

# **Safety System Design Adequacy**

Submitted by  
Engineering Practices Working Group  
For  
Energy Facilities Contractors Group



Design Adequacy Sub-Group  
Ken Keith, Chairman

Y-12 National Security Complex  
P. O. Box 2009  
Oak Ridge, Tennessee 37831-8169

**Date of Issue: August 2004**

**Prepared by  
Design Adequacy Sub-Group**

Sean Fargo	Fluor Hanford
Gurinder Grewal	LANL
Ken Keith, lead	BWXT Y-12
Dave Lowe	Kaiser Hill Rocky Flats
Toney Mathews	AREVA Framatome ANP
Tom Monahon	WSRC
Joe Papp	BWXT Pantex
Barb Quivey	LLNL

## **Safety System Design Adequacy**

### **Executive Summary**

Within the Department of Energy and National Nuclear Security Administration, structures, systems, and components (SSCs) previously designed and installed (i.e., existing) have been designated as safety SSCs (i.e., safety class or safety significant) through upgraded safety analyses. In some instances, these SSCs have not been evaluated to ensure that they can reliably perform their credited safety function, and they may not satisfy current codes and standards for design or current quality expectations.

This paper describes a graded process to systematically evaluate these existing SSCs to identify their safety functional requirements, current applicable requirements, need for compensatory measures or modifications, or to document and accept any identified risk, if necessary. The evaluation process ensures that existing SSCs elevated in importance to safety class or safety significant undergo an appropriate technical evaluation.

## 1. Purpose

The designation of structures, systems, or components (SSCs) as safety SSCs is intended to ensure an increased level of reliability in those SSCs commensurate with their importance to safety. In the rules, orders, and guidance provided by the Department of Energy (DOE), a graded approach is fashioned into an overall framework for design, testing and inspection, and quality requirements to provide this increased level of reliability. This framework is relatively new in relation to the age of many of DOE's sites and facilities. In addition, many of these sites have completed, or are in the process of completing, safety analyses compliant with 10 CFR 830 that have potentially designated previously designed and built equipment as safety SSCs, i.e., safety class or safety significant. Therefore, SSCs previously designed and installed may not have been designed to current design or quality requirements for safety SSCs.

The purpose of this paper is to define a process to perform design adequacy evaluations. This evaluation process, if applied, will ensure that existing SSCs elevated in importance to safety class or safety significant undergo an appropriate technical evaluation. The process also applies to the evaluation of code changes that apply to the design of safety SSCs. In addition, supporting information and related considerations to this process are discussed.

A graded approach is employed where the extent of analysis and expectations increase with the complexity of an SSC and the importance of the safety function of the SSC.

## 2. Background

The Defense Nuclear Facilities Safety Board (DNFSB) has identified a number of situations throughout DOE's and National Nuclear Security Administration's (NNSA) Nuclear Weapons Complex where previously designed and installed SSCs have subsequently been identified as safety SSCs. These SSC designations have typically occurred during the general upgrade to safety analyses that began in the late 1980s and culminated in the 1990s with the promulgation of the Price-Anderson Amendments Act (PAAA) rules for quality and safety analysis (10 CFR 830.120 and .200, respectively). The Board has identified that, in some cases, these existing SSCs designated as safety SSCs have not been evaluated to ensure that they can reliably perform their credited safety function and the SSCs may not satisfy current codes and standards for design or current quality expectations.

This evaluation of "upgraded" SSCs has been referred to as a "backfit analysis" process in some instances. This terminology is distinct from the interpretation of the process employed by the Nuclear Regulatory Commission (NRC), which requires an evaluation in proposed regulation changes based on the cost and

benefits to safety. In this paper's application, a "backfit" is a specific modification that was necessary to upgrade an existing system and/or component to make it suitable in quality and reliability for service as a safety-class or safety-significant SSC.

There is, however, a related precedent in NRC's purview. In 1977, NRC initiated the Systematic Evaluation Program to review the designs of older, operating power plants. The purpose of the program was to:

1. identify issues for which regulatory requirements had changed enough over time to warrant an evaluation of those plants licensed before the issuance of the Standard Review Plan in 1975, and
2. evaluate the safety significance of the issues relative to the adequacy of the licensing basis of those affected plants.

The process proposed herein is not dissimilar to the overall process NRC followed.

The intent is not necessarily to force upgrades of SSCs but rather to ensure that a conscious, technically-based decision is made regarding the use and/or upgrade of existing equipment. Typically, this decision is risk based and, as such, should be coordinated with and documented in the facility's Safety Analysis Report (SAR) and, if appropriate, risk acceptance indicated in the Safety Evaluation Report (SER).

This paper provides a process to systematically address this issue as a template for use in evaluating existing SSCs upgraded to safety application. Note that although the above discussion points to NNSA facilities, the issue is equally applicable to DOE facilities.

### **3. Applies to**

The process outlined below is intended to provide a systematic process for the evaluation of safety SSCs. The graded approach provides greater expectations for safety-class (or higher risk) SSCs than for safety-significant SSCs.

This process is intended for application only to existing nuclear facilities and to safety SSCs (that is, safety class or safety significant) identified in accordance with DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*.

#### **4. When to Apply**

The design adequacy evaluation process may be invoked in the following situations:

- identification of a new or modified safety function or functional requirement for an existing SSC, including initial designation as safety class or safety significant;
- identification of a generic component deficiency through industry reporting processes that may affect safety SSC functional performance or reliability;
- identification of new information, lessons learned, or operational experience that may affect safety SSC functional performance or reliability;
- requirement by DOE/NNSA through the Authorization Agreement to comply with certain conditions that may affect an SSC's design or operability; and
- significant change in a national consensus code or standard that may affect previous understanding of SSC functional performance or reliability.

In addition, the discovery of potential inadequacies in the safety analysis through the unreviewed safety question determination process may lead to questions about an SSC's ability to perform its intended function. The design adequacy process may be germane in such circumstances as well.

Ideally, the evaluation should be conducted in conjunction with the safety analysis process, such as when specific, credited hardware controls are proposed. Results of the evaluation should be factored into the facility's documented safety analysis (DSA). If the DSA is already established, an evaluation of the credited hardware controls may be in order so that the DSA reflects the evaluation's results, particularly where risk acceptance decisions may be made. Use of the DSA approval process allows, as appropriate, the proper documentation and approval of any residual risk acceptance through the SAR/SER process.

#### **5. Conducting the Evaluation**

The intent of the process is to:

1. evaluate adequacy of existing SSC design;
2. identify attributes that may need additional specification (or modification) to ensure intended reliability and functionality; and
3. determine the need for any compensatory measures, design modifications, or replacement.

In some cases, the decision may result in a risk acceptance decision by DOE/ NNSA. Figure 1 provides a graphical flow of the process.

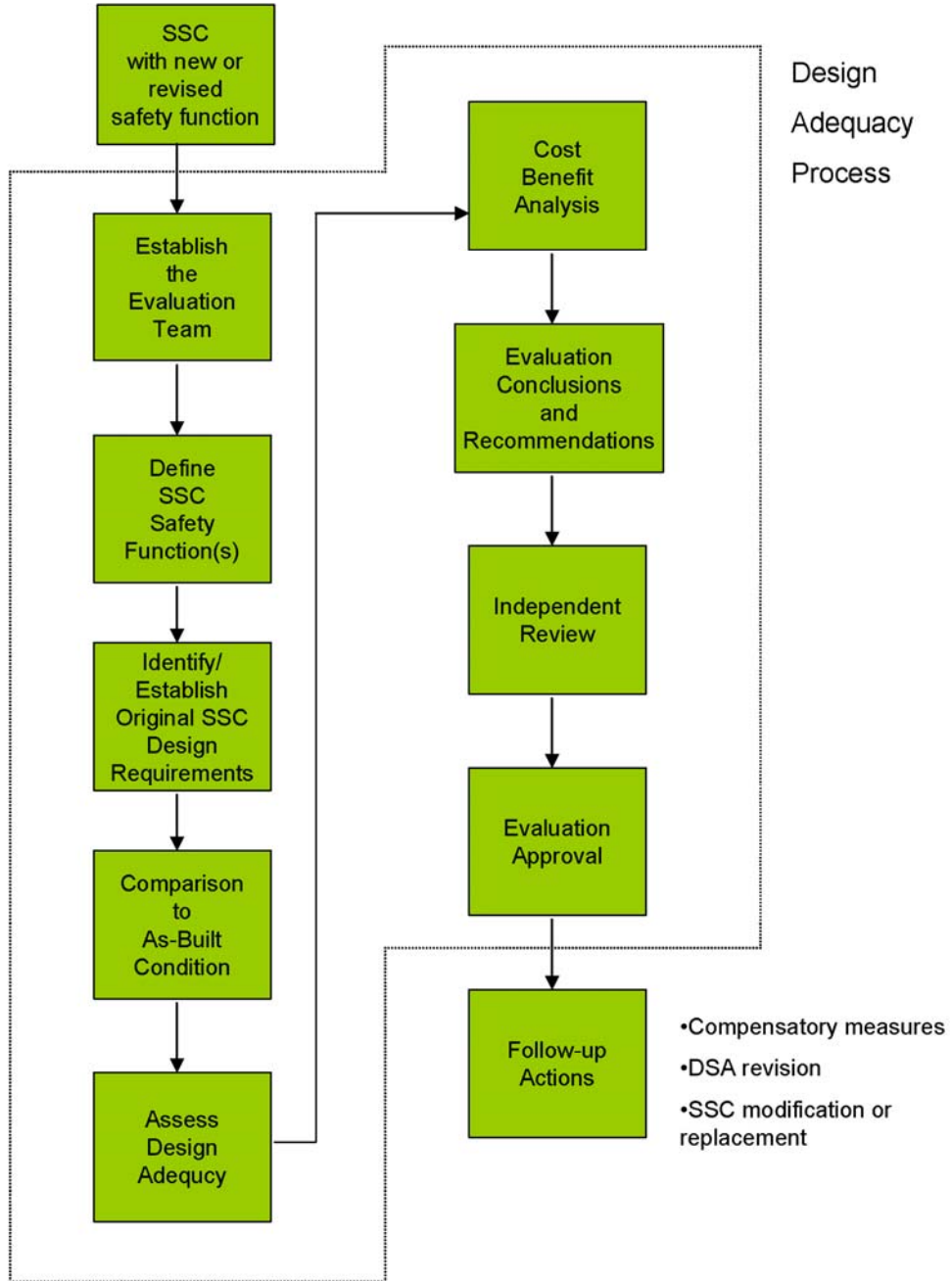


Figure 1. SSC evaluation flowchart.

## 5.1 Establish the Evaluation Team

The evaluation should be conducted by a competent individual or team of individuals with sufficient expertise in the following areas:

- knowledge of the SSCs involved;
- knowledge of the safety basis, and supporting hazard and accident analyses;
- experience or training in performing safety system design adequacy reviews;
- working knowledge of the requirements for design (including national consensus codes and standards), procurement, and construction or installation of safety SSCs; and
- working knowledge of the facility's operation.

Typically this team will consist of safety analysis personnel, appropriate engineering personnel (who represent the Design Authority), and operations personnel knowledgeable of the specific operations. Additionally, there may be instances (e.g., site-wide systems) when interfaces with other facilities require other expertise. An adequate mix with appropriate seniority and experience is crucial to ensuring a comprehensive and credible evaluation. Participation of DOE or NNSA representatives is encouraged to facilitate review and acceptance by regulatory entities.

## 5.2 Define the SSC Safety Functional Requirements

The evaluation process's aim is to ensure that the SSC safety function(s) can be performed reliably when required. Therefore, the initial step is to clearly define the safety functional requirements as credited in the facility DSA. These functional requirements include the specific functions the SSC is expected to perform (e.g., prevent overpressure) and under what conditions (normal and for post-accident environmental conditions) or scenarios (e.g., natural phenomena). These functional requirements are then the focus of the evaluation process. The SSC to be evaluated should be clearly defined. Any supporting systems should be considered, and any requirements related to accomplishing safety function(s) should be identified and addressed in the evaluation. The basis for how far beyond the SSC boundaries to go in the backfit analysis should be clearly documented. This defined basis will make clear the function of supporting systems, adjacent systems, or connecting systems as they pertain to the ability of the identified SSC to perform its safety function under required conditions.

### **5.3 Identify or Establish the Original Design Requirements**

The second step in the adequacy evaluation process is to identify the design requirements for the existing SSC. This important step is required to establish the functional attributes of the existing SSC design. Functional attributes, in this context, are defined as the system characteristics that directly resulted from or that satisfied original design, procurement, installation, or construction requirements that were imposed to ensure reliable and effective operation. Note that the focus of the evaluation should be on those requirements necessary to assure or support the safety function(s) only. It is expected that these functional attributes can be readily determined from archived design and construction records. If such records are not available, the decision must be made as to whether it is more cost effective to re-establish or reconstitute this information or simply abort the evaluation process and replace the SSC with equipment satisfying appropriate requirements.

### **5.4 Comparison to As-Built Condition**

Once the as-designed requirements are known, careful consideration of the original design requirements vs the as-installed or as-built condition is required. In particular, assurance is expected that the installed equipment represents and/or satisfies the documented as-designed requirements related to the safety function(s) or that the documentation was revised to reflect field conditions. As such, field confirmation, potentially including testing data, may be required to establish a reasonable confidence in the existing SSC documentation.

If significant resources are required to evaluate the as-built condition, judgement must be used to determine the cost benefit of reconstituting or updating the design basis vs replacement.

### **5.5 Assessment of Design Adequacy**

With an understanding of the functional requirements, design basis, and as-built conditions, the evaluation team may then assess the design adequacy. This evaluation is expected to be a qualitative, technical discussion aimed at demonstrating that the SSC can adequately and reliably perform its designated safety function(s) as intended. This may be accomplished by:

- comparing the SSC design attributes to a set of appropriate design, quality, or maintenance requirements, specifically including applicable current codes and standards for the SSC and demonstrating compliance;

- demonstrating that the existing SSCs satisfy equivalent requirements of codes and standards;
- demonstrating acceptable system reliability and operability for existing SSCs given their specific credited safety functions, despite noncompliance with applicable requirements; or
- explicitly accepting the risk associated with the deviations using rational and appropriate engineering judgements or cost-benefit studies. In some cases, it may be appropriate to base the risk acceptance on the results of a probabilistic risk assessment.

In addition, there may be other alternatives for demonstrating an acceptable level of reliability. For instance, using existing SSCs with some design modifications or existing SSCs in conjunction with backup SSCs may provide a similar level of reliability for the intended function. Existing SSCs may also be supplemented with administrative controls to achieve the desired reliability. This approach should be considered as a compensatory measure and, hence, temporary. Compensatory measures should generally not be considered a long term solution. However, the remaining life of the SSC should factor into this decision and could justify continued operation with compensatory measures.

To guide the performance of these evaluations, Tables 1 and 2 have been derived from DOE G 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide for use with DOE O 420.1, Facility Safety*. These tables provide a set of standardized design criteria for evaluation. Table 1 provides a listing of attributes that should be addressed for safety-class items; Table 2 addresses attributes for safety-significant items. These tables reflect a graded approach based on G 420.1-1: Expectations are greater for safety-class SSCs than for safety-significant SSCs. Each of these attributes should be explicitly addressed in the design adequacy evaluation as they pertain to the SSC's credited safety function.

Attachment 1 provides an explanation of Tables 1 and 2 requirements. Note DOE G 420.1-1 may be consulted for more specific consensus code and standard citations.

The assessment logically reduces to two sub-steps. The first sub-step is to compare the SSC to the list of applicable requirements (e.g., Table 1). The second sub-step is to then evaluate for any identified deviations.

### **5.5.1 Evaluation of SSC to Requirements**

Evaluate the SSC to a defined set of requirements (such as Table 1 or 2). The evaluation should document the basis, addressing each of the requirements for satisfying the requirements or identifying the

deviations. For consensus code and standard reviews, a comprehensive line-by-line examination of the code or standard is not intended. However, sufficient evidence of adherence to the key functional points of the code or standard is imperative (e.g., fire protection sprinkler system should satisfy appropriate flow requirements of NFPA 13) if these standards are used or compliance assumed in the development of the safety basis. Due to the age of some existing SSCs and the changes to applicable consensus codes and standards, it is recommended that the evaluation be based on current code and standard editions. The intent of such a comparison is not to upgrade to current codes, but to understand the differences, the safety significance of those gaps as related to the safety functional requirements of the SSC, and the acceptance of the risk or adequacy of the current SSC to fulfill its safety function.

### **5.5.2 Evaluation of Deviations from Design Requirements**

For each deviation noted from the comparison, analyze the design requirement against the safety function requirement. In some cases, the safety function may not require compliance with the requirement. In other cases, additional analysis, inspection, or testing may be required to assess the deviation. Finally, it may not be possible to satisfy the requirement with the existing SSC, and replacement or re-design is necessary. In these cases, compensatory measures should be explored to allow for continued operation in the current state. In addition, a basis for acceptance of residual risk may be explored with appropriate technical justification. The determination of path to proceed may require a cost-benefit analysis.

In evaluating the deviations, the assessment should consider:

- procedural and administrative controls not previously credited, such as increased calibration/inspection frequencies, increased surveillances, etc.;
- limitations on future usage of the SSC;
- any existing risk analyses or reliability analyses;
- reliability evidence from operating history or industry databases;
- defense-in-depth—i.e., the presence of other SSCs with no common mode failures that provide additional levels of protection for a given safety function; and
- other compensatory measures.

## **5.6 Cost-Benefit Analysis**

A cost-benefit analysis may be needed to determine whether to upgrade an existing SSC, identify alternative SSCs to supplement the function of the existing SSC, replace the SSC, or accept the risk. The analytical cost associated with the design adequacy review is dependent on the condition and available documentation of the existing SSC. It is incumbent upon the evaluation team to determine the appropriate path forward, considering several factors:

- program mission of the activities performed in the facility;
- remaining life of the facility or the specific SSC;
- cost of the analysis vs immediate replacement or modifications; and,
- availability of other alternatives to the SSC to support the safety basis of the facility based on the outcome of the design adequacy review.

## **5.7 Adequacy Evaluation Conclusions and Recommendations**

The evaluation team is responsible for proposing the preferred approach to resolution of any identified deviations through technical justification of non-applicability, compensatory measures, replacement or upgrade, or risk acceptance. It should be understood that their goal is to continue mission program activities in a manner that ultimately provides protection of the health and safety of the public and workers.

## **5.8 Independent Review**

Given the role of the design adequacy process in supporting the safety basis, quality assurance requirements appropriate for the SSC should be applied to the evaluation. Therefore, an independent review panel or committee should review and approve the methodology and products of the design adequacy review.

## **5.9 Evaluation Approval**

The evaluation, conclusions, and recommendations, along with the results of the Independent Review, require final approval by the Design Authority.

## **6. Interfacing Processes and Other Considerations**

The scope of the design adequacy evaluation is quite broad: the safety analysis, design, quality, and maintainability characteristics all contribute to the overall reliability argument. With the scope and depth of the issue, a number of related issues warrant discussion.

### **6.1 Defined Design Criteria—Site Level/Facility or System Level**

Contractors need to have a defined set of manuals and/or procedures that clearly identify the requirements for design, procurement, and construction or installation of safety SSCs. These requirements may reference the appropriate industry codes and standards or provide them in detail by functional classification (e.g., electrical, mechanical, civil, and structural). Additionally, the requirements should be classified to differentiate among safety class, safety significant, general purpose, and supporting safety functions of the SSCs. Ideally, this set of requirements should form the evaluation basis for the design adequacy assessment. As noted earlier, DOE G 420.1-1 provides a comprehensive listing of criteria potentially applicable to safety-class and safety-significant SSCs. These criteria should be used in the development of the set of implementing manuals and/or procedures. These general criteria should be maintained as codes and standards change.

For individual SSCs, specific design criteria should be established and maintained throughout the life of the SSC. These criteria should then document the specific versions of the codes and standards invoked at the time of design. This code of record should then be the basis on which future change is judged or updated, based on the significance of modifications.

### **6.2 Reliability of Safety-Significant SSCs**

Expectations for safety-class SSCs are quite explicit in DOE rules, orders, and guidance. The comprehensive set of requirements that address design (including single-failure criteria), quality in procurement and installation, and surveillance afford a fairly high reliability without explicit analysis. Each of these attributes contributes to the overall reliability. No specific reliability criteria are defined, however.

For safety-significant SSCs, many of these expectations—including, for example, single failure criteria—are generally not invoked. Reliability requirements, then, are subjective. Some sites have defined processes in their safety analysis procedures to evaluate defense-in-depth features to provide increased reliability, while other sites have not. For example, an

expected level of reliability is required as input to some safety-significant criteria defined by G 420.1-1, *Instrument Society of America (ISA) S84.01*.

The result is a large uncertainty that may require additional consideration and work to obtain a consensus. With the large uncertainty, differences in experience and judgment can lead to disagreements between DOE, NNSA, and the managing or operating contractor. Reliability expectations for safety-significant equipment, therefore, warrants further guidance.

### **6.3 Impacts from the Adequacy Review Process**

A safety-system design adequacy review process may result in modifications to SSCs to improve the performance or reliability of the safety or complementary non-safety components; address system interaction issues; or changes to safety basis-related documents. Special consideration should be given to ensuring that the facility and its safety basis are consistent with the outcome of this analysis when it is completed. The following examples are areas when such consideration may be warranted:

- The safety basis, and perhaps the Authorization Agreement of the facility, needs to be updated to incorporate any changes resulting from the implementation of the design adequacy review.
- Compensatory measures should be given special consideration to ensure safe operation of the facility or activity while the results of the design adequacy evaluation are being implemented. These measures may include additional administrative or defense-in-depth controls to compensate for shortcomings of the existing safety SSCs.
- The system design description documents and their associated records and drawings need to be updated for any design changes resulting from implementation of the safety systems design adequacy review.
- Any changes to the safety SSCs need to be incorporated into the facility's configuration management program to prevent future deviations or violations.
- Facility personnel may need to be trained on the modifications to the facility or its safety basis to ensure proper conduct or operations and reduce undesired occurrences.

## **6.4 Conclusion**

A process to perform design adequacy evaluations has been defined. This process, if applied, will ensure that existing SSCs elevated in importance to safety class or safety significant undergo an appropriate technical evaluation. The results will provide a basis for the acceptance of these elevated SSCs, provide an avenue for risk acceptance, or determine the need to replace the SSC or remove it from service.

**Table 1. Safety-Class Design Criteria \***

<p>Natural Phenomena Hazards Design</p> <ul style="list-style-type: none"> <li>• Evaluation Basis Earthquake</li> <li>• Evaluation Basis Wind/Tornado</li> <li>• Probable Maximum Flood</li> <li>• Probable Maximum Precipitation</li> </ul>	<p>Safety functions must not be compromised by events for which they are credited.</p>
<p>Resistance to External Events (External)</p>	<p>Safety functions must not be compromised by events for which they are credited. (Examples include explosions or fires that originate external to the facility.)</p>
<p>Single Active Failure Resistance</p>	<p>Active safety components must not be compromised by a single failure. Active component defined to be that requiring mechanical motion in the completion of the required action.</p>
<p>Equipment Environment Qualification</p>	<p>Safety Class items must be qualified to function under the most limiting conditions at end of life. Environmental conditions include temperature, pressure, radiation, and/or chemical exposures.</p>
<p>Safety Class Electrical Requirements</p>	<p>Safety class electrical equipment must conform to certain IEEE standards (e.g., IEEE 379) for separation, redundancy, and single failure.</p>
<p>ASME code or Other Applicable Requirements</p>	<p>Piping, piping components and pressure vessels must satisfy applicable portions of the ASME piping or boiler and pressure vessel codes.</p>
<p>Quality Assurance Requirements</p>	<p>QA requirements may be applicable to ensure safety class components function reliably and as designed.</p>
<p>Internal Hazard Resistance</p>	<p>Safety functions must not be compromised by internal events for which they are credited including missiles, fire, explosions, flooding (internal), damage due to failure of non-safety components (e.g., II/I) and any other postulated events.</p>
<p>Specific Functional Requirements</p>	<p>SSC must be able to accomplish the specific safety action for which the SSC is credited. Evaluation of the ability of the SSC to perform the action in conjunction with the other applicable requirements in this table are necessary to demonstrate the safety function can be reliably performed and under appropriate conditions.</p>
<p>Maintainability/Testability</p>	<p>Safety Class items shall be designed to allow inspection, maintenance, periodic testing, and/or surveillance to ensure their continued functioning readiness for operation, and accuracy. Testing must be capable of being performed in place, on a regular schedule, and under simulated emergency conditions.</p>

\*Criteria subjects are based on DOE Guide 420.1-1, *Nonreactor Nuclear Facility Design Criteria*.

**Table 2. Safety-Significant Design Criteria**

<p>Natural Phenomena Hazards Design</p> <ul style="list-style-type: none"> <li>• Evaluation Basis Earthquake</li> <li>• Evaluation Basis Wind/Tornado</li> <li>• Probable Maximum Flood</li> <li>• Probable Maximum Precipitation</li> </ul>	<p>Safety functions must not be compromised by events for which they are credited.</p>
<p>Equipment Environment Conditions</p>	<p>Safety Significant items must be selected to function under expected limiting environmental conditions. Environmental conditions include temperature, pressure, radiation, and/or chemical exposures.</p>
<p>Industry or Consensus Codes and Standards</p>	<p>Piping, piping components and pressure vessels must satisfy applicable portions of the ASME piping or boiler and pressure vessel codes.</p>
<p>Specific Functional Requirements</p>	<p>SSC must be able to accomplish the specific safety action for which the SSC is credited. Evaluation of the ability of the SSC to perform the action in conjunction with the other applicable requirements in this table are necessary to demonstrate the safety function can be reliably performed and under appropriate conditions.</p>
<p>Maintainability/ Testability</p>	<p>Safety Significant items shall be designed to allow inspection, maintenance, periodic testing, and/or surveillance to ensure their continued functioning readiness for operation, and accuracy. Testing must be capable of being performed in place, on a regular schedule, and under simulated emergency conditions.</p>

## **Attachment 1 Guidelines for Design Requirements**

1. Natural Phenomena Hazard (NPH) qualification: A technical review of the necessary calculations, installation and design vs the applicable NPH criteria. II/I considerations should also be included in this review.
2. Single failure analysis: No active single failure shall be permitted for SSCs newly designated or upgraded to safety class unless justified by the design adequacy process. Passive single failures are generally acceptable if justified by low probability or mitigating responses.
3. Quality of Parts and Procurement Requirements: A technical review of the specifications for the original and replacement parts should be conducted. This should involve an evaluation of installed parts, spare parts, in-service inspection requirements, and vendor information to assess adequacy. Consideration for suspect or counterfeit parts should be given.
4. Applicable Codes and Standards: The review should address the technical aspects of applicable codes.
5. Environmental Qualification: Special or unique normal or post-accident environmental conditions must be evaluated. Post-accident applies only if the SSC is expected to operate under such conditions.
6. Testability, operability, and maintainability: Critical features and functions of the SSC should be testable, inspectable, and replaceable as appropriate.