

## Appendix K

### MAINTENANCE RISK ASSESSMENT AND RISK MANAGEMENT SIGNIFICANCE DETERMINATION PROCESS

#### 1.0 OBJECTIVE

To determine the significance of inspection findings related to licensee assessment and management of risk associated with performing maintenance activities under all plant operating or shutdown conditions in accordance with Baseline Inspection Procedure (IP) 71111.13, "Maintenance Risk Assessment and Emergent Work Control."

#### 2.0 BASIS

NRC requirements in this area are set forth in paragraph (a)(4) of 10 CFR 50.65, "Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants." Detailed bases information for this appendix is provided in Inspection Manual Chapter (IMC) 308, "Reactor Oversight Process (ROP) Basis Document, " Attachment 3, Appendix K.

#### 3.0 GENERAL GUIDANCE

Appendix K is to be used as a Phase 1/2 Significance Determination Process (SDP) tool for assessing the significance of inspection findings related to compliance with Maintenance Rule (a)(4) requirements. The input to this SDP evaluation tool is a greater than minor inspection finding that results from the licensee's underestimate of plant risk or lack of risk assessment from ongoing or completed maintenance activities and/or the licensee's ineffective implementation of risk management actions (RMAs). Examples of greater than minor inspection findings are provided in Appendix E of IMC 0612, "Power Reactor Inspection Reports." In addition, minor and SDP screening questions are included in Appendix B of IMC 0612. A licensee performance deficiency of the paragraph (a)(4) of 10 CFR 50.65 requirements must exist for the significance of a finding to be evaluated using this SDP. If appropriate, a more detailed assessment may be performed in an SDP Phase 3 evaluation.

Attachment 1 provides the assumptions and defined terms used in this SDP. Flowcharts 1 and 2 are used to categorize individual inspection findings as either Green, White, Yellow, or Red. Specifically, flowchart 1 provides guidance to determine the significance of inspection findings related to inadequate risk assessment and risk management actions. Flowchart 2 is to be used for evaluating the significance of failure to implement risk management actions when the maintenance risks are adequately assessed.

It is expected that resident inspectors will support Senior Reactor Analysts (SRAs), or other risk analysts, as necessary to assess the significance of maintenance rule a(4) related inspection findings.

**Note: This guidance does not apply to the following situations: (1) those licensees who only perform qualitative analyses of plant configuration risk due to maintenance activities, or (2) performance deficiencies related to maintenance activities affecting SSCs needed for fire or seismic mitigation. When performance deficiencies are identified with either 1 or 2 above, the significance of the deficiencies must be determined by an internal NRC management review using risk insights where possible in accordance with IMC 612, “Power Reactor Inspection Reports.”**

## 4.0 SPECIFIC GUIDANCE

### Step 4.1 Determination of Actual Risk

This SDP uses the Incremental Core Damage Probability (ICDP) metric rather than  $\Delta$ CDF (annualized risk increase) used in other reactor safety SDPs. The ICDP accounts for the amount of the time in which the plant configuration change existed. Attachment 1 provides the mathematical formulas for these metrics.

The risk deficit for performance deficiencies is determined in an increasing order of magnitude to reflect the amount of the risk increase due to an inadequate risk assessment and lack of risk management actions. Specifically, the incremental core damage probability deficit (ICDPD) and the incremental large early release probability deficit (ILERPD) are the risk metrics used to evaluate the magnitude of the error in the licensee’s inadequate risk assessment of the temporary risk increases due to maintenance activities/configurations.

#### Step 4.1.1 - Licensee Evaluation of Risk

When the inspector has identified that the licensee has performed an inadequate risk assessment, or none at all, the actual maintenance risk configuration-specific CDF must first be adequately or accurately assessed. The inspector should discuss the results of the risk assessment with the licensee before proceeding with any further risk assessment. The new risk assessment value may be obtained in several ways including having the licensee perform the omitted maintenance risk assessment; or re-perform the assessment, correcting those errors and/or omissions that rendered the original risk assessment inadequate. It is expected that having the licensee re-evaluate the actual maintenance configuration would be the norm for (a)(4) issues.

#### Step 4.1.2 - NRC Evaluation of Risk

Alternatively, the inspector may request the regional SRA or other risk analyst to independently evaluate the risk if there are specific concerns regarding the adequacy of the licensee’s assessment such as:

- a. The licensee’s maintenance configuration change excluded multiple systems.
- b. There are notable limitations with the licensee’s configuration risk assessment tool (e.g., does not address potential changes to initiating event frequencies).

- c. There are known quality issues with the licensee's configuration risk assessment tool (e.g., is not consistent with the plant PRA).
- d. The quantitative risk assessment contained invalid assumptions and/or omissions.

To request an independent risk assessment, the inspector should provide the following information to the regional SRA or risk analyst:

- a. Structures, Systems, and Components (SSCs) configuration in the specific time window of concern with actual time of SSCs removed from service and when returned to service.
- b. Description of testing or other maintenance activities that potentially increased the likelihood of an initiating event
- c. Description of actual compensatory actions implemented
- d. Licensee's risk assessment

If the finding involves maintenance activities during shutdown conditions, then the appropriate checklist reflecting the plant shutdown mode from IMC 0609, Appendix G, Attachment 1, should be checked and provided to the SRA.

For findings that have significance preliminarily determined to be White, Yellow, or Red, an SRA may perform a Phase 3 analysis, if necessary.

#### **Step 4.2 Determination of Risk Deficit**

If the licensee did not perform a risk assessment at all, the actual risk increase ( $ICDP_{actual}$ ) is the product of the incremental CDF and the annualized fraction of the duration of the configuration [i.e.,  $ICDP_{actual} = ICDF_{actual} \times (\text{duration in hours}) \div (8760 \text{ hours per reactor year})$ ], where  $ICDF_{actual} = CDF_{actual} - CDF_{zero-maintenance}$

The risk deficit,  $ICDPD$ , is equal to  $ICDP$  when the licensee's performance deficiency involves not conducting a risk assessment.

For a flawed risk assessment, the risk deficit,  $ICDPD$ , =  $ICDP_{actual} - ICDP_{flawed}$  assuming the  $ICDP_{actual} > ICDP_{flawed}$ .

If the actual, correctly assessed  $ICDP$  is significantly greater than  $1E-6$  (i.e., one order of magnitude or greater), the net risk deficit is determined by subtracting  $1E-6$  from the risk deficit ( $ICDPD$ ) as determined above, prior to determining an SDP color.

The significance of the licensee's underestimate (or lack of estimate) of the risk ( $ICDPD$ ) is then determined by using Flowchart 1. The significance of the  $ILERP$ , if applicable, is determined in a similar fashion.

#### **Step 4.3 - Evaluation of Risk Management Actions**

As discussed in NUMARC 93-01, Section 11.3, "Assessment of Risk Resulting from Performance of Maintenance Activities," and in Appendix A of IP 71111.13, the following categories of appropriate RMAs can be used to manage risk associated with a maintenance activity.

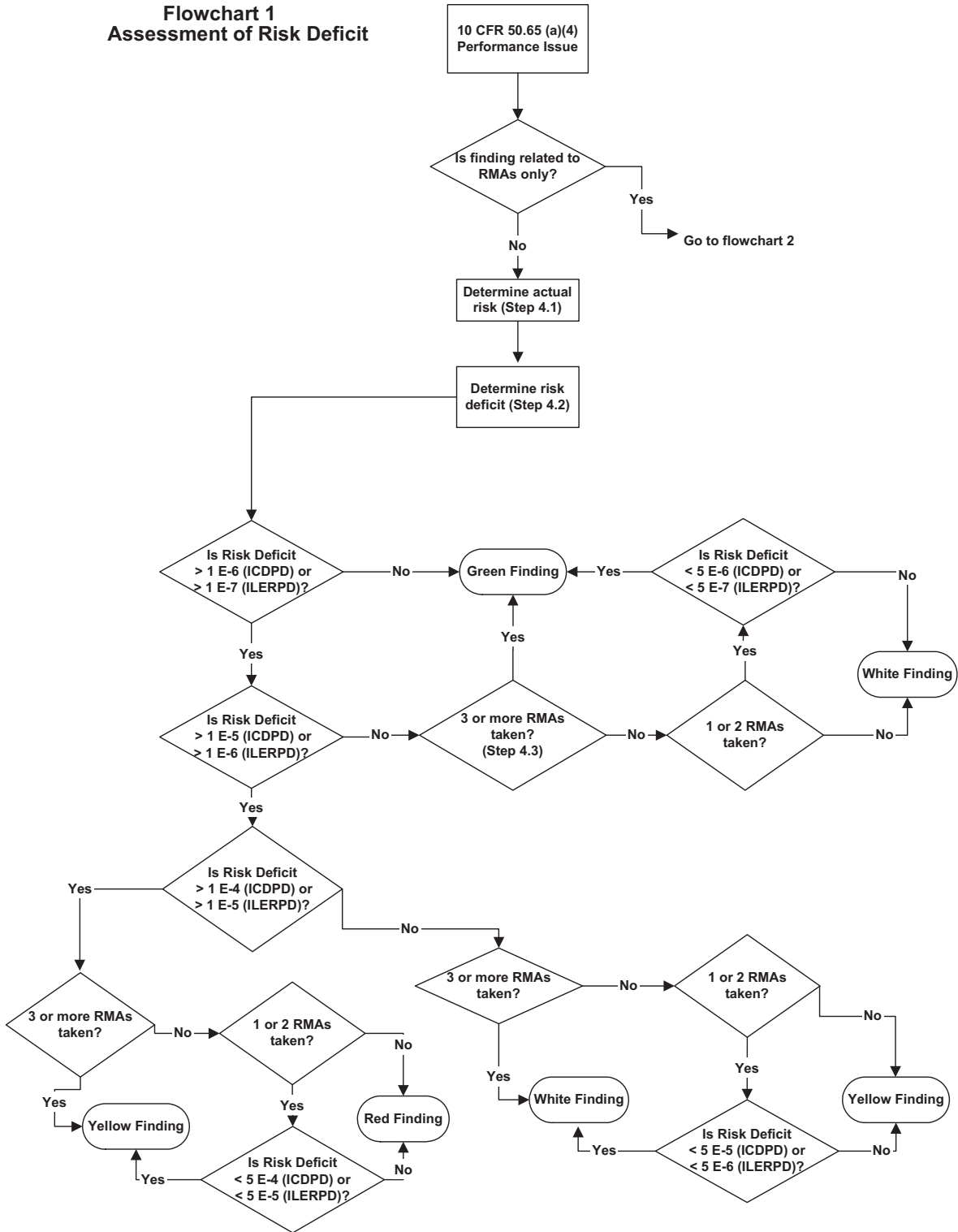
- increasing risk awareness and control
- reducing duration of maintenance activity
- minimizing magnitude of risk increase
- establishing other compensatory measures to provide alternate success paths for maintaining the safety function of the out-of-service SSC (e.g., using diverse means of accomplishing the intended safety function)

Because the risk benefits of some of these RMAs are generally not quantifiable, the approach chosen for quantitatively determining the significance of failure to manage risk is to assign credit for these actions in reducing the risk impact of the assessed configuration. Therefore, the simple screening rule used in this SDP is to assign a credit of one half order of magnitude reduction in risk to the correctly calculated risk if the licensee effectively implemented one or two categories of the RMAs to manage risk. The RMAs credited for risk reduction are only those for which credit was not already taken in the risk calculation. If the licensee effectively implemented three or more categories of the RMAs that have not already been evaluated in the risk calculation, an order of magnitude reduction in risk is credited against the actual maintenance risk. This approach allows the significance of failure to manage risk to be expeditiously determined without using quantitative approaches that would likely require intensive resources.

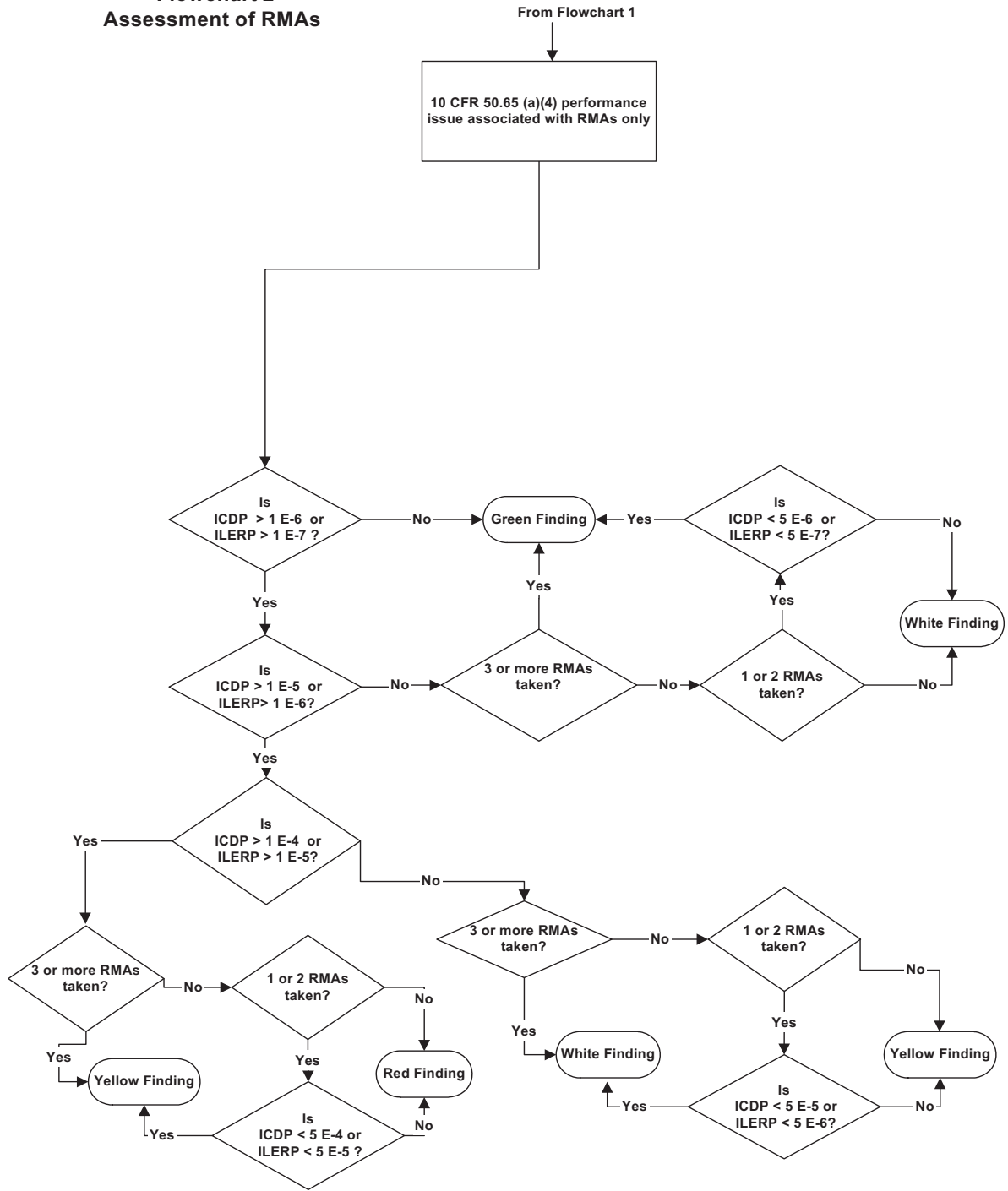
If the risk is inadequately assessed, or not assessed at all, the significance of the performance deficiency is evaluated using this SDP. The resultant failure to take RMAs due to lack of risk recognition merely provides no mitigation of the risk deficits.

When the risk is adequately assessed, the licensee will normally be expected to effectively implement only those RMAs prescribed for the assessed risk by site procedures. Under certain circumstances, specific compensatory measures may also be prescribed by license conditions, technical specifications, notices of enforcement discretion, and/or special commitments, as applicable. Flowchart 2 is provided to evaluate the significance of a licensee's failure to implement one or more categories of RMAs either as prescribed by any of the sets of requirements discussed above. The adequacy of licensee's RMAs should be assessed using the guidance provided in baseline IP 71111.13 and licensee's applicable implementing procedures.

**Flowchart 1  
Assessment of Risk Deficit**



**Flowchart 2  
Assessment of RMAs**



# ATTACHMENT 1

## ADDITIONAL GUIDANCE

The following assumptions and defined terms regarding licensee risk assessments and risk management actions (RMAs) are necessary to understand and efficiently use this maintenance rule (a)(4) SDP evaluation tool.

### 1.0 RISK ASSESSMENTS AND RISK MANAGEMENT ACTIONS

The intent of paragraph (a)(4) is for licensees to appropriately assess the risks of proposed maintenance activities that will:

- directly, or may inadvertently, result in equipment being taken out of service,
- involve temporary alterations or modifications that could impact SSC operation or performance,
- be affected by other maintenance activities, plant conditions, or evolutions, and/or
- be affected by external events, internal flooding, or containment integrity.

Paragraph (a)(4) requires management of the resultant risk using insights from the assessment. Therefore, licensee risk assessments should properly determine the risk impact of planned maintenance configurations to allow effective implementation of RMAs to limit any potential risk increase when maintenance activities are actually being performed. Although the level of complexity in an assessment would be expected to differ from plant to plant, as well as from configuration to configuration within a given plant, it is expected that licensee risk assessments would provide insights for identifying risk-significant activities and minimizing their durations. In general, the following two types of licensee performance deficiencies in meeting (a)(4) requirements can be defined.

- A. Failure to Perform an Adequate Risk Assessment. The failure to perform an adequate risk assessment in accordance with 10CFR50.65 (a)(4) prior to the conduct of maintenance activities includes the following deficiencies which result in underestimating the risk.
1. Failure to perform a risk assessment for maintenance configuration changes.
  2. Failure to update a risk assessment for changes in the assessed plant conditions (e.g., changes in maintenance activities or emergent conditions). However, performance or re-evaluation of the assessment should not interfere with, or delay, the operator and/or maintenance crew from taking timely actions to restore the equipment to service or take compensatory actions. If the plant configuration is restored prior to conducting or re-evaluating the assessment, the assessment need not be conducted, or re-evaluated if already performed.

3. Failure to perform a complete risk assessment including all affected/involved SSCs within the scope of SSCs required for (a)(4) assessments, and considering (or adequately considering) all plant-relevant plant conditions or evolutions, external events (excluding fire and seismic), internal flooding, and/or containment integrity
4. Failure to consider maintenance activities which have historically had a high likelihood of introducing a transient leading to an initiating event that would result in risk-significant configurations
5. Improper use of the risk assessment tool or process (i.e., beyond its capabilities or limitations, or under plant conditions for which it was neither designed nor in accordance with site procedures)
6. Deficient risk-informed evaluation process for limiting the scope of SSCs to be included in (a)(4) risk assessments as identified by NRC inspection (e.g., IP 62709).
7. Flawed risk assessment tool or process as identified by NRC inspection (e.g., IP 62709).

Underestimating or not estimating the risk of maintenance activities may not significantly increase the expected overall plant risk, in terms of core damage frequency (CDF) or large early release frequency (LERF). However, underestimating the risk may result in lack of risk awareness that could preclude RMAs and allow a high-risk configuration to persist unrecognized and uncompensated. Allowing a high-risk configuration with an unassessed CDF increase to persist longer than necessary, or desirable, will increase the exposure time and hence the incremental (integrated) core damage probability (ICDP) and/or the incremental large early release probability (ILERP) as defined below. Finally, unawareness of unassessed or inadequately assessed risk may allow actions or events to occur that could directly increase risk or hamper recovery from accidents or transients.

Licensees that have adopted RMA color thresholds that are not ICDP or ILERP based, may need to have performance converted to correspond to a probability unit of measure.

- B. Failure to Manage Risk. Failure to manage the risk impacts of proposed maintenance activities means a failure to implement, in whole or in part, the key elements of the licensee's risk management program. However, this deficiency will not result in an additional risk increase to the assessed risk of the maintenance configuration in terms of CDF or LERF. Measures to minimize the duration of the risk associated with a maintenance activity/configuration are a principal RMA. Nevertheless, failure to implement such measures when they are possible and practicable will allow the ICDP and/or the ILERP to increase further as the elevated risk condition persists. Appropriate and suitable RMAs can only reduce the risk incurred from a given configuration change.



RMAs should be implemented in a graduated manner, commensurate with various increases above the plant's baseline risk, to control the overall risk impact of an assessed maintenance configuration. However, licensees use a variety of methods for categorizing risk significance and managing the risk according to the significance category.

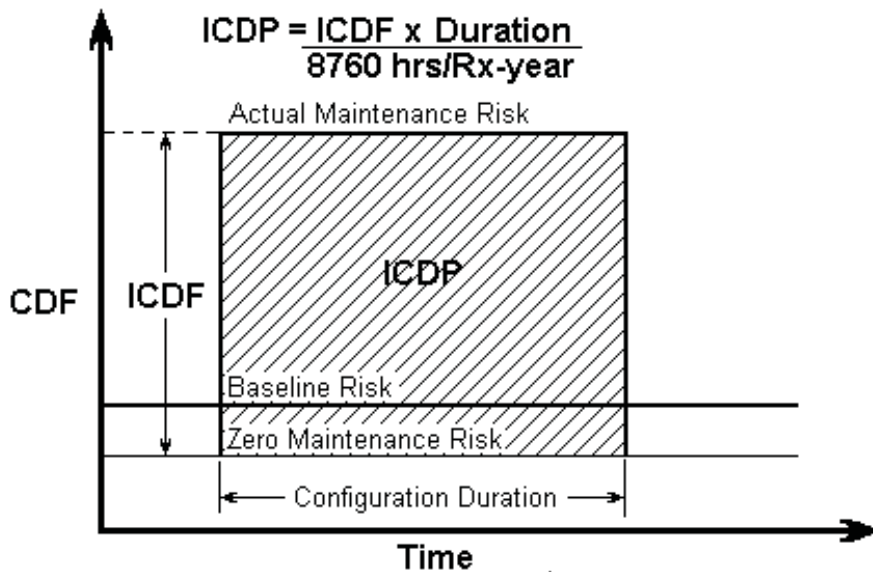
In Regulatory Guide 1.182, the NRC endorsed the RMA levels or categories/bands prescribed in the revised Section 11 of NUMARC 93-01, Revision 2, and subsequently incorporated in Revision 3 of NUMARC 93-01. These risk bands are defined in terms of the ICDP, making them readily comparable to the risk levels used in determining the significance of the risk deficits. For licensees that have adopted this guidance, normal work controls are allowed by site procedures for ICDPs less than 1 E-6. For ICDPs of 1E-6 or greater, RMAs are prescribed. Section 11 of NUMARC 93-01 states that maintenance risk configurations above ICDP value of 1E-5 should not be entered voluntarily. Site procedures will prohibit this activity entirely or will allow it only with fairly rigorous restrictions that typically include the plant manager's written permission along with extensive RMAs. Site procedures may further define specific detailed RMAs or plans for routinely allowable risk categories as well. It should be noted that when evaluating the adequacy of a licensee's RMAs, the inspector should consider only those actions that could have potential risk implications and are required by the licensee's procedures, such as working around the clock, installing backup equipment, and reducing duration of maintenance activity.

## 2.0 DEFINITIONS

The following are definitions of terms used throughout this SDP.

Incremental Core Damage Frequency (ICDF). The ICDF is the difference between the actual, adequately assessed, maintenance risk (configuration-specific CDF) and the zero-maintenance CDF. The configuration-specific CDF or ICDF are annualized risk estimates with the out-of-service or otherwise affected SSCs considered unavailable. The term, "Incremental Core Damage Frequency" is also equivalently referred to as delta CDF, or change in CDF.

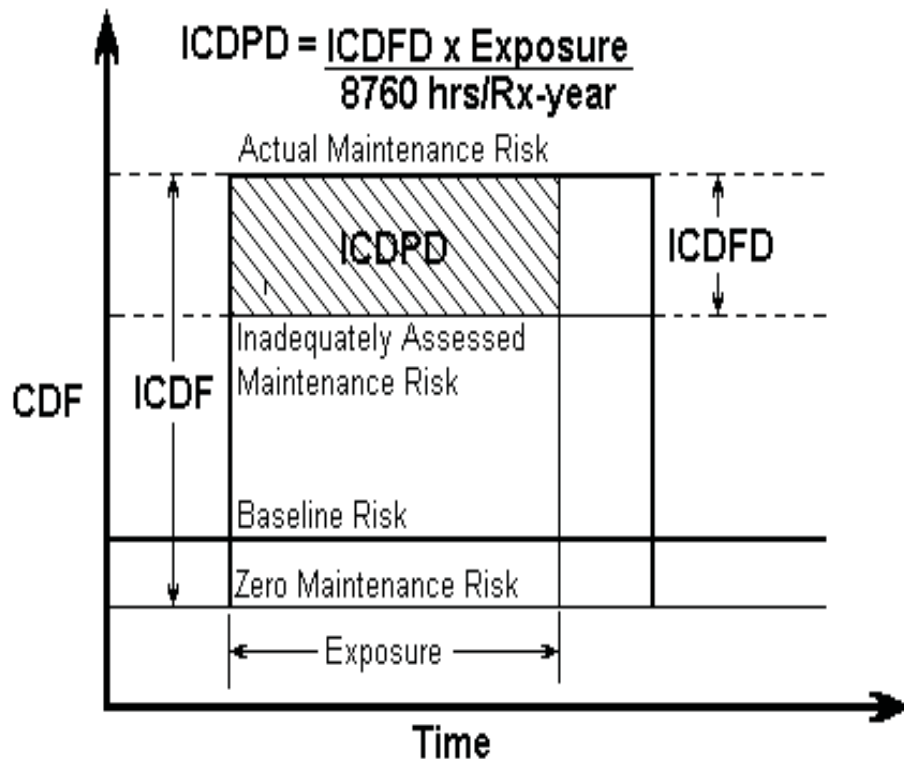
Incremental Core Damage Probability (ICDP). The ICDP is the product of the incremental CDF and the annual fraction of the duration of the configuration [ i.e.,  $ICDP = ICDF \times (\text{duration in hours}) \div (8760 \text{ hours per reactor year})$ ]. Note that the ICDP is sometimes expressed as the integrated or integral ICDP ( i.e., the delta CDF or ICDF integrated over the time of its duration which increases as the elevated-risk configuration persists). Figure 1 is a graphical representation of this concept.



**Figure 1 - Relationship of ICDF to ICDP**

Incremental Core Damage Frequency Deficit (ICDFD). The ICDFD is that portion of the ICDF defined as the difference between the actual maintenance-configuration-specific CDF (called  $ICDF_{actual}$  for purposes of this definition) and the maintenance-related ICDF as originally and inadequately assessed (flawed) by the licensee ( $ICDF_{flawed}$ ). Therefore, the  $ICDFD = ICDF_{actual} - ICDF_{flawed}$ . Note that if the licensee has failed to assess maintenance risk entirely when required (i.e., there is no licensee risk assessment), then the ICDFD will be equal to the entire value of the ICDF. The safety significance of the ICDFD (i.e., the magnitude of the licensee's underestimate (or lack of estimate) of the risk) is determined by means of this SDP.

Incremental Core Damage Probability Deficit (ICDPD). The ICDPD is the product of the ICDFD and the exposure (i.e., the annual fraction of the duration of the unassessed or inadequately assessed configuration, or that portion of the annual fraction of the duration of the maintenance configuration during which its risk remained unassessed or inadequately assessed). Thus the  $ICDPD = ICDFD \times (\text{exposure in hours}) \div (8760 \text{ hours per reactor-year})$ . Note that similar to the ICDFD, the ICDPD equals the ICDP when there is no risk assessment, rather than a flawed risk assessment. Note also that Exposure equals Duration if the risk remained unassessed or inadequately assessed for the entire duration of the configuration. The safety significance of the ICDPD (i.e., the magnitude of the licensee's underestimate (or lack of estimate) of the risk (in terms of ICDP)), may also be determined by means of this SDP. Figure 2 is a graphical representation of this concept.



**Figure 2 - Relationship of ICDFD to ICDFD**

Incremental Large Early Release Frequency (ILERF). The ILERF is the difference between the actual, adequately determined maintenance activity/configuration-specific LERF and the zero maintenance model results, if determinable. Note that LERF and ILERF are determinable only if the plant has a Level-II PRA and a risk tool or process capable of quantitatively assessing Level-II risk beyond a qualitative assessment of the impact of containment integrity. If calculated, the ILERF may also be referred to as the delta LERF or LERF difference.

Incremental Large Early Release Frequency Deficit (ILERFD). The ILERFD is used to evaluate the significance of a finding under the following conditions (1) an impact on containment integrity from or concurrent with the maintenance activity occurs, (2) this impact is/was not qualitatively assessed, and (3) the impact is/was quantitatively assessed, but not adequately. Then the ILERFD is meaningful and is that portion of the ILERF defined as the difference between the actual maintenance-configuration-specific LERF (called  $ILERF_{\text{actual}}$  for purposes of this definition) and the maintenance-related ILERF as originally and inadequately assessed by the licensee ( $ILERF_{\text{flawed}}$ ). Therefore, the  $ILERFD = ILERF_{\text{actual}} - ILERF_{\text{flawed}}$ . Note that if the licensee has failed to assess maintenance risk entirely when required (i.e., there is no licensee risk assessment) and there is an impact on containment integrity from or concurrent with the maintenance activity, this impact can be neither qualitatively nor quantitatively assessed. Therefore, the ILERFD will be equal to the entire value of the ILERF. The safety significance of the

licensee's underestimate (or lack of estimate) of the Level-II risk ( i.e., ILERFD) may also be determined by means of this SDP, if appropriate.

Incremental Large Early Release Probability (ILERP). The ILERP is the product of the incremental large early release frequency (ILERF) and the annual fraction of the duration of the configuration. The  $ILERP = (ILERF \times \text{duration in hours}) \div (8760 \text{ hours per reactor-year})$ .

Incremental Large Early Release Probability Deficit (ILERPD). The ILERPD is the product of the ILERFD with the annual fraction of the duration of the unassessed or inadequately assessed configuration, or that portion of the annual fraction of the duration of the maintenance configuration during which its risk (in terms of ILERF or ILERP) remained unassessed or inadequately assessed.

NOTE: Although an adequate maintenance risk assessment is expected to include the impact of containment integrity, at least qualitatively, there is no regulatory requirement for a quantitative risk assessment using a Level-II PRA. Paragraph (a)(4) of 10 CFR 50.65 neither prohibits nor explicitly discourages incurring maintenance risk. It only requires that the risk of maintenance activities be assessed (which can be done qualitatively, quantitatively, or, as is often the case, in a blended fashion) and managed.

Zero-Maintenance CDF(Risk). The CDF estimate of plant baseline configuration where all SSCs modeled in PRA are considered available.

Baseline CDF(Risk). The CDF estimate derived from a PRA model that considers average annual maintenance (preventive and corrective maintenance) unavailability data, and plant specific reliability data (failure rates).

Note that inadequate risk assessment or risk management for work not yet started is not an (a)(4) violation, but it still represents a licensee performance deficiency and may be indicative of deficiencies in previous risk assessments, RMAs and/or in the licensee's (a)(4) program. This SDP is not suited for determining the significance of this type of performance deficiency. This type of issue can normally be expected to be screened to Green in accordance with Reactor SDP Phase 1 screening.