Journal of Energy and Power Engineering 14 (2020) 211-224
doi:10.17265/1934-8975/2020.07.001

A Framework for Modern Risk-Informed Root Cause Analysis Process

Dorian Conger[1], Ivan Vrbanic[2] and Ivica Basic[2]

1. Conger Enterprises LLC, 4535 Ponte Vedra Drive, Marietta, GA 30067, USA

2. APOSS, Repovec 23B, Zabok 49210, Croatia

Abstract: The paper discusses the framework for a risk-informed root cause analysis process. Such process enables scaling of the analysis performed based on the risk associated with the undesired event or condition, thereby creating tiers of analysis where the greater the risk, the more sophisticated the analysis. In a risk-informed root cause analysis process, a situation is normally not analyzed at a level less than what actually occurred. However, a situation may be investigated as though the consequence were greater than actually happened, especially if only slight differences in circumstances could result in a significantly higher consequence. While operational events or safety issues are normally expected to result only with negligible or marginal actual consequences, many of those would actually have certain *potential* to develop or propagate into catastrophic events. This potential can be expressed qualitatively or quantitatively. Risk-informing of root cause analysis relies on mapping the event or safety issue into a risk matrix which, traditionally, is a two-dimensional probability-consequence matrix. A new concept employed in the risk matrix for root cause analysis is that, while the probability reflects the observed or expected range of values (retaining, thus, its "traditional" meaning), the consequence reflects not only the observed or materialized impact (such as failure of equipment) but, also, its potential to propagate or develop into highly undesirable final state. The paper presents main elements of risk-informed root cause analysis process and discusses qualitative and quantitative aspects and approaches to determination of risk significance of operational events or safety issues.

Key words: Root cause, risk-inform, risk, probability, cause analysis, safety precedence, significance determination, risk matrix, probabalistic margin, conditional probability, conditional risk, analyst, training, methods.

1. Introduction: On "Root Cause Analysis" and Why "Risk-Informing" It

Root causes are generally considered to be the most fundamental reasons for undesired events or conditions that if removed, then the undesired events or conditions would not occur or exist [1]. "Root causes" (the plural) are preferred, especially in significant situations. The singular term "root cause" may be most beneficially used as an adjective modifying "analysis" rather than as a noun.

By modern standards "root cause analysis" must employ one or more root cause analysis methods, tools, or analytical techniques. Without use of at least one method, someone might claim that a "root cause determination" was made or that a "conclusion" had been reached, but not that a legitimate "root cause analysis" had been performed. No method means no root cause analysis.

Some definitions of root causes are limited to those items "under management's control" or those items which are "reasonably discoverable". However, both terms limit the range of possible root causes unnecessarily and may constrict a proper, complete search for root causes. The analyst may misjudge, for example, what is "under management's control" and unfairly restrict possible root causes. Similarly, to look only for what is "reasonably discoverable" may be expeditious but is not thorough and may thus miss important issues.

There are generally two different types of root cause analysis (RCA). First, organizations may perform a requirement-driven root cause analysis. If the analysis is done only to meet the requirement, there may be a

Corresponding author: Kenneth J. Elsea, M.A., former President of Conger & Elsea, Inc., research fields: root cause analysis and human performance.

tendency to meet *minimum* requirements and to meet the *letter of the requirement*. In this case, the organization may miss or fail to consider the risk significance of the undesired event or condition. The second type is a risk-informed root cause analysis, the purpose of which is to learn as much as possible about the undesired event or condition in question. This maximized learning is usually undertaken to be able to: (1) prevent or reduce the probability of a recurrence, or (2) manage or ameliorate the consequences should there be a recurrence. Those organizations which are guided by a desire to learn how to reduce the risk of an occurrence rather than merely meet a requirement are likely to scale the analysis performed based on the risk associated with the undesired event or condition, thereby creating tiers of analysis where the greater the risk, the more sophisticated the analysis. Additionally, the corrective actions derived from a risk-informed root cause analysis (RI-RCA) process are typically measured by the ability to reduce the risk of future occurrences.

The above mentioned RI-RCA process can be established through the following elements:

- Organization which is subject to analysis;
- Event (or issue) Risk Significance Determination, including the accompanying Risk Matrix for RI-RCA with supporting risk assessment methodologies and tools;
- RI-RCA analysts/investigators;
- Training program;
- RCA methods.

These elements are discussed in the paper. As may have been expected, the section devoted to the event (issue) risk significance determination is somewhat longer than the others. This comes from the fact that it introduces some new concepts into the RCA framework, while the other sections extend from the features and methods already existing and known.

2. Organization as a Subject to Analysis

2.1 Systems

As subjects for analysis, organizations have certain structuring characteristics that are taken into account by the root cause analyst. All systems (of which organizations are a subset) may be broadly viewed as being composed of these elements: (1) people, (2) procedures, and (3) plant and equipment (the 3 P's). A thorough risk-informed root cause analysis (RI-RCA) would look at each of the three elements individually and then together. A problem might be caused by weaknesses in one or more of the elements and/or by weaknesses in the inter-relationships between and among the elements. For instance, the people element might not have a problem, and the procedures element might not have a problem. However, the people and the procedures might not "mesh", so the *interface* is a problem. A thorough inquiry (such as a proper risk-informed root cause analysis) looks both finely and broadly at such issues.

2.2 Safety Precedence Sequence

The safety precedence sequence (SPS) [2], builds upon this "3 P's" view of systems and incorporates the risk-informing process. The SPS is a ranked ordered set of ways to achieve safety/risk reduction/reliability. The higher order (lower number) levels are generally more effective than the lower order (higher number) levels. The SPS has six steps:

(1) Design for minimum hazard;

(2) Safety devices;

(3) Safety warnings;

(4) Procedures;

(5) Training, awareness;

(6) Notify management of risk and accept the situation without corrective action.

The SPS is useful in assessing how a system's protective features are designed to obtain a certain level of risk. How much, for example, are the hazards "designed" or "engineered" out? How many "protective barriers" depend on the people (the *least* reliable element in most systems) to activate them? How much "residual risk" (that risk which is left after all system features are factored in) does the

organization assume? The SPS can be used during the risk-informed root cause analysis to evaluate the amount of risk that is acceptable to the organization and can be used after the determination of the root causes to assess the relative effectiveness of potential corrective actions in reducing the risk of a recurrence.

3. Risk Significance Determination of Event or Issue

3.1 On Risk as a Measure of Significance

The ability to risk-inform the RCA process is the linch-pin concept that holds everything together. Risk provides a useful way to determine the significance of situations. Typically, the riskiest situations would be the most undesired. Since some risk is unavoidable, there are at least two implications. First, did the organization properly recognize, prepare for, and respond to the risk of a given situation? Second, is the RCA being conducted at a level appropriate for the risk (or significance) of the situation?

Before going into a discussion of the principles for risk-informing the RCA, the term "risk", which is used in every day's life, needs to be put into the context of safety evaluations. In engineer's terms, the risk can be quantitatively defined by the famous "risk curve" representing the probability (or frequency) of exceedance as a function of magnitude of consequences, as shown in Fig. 1. This presentation corresponds, for example, to the complementary cumulative distribution function used to depict the risk in NUREG-1150 [3]. The overall risk is presented by the area below the risk curve.

The purpose of the "safety management" or "risk management" in the design and operation of the facilities then, basically, is to minimize the area below the risk curve, or to suppress its "belly" as much as (practicably) achievable. This is illustrated by Fig. 2, which also shows the two basic and most obvious principles of the risk/safety management, denoted as (a) and (b). The approaches used in the practice usually represent their combination, as also indicated in Fig. 2.

In practical applications the risk curve usually comes in the simplified form of a "risk matrix" [4] where the whole range of both probabilities and consequences is divided in a limited number (e.g. three to five) of intervals specified in a qualitative or a quantitative manner. The whole area of risk (i.e. area below the risk curve) is, thus, divided into a limited number of rectangles usually referred to as "risk categories". In such simplified presentation the risk contribution from particular category can be expressed by the well-known formula:

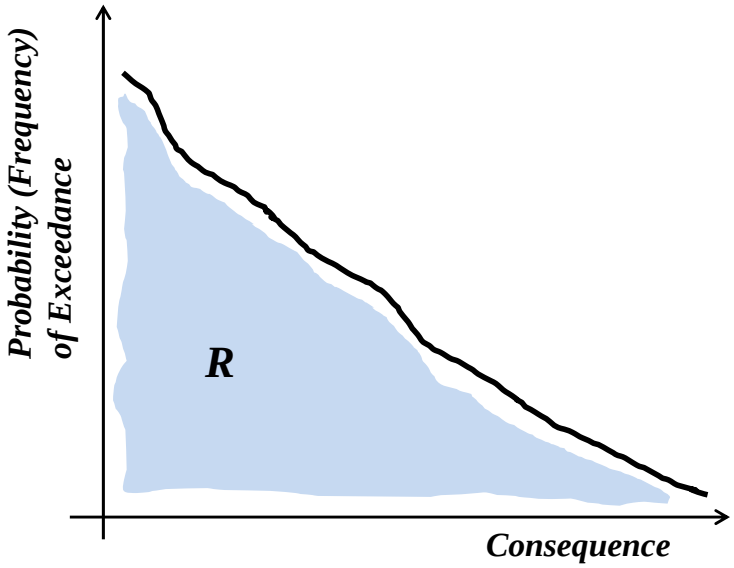


Fig. 1 Theoretical definition of "risk" for an engineer.

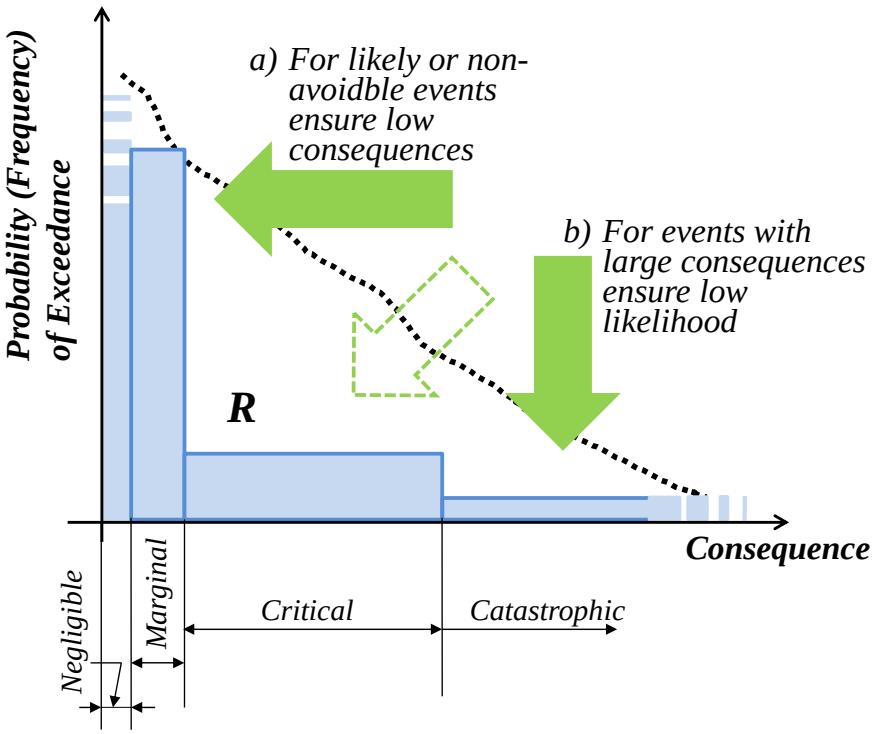


Fig. 2 Two basic principles for risk management.

Risk = Probability × Consequence

In operation of the facility, certain risk categories may be considered allowable, certain categories may be tolerable for limited time, while operation in others would be considered non-tolerable. To illustrate the concept, the consequence axis in Fig. 2 is divided into four intervals, from "negligible" to "catastrophic" (representing four consequence categories). More severe the consequences, smaller the probability or likelihood would be allowed. Shadowed area in Fig. 2 indicates the controlled (sometimes even regulated) risk area in the operation of a facility.

Use of consequence categories such as the above mentioned "negligible" to "catastrophic" (or similar), as well as the risk matrix, in the RCA is further discussed in Sections 3.2 and 3.3 and in the Appendix.

3.2 Assessment of Risk Significance of Considered Event or Issue

Once the existence of an undesired event or condition is known, a determination of its actual and potential significance is the first step toward determining if a risk-informed root cause analysis is to be done. Organizations typically have in place a scheme using multiple significance levels. These levels should be risk-informed, but generally are not to a sufficient degree. Often, they are defined by examples so that an individual can make a significance determination. A good risk significance determination takes into account the nature of the occurrence (where *actual* harm is done or a "close call" where consequences are avoided) and its historical context. For instance, knowing whether this or similar situations have occurred before is useful, as it informs the risk determination. It may also be useful to know how many similarly configured locations are in the system, helping identify the full extent of the risk to the organization.

Normally a situation is not analyzed in a risk-informed process at a level *less* than what actually occurred (a fatality, for example, is always investigated as a fatality no matter how unlikely the circumstances). However, in a risk-informed process, a situation may be investigated as though the consequence *were*

greater than actually happened, especially if only slight differences in circumstances (time of day, shift in wind direction, and other "chance" elements) would have resulted in a greater consequence (this is the key concept for risk-informing the RCA and it is further explored in Section 3.3 below). A risk-informed root cause analysis may also be done based on the *collective risk significance* of a number of less significant situations.

If a determination is made that the situation has reached a threshold of high significance, then a major investigative effort is expected. Generally speaking, a high significance level dictates that more resources be expended than does a low significance level. Using such a *graduated* approach aids in proper resource allocation and in doing just the right number of root cause analyses. Doing too many costs too much and doing too few means missing important lessons learned. The objective of a RI-RCA process is to assure the organization resources of appropriate level are applied for the evaluation of any given problem based on the level of risk the problem presents to the organization. Risk significance determination task within a RI-RCA means the mapping of the considered event (safety issue, inspection finding…) to the risk-matrix mentioned in Section 3.1. This would, in turn, enable a proper allocation of resources for RCA, i.e. such that it is in accordance with risk significance of considered event. One qualitative risk matrix (based on applications carried out for many years in a multitude of industries), is shown in Section 3.3.

Mapping of the considered event (issue, finding…) to the risk matrix may require supporting methodological approaches and tools which may be qualitative or quantitative (or blended). These aspects are further discussed in the same Section 3.3 and, to some more details, in Appendix B.

3.3 Risk Matrix for RI-RCA

Traditional "risk matrix", as already mentioned in Section 3.1, is a two-dimensional matrix with *probability* (likelihood) on one axis and *consequences* on another. New concept employed in the risk matrix for RI-RCA is that, while the *probability* (likelihood) reflects the observed or expected range of values (retaining, thus, its "traditional" meaning), the *consequence* reflects not only the observed or materialized impact (such as failure of equipment) but, also, its *potential to propagate or develop into highly undesirable final state* (which, e.g., may involve fatalities, pollution to the environment or large material loss).

In the context of this paper, we will refer to such consequences (i.e. those reflecting not only *what has* actually happened but, also, *what could have* additionally happened) *as risk-informed consequences*.

An example set of *Risk-Informed Consequences* can be as follows:

- *CATASTROPHICPOTENTIAL*—Death, loss of system or plant, such that significant loss of production, significant public interest or regulatory intervention occurs or *reasonably could occur* (considering the potential discussed above).
- *CRITICAL POTENTIAL*—Severe injury, major system damage or other event which causes some loss of production, effects more than one department, or *could have resulted in catastrophic consequences under different circumstances* (considering, again, the potential discussed above).
- *MARGINAL*—Minor injury, minor system damage, or other event generally confined to one department without potential to propagate or develop into critical consequences.
- *NEGLIGIBLE*—no potential to affect safety.

It is very important to understand that, in operation of any facility, the "catastrophic" or "critical" consequences should really not be expected (i.e. the facility should have the means, design features or/and administrative provisions to prevent them). Therefore, operational events or safety issues are really expected to result only with "negligible" or "marginal" consequences. However, many of them would actually

have a *potential* to develop or propagate into real "critical" or "catastrophic" events or issues (e.g., maybe only one additional failure or small time difference would have resulted in severe injury). A proper RI-RCA process should be able to recognize it and treat it appropriately.

This *potential* can be expressed qualitatively or quantitatively.

Fig. 3 provides a possible example of *qualitative determination* of risk-informed consequences (given only for illustration). It relies on the approach with counting the "lines of defense" (LOD), which is sometimes used for design verification. In this example, which relates to nuclear power plants (NPP) design or operation, considered safety issue is represented in terms of remaining LODs and then evaluated against a set of critical and catastrophic consequences ("Design Basis Accident with last LOD" can be considered as "critical" consequence, while any consequence involving "core damage" can be considered as "catastrophic"). The above discussed *potential* is "measured" by a number of remaining LODs, i.e. those which are not affected by the issue. LODs are characterized as "strong" (e.g. safety-classified system with design basis accident mitigation function) or "weak" (e.g. non-safety classified system or system requiring complicated human action) (Note the different meanings of the term "system" in the context of an NPP design or operation and "system" in the context of Section 2.1). The impact of an issue under consideration can, for example, be: unavailability of single or multiple LOD (either "strong" or "weak"); degradation of "strong" LOD to "weak" LOD, etc.

Fig. 3 (which is, to mention it once again, given only as an illustration of principles) provides a logical framework for determining risk-informed consequences. Thus, for example:

- Issue which would leave the plant with only two "weak" LODs against the core damage (in the absence of any "strong" LOD) would be considered to have "critical potential";
- Issue which would leave the plant with less than two "weak" LODs against the core damage would be considered to have "catastrophic potential", etc.

This kind of logic can be further refined by considering duration of issue or/and by additional rules. Similar simple models for risk-informed consequences can be developed for other facilities and industries (compare, for example, LOD concept with the concept of a *barrier* in the traditional "Hazard, Barrier and Target Analysis" done as a part of many RCAs).

The above discussed *potential* involved in observed consequences can, also, be expressed *quantitatively*. This is, actually, done in a number of applications associated with NPPs. This has its advantages because quantitative measure enables direct comparison of different issues or events and ranking of corrective measures by their risk importance. In those applications the quantitative consequence potential is usually considered as *probabilistic margin* between actually observed state and final undesired state (such as fatality, large loss, release of hazardous material, etc.). In other words, it is represented as *conditional probability* that observed state develops into the final undesired state. Thus, for example, qualitative framework from Fig. 3 can be "translated" into quantitative one by considering the probabilities of failure of remaining LODs (including the common cause failure potential, if applicable).

Fig. 4 shows two examples of quantitative thresholds for *conditional* risk potential based on two applications of the U.S. Nuclear Regulatory Commission: Significance Determination Process (SDP) [5], and Accident Sequence Precursor (ASP) Program [6] (without further elaboration, it is pointed here that the above term *conditional risk potential* corresponds to the term *consequence potential* as discussed above. Attribute "conditional" refers to the condition where the considered hazard has occurred). Since in the field of risk assessment for NPPs in U.S. two main risk metrics are Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) [7], the quantitative

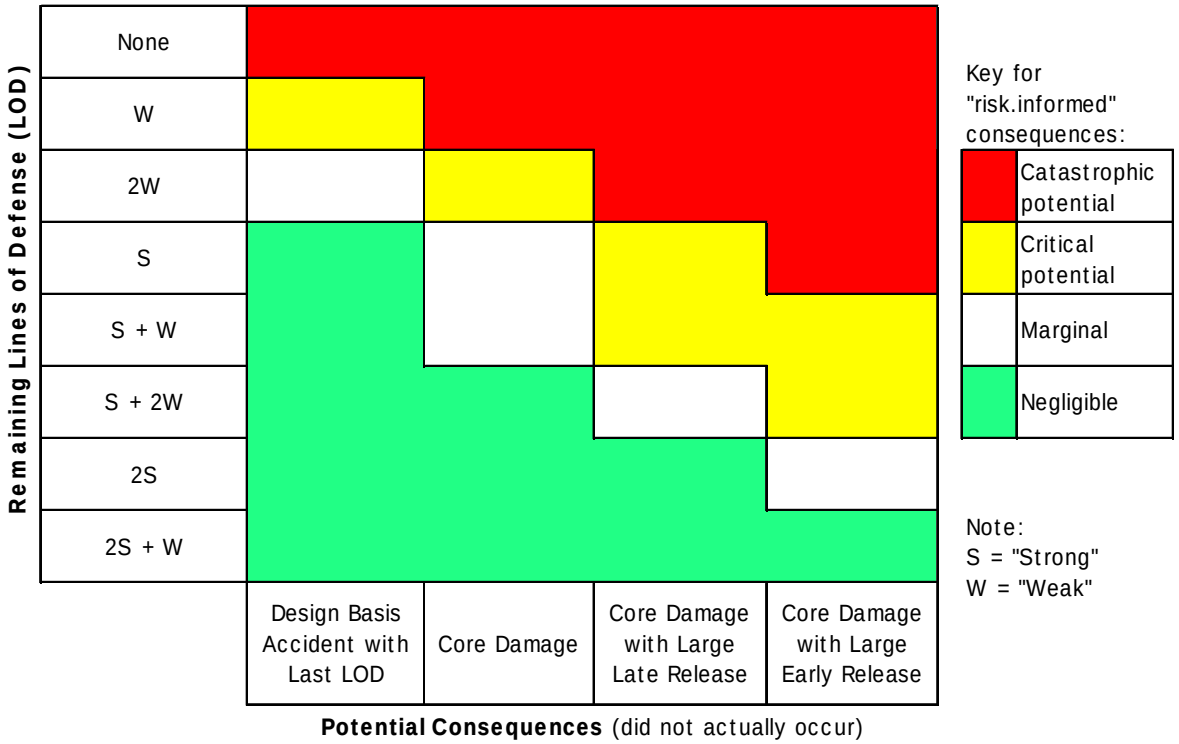
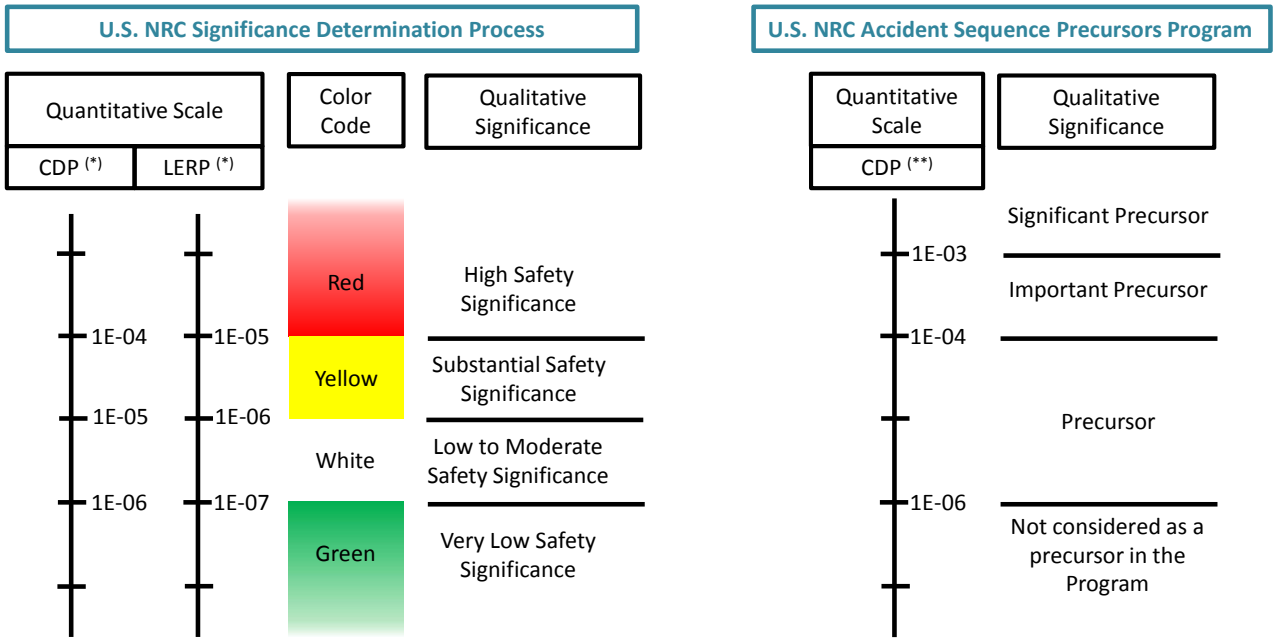


Fig. 3 Illustration for qualitative determination of "risk-informed consequences".



Notes:

* In NRC's SDP, [5], quantitative risk potential measures are referred to as "Increase in CDF" and "Increase" in LERF (even if calculated are, actually, increases in CDP and LERP). This, however, needs to be viewed in the context of interpretation of CDF (LERF) as CDP (LERP) on a yearly basis.

** Quantitative risk measure in NRC's ASP Program, [6], is specifically defined as Conditional CDP, CCDP, or as ΔCCDP, depending on the type of event (initiator or condition)

Fig. 4 Examples of quantitative thresholds for conditional risk potential based on significance of inspection findings and operational events (precursors).

measures for the *conditional* risk potential were defined, accordingly, as (conditional) Core Damage Probability (CDP) and (conditional) Large Early Release Probability (LERP). Examples like these can be considered in establishing the quantitative thresholds for the risk-informed consequences in the RI-RCA process (of course, the thresholds should be viewed in the context of corresponding applications. U.S. NRC's SDP and ASP Program have two different purposes [5, 6]).

Beside the above two, there are numerous other examples of applications where conditional probabilities of pre-specified undesired states were used as quantitative "risk-informed consequences". For example, one of the industry approaches for risk-informed in-service inspection (RI-ISI) of piping, developed in accordance with U.S.: NRC Regulatory Guide 1.178 [8], uses the concept in which the risk importance of particular piping segment is obtained from separated (and then combined through a risk matrix) assessments of failure likelihood and failure consequences. Consequences are expressed quantitatively in terms of conditional CDP and conditional LERP.

Another question is how these quantitative risk potential measures (e.g. CDP, LERP or conditional probabilities for other undesirable states from other industries) can actually be assessed. Some concepts for quantitative determination of "risk-informed consequences" are discussed in Appendix B.

Risk-informed consequences discussed above represent one axis of the risk matrix for the RI-RCA process. The other axis, as already mentioned above, represents the probability (frequency, likelihood) of considered issues or events. An example set of *probability* categories can be:

- *FREQUENT*—Likely to occur often during the life of an individual item or system or very often in operation of a large number of similar items.
- *PROBABLE*—Likely to occur several times in the life of an individual item or system or often in operation of a large number of similar items.
- *OCCASIONAL*—Likely to occur sometime in the life of an individual item or system, or will occur several times in the life of a large number of similar components.
- *REMOTE*—Unlikely, but possible to occur sometime in the life of an individual item or system, or can reasonably be expected to occur in the life of a large number of similar components.
- *IMPROBABLE*—So unlikely to occur in the life of an individual item or system that it may be assumed not to be experienced, or it may be possible, but unlikely, to occur in the life of a large number of similar components.

Unlike the consequences, the probability of occurrence of issues or events is in the RI-RCA framework represented by its observed or expected values. One point, though, which was already made, is that the number of similarly configured locations in the system (organization, facility, fleet…) should be considered in order that probability or frequency is not underestimated. Also, if a *collective risk significance* of a number of less significant situations is assessed, then corresponding collective frequency (probability) should be taken into assessment.

Two risk dimensions, probability and (risk-informed) consequences, are combined into a risk matrix. One example of possible risk matrix for RI-RCA is presented in Fig. 5. As shown, this model establishes four risk-informed categories for undesired events or conditions. Category 1 (High Risk) would require the most sophisticated of root cause analysis and likely require the longest amount of time to complete by a qualified team of people. Category 2 (Moderately High Risk) would require a sophisticated root cause analysis, but require less time to complete and with a smaller contingent on the team. Category 3 (Moderate Risk) would require a lower level systematic cause analysis to be performed in a matter of days by a qualified individual. Category 4 (Low or No Risk) would require very basic systematic analysis, or none at all (It is pointed out that color codes in Fig. 5 do not have the

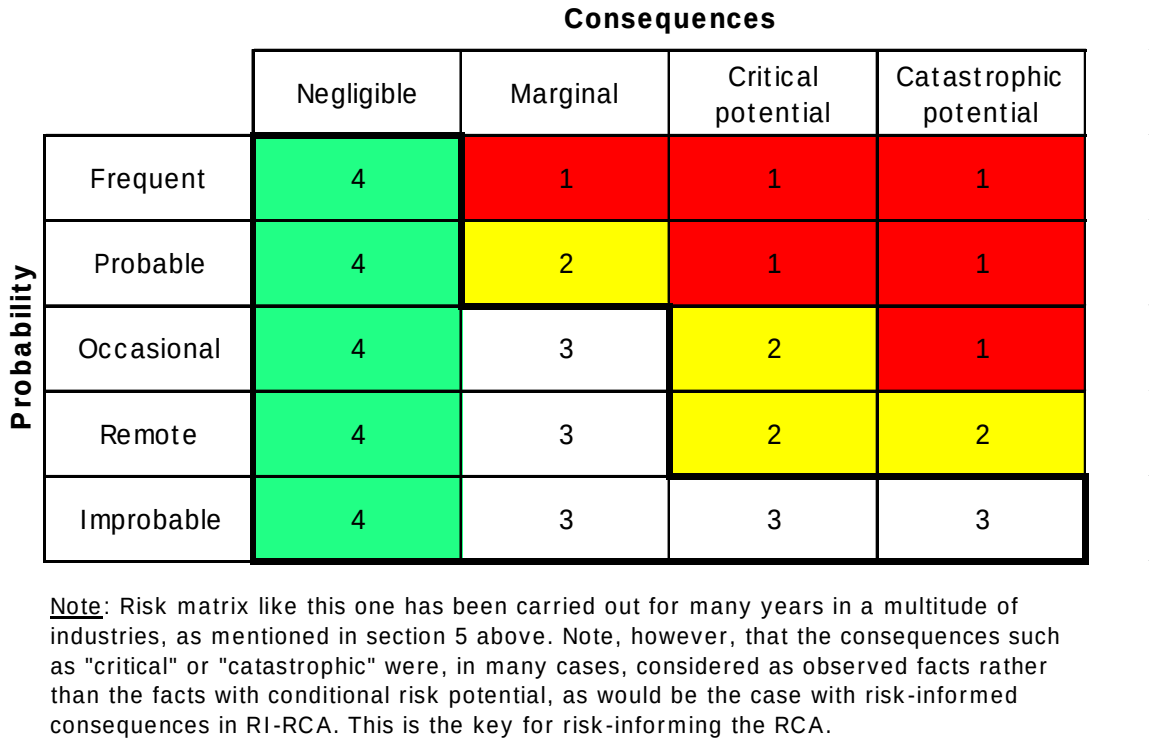


Fig. 5 An example of risk matrix for RI-RCA.

same meaning as those in Figs. 3 and 4. Colors in Fig. 5 reflect the level or *risk*, while the colors in Figs. 3 and 4 reflect the level of *consequences* (considering their potential). "Yellow" consequence does not mean "yellow" risk. It needs to be combined with likelihood. Further, individual organizations may establish the risk thresholds differently based on the willingness to accept or tolerate risk).

The analytical requirements for the above four risk categories, in terms of the RCA methods, tools and effort, are further discussed below. They are summarized in Appendix A.

4. Analyst(s)/Investigator(s)

Three major considerations are necessary to select the proper analyst(s)/investigator(s). First, deciding whether to use a single analyst or a team of root cause analysts should be determined by the significance level of the event or situation. Generally, high significance situations call for a team of investigators. The team not only sends a public message of importance, it also encourages a variety of individual views for consideration. Second, subject matter *expertise* ensures a good technical background and may help with "buy-in" of solutions. Third, sometimes *independence* (having no vested interest) from the situation is a scarce and valuable quality for the analyst(s). Independence helps assure that *bias* is properly kept at bay and that *fear* does not keep the analyst(s) from making the proper determinations. As a rule of thumb, the higher significance situations usually call for a higher level of independence. Ideally the analyst(s) should have independence while still being able to access the expertise (e.g. through interviews) and by use of "consultants" (subject matter experts) to the analyst(s). In general, *expertise* can be found *after* an investigation begins. *Independence* is more difficult to add on and should be built in from the beginning.

5. Training Program

Training in risk-informed root cause analysis processes and methods is necessary for the proper

conduct of a thorough root cause analysis. Organizations with mature programs typically offer levels of cause analysis training commensurate with the risk level of events they are expected to analyze. The higher significance level situations should have more trained analysts, trained in higher order methods than lower significance level investigations. At the highest significance level, all analysts should be trained in advanced root cause analysis approaches.

6. RCA Methods

Root cause analysis methods, also called analytical techniques or analytical tools, are the *essential* element of root cause analysis. In 1980, one author had compiled a listing of thirty tools. By 2005, more than one hundred such tools had been collected [9].

For the analyst, methods have two primary functions. First, early in the investigation, tools are helpful in formulating questions to be researched and answered. Second, methods organize information so that patterns can be seen and conclusions drawn. Without root cause analysis methods the important functions of gathering and analyzing data would be idiosyncratic at best and haphazard at worst.

Methods also provide traceability. That is, a reviewing individual who is not an analyst on a given inquiry should be able to follow the root cause analyst's thinking. The reviewer need not *agree* with the analyst's conclusion, but the reviewer should be able to understand the analyst's work. Methods can provide a check on bias and aid in understanding the reasoning as conclusions are drawn. Reviewing a method of analysis is similar to verifying a calculation or doing a peer or second party review. Methods thus function to provide a check on the analyst's work and provide the basis for a chosen supporting or dissenting opinion.

Methods differ in the *power* to analyze. Usually methods which are quicker to completion such as change analysis and hazard-barrier-target analysis are less powerful in that they have a limited scope (breadth or depth). Such "lower level" methods are useful in analyzing a small portion of a high significance event, but by *themselves* are usually not sufficient for a full analysis. Some methods, such as events and causal factors analysis, are very flexible and thus may serve as the beginning analytical point for a wide variety of investigative situations. Table 1 [10] contains selected methods with their respective strengths and weaknesses.

One of the most effective ways to "boost" the power of methods is to use more than one method on a given inquiry. Using more than one method can show a "convergence" of conclusions, increasing confidence in the outcome. If multiple methods show "divergence", that may be an indication that more work needs to be done to resolve inconsistencies. When multiple methods are used, care should be taken to apply the methods independently rather than trying to combine them before application. Such methodological "hybrids" usually have neither the power nor credibility of previously known and accepted methods.

Table 1 Strengths and weaknesses for various root cause analysis methods.

Method	Strengths	Weaknesses
Change analysis	Quick, almost intuitive.	Depends upon listing *all* features; easy to miss combined effects of changes.
Hazard-barrier-target analysis	Elegant model for "protection"; equally applicable to people, equipment, and environment.	Requires precision in definitions, deceptively simple.
Fault tree analysis	Great on hardware, shows multiple possible failures.	Requires accurate info on hardware, difficult for some to learn.
Events & causal factors analysis	Flexible, focus on *facts*.	Can be time consuming, no suggestions of possible causal factors.
MORT analysis	Comprehensive, complete, looks for *systemic* weaknesses, *content laden*, can use for common cause analysis.	Takes time to do whole tree, looks complex.

6.1 A Final Note on RCA Methods

All root cause analysis methods require information to drive them. No method or combination of methods can fully substitute for lack of information. However, given good information, appropriate analytical methods in the hands of an independent, trained team can lead to valuable lessons learned from high significance situations. In general, the quality of a root cause analysis can be examined in narrow (micro) or broad (macro) focus by asking certain questions, listed below.

Micro questions to be asked for a given root cause analysis:

(1) What are bases for the causes in the analytic technique?

(2) What is the factual support for the root causes?

(3) What are the recommendations for each root cause?

(4) How are the recommendations "validated" on the analytical techniques?

(5) Are all root causes adequately supported? Are all recommendations validated?

Macro questions to be asked for a given root cause analysis:

(1) Is the analysis chartered so as to take a broad and deep look to maximize learning?

(2) Are the techniques appropriate for the situation analyzed?

(3) Is the analyst(s) properly trained and qualified?

(4) Is more than one technique used?

(5) Is there appropriate independence represented by the analyst(s)?

Satisfaction with all the answers would, generally, point to the RCA (including the methodology and its implementation) of appropriate level of quality. On the opposite, the lack of the answers (e.g. no clear identification of factual support to the root causes) or the "wrong" answers (e.g. "No, only one technique used") may indicate the need for questioning whether the RCA has fulfilled its purpose.

7. Concluding Remarks

Maximizing lessons learned and reducing or eliminating the risk of an occurrence are the desired goals of a sophisticated root cause analysis process. Perhaps the most important part of meeting those objectives is to assure that the process is based on a foundation of understanding the risk involved. The very purpose of a risk-informed root cause analysis is to learn as much as possible about the undesired event or condition in question. This approach, as described here, maximizes learning. The usual result of a risk informed root cause analysis is to: (1) prevent or reduce the probability of a recurrence, or (2) manage or ameliorate the consequences should there be a recurrence. Organizations guided by reducing the risk of an occurrence rather than merely meeting a requirement are likely to scale the analysis performed based on the risk associated with the undesired event or condition, thereby creating tiers of analysis where the greater the risk, the more sophisticated the analysis. Therefore, the corrective actions derived from a risk-informed process are typically enhanced by the ability to reduce or eliminate the risk of future occurrences.

References

[1] 2016. *U.S. NRC Inspection Proceudre 95-001, Supplemental Inspection Response to Action Matrix Column 2 Inputs*.

[2] Johnson, W. G. 1980. *MORT Safety Assurance Systems*. Marcel Dekker Publishing.

[3] U.S. NRC. 1990. *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants—Final Summary Report*. NUREG-1150.

[4] MIL-STD 882E. 2012. *DoD Standard Practice—System Safety*, Section 4.3.3.

[5] 2015. *U.S. NRC Inspection Manual Chapter 0609, Significance Determination Process*.

[6] 2015. *U.S. NRC Policy Issue (Information) SECY-15-0124, Status of the Accident Sequence Precursor Program and the Standardized Plant Analysis Risk Models*.

[7] 2011. *U.S. NRC Regulatory Guide 1.174, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*.

[8] 2003. *U.S. NRC Regulatory Guide 1.178, An Approach for Plant-Specific Risk-Informed Decision-Making for In-Service Inspection of Piping*.

[9] International System Safety Society. 2005. *Compendium of Root Cause Analysis Methods/Techniques, New Mexico Chapter*.

[10] Elsea, K., and Conger, D. 2012. *Root Cause Analysis and Incident Investigation Workshop*. Conger & Elsea, Inc.

[11] Smith, C. L. 1998. "Calculating Conditional Core Damage Probabilities for Nuclear Power Plant Operations." *Reliability Engineering and System Safety* 59: 299-307.

[12] Vrbanic, I., and Basic, I. 2014. "On Use of PSA for Characterization of Risk Significance of Operational Events and Issues in NPPs." In *Proceedings of the 10th International Conference on Nuclear Option in Countries with Small and Medium Electricity Grids*.

Appendix A: Summary of Requirements for a Root Cause Analysis in RI-RCA Process.

Incident classification	People/resources involved	Useful tools	Estimated company time	Likely number of occurrences
1. High risk	Trained and qualified team of 5-7 people; all "independent" from the event or condition.	- Change analysis. - Hazard-barrier-target. - Fault tree. - Events and causal factors. - MORT analysis (all or partial, as needed). MULTIPLE TOOLS REQUIRED.	30-45 days	Rare
2. Moderately high risk	Trained and qualified team of 3-4 people; at least two "independent" from the event or condition.	- Events and causal factors - MORT analysis (all or partial, as needed) - Others as needed. MULTIPLE TOOLS REQUIRED.	20-30 days	Seldom
3. Moderate risk	Trained and qualified individual; "independence" not required.	- Events & causal factors. - Change analysis. - Hazard-barrier-target. - Fault tree. ONE OR MORE TOOLS AS NEEDED.	5-10 Days	Some
4. Low or no risk	None required; may assign an individual at management's discretion.	- MORT (all or partial). - Events & causal factors. - Others as needed.	< 1 day	Most

Appendix B: Some Concepts for Quantitative Determination of "Risk-Informed Consequences".

The discussion which follows is built on concepts from probabilistic risk assessments (PRA) for NPPs, with quantitative "risk-informed consequences" such as "conditional core damage probability" (CCDP), in the context of Section 3.3 above. Principles of calculating CCDP for operational events at NPPs can be found, for example, in Ref. [11], as well as in a number of other sources.

From the perspective of risk significance analysis, operational events can be, most generally, divided into two types. The first one is an initiator type of event. This is an operational event which represents or could cause, together with other events, a PRA initiating event. It is a triggering type of event, which interrupts normal plant operation and has a potential for triggering an accident sequence. The second one is an event which represents a condition which fails or reduces reliability of safety related equipment or operators' response over some period of time. This is not a triggering type of event. It represents a condition which may be present, and may, even, be allowed to be present, for a certain period of time.

Both types of events can be, quantitatively, characterized by the risk significance metric such as CCDP. A significance determination of a safety issue, in the context of SDP [5], relies on the similar principles as accident sequence precursor (ASP) analysis [6], for the condition events. It may be useful to remember that SDP as initially formulated represented a simplified PRA-based technique with aim to provide a tool for classifying the safety issues into the risk significance categories such as "very low" (green), "low to moderate" (white), "substantive" (yellow) and "high" (red). This was done on the basis of PRA information condensed into three types of tables: (1) initiator likelihood table; (2) initiator and system dependency matrix, and (3) worksheets representing accident sequences in tabular form. Therefore, if a final result of ASP analysis for condition event is a quantitative measure in the form of CCDP, the final result of

SDP is determination of risk significance category which can be related to an order of magnitude of CCDP.

The principles for risk significance characterization of "initiator" and "condition" events are here illustrated by Fig. B1, on the simplified example of a pressurized water reactor (PWR) NPP for which a response to the reactor trip caused by the loss of main feedwater (LOMFW) can be characterized by two functions: Emergency Feedwater (EFW) supply to steam generators and primary "feed and bleed" procedure.

Based on the probabilities provided in the figure, the "nominal CCDP" (as a "probabilistic margin" against core damage) in the case of LOMFW is 1E-06. This is taken as a quantitative risk significance measure for this "*initiator*" type event. However, if the trip event is accompanied by some additional failures associated with EFW or "feed and bleed" functions, then this CCDP value increases due to the higher failure probabilities of those functions (e.g. 1E-02 instead of "nominal" 1E-03), or their actual loss. In other words, the event becomes more and more risk significant. To better present the decreasing of a "probabilistic margin", one can take "$(-)\log(CCDP)$" as a measure of risk significance. In this manner, instead of increasing probabilities such as 1E-06, 1E-05, 1E-03, etc., one obtains decreasing numerical values such as 6, 5, 3… (Refer to Fig. B1).

For the "condition" event, quantitative risk significance is assessed in a different manner. This is illustrated in Fig. B1 for the condition representing the unavailability of the EFW system. With EFW unavailable, the probabilistic margin in the case of LOMFW decreases from nominal value $(-)\log(CCDP)$ = 6 to the value $(-)\log(CCDP)$ = 3 (i.e. CCDP increases from nominal 1E-06 to 1E-03).

In most of the cases, the onset of unavailability of standby system is not recognized immediately and plant would continue to operate for a time being. (The condition would, ultimately, end with restoration of availability or reaching the allowable time limit from the Technical Specifications, whichever would come first). Considering the daily LOMFW likelihood of *0.1/365 = 2.7E-04 per day* (as indicated in Fig. B1), the daily risk increase due to present condition would be estimated as:

$$\Delta CCDP = \left(10^{-3} - 10^{-6}\right) \times \left(2.7 \times 10^{-4}\right) \approx 10^{-3} \times \left(2.7 \times 10^{-4}\right) = 2.7 \times 10^{-7} \ /day$$

Each day spent operating at this condition would increase the risk due to this specific condition by the above amount. (Note: $\Delta CCDP \approx CCDP$). The overall risk significance depends on both the increment of CCDP per day and total time spent operating at this condition. (Normally, the system surveillance requirements imposed by plant's Technical Specifications should be set at such intervals that this kind of the risk increase would be very small, i.e. the condition would be discovered before it would produce any significant amount of risk increase).

Methodological frameworks can be established which would enable that an assessment of risk significance of events or issues is, at least to a certain extent, done by people who are not necessarily PRA specialists. They can be customized for use by specialists such as operating experience evaluators. Instead of requiring the PRA models and sophisticated analyses, the approaches can rely on the use of *PRA information*, i.e. the information which is either readily available from PRA results and documentation or can easily be generated by "PRA people" upon request. Such PRA information may include:

- List of equipment/basic events in the PRA model structure;
- Failure probabilities (including common cause failure (CCF) probabilities), initiator categories frequencies and other parameters of a PRA model;
- Lists of risk-increase and risk-decrease importance measures for basic events representing equipment failures or human errors;
- Contributions to risk metrics such as core damage frequency, CDF (e.g. breakdown of CDF on initiating events contributions).

Some examples which show how PRA information, readily available from PRA documents or obtainable from PRA model in a straightforward manner, can be used for the purposes of characterization of risk significance of operational events, can be found in Ref. [12]. The same examples also show that, in many cases, risk significance characterization of an operational event or an issue can be obtained in a relatively simple and straightforward manner which can also, many times, be done by evaluators who are not necessarily PRA specialists.

As a final remark, it is pointed out that similar quantitative approaches can be used in other industries, as well. NPPs are complex systems which require complex PRA models and specialized tools. However, many times, simple risk model, sufficient for the RI-RCA purposes, can be built by means of simple event trees (such as one shown in Fig. B1) or/and fault trees, with failure probabilities at the level of order-of-magnitude. It can be contained in and quantified by such simple tools as spreadsheets.

Actually, the initial form of the U.S. NRC SDP process, with its tables and worksheets, is the best demonstration of the point.

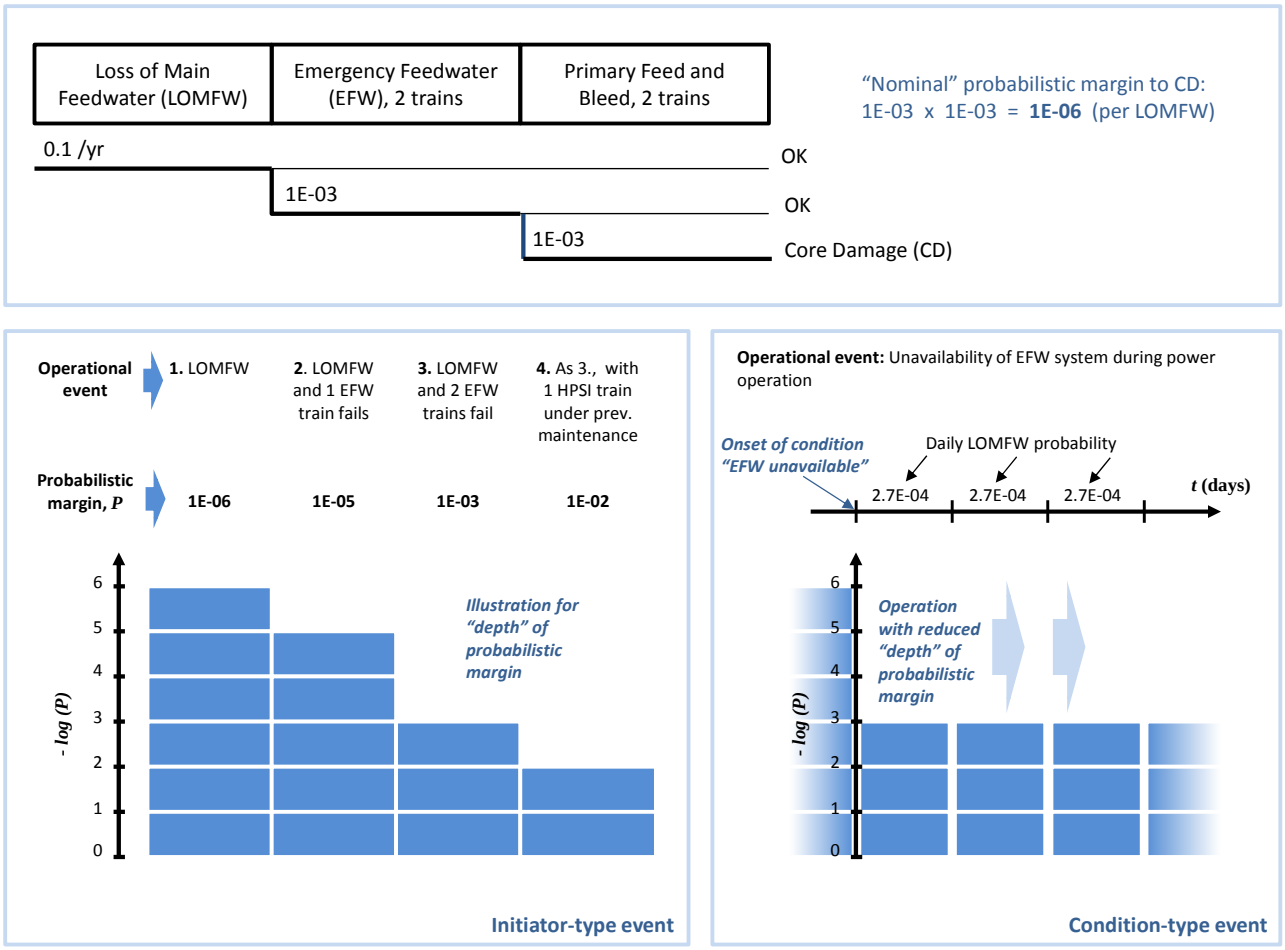


Fig. B1 Illustration for determination of "risk-informed consequences" for two types of operational event.