

Categorization by Safety Significance

2.1 Introduction

A plant consists of a variety of systems, structures, and components (SSCs) operated and maintained directly or indirectly by humans. Some SSCs and human activities (HAs) are more important than others from the point of view of risk. A risk-informed safety assurance utilizes risk information to 1) satisfy safety goals, 2) gain public trust, 3) increase safety assurance effectiveness, and 4) to remove unnecessary burden. The first step of the risk-informed safety assurance is the categorization of SSCs and HAs. The second step is the realization of requirements demanded for each category (Chapter 3)

This chapter first describes the categorization process advocated by IEC 61508, IEC 61511, and BS EN 951. These categorizations are based on the amount of risk reduction by the SSC. More complicated cases of risk-informed safety assurance are seen in the US NRC's risk-informed regulations. Categorizations of SSCs and HAs are described. The same "pressure-tank" example is used to illustrate common principles of these unrelated methodologies at a first glance.

2.2 Safety Integrity Level: IEC 61508 and IEC 61511

2.2.1 Hazardous Situation and Event

Hazard is defined as a potential ability to cause harm. Hazard has a source. For example, movement is a hazard. The source is a vehicle and the harm is a fatal injury by a collision. Hazard does not necessarily mean actual occurrence of harm or high probability of harm.

A hazardous situation is defined as a circumstance immediately before the harm is produced by the hazard. This is simply an occurrence of an initiating event. The hazardous situation would eventually yield harm if nothing stops it.

The hazardous situation, or the initiating event, occurs when a hazard comes into a play through some mechanism. A typical activation is through a failure of a control system that has suppressed the hazard. An intersection with a traffic signal is a hazard (source) of collision. The failure of the traffic signal yields a hazardous situation where extreme care is required for any drivers going through it.

The hazardous situation becomes a hazardous event when the harm becomes existent.

2.2.2 Definition of Function

A function is an action that is required to achieve a desired goal. Safety functions are those functions that serve to ensure safety. A typical safety function in a nuclear power plant is a “reactivity control”. A high-level objective, such as preventing the release of radioactive materials to the environment, is one that designers strive to achieve through the design of the plant and that plant operators strive to achieve through proper operation of the plant.

The function is often described without reference to specific plant systems and components or humans that are required to carry out this action. Functions are often accomplished through some combination of lower-level functions such as detection of an abnormal event. The process of manipulating lower-level functions to satisfy a higher-level function is sometimes called a *control function*. During function allocation the control function is assigned to human and machine elements [13].

2.2.3 Functional Safety System

A functional safety system prevents the occurrence of a hazardous event, given a hazardous situation. Some functional safety systems mitigate the hazardous event, such as an automobile collision, that has occurred. The mitigation reduces the fatal effect on people. IEC 61508 contains detailed descriptions about the functional safety systems [1].

The functional safety system consists of 1) monitor, 2) judge, 3) actuator, 4) power source, 5) piping and wiring, *etc.* This is similar to a human. In the process industries, the functional safety system is called a safety-instrumented systems (SIS) [11]. The present day machine industries take these systems for granted.

Operations of functional safety system include: 1) potentially hazardous movements of a machine are shut down or reversed when an emergency button is actuated, 2) potentially hazardous movements are prevented when the safety guard covering a machine is opened or when an approach of a worker is detected [23], 3) overspeed is detected and the machine is made to stop, 4) prestart warning device alarms a worker that the machine is about to start when the waiting time has elapsed [24]. An extreme is an emergency cooling system that is activated upon detection of loss of coolant at a nuclear power plant.

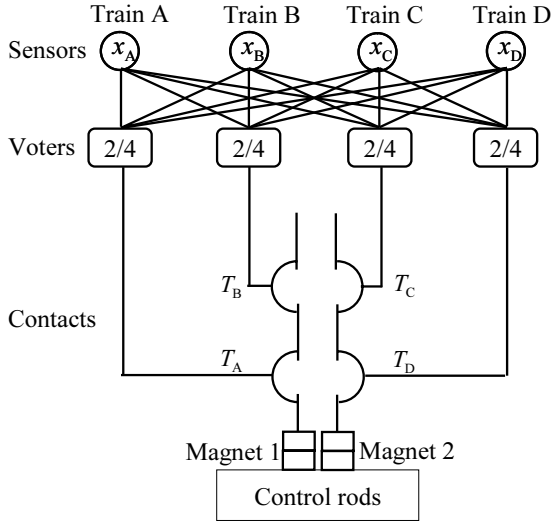


Fig. 2.1. An example of a functional safety system

2.2.4 Example: Reactor Scram System

Consider a reactor scram system shown in Figure 2.1. When a hazardous situation at a nuclear power plant is detected, the system drops enough control rods into the reactor to halt a so-called chain reaction. This insertion is a reactor scram or a reactor trip.

Five features of the scram system are listed.

- 1) Inadvertent events are monitored by four identical channels, A, B, C, and D.
- 2) Each channel is physically independent of the others. For example, every channel has a dedicated sensor and a voting unit.
- 3) Each channel has its own two-out-of-four:G voting logic. Capital G, standing for “good” means that the logic can generate the scram signal if two or more sensors successfully detect an inadvertent event. The logic unit in channel A has four inputs, x_A, x_B, x_C, x_D , and one output, T_A . Input x_A is a signal from a channel A sensor. This input is zero when the sensor detects no inadvertent events, and unity when it senses one or more events. Inputs x_B, x_C , and x_D are defined similarly. Note that a channel receives sensor signals from other channels. Output T_A represents a decision by the voting logic in channel A; zero values of T_A indicate that the reactor should not be tripped; a value of 1 implies a reactor trip. The voting logic in channel B has the same inputs, x_A, x_B, x_C , and x_D , but it has output T_B specific to the channel. Similarly, channels C and D have output T_C and T_D , respectively.

- 4) A one-out-of-two:G twice logic with input T_A , T_B , T_C , and T_D is used to initiate control-rod insertion. The rods are suspended by magnets energized by two circuits. The two circuits must be cut off to de-energize the magnets; $(T_A, T_C) = (1, 1)$, or $(T_A, T_D) = (1, 1)$, or $(T_B, T_C) = (1, 1)$, or $(T_B, T_D) = (1, 1)$. The two 1-out-of-2:G logic units are ANDed. The rods are then released from the magnets and dropped into the reactor core by gravity. This is a “de-energize to drop” principle.

2.2.5 Example: Risk-averse Safety Goal

Section 1.7 describes upper bound U and lower bound L of a tolerable risk region. Consider a case where these bounds are functions of the severities listed in Table 2.1. Frequency ratings are shown in Table 2.2.

Introduce a risk matrix where each column represents a severity rating, and each row denotes a frequency rating. Each cell in this hypothetical matrix is labeled as \bigcirc for unconditional acceptance, as \diamond for conditional tolerability, and as \times for unconditional rejection. A result is shown in Table 2.3. The term ALARP means that the risk level becomes tolerable in the conditional tolerability region if the risk can be justified (Section 1.7.2). Cost and availability of technology are major bases for this justification. We see from Table 2.3 that the conditional tolerability region for 1 fatality is the interval of annual frequencies $(10^{-4}, 10^{-2}]$.

Consider the expected number of fatalities for each lower bound L . The expected number is $1 \times 10^{-4} = 10^{-4}$ for the 1-fatality case, and $10 \times 10^{-6} = 10^{-5}$ for the 10-fatality case. Thus, the 10-fatality goal is more demanding than the 1-fatality case. The annual frequency decreases more rapidly than the one that yields a constant number of fatalities over different fatality consequences. This tendency of disliking a severe accident more severely than the expected value level is called a risk aversion (Section 1.8.2). The upper bound of Table 2.3 follows a constant, expected number of fatalities. This is called the risk-neutral preference.

2.2.6 Safety Integrity Level

Suppose that failure rate of 10^{-6} /year or approximately 10^{-10} /h is specified as a performance objective for a functional safety system. This is a strict requirement, and its manufacturer should reflect this objective in design and production.

Design, production and other activities should be varied according to the requirement level. This practice is symbolically expressed in terms of a safety integrity level (SIL) in standards IEC 61508 [1], IEC 61511 [11], EN 50126 [26], 50128 [27], and 50129 [28]. The SIL is determined from the failure rate or demand-failure probability required for a functional safety system.

Two types of failures are considered: random failure and systematic failure. The random failure can be quantified, while the systematic failure is difficult

Table 2.1. Example of severity rating of accident [25]

No	Rating	Consequence
IV	Insignificant	Minor injuries
III	Marginal	Major injuries
II	Critical	1 fatality
I	Catastrophic	10 fatalities
0	Disastrous	100 or more fatalities

Table 2.2. Example of frequency rating of accident [25]

Label	Rating	Annual frequency
A	Frequent	10^{-1}
B	Probable	10^{-2}
C	Occasional	10^{-3}
D	Remote	10^{-4}
E	Improbable	10^{-5}
F	Incredible	10^{-6}

Table 2.3. ALARP region designated as \diamond [25]

Annual frequency	Minor injuries	Major injuries	1 fatality	10 fatalities	100 fatalities
$10^{-1} < f \leq 10^{-0}$	\diamond	\times	\times	\times	\times
$10^{-2} < f \leq 10^{-1}$	\diamond	\diamond	\times	\times	\times
$10^{-3} < f \leq 10^{-2}$	\diamond	\diamond	\diamond	\times	\times
$10^{-4} < f \leq 10^{-3}$	\bigcirc	\diamond	\diamond	\diamond	\times
$10^{-5} < f \leq 10^{-4}$	\bigcirc	\bigcirc	\bigcirc	\diamond	\diamond
$10^{-6} < f \leq 10^{-5}$	\bigcirc	\bigcirc	\bigcirc	\diamond	\diamond
$10^{-7} < f \leq 10^{-6}$	\bigcirc	\bigcirc	\bigcirc	\bigcirc	\bigcirc

to quantify. Design and production are typical sources of systematic failures. Furthermore, the common-cause failures are frequently brought about by the systematic failures. Thus, special treatment in quality assurance is required to decrease the systematic failures for the functional safety system. IEC 61511 considers the SIL from the point of view of the process-industry users.

The SIL resembles the hotel star ranking. The manufacturer can provide functional safety systems graded by SIL. Users can use the safety system having a suitable grade. Functional safety systems are categorized according to the SIL, and the safety significance becomes apparent.

For a given SIL, the safety system is quantitatively evaluated for the random failures whether the system satisfies the SIL or not. To cope with systematic failures and unknown random failures, safety principles such as redundancy, diversity, failure detection, and others are applied to design, production, operation and maintenance. This is analogous to the probabilistic approach coupled with a deterministic one, as described in Regulatory Guide

1.174 for the nuclear power plant, *i.e.* risk-informed integrated decision making. This point will be described in more detail in this chapter and in Chapter 3.

Table 2.4 of EN 50126 defines the SIL for the railroad. IEC 61508 and IEC 61511 define the SIL as in Table 2.5. There are differences between these two table definitions.

Demand-failure probability is the probability of failure per demand when the safety system is demanded to operate. A safety belt should have a small demand-failure probability. The dangerous-failure rate is applicable to a high-demand case such as an automobile brake where its failure immediately leads to an accident.

IEC 61508 defines the “low-demand mode” as the case when the frequency of demands for operation is not greater than one per year and not greater than the proof-test frequency. The “high-demand or continuous mode” is the case where the frequency of demands is greater than one per year or greater than the proof-test frequency. These criteria come from a convention to calculate a demand-failure probability averaged over the proof-test interval for the low-demand mode (Section 3.9.2). The phrase “twice the proof-test frequency” in IEC 61508 is modified here.

The highest SIL of 4 indicates that the system is markedly dangerous and tremendous risk reduction is necessary. It is desirable to avoid the use of SIL 4 safety system. To implement the SIL 3 system, it is recommended to use a redundant system consisting of two or more SIL 2 systems. This redundancy can cope with the uncertainty except for dependencies such as common-cause failures. When a quantitative approach is used, Tables 2.4 and 2.5 are used to derive the SIL from the target demand-failure probability or the failure rate. On the other hand, when a qualitative approach is used, the SIL is first determined, and the quantitative numbers are obtained for demand probability or failure rate from the tables. These two types of approaches will be described more fully in this section.

2.2.7 Example: High-demand Mode

Consider an automatic train-protection (ATP) system of a hypothetical railroad [25]. The ATP operates in a high-demand mode in a similar way to a traffic signal. Assume, for simplicity, that the ATP failure yields 10% of the fatal accidents on this railroad. This assumption is used to allocate performance objectives to a variety of accidents of different origins.

The number of fatalities due to the ATP failure is relatively small as compared with railroad fire accidents; it is sufficient to consider two types of accidents with 1 and 10 fatalities, respectively. The demand always exists for the ATP. An ATP failure yields a 1 fatality accident with a percentage of 5%, a 10-fatality accident with the same 5%, and no accident with the remaining 90%. The ATP failure is temporal, and is repaired quickly.

Table 2.6 simply extracts upper and lower bound frequencies for the two accidents from Table 2.3.

Note that the bounds include contributions other than the ATP-oriented accidents. Thus, the annual frequencies for the ATP-oriented accidents must be one tenth of the values in Table 2.6. On the other hand, the ATP failure yields 1 and 10 fatality accidents with the same 5% probability. As a result, the frequencies in Table 2.6 should be multiplied by $0.1 \times 20 = 2$. The result is shown in Table 2.7. The ATP failure frequency is constrained by the lower bound for the 10-fatality accident. The unconditionally acceptable frequency value is 2×10^{-6} /year. The acceptable bound 2×10^{-6} /year becomes 2×10^{-10} /h when the unit changes from “year” to “hour”. The dangerous-failure rate of the ATP is 2×10^{-10} . Thus, the SIL is determined as 3 from Table 2.4.

Table 2.4. Definition of SIL by EN 50126 (railroad)

SIL	Per hour	Per demand
	failed-dangerous rate λ	failed-dangerous probability P
4	$(0, 10^{-10})$	$(0, 10^{-7})$
3	$[10^{-10}, 0.3 \times 10^{-8})$	$[10^{-7}, 10^{-6})$
2	$[0.3 \times 10^{-8}, 10^{-7})$	$[10^{-6}, 10^{-5})$
1	$[10^{-7}, 0.3 \times 10^{-5})$	$[10^{-5}, 10^{-4})$

Table 2.5. Definition of SIL by IEC 61508 and IEC 61511

SIL	Per hour	Per demand	Risk-reduction factor
	failed-dangerous rate λ	failed-dangerous probability P	
4	$[10^{-9}, 10^{-8})$	$[10^{-5}, 10^{-4})$	$(10\ 000, 100\ 000]$
3	$[10^{-8}, 10^{-7})$	$[10^{-4}, 10^{-3})$	$(1000, 10\ 000]$
2	$[10^{-7}, 10^{-6})$	$[10^{-3}, 10^{-2})$	$(100, 1000]$
1	$[10^{-6}, 10^{-5})$	$[10^{-2}, 10^{-1})$	$(10, 100]$

Table 2.6. Upper and lower bounds of ALARP region

Fatalities/ upper and lower	1 fatality	10 fatalities
U	10^{-2}	10^{-3}
L	10^{-4}	10^{-6}

Table 2.7. Upper and lower bounds of ATP failure frequency

Fatalities/ upper and lower	1 fatality	10 fatalities
ATP upper bound	2×10^{-2}	2×10^{-3}
ATP lower bound	2×10^{-4}	2×10^{-6}

Suppose that the railroad uses 20 identical ATP units. Thus, the failure rate of each unit must be $10^{-11}/\text{h}$ because the unit can cause the ATP failure. The SIL 3 indicates the safety-significance level of the ATP system. The unit supports the safety function of the ATP. Thus, each unit is categorized into the same safety-significance level as the parent system. This is similar to the approach for the nuclear power plant. Of course, the quality assurance would be more intensive if the ATP contains more units.

When the upper bound in Table 2.7 is used, the target failure-rate value of ATP becomes $2 \times 10^{-7}/\text{h}$. This is a maximum value of the conditional-tolerability region. The failure rate should be decreased until the ALARP principle can justify the cessation of risk reduction. Assume a criterion that 3 million dollars should be spent to save life. Then, the risk reduction continues until the failure rate reaches the broadly acceptable lower bound of $2 \times 10^{-10}/\text{h}$ or the further reduction requires cost exceeding the criterion.

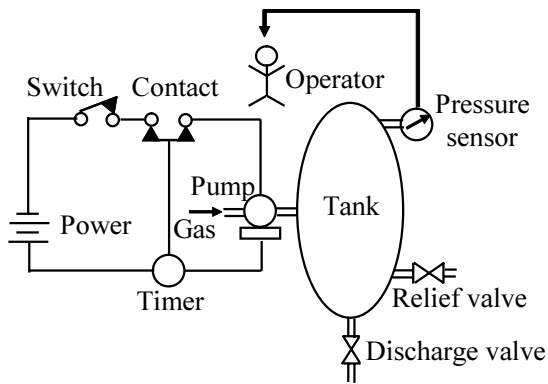


Fig. 2.2. Schematic of pressure-tank system

2.2.8 Semiquantitative Method using Subsidiary Objective

In the semiquantitative method the plant performance is evaluated quantitatively, while the consequence of an accident is assessed only qualitatively. The method is illustrated by the following example that is used throughout this chapter.

Pressure-tank Example

The system shown in Figure 2.2 pumps flammable gas from a reservoir into a pressure tank [29]. The switch is normally closed and the pumping cycle is initiated every month by an operator who manually resets the timer. The timer contact closes and pumping starts. Well before any overpressure condition exists the timer times out and the timer contact opens. Current to the pump

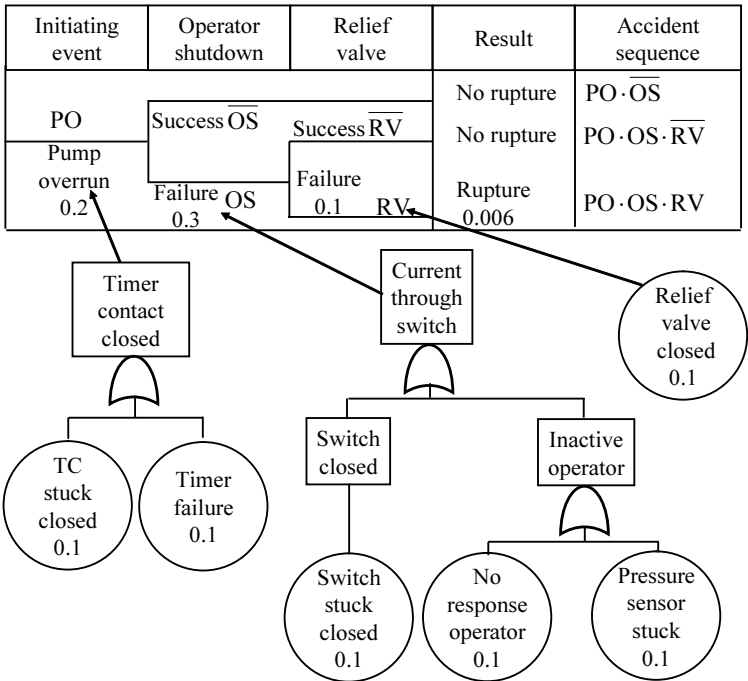


Fig. 2.3. Event tree coupled with fault trees

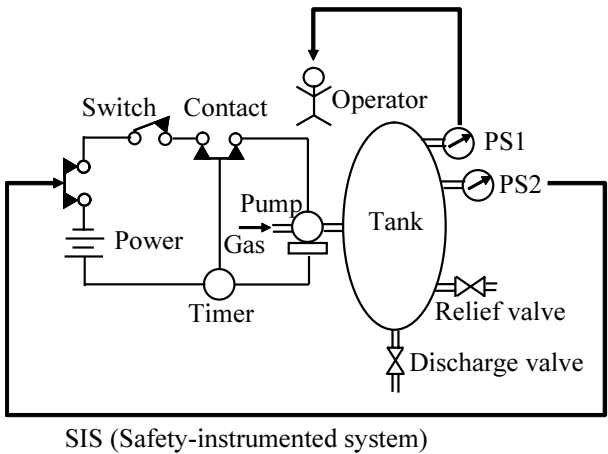


Fig. 2.4. Pressure-tank system with additional SIS

cuts off and pumping ceases (to prevent a tank rupture due to overpressure). This timer system can be regarded as a basic process-control system (BPCS) shown in Figure 1.7. This terminology of BPCS originates from IEC 61511.

The failure of the BPCS causes an initiating event labeled as “pump overrun” that has a potential leading to a flammable gas release to the environment via the tank rupture. The BPCS does not perform any safety functions. Its failure contributes to the occurrence of the initiating event. As shown in Figure 2.3, the initiating event is assumed to occur with a frequency of 0.2/year according to a rare-event approximation (Section 7.6.5) because the two basic events “Timer contact stuck closed” and “Timer failure” occurs with frequencies 0.1/year, respectively. Other initiating-event candidates are leaks from process equipment, pipe ruptures, and external events such as earthquakes.

If the timer contact does not open due to the BPCS failure, the operator is instructed to respond to the pressure-sensor alarm and to open the manual switch, thus causing the pump to stop. This is a process-monitoring system, a type of protection layer shown in Figure 1.7. The process-monitoring system fails with probability 0.3 as shown in Figure 2.3.

Even if the timer and operator both fail, overpressure can be relieved by the relief valve, a type of noninstrumented, mechanical protection shown in Figure 1.7. Releases from the relief valve are piped to a flare system whose failures are not considered for simplicity of description. As shown in Figure 2.3 this noninstrumented protection fails with probability of 0.1.

Other types of noninstrumented protection are the structural protection shown in Figure 1.7. A dyke is an example of the structural protection. For the flammable gas released by the tank-rupture event, the dyke is not a good measure for risk reduction.

Before the start of each cycle, the tank is emptied by opening the discharge valve to dump the residual gas. This valve is then closed. The operator is instructed to observe the pressure sensor to confirm the depressurized tank. Note that the pressure sensor may fail before the new cycle. An undesired event, from a risk viewpoint, is a pressure-tank rupture by overpressure.

Figure 2.3 shows the event tree and fault tree for the pressure-tank rupture due to overpressure. The event tree starts with an initiating event that initiates the accident sequence. The tree describes combinations of success or failure of the system’s mitigative features that lead to desired or undesired plant states.

In Figure 2.3, PO denotes the event “pump overrun,” the first type of initiating event that starts the potential accident scenarios. The second type is the tank discharge failure before the start of the cycle. This initiating event will be described later.

Symbol OS denotes the failure of the operator shutdown system, PP denotes failure of the pressure-protection system by relief-valve failure. The overbar indicates a logic complement of the inadvertent event, that is, successful activation of the mitigative feature. There are three sequences or scenarios displayed in Figure 2.3. The scenario labeled PO·OS·PP causes overpressure and tank rupture, where symbol “·” denotes the logic intersection, (AND).

Therefore the tank rupture requires three simultaneous failures. The other two scenarios lead to safe results.

The event tree defines top events, each of which can be analyzed by a fault tree that develops more basic causes such as hardware or human faults. We see, for instance, that the pump overrun is caused by timer-contact failure stuck closed, or timer failure. By linking the three fault trees (or their logic complements) along a scenario on the event tree, possible causes for each scenario can be enumerated.

For instance, tank rupture, the most dangerous scenario, occurs when the following three basic causes occur simultaneously: 1) timer contact stuck closed, 2) switch stuck closed, and 3) pressure relief closed. Probabilities for these three causes can be estimated from generic or plant-specific statistical data, and eventually the probability of the tank rupture due to the initiating event of pump overrun can be quantified.

SIL for Demand Mode SIS

A tolerable frequency of the tank-rupture event may be specified by reflecting

- 1) national and international standards and regulations,
- 2) corporate policies, and
- 3) community, local jurisdiction and insurance companies.

The rupture frequency in the current example is 0.006/year for the first initiating event, as shown in Figure 2.3. The tank rupture is a hazardous event, the term being defined in Section 2.2.1. Assume a tolerable frequency of 10^{-4} /year, considering the large release of flammable gas into the environment following the rupture. This frequency has a similar role to the subsidiary CDF objectives for the nuclear power plant. The approach is called semiquantitative because the frequency of the tank rupture is evaluated quantitatively, while its consequence is assessed only qualitatively. Moreover, the subsidiary LERF objective is not considered for the tank-rupture problem without a containment.

Assume that inherently safe designs such as replacing the flammable gas by a nonflammable one have already been reviewed. The process-monitoring system and relief valves are implemented. The structural protection such as containment is not feasible for the current case.

The last measure is the SIS shown in Figure 2.4. This consists of a new pressure sensor, a logic solver, and a new relay contact. The SIS opens the contact when high pressure is detected. This is an automated version of the process-monitoring system relying on the operator.

Note that the sharing of the same pressure sensor between the process-monitoring system and the SIS would introduce dependency. When the pressure sensor fails to alarm the high pressure, the sensor also fails to detect the high pressure for the SIS. A similar dependency would be introduced when the same switch is shared between the process-monitoring system and the SIS, or the same contact between the BPCS and the SIS.

If the operator fails to depressurize the tank before the cycle begins, then the timer BPCS fails because the initial tank pressure is sufficiently high. The depressurization failure thus becomes another initiating event that has the two causes: 1) operator depressurization error (omission), and 2) pressure-sensor failure (stuck low). The operator incorrectly thinks that the tank has been emptied when the pressure sensor fails in stuck-low mode. Even if the pressure sensor indicates the correct high pressure, the operator may forget the depressurization (omission). The minimal cut sets of the initiating event coupled with the failure of the process-monitoring system are:

- 1) {operator discharge failure, operator no response}
- 2) {pressure sensor stuck low}
- 3) {operator discharge failure, switch stuck closed}

Table 2.8 summarizes the components of the pressure-tank system. The above minimal cut sets can be expressed as: 1) {OP0, OP1}, 2) {PS1}, and 3) {OP0, SW}. Note that the pressure-sensor failure is a single-event cut set (*i.e.* system-failure mode, Section 7.4) for the initiating event along with the BPCS failure. The initiating-event frequency is approximated by the sum of cut set frequencies: $0.01 + 0.1 + 0.01 = 0.12/\text{year}$.

Table 2.8. Component list of pressure-tank system

Label	Description	Failure mode	Prob.	Frequency
OP0	Operator	Discharge failure		0.1/year
C1	Contact 1	Stuck closed		0.1/year
TM	Timer	Failure		0.1/year
SW	Switch	Stuck closed	0.1	
OP1	Operator	No response	0.1	
PS1	Pressure sensor 1	Stuck low	0.1	0.1/year
RV	Relief valve	Stuck closed	0.1	
SIS	SIS	Failure	0.005	

The demand rate to the relief valve is thus 0.12/year. The relief valve fails with probability 0.1. The demand to SIS becomes 0.012/year. The total demand to SIS from the two types of initiating events becomes $0.006 + 0.012 = 0.018$, and the SIS must have a risk-reduction factor of $1.8 \times 10^{-2}/10^{-4} = 180 \simeq 200$ in order to satisfy a tolerable frequency of 10^{-4} , resulting in SIL 2 SIS from Table 2.5.

2.2.9 Layer of Protection Analysis

An example of layer of protection analysis (LOPA) is shown in Table 2.9. This portion of LOPA is similar to the semiquantitative method described in the last section, except for the tabular format. LOPA, however, considers consequences, as described shortly.

Table 2.9. Layer of protection analysis table

1	2	3	4	5	6	7	8	9	10	11
	Hazardous event		Initiating event		BPCS	Protection layers without SIS			PLs with SIS	
	Consequence	Severity	Initiator	Initiator likelihood	BPCS	Monitoring system	Relief valve	Likelihood without SIS	SIS risk reduction	Likelihood with SIS
1	Fire from tank rupture	S	BPCS failure	0.2		0.3	0.1	0.006	0.005	0.00003
2	Fire from tank rupture	S	Discharge failure	0.12			0.1	0.012	0.005	0.00006

Table 2.10. Severity ratings of safety-layer matrix, LOPA, and risk graph

Safety-layer matrix	LOPA	Risk graph
Hazardous event severity	Impact event severity levels	Consequence on person and environment
Minor: Minor damage to equipment. No shutdown of the process. Temporary injury to personnel and damage to the environment.	Minor: Impact initially limited to local area of event with potential to broader consequence, if corrective action not taken.	C₁: Light injury to persons. A release with minor damage that is not very severe but is large enough to be reported to plant management.
Serious: Damage to equipment. Short shutdown of the process. Serious injury to personnel and the environment.	Serious: Impact event could cause serious injury or fatality on site or offsite.	C₂: Serious permanent injury to one or more persons; death of one person. Release within the fence with significant damage.
Extensive: Large-scale damage of equipment. Shutdown of a process for a long time. Catastrophic consequence to personnel and the environment.	Extensive: Impact event that is five or more times severe than a serious event.	C₃: Death of several persons. Release outside the fence with major damage that can be cleaned up quickly without significant lasting consequences.
		C₄: Catastrophic effect, many people killed. Release outside the fence with major damage that cannot be cleaned up quickly or with lasting consequences.

Each row of Table 2.9 starts with a hazardous event yielding a consequence with a severity level. By the LOPA terminology, the consequence is called an impact event. The severity-level classification is shown in the “LOPA” column of Table 2.10. For the current case, the severity is labeled as “Serious (S)”.

There are two initiating events leading to the consequence. Both of the initiating-event likelihoods are “High”. As a matter of fact, the BPCS failure has the initiator likelihood of 0.2/year, while the depressurization failure has the likelihood of 0.12/year.

Note that the BPCS-failure initiating-event can not be dealt with by the BPCS. This initiator can be dealt with the process-monitoring system and the relief valve. Thus, the likelihood of the hazardous event without an SIS is 0.006/year for the first initiating event.

The BPCS cannot deal with the second initiator, depressurization failure, because the time-out mechanism is too late for the pressurized tank at the startup time. There is a shared-component dependency via the pressure sensor between the initiator and the process-monitoring system. Thus, the demand frequency to the relief valve must be evaluated by a combined system of initiator and the process-monitoring system. The minimal cut sets were already shown. It was determined that the demand frequency to the relief valve was 0.12/year. This frequency is shown in Table 2.9. The hazardous event likelihood without SIS is 0.012/year.

The SIS risk-reduction factor is specified as 200, *i.e.* the SIS demand-failure probability is 0.005. This is SIL 2. This reflects the event likelihoods without the SIS, and the consequence severity. The resulting likelihoods for the two initiating events are 0.00003 and 0.00006, respectively. The total likelihood of the consequence is 0.00009, which is judged tolerable by the analyst of the pressure-tank example system. Recall that the tank-rupture likelihood has a similar role to the CDF.

Now let us consider a consequence analysis. The fatality frequency due to fire is calculated by:

$$FF = RF \times PI \times PE \times PF \quad (2.1)$$

where

- 1) FF: Fatal frequency due to the fire.
- 2) RF: Frequency of flammable material release. This frequency is the tank-rupture frequency, 0.00009/year for the current example.
- 3) PI: Probability of ignition. The tank area has explosion-proof equipment, and the electrical equipment maintenance follows the guidance for ignition reduction. No transfer of ignition from other areas. The ignition probability is determined as 0.1.
- 4) PE: Probability of a person in the tank area. This is estimated as 0.1.
- 5) PF: Probability of fatality by fire. This is estimated as 50%.

The fatality frequency due to fire becomes:

$$FF = 0.00009 \times 0.1 \times 0.1 \times 0.5 = 4.5 \times 10^{-7}/\text{year} \quad (2.2)$$

This frequency is judged to satisfy the company's quantitative health objective for a single fatality by the flammable material. When the tank contains toxic gas the fatality frequency due to the toxic release must be evaluated too.

The subsidiary CDF objective avoids this type of consequence analysis because considerable uncertainties may exist, for instance, in estimating the probability of ignition, the probability of a person in the area, and the probability of fatality by fire.

Table 2.11. Frequency ratings of safety-layer matrix, LOPA, and risk graph

Safety-layer matrix	LOPA	Risk graph
Hazardous event likelihood	Initiation likelihood	Demand frequency
Low: Events such as multiple failures of diverse instruments or valves, multiple human errors in a stress free environment, or spontaneous failures of process vessels.	Low: A failure or series of failures with a very low probability of occurrence within the expected lifetime of the plant. $f < 10^{-4}$ /year. Examples: 1) Three or more simultaneous instrument, or human failures. 2) Spontaneous failure of single tanks or process vessels.	W₁: A very slight probability that the unwanted occurrences occur and only a few unwanted occurrences are likely. $f < 0.1$ /year
Medium: Events such as dual instrument, valve failures, or major releases in loading/unloading areas.	Medium: A failure or series of failures with a low probability of occurrence within the expected lifetime of the plant. $10^{-4} \leq f < 10^{-2}$ /year. Examples: 1) Dual instrument or valve failures. 2) Combination of instrument failures and operator errors. 3) Single failures of small process lines or fittings.	W₂: A slight probability that the unwanted occurrences occur and a few unwanted occurrences are likely. $0.1 \leq f < 1$ /year
High: Events such as process leaks, single instrument, valve failures or human errors that result in small releases of hazardous materials.	High: A failure can reasonably be expected to occur within the expected lifetime of the plant. $10^{-2} \leq f$ /year. Examples: 1) Process leaks. 2) Single instrument or valve failures. 3) Human errors that could result in material releases.	W₃: A relatively high probability that the unwanted occurrences occur and frequent unwanted occurrences are likely. $1 \leq f < 10$ /year

2.2.10 Safety-layer Matrix

The safety-layer matrix is shown in Figure 2.5. The labels a, b, and c in this figure indicate the following remarks.

- 1) a: One SIL 3 safety-instrumented function does not provide sufficient risk reduction. Additional modifications are required in order to reduce risk.
- 2) b: One SIL 3 safety-instrumented function may not provide sufficient risk reduction. An additional review is required.
- 3) c: SIS independent layer is probably not needed.

The PLs in the third axis are defined as all the PLs protecting the process including the SIS being classified. This matrix does not consider SIL 4 SIS.

The severities of a hazardous event without considering PLs are defined in the “safety-layer matrix” column of Table 2.10. The tank rupture and the resulting release of flammable material and the potential fire can be regarded as large-scale damage of equipment, shutdown of a process for a long time,

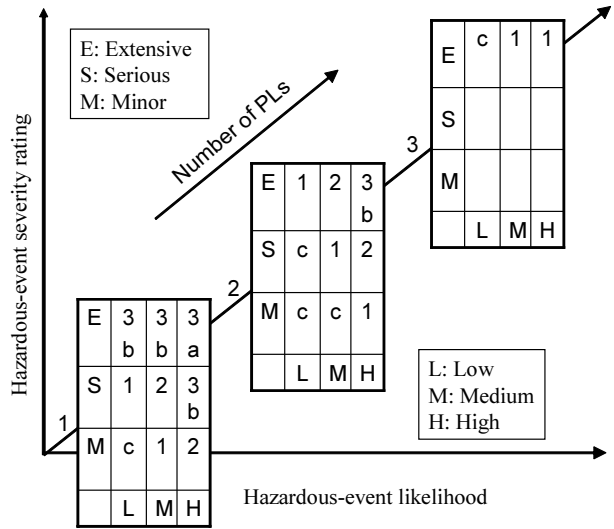


Fig. 2.5. Safety-layer matrix consisting of dimensions of likelihood, severity, and protection layers

and catastrophic consequence to personnel and the environment. Thus the severity rating is classified as “Extensive”.

The original design of the pressure-tank system has two PLs: 1) process-monitoring system, and 2) relief valve. The frequency of hazardous-event likelihood without considering PLs is defined in the “safety-layer matrix” column of Table 2.11. The frequency of a hazardous event becomes the initiating-event frequency, *i.e.* failure frequency 0.2/year for the BPCS initiating event and 0.12/year for the discharge-failure initiating-event. The hazardous-event likelihood is labeled as “High”. This labeling, of course, should be performed without the quantitative information about the initiating-event frequency. We cite the number only to illustrate the approach.

The pressure-tank system has 3 PLs including the SIS for the first initiating event. IEC 61511 requires that each PL should reduce at least the hazardous event by a factor of 10. In this sense, the process-monitoring system is not a PL because its risk-reduction factor is $1/0.2 = 5$. Thus, the number of PLs decreased to 2.

The system has only 2 PLs for the second initiating event because the monitoring system has a strong dependency on the discharge failure via the shared pressure sensor. The number of PLs is conservatively estimated again as 2 in Figure 2.5.

The cell at “E” row and “H” column shows that the SIS should be a SIL 3 safety-instrumented system. This is higher than the SIL 2 result of the LOPA.

Table 2.12. Risk graph consisting of consequence, exposure, avoidance, and demand frequency

Case number		1	2	3	4	5	6	7	8	9	10	11	12	13
Consequence severity		C_1	C_2				C_3				C_4			
Personnel exposure			F_1		F_2		F_1		F_2		F_1		F_2	
Possibility of avoidance			P_1	P_2	P_1	P_2	P_1	P_2	P_1	P_2	P_1	P_2	P_1	P_2
Demand frequency	W_1	–	–	a	a	1	a	1	1	2	1	2	2	3
	W_2	–	a	1	1	2	1	2	2	3	2	3	3	4
	W_3	a	1	2	2	3	2	3	3	4	3	4	4	b

2.2.11 Risk Graph

A risk graph is shown in Table 2.12. The labels “–”, “a”, “b” and numbers 1 to 4 in this table indicate the following remarks.

- 1) –: No safety requirements.
- 2) a: No special safety requirements.
- 3) b: A single SIS is not sufficient.
- 4) 1, 2, 3, and 4: Safety integrity levels.

The numbers associated with labels C , F , and P can be regarded as scores. It turns out that the total score determines the 3-dimensional column vector, where W_1 , W_2 , and W_3 correspond to the first, second, and third dimension, respectively. For instance, (C_2, F_2, P_2) , (C_3, F_1, P_2) , and (C_4, F_1, P_1) result in the same vector (1, 2, 3).

The risk graph assumes first that no SIS is in place except for BPCS, monitoring systems and relief valves for the pressure-tank example.

There are two types of initiating events: 1) timer BPCS failure, and 2) operator discharge error. The frequency of tank rupture without the SIS was 0.018/year, as was shown in Table 2.9. The frequency is less than 0.1, and is labeled as W_1 from the “risk graph” column of Table 2.11. The consequence is evaluated as C_3 from the column of Table 2.10.

The frequency of human presence in the hazardous zone multiplied by the exposure time is rated as follows.

- 1) F_1 : Rare to frequent exposure in the hazardous zone.
- 2) F_2 : Frequent to permanent exposure in the hazardous zone.

For the pressure-tank system, access to the tank area is restricted for workers and public. Online maintenance is not performed. Thus, the frequency of human presence is labeled as F_1 .

The possibility of avoiding the consequences of the hazardous event is rated as follows:

- 1) P_1 : Possible under certain conditions.
- 2) P_2 : Almost impossible.

The factors to be considered for determining the avoidance possibility rating are [11]:

- 1) Operation of a process is supervised or unsupervised. The supervision means operation by both skilled and unskilled persons.
- 2) Speed of development of hazardous event. For example, suddenness, quickness, or slowness.
- 3) Ease of recognition of danger such as (1) being recognized immediately, (2) being detected by technical measures, or (3) being detected without technical measures.
- 4) Ease of avoidance from hazardous event. For example, (1) escape routes possible, (2) not possible, or (3) possible under certain conditions.
- 5) Actual safety experience. Such experience may exist for an identical process or for a similar process or they may not exist.

For the pressure-tank system, the rupture occurs so rapidly, the avoidance possibility is labeled as P_2 , *i.e.* almost impossible. The combination of C_3 , F_1 , P_2 , and W_1 yields SIL 1 SIS. If the frequency is F_2 in Table 2.10, then the SIL would increase to 2.

2.2.12 Category for Machinery Safety: EN 954

Consider, for instance, a driverless vehicle that moves at low speeds (3.5 km/h) along a specified route in a factory [23]. A categorization by a risk graph from BS EN 954-1 [30] is shown in Figure 2.6.

A pedestrian may be seriously and irreversibly injured (S2) when a collision occurs because the vehicle carries a heavy load. The pedestrian is continuously exposed (F2) to the hazard because they have free access to the vehicle's route. The hazard avoidance is possible (P1) because of the low speed of the vehicle. The collision-prevention safety system turns out to have category 3, as shown by the thick lines in Figure 2.6.

Definitions of categories B, 1, 2, 3 and 4 are given in Table 2.13. Categories B and 1 are mainly characterized by the selection of components, while categories 2 to 4 are by the structure.

The BS EN 954-1 is qualitative and much easier to use than the IEC 61508 that tends to be quantitative to deal with statistical data such as mean time to dangerous failure and a so-called diagnostic coverage (Section 3.7). A revised version of BS EN 954-1 is ISO 13849-1. The EN 954 does not address the software used for PLCs.

A correspondence between SIL and the EN 954 category is shown in Table 2.14 [23, 24].

2.3 SSC Categorization Guideline: NEI 00-04

This section describes a categorization process NEI 00-04 proposed by the US Nuclear Energy Institute in 2004 [18]. We will see, for instance, that the risk-reduction factor is simply an importance measure called a "risk-achievement worth (RAW)" used for the SSC categorization.

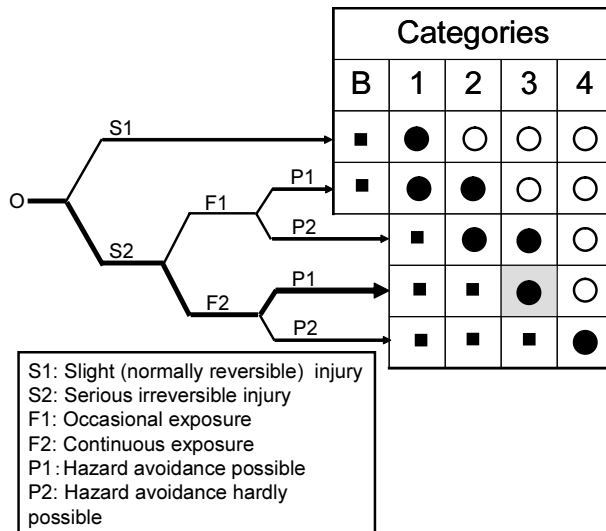


Fig. 2.6. Risk graph for categorizing safety function for machinery

2.3.1 Safety-related SSCs

The design of nuclear power plant ensures that 1) the reactor can be shut down quickly to stop the reaction, 2) the core can be cooled reliably, *and* 3) all radioactive material remains contained within the passive barriers such as reactor-coolant pressure boundary or containment structure [19].

Safety-related SSCs mean those that are relied upon to remain functional during and following design basis events to assure [31]:

- 1) The capability to shut down the reactor and maintain it in a safe shutdown condition,
- 2) The integrity of the reactor-coolant pressure boundary, *or*
- 3) The capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures.

Consider as an illustrative example the improved version of the pressure-tank system of Figure 2.4 where a SIS is introduced. The components were listed in Table 2.8. All the components other than the timer and the timer contact are safety related because they are relied upon to remain functional to deal with the initiating event. This is obvious from the deterministic behavior of the pressure-tank system. It is intuitively seen that pressure sensor (PS1) is more safety significant than switch (SW) because the sensor not only protects the tank by sensing the overpressure but also its failure causes an initiating event, *i.e.* operator discharge failure.

Table 2.13. Definition of categories

Cat.	Requirements in brief	System behavior
B	Components of safety-related control systems must be designed, constructed, selected, assembled and combined in accordance with the relevant standards such that they can withstand the expected influence.	The occurrence of a fault can lead to the loss of the safety function.
1	The requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function, but the probability of occurrence is lower than in category B.
2	1) The requirements of B and the use of well-tried safety principles shall apply. 2) The safety function shall be checked at suitable intervals by the machinery control system.	The loss of the safety function is detected by the check. The occurrence of a fault can lead to the loss of the safety function between the checks.
3	1) The requirements of B and the use of well-tried safety principles shall apply. 2) Safety-related components shall be designed such that: 2-1) a single fault in any of these components does not lead to the loss of the safety function, and 2-2) the single fault is detected whenever reasonably practicable.	1) If the single fault occurs, the safety function is still maintained. 2) Some but not all faults are detected. 3) Accumulation of undetected faults can lead to the loss of the safety function.
4	1) The requirements of B and the use of well-tried safety principles shall apply. 2) Safety-related components shall be designed such that: 2-1) a single fault in any of these components does not lead to the loss of the safety function, and 2-2) the single fault is detected during or prior to the next demand on the safety function, or, if this is not possible, an accumulation of faults should not as a result lead to the loss of the safety function.	If faults occur, the safety function is still maintained. Faults are detected in good time to prevent the loss of safety function.

2.3.2 Quality-assurance Program

Because of the importance of the safety-related equipment to protecting public health and safety, the quality-assurance (QA) program (described in Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants,” to 10 CFR Part 50) is applied to all activities affecting the safety-related functions of that equipment. These activities range over

Table 2.14. Correspondence between SIL of IEC 61508 and category of EN 954-1

Category	SIL	Remarks
B	-	State-of-the-art safety-related control systems
1 or 2	1	Discrete time periodic testing
3	2	Single-failure criteria with partial fault detection
4	3	Continuous self-monitoring
-	4	Not typical in machinery protection

designing, purchasing, fabricating, handling, shipping, storing, cleaning, erecting, installing, inspecting, testing, operating, maintaining, repairing, refueling, and modifying.

Here, the quality assurance is defined to comprise all those planned and systematic actions necessary to provide adequate confidence that a SSC will perform satisfactorily in service.

The Appendix B, for instance, states the following actions for instructions, procedures, and drawings: “Activities affecting quality shall be prescribed by documented instructions, procedures, or drawings, of a type appropriate to the circumstances and shall be accomplished in accordance with these instructions, procedures, or drawings. Instructions, procedures, or drawings shall include appropriate quantitative or qualitative acceptance criteria for determining that important activities have been satisfactorily accomplished.”

The QA program follows a PDCA cycle: 1) assuring that an appropriate quality-assurance program is established and effectively executed and 2) verifying, such as by checking, auditing, and inspection, that activities affecting the safety-related functions have been correctly performed.

2.3.3 Safety-significance Categorization

The 10 CFR Part 50 recognizes that the QA program should be applied in a manner consistent with the importance to safety of the associated plant equipment. In the past, engineering judgment provided the general mechanism to determine the relative importance to safety of plant equipment [32].

Insights from PRAs have revealed that certain plant equipment important from a deterministic point of view is of little significance to safety. Conversely,

Table 2.15. Risk-informed safety classifications by NEI 00-04 categorization process

	Safety related	Nonsafety related
High safety significant	RISC-1	RISC-2
Low safety significant	RISC-3	RISC-4

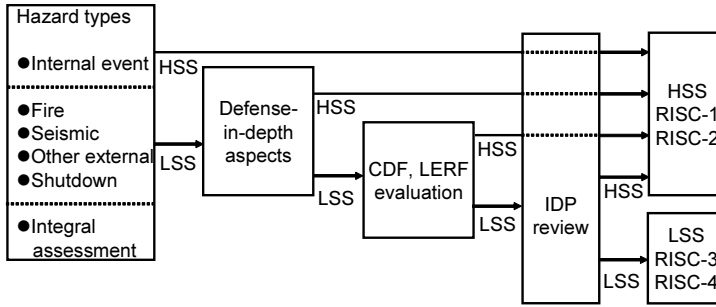


Fig. 2.7. NEI 00-04 categorization process into HSS and LSS

certain plant equipment turns out to be significant to safety but is not classified as a safety-related SSC.

As a consequence, Section 50.69 of 10 CFR Part 50 titled as “Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors” has come to give the following definitions where RISC is the abbreviation of risk-informed safety class:

- 1) RISC-1 SSCs means safety-related SSCs that perform (high) safety-significant (HSS) functions.
- 2) RISC-2 SSCs means nonsafety-related SSCs that perform (high) safety-significant functions.
- 3) RISC-3 SSCs means safety-related SSCs that perform low safety-significant (LSS) functions.
- 4) RISC-4 SSCs means nonsafety-related SSCs that perform low safety-significant functions.

These four classes are shown in Table 2.15 [18]. A low safety-significant SSC, for instance, may have availability 2 or 5 times larger than a high safety-significant SSC in evaluating CDF or LERF.

Qualitative Criteria for High Safety-significance

The concept of high safety significance can be best illustrated by qualitative criteria used by NEI 00-04 to make a categorization not by PRAs but by screening tools. The qualitative criteria result in more conservative categorization. In other words, more SSCs are identified as high safety significant.

- 1) All SSCs that are involved in the mitigation of any unscreened scenario are identified as safety significant. Containment challenges include bypass events such as interfacing systems loss of coolant accident (ISLOCA) and steam generator tube rupture (SGTR). Operator action to isolate the ISLOCA is considered safety significant. A strategy during an SGTR event is the depressurization of primary and secondary systems and the equalization of pressures between primary and secondary. These all help to limit the leakage and are safety significant [13].

- 2) All screened scenarios are reviewed to identify any SSCs that would result in a scenario being unscreened, if that SSC was not credited. This review assures that the SSCs that were required to maintain low risk are retained as safety significant. For instance, a tank rupture due to tank defects may be screened out due to an inherently high reliability of the pressure tank. For potentially high-consequence events, even if the event frequency is below a screening criterion, the features that lead to the frequency being low (for example, surveillance test practices, startup procedures) are safety significant [9].
- 3) When multiple SSCs are available to satisfy the safety function, only SSCs that support (1) the primary method and (2) the first alternative method to satisfy the function are considered to be safety significant. Assume that the SIS of the pressure-tank system consists of three independent trains. Then, trains 1 and 2 are considered to be safety significant.
- 4) When a SSC failure would initiate a shutdown event, then it is safety significant. The stuck-closed timer contact initiates the pump shutdown, and this contact is safety significant.
- 5) Failure of the SSC may compromise the reactor-coolant pressure boundary or containment integrity. These SSCs are safety significant.
- 6) Failure of the SSC will directly fail another safety-significant SSC, including SSCs that are assumed to be inherently reliable (*e.g.*, piping and tanks) and SSCs that may not be explicitly modeled (*e.g.*, room-cooling systems). These SSCs are safety significant.
- 7) The SSC is necessary for safety-significant operator actions credited. An example is instrumentation equipment. The pressure-sensor failure directly leads to the operator-discharge failure. Thus, the pressure sensor is safety significant for the pressure-tank system.
- 8) The SSC is necessary for safety-significant operator actions to assure long-term containment integrity or offsite emergency planning activities.

If none of the above conditions is true, low safety significance can be assigned, if the following condition is met:

- 1) Historical data show that these failure modes are unlikely to occur and such failure modes can be detected and mitigated in a timely fashion, or
- 2) A condition-monitoring program would identify the degradation of the SSC prior to its failure.

Risk-informed Categorization

PRA provides insights that may be utilized to support the determination of the relative safety significance of plant SSCs. The probabilistic insights help identify low safety-significant SSCs that are candidates for reductions in QA treatment. The QA is graded commensurately with these categorizations [32].

The principles for categorizing SSCs are [18]:

- 1) Use applicable risk-assessment information. The categorization is thus risk informed.

- 2) The categorization process should employ a blended approach considering both quantitative PRA information and qualitative information. The process is called an integrated decision making panel (IDP). There should be at least five experts as members of the IDP in the fields of: (1) plant operations, (2) design engineering (including safety analyses), (3) systems engineering, (4) licensing, and (5) PRA.
- 3) The Regulatory Guide 1.174 principles of the risk-informed approach to regulations should be maintained.
- 4) A safety-related SSC will, as a default, be categorized as RISC-1 unless a basis can be developed for recategorizing it as RISC-3.
- 5) Attribute(s) that make a SSC safety significant should be documented.

Table 2.16. Example importance summary

Component-failure mode	FV	RAW	CCF RAW
1) Valve “A” fails to open	0.002	1.7	n/a
2) Valve “A” fails remain closed	0.00002	1.1	n/a
3) Valve “A” in maintenance (closed)	0.0035	1.7	n/a
4) Common-cause failure of valves “A”, “B” and “C” to open	0.004	n/a	54
5) Common-cause failure of valves “A” and “B” to open	0.0007	n/a	5.6
5) Common-cause failure of valves “A” and “C” to open	0.0006	n/a	4.9
Component importance	0.01082	1.7	54
	(sum)	(max)	(max)
Criteria	> 0.005	> 2	> 20
Candidate safety significant?	Yes	No	Yes

2.3.4 Internal Event Assessment Example

Redundant-valve Example

Consider an example in reference [18]. The importance-measure criteria used to identify candidate safety significance are:

- C1) Sum of FV (Fussell–Vesely) importance values for all basic events modeling the SSC of interest, including common-cause events > 0.005.
- C2) Maximum of component basic event RAW (risk-achievement worth) values > 2.
- C3) Maximum of applicable common-cause basic events RAW values > 20.

The importance measures are defined and discussed in NUREG/CR-3385 [33] and [29]. See Equations 2.3 and 2.4.

Three failure modes are considered for valve “A”: 1) failure to open, 2) failure to close, 3) closed by maintenance. Common-cause failure (CCF) events

(failures to open) are considered for the three sets of valves including valve “A”: 1) “A”, “B” and “C”, 2) “A” and “B”, and 3) “A” and “C”. These sets are called common-cause component groups (Section 8.2.2).

The FV condition C1 is met because $0.01082 > 0.005$. The CCF RAW condition C3 is also satisfied for common-cause group “A”, “B” and “C”: $54 > 20$. The three valves would be identified as candidate HSS.

Attribute(s) that make a SSC safety significant should be documented. The component-failure mode dominating the screening criteria is failure to open. This mode is used as a safety-significant attribute.

Table 2.17. Minimal cut sets of pressure-tank system

1	2	3	4	5	6	7
No.	Minimal cut	Freq./year	FV PS1	RAW PS1	FV C1	RAW C1
1	{C1,SW,RV,SIS}	0.000005	col 3	col 3	col 3	0.00005
2	{C1,OP1,RV,SIS}	0.000005		col 3	col 3	0.00005
3	{C1,PS1,RV,SIS}	0.000005		0.00005	col 3	0.00005
4	{TM,SW,RV,SIS}	0.000005		col 3		col 3
5	{TM,OP1,RV,SIS}	0.000005	col 3	col 3		col 3
6	{TM,PS1,RV,SIS}	0.000005		0.00005		col 3
7	{OP0,SW,RV,SIS}	0.000005		col 3		col 3
8	{OP0,OP1,RV,SIS}	0.000005	col 3	col 3		col 3
9	{PS1,RV,SIS}	0.00005		0.0005		col 3
Total		0.00009	0.00006	0.00063	0.000015	0.000225

Table 2.18. Summary of FV and RAW importance for pressure sensor, relay contact and switch

Description	FV	RAW
PS1 (Stuck low)	$\frac{0.00006}{0.00009} = 0.66$	$\frac{0.00063}{0.00009} = 7$
C1 (Stuck closed)	$\frac{0.000015}{0.00009} = 0.16$	$\frac{0.000225}{0.00009} = 2.5$
SW (Stuck closed)	0.16	2.5

Pressure-tank Example

A calculation process of FV importance and RAW is shown in Table 2.17 for the pressure-tank problem. Column 2 enumerates minimal cut sets. Column 3 gives the annual frequencies of the cut sets. Each cut set frequency

is calculated by a product of a cut set component frequency multiplied by probabilities. The bottom row is the total to give the frequency of the tank rupture.

Column 4 indicates the minimal cut sets containing component PS1, the first pressure sensor. The bottom row shows the total frequency when the summation is restricted to these 3 minimal cuts. It turns out that the FV importance of PS1 is $0.00006/0.00009 = 0.66$, as shown in Table 2.18.

Column 5 shows the cut set frequencies when PS1 fails, *i.e.* its failure probability or frequency is set to unity. Only cut sets 3, 6 and 9 are affected. The total is the tank-rupture frequency when PS1 is being failed (or *not used*). The RAW thus becomes $0.00063/0.00009 = 7$. This means that the risk-reduction factor of PS1 is 7. The RAW value turns out to be a risk-reduction factor used in IEC 61508 and 61511.

FV and RAW measures for contact C1 can be calculated in a similar way. It is easily examined from Table 2.17 that switch SW would have the same FV and RAW as contact C1. These results are summarized in Table 2.18.

The three components PS1, C1, and SW are high safety significant (HSS) according to the criteria just mentioned: FV larger than 0.005 or RAW larger than 2 for independent failures. Note that contact C1 of the timer system is not safety related but HSS because the contact failure may cause the first initiating event, *i.e.* pump overrun.

A SSC is not automatically low safety significant even if the risk importance measure criteria are not met, It must go through checks by other types of PRAs, defense-in-depth assessment, CDF and LERF impact evaluation and IDP review, as shown in Figure 2.7. The CDF and LERF evaluation is called “Sensitivity studies” by the NEI 00-04 document, which may be confused with the ordinary sensitivity studies described next.

Sensitivity Studies

The NEI 00-04 recommends sensitivity studies for internal events PRA:

- 1) Increase all human-error basic events to their 95th percentile values.
- 2) Decrease all human-error basic events to their 5th percentile values.
- 3) Increase all component common-cause events to their 95th percentile values.
- 4) Decrease all component common-cause events to their 5th percentile values.
- 5) Set all maintenance unavailability terms to 0.0.
- 6) Any applicable sensitivity studies to ensure PRA adequacy.

If, following the sensitivity studies, the component is still found to be low safety significant and if it is safety related, it is still a *candidate* for RISC-3. In this case the analyst is to define why the SSC is of low risk significance. For instance, the SSC does not perform an important function, the SSC is in excess redundancy, the SSC is rarely used, [18]. The risk-importance process, including sensitivity studies, is performed for both CDF and LERF.

The SSC can cause initiating events for the internal events PRA. This should be reflected in calculating the importance values. As a matter of fact, the pressure sensor PS1 causes the second initiating event, discharge failure. This has been reflected as the failure of the monitoring system sharing the same pressure sensor.

External Event and Shutdown PRAs

Similar categorization using the importance measures are carried out for external event PRAs including the fire PRA (Section 5.9). This is shown in the hazard-type column of Figure 2.7. A weighted sum of these importance measures is used in the NEI document to integrate internal PRA with external PRAs. Similar criteria as the internal event PRA are used for the weighted importance.

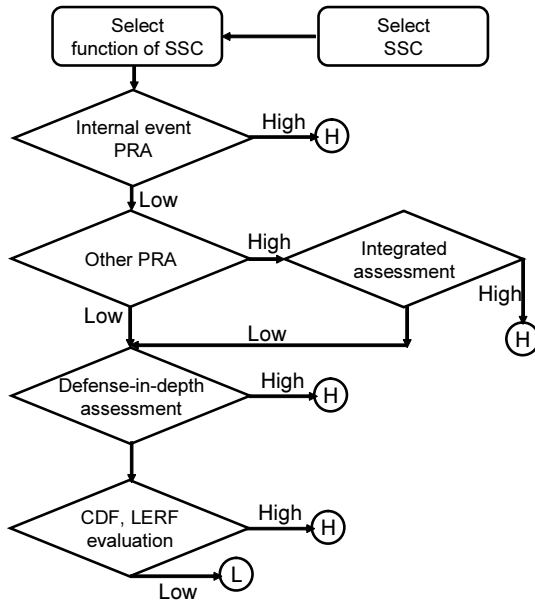


Fig. 2.8. Determination of low safety-significance candidate to be fed into IDP

Figure 2.8 shows two paths ending in LSS in the categorization process using risk information prior to a defense-in-depth assessment described in Section 3.8.

- 1) LSS by internal event PRA and LSS by other PRAs, or
- 2) LSS by internal event PRA but HSS by other PRAs and yet LSS by integral assessment.

Categorization of Function and SSC

A safety function supported by a HSS SSC is regarded as HSS. Otherwise, the safety function is a LSS candidate.

Once a function is labeled as HSS, all SSCs that support this function are, as default, assigned as HSS. Some SSCs support multiple functions. The SSC should be assigned the highest risk significance of the functions that the SSC supports. These conditions may override individual SSC evaluations by importance measures. Final decisions are made by the IDP.

The criterion for nondefault assignment of low safety significance for an SSC supporting a safety-significant function is that its failure would not preclude the fulfillment of the safety-significant function.

For each RISC-1 (or RISC-2) SSC, attributes are clarified. Examples include high-level features such as “provide flow”, “isolate flow”, *etc.* These attributes are monitored and maintained by the special treatment activities.

2.4 Safety Significance of Human Actions: NUREG-1764

2.4.1 Human-factors Engineering Review

Consider the pressure-tank system, The process-monitoring system includes the human action of opening the electric switch to shutdown the pump upon detection of overpressure. The tank system also contains a human action causing an initiating event, *i.e.* discharge failure.

Using a manual action in place of an automatic action and reducing the time available are typical changes to human actions (HAs). Plant modifications, procedure changes and others yield changes in HAs. A plant change may include changes to equipment, as well as to HAs. Changes to HAs involve new actions, modified actions, or modified task demands.

NUREG-1764 [13] provides guidance to determine the appropriate level of human-factors engineering review of human actions based upon their safety significance. The guidance can be applied to categorization of the existing human actions even if these are not the changes. This section describes the safety-significance categorizations of existing human actions from the point of view of the NUREG-1764 approach.

The guidance now has three steps for the existing HAs. The first step is quantitative, while the second is qualitative. The third step is an integrated assessment [13]:

- Step 1) A quantification of the risk importance of the HA to be categorized,
- Step 2) A qualitative evaluation of the safety significance of the HA, and,
- Step 3) An integrated assessment of HA safety significance to determine the appropriate level of human-factors (HF) engineering review.

The human actions are assigned to one of three safety-significance levels (high, medium, low). After the categorization of human actions, these are reviewed using standard criteria in human-factors engineering to verify that the

actions can be reliably performed when required. A risk-informed approach is used to determine the safety significance for graded human-factors engineering review.

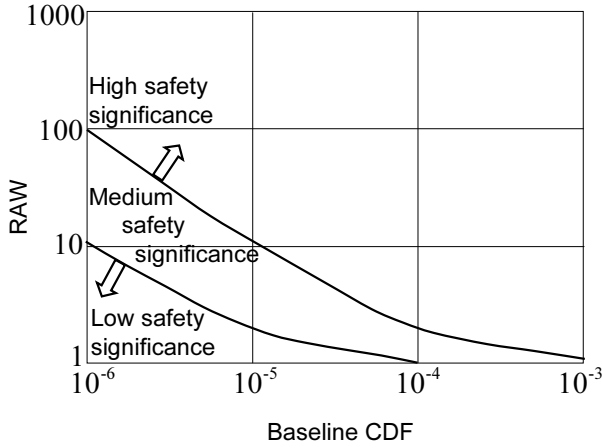


Fig. 2.9. RAW and baseline CDF

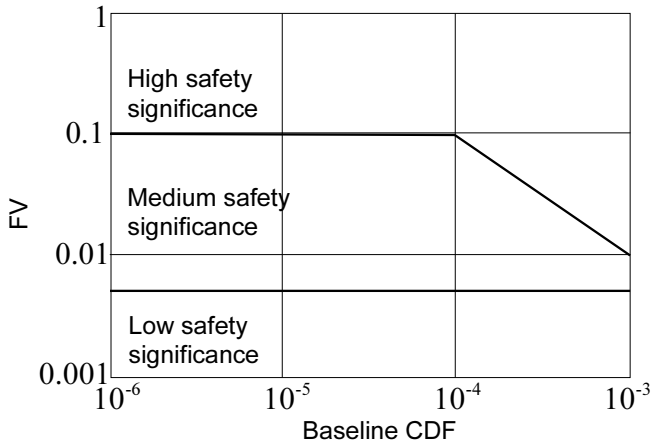


Fig. 2.10. FV and baseline CDF

2.4.2 Step 1: Quantitative Assessment

High safety-significant HAs should be identified from the PRA and human-reliability analysis (HRA). The PRA is level 1 (core damage) and/or level

2 (release from containment) including both internal events and/or external events (if available). Refer to Chapter 5 for the PRA levels.

HAs should be categorized using more than one importance measure and HRA sensitivity analyses to provide adequate assurance that an important human action is not overlooked because of the selection of the measure or the use of a particular assumption in the analysis.

The RAW and FV importance measures are typically used as in the case of SSCs. They are evaluated relative to the plant baseline CDF. The RAW is the increase in CDF when the HA fails. That is, the HEP (human-error probability) of the HA is increased from its base-case value to 1.0 and the overall CDF is recomputed. The equation for RAW for HA is:

$$\text{RAW(HA)} = \frac{\text{CDF with HA being failed}}{\text{Baseline CDF}} \quad (2.3)$$

A high RAW value means that failure of the HA results in a risk-significant situation. In other words, the HA with the base-case reliability reduces the risk by the factor of RAW. The HA reliability should be verified by a thorough human-factors engineering review for high RAW values.

FV is defined as the CDF of core-damage cut sets (or accident sequences or scenarios) that contain the HA in question, divided by the total CDF:

$$\text{FV(HA)} = \frac{\sum \text{Pr}\{\text{CDF cut sets containing HA}\}}{\text{Baseline CDF}} \quad (2.4)$$

If FV is high, the HA with the base-case reliability contributes to a relatively large portion of risk. Thus, for defense-in-depth purposes, the HA reliability should not be degraded further to result in a large increase of CDF. A thorough human-factors engineering review is required to prevent and detect the degradation.

The FV is included to obtain a more robust evaluation of safety significance because if the HEP is too high or too low due to uncertainty or poor modeling, this will affect both the RAW and FV measures, but in opposite directions. The FV importance measure addresses HAs that may not have a high RAW value (*e.g.*, due to a relatively low HEP), but that contribute notably to the CDF.

Figures 2.9 and 2.10 show the safety-significance assignments for RAW and FV. The terms “Level I, II, III” were used in NUREG-1764 to represent the safety significance of the HA. However, this terminology is confusing when we say “increase level by one”. In NUREG-1764 the increase from Level II means a move to Level I. The level numbering is in the reverse order compared to SIL.

This section rewrites the levels in the following way: 1) Level I: high safety significance (HSS), 2) Level II: medium safety significance (MSS), 3) Level III: low safety significance (LSS).

After both RAW and FV are determined, the HAs should be placed in the most conservative or highest safety significance of the two figures. Similar assignments can be made for LERF evaluations.

Human actions of HSS receive a detailed human-factors engineering review and those of MSS undergo a less-detailed one, commensurate with their safety significance. For human actions placed in LSS, there is a minimal human-factors review or none except for verification that the action is in fact in this safety significance.

The curve between the HSS and MSS areas of Figure 2.9 is roughly based on a CDF of 10^{-4} core-damage events per reactor-year, given the failed HA. This CDF is the subsidiary objective. Similarly, the curve between the MSS and LSS areas are roughly based on a CDF of 10^{-5} core-damage events per reactor-year, one order of magnitude less than the subsidiary objective.

The evaluation should consider all of the relevant HAs. Any dependent HAs should be aggregated together. Any HAs that are not dependent can be treated separately.

Consider the pressure-tank system as an illustrative example. The human action OP1 has the same importance measures as timer contact C1: RAW of 2.5 and FV of 0.16. The baseline value is 0.9×10^{-4} . A conservative classification yields HSS from Figure 2.9. The same HSS is obtained from Figure 2.10.

The assessment of the safety significance of an HA may be checked by performing appropriate sensitivity studies, varying the HEP through its range of uncertainty, as, for example, characterized by the 90% confidence interval. The final assessment should be conservative.

Furthermore, if there are judged to be dependent HAs that were not properly modeled in the HRA and if the reviewer is unable to adequately address them, then increasing the human-factors review of the set of dependent HAs should be considered. For the pressure-tank system, human actions OP0 and OP1 are dependent HAs because both are performed by the same operator.

There also may be cases when a lessening of the defense-in-depth or safety margin is only relied on a HA. Then, an increase of the human-factors review would be appropriate.

2.4.3 Step 2: Qualitative Assessment

Step 2 modifies the safety-significance assignment of Step 1 by qualitative criteria. These results can be either: 1) no change, 2) elevate one level, or 3) reduce one level.

Elevate Level of HF Review by One

If “yes” responses are obtained for many qualitative criteria described below, the level of review of the HA should probably be increased. If a “yes” response is received for only one or two criteria, then the analyst should consider whether the “yes” response is sufficient to warrant elevating the level of review.

- 1) Operating experience: Experience/events at that plant or plants of similar design show poor performances of the HAs under consideration.

- 2) New responsibility: The human actions require new responsibilities for the success of safety functions. An example may be the reallocation of responsibility from an automatic system to personnel for the initiation, ongoing control, or termination of a function. The operator of the pressure-tank example has two responsibilities: prevention of initiating event and mitigation of pump-overrun event.
- 3) Difficult tasks: The HA is significantly different from the way in which personnel usually perform their tasks (*e.g.*, making them more complex, significantly reducing the time available to perform the action, increasing the operator workload, changing the operator role from primarily “verifier” to primarily “actor”).
- 4) Difficult context: Here, context is defined as the overall performance environment, including plant conditions and behavior that, for example, affect the time available for the operator response and the effectiveness of job aids. A manual action for a safety-related function is now required under new circumstances. The operator of the pressure-tank example may be asked to initiate the pumping cycle urgently, forgetting to discharge the gas.
- 5) Degraded HSIs (human–system interfaces): The HA changes the HSIs significantly that are used by personnel to perform the task. For example, the pressure-tank operator now performs tasks from a control room, whereas previously the tasks were performed onsite where the operator could hear the gas discharged.
- 6) Degraded procedures: The HA significantly changes the procedures that personnel used to perform the task, or the task is not supported by procedures.
- 7) Problem of training: The HA significantly modifies the training, or the task is not addressed in training.
- 8) Less teamwork: For example, (1) one operator is now performing the tasks accomplished by two or more operators in the past, (2) it is now more difficult to coordinate the actions of individual crew members, or, (3) task performance is more difficult to supervise.
- 9) Less skill: It is necessary for an individual who is less trained and has lower qualifications to take the action.
- 10) More communication demands: The HA significantly increases the level of communication needed to perform the task. For example, an operator must now communicate with other personnel to perform actions as compared with a task at a local panel containing all necessary HSIs.
- 11) Degraded environment: The HA significantly increases the environmental challenges (such as radiation, or noise) that could negatively affect task performance.

Reduce Level of HF Review by One

The analyst should consider reducing the level of HF review if the HA has the following characteristics.

- 1) The answers are “no” to most of the qualitative criteria. One “yes” answer should not necessarily preclude a reduction in the level of the review, unless it is a “yes” to a significant criterion.
- 2) The action is well defined and the analyst is confident that it can be easily performed. For example, (1) it is clear when to perform the action, (2) there are clear procedures, (3) there is sufficient time and staff available, and (4) the action is similar to those routinely taken.

When the review is reduced to LSS, the following criteria taken from Chapter 19 of the Standard Review Plan (SRP), Appendix C.2 should be used to verify that the SSCs or human actions are of LSS [9]:

- 1) The HA does not relate to the performance of a safety function or a support function to a safety function, or does not complement a safety function. The HA does not support other operator actions that are credited in PRAs for either procedural or recovery actions.
- 2) The failure of the HA will not result in the eventual occurrence of a PRA initiating event.
- 3) The HA is not required in maintaining barriers to the release of fission products during severe accidents.
- 4) The failure of the HA will not unintentionally release radioactive material, even in the absence of severe accident conditions.

If any of the above criteria are not satisfied, then re-elevation to a MSS human-factors review is recommended.

2.4.4 Step 3: Integrated Assessment

This step integrates the results from Steps 1 and 2. For example, assume that Step 1 gives LSS, and Step 2 results in “elevate”. Then, Step 3 may yield MSS.

2.5 Concluding Remarks

Three types of categorization are described to determine the safety significance of safety-instrument systems, SSCs, and human actions, respectively. The next chapter develops how the performance required for each category can be materialized.

Satisfying Safety Goals by Probabilistic Risk Assessment

Kumamoto, H.

2007, XVI, 253 p., Hardcover

ISBN: 978-1-84628-681-0