NEI 04-08

Risk-Informed Technical Specifications Initiative 7a

Allowance for Non-Technical Specification Barrier Degradation on Supported System OPERABILITY (TSTF-427)

Industry Implementation Guidance

February 2006

TABLE OF CONTENTS

FIGURES

TABLES

1.0 Executive Summary

This document provides guidance for implementation of a generic Technical Specification improvement that establishes a new Technical Specification Limiting Condition for Operation (LCO) Applicability rule, LCO 3.0.9, and its associated Bases, to address degraded barriers that cannot provide their protective function(s) for Technical Specification systems.

LCO 3.0.9 establishes a risk management approach for control of degraded barriers that allows supported LCOs to not be declared not met for up to 30 days when degraded barriers, which support one or more trains of a system, cannot perform their required support (protective) function(s).

The Technical Specification revision modifies the provisions on equipment Operability for supported systems and would allow plants to provide a limited period of time to consider the supported system Operable when the degraded barrier is not capable of performing the required support function(s). It implements a risk assessment and management approach, using the plant program established to meet paragraph (a)(4) of the Maintenance Rule, 10 CFR 50.65.

This document discusses the following:

- Risk management Technical Specifications background
- Description and implementation of the Technical Specification revision
- Impact on plant procedures for Maintenance Rule (a)(4) risk assessment and management
- Risk assessment and management considerations for barriers that cannot perform their related support function(s)
- Use of the Maintenance Rule model to determine the impact of removal of a barrier

2.0 Risk Management Technical Specifications – Background

This section provides a brief background discussion on the overall philosophy and intent of introducing risk management concepts into Technical Specifications. The term "risk management" is used because each of the risk-informed Technical Specification initiatives relies on the risk assessment and management requirement of the Maintenance Rule as part of the basis for change, and the overall intent is to provide a "risk management" approach to plant configuration control within the Technical Specifications.

Historically, Technical Specifications address plant configuration control by specifying limits on plant operation with equipment out-of-service, and actions, often leading to plant shutdown, when these limits are not met. Technical Specifications are primarily based on the deterministic design basis accidents, and have not traditionally considered the plant risk impact as a factor in the action requirements. Further, Technical Specifications consider the synergistic effects of multiple out-of-service conditions for only a limited subset of cases (e.g., multiple inoperabilities associated with a common safety function). 10 CFR 50.36 provides the general requirements for the content of Technical Specifications, and, while not explicitly structured to consider risk-informed content, provides opportunity for a number of risk-informed improvements without the need for rulemaking.

The industry has achieved substantial gains in plant capacity factors over the last several years through reduced planned outage duration and increased use of on-line maintenance. This transition was facilitated through the use of probabilistic risk assessment (PRA) and corresponding configuration management tools. In November of 2000, a new provision, section (a)(4), was added to the Maintenance Rule, 10 CFR 50.65, requiring assessment and management of risk due to plant maintenance activities. NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," as endorsed by NRC Regulatory Guide 1.182, "Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants," provides guidance for implementation of this rule. This document addresses the use of PRA, qualitative risk assessment, and plant operating experience to assess plant risk due to maintenance activities, as well as actions that may be taken to manage the risk as determined by the assessment.

It was recognized that the configuration control requirements of Technical Specifications (deterministic) and the Maintenance Rule (risk-informed) may be in conflict; however, the licensee is required to comply with both, resulting in limitations on configuration control flexibility that are not in proportion to plant safety. Thus, industry has developed a series of initiatives intended to provide greater flexibility and safety to decisions involving plant configuration control. These initiatives involve:

- Equipment out-of-service times
- Equipment surveillance test intervals
- Plant shutdown requirements
- Mode change restrictions
- Missed surveillance requirements

All of these initiatives rely on the risk assessment and management techniques developed for the Maintenance Rule provision described above. The overall philosophy is that plant configuration control decisions should maintain the plant's existing baseline risk metrics, such as core damage frequency (CDF), within a reasonable interval over time. Thus, the additional flexibility afforded by risk management Technical Specifications should be used judiciously. For example, the capability to use longer equipment outage times should not be employed to the extent that the plant's baseline risk metrics increase over time due to increased unavailability of key equipment. Additional regulatory elements, such as the NRC Reactor Oversight Process, and other sections of the Maintenance Rule, provide further controls over these activities, but should not be relied on as the basis for control of plant configuration decisions.

It is recognized that the risk assessment and management techniques, and models developed by licensees to implement the Maintenance Rule may vary in level of sophistication. The process provided in this implementation guidance document allows a plant to use its existing risk assessment tools to determine if the LCO 3.0.9 allowance is acceptable for use.

This initiative will result in some safety benefits for the industry. Implementation of this initiative will better focus plant maintenance and configuration control on safety significant items, rather than application of Technical Specification system LCOs that are deterministically based. Additionally, implementation of this initiative will shift the licensee's focus to a consistent risk assessment and management approach for barrier removal.

3.0 Reference Materials

The following materials are useful for implementation of this initiative:

3.1 *Federal Register* Notice - xxx x, 2006 (xx FR xxxxx)

This provides the notice of availability, and the model safety evaluation for TSTF-427, which is available through the consolidated line item improvement (CLIIP) process.

3.2 TSTF-427, Revision 1, "Allowance for Non Technical Specification Barrier Degradation on Supported System OPERABILITY"

This TSTF is posted on the NRC Web site at: http://www.nrc.gov/reactors/operating/licensing/techspecs/changes-issued-for-adoption.html.

TSTF-427 provides the following information necessary for implementation of the license amendment:

- Justification of change,
- Determination of no significant hazards, and
- Marked up pages for the Improved Standard Technical Specification NUREGs.

3.3 NUMARC 93-01, Revision 3, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants"

Section 11 of the above document provides guidance for assessment and management of risk due to maintenance activities. This section is endorsed by NRC for implementation of 10 CFR 50.65 (a)(4) through Regulatory Guide 1.182, "Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants."

3.4 NRC Regulatory Information Summary (RIS) 2001-09, "Control of Hazard Barriers"

This document provides further discussion of the considerations for determining Operability when barriers are degraded.

4.0 Description of Technical Specification Revision

The following is a general description of the changes to the Technical Specifications.

This initiative adds a new LCO Applicability rule, LCO 3.0.9, and its associated Bases, to the Improved Standard Technical Specifications, to address barriers that cannot perform their required support function for Technical Specification systems. (This new requirement is numbered LCO 3.0.9 because TSTF-372 adds LCO 3.0.8.)

This LCO provides an allowance to not declare any associated LCOs not met for up to 30 days if at least one train of the system is Operable and supported by barriers capable of providing their required support (protective) function(s), and risk is assessed and managed. Multiple trains of the same system may be impacted if the barriers supporting each of the trains provide their related function(s) for different initiating events, subjected to risk considerations. LCO 3.0.9 provides that at the end of this time, the barrier(s) must be able to perform their required function(s) or the associated LCO(s) shall be declared not met.

If the inability of a barrier to perform its support function does not render a supported system governed by the Technical Specifications inoperable (see NRC Regulatory Issue Summary 2001-09, Control of Hazard Barriers, dated April 2, 2001), the provisions of LCO 3.0.9 are not necessary, as the supported system is Operable.

The new LCO 3.0.9 states:

"When one or more required barriers are unable to perform their related support function(s), any supported system LCO(s) are not required to be declared not met

solely for this reason for up to 30 days provided that at least one train or subsystem of the supported system is OPERABLE and supported by barriers capable of providing their related support function(s), and risk is assessed and managed. This specification may be concurrently applied to more than one train or subsystem of a multiple train or subsystem supported system provided at least one train or subsystem of the supported system is OPERABLE and the barriers supporting each of these trains or subsystems provide their related support function(s) for different categories of initiating events.

[For the purposes of this specification, the [High Pressure Coolant Injection / High Pressure Core Spray] system, and the [Reactor Core Isolation Cooling] system, and the [Automatic Depressurization System] are considered independent subsystems of a single system.]

If the required OPERABLE train or subsystem becomes inoperable while this specification is in use, it must be restored to OPERABLE status within 24 hours or the provisions of this specification cannot be applied to the trains or subsystems supported by the barriers that cannot perform their related support function(s).

At the end of the specified period the required barriers must be able to perform their related support function(s) or the supported system LCO(s) shall be declared not met."

The bracketed second paragraph is only included in NUREG-1433 and NUREG-1434, the Improved Standard Technical Specifications for BWR/4 and BWR/6 design plants. This difference is discussed in Section 5.1, "Definitions," under the topic "Single train systems (BWR)."

The Bases of LCO 3.0.9 are also new and establish the definition of what constitutes a barrier and what types of barriers are excluded. It lists the low probability initiating events that form the justification for use of LCO 3.0.9, and states that risk assessment and management must be addressed pursuant to the Maintenance Rule, 10 CFR 50.65 (a)(4), and associated implementation guidance. It further discusses the condition that must be met for application of LCO 3.0.9 to more than one train of a system.

The new Bases of LCO 3.0.9 states:

"LCO 3.0.9 establishes conditions under which systems described in the Technical Specifications are considered to remain OPERABLE when required barriers are not capable of providing their related support function(s).

Barriers are doors, walls, floor plugs, curbs, hatches, installed structures or components, or other devices, not explicitly described in Technical Specifications, that support the performance of the safety function of systems described in the Technical Specifications. This LCO states that the supported system is not *considered to be inoperable solely due to required barriers not capable of performing their related support function(s) under the described conditions. LCO 3.0.9 allows 30 days before declaring the supported system(s) inoperable and the associated LCO(s) associated with the supported system(s) not met. A maximum time is placed on each use of this allowance to ensure that as required barriers are found or are otherwise made unavailable, they are restored. However, the allowable duration may be less than the specified maximum time based on the risk assessment.*

If the allowed time expires and the barriers are unable to perform their related support function(s), the supported system's LCO(s) must be declared not met and the Conditions and Required Actions entered in accordance with LCO 3.0.2.

This provision does not apply to barriers which support ventilation systems or to fire barriers. The Technical Specifications for ventilation systems provide specific Conditions for inoperable barriers. Fire barriers are addressed by other regulatory requirements and associated plant programs. This provision does not apply to barriers which are not required to support system OPERABILITY (see NRC Regulatory Issue Summary 2001-09, Control of Hazard Barriers, dated April 2, 2001).

The provisions of LCO 3.0.9 are justified because of the low risk associated with required barriers not being capable of performing their related support function. This provision is based on consideration of the following initiating event categories:

------------------------------------ Reviewer's Note -----------------------------------
LCO 3.0.9 may be expanded to other initiating event categories provided plant-specific analysis demonstrates that the frequency of the additional initiating events is bounded by the generic analysis or if plant-specific approval is obtained from the NRC.

- *Loss of coolant accidents;*
- *High energy line breaks;*
- *Feedwater line breaks;*
- *Internal flooding;*
- *External flooding;*
- *Turbine missile ejection; and*
- *Tornado or high wind.*

The risk impact of the barriers which cannot perform their related support function(s) must be addressed pursuant to the risk assessment and management provision of the Maintenance Rule, 10 CFR 50.65 (a)(4), and the associated implementation guidance, Regulatory Guide 1.182, "Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants." Regulatory Guide 1.182 *endorses the guidance in Section 11 of NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants." This guidance provides for the consideration of dynamic plant configuration issues, emergent conditions, and other aspects pertinent to plant operation with the barriers unable to perform their related support function(s). These considerations may result in risk management and other compensatory actions being required during the period that barriers are unable to perform their related support function(s).*

LCO 3.0.9 may be applied to one or more trains or subsystems of a system supported by barriers that cannot provide their related support function(s), provided that risk is assessed and managed. If applied concurrently to more than one train or subsystem of a multiple train or subsystem supported system, the barriers supporting each of these trains or subsystems must provide their related support function(s) for different categories of initiating events. For example, LCO 3.0.9 may be applied for up to 30 days for more than one train of a multiple train supported system if the affected barrier for one train protects against internal flooding and the affected barrier for the other train protects against tornado missiles. In this example, the affected barrier may be the same physical barrier but serve different protection functions for each train.

[[HPCI (high pressure core injection) / HPCS (high pressure core spray)] and RCIC (reactor core isolation cooling) systems are single train systems for injecting makeup water into the reactor during an accident or transient event. RCIC system is not a safety system, nor required to operate during a transient, therefore, it does not have to meet the single failure criterion. The [HPCI / HPCS] system provides backup in case of a RCIC system failure. The ADS (automatic depressurization system) and low pressure ECCS coolant injection provide the core cooling function in the event of failure of the [HPCI / HPCS] system during an accident. Thus, for the purposes of LCO 3.0.9, the [HPCI / HPCS] system, and the RCIC system, and the ADS are considered independent subsystems of a single system and LCO 3.0.9 can be used on these single train systems in a manner similar to multiple train or subsystem systems.]

If during the time that LCO 3.0.9 is being used, the required OPERABLE train or subsystem becomes inoperable, it must be restored to OPERABLE status within 24 hours. Otherwise, the train(s) or subsystem(s) supported by barriers that cannot perform their related support function(s) considered must be declared inoperable and the associated LCOs declared not met. This 24 hour period provides time to respond to emergent conditions that would otherwise likely lead to entry into LCO 3.0.3 and a rapid plant shutdown, which is not justified given the low probability of an initiating event which would require the barrier(s) not capable of performing their related support function(s). During this 24 hour period, the plant risk associated with the existing conditions is assessed and managed in accordance with 10 CFR 50.65(a)(4)."

The bracketed paragraph is only included in NUREG-1433 and NUREG-1434, the Improved Standard Technical Specifications for BWR/4 and BWR/6 design plants. This difference is discussed in Section 5.1, "Definitions," under the topic "Single train systems (BWR)."

5.0 Impact on Maintenance Rule (A)(4) Program for Assessment And Management of Risk

5.1 Definitions

Degraded barrier

The Bases for LCO 3.0.9 state: "Barriers are doors, walls, floor plugs, curbs, hatches, mechanical devices, or other devices, not explicitly described in Technical Specifications that support the performance of the function of systems described in the Technical Specifications."

For the purposes of LCO 3.0.9, "barrier" refers to a barrier, or system of barriers, protecting one train of a safety system from a given initiating event. For example, an HELB barrier may contain multiple physical components, but is defined as a single "barrier" since it protects a train of a system from a specific initiating event. For the cases where multiple physical components make up the barrier, licensees will ensure that the degraded condition does not collectively last more than 30 days every time LCO 3.0.9 is used without declaring the supported systems LCOs not met.

A "degraded barrier," as discussed in this document, means a barrier that has been found to be degraded and must be repaired, or that is purposefully removed or reconfigured to facilitate maintenance activities. Momentary opening of a door to permit access to or egress from a room does not require assessment as a "degraded barrier" under this allowance. This activity should be covered through administrative controls. However, propping open doors, or running cables, ventilation devices, or other equipment through an open doorway that functions as a barrier constitutes a "degraded barrier."

Single train systems (BWR)

Most safety functions are served by dual or multi-train systems. For BWRs, HPCI (high pressure core injection), HPCS (high pressure core spray) and RCIC (reactor core isolation cooling) systems are single train systems for injecting makeup water into the reactor during an accident or transient event. RCIC system is not a safety system, nor required to operate during a transient, therefore, it does not have to meet the single failure criterion. Additionally, the HPCI or HPCS system provides backup if necessary in case of a RCIC system failure. The ADS (automatic depressurization system) and low pressure ECCS provide the core cooling function in the event of failure of HPCI or HPCS system during an accident. The ECCS, as a whole, not HPCI or HPCS system alone, must meet the single failure criterion.

Thus, for the purposes of LCO 3.0.9, the HPCI/HPCS, the RCIC system, and the ADS are considered independent subsystems of a single system. Therefore, these systems would be treated in the same manner as two redundant trains (of the same system) in a PWR. This allowance is stated in LCO 3.0.9 in the BWR ISTS (NUREG-1433 and NUREG-1434) and described in the BWR LCO 3.0.9 Bases.

5.2 Maintenance Rule Risk Assessment Program Implications

Use of LCO 3.0.9 requires that a risk assessment and management of the risk be conducted prior to using the degraded barrier allowance. Each licensee has a program in place to meet the requirements of the risk assessment and management provision of the Maintenance Rule, 10 CFR 50.65(a)(4). TSTF-427 relies on this program to address risk considerations, and requires some modification of the applicability of the current (a)(4) program.

It is recognized in NUMARC 93-01 that the rigor of licensee risk assessment programs may vary depending upon the degree to which plants perform online maintenance on multiple systems simultaneously. Thus, the ability to address the risk impact of multiple combinations of degraded barriers should be considered, and, as appropriate, restrictions may need to be placed on the use of LCO 3.0.9. This includes limiting the use of the LCO 3.0.9 to a reasonable number of degraded barriers at a given time, such that combinations of barriers/initiators are capable of being addressed by the risk assessment and management tool.

Procedures in place to implement this program will need certain modifications, as discussed below:

1. As part of the license amendment request to implement TSTF-427, the licensee must commit to the guidance of NUMARC 93-01, Section 11. Currently, NRC Regulatory Guide 1.182 provides that the NUMARC guidance is one acceptable approach to implement 10 CFR 50.65(a)(4). Implementation of TSTF-427 will require that the guidance is followed as written, and that alternative methods for assessment and management of risk are not used. The guidance as written provides some flexibility with respect to risk assessment and management approaches.

NUMARC 93-01 Section 11.3.2.6 states:

"Performance of maintenance *may involve alterations to the facility or procedures for the duration of the maintenance activity. Examples of these alterations include jumpering terminals, lifting leads, placing temporary lead shielding on pipes and equipment,* **removal of barriers***, and use of temporary blocks, bypasses, scaffolding and supports. The assessment should include consideration of the impact of these alterations on plant safety functions."* [emphasis added]

2. For implementation of this initiative, the plant program and procedures will need to be revised to ensure that the risk assessment and management process is used whenever a barrier that falls within the scope of LCO 3.0.9 is considered degraded, as per the definition in Section 5.1.

A comprehensive listing of plant barriers and their design basis function is not required to implement TSTF-427 as the risk analysis can be performed for degraded barrier(s) on a case-by-case basis. However, if one is available, it will save the licensee time in the performance of the risk assessment.

6.0 Risk Assessment and Management Considerations

This section describes considerations for risk assessment and management relative to the use of LCO 3.0.9. Licensees should consider barriers like any other piece of equipment that is out-of-service and to take appropriate actions. Existing Maintenance Rule (a)(4) programs are expected to be used.

6.1 Methods of Assessment

NUMARC 93-01 provides guidance for risk assessment during power operations (section 11.3.4) and during shutdown conditions (section 11.3.6). NUMARC 93-01 does not contain additional risk assessment guidance that specifically addresses plant conditions between power operations and shutdown. (The guidance notes that a transition risk assessment may be used if it is available, but this is an optional consideration in that it would generally be used to demonstrate offsetting risk impacts to support online maintenance.) However, the approach of NUMARC 93-01 can be used to address the use of LCO 3.0.9 with degraded barriers.

It is expected that consideration of the risk impacts of using LCO 3.0.9 will generally be performed qualitatively, or through a combination of quantitative and qualitative methods. For those plants capable of quantification, (i.e., have the barrier explicitly modeled in the PRA), the risk impact can be quantified and compared to the risk management thresholds provided in section 11.0 of NUMARC 93-01 as stated above. Appropriate risk management actions can then be implemented.

In performing this assessment, it should be ensured that adequate defense-in-depth for key safety functions will be preserved.

To ensure that the plant risk is quantitatively addressed in an integrated fashion, the actual plant configuration should be used when invoking LCO 3.0.9. When an emergent condition occurs, the original risk assessment will be re-evaluated in accordance with (a)(4).

6.2 Process for Risk Assessment for LCO 3.0.9

The overall process for determining if the use of LCO 3.0.9 is acceptable is shown in Figures 1 and 2. The steps in the process are discussed in more detail following the flowchart.

While LCO 3.0.9 does not limit the applicability to specific numbers of degraded barriers, caution should be used relative to the total number of barriers and/or systems for which the allowance is applied at any one time. In general, the scope of applicability of the allowance should be limited, as appropriate, based on the following considerations:

1. The overall risk importance of the system or combination of systems to which the allowance would be applied at a given time.

2. The dependencies between systems to which the allowance is applied at a given time.

3. The capability of the risk assessment tool to quantify the impact of the combinations of barriers to which the allowance is applied.

With regard to item 2, it is expected that either dependencies will be accounted for in the configuration-specific modeling or a qualitative assessment of dependencies will be performed. If the systems are independent, then the flowchart (Figures 1 and 2) can be used successively for each system, and the results added to determine the total risk. If there are dependencies between the systems, the actual risk may be greater than that indicated by adding the results of the flowchart applications. In this case, the barrier(s) should not be removed from both systems unless they are protecting against different (independent) initiating events, or unless the risk impact of the dependency is capable of being addressed by the risk assessment tool.

As general guidance, it is recommended that the use of LCO 3.0.9 to facilitate planned maintenance activities should consider the following:

1. The allowance should not normally be applied to more than two degraded barriers on a given train (e.g., more than two degraded barriers protecting the same train against different initiators).

2. The use of the allowance should normally be limited to no more than two degraded barriers on a given system at a single time (e.g., one degraded barrier protecting against one initiator on train A, and a degraded barrier protecting against another initiator on train B). However, this does not infer that the use of LCO 3.0.9 permits different barriers, protecting redundant trains against the same initiating event, to be removed from service simultaneously.

3. For maintenance planning purposes, it is a good practice to apply the allowance in a train-wise fashion, in conjunction with other plant-wide maintenance activities on the same train. This simplifies the assessment process, allows for risk management actions to ensure the availability of the opposite train, and is a standard risk management good practice.

4. If the barrier(s) in question protects against an external event (e.g., tornado), the use of LCO 3.0.9 for initiating events not modeled quantitatively should be limited to a barrier(s) on a single train at a time. See NUMARC 93-01 for severe weather guidance information.

The flowchart and corresponding discussion of the process is intended to evaluate the removal of one or more degraded barriers from service per system. The process needs to be repeated if considering additional degraded barriers protecting another system.

Figure 1
Process for Assessing the Acceptability of Using the Degraded Barrier Allowance – Part 1

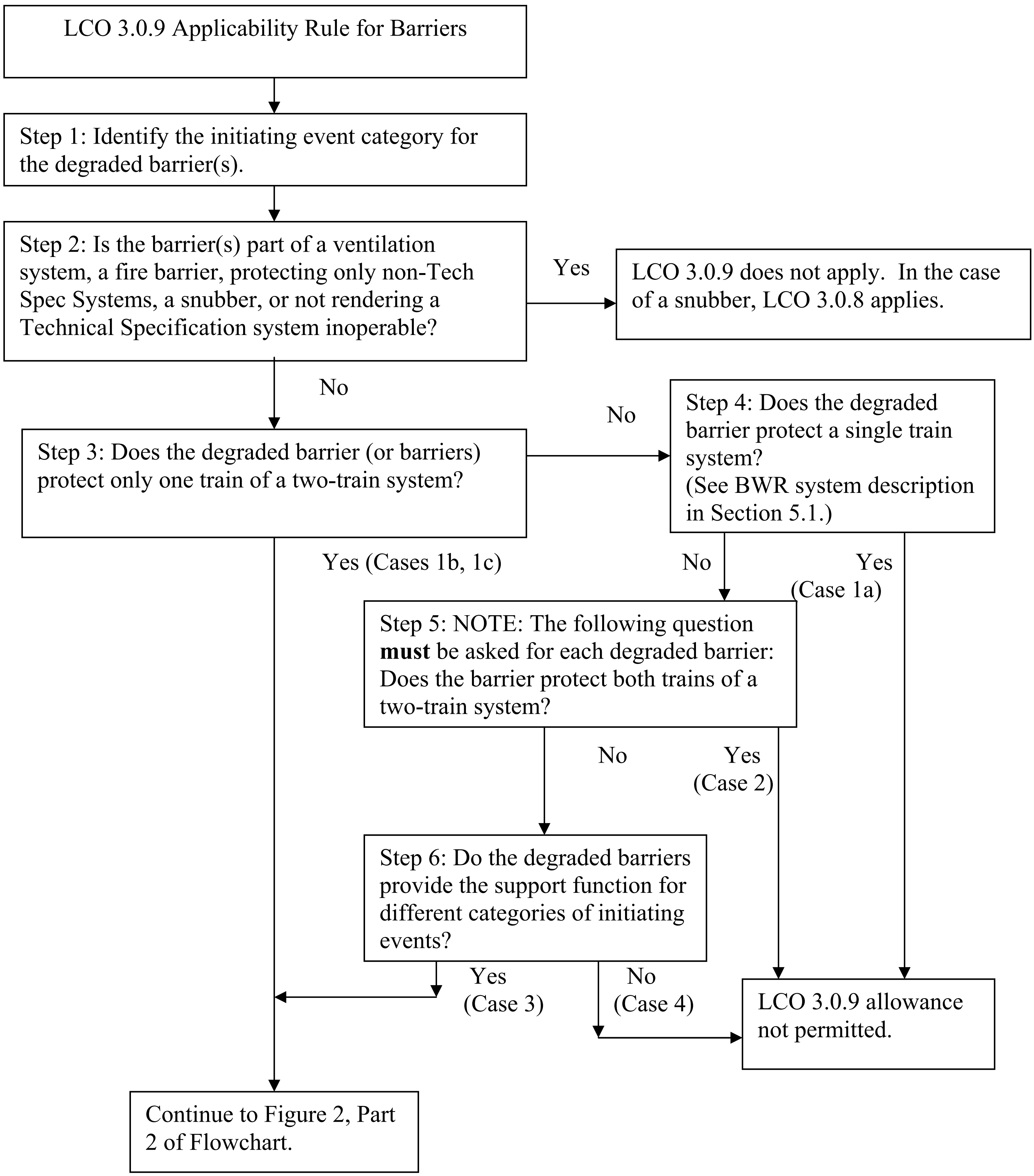
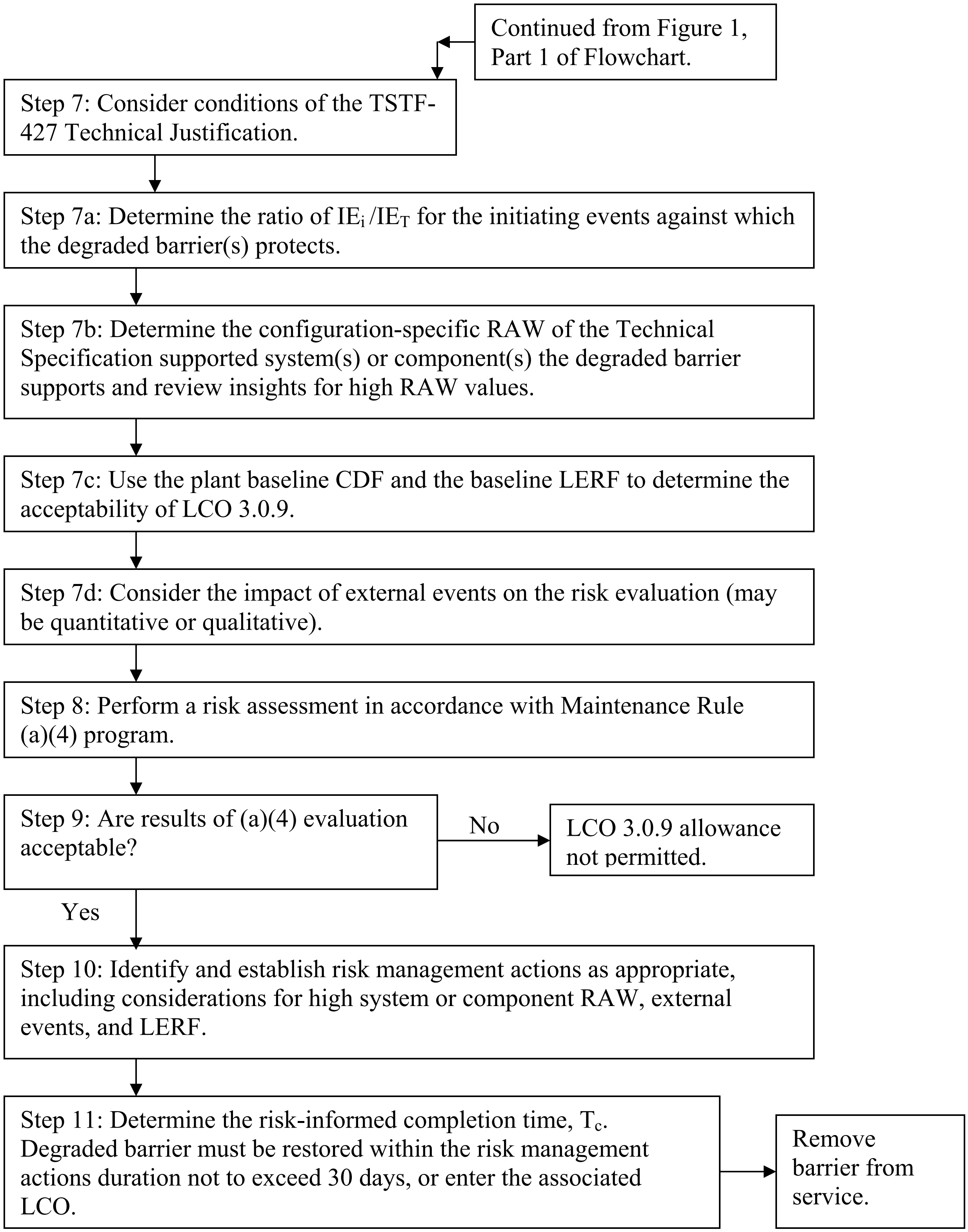


**Figure 2
Process for Assessing the Acceptability of Using the Degraded Barrier Allowance – Part 2**



Step 1: Identify the Initiating Event Category for the Degraded Barrier(s)

As stated in the Bases to LCO 3.0.9, the provisions of LCO 3.0.9 are based on the following initiating event categories:

- Loss of coolant accidents,
- High energy line breaks,
- Feedwater line breaks,
- Internal flooding,
- External flooding,
- Turbine missile ejection, and
- Tornado or high wind.

For the barrier(s) in question, determine the initiating event category (or categories) against which the barrier(s) is protecting the Technical Specification system.

If it is desired to use LCO 3.0.9 for a barrier protecting against an initiating event not on the above table, but within the frequency ranges considered in TSTF-427, (as discussed further in Step 7a), the Initiative 7a analysis is applicable for that initiator. However, should the initiating event frequency not be bounded by the frequencies given, plant-specific information must be provided for NRC approval.

Step 2: LCO 3.0.9 Barrier Exclusions

As stated in the Bases to LCO 3.0.9, this provision does not apply to barriers that support the following:

1. Ventilation systems (TSTF-287, Revision 5, "Ventilation System Envelope Allowed Outage Time," approved by the NRC on March 16, 2000, provides a 24-hour Completion Time for ventilation trains made inoperable by inoperable barriers),

2. Fire barriers (compensatory actions for degraded fire barriers are addressed in other regulatory requirements and associated plant programs),

3. Snubbers (which are covered by TSTF-372 and LCO 3.0.8.),

4. Non-Technical Specification systems, and

5. Supported Technical Specification system(s) if the inability of a barrier(s) to perform its support function does not render the supported system inoperable.

If "Yes," then LCO 3.0.9 does not apply. If "No," then proceed to Step 3.

Step 3: Number of Trains of a Two-Train System Impacted

There are four specific cases of combinations of trains and barriers that are considered in the process. The four cases are:

Case 1: One or more barriers protect one train of a system
Case 2: One barrier protects both trains of a two-train system
Case 3: Different barriers protect different trains of the same system for different initiating events (no dependencies)
Case 4: Different barriers protect different trains of the same system for the same initiating event

The individual cases can be further described as shown in Table 1. See Appendix B for a corresponding table and notes for plants with three-train systems. The IE_i indicates that the barrier protects the Technical Specification equipment from initiating event "i."

Table 1 – Process Cases for a One or Two-Train System

Case	Train 1 of System A Impacted by Barrier(s)	Train 2 of System A Impacted by Barrier	Comment
1a	Barrier 1 - IE_1	N/A - Single Train System	LCO 3.0.9 not allowed.
1b	Barrier 1 - IE_1	No	LCO 3.0.9 allowed subject to MR risk assessment (Step 8).
1c	Barrier 1 - IE_1 Barrier 2 - IE_1 or IE_2	No	LCO 3.0.9 allowed subject to MR risk assessment (Step 8).
2	Barrier 1 - IE_1	Barrier 1- IE_1	LCO 3.0.9 not allowed.
3	Barrier 1 - IE_1	Barrier 2 - IE_2	LCO 3.0.9 allowed subject to MR risk assessment (Step 8).
4	Barrier 1 - IE_1	Barrier 2 - IE_1	LCO 3.0.9 not allowed.

Case 1 represents a barrier or barriers that impact only one train of a system. The system may have only one train or two trains. Case 1a is not allowed regardless of the initiating event since a loss of system function could result. An example of this would be a barrier on the Refueling Water Storage Tank, which is considered a single system (component). Cases 1b and 1c may be acceptable after satisfying the performance of a risk assessment in Step 8.

Case 2 represents a single barrier that impacts both trains of a two-train system. This condition is not allowed by LCO 3.0.9 as it also involves a potential loss of system function.

Case 3 represents different barriers impacting both trains of a two-train system with each barrier protecting against a different initiating event. This situation may be acceptable after performance of a risk assessment in Step 8.

Case 4 represents different barriers impacting both trains of a two-train system with each barrier protecting against the same initiating event. This condition is not allowed by LCO 3.0.9, as it involves a potential loss of system function.

Step 3 asks if only one train of a two-train system is protected by a barrier(s). If "Yes," then Cases 1b and 1c apply and the process proceeds directly to Step 7. If "No," then a check of the other combinations of trains and barriers is made in the next three steps.

Step 4: A Barrier Protecting a Single Train System

This step checks for Case 1a, where a degraded barrier protects a single train of a single train system. (See BWR system description in Section 5.1.) If the answer is "Yes," then this condition is not allowed by LCO 3.0.9, as it involves a potential loss of system function. If the answer is "No," then proceed to the next step to check for Cases 2, 3, and 4.

Step 5: Check for Acceptable Combinations of Barriers and Trains: Single or Multiple Barriers, Both Trains of Same System

Does the degraded barrier protect both redundant trains of the same system from the same initiating event? (This question must be asked for each degraded barrier.) If "Yes," then Case 2 is in effect and the LCO 3.0.9 allowance is not permitted to be applied to the barrier, as this results in a potential loss of system function. If the response is "No," then it is implied that there are different barriers that protect each train of a system. This may or may not be acceptable depending on the initiating event(s) and the results of the risk assessment. The process continues to the next step to check Cases 3 and 4.

Step 6: Different Barriers That Impact Both Trains

Do the degraded barriers impact both trains of the same system and provide protection against different categories of initiating events? If "Yes," then Case 3 is in effect. These conditions may be acceptable after the performance of a risk assessment in Step 8. If "No," then Case 4 is in effect since the barriers must protect against the same initiating event. LCO 3.0.9

allowance would not be permitted for this condition, as a potential loss of system function could result.

Step 7: Consider Conditions of the Technical Justification for use of LCO 3.0.9

To arrive at Step 7, one of two situations must have occurred: 1) one or more barriers protect a single train of a two-train system, or 2) two or more barriers protect both trains of a two-train system, each providing support for different initiating events. Step 7 evaluates and determines plant-specific parameters discussed in the technical justification provided in TSTF-427 that are used in the plant risk assessment to justify the use of the LCO 3.0.9 allowance. (The user is not limited by the example used in the TSTF-427 technical justification.) When these data are determined, insights from the information can be used in the performance of a risk assessment in accordance with the licensee's (a)(4) program for the barrier(s) in question.

The technical justification for removal of a barrier in TSTF-427 is based on the following equation for the incremental core damage probability (ICDP) and input parameters:

$$ICDP = \left[\frac{T_C}{8766} \times \frac{IE_i}{IE_T}\right] \times [(RAW_j \times CDF_{base}) - CDF_{base}]$$

where,

1. IE_i / IE_T is the ratio of the initiating event frequency for which the degraded barrier is designed to mitigate to the total initiating event frequency for the plant.
2. Configuration-specific Risk Achievement Worth (RAW_j) for the protected equipment j is the importance (to CDF) of the Technical Specification equipment (train or component) for which the degraded barrier is designed to protect.
3. CDF_{base} (per reactor year) is the base case CDF.
4. T_c (hours) is the length of time the affected barrier is unavailable, or the allowed time.

Step 7a: Determine the Ratio of IE_i / IE_T

The provisions of LCO 3.0.9 are justified because of the low risk associated with barriers not being capable of performing their required support function. This provision is based on consideration of the following initiating event categories:

- Loss of coolant accidents,
- High energy line breaks,
- Feedwater line breaks,
- Internal flooding,
- External flooding,
- Turbine missile ejection, and
- Tornado or high winds.

The user is not limited by the example used in the TSTF-427 technical justification. LCO 3.0.9 may be expanded to other initiating event categories, provided plant-specific analysis demonstrates that the frequency of the additional initiating events is bounded by the generic analysis provided in TSTF-427 or plant-specific approval is obtained from the NRC.

The user should determine the ratio of IE_i / IE_T and confirm on a plant-specific basis that for any initiator used to justify use of LCO 3.0.9, the bounding value of 9.1E-3[1] is not exceeded. The user should determine on a plant-specific basis the ratio of IE_i / IE_T for each initiator against which the barrier protects where each term is defined as follows:

- IE_i (per year) is the frequency of the initiating event for which the affected barrier is designed to mitigate, and
- IE_T (per year) is the total initiating event frequency for the plant.

This ratio should be determined for each initiating event for which the affected barrier is designed to protect against whether or not the affected initiator was considered in the example in TSTF-427. The resultant sum of all the ratios should be less than the bounding value of 9.1E-03.

For those users that have only internal events PRAs and the barrier(s) in question protects against an external event (e.g., tornado), the expectation is that the user will make a reasonable effort to determine the initiating event frequency on a generic basis taking into account the physical location of the plant. For example, a plant in Kansas should ensure that an appropriate tornado initiating event frequency is determined for that area of the country.

Step 7b: Determine the Risk Achievement Worth (RAW) Value

Determine the configuration-specific RAW value[2] of the Technical Specification supported system(s). If the RAW value is high or expected high, generally taken to be on the order of 100 or above for a single

[1] 9.1E-03/yr is the value of the most likely initiator for which this LCO would apply, based on a steam line break, per NUREG 5750, Table G-1. Further, IE_T was assumed equal to 1/yr. This was the limiting case used in NRC's review of the initiative. See TSTF-427 for additional discussion.

[2] All subsequent references to RAW values are intended to be configuration specific.

component or for several systems or components considered collectively, the expectation is that the rigor of the risk analysis and review of insights will correspondingly increase. In general, when the RAW value is 100 or greater, LCO 3.0.9 should not be invoked. However, an assessment can be performed that considers more than the numerical value of RAW. If the equipment is modeled in the PRA (or an acceptable surrogate is used), then a review of the important sequences that drive the RAW value is recommended to better understand the risk profile. This cut set review will provide valuable information and insights relative to the barrier(s) being taken out-of-service and will increase the overall understanding of the risks associated with the barrier removal.

The following guidance is provided to help determine the RAW value.

1. If a single barrier affecting a single Technical Specification component in a system is degraded, the RAW value is just the RAW value of the protected component (or suitable surrogate, e.g., RAW value of the system train) obtained from configuration-specific PRA. This can be obtained directly from the basic event(s) in question.

2. If a single barrier affecting a single Technical Specification component in a system is degraded, the RAW value can be estimated by setting the component to out-of-service in the PRA and solving the model. The resultant RAW value of the protected component (or suitable surrogate) is the ratio of the new CDF to the base case CDF.

3. If multiple Technical Specification equipment in different systems are involved due to multiple barriers being removed at the same time, the configuration-specific RAW from all affected systems/components needs to be considered.

   If there are interactions or dependencies between the affected components or systems (or it is desired to determine if such dependencies exist), perform a specific evaluation using a configuration-specific model to determine the RAW value of the combined failure of the components. This can be performed by solving for (or by using pre-solved configurations of) out-of-service plant equipment to determine the combined RAW value of the Technical Specification systems/components for the degraded barriers. The RAW value is estimated from the ratio of the CDF to the base case CDF.

Step 7c: Check the Plant Baseline CDF and LERF

The example in the technical justification assumes that the baseline CDF and large early release frequency (LERF) is such that the estimated ICDP and incremental large early release probability (ILERP) remain within acceptable limits for up to a maximum of 30 days. The maximum values used in the Technical Justification are CDF < 1E-04/reactor-year and LERF < 1E-05/reactor-year. While the licensee is not limited by the values in the technical justification, the licensee should use the plant baseline CDF and LERF in conjunction with the RAW value and initiating event frequency previously evaluated in determining any risk management actions.

Step 7d: Consider the Impact of External Events on the Risk Evaluation

If the plant baseline CDF and LERF already contain external events, then no further action is needed in Step 7d since these events have already been considered in the quantitative analysis.

It is recognized, however, that in some cases, the above values are calculated using only an internal events PRA. In this case, consideration should also be given to the CDF and LERF contribution from external events. Based on the barrier(s) involved, a qualitative assessment should be made. Based on this assessment and the impact of the external events involved, some additional margin to account for their contribution to the CDF and LERF should be considered.

Note: If the PRA considers internal events only and the initiator(s) of interest is related to an external event, then for these initiating event categories there will be no contribution to the internal CDF and consequently no risk delta unless generic data or PRA surrogate information are used for Steps 7a through 7d. For this situation, a qualitative assessment should be made for the barrier(s) being considered for removal from service to determine any additional insights to be used in the risk assessment performed in Step 8.

Plant studies have been performed for the purposes of the Individual Plant Examination for External Events (IPEEE). These studies have involved either PRAs, or screening methods such as Fire Induced Vulnerability Analysis (FIVE) or Seismic Margins Analysis (SMA), and screening studies for other external events (such as external floods or high winds). These studies provide information that may be helpful in determining the external events risk contribution. For example, plant systems or components that participate in safe shutdown paths identified through FIVE or SMA evaluations should be considered to have external events risk importance. Another way external events risk importance can be accounted for is by modifying the RAW value using the insights from the IPEEE and similar analyses. Risk management actions should take this into account, even if the external events risk importance cannot be directly quantified.

If PRAs have been performed for external events, then insights from these PRAs can be used to establish risk management actions. Caution should be used in adding the results of various PRA models, depending upon their biases, degree of modeling detail, and other considerations.

Step 8: Risk Assessment

The technical justification assumes acceptable ICDP values will result to justify up to a 30-day time period based on consideration of the ratio of IE_i /IE_T being less than the bounding value of 9.1E-03, acceptable RAW value of the Technical Specification supported system, and acceptable plant baseline CDF and LERF values. The risk assessment may determine up to a maximum 30-day acceptable time period before the LCO of the Technical Specification supported system must be entered if the barrier(s) has not been restored to fulfill its support function. If the risk assessment does not support removal of the barrier from service without declaring the supported system inoperable, then the LCO 3.0.9 allowance should not be used.

Performance of a risk assessment necessitates having some basic information regarding the barrier in question. Specifically the following must be known about the barrier and its supported system:

1. The Technical Specification system or equipment that it supports
2. The initiator(s) for which the barrier is protecting against
3. The initiating event frequency for the initiator in question
4. The RAW value of the Technical Specification supported system(s) or component(s)

The barrier that cannot perform its required support function will be evaluated and managed under the Maintenance Rule 10 CFR 50.65(a)(4) risk assessment and management program (see Section 5.0), and associated industry guidance (NUMARC 93-01, Revision 3). This provision is applicable whether the barrier is degraded due to planned maintenance or due to a discovered condition. Should the risk assessment and risk management actions for a specific plant configuration, or emergent condition, not support the maximum 30-day allowed time period, the (a)(4) risk management action must be implemented for the acceptable time frame or the supported system's LCO be considered not met.

Step 9: Results of Risk Assessment

The process for defining actions to be taken based on the risk assessment is listed in NUMARC 93-01 and is shown below for illustrative purposes.

NRC Regulatory Guide 1.182, "Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants," provides the following table of ICDP values and risk management actions:

"ICDP and ILERP, for a specific planned configuration, may be considered as follows with respect to establishing risk management actions:"

ICDP	ACTION	ILERP
$> 10^{-5}$	- configuration should not normally be entered voluntarily	$> 10^{-6}$
10^{-6} to 10^{-5}	- assess non-quantifiable factors - establish risk management actions	10^{-7} to 10^{-6}
$< 10^{-6}$	- normal work controls	$< 10^{-7}$

There may be other similar processes based on RG 1.182 and NUMARC 93-01 that define risk management actions and determine acceptable time frames, such as those that result in colors or use other defense-in-depth methods to define specific risk levels and risk management actions.

If the results of the risk assessment are acceptable (“Yes”), continue to Step 10 for final considerations prior to barrier removal. If the results are not acceptable (“No”), then the LCO 3.0.9 allowance is not permitted.

Step 10: Risk Management Actions

There are additional actions that may need to be taken based on considerations of the risk assessment. It is recognized that typically the above values are estimated using the internal events PRA. If this is the case, consideration should also be given to the CDF and LERF contribution from external events. Since these metrics are not quantified, or integrated with internal events at many plants, it is reasonable to provide some margin to account for their contribution. Additionally, it would be prudent to consider risk management actions for the removal of barriers from components with higher RAW values, even if the ICDP and ILERP (or equivalent) are within the “normal work controls” region. In particular, controls on maintenance unavailabilities of the remaining train should be considered.

Step 11: Determine the Risk-Informed Completion Time, T_c

Using an ICDP equation, such as is given in Section 6.2 Step 7, determine the risk-informed completion time, T_c. The equation in Step 7 solved for T_c is given below (variables defined in Step 7):

$$T_C = \frac{ICDP \times 8766}{\frac{IE_i}{IE_T} \times [(RAW_j \times CDF_{base}) - CDF_{base}]}$$

This guideline recommends an ICDP value of 1.0E-06 be used in the calculation. (Such a value is used in the example in Appendix A.)

After the risk management actions are defined and implemented, and the risk-informed completion time has been determined, the barrier(s) may be removed from service.

6.3 Inoperability of the Second Train

With a barrier out of service as per the process described in Section 6.2, an emergent or planned condition may affect the required Operable redundant (second) train. If the required Operable train or subsystem becomes inoperable while LCO 3.0.9 is in use, the second train must be restored to Operable status within 24 hours or the provisions of LCO 3.0.9 cannot be applied.

There are three cases that apply:

- The second train is impacted by the failure of Technical Specification equipment itself. In this case, the 24-hour limit applies.

- The second train is impacted by the failure of a barrier that protects the Technical Specification equipment from the same initiating event as the barrier on the first train. In this case, the 24-hour limit applies.

- The second train is impacted by the failure of a barrier that protects the Technical Specification equipment from a different initiating event as the barrier on the first train. In this case, the 24-hour limit does not apply. LCO 3.0.9 is still in effect as per Case 3 of Table 1. However, the risk assessment must be performed again to determine if a) new risk management actions are required, and b) there is a change to the risk-informed completion time, T_c.

7.0 Example Assessment

Appendix A provides an example of a risk assessment approach based on Reg Guide 1.182 and NUMARC 93-01 that defines risk management actions resulting in "colors" to define specific risk levels and risk management actions.

Note: Appendix A provides a plant-specific example. As such, the risk management thresholds and assessment methods reflect one approach, but other methods are acceptable. The example is provided for illustration purposes only.

8.0 Documentation

Programs for risk assessment and management are required to be proceduralized in accordance with NUMARC 93-01. For a single barrier removed from service, documentation should be consistent with that currently used for Maintenance Rule risk assessments. However, for cases when multiple systems and/or multiple occurrences of LCO 3.0.9 are involved, documentation of the risk assessment and the risk management actions should be retrievable and available for inspection by the NRC staff. Examples of information that could be requested by the NRC are: qualitative considerations and compensatory measures (if needed), what barriers are removed, the applicable calculations, the applicable risk management actions, the calculated allowed time, and the times of barrier removal and restoration to show that the 30-day limit was met.

APPENDIX A

Example of a Risk Assessment Program for Barriers

This is an example of a matrix process that uses pre-solved configurations of various single and combination maintenance events for Technical Specification (TS) equipment that are impacted by removal of a barrier from service that protects the TS equipment. It is assumed that the ratio of the initiating event frequency in question to the total initiating event frequency (IE_i / IE_T) is equal to the bounding value of 9.1E-03 and the plant baseline CDF and LERF values are 2.48E-05/reactor year and 5.00E-06/reactor year, respectively. This process could be extended to any number of TS systems or components. Only selected systems/components were chosen for this example.

To use the PRA matrix, the user highlights the row(s) and column(s) for each TS system/function(s) that is in maintenance and (absent use of LCO 3.0.9) would not be Operable due to a degraded barrier. The intersections are quantified by calculating a core damage frequency (CDF) and subsequently a Risk Achievement Worth (RAW) value with the single or two systems/functions placed in maintenance. Using an incremental core damage probability (ICDP) limit of 1.0E-06[3], an allowed time can be calculated for the barrier to be out-of-service before the TS of the protected system(s) must be entered. If the calculated time, T_c, exceeds 30 days, then the backstop of 30 days is used. If the time is less than 30 days, then the actual time calculated is used. The colors (discussed later), which are determined from either the RAW value obtained or the conditional CDF, identify the level of management compensatory actions needed during the period when the barrier is out-of-service. Table A-2 contains a listing of the systems/components used in this example.

The first step in quantifying the PRA matrix is to determine the CDF_1 for the single TS component out-of-service and the CDF_2 for combinations of TS equipment out-of-service. Table A-3 contains the results of this analysis. The calculations are performed by taking the affected system(s)/functions(s) out-of-service and solving the PRA. Only one train of a system is assumed to be in maintenance for this example.

Each intersection on Table A-3 has been divided into two columns. The first column contains the CDF_2 associated with the intersection of the systems/components. The second column contains the RAW value associated with the combination of systems/component out-of-service referenced to the base case CDF. The RAW value can be determined by dividing the CDF_2 for the intersection by the base case CDF of 2.48E-05.

From Table A-3 it can be seen that the CDF for an intersection is dependent on which piece of equipment was initially taken out-of-service in the PRA. For example, the CDF for the AFWtp, EDG intersection is 6.5E-04 based on the cut set with AFWtp in maintenance. Using the cut set file with the EDG in maintenance, the CDF is 5.95E-04.

[3] Note this is a plant-specific value, and NUMARC 93-01 provides for other values to be chosen as appropriate.

These differences are mainly due to truncation of cut sets below a certain value. If the truncation limit were low enough, there would be no difference in the numbers. When differences exist, the higher CDF (RAW) value is used for the final determination of acceptability to remove the barrier. This is reflected in the subsequent tables.

Table A-4 shows the PRA Matrix with the limiting RAW values from Table A-3 for the case where a degraded barrier impacts two TS systems/functions. It also shows (under the RAW column) the RAW value for a degraded barrier that impacts only one TS system. As before, these RAW values were calculated from Table A-3 by dividing CDF_1 by the base case CDF of 2.48E-05/year.

Determination of Risk Management Actions Levels

Apply the following guidelines to the RAW values on Table A-4 to determine the level of management actions needed prior to removal of the barrier.

1. **Set the Yellow-Orange Conditional CDF Threshold Value**

   The Yellow-Orange threshold value is based on the base case CDF of the plant. All other threshold levels are fixed. The Green-Yellow threshold is twice the baseline CDF and is based on NUMARC 93-01 criteria, i.e., a system or component is not considered risk significant if it has a RAW value less than 2.

   The Orange-Red threshold is also based on NUMARC 93-01 criteria where it states, *"maintenance configurations with a configuration specific CDF in excess of 10^{-3} / year should be carefully considered before voluntarily entering such conditions."*

   The Yellow-Orange threshold value is taken to be the time it takes to reach an ICDP of 1.0E-06. This time period is chosen to be 36 hours, which represents one half of a 72-hour Technical Specification Completion Time. (A 72-hour Completion Time is used for illustrative purposes.) If a maintenance activity is expected to last longer than one half of the Technical Specification Completion Time, the Plant Operations Review Committee (PORC) will typically convene to discuss specific additional risk management actions to be taken to minimize the risk during the maintenance evolution.

   The equation used to set the Yellow-Orange threshold is as follows:

   Y-O threshold = [(1.0E-06 x 8760 hrs/yr x 0.9 plant capacity factor)/36 hrs]

   + base case CDF/yr

   For this specific example, the base case CDF is 2.48E-05/year. Yellow-Orange threshold is therefore 2.5E-04/year. The remaining discussion in this section assumes a base case CDF of 2.48E-05/year. (Note: If a plant had a base case CDF of 2.0E-04/year, the Yellow-Orange threshold (assuming 0.9 capacity factor) would be 4.2E-04/year with Yellow being less than or equal to 4.2E-04/year and Orange being greater than 4.2E-04/year.)

2. **<u>Green Conditions: Risk Level – Green</u>**

Is the RAW value 2 or less? For the Maintenance Rule (NUMARC 93-01 criteria), a system or component is not considered risk significant if it has a RAW value less than 2.

Green conditions denote minimum risk. The plant is fully capable of performing the associated safety functions. No additional risk assessment actions are required from plant personnel.

Management Action – Green

Normal work controls would be employed for configurations having nominal safety significance. This means that the normal plant work control processes are followed for the work activity, and that no additional actions to address risk management actions are necessary.

Work Planning Phase

Work Control Staff reviews the scheduled risk evaluation.

Work Execution Phase

Work Control Operations SRO shall verify the work schedule and issue clearance to begin work once the acceptable length of time the degraded barrier can be unavailable is determined.

3. **<u>Yellow Conditions: Risk Level – Yellow</u>**

Is the RAW value greater than or equal to 2 and the CDF associated with the TS equipment (i.e., taking the RAW value listed on Table A-4 and multiplying it by the base case CDF of 2.48E-05/year) less than or equal to 2.5E-04/year? For the Maintenance Rule, a system or component is considered risk significant if it has a RAW value greater than or equal to 2.

The CDF value of 2.5E-04/yr is shown on Table A-1 and is based on the time it takes to reach an ICDP of 1.0E-06. This value was determined in step 1 of this Section. This time period corresponds approximately to 36 hours. Many TS completion times are 72 hours. As stated earlier, typically, a plant will not exceed half of this value (36 hours) without an additional level of planning and authorization from, for example, the PORC. While an ICDP of 1E-05 is acceptable for planning and work execution with the proper risk management actions in place, setting a value of 1E-06 provides an acceptable threshold to address increased risk levels above the Green level.

Yellow conditions denote a reduced safety condition. The plant's ability to perform the associated safety function is reduced, but acceptable.

Management Action – Yellow

Risk management actions for yellow conditions are focused on providing increased risk awareness. Operations and Maintenance personnel shall discuss the planned work activity within their respective organizations to increase Operator and Maintenance awareness of the risk of the work activity.

Work Planning Phase

Work Control Staff reviews the scheduled risk evaluation.

Work Execution Phase

Operations SRO assigned to Work Control Center shall verify the work schedule. Maintenance Teams shall be aware of the risks associated with their tasks, and shall review any risk reduction measures they are responsible for completing. Clearance will be given to begin work once the acceptable length of time the degraded barrier can be unavailable is determined.

4. **Orange Conditions: Risk Level – Orange**

Is the CDF associated with the TS equipment (i.e., taking the RAW value listed on Table A-4 and multiplying it by the base case CDF of 2.48E-05/year), greater than 2.5E-04/yr but less than 1E-03/year (see Table A-5)?

Orange conditions denote that the key safety function is in a degraded condition, and steps shall be taken to manage this condition.

Management Action – Orange

When entering a planned activity that has been assessed as an orange condition, prior PORC approval is required. Identical planned activities that have already received PORC approval in the past do not require additional PORC review. Changes made to planned activities that have been previously reviewed and approved by the PORC shall be reviewed by the PORC Chairperson to determine if a subsequent review by the PORC is required. There must be a written Risk Management Plan overseen by the Work Control organization with input from other groups as necessary. This Risk Management Plan shall be developed as outlined in the Risk Management Process directive.

When entering an orange condition from emergent work, an Operations SRO assigned to the Work Control Center will ensure development of a work plan to restore the degraded barrier. This may require input from other groups as necessary. The Operations Shift Manager (OSM) will evaluate the restoration plan and have final authority whether the plan is implemented. Additionally, at the OSM's discretion, development of a written risk management plan for actions to be taken in the event of further degradations may be required.

Work Planning Phase

Work Control shall ensure the development of a written Risk Management Plan, including risk reduction measures.

Work Execution Phase

Operations will verify the work schedule and guidance on the activities then release the work for execution. Maintenance must understand when a work activity affects risk significant SSCs, the risk level of that work and any required actions as designated in a Risk Management Plan. Clearance will be given to begin work once the acceptable length of time the degraded barrier can be unavailable is determined.

5. **Red Conditions: Risk Level – Red**

Is the CDF associated with the TS equipment (i.e., taking the RAW value listed on Table A-4 and multiplying it by the base case CDF of 2.48E-05/year) greater than or equal to 1E-03/year as shown on Table A-5? The CDF threshold guideline of NUMARC 93-01 is exceeded, and LCO 3.0.9 should not be used.

Management Action – Red

The barrier cannot be removed without entering the TS action statement for the affected equipment.

In Summary:

Table A-1
Summary Table Based on Base Case CDF of 2.48E-04/year

Risk Assessment Tool Color	RAW or CDF Value used to Determine Risk Assessment Tool Color
Green	RAW ≤ 2
Yellow	RAW > 2 and CDF ≤ 2.5E-04/year
Orange	2.5E-04/year < CDF ≤ 1E-03/year
Red	CDF > 1E-03/year

Table A-5 indicates those interactions that result in a CDF between 2.5E-05 and 1E-03/year (Orange condition) as well as those that result in a CDF > 1E-03/year (Red condition). As stated above, for a red condition, the barrier could not be made unavailable without entering the action statement for the affected TS equipment. Table A-6 contains the final results of the assessment converted to the Risk Assessment Tool colors using the above guidelines.

The Risk Assessment Tool colors define the appropriate management and compensatory actions to be taken when the barrier is out-of-service. The maximum time the barrier can be out-of-service (up to a backstop of 30 days) until the TS for the supported equipment must be entered still needs to be calculated.

<u>Determination of the Completion Time, T_c</u>

As stated in the body of this document T_c, the length of time the degraded barrier can be unavailable, is given by:

$$T_C = \frac{ICDP \times 8766}{\frac{IE_i}{IE_T} \times [(RAW_j \times CDF_{base}) - CDF_{base}]}$$

In this Appendix, IE_i / IE_T is equal to the bounding value of 9.1E-03, the plant baseline CDF = 2.48E-05/reactor year, and the ICDP is 1E-06. The values of RAW_j for both a barrier impacting one TS system/function and a barrier impacting two TS systems/functions come from Table A-6. Substituting in the values and solving for T_c provides the maximum allowed time the barrier can be out-of-service without entering the action statement for the supported TS system(s)/function(s). If the value of T_c exceeds 30 days, then a 30-day time limit is used.

Table A-7 provides the calculated values of T_c. As can be seen, the barrier can be removed for up to the 30-day limit for those single and double TS impacted systems/functions indicated by the green, yellow, and orange conditions after implementing the appropriate risk management actions. For those red conditions where the conditional CDF exceeds 1E-03, the barrier cannot be removed from service without entering the TS action statement of the affected system(s)/function(s) even though the calculated allowed time may be acceptable due to the risk impact of the barrier removal.

TABLE A-2

Listing of Systems/Components Used in the Example

	System	**Identifier**
Electrical	230/525 kV Switchyard Systems	SYD
	Emergency Diesel Generator System	EDG
	4.16 kV Essential Power	4.16KV
	Shared Transformer - the function of being able to tie power between units	SAT
SG Cooling	Auxiliary Feedwater Motor Driven Pump	AFWmp
	Auxiliary Feedwater Turbine Driven Pump	AFWtp

Table A-3
Example PRA Matrix for Barriers Impacting the Following Tech. Spec. Systems/Components

	CDF_1*	**Electrical**		**Electrical**		**Electrical**		**Electrical**		**S/G Cooling**		**S/G Cooling**	
Base PRA		**SYD**		**EDG**		**4.16 KV**		**SAT**		**AFWmp**		**AFWtp**	
	2.48E-05	CDF_2#	RAW+	CDF_2#	RAW+	CDF_2#	RAW+	CDF_2#	RAW+	CDF_2#	RAW+	CDF_2#	RAW+
SYD	3.64E-05	N/A	N/A	1.22E-04	4.9	4.66E-04	18.8	4.76E-05	1.9	3.64E-05	1.5	1.15E-04	4.6
EDG	8.50E-05	3.85E-04	**15.5**	N/A	N/A	1.43E-03	57.6	1.16E-04	4.7	8.50E-05	**3.4**	5.95E-04	24.0
4.16 KV	1.43E-03	3.06E-03	**123.3**	1.43E-03	57.6	N/A	N/A	1.57E-03	63.2	1.43E-03	**57.6**	6.84E-03	**275.5**
SAT	2.59E-05	4.76E-05	1.9	1.16E-04	4.7	1.57E-03	63.2	N/A	N/A	4.22E-05	1.7	1.73E-04	7.0
AFWmp	4.10E-05	7.64E-05	**3.1**	6.93E-05	2.8	4.65E-04	18.8	4.22E-05	1.7	N/A	N/A	8.61E-04	**34.7**
AFWtp	1.30E-04	5.58E-04	**22.5**	6.50E-04	**26.2**	2.10E-03	84.7	1.73E-04	7.0	7.67E-04	30.9	N/A	N/A

*This column represents the base case CDF/year and CDF/year with a barrier affecting only one TS system/function.
CDF/year with a degraded barrier that impacts two systems/functions.
+ RAW for the combined systems/functions out-of-service calculated by dividing the CDF_2 by 2.48E-05 (base case CDF).
Note: RAW values in bold show differences in PRA solution dependent upon which equipment is first taken out-of-service. These values are limiting and should be used.

Table A-4
**Summary of RAW Values for Combinations of Tech. Spec.
Equipment Out-of-Service (from Table A-3)**

	A	C	D	E	F	G	H	I	J
1			**RAW**	Electrical				SG Cooling	
2				SYD	EDG	4.16 KV	SAT	AFW mp	AFW tp
3	Base Case		1.0	1.5	3.4	57.6	1.0	1.7	5.2
4	Electrical	SYD	1.5		15.5	123.3	1.9	3.1	22.5
5		EDG	3.4	_		57.6	4.7	3.4	26.2
6		4.16 KV	57.6	_	_		63.2	57.6	275.5
7		SAT	1.0	_	_	_		1.7	7.0
8	SG Cooling	AFWmp	1.7	_	_	_	_		34.7
9		AFWtp	5.2	_	_	_	_	_	

Note: The values listed in the RAW column are for the case of one or more barriers impacting one TS system/component and are calculated from data on Table A-3. Example: RAW for only the 4.16 KV system that has a degraded barrier = 1.43E-03/2.48E-05 = 57.6, where 1.43E-03 is the CDF_1 from Table A-3.

Table A-5
Determination of Red Interactions that Indicate a CDF > 1E-03/year
or Orange Interactions between 2.5E-04/year < CDF ≤ 1E-03/year

		RAW	Electrical				SG Cooling	
			SYD	EDG	4.16 KV	SAT	AFWmp	AFW tp
Base Case		1.0	1.5	3.4	> 1E-03	1.0	1.7	5.2
Electrical	SYD	1.5		>2.4E-4 ≤1E-03	> 1E-03			>2.4E-4 ≤1E-03
	EDG	3.4	_		> 1E-03			>2.4E-4 ≤1E-03
	4.16 KV	> 1E-03	_	_		> 1E-03	> 1E-03	> 1E-03
	SAT	1.0	_	_	_			
SG Cooling	AFWmp	1.7	_	_	_	_		>2.4E-4 ≤1E-03
	AFWtp	5.2	_	_	_	_	_	

Note: Determine if the CDF > 1E-03/year or between 2.5E-04/year and 1E-03/year by taking the combined RAW value listed on Table A-4 and multiplying it by the base case CDF of 2.48E-05/year. If the CDF is greater than 1E-03/year, then a Red condition exists and the barrier cannot be removed without declaring the TS system inoperable (regardless of the allowed time calculated). If the CDF is >2.5E-04 but ≤ 1E-03/year, then an Orange condition exists.

Table A-6
Final Risk Assessment Tool PRA Matrix For Consideration of Barrier Removal

	A	C	D	E	F	G	H	I	J
1			**RAW**	Electrical				SG Cooling	
2				SYD	EDG	4.16 KV	SAT	AFW mp	AFW tp
3	Base Case		1.0 G	1.5 G	3.4 Y	57.6 R	1.0 G	1.7 G	5.2 O
4	Electrical	SYD	1.5 G	N/A	15.5 O	123.3 R	1.9 G	3.1 Y	22.5 O
5		EDG	3.4 Y	15.5 O	N/A	57.6 R	4.7 Y	3.4 Y	26.2 O
6		4.16 KV	57.6 R	123.3 R	57.6 R	N/A	63.2 R	57.6 R	275.5 R
7		SAT	1.0 G	1.9 G	4.7 Y	63.2 R	N/A	1.7 G	7.0 O
8	SG Cooling	AFW mp	1.7 G	3.1 Y	3.4 Y	57.6 R	1.7 G	N/A	34.7 O
9		AFW tp	5.2 O	22.5 O	26.2 O	275.5 R	7.0 O	34.7 O	N/A

N/A	Same System
G	Green RAW ≤ 2
Y	Yellow RAW > 2 and CDF ≤ 2.5E-4/year
O	Orange 2.5E-04/year < CDF ≤ 1E-03/year
R	Red CDF > 1E-3/year Combination not allowed

Note: The letter next to the value in the table indicates the risk color of the matrix block.

Table A-7
Calculation of Allowed Time T_c (Days)

	A	C	D	E	F	G	H	I	J
1				Electrical				SG Cooling	
2				SYD	EDG	4.16 KV	SAT	AFW mp	AFW tp
3	Base Case			30 G	30 Y	29 R	30 G	30 G	30 Y
4	Electrical	SYD	30 G	N/A	30 O	13 R	30 G	30 Y	30 O
5		EDG	30 Y	30 O	N/A	29 R	30 Y	30 Y	30 O
6		4.16 KV	29 R	13 R	29 R	N/A	26 R	29 R	6 R
7		SAT	30 G	30 G	30 Y	26 R	N/A	30 G	30 Y
8	SG Cooling	AFW mp	30 G	30 Y	30 Y	29 R	30 G	N/A	30 O
9		AFW tp	30 Y	30 O	30 O	6 R	30 Y	30 O	N/A

CAUTION: A red condition does not allow the barrier to be removed without entering the action statement for the affected TS system(s)/function(s). Apply appropriate level of risk management actions as needed for the color condition entered.

CAUTION: Regardless of the allowed time calculated, if the conditional CDF exceeds 1E-03, then a red condition exists and the degraded barrier cannot be removed without declaring the TS system inoperable.

Note: The letter next to the value in the table indicates the risk color of the matrix block.

APPENDIX B

Three-Train Systems

If applied to a plant with more than two trains per safety system, additional combinations of degraded barriers may be considered. The appendix provides a modified table of process cases, and a modified flowchart to describe the process for this situation. (Note: only Steps 3 and 6 of Part 1 of the flowchart is changed from the two-train case),

Table B-1 – Process Cases for a Three-Train System

Note: The cases below represent typical barrier/train/initiating event configurations. Other combinations are possible.

Case	Train 1 of System A Impacted by Barrier(s)	Train 2 of System A Impacted by Barrier	Train 3 of System A Impacted by Barrier	Comment
1a	Barrier 1 - IE_1	N/A - Single Train System	N/A - Single Train System	LCO 3.0.9 not allowed.
1b	Barrier 1 - IE_1	No	No	LCO 3.0.9 allowed subject to MR risk assessment (Step 8).
1c	Barrier 1 - IE_1 Barrier 2 - IE_1 or IE_2	No	No	LCO 3.0.9 allowed subject to MR risk assessment (Step 8).
1d	Barrier 1 - IE_1	No	Barrier 2 - IE_1	LCO 3.0.9 allowed subject to MR risk assessment (Step 8).
1e	Barrier 1 - IE_1	Barrier 2- IE_2	No	LCO 3.0.9 allowed subject to MR risk assessment (Step 8).
2	Barrier 1 - IE_1	Barrier 1 - IE_1	Barrier 1 - IE_1	LCO 3.0.9 not allowed.
3a	Barrier 1 - IE_1	Barrier 2 - IE_2	Barrier 3 - IE_3	LCO 3.0.9 allowed subject to MR risk assessment (Step 8), but removal of more than two barriers is not recommended.
3b	Barrier 1 - IE_1	Barrier 2 - IE_1	Barrier 3 - IE_2	LCO 3.0.9 allowed subject to MR risk assessment (Step 8), but removal of more than two barriers is not recommended.
4	Barrier 1 - IE_1	Barrier 2 - IE_1	Barrier 3 - IE_1	LCO 3.0.9 not allowed.

Case 1 represents a barrier or barriers that impact only one train of a system. The system may have only one train or multiple trains. Case 1a is not allowed regardless of the initiating event since a loss of system function could result. An example of this would be a barrier on the Refueling Water Storage Tank, which is considered a single system (component). Cases 1b, 1c, 1d, and 1e may be acceptable after satisfying the performance of a risk assessment in Step 8.

Case 2 represents a single barrier that impacts all trains of a three-train system. This condition is not allowed by LCO 3.0.9 as it also involves a potential loss of system function.

Case 3a represents different barriers impacting all trains of a three-train system with each barrier protecting against a different initiating event. Case 3b represents different barriers impacting all trains of a three-train system with two of the barriers protecting against the same initiating event. These situations may be acceptable after performance of a risk assessment in Step 8. However, it is not recommended that more than two barriers be removed from service at the same time.

Case 4 represents multiple different barriers that impact all trains of a three-train system with each barrier protecting against the same initiating event. This condition is not allowed by LCO 3.0.9, as it involves a potential loss of system function.

Figures B-1 and B-2 outline the process for the three-train system.

The changes from the two-train process in Figures 1 and 2 involve Step 3 and Step 6 of Figure B-1. Step 3 asks if only one or two trains of a three-train system are protected by a barrier(s). If “Yes,” then Cases 1b, 1c, 1d, or 1e are in effect and the process proceeds directly to Step 7. If “No,” then a check of the other combinations of trains and barriers is made in the next three steps. Step 6 asks if the degraded barriers provide the support function for different categories of initiating events. If “Yes,” then Cases 3a and 3b are in effect and the process proceeds directly to Step 7. If “No,” then Case 4 is in effect.

Refer to Section 6.2 of this document for more details on each step.

Figure B-1
Process for Assessing the Acceptability of Using the Degraded Barrier Allowance for a Three-Train System – Part 1

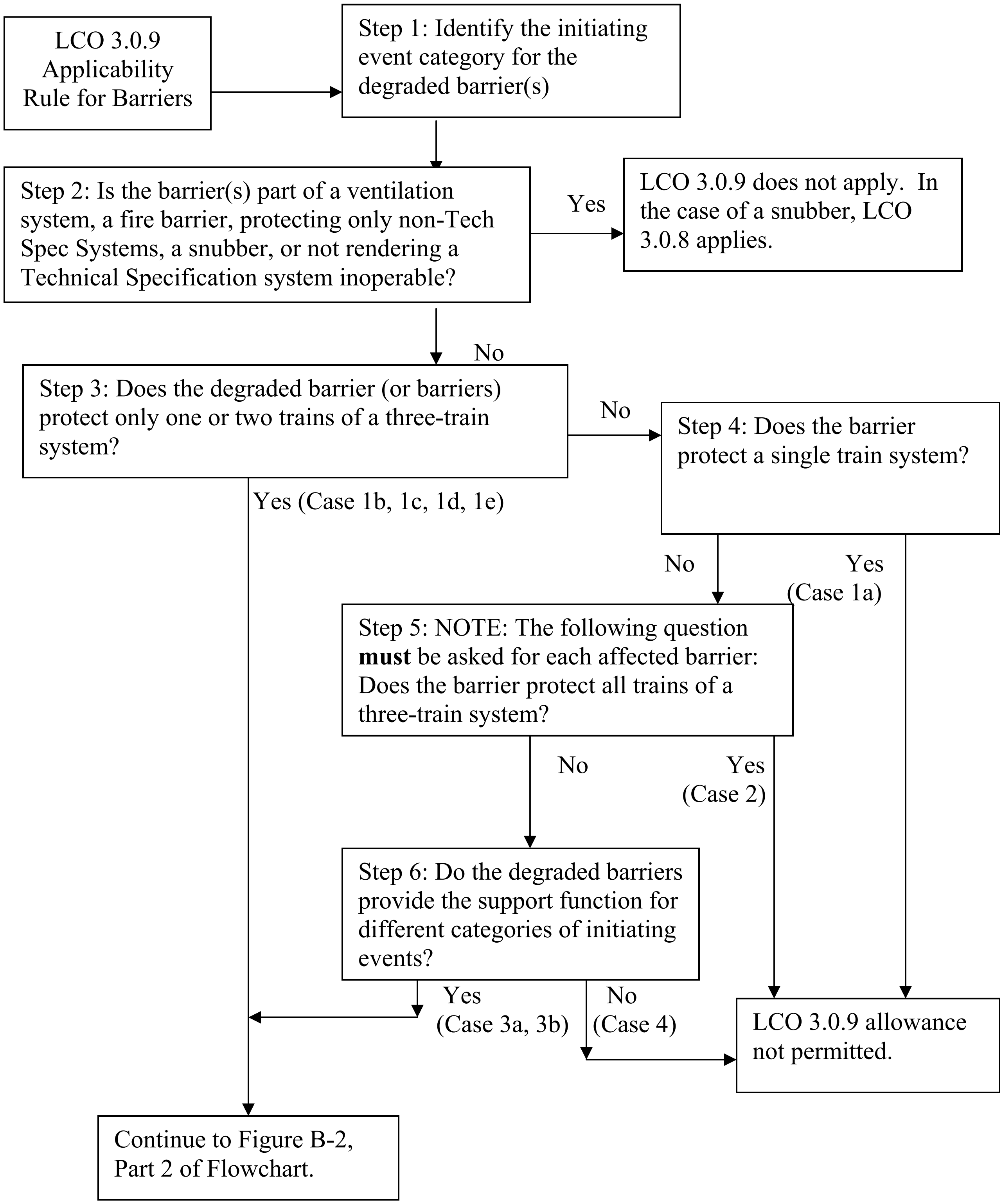


Figure B-2
Process for Assessing the Acceptability of Using the Degraded Barrier Allowance for a Three Train System– Part 2

Continued from Figure B-1, Part 1 of Flowchart.

Step 7: Consider conditions of the TSTF-427 Technical Justification.

Step 7a: Determine the ratio of IE_i/IE_T for the initiating events against which the degraded barrier(s) protects.

Step 7b: Determine the configuration-specific RAW of the Technical Specification supported system(s) or component(s) the degraded barrier supports and review insights for high RAW values.

Step 7c: Use the plant baseline CDF and the baseline LERF to determine the acceptability of LCO 3.0.9.

Step 7d: Consider the impact of external events on the risk evaluation (may be quantitative or qualitative).

Step 8: Perform a risk assessment in accordance with Maintenance Rule (a)(4) program.

Step 9: Are results of (a)(4) evaluation acceptable?

No → LCO 3.0.9 allowance not permitted.

Yes →

Step 10: Identify and establish risk management actions as appropriate, including considerations for high system or component RAW, external events, and LERF.

Step 11: Determine the risk-informed completion time, T_c. Degraded barrier must be restored within the risk management actions duration not to exceed 30 days, or enter the associated LCO.

→ Remove barrier from service.