source: "Automatic Sprinkler Performance Tables, 1970 Edition," *Fire Journal,* July 1970, page 37. Based on 3,134 fires reported to NFPA during 1925 to 1969 for which sprinkler performance was deemed unsatisfactory. Of these, 75.0% were in industrial facilities, 12.0% were in storage facilities, 5.6% were in stores, and 7.4% were in all other properties.

The Grade Point Average (GPA)

The GPA for each FPS subsystem is calculated by:

$$\sum_{\text{PIMs } 1 \rightarrow 7} \text{Grade} \times \text{IMP} \;/\; \sum \text{IMP}$$

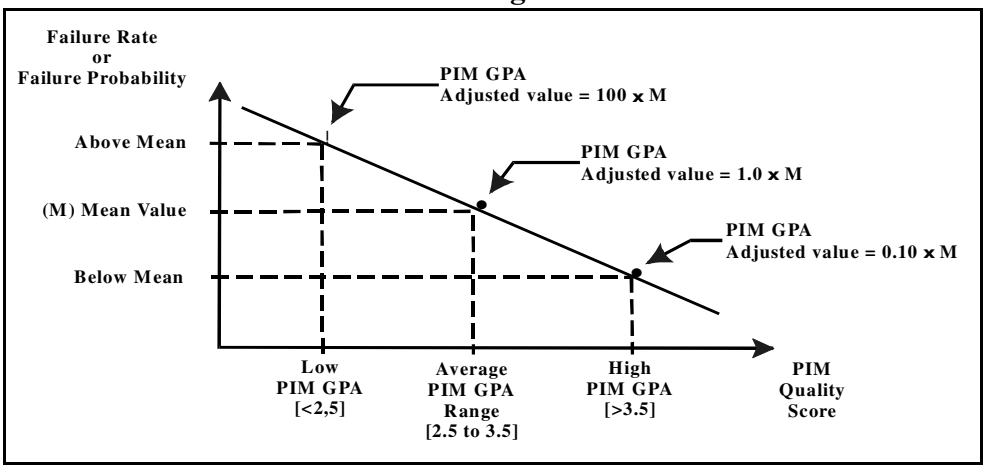
For example, the GPA for the subsystem "Detection Devices" in Table 6.13 would be computed as follows:

	Grade x (times) Importance	**Importance (IMP) Rating**
PIM – 1	20	5
PIM – 2	20	5
PIM – 3	16	4
PIM – 4	10	5
PIM – 5	10	5
PIM – 6	16	4
PIM – 7	12	3
PIM – 8	20	5
PIM – 9	15	5
Totals	139	41

GPA = 139/41 = 3.39

Figure 6.50 provides a general illustration of establishing a relationship between the PIM GPA and a failure data bandwidth.

Fig. 6.50: PIM GPA Versus Failure Data Range



The concept behind developing a relationship as shown in Fig. 6.50 is described in Chap. 4.

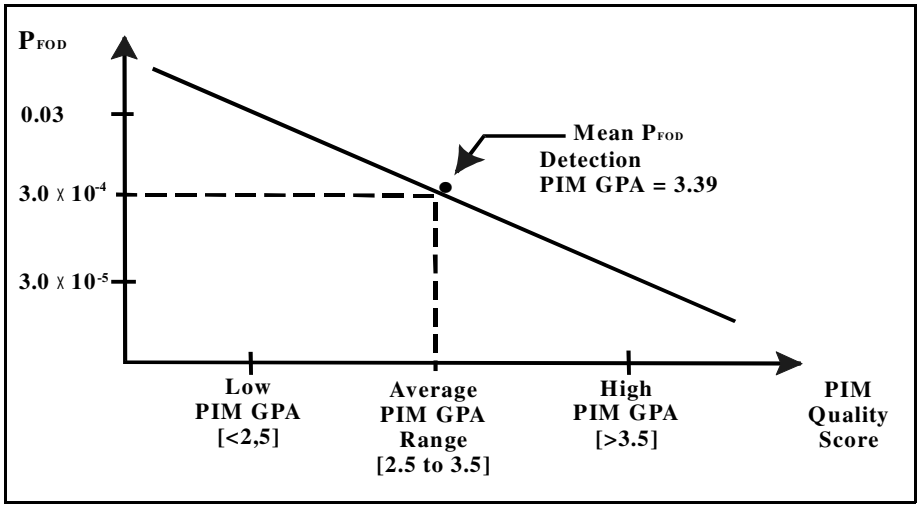
As an example, the first row in Table 6.15 lists some generic failure data, which we will assume are for a fire detection device.

Table 6.15: Example Generic Failure Data for a Fire Detection Device

FAILURE DATA RANGE	LOWER	MEAN (M)	UPPER	REMARKS
Generic Failure Rates	—	0.30 per 1,000 demands	—	Assumes only mean failure rate value is available
P_{FOD} Probability of Failure On-Demand	—	3.0×10^{-4}	—	
P_{FOD} with Adjustment Limits	(M x 0.10) 3.0×10^{-5}	(M x 1.0) 3.0×10^{-4}	(M x 100) 0.03	

From Table 6.15 the mean P_{FOD} for a single detector device is 3.0×10^{-4} failures/demand. Since in our example the detection PIM GPA was estimated at 3.39, we would select the mean P_{FOD} value in our evaluation as shown in Fig. 6.51.

Fig. 6.51: Detection PIM GPA Versus P_{FOD} Selection



The use of this type of PIM GPA quality scoring model provides the following advantages:

1. Forces identification and evaluation of PIMs that will affect the failure rate or failure probability. Remember, we want to identify weak links so that improvements can be evaluated in terms of risk reduction benefit versus cost.
2. Provides a systematic and consistent support tool for engineering judgement and a level of technical justification for modifying generic failure data based on plant specific knowledge.

3. The PIM GPA evaluation format is relatively easy to set up in a spreadsheet, and the method can be expanded for increased rigor and sophistication in the evaluation.

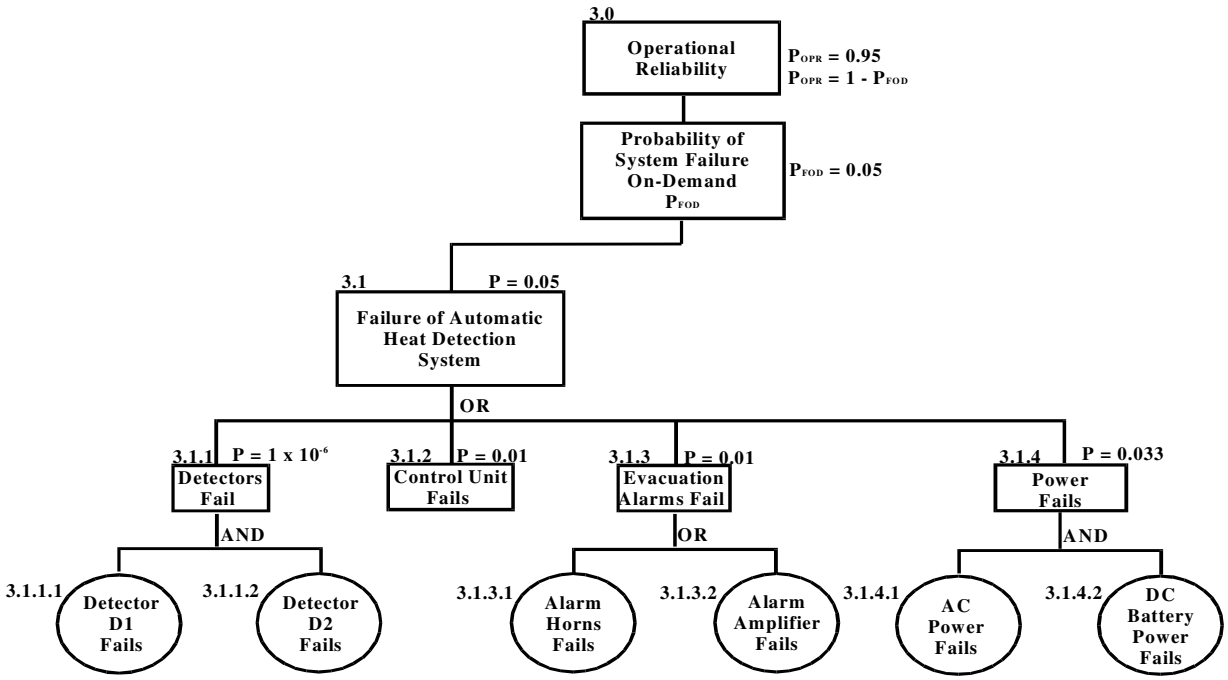
Failure rate data presented in most generic data bases are based on failure data from a variety of operating environments, and the actual operating and environmental conditions (such as temperature, humidity, and mechanical stress) may not be listed or described as part of the data base. If we are interested in the reliability of systems or equipment components that are expected to operate in a particular plant specific environment, we may need to multiply the generic failure rate data by an adjustment factor. The failure rate adjustment factors may be estimated through methods such as the PIM GPA Quality Scoring Method presented here.

Some data bases suggest their own adjustment factors. The *IEEE Guide* (Institute of Electrical and Electronics Engineers) provides environmental factors (correction factors) for some electrical and electronic components. For example, it is recommended there that failure rates for electric valve operators and actuators be multiplied by a factor of 1.57 if the environmental temperature is very high; a factor of 2.04 is recommended if the humidity is very high.[9]

In some cases, engineering judgement and expert opinion will be needed to adjust failure data with large failure rate bandwidths, however, it is unwise to rely on a single expert (for example, a knowledgeable engineer, operator, or maintenance-test person); seek the opinion of at least a few experts. The experts' estimates of failure data modification can be averaged or weighted-averaged.

It is important to document the method used to adjust generic failure data. Figure 6.52 provides an example of a probability data table for a first-order operational reliability (OPR) fault tree evaluation of a heat detection system. In this table, the mean failure data adjustment factor is shown. Evident in Fig. 6.52 is that the power supply reliability is the weak link based on the adjustment factor. Although not added in Fig. 6.52 because of space limitations, the data reference(s) and data adjustment methods would be added to this type of table.

Fig. 6.52: OPR Example, Heat Detection System



Probability Data Table

DESCRIPTION			MEAN FAILURE DATA*	ADJUSTMENT FACTOR	ADJUSTED FAILURE PROBABILITY
I.D.	ITEM	MODE OF FAILURE			
3.1.1.1	Detector D1	Fails to transmit a signal on emergency demand	0.001 (1)	x 1	0.001
3.1.1.2	Detector D2	Fails to transmit a signal on emergency demand	0.001 (1)	x 1	0.001
3.1.2	Control unit and associated signaling wiring	Fail to recognize and respond to detection input signal	0.01 (2)	x 1	0.01
3.1.3.1	Alarm horns	Fail to operate	0.001 (1)	x 1	0.001
3.1.3.2	Alarm amplifier	Fail to operate	0.01 (2)	x 1	0.01
3.1.4.1	AC power	AC power to system fails	0.33 (2)	x 1	0.33
3.1.4.2	DC battery	DC battery backup to system fails	0.001 (1)	x 100	0.10

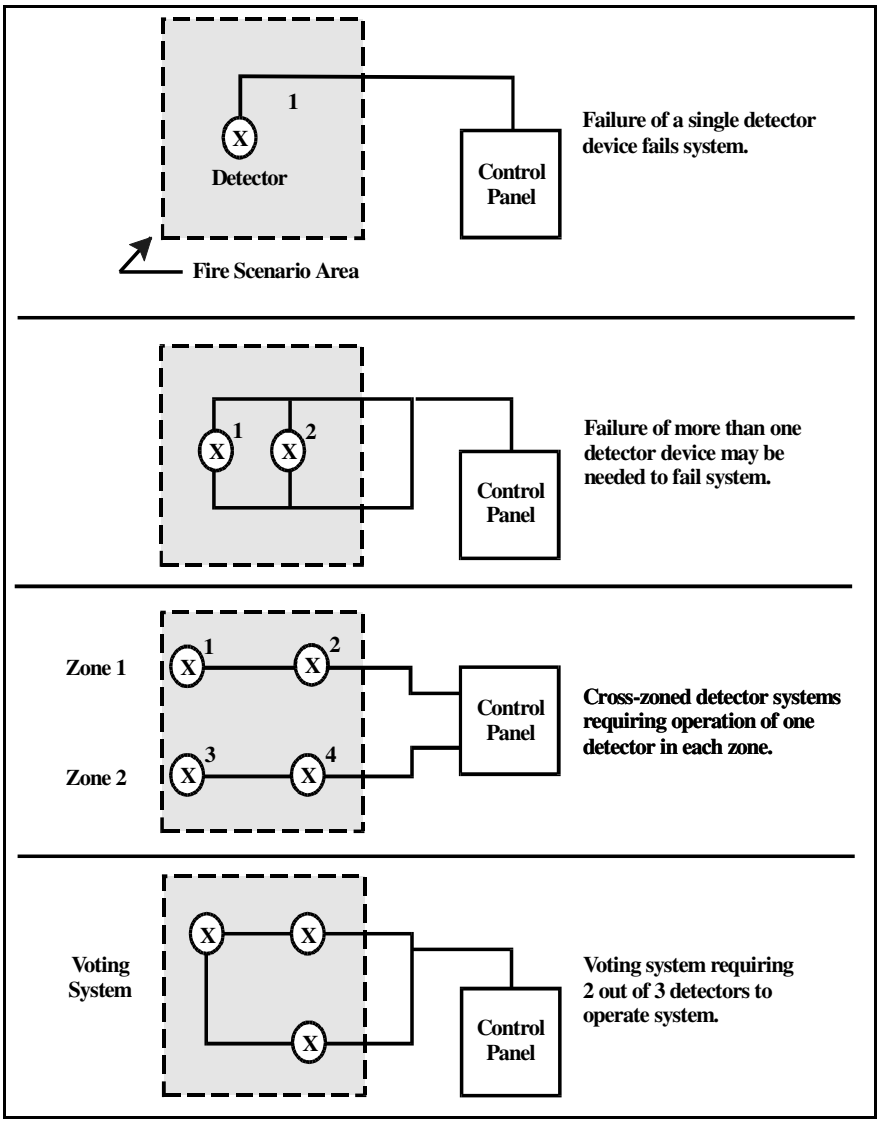
* (1) Demand-related failure
(2) Time-related failure – failures per 8,760 hr per year

Note: Data are not actual failure rate data — added for example purposes only.

Another item to note in Fig. 6.52 is that it takes two detectors (D1 and D2) to fail. Based on the operational requirements, the number of component failures must be identified. For example, with detection systems, it is important to identify the detection device failure modes (see Fig. 6.53) and recognize which modes of failure affect the functional performance requirements:

- Failure of a single detection device
- Failure of more than one detection device
- Failure within a "cross-zoned" detection system
- Failure within a "voting" or "addressable" detection system

Fig. 6.53: Some Detection Performance Considerations



6.5.3 Failure Data Sources

In the probability documentation tables, the failure data sources used in the evaluation should be listed. Remarks might include what failure rate adjustment method if applicable, was used. Some primary failure data sources are listed in Table 6.16.

Table 6.16: Some Failure Data Sources

DATA TYPE	DATA SOURCE
Plant specific	• Plant records • Plant walkdowns and interviews
Equipment manufacturers	• Equipment components – mean time between failure (MTBF) data • System level reliability data
Relative failure incident	• Industry associations • Insurance companies
Published failure rate	• Industry specific data • Generic failure rate data
Human error	• Plant records • Generic human reliability data
External event	• Plant data • Natural event data bases
Judgmental	• Internal expert opinion

As a starting point, the availability of potential data sources can be identified in a table, similar to example Table 6.17.

Plant Specific Data

Plant data are the best data to compile and apply because they are specific to the process, environment, and IMT practices. Drawbacks of this approach are that sufficient plant specific historical (operational) data may not be available. Available data may not pertain to a specific system but to subsystems or components of different manufacture, design, size, and ratings.

If sufficient operational history pertaining to a particular system or subsystem is available, it may provide accurate estimates of reliability. However, in many situations, the available data may be very limited, and the estimation of reliability from such a limited amount of data may be accurate in an order-of-magnitude sense only.

Table 6.17: Example – Identifying Data Source(s) – Fire Protection Water Supply

FAILURES	PLANT RECORDS	EQUIPMENT MANUFACTURERS' DATA	PUBLISHED FAILURE RATE DATA	OTHER
• Tank failure	X			Design review, engineering judgement
• Level indicators	X	X	X	
• Pressure sensors (i.e., pump cut-in)	X	X	X	
• Controllers (i.e., pump controllers)	X	X	X	
• Trouble/supervision alarms (i.e., relays)	X		X	
• Pump failures	X	X	X	
• Electrical feed failures	X			Design review, engineering judgement
• Control valves	X		X	
• Check valves	X		X	
• Piping (tees/connections)	X		X	

The advantages of gathering plant specific data are that they reflects the plant's historical loss profile based on specific:

- Design factors
- IMT programs
- Operating procedures
- Management loss control programs

The realities of collecting plant specific data include:

- Many failures and near-loss incidents are not recorded
- Raw data in maintenance and operation log's may be incomplete and are usually not in a form readily usable for failure and reliability analysis
- The population or operating time of a facility, process, or equipment may be limited and thus not reflect the long term failure potential

Methods that can be applied to compile plant specific information include:

- Conducting structured interviews with plant personnel with experience in the operations and maintenance of the specific facility or operation being evaluated to categorize the potential likelihood of events based on historical experience
- Compiling raw plant site data into a data base format
- Conducting an audit of the plant's management loss control programs; resulting information can be used as input and support for modifying historical failures based on present plant practices

Performing plant site interviews to gather data is discussed in Chap. 4, Initiating Event Likelihood.

Equipment Manufacturers' Data

FPS equipment failure rate data provided by equipment manufacturers in a useable form is rare. From my experience in contacting equipment manufacturers to obtain this type of information, I have usually encountered three levels of response:

1. If you talk with the right person concerning system failures, you can obtain qualitative insights into potential failure modes, built-in reliability features, experience concerning major failure contributing factors, and usually a few good service department lessons. This is good starting information. Remember you will need to talk to someone in the engineering or technical service departments, not a salesman.
2. Mean time between failure (MTBF) data may be available for some equipment components, usually electronic components such as instrumentation, valve actuators, controllers, power supply components. However, recognize that in most cases these are data from tests run under very controlled conditions. The MTBF for a component installed in a corrosive chemical environment may turn out to be quite different from the MTBF data under controlled laboratory conditions. Therefore, it is important to recognize how the MTBF data were developed: from simulated field conditions, from actual field installations, or from very controlled laboratory conditions.
3. Some manufacturers may be willing to provide an estimate of FPS equipment MTBF based on service repair records. For example, one manufacturer of diesel-driven fire pumps provided an estimate of an average MTBF of 15,200 hr. This was based on a population of approximately 1700 diesel fire pumps over a 5-year period. A diesel fire pump system primarily consists of the pump, the diesel engine driver, the fuel system, and the controller. The MTBF data compiled by the manufacturer's or vendor's service departments were primarily for major failures and repairs concerning the diesel engine only and did not include failures and repairs made by the plant. Again, it is important to research and recognize MTBF data boundaries, assumptions, and limitations.

Published Failure Rate Data

Probabilistic failure data are preferably extracted from plant specific data sources, which are the best source of data, and can be obtained from operational and maintenance logs and records and from interviews conducted with experienced plant personnel. Engineering judgments can be based on plant surveys, available data, interviews, and experience and should preferably be made by risk evaluation team consensus. Published failure rate data sources of interest include the following:

- Center for Chemical Process Safety (CCPS), *Guidelines for Process Equipment Reliability Data* (with data tables), AIChE, New York, 1989. Provides data on process related equipment.
- IEEE Standard 500, "Equipment Reliability Data for Nuclear-Power Generating Stations." Provides failure data for a variety of electrical and electronic computers.
- OREDA, *Offshore Reliability Data Handbook, Second Edition*. Published by the OREDA participants, Norway, 1992. Detailed information on equipment found on offshore platforms.
- "Nonelectric Parts Reliability" (NPRD-91), Reliability Analysis Center, 1991. Contains information of failure rates for valves, instruments, pumps, hardware, etc.

A listing of some additional published failure rate data sources is provided in Chap. 4.

Some important issues to note when using generic failure data:

- Published generic failure rate data are derived from:
  - Equipment of many manufacturers,
  - A number of processes,
  - Plants with various environments,
  - Various maintenance/testing policies, and
  - Various operating strategies.
- Such data generally span 1 – 3 orders of magnitude with a mean value provided.
- The user should apply a credible consistent method of adjusting data (i.e., use of performance integrity measures as previously discussed).

Published failure rate data are usually provided in the form of reliability data tables such as the one presented in Fig. 6.54. Reliability data tables will vary in content and level of detail but will typically include:[7]

- A breakdown of failure modes
- Failure rate mean values, either time-related or demand-related
- Equipment boundaries
- A listing of data reference sources used to develop the table

As with any failure or reliability data, it is very important to understand the sources of data (see bottom of Fig. 6.54 – data reference no.) used to compile the reliability data table. This is necessary to lend credibility to the use of these data in your particular risk study.

Fig. 6.54: Example Reliability Data Table[7]

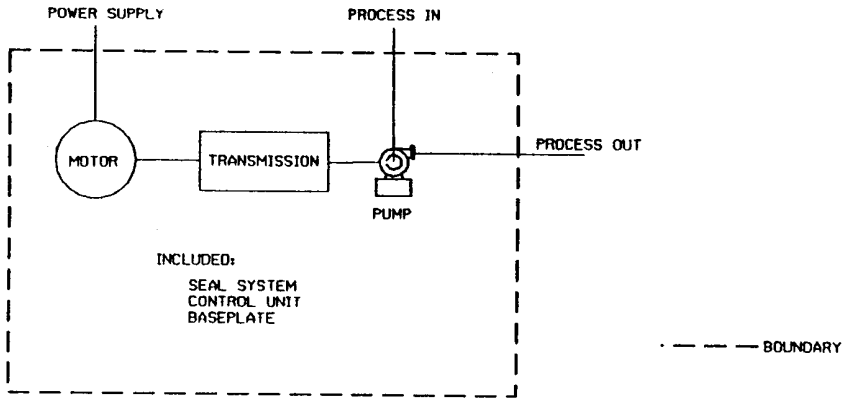
DATA ON SELECTED PROCESS SYSTEMS AND EQUIPMENT

Taxonomy No. 4.2.4.2	**Equipment Description** PROTECTION SYSTEMS-FIRE-FIRE WATER PUMPS-ELECTRIC
Operating Mode	**Process Severity** UNKNOWN

Population	Samples	Aggregated time in service (10^6 hrs)		No. of Demands		
		Calendar time	Operating time			

Failure mode	Failures (per 10^6 hrs)			Failures (per 10^3 demands)		
	Lower	Mean	Upper	Lower	Mean	Upper
CATASTROPHIC a. Fails to Start b. Fails While Running				3.62	42.5	143.0
DEGRADED a. Low Output						
INCIPIENT a. Vibration b. Leakage						

Equipment Boundary



Data Reference No. (Table 5.1): 8

American Institute of Chemical Engineers (AIChE). Center for Chemical Process Safety (CCPS), Guidelines for Process Equipment Reliability Data With Data Tables, New York, NY, 1989.

Copyright 1989 by American Institute of Chemical Engineers, and reproduced by permission of AIChE.

Equipment Boundaries

System failure rate parameters are defined by the equipment boundaries identified in various failure data base reference sources. The system boundaries may include the equipment, related components, utility connections (electric power, cooling water, etc.), or input-output process functions (alarm signal processing, etc.).

Figure 6.54 presents an example of a defined equipment boundary for an electric pump.[7] The associated failure rate data relate only the failure potential of the electric motor drive pump equipment. The failure potential of the electric power supply and the fluid being pumped (denoted as process in-process out), which are critical items, would have to be evaluated to determine the overall system failure potential if relevant to the study.

Failure Mode Definition

It is important for the user to know where the data came from and understand what failure modes are being addressed prior to applying the data in a reliability assessment. Some of the information pertaining to Fig. 6.55, which is an example data sheet from the CCPS reference, Guidelines for Process Equipment Reliability Data,[7] includes:

- The detector is a flame detector
- The data come from a single source – the liquefied natural gas (LNG) industry
- The majority of reported failures were false (spurious) operation of UV type detectors reported as time-related failures. There were very few failures during emergency demand or proof testing.
  [Note in Fig. 6.55, Under "Catastrophic Failure Mode Grouping," both "Fails to Operate" and "Spurious Operation" are listed.]

Fig. 6.55: Example Reliability Data Table[7]

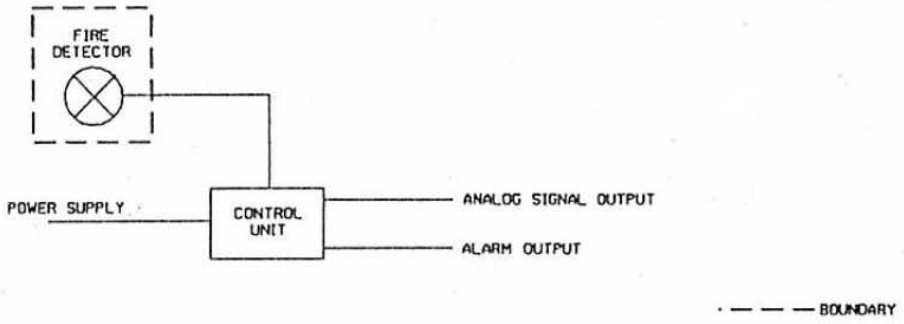
DATA ON SELECTED PROCESS SYSTEMS AND EQUIPMENT

Taxonomy No. 4.2.2	Equipment Description PROTECTION SYSTEMS-FIRE-FIRE DETECTION
Operating Mode	Process Severity UNKNOWN

Population	Samples	Aggregated time in service (10^6 hrs)		No. of Demands
		Calendar time	Operating time	

Failure mode	Failures (per 10^6 hrs)			Failures (per 10^3 demands)		
	Lower	Mean	Upper	Lower	Mean	Upper
CATASTROPHIC a. Fails to Operate b. Spurious Operation c. Plugged d. Leaks Through	0.0198	1.14	4.41			
DEGRADED a. Improper Operation b. Minor Leak Through						
INCIPIENT a. External Leakage b. Faulty Indication						

Equipment Boundary



Data Reference No. (Table 5.1): 1

American Institute of Chemical Engineers (AIChE). Center for Chemical Process Safety (CCPS), Guidelines for Process Equipment Reliability Data With Data Tables, New York, NY, 1989.

Copyright 1989 by American Institute of Chemical Engineers, and reproduced by permission of AIChE.

Tables 6.18 and 6.19 provide some example data from the Electric Power Research Institute report, EPRI NP-4144, *Turbine Generator Fire Protection by Sprinkler System*.[10]

Table 6.18: Some Fire Protection System Failure Rates[10]

TYPE OF SYSTEM	PROBABILITY OF FAILURE TO OPERATE ON-DEMAND[a]	
	NFPA INSPECTION INTERVALS	YEARLY INSPECTION INTERVALS
Manual spray — open head	0.0056	0.0056
Manual spray — closed head	0.0056	0.0056
Automatic sprinkler — wet pipe		
without limit switches on isolation valve[b]	0.00067	0.028
with limit switches on isolation valve[b]	0.00015	0.00092
Automatic water spray — open head		
without limit switches on isolation valve[b]	0.0028	0.03
with limit switches on isolation valve[b]	0.0023	0.0030
Automatic water spray — closed head		
without limit switches on isolation valve[b]	0.0028	0.03
with limit switches on isolation valve[b]	0.0023	0.0030

[a] The reliability of the fire protection water supply was assumed to be 100%. This assumption was made because the water supply is highly reliable and affects all systems equally.

[b] Normally open valves.

Table 6.19: Manual Open Head Water Spray System Failure Data[10]

FAILURE TO OPERATE

FAILURE MODES	PROBABILITY PER DEMAND	
	NFPA INTERVAL[a]	ANNUAL INTERVAL[a]
Normally closed manual spray valve fails closed	2.7×10^{-4}	2.7×10^{-4}
Operator fails to open manual spray valve	0.005	0.005
Fire detector fails to detect fire	0.0003	0.0003
Alarms fail (local and control room)	10^{-8}	1.3×10^{-7}
Spray head clogged	2.4×10^{-7}	2.4×10^{-7}
Total	0.0056	0.0056

INADVERTENT OPERATION[b]

FAILURE MODES	OCCURRENCES PER YEAR	
	NFPA INTERVAL[a]	ANNUAL INTERVAL[a]
Operator inadvertently opens manual spray valve (two exposures/year)	2×10^{-3}	2×10^{-3}
Manual spray valve fails open (stem or weld break, etc.)	9×10^{-5}	9×10^{-5}
Total	2.1×10^{-3}	2.1×10^{-3}

[a] Statistics are given based on test and inspection intervals as specified in the NFPA codes and with only annual tests and inspections.

[b] Assumed that "fire alarm fails on" would not by itself cause operator to turn on water, but that operator would check for fire.

Engineering Judgement

In many cases, historical data must be reviewed, adjusted, and modified using experienced engineering judgements and expert opinion. This leads to the question of the validity of using subjective likelihoods. Many times subjective estimates provide the only source of input. However, likelihood estimates provided by experienced risk evaluation team members, plant operations managers, maintenance personnel, etc., can be more accurate and valid than using external (i.e., nonplant specific) data base sources. The key here is to use a consistent method to generate data and to provide documentation of the method and assumptions used. Chapter 4 discusses methods to combine failure rates from multiple data bases and sources.

6.6 REDUNDANCY AND INADVERTENT OPERATION

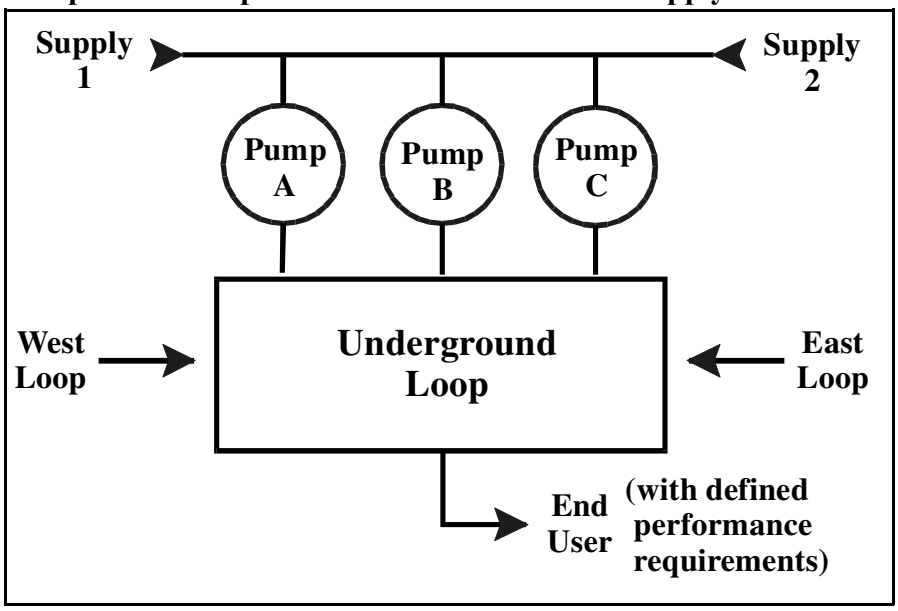
Redundancy can be defined as a measure to reduce the probability of failure or error. Provision of FPS redundancy generally focuses on reducing the probability of equipment failure or reducing the probability of inadvertent (i.e., false) system operation by installing independent secondary or back-up equipment. From a design perspective, these two focuses are not necessarily the same. While the provision of independent back-up systems (e.g., installation of two fire pumps when only one is needed to meet defined performance requirements) will increase the overall system reliability, the provision of dependent equipment or devices (e.g., two detectors needed to activate an emergency shutdown system), while decreasing the probability of inadvertent operation, may also decrease the overall operational reliability.

6.6.1 Redundant or Back-Up Equipment

FPS equipment redundancy affects both availability and reliability evaluations. The following simplified example illustrates this point. Let's assume we have a system similar to that portrayed in Fig. 6.56. Based on our defined performance requirements (e.g., capacity, duration needs) we establish:

1. One water supply is needed.
2. Two out of three pumps are needed.
3. One leg (east or west) of the underground loop is needed.

Fig. 6.56: Simplified Example — Fire Protection Water Supply



For addressing failure logic within the FTA for the water supply and underground loop, "AND" gate logic is applied. This is illustrated in Figs. 6.57 and 6.58.

Fig. 6.57: Fire Protection Water Supply Failure

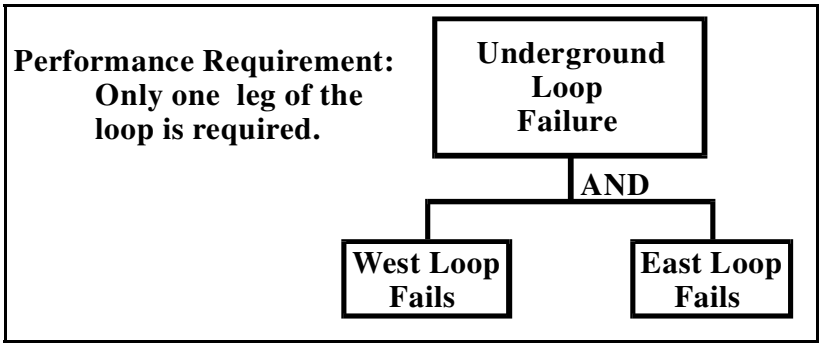
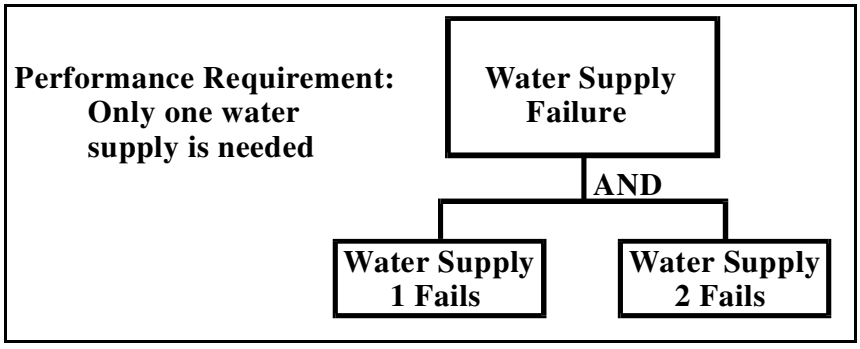
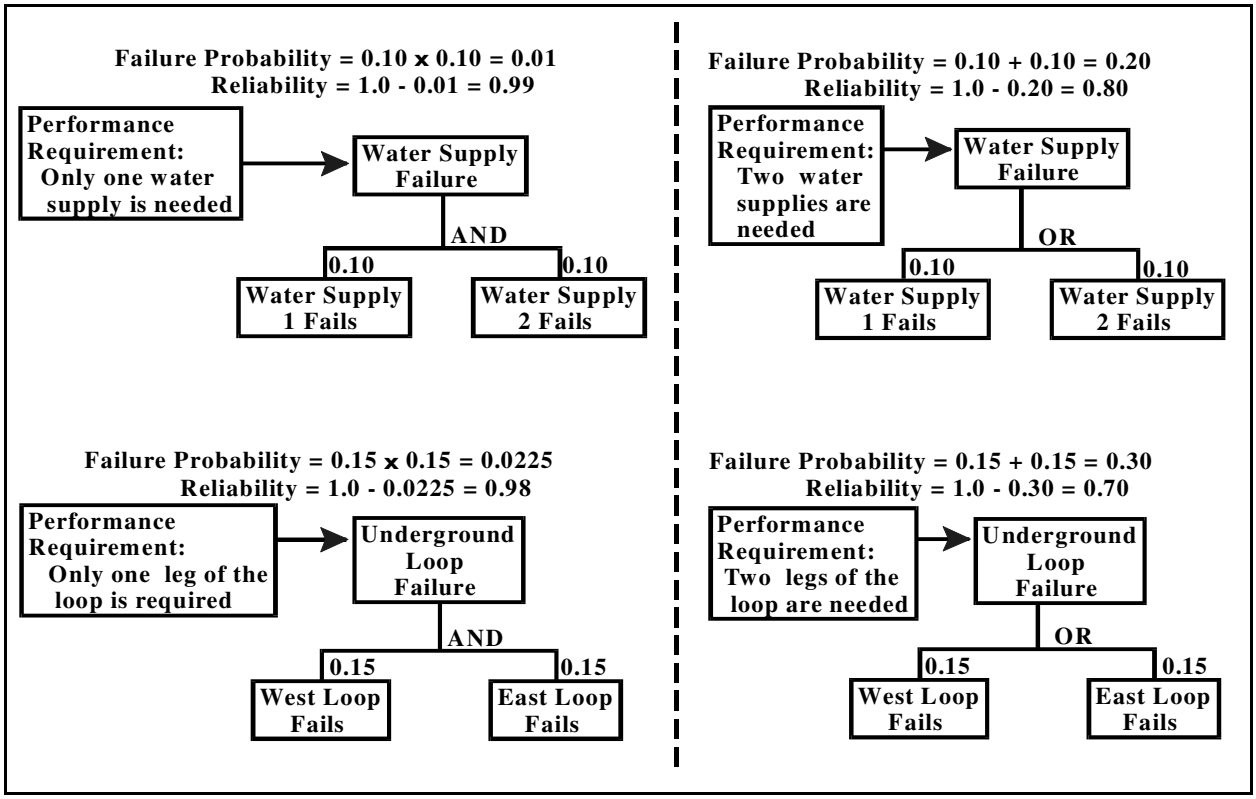


Fig. 6.58: Underground Water Main Loop Failure



If our performance requirements established that both fire protection water supplies and both sides of the underground water main loop are needed, then an "OR" gate would be used in place of the "AND" gate. Figure 6.59 illustrates the differences between defined performance requirements and reliability estimates. In the first column of Fig. 6.59, the performance requirement indicates that only one water supply or leg of the underground water loop is needed. The second column indicates a performance requirement of two water supplies and two legs of the underground loop being needed.

Fig. 6.59: Simplified Example of Performance Requirements Versus Reliability Estimates



As presented in Fig. 6.59, reliability, redundancy and back-up system failure impacts must be addressed via the "defined performance requirements." Based on the example failure probabilities inserted into Fig. 6.59, the following observation can be made:

- For the performance requirement of only one water supply being needed, the reliability is 0.99 as both water supplies (assuming they are equivalent) would have to fail. If both water supplies are needed to meet performance requirements, then the reliability is decreased to 0.80.
- For the performance requirement of only one leg of the underground fire main loop being needed, then both loops (assuming equivalent water flow capabilities) must fail, and the reliability is 0.98. If both legs of the loop are required, then the reliability is reduced to 0.70.

It should again be noted that Fig. 6.56 presents a simplified example, especially as isolation and control valves are not shown. The point of this example is that the defined performance requirements drive the reliability logic structuring used to quantify the overall performance success.

In many fire protection applications, we encounter evaluations that must address multiple failure analysis. Examples include the following: two out of three fire pumps must operate, fire detection cross zoning or voting systems, flame failure combustion safeguards that may require two out of three flame detectors to operate, dual systems where there are local application systems backed up by area wide suppression systems, on-line connected reserves of special extinguishing agents, stand-by or back-up systems that require manual intervention, etc. In our example, Fig. 6.56, if we assume that two out of three fire pumps are needed to meet performance requirements, then this logic must be incorporated into the availability and reliability evaluation. The reliability engineering references listed at the beginning of this chapter address reliability methods that can be used for quantifying multiple back-up systems.

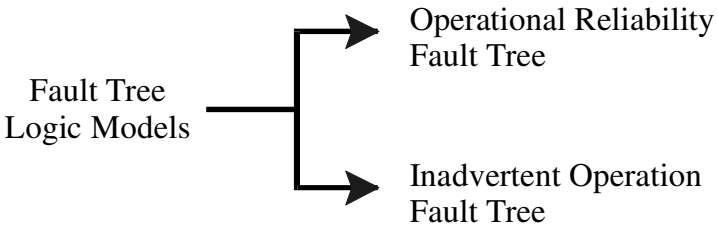
6.6.2 Inadvertent Operation

Inadvertent operation (i.e., false trips) of FPSs typically raises an issue when:

- Detection and emergency control systems (ECSs) are automatically interlocked or tied into shutdown of production equipment
- When discharge of the fire extinguishing agent (i.e., water spray, dry chemical) during a "nonfire" situation can cause damage to the equipment or area it is protecting or create a safety hazard to personnel in the area
- False alarms cause personnel to ignore evacuation warnings

In these cases, design considerations generally include a balance between minimizing inadvertent or false trips while still maintaining system response time (SRT) and operational reliability (OPR).

When quantifying the balance between the OPR versus design concerns related to inadvertent operation, the development of two separate models may be needed:



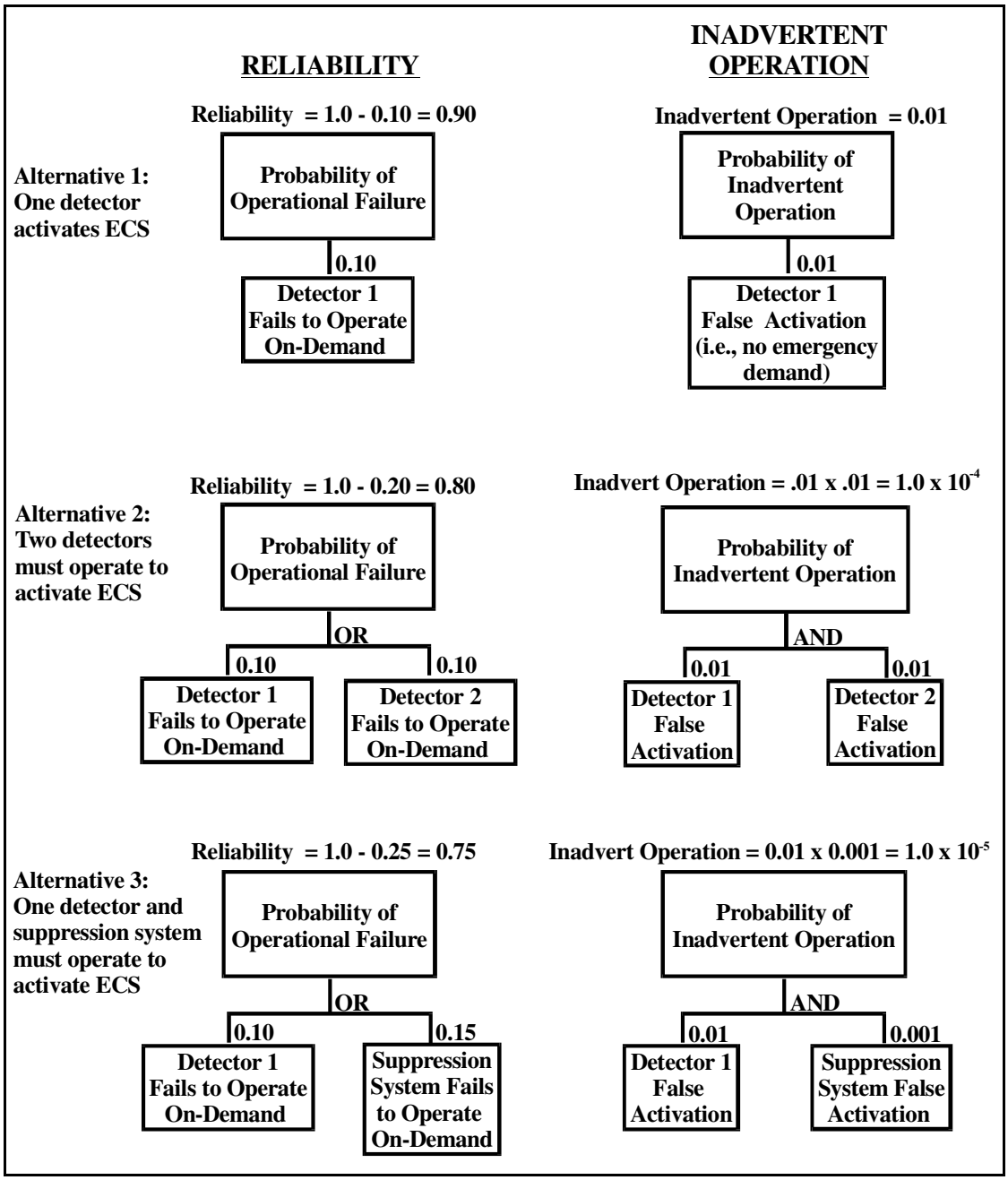
The following presents a simplified example. Let's assume the concern is inadvertent activation of an ECS, which shuts down production equipment. We select three design alternatives for evaluation:

1. One detection device activates the ECS.
2. Two detection devices must operate to activate the ECS.
3. One detection device and operation of the suppression system activates the ECS.

Figure 6.60 presents an example of reliability versus inadvertent operation probability for these three selected alternatives. The probabilities have been inserted for example purposes.

As illustrated in this example, the highest reliability is obtained for alternative 1, one detection device activates the ECS. However, this item also creates the highest probability of inadvertent operation. Alternative 3, one detector and operation of the fire suppression system are needed to activate the ECS, represents the lowest reliability; however it also represents the lowest probability of inadvertent operation.

Fig. 6.60: Example of Reliability Versus Inadvertent Operation



Some primary issues of concern in balancing reliability aspects versus minimizing inadvertent operation probability include:

- In many cases, detection system sensitivity is adjusted downward. Time delays are added that increases response time. Manual intervention error potential may be introduced with the addition of FPS abort features.
- If the sole focus is on designing for a low probability of inadvertent activation, this may make it more difficult for a system to respond to an actual fire; therefore, response effectiveness and reliability may be compromised.
- If a fire detection or suppression system is designed properly, the probability of false inadvertent activation should be inherently very low.

Inadvertent Operation Data

Developing a fault tree logic model for potential inadvertent operation requires data, which may be difficult to obtain. Information sources include:

- Plant specific data
- Manufacturers' data
- Published generic data
- Engineering judgments

The following table provides some generic data on detection system false activation.[10]

Table 6.20: Detection Systems – Some False Activation Data[10]

COMPARISON OF FIRE DETECTOR RELIABILITIES			
FIRE DETECTOR TYPE	FAIL TO OPERATE	FALSE ALARMS	
	Failures/1000 detector-years	Failures/1000 detector-years	Failures per detector-year
Heat (all types)	0.3	9.02	0.009
Photoelectric (smoke)	0.5	536.0	0.536
Ultraviolet	108.0	200.0	0.2
Infrared	108.0	2,135.0	2.135
Ionization (smoke)	data not available	186.0	0.186

The same reference [10] reports that the inadvertent operation of an automatic wet pipe sprinkler system in terms of sprinkler head fusible link failing open is 9.8×10^{-6} occurrences per year. This report, published in 1985 by EPRI (EPRI NP-4144) for Turbine Generator Fire Protection by Sprinkler Systems, presents data gathered from a number of power plants.

Use of inadvertent failure data requires careful scrutiny of the contributing factors, data sources, and data collection methods. From my experience, many incidents recorded as "false

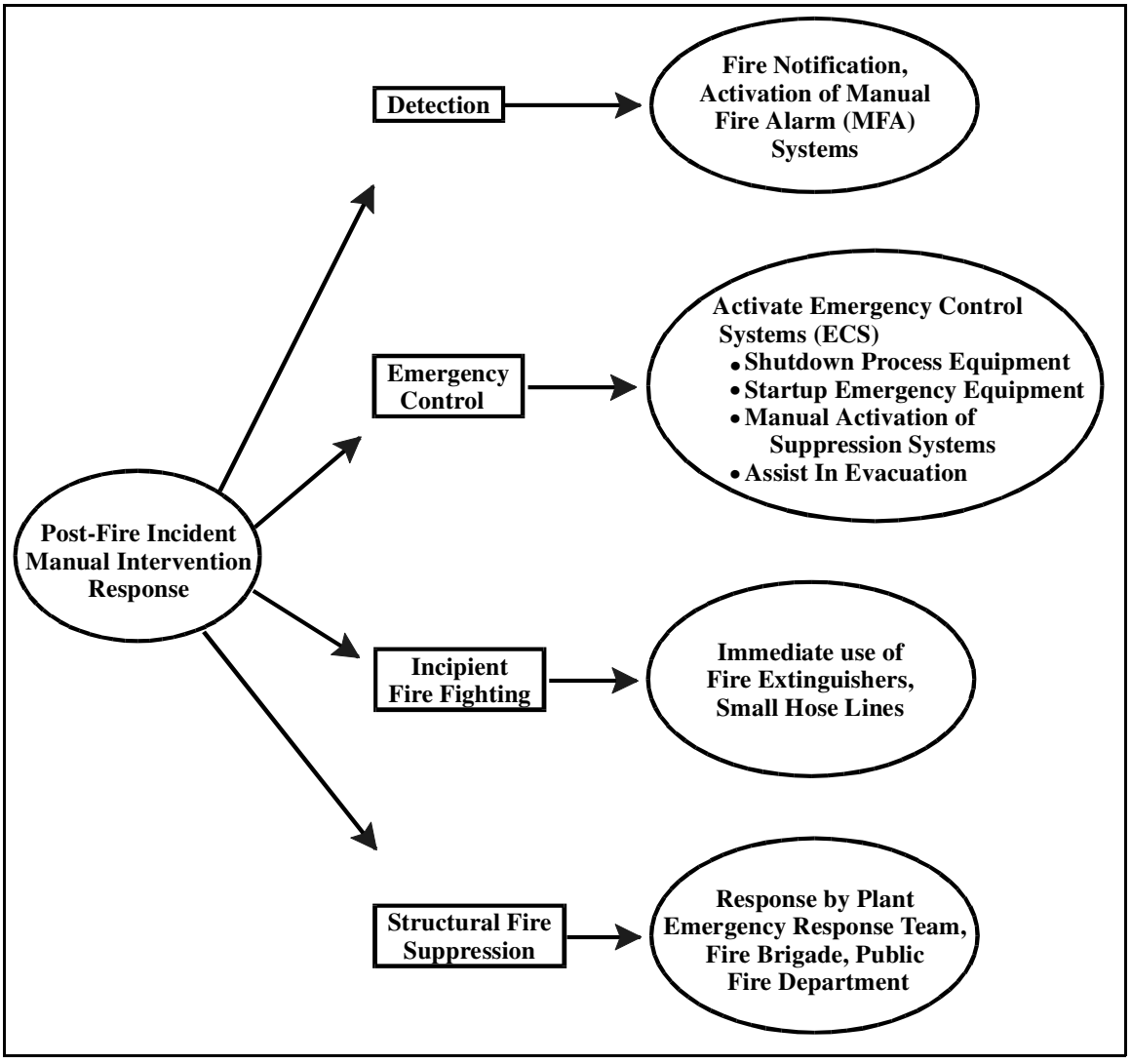
trips" were the result of improper design or installation and did not account for the operating environment of the system or any mechanical/physical damage to the equipment.

When inadvertent operation is a major concern, a balance must be made between the performance requirements and the minimization of inadvertent operation. Response time, availability, and reliability must be examined in parallel with inadvertent or false activation probability.

6.7 MANUAL INTERVENTION

As depicted in Fig. 6.61, FPS responses based on manual intervention may include detection and notification of emergencies by people, manual operation of emergency control and protection systems, and manual fire fighting and suppression efforts.

Fig. 6.61: Manual Intervention Responses



This section provides an overview of "post-fire" human error potential where manual intervention represents a significant aspect of the overall FPS performance success. Manual intervention needs to be integrated into the FPS performance success logic trees and quantified.

As presented in Fig. 6.62, the primary contributing factors to the probability of failure of manual intervention response under post-fire emergency conditions are:

- Human failure to perform functional requirements
- Failure of the equipment interface

Manual intervention functional requirements are the defined tasks of the personnel or operators needed to meet overall FPS performance requirements. Figure 6.63 illustrates a breakdown of performance measures, similar to the FPS hardware logic tree structures discussed in preceding sections. The framework for evaluating the probability of failure on-demand of manual intervention involves:

- Design application basis (DAB) not effective
- Personnel not available
- Human response failure

Fig. 6.62: Manual Intervention Failure Potentials Under Emergency Conditions

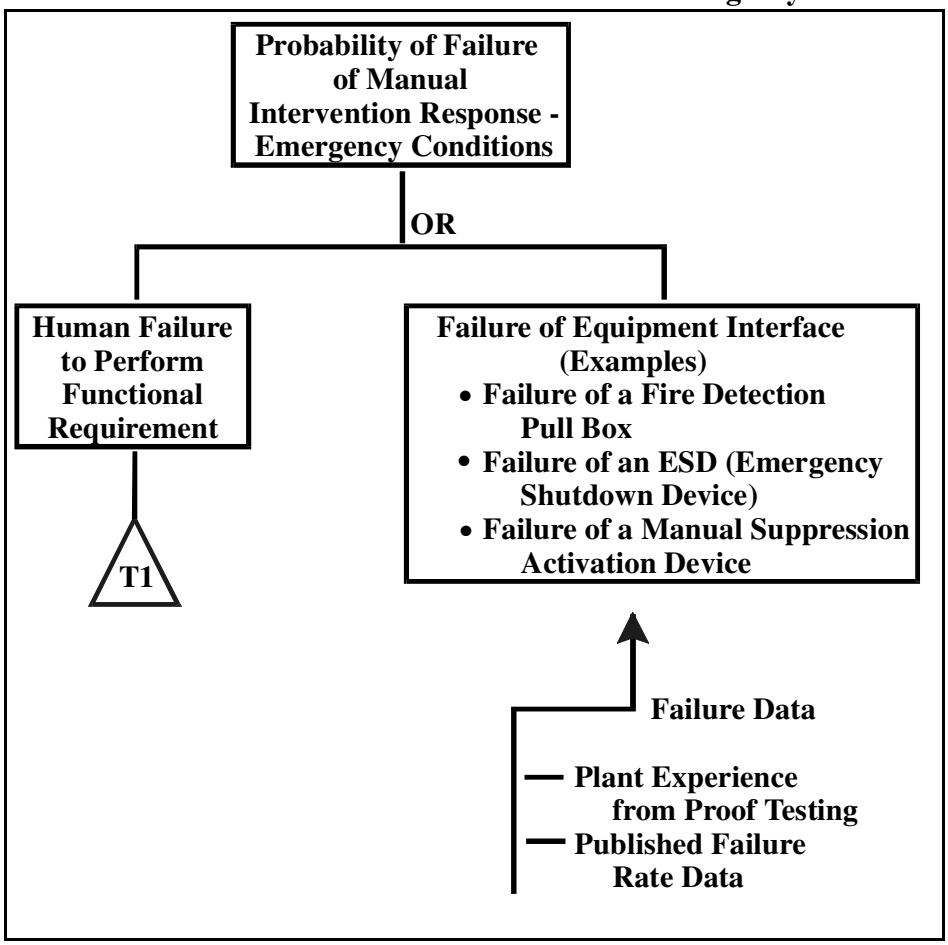
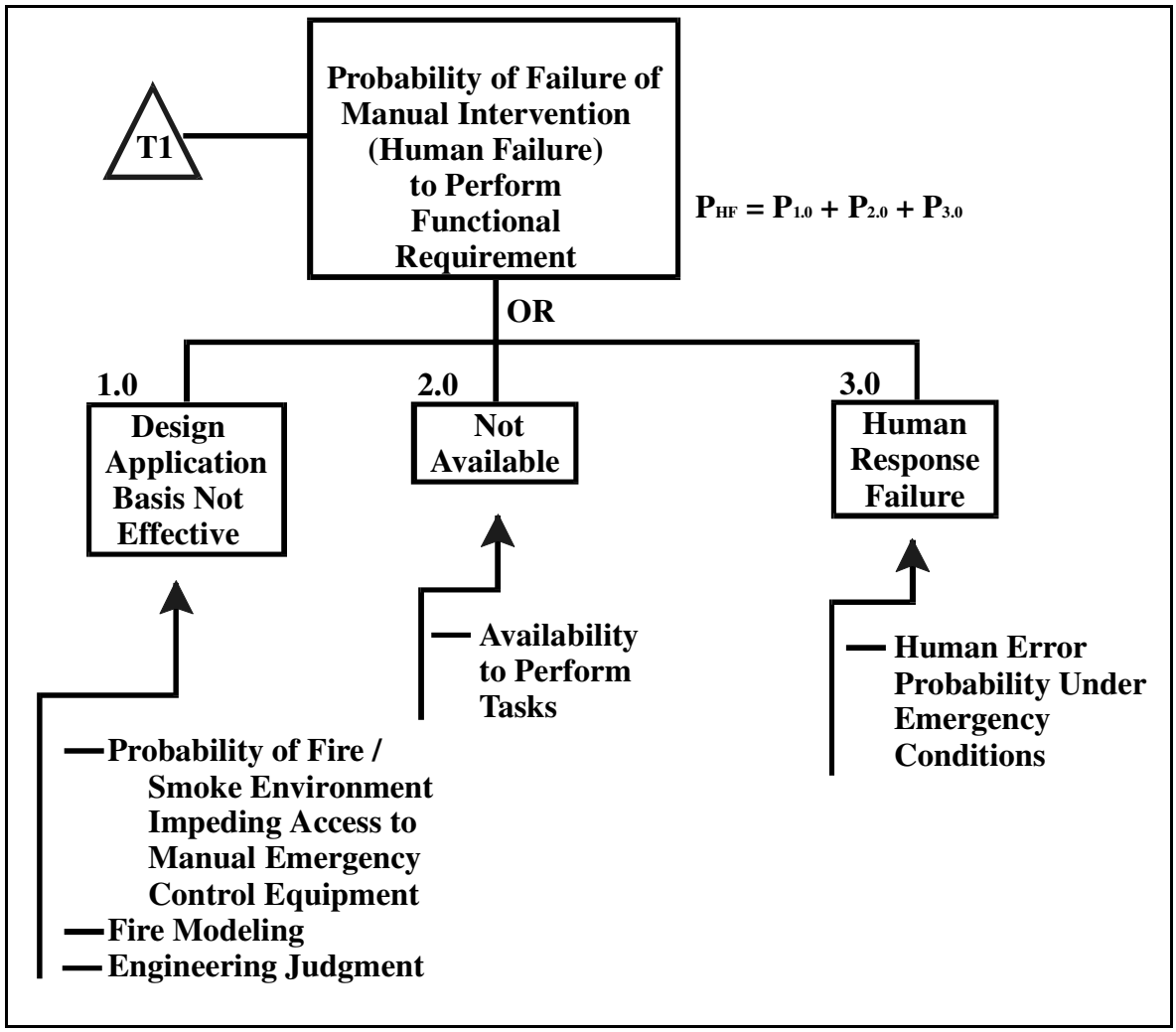


Fig. 6.63: Example Logic Tree Framework — Manual Intervention Failure



6.7.1 Performance Evaluation Factors

Design Application Basis (DAB)

By modeling the exposure profile (i.e., temperature, radiant heat, smoke) the probability of the person assigned emergency tasks having clear access to the emergency equipment can be evaluated. This is a very important consideration and one that is often overlooked.

For example, if our initiating fire scenario is a pool fire inside a production building and the emergency shutdown device (ESD) is within the area of fire origin and exposure zone, then what is the probability of the operator activating the ESD within a defined time limit? The probabilities

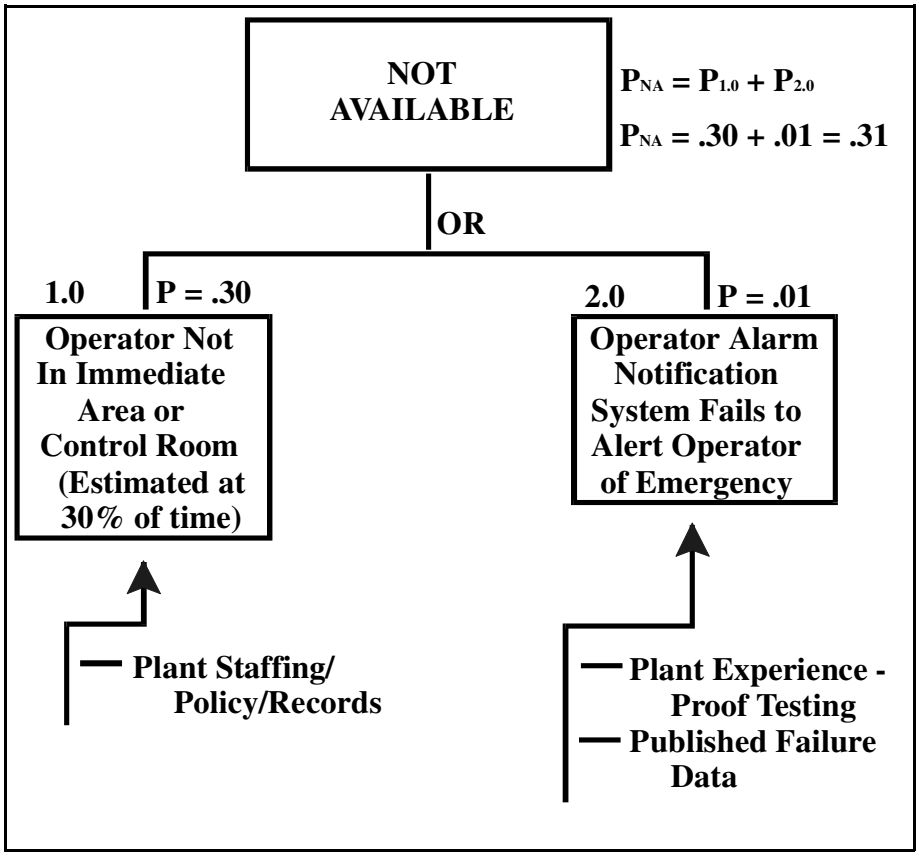
developed to support this evaluation rely on the integration of deterministic fire modeling (exposure environment versus time), operator procedures and training, and engineering judgement.

Availability

This is an evaluation of the percent of time a person is available in the area under risk evaluation to perform emergency tasks. This can also be related to the probability of the person being notified via local or remote alarms of the emergency, as presented in Fig. 6.64.

In many cases, plants have downsized, have undergone staff turnovers, have more unoccupied areas than in the past, and as a result, the availability of personnel to detect incipient stage fires, activate emergency control systems, and operate manual suppression system becomes questionable. The probabilities developed to support this evaluation are usually derived from on plant staffing data over a continuous time period, engineering judgement, and expert opinion.

Fig. 6.64: Example Manual Intervention Not Available



Human Response Failure

Human response failure is an evaluation of the failure of the person assigned emergency tasks to perform effectively within a given time frame. Because of the many factors that contribute to human error, this can pose one of the most uncertain probabilities. Knowledge, training, experience, the ability to perform under emergency (panic mode) conditions can vary from person to person.

In general, human error analyses involves some common characteristics:

- Identification of the relevant tasks to be performed (or, if the plant is at the design stage, to be performed) by operators
- Representation of each task by some method, such as breaking down the task into component parts to identify possibilities for error and points of interaction with plant emergency equipment
- For initial quantification, use of data or estimates derived from historical records and databases (plant specific, industry specific, or published generic data)
- For adjustment of human error probability data, the use of performance modification factors that take into account stress, experience, training, and the quality of man-machine factors. A consistent systematic application method, engineering judgement, and expert opinion are used

The illustration in Fig. 6.65 provides a profile of human error failure rate variation for pre-ignition versus post-ignition. In general, human error potential is higher during emergency fire conditions..

Fig. 6.65: General Illustration of a Human Error Failure Rate Profile for Post-Ignition Fire Incidents

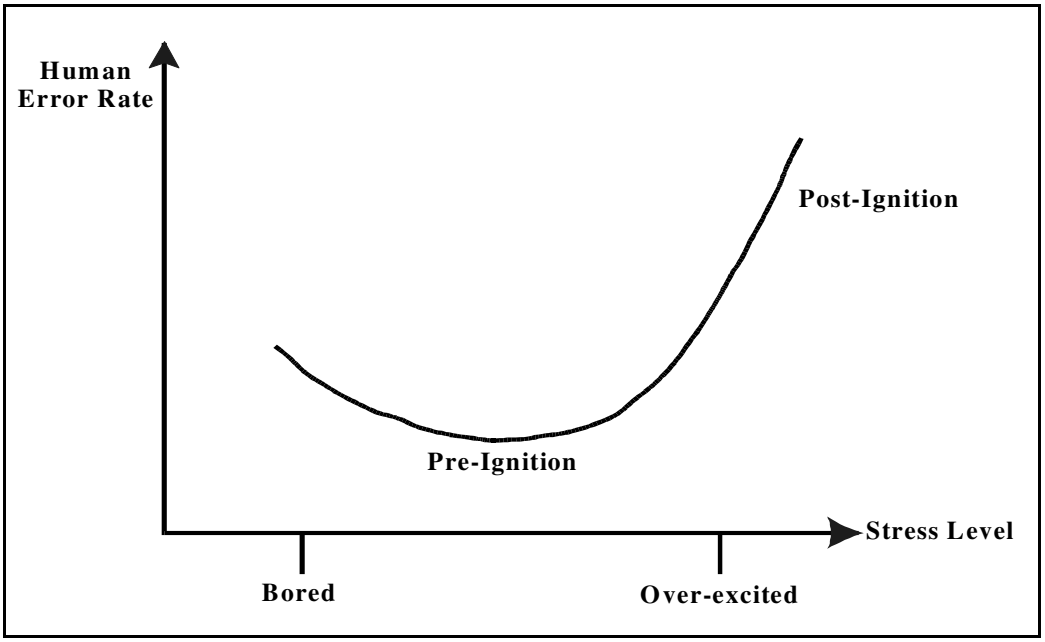


Figure 6.66, which is also discussed in Sect. 4.2 of Chap. 4, is based on a compilation of a number of human error data sources. Post-ignition human element failure probabilities will generally range between Level 2(b) and the Level 1(b) range. Inserting manual intervention human error probabilities into FPS performance logic trees can have a large impact on the top event, which is overall system performance success.

Fig. 6.66: An Example of Human Failure Probability Ranges

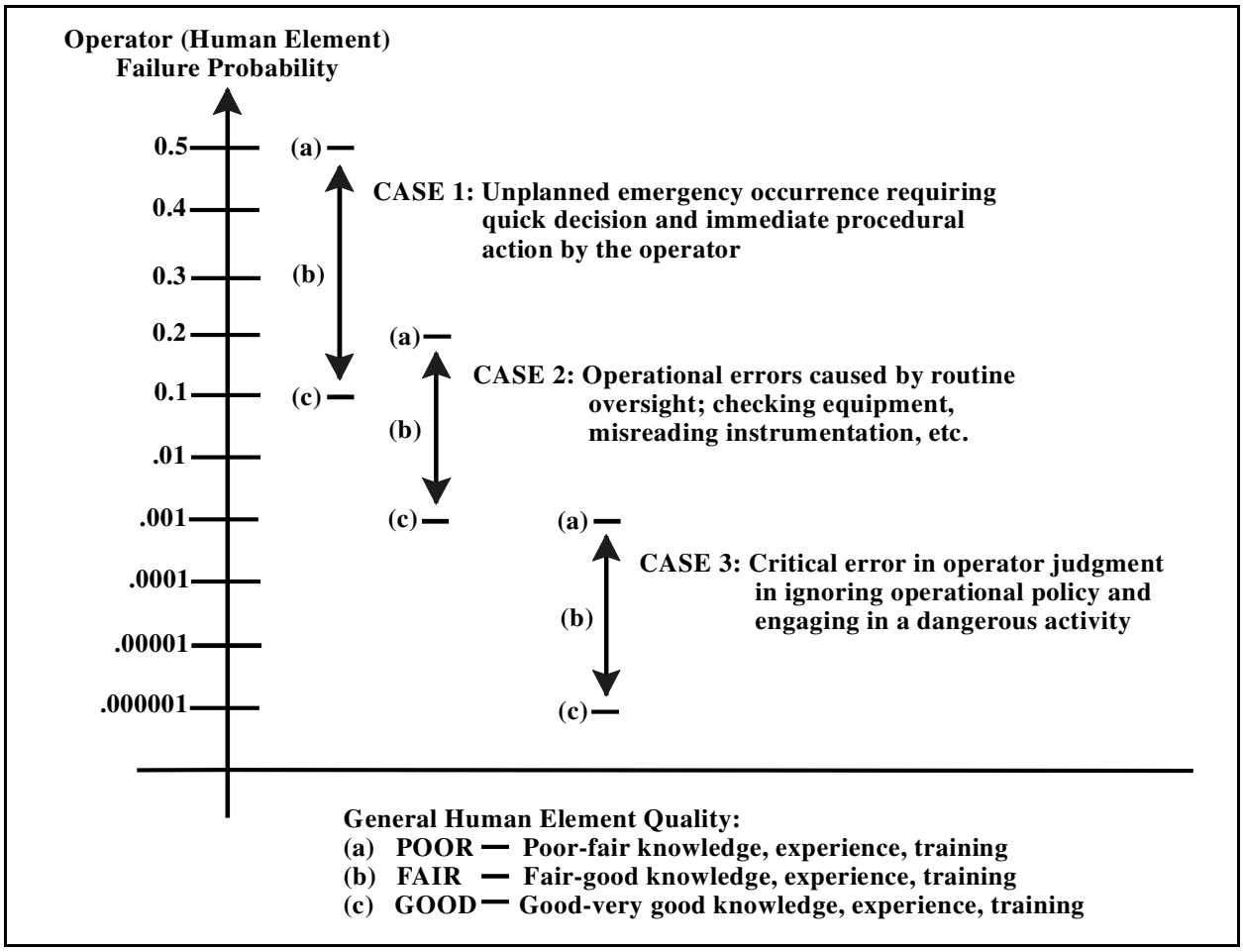
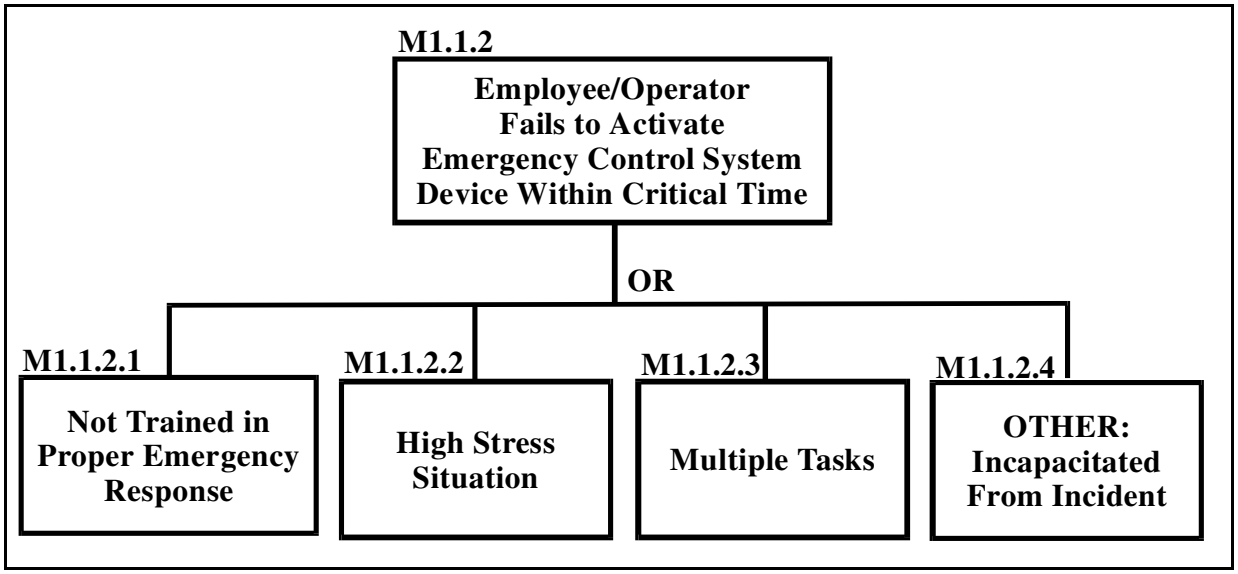


Figure 6.67 provides an example of some factors that may need to be examined to select and adjust historical human error probabilities (i.e., selection of a probability within the case level ranges shown in Fig. 6.66). If the manual intervention human error aspect has a significant impact on FPS performance success, then detailed human reliability analysis may be warranted.

Fig. 6.67: Example of Some Human Error Contributing Factors



The Reduction of Manual Intervention, Human Error

To reduce human error, human reliability under post-ignition conditions must be improved. To evaluate human reliability, major contributing factors leading to human error must be identified. The use of qualitative fault tree structuring provides a method to break down and examine these factors. Next, a consistent methodology to conduct the probabilistic assessments needs to be put in place as typically much engineering judgement and expert opinion will be used to assess each factor and assign probabilities.

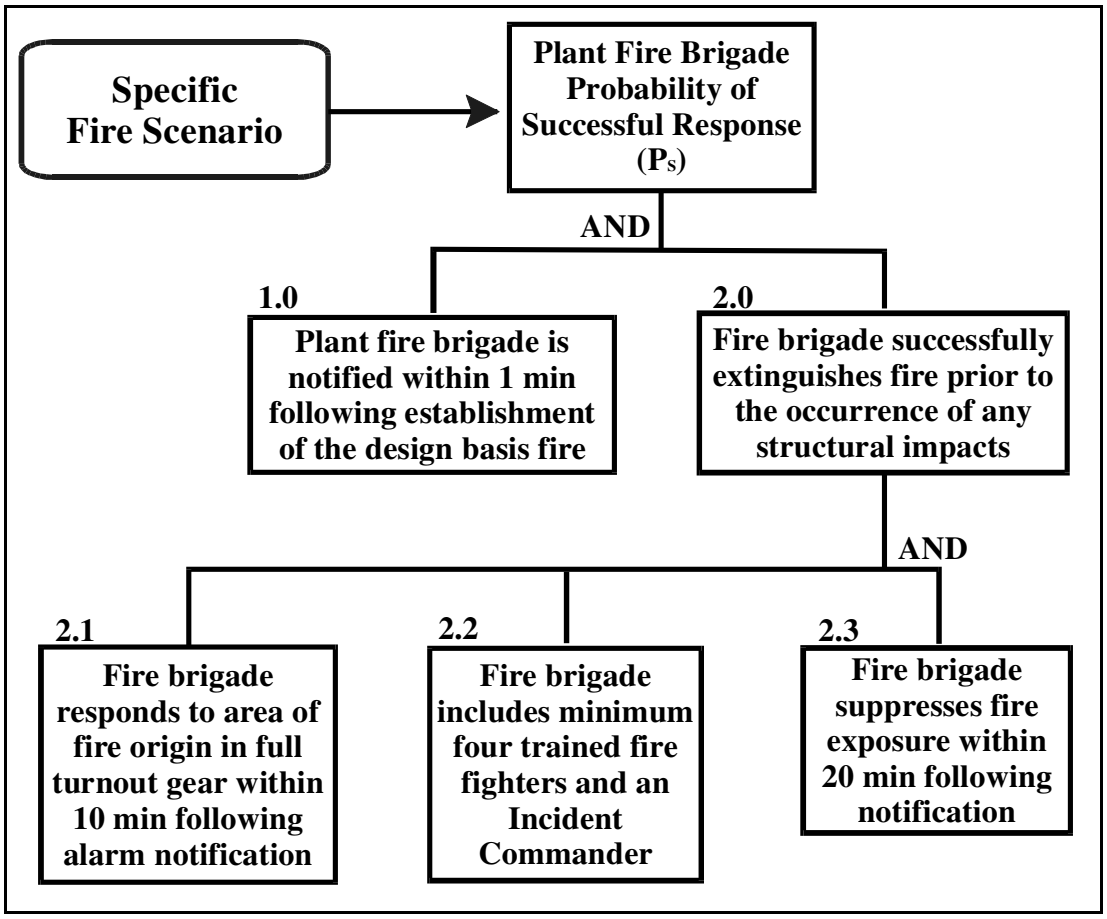
Depending on the significance of the manual intervention aspect on the overall FPS performance success, the complexity of the situation, and level of detail needed, more formal human reliability assessment techniques may be needed to estimate human error potentials and opportunities for reduction. Chap. 8 provides a discussion on human error reduction.

6.7.2 Fire Fighting

If the response of the plant fire brigade or public fire department is a part of the event tree fire risk model, then the probability of successful response needs to be quantified. Primary success measures include:

- Response time
- Resources (personal, equipment)
- Effectiveness

Fig. 6.68: Example of Plant Fire Brigade Success Tree Logic



Primary response time factors include:

- Notification and assembly of the fire brigade
- Response to the area of fire origin in full turn out gear with fire fighting equipment
- Time to achieve the performance objective

Performance success is evaluated in terms of the specific fire scenario, functional performance objectives and requirements, and potential exposure level (i.e., temperature, radiant heat, smoke intensity) at the start of fire fighting efforts. In the Fig. 6.68 example, the

performance objective is fire suppression within 20 min to prevent structural building damage. The requirements based on the exposure potential time line include:

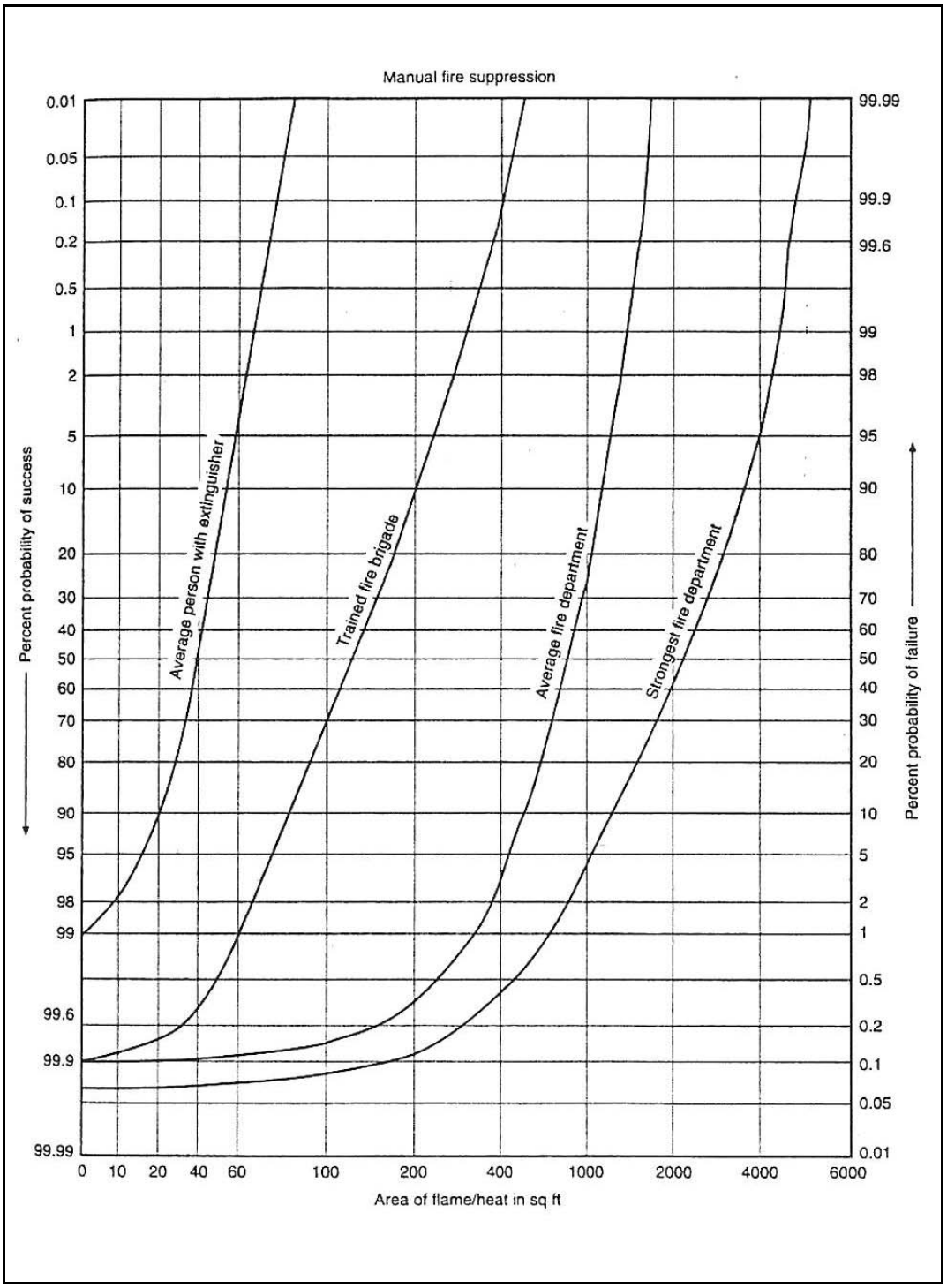
1. Fire brigade needs to be notified within 1 minute following initiation of the design-basis fire event.
2. Response into the area of fire origin, in full turnout gear with fire fighting equipment within 10 min.
3. Response involves a minimum of 4 trained fire fighters and an incident commander.
4. Fire brigade is effective in suppressing the fire within 20 min.

Probabilities for fire brigade or fire department response time and resource availability are usually informed subjective estimates based on assessment of staffing, training, interviews, and past response experience. Developing time lines and conducting drills are good probability support tools.

Fire fighting effectiveness, defined as the ability to achieve fire suppression and extinguishment within a certain time frame under defined scenario and exposure conditions, may be an uncertain probability to estimate and therefore should be approached in a conservative manner.

Figure 6.69, is an example of probability of success for manual extinguishment versus fire size. In this example, fire size is equated in terms of fire exposure area. However, this concept could also be examined in terms of heat release rate (HRR) at time of response, radiant heat, smoke, or toxic gas environment at the time of response.[12]

Fig. 6.69: Example Probability Profile of Manual Extinguishment Success Versus Fire Size[12]



Reprinted with permission from the NFPA Fire Protection Handbook, Copyright 1997, National Fire Protection Association, Quincy, MA. 02269. This reprinted material is not the complete and official position of the National Fire Protection Association on the referenced subject, which is represented only by the standard in its entirety.

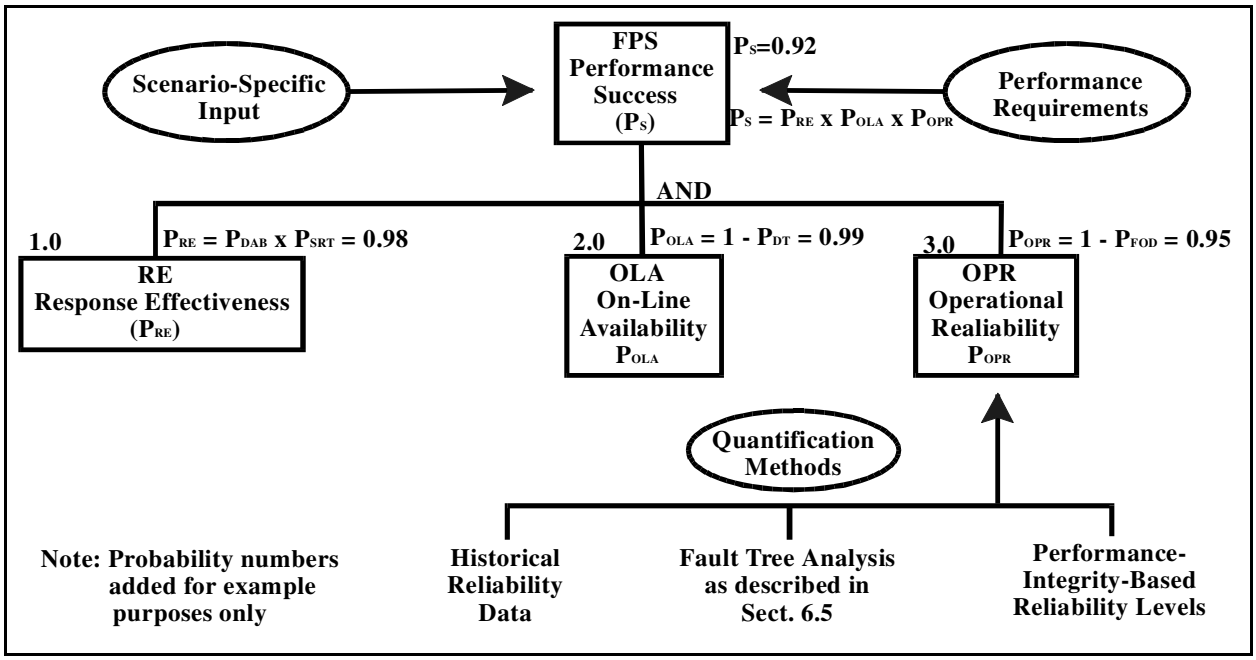
6.8 PERFORMANCE-INTEGRITY-BASED RELIABILITY LEVELS

As stated in the beginning of Sect.6.5, in risk-informed, performance-based fire protection studies there are generally three approaches for quantifying FPS operational reliability:

1. Historical reliability data
2. Fault tree analysis (FTA)
3. Performance-integrity-based reliability levels

These quantification approaches are shown in Fig. 6.70.

Fig. 6.70: Example Primary FPS Performance Success Factors



In most cases, by following the evaluation methods discussed in this chapter, the FPS response effectiveness (RE) and on-line availability (OLA) can be assessed and quantified in a relatively short time. The FPS performance measure, which can become very time consuming to quantify depending on the complexity of the system and availability of failure data, is the OPR.

Conducting performance-integrity-based analysis for estimating FPS OPR involves:

1. Detailed review of the FPS for conformance with applicable design codes, standards, practices.
2. Review of available reliability data from manufacturers, reliability databases, or previous reliability studies.
3. Quality scoring of FPS performance integrity measures (PIMS), including detailed evaluation of inspection, testing, and maintenance records.
4. Developing an FPS reliability estimate based on items 1 to 3 above and engineering judgement.

6.8.1 Review of Applicable Design Codes, Standards, Practices

Present day codes such as mechanical, plumbing, or electrical codes, along with specific NFPA standards, provide various levels of FPS design criteria. In addition, some industry associations and property insurance companies provide interpretive guides to certain NFPA standards and "good practice" design supplements based on lessons learned from fire and explosion losses.

In general, design criteria developed by these sources focus on equipment, components, materials of construction, installation requirements, and acceptance testing. Normally, very little information is provided on FPS performance factors such as:

1. System response time (SRT) design guidance and quantification methods
2. On-line availability (OLA) issues such as design factors, which could minimize downtime
3. Failure rate data references for systems, equipment, components
4. CCF effects (i.e., corrosion, freezing, etc.)
5. Relationship of system reliability versus various design options
6. Effect of inspection, maintenance, and testing on FPS reliability

What FPS design codes and standards do provide however, is design guidance based on past failure experience; therefore, in a qualitative sense, they provide a level of reliability. In addition, FPS equipment and components must be listed or approved by nationally recognized testing laboratories. A very useful future addition to NFPA type standards would be a section on reliability that relates system reliability levels to various design options. An example of such an attempt is made in NFPA 72, National Fire Alarm Code, the section on dwelling fire warning systems. [3]

> **8-3 Reliability.**
>
> **8-3.1** Fire warning systems located in dwelling units and having all of the following features shall be considered to have a functional reliability of **95 percent:**
>
> 1. Utilizes a control panel
> 2. Has at least two independent sources of operating power
> 3. Monitors all initiating and notification circuits for integrity
> 4. Transmits alarm signals to a constantly attended, remote monitoring location
> 5. Is tested regularly by the homeowner and at least every 3 years by a qualified service technician
>
> **8-3.2** Fire warning systems for dwelling units with all of the features of 8-3.1 except (4) or systems that use low-power wireless transmission from initiating devices within the dwelling units shall be considered to have a functional reliability of **90 percent**.
>
> **8-3.3** Fire warning systems for dwelling units comprised of interconnected smoke alarms where the interconnecting means is monitored for integrity shall be considered to have a functional reliability of **88 percent**. If the interconnecting means is not supervised or the alarms are not interconnected, such systems shall be considered to have a functional reliability of **85 percent**.

To further develop this type of reliability information, the underlying failure data sources, reliability assessment method, and uncertainty issues would need to be addressed. Equipment manufacturers would have to make failure data available. Equipment listing and testing agencies would need to develop approvals based on defined, quantitatively supported levels of reliability.

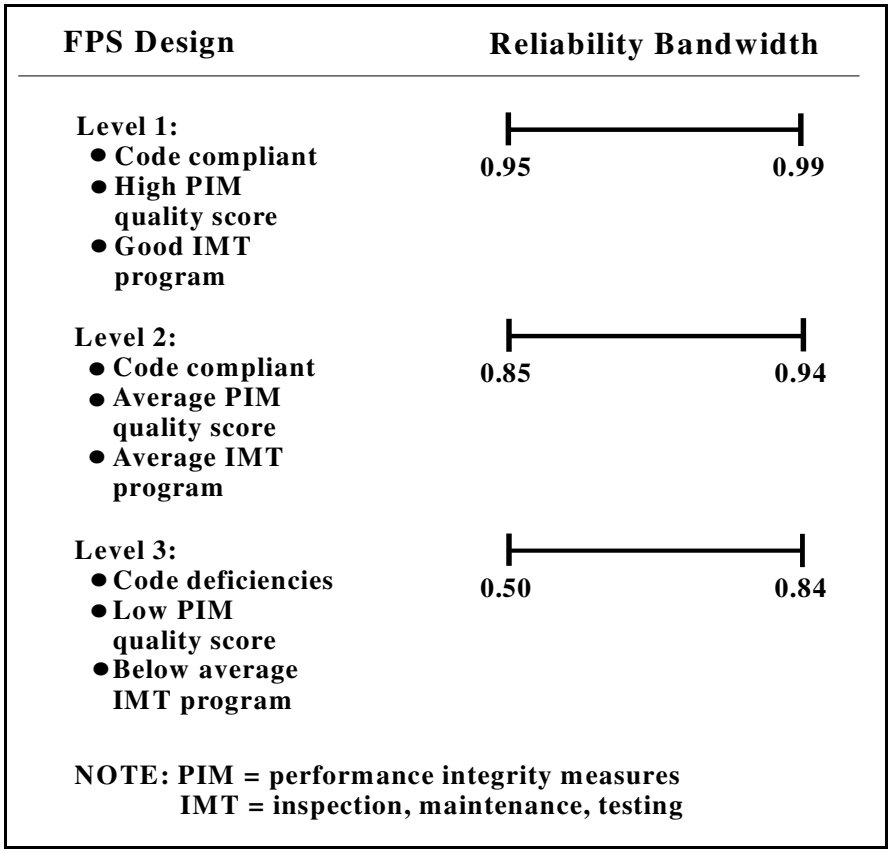
It is hoped that as the use of risk-informed performance-based standards progress, information will be incorporated into codes, standards, and design practices to address design options versus reliability levels.

6.8.2 Reliability Data Review

Research and review of relevant "system level" reliability data from manufacturers, reliability data bases, and previous reliability studies should be conducted. The focus of this effort is to try to develop a bandwidth, or range, of system reliability and an understanding of the major factors that contribute to reliability levels. Failure and reliability data sources were addressed in Sect. 6.5.

From my experience conducting reliability analyses on fire detection and fire protection systems (which has included both existing and new systems), results generally fit into a reliability bandwidth as illustrated in Fig. 6.71.

Fig. 6.71: General Example Reliability Bandwidth



6.8.3 Quality Scoring of FPS Performance Integrity Measures

Development of a PIM quality grading approach as an adjustment to generic failure rate data was discussed in Sect. 6.5.

Primary PIMs for FPS evaluation might include:

- Design standards
- Life-cycle (age)
- Management of change (MOC) program
- Inspection/maintenance programs
- Proof testing program
- Operating environment (temperature, vibration, corrosion)
- Redundancy features (i.e., to minimize CCF potentials)
- Diagnostics (i.e., continuous electronic fault detection, supervision)

By applying the methods described in Sect. 6.5, an FPS PIM quality score (i.e., PIM GPA) can be developed:

Qualitative PIM Score	Quantitative PIM GPA Score
Low	< 2.5
Average	2.5 to 3.5
High	> 3.5

6.8.4 FPS Reliability Estimate

Table 6.21 provides an example FPS reliability evaluation worksheet. This worksheet incorporates the performance-integrity-based reliability concepts presented in this section and includes the following information:

1. FPS description
2. Design code compliance review
3. PIM quality scoring
4. Reliability estimate using a PIM score versus reliability range relationship
5. Review comments
6. Recommendations to improve or maintain system reliability

On the right-hand side of the worksheet is an area to identify attachments. As with any evaluation, the more knowledge and technical support documentation attached, the more confidence in the results. Understanding the system, subsystem, and component failure modes and major contributing factors minimizes evaluation uncertainties.

Table 6.21: Example FPS Reliability Evaluation Worksheet

FPS RELIABILITY EVALUATION

1. FPS Description:

Date:

☐ Existing System
☒ Modified System
☐ Proposed new system

Evaluation by:

Review by:

2. Design:

List applicable codes/standards/design practices
- •
- •
- •

☒ Fully compliant
☐ Minor deficiencies
☐ Major deficiencies

ATTACHMENTS
☒ design review checklist
☒ design diagrams, specifications
☐ other

3. Performance Integrity Measures (PIMs):

Subsystem	Input	Control	Output	Overall Rating
PIM GPA Score	3.5	3.7	3.6	3.6 – High
IMT Program Quality	—	—	—	High

☒ PIM worksheets
☒ IMT program review
☐ Other

4. Reliability Estimate:

Relating PIMs to Reliability Ranges

PERFORMANCE INTEGRITY MEASURE (PIM) SCORE/GRADE	RELIABILITY RANGE		PROBABILITY OF FAILURE ON-DEMAND (P_{FOD}) (> 1 – RELIABILITY)	
Very High	Very High	.99 – .999	Very Low	.01 – .001
↓	High	.95 < .99	Low	.05 < .01
	Average	.90 < .95	Average	.10 < .05
	Low	.80 < .90	High	.20 < .10
Very Low	Very Low	< .80	Very High	> .20

☐ Reliability data
☐ Previous reliability evaluations
☐ Other

Reliability Estimate Selected: 0.95

5. Review Comments:
(Comment on design deficiencies, PIM evaluation weak links, unusual features, etc.)

6. Recommendations:
(To improve or maintain system reliability)

NOTE: Data added for example purpose only

6.9 Discussion

The FPS performance success logic presented in this chapter provides a consistent logical approach towards quantifying performance-based on:

- Specific scenario input
- Defined functional performance requirements

The methodology provides a breakdown of experience-based performance success factors that include response effectiveness, on-line availability, and operational reliability. The methodology allows integration of probabilistic failure of equipment, human error aspects, deterministic modeling to support failure or success probabilities, and incorporation of engineering judgement and expert opinion.

The methodology can be used to evaluate:

- Existing systems
- Modifications to existing designs
- New or proposed system designs

The methodology lends itself to an innovative approach towards quantifying FPS performance success by structuring an engineering-based evaluation model that is plant specific, scenario-specific, and guided by risk tolerance criteria.

An engineering-based evaluation model used in conjunction with available statistical data is better than application of statistical data only. To illustrate briefly: I was involved in a project involving a hazardous waste storage building. Following a site survey, I visited the safety analysis staff involved in this project. They had constructed an event tree and in their event tree, they had inserted a 0.95 probability of sprinkler system performance success, based on purely statistical data. They indicated the 0.95 was "conservative" as the sprinkler performance was close to 0.99, according to their own statistical data. Based on the plant field survey, the hazardous waste storage building contained many nonwater miscible contaminated solvents and oxidizers. The sprinkler heads were on-off type heads, which were very corroded and would do little to control or suppress a fire in the building. Following the methodology presented in the chapter, the estimated performance success of this sprinkler system was in the 0.10 – 0.15 range, a big difference from their statistical estimate. The lesson — build an engineering-based performance success model as presented in this chapter, and don't just rely on some general statistics.

Problems I have found in reviewing probabilistic fire risk assessments that rely heavily on statistical data include:

- System performance success was only associated with the system being available. This approach assumes:
  - Response effectiveness = 100%
  - OPR on-demand = 100%
- Time is not properly integrated into fire suppression success probability.
  - Time at which damage starts versus time at which the system automatically operates
  - Time delays involving operation of manually actuated suppression systems
- CCF potentials and FPS interfaces were not adequately addressed.

Fire Protection System Interfaces

Fire protection systems (FPSs) evaluated in event trees must be analyzed as independent systems in terms of functional performance requirements and sequence of operations. When incorporating FPS into event tree logic, sometimes there is confusion over what I call "system interfaces."

The best way to discuss this is with a brief example. Let's assume we have an automatic wet pipe sprinkler system protecting a lubricating system oil hazard in a production area. The general design criteria is that when a fire occurs, the sprinkler head fusible link operates, local and remote fire alarms are transmitted, an automatic interlock shuts down in gas line safety shut-off valve associated with a production furnace, and the sprinkler system suppresses and extinguishes the oil fire scenario.

When structuring event tree logic, the sequence of FPS operation should parallel the design objectives. As shown in Table 6.22, items 1 and 2, for this example the sequence involves quick detection of the initiating fire, activation of the ECS in the area of fire origin, and suppression of the fire prior to secondary fuel(s) involvement.

The design objectives related to risk tolerance and the associated FPS functional performance requirements support the event tree logic structuring. For example, item 3 in Table 6.22, functional performance requirements, indicates an operational time frame, which is a primary measure of system success.

An important concept in developing first-order fault trees to quantify top events in the ETA is not to duplicate failure or success probabilities for subsystem components. Item 4 in Table 6.22 lists common subsystem components for our example, which include the sprinkler head and control panel.

The sprinkler head is a common component of interest in evaluating both fire detection success and automatic sprinkler system success. When the sprinkler head operates, two things occur, a water-flow signal is sent to the control panel and water flow from the sprinkler head starts fire suppression. As suggested in item 5, Table 6.22, evaluate the sprinkler head response time and OPR as part of the "Fire Detection System" performance success analysis.

The control panel has some common functions related to receiving detection input signals and relaying the signals to the actuation components of the ECS. For the detection system, this is a control panel detection signal output function, and for the ECS, it is a control panel actuation input signal function. These functions taken together are termed an "interface function." As suggested in item 5, Table 6.22, to avoid duplication of failure probabilities, evaluate the control panel as a subsystem (with input and output functions) associated with fire detection system success. Performance success analysis of the ECS can then be concentrated on the OPR of the ECS equipment following receipt of the actuation signal from the control panel.

FPSs incorporated into event tree logic need to be analyzed in terms of sequence of operation and time-related functional performance requirements. FPSs need to be quantified in a manner that avoids duplication of failure probabilities for common subsystem components.

Table 6.22: Example of Common Subsystem Components

	[A]	[B]	[C]
1. Event Tree Logic	Fire Detection Is Successful	Emergency Control System (ECS) Is Successful	Automatic Sprinkler System Is Successful
2. Design Objectives	Following fire initiation, minimize the time for notification and evacuation of people	Minimize any chance of having an uncontrolled gas release in the fire area	Minimize production equipment damage, building damage, and production down time
3. Functional Performance Requirements	• Detect fire within 2 min • Sound local alarms/ strobes • Transmit remote alarm to Control Room • Transmit activation signal to ECS	Within 30 seconds, following fire detection, automatically shut down furnace safety shut-off valves located outside of fire area	Within 3 – 10 min, suppress and extinguish oil fire scenario
4. Common Subsystem Components Input (I) Control (C) Output (O)	(I) Sprinkler head operation (C) Control panel interface	(C) Control panel interface	(O) Sprinkler head operation
5. Suggestions/Remarks • Evaluate sprinkler head response time and OPR as part of [A] fire detection system performance success. • Evaluate control panel as a subsystem with input function (i.e., receipt of fire detection signals) and output functions (i.e., transmittal of ECS actuation signal) as part of [A] fire detection system performance success.			

Use of a Computer Program Model

Since the general FPS performance success tree logic framework is similar for evaluating various systems, the logic can be structured in a "generic" form using an FTA computer program or using a computer spreadsheet such as Excel. Once the generic framework is set up, it can usually be customized fairly easily for a specific FPS. I have set up approximately ten generic Excel spreadsheet models for various detection, emergency control, and suppression systems; these can be customized in a fairly short time.

For doing first-order FTA (evaluating primary contributing events), the importance of contributing factors and cut-set analysis of contributors to the top event can be performed on a gate-by-gate evaluation. For more detailed FTA, computer programs provide additional

sophistication. A listing of some FTA and ETA computer programs is provided in Chap. 4, Sect. 4.3.3.

The advantages of setting up a generic computer model template is that this allows what-if analysis, allows evaluation of sensitivity and importance of contributing factors, and provides means to conduct an uncertainty assessment. Many FTA computer programs include the use of probability distributions as input and Monte Carlo simulation capability. Also, there are available computer programs that provide similar capabilities for use with spreadsheets such as Excel (discussed in Chap. 7).

Performance and Risk Management

Risk managers are very interested in quantifying the performance of loss control systems. From my experience, a common concern is this: given a fire incident occurs, how will the detection systems, emergency control systems, and fire suppression system perform to minimize the risk impact? Motivation for quantitative performance evaluation as expressed by risk managers includes: FPSs are getting old, numerous occupancy changes have taken place since the fire systems were installed, insurance deductibles are much higher as is the need to quickly control initiating fires, business interruption (BI) risks are much higher due to increased competition, etc.

The quantitative performance assessment method described in this chapter allow evaluation of existing FPSs as well as new system alternatives. In addition, the method can be customized or enhanced as needed to meet specific performance assessment objectives. For example, the efficiency and cost-effectiveness of FPS IMT can be examined in more detail by applying risk and reliability centered maintenance (RCM) techniques.

Summary

The methodology discussed in this chapter is based on realistic experience and application, not an academic exercise. Application has included evaluation of prevention and protection systems in the chemical, oil, gas, and electric power industries, hazardous material processes, storage, nuclear fuel processing, and other industrial production operations. The application of this methodology, although based on industrial type risks, also lends itself to other commercial applications.

As for prescriptive codes, the movement will be more and more towards risk-informed, performance-based methods. Existing codes primarily concentrate on hardware design criteria based on loss experience. Most existing codes do not address risk tolerance criteria, specific scenario input, response time of FPS actuation, system availability factors, and quantification of reliability versus system design and testing options.

It is certainly expected that the methodology described in this book will be refined based on users' input and the progression of performance-based fire protection standards and applications. The main thought process, however, needs to extend beyond some of the current trends that only

equate performance success to the results of deterministic fire modeling efforts. Performance success is a probabilistic measure involving a three dimensional evaluation of:

- Response effectiveness (RE)
- On-line availability (OLA)
- Operational reliability (OPR)

6.10 REFERENCES

1. Hadjisophocleous, G.V., Benichou, N., and Tamim, A. S.,1998. "Literature Review of Performance-Based Fire Codes and Design Environment." *Journal of Fire Protection Engineering*, 9(1), pp. 12 – 40.

2. *Fire System Integrity Assurance*, Report No. 6.85/304, June 2000, The International Association of Oil & Gas Producers.

3. NFPA Standard 72, "Automatic Fire Alarm Code," National Fire Protection Association, Quincy, MA.

4. Cholin, John M. and Chris Marrion, "Performance Metrics For Fire Detection," *SFPE Fire Protection Engineering Magazine, Summer 2001*, Issue No.11, published quarterly by the Society of Fire Protection Engineers (SFPE)

5. Proceedings of the 35th Annual Loss Prevention Symposium, Houston, Texas, April 22 – 26, 2001, Sponsored by the American Institute of Chemical Engineers (AIChE), New York, N.Y. Paper LPS-le, Dr. Peter E. More and Richard Siwek, "An update on the European Explosion Suppression and Explosion Venting Standards"

6. Sutton, Ian S., *Process Reliability and Risk Management*, Van Nostrand Reinhold, N.Y., 1991

7. *Center for Chemical Process Safety, Guidelines for Process Equipment Reliability Data, with Data Tables*, AIChE, New York, NY, 1989.

8. *Center for Chemical Process Safety, Guidelines for Chemical Process Quantitative Risk Analysis*, American Institute of Chemical Engineers, New York, NY, 1989.

9. *Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations*. IEEE Std 500-1984, Institute of Electrical and Electronic Engineers, New York, N.Y.

10. EPRI (Electric Power Research Institute) Report EPRI NP-4144, *Turbine Generator Fire Protection by Sprinkler System*, Final report, July 1985

11. Thompson, J. R., *Engineering Safety Assessment, An Introduction*, John Wiley & Sons, New York, N.Y., 1987

12. Cote, A. E., ed., *Fire Protection Handbook, 18th ed.*, Natural Fire Protection Association, Quincy, MA, 1996

13. *The SFPE Handbook of Fire Protection Engineering, Second Edition*, DiNenno, P. J., Editor, published by the Society of Fire Protection Engineers and National Fire Protection Association, Quincy, MA, 1995

14. Instrument Society of America (ISA), ISA-S84.01. Application of Safety Instrumented Systems to the Process Industries. Research Triangle Park, N.C., 1996