# How to Incorporate Design Aspects in Peer Review Activities

## Introduction

Following the Fukushima event, WANO concluded that it was important to include some aspects of design in the scope of WANO activities. In terms of peer reviews, it was concluded that there was an opportunity to improve the way that design aspects and potential challenges to the associated safety functions are developed and documented in peer review reports.

First, reviewers should be better armed with knowledge about the fundamental design aspects of the plant they are reviewing and about the unique and specific issues surrounding the station.

Second, reviewers should be provided with the information needed to review and analyse the data collected in the peer review process in terms of safety function impacts.

This document provides guidance regarding how these influences can be brought to greater focus in the peer review programme and into the peer review products (principally AFIs).

## General Philosophy

Nuclear safety depends on both operational performance and the robust implementation of design characteristics. The reliable performance of critical safety functions is dependent upon a wide range of operational factors such as:

* Effectiveness of maintenance activities
* Proficiency of operations staff
* Decision making by leaders and managers
* Robustness of performance monitoring activities
* Quality of procedures needed to respond to events
* Reliability of equipment relied on to identify degrading conditions and to respond to operational transients/events
* Etc., etc.

The relative importance of any of the factors can be influenced by the fundamental design characteristics of the plant. For example, an effective combustible loading programme (fire protection) is of particular importance in plants whose design lacks robust separation of safety trains. Conversely, the importance of operator fundamentals, design knowledge and operating proficiency are not diminished in plants featuring a high degree of redundancy, separation, or diversity.

Peer reviewers and team leaders are challenged to identify occasions when safety functions could be compromised by accumulated weaknesses in any of the factors mentioned above. When they exist, these occasions should be brought to prominence in the peer review report.

## The Safety Functions:

All reactor designs include features that are intended to fulfil three fundamental safety functions, namely control of reactivity, removal of residual heat and confinement of radioactive materials (including control of releases). The safety functions are applicable to all anticipated modes of operation. For example, the “reactivity” function includes reactivity control both during normal operation, shutdown and upset conditions. It also includes emergency shutdown functions and those provisions that maintain the reactor sub-critical following an accident. The heat removal function includes shutdown core cooling provisions as well as emergency core cooling provisions for use following LOCA. It also includes features that are designed to remove residual heat following a severe accident. The confinement function includes provisions to contain radioactive materials under normal operating conditions, as well as post-accident conditions (including severe accidents). This function includes control of releases under all such conditions.

The safety of a nuclear power plant depends upon the degree to which these features are implemented, both by design characteristics and operational practices. The scope of safety functions can extend beyond the design basis of the plant to include beyond design basis conditions, or “design extension conditions”.

The peer review process aims to identify performance gaps in the areas of highest safety significance. To achieve this aim, identified gaps should be placed within the context of potential impacts on the fundamental safety functions. This concept applies not only to design related gaps, but also to areas not specifically related to plant design features. The importance of gaps in human or organizational performance is proportional to their potential impact on plant safety functions. It is therefore important that all peer reviewers have sufficient knowledge of plant design features to understand how their observations could relate to fundamental safety functions.

## Peer Review Preparation:

Prior to the peer review, the team will be provided with a design information package (details to be finalized) that includes the following:

* Design Fundamentals Reference Manual containing basic design information such as descriptions of safety systems and related auxiliary systems.
* Information regarding specific design aspects that would either increase or decrease the significance of particular facts or AFIs.  Items such as the level of redundancy, diversity, or train or fire separation are included.
* Information from the Probabilistic Safety Analysis (PSA), including main contributors to core damage frequency, critical equipment and operating actions (if available).
* Analysis of plant events and operating experience, and grouping of data according to safety function impact.

Review of the design information package during the preparation phase will help team members to:

1. Organize information (operating experience data, and plant events information, performance indicators) according to potential impacts on fundamental safety functions.
2. Create gap focus areas and review plans (including plant walk down plans) that concentrate on the areas of highest potential impact on nuclear safety.

## Integration of Design Aspects With Peer Review Activities

During the peer review, team members are faced with the challenging task of processing large volumes of information from a variety of sources. The goal is to determine areas for improvement that have the most value to the plant in improving their nuclear safety performance. By viewing the information through the lens of safety function impacts, the reviewer is best able to sort and prioritize the information to focus on areas of highest safety significance. The following is a description of how design aspects could factor into the various activities undertaken during the peer review.

### White Cards

During the first days of the peer review, reviewers will be required to generate white cards in assigned areas. The reviewer should pay particular attention to equipment and activities that have direct safety function relevance. The reviewer should apply knowledge of design gained from the design information package by asking:

* What safety function is related to this equipment and/or activity?
* What is the potential impact of observed gaps, in terms of safety function performance?

The reviewer should document, to the extent practical, the safety function relevance of the observed issue. For example:

Wrong: “Rain water was leaking onto and near switch gear”

Right: “Rain water was leaking onto and near 250 VDC emergency power switchgear (identify which switchgear). Old stains on the floor appear to indicate this is a longstanding problem. Could result in corrosion/degradation of emergency power equipment”

### Focused Walk Downs

The design information package may suggest some plant specific design related issues such as redundancy, train or fire separation, or protection against external hazards that could warrant focused walk downs, usually by the Engineering peer. Such walk downs would normally be included in the peer review plan. The reviewer(s) would apply their knowledge of the plant design to determine if particular vulnerabilities exist, and if such vulnerabilities, combined with operational factors, could significantly challenge one or more of the safety functions. The results of such walk downs should be documented in the form of facts that specifically state the potential impact to safety functions.

### Observations of Work Activities

During any peer review, workers of all disciplines are observed performing tasks in a wide variety of situations. Reviewers are encouraged to reach beyond general gaps in human performance to document specifically how worker performance could impact nuclear safety. Here are some examples:

Weak “so-what” statement:

“During Operator rounds of the Auxiliary and Emergency Diesel Generator buildings the viewing of the oil levels of Emergency Diesel Generators 1 and 2 was hindered due to all 4 perspex viewing screens being cracked. *Toleration of degraded conditions could lead to mistakes and increased degradation of plant conditions.”*

Better:

… “Tolerance of degraded conditions in both diesel trains could contribute to common cause failures of the emergency generators.”

Weak:

“During preventative maintenance on an air-operated valve, workers were observed making open and closed position marks on the actuator mechanism, using a permanent marker. Such marks could cause confusion for future maintainers, as to their accuracy and meaning.”

Better:

“During preventative maintenance work on an air-operated valve in the emergency coolant injection system, workers were observed making open and closed position marks on the actuator mechanism, using a permanent marker. The workers acknowledged that such marks could cause confusion for future maintainers, as to accuracy and meaning. The AOV was one of two 100% valves designed to admit emergency coolant following a LOCA. Both valves had extensive markings from previous maintenance. Confusion could result in maintenance errors on both trains, which could impair the emergency cooling safety function.”

### Plant Staff Interviews

Reviewers should seek to understand not only what performance gaps exist, but also why. Interviews should be focused on asking “why” questions. Often, a key component of such questions is to determine the extent to which workers understand the nuclear safety significance of the issue under discussion. For example, if human performance gaps were observed during work on safety related equipment, the worker should be asked if he understands the function of the equipment and the potential consequences of errors. Follow-up interviews with the worker’s supervisor may include questions about how situational awareness is promoted.

### Investigation of Gap Focus Areas

It is the responsibility of reviewers to investigate potential focus areas within the context of the overall scope of their peer review plan. Often such investigations will require input from different functional areas, and the team leader may assign groups of reviewers as appropriate.

The potential focus areas should serve to help guide the reviewers’ plans for the on-site peer review. For example:

1. If the analysis of plant events and operating experience identifies that there has been a string of maintenance errors on safety injection equipment, the maintenance team should make sure that they observe maintenance on safety injection equipment during the peer review.

2. If the analysis of plant events and plant events and operating experience identified that operators have had difficulty controlling steam generator level on feedwater transients (affects cooling), then the operations reviewers might consider asking questions about the training of operators on level control or even observe a simulator scenario where level control is important.

3. If the plant performance data shows that there have been a greater number of unresolved failures of breakers in the AC power system, reviewers may want to more thoroughly walk down the switchgear to identify any material condition or environmental conditions that contribute, or they may also want to look at preventive maintenance practices for breakers at the station and compare those to industry recommendations.

The point here is that the design information package should be used as a way to help focus the reviewers’ activities in the areas of greatest safety significance and to establish whether or not there is a significant problem worthy of an AFI. In addition, facts established during the peer review need also to be looked at in this structure to identify any emerging issues based on direct observation of plant activities.

### Developing Areas for Improvement

If a gap in the performance of a safety function exists, it may be documented as a separate AFI or as a clear consequence (actual or potential) in a particular AFI. How this is documented is a matter of choice of the associated reviewer and the team leader based on the overall strength of facts and the overall results of the peer review.

If it is considered that a separate AFI on a particular safety function is appropriate, the facts must show a clear relationship to the safety function that is the topic of the AFI. For example, if the AFI addresses Emergency AC power safety functions; examples of maintenance weaknesses need to address direct consequences on EAC sources or equipment (general maintenance weaknesses that are not specific should not be used); operator and operations procedure weaknesses should be noted to affect EAC issues (general statements that many operations procedures are weak should not be used). It is not enough to use general weaknesses or even narrowly focused weaknesses (such as a specific single procedure that is weak or a single missing preventive maintenance activity) to justify an overall AFI for a safety function.

For situations where there is not sufficient justification for an AFI on a particular safety function, it may be appropriate to point out the safety function impact/consequence in the AFI problem statement. For example, consider an AFI in the area of configuration management that cites failures to update drawings or procedures following modifications, with particular examples from recent modifications to the AFW system. In this case, it would be appropriate to point out potential consequences in the AFI problem with words such as, “…a number of examples were identified in recent AFW system modifications and reduce the reliability of these documents supporting the cooling safety function”

For AFIs that are not specifically related to a threat to safety function, examples used to support the AFI should, where appropriate, include how such gaps could potential impact safety functions.

## Example 1 – AFI on Degraded Safety Function

The following items from design information package:

1. Extreme high and low air temperatures are included in the plant’s design basis.
2. Emergency diesels are 2 x 100%, with a 3rd diesel recently added.
3. Each of the 2 existing diesel rooms, the common electrical room and the common fuel oil pump house have 2 x 100% electrical heating units.
4. The PSAS indicates the emergency power is a major contributor to Core Damage Frequency (CDF) at 50%.
5. Extreme low temperatures (beyond design basis) have not been included in PSA analysis.

In pre-review discussions with the plant, it is identified that a review of weather records for the area includes several occurrences of temperatures below the plant’s design basis value in the past 50 years. In addition the low temperature events have not been specifically analysed to determine if there may be any cliff-edge effects. In a review of the plant’s corrective action database, the following entries are noted:

1. During extreme low temperature event resulting in freezing of a firewater pipe
2. Failure to complete winter preparation maintenance,
3. Extreme high temperature in control room due to failed Air Conditioning Units,
4. Battery rooms high temperatures and temperature-related degradation requiring early replacement of battery banks (including temporary cell replacement and load reductions to maintain battery mission time capabilities)
5. Temperature related failures of control computers,
6. Temperature related failures of safety system inverters,
7. High temperatures in safety system instrument rooms,
8. High maintenance backlog on Heating, Ventilation and Air Conditioning systems,
9. Longstanding temporary modification for Air Conditioning Units in main control room.

A gap focus area is written and the Equipment Reliability reviewer is assigned by the team leader to lead a small team to investigate. The team includes Operations and Engineering reviewers.

Based on this gap focus area, reviewers are asked to look into the following areas:

1. Detailed safety function walkdowns paying particular attention to HVAC (all reviewers).
2. System health reports for HVAC systems and review of Plant Health Committee ranking of HVAC issues (Equipment Performance reviewer);
3. Prioritization of HVAC deficiencies and winter/summer readiness work orders in the work management system (Equipment Reliability reviewer).
4. Preventive maintenance on HVAC systems (Equipment Reliability reviewer).
5. Interview system engineer regarding advocacy (Equipment Reliability reviewer).
6. Ask how extreme temperature events are analysed in the PSA (Engineering reviewer). Are beyond design basis conditions considered?.
7. Operations impact – workarounds? Operator burden? Operations advocacy? (Operations reviewer).
8. System reviews and periodic safety reviews – what actions have been put in place and what is the plan to implement them?
9. Margin management database information relating to HVAC issues (how has the plant prioritized actions based on aspects such as safety, productivity, cost / benefits, timing / urgency...?).

As a result of the follow-up investigations, the following facts are noted:

1. Many examples of poor material condition – tags are old and sometimes missing. Some deficiencies were not entered into the work management system. Operations staff indicate “they have entered so many work requests, and nothing gets done because of low priority”, so they have stopped entering such issues.
2. Undocumented temporary modifications (e.g. fans in battery room doors).
3. Seven temporary modifications related to HVAC, some dating back 10 years.
4. During an interview, the system engineer complained that HVAC gets very low priority at Plant Health Committee, and that he gets little attention when he attempts to raise HVAC issues. Perception that HVAC systems are “not sexy” and HVAC system engineer role is not respected.
5. Interviews with Work Management coordinator indicates HVAC deficiencies get “normal” priority but because of a high backlog of higher priority Work Orders, most HVAC deficiencies have long wait times.
6. High number of longstanding deficiencies related to obsolete components.
7. Design engineering manager indicates process deficiencies prevent straightforward replacement of obsolete components with modern equivalents because of inefficient procurement engineering and supply chain processes.
8. Last year, 50% of winterization Work Orders were not completed by the due date.
9. High number of preventive maintenance deferrals on HVAC equipment. PM basis for safety critical HVAC components is “non-safety related”.
10. Plant Health Committee records show low ranking from HVAC related upgrade proposals (scoring system for prioritization does not properly credit potential common mode impacts).
11. PSA does not analyse extreme temperatures and no analysis of potential cliff-edge effects have been done.
12. Lubricating oil for 3rd diesel has acceptable viscosity down to the design basis minimum temperature.
13. Operators do frequent manual interventions in response to HVAC deficiencies (automatic controllers don’t work, dampers are stuck and require manual adjustment, etc).

Based upon the above, the following AFI is drafted:

***Degraded HVAC reliability and material condition has resulted in impairments to safety related systems, temperature related degradation to important equipment, and increases the risk of common mode failures.*** *Plant management has not placed sufficient priority on corrective maintenance, preventive maintenance, and projects to achieve the necessary level of reliability.*Primary supporting facts include:

Examples of impact on safety functions:

1. Frozen fire water line.
2. Temperature related failures of safety related power supplies.
3. Temperature related failures of control computer.
4. Temperature related degradation of battery cells.

Causes and contributors:

1. Low priority:
   * PHC ranking – ranking system does not credit impact on multiple systems/common mode potential.
   * corrective maintenance backlog.

Incomplete winter/summer preparation WOs.

1. PM program gaps – “non safety related”
2. Procurement Engineering process problems resulting in excessive lead time and cost of minor mods, resulting in large number of temporary modifications pending permanent solutions

## Example 2 – Design Related factors that do not themselves warrant an AFI, but contribute to an AFI

To be developed

## Example 3 – Design Related factors that do not warrant inclusion in an AFI

To be developed.