DOE/NV/25946--1891

Margin of Safety Definition and Examples used in Safety Basis Documents and the USQ Process

Ronald A. Beaulieu
Safety Basis Program Manager
Nuclear Operations Directorate
National Security Technologies, LLC (NSTec)
Las Vegas and Mercury, NV
Beaulir1@nv.doe.gov
October 3, 2013

Abstract

The Nuclear Safety Management final rule, 10 CFR 830, provides an undefined term, margin of safety (MOS). Safe harbors listed in 10 CFR 830, Table 2, such as DOE-STD-3009 use but do not define the term. This lack of definition has created the need for the definition. This paper provides a definition of MOS and documents examples of MOS as applied in a DOE approved safety basis for an existing nuclear facility. If we understand what MOS looks like regarding Technical Safety Requirements (TSR) parameters, then it helps us compare against other parameters that do not involve a MOS. This paper also documents parameters that are not MOS. These criteria could be used to determine if an MOS exists in safety basis documents. This paper helps Department of Energy (DOE), including the National Nuclear Security Administration (NNSA) and its contractors responsible for the safety basis improve safety basis documents and the unreviewed safety question (USQ) process with respect to MOS.

Margin of Safety Definition

Noun; margin of safety - the margin required in order to ensure safety; in engineering the margin of safety is the factor of safety (strength of the material divided by the anticipated stress) minus one.

Webster's dictionary includes among its definitions for margin, "something that is over and above what is strictly necessary and that is designed to provide for emergencies: a spare amount or measure or degree allowed or given for contingencies or special situations."

Margin of safety is defined by the range between two conditions identified in a hazard control document such as the TSRs. The first is the most adverse condition estimated or calculated in safety analyses to occur from an operational upset or family of related upsets. The second condition is the worst-case value known to be safe, from an engineering perspective. This value would be expected to be related to the condition at which some accident prevention or mitigation action is taken in response to the upset or accident, not the actual predicted failure point of some component. (DOE G 424.1-1B, p A-5)

A MOS is the range between two TSR parameter values: an upper limit above which a most adverse condition (e.g., significant offsite consequences ≥ 25 rem to the public) would occur and an administrative limit below the upper limit which could allow for transients (e.g., automatically activate Limiting Control Settings [LCS] equipment) that occur without having a catastrophic event. A MOS can only reside in the range between two values for a credited TSR parameter. If the parameter is not in the TSR, then the range between two values of the parameter cannot be a MOS.

Designed Factor of Safety and Derivation of Margin of Safety

In design, a factor of safety (aka safety factor) is normally used for safety related components. The maximum load that a structure, system or component (SSC) will be allowed to carry under normal conditions of operations is considerably smaller that the ultimate load or capacity of that SSC. This smaller load is referred to as the allowable load, and sometimes, as the working load or design load. Thus, only a fraction of the ultimate-load capacity of an SSC is used when the allowable load is applied. The remaining portion of the load-carrying capacity of the SSC is kept in reserve to assure safe performance. The ratio of the ultimate load to the allowable load is used to define the factor of safety[1].

$$\text{Factor of safety} = \text{FS} = \frac{\text{ultimate load}}{\text{allowable load}} \text{ or } \frac{\text{design overload}}{\text{normal load}}$$

where the design overload is defined as being just sufficient to cause failure[2].

An alternate definition of factor of safety is based on the use of stresses.

$$\text{Factor of safety} = \text{FS} = \frac{\text{ultimate stress}}{\text{allowable stress}}$$

In nuclear safety and in aeronautical engineering, the margin of safety is used in place of the factor of safety. The margin of safety is defined as the factor of safety minus one; that is margin of safety = FS-1.0. The margin of safety allows extra load range in the event the material is weaker than expected or an allowable load that may be higher than anticipated.

$$\text{Margin of safety} = \text{MOS} = \text{FS} - 1.0$$

Designs and codes may have safety factors or design margins. For example fire protection/sprinkler design, mechanical designs, etc. all include design margins. However, for purposes of the USQ Process, relevant margins of safety should be limited to the applications related to TSR SSC controls as described below.

Conservative Design Margins – Safety SSCs must be designed to withstand design basis loadings with an appropriate margin of safety. The design should incorporate multiple levels of protection against normal, anticipated, and accident conditions. For example, while built-in process controls may maintain pressure within a conservative limit, the design may also require provisions for relief valves, automatic shutdown capability, or other preventive features. (DOE-STD-1189, p I-22, 23)

Nuclear Regulatory Commission Handling of Margin of Safety and Technical Specifications

Let us look at available information regarding how the Nuclear Regulatory Commission (NRC) uses margin of safety in the nuclear facilities that it regulates. One of the NRC's key responsibilities is to

---

1 Mechanics of Materials, 4th Ed., Beer, F.P. and others, McGraw Hill, NY, NY, 2006.

2 Fundamentals of Machine Component Design, 4th Ed., Juvinall, R. C. and Marshek, John Wiley and Sons, Inc., Hoboken, NJ, 2006.

ensure the operation of nuclear power plants and other NRC-licensed facilities present no undue risk to public health and safety. The agency does this by applying and enforcing a set of technical requirements on plant design and operations, described in Title 10 of the Code of Federal Regulations (10 CFR).

The NRC considers design margins for safety related structures, systems, and components (SSC). Margin of Safety is found only in Technical Specification basis: e.g., 10 CFR 72.122, (4) (ii) "Reduce the margin of safety as defined in the basis for any technical specifications..."

10 CFR 52.79, section (4) The design of the facility including:

> (iii) Information relative to materials of construction, arrangement, and dimensions, sufficient to provide reasonable assurance that the design will conform to the design bases with adequate margin for safety.
>
> (5) An analysis and evaluation of the design and performance of structures, systems, and components with the objective of assessing the risk to public health and safety resulting from operation of the facility and including determination of the margins of safety during normal operations and transient conditions anticipated during the life of the facility, and the adequacy of structures, systems, and components provided for the prevention of accidents and the mitigation of the consequences of accidents.

NRC Regulatory Guide 1.176, considers the importance of the safety related SSC and the supporting SSCs when applying system categorization and margin of safety:

> Determination of the safety significance of system functions is inherently a "top down" process, starting with the front-line systems and system functions directly involved in plant-level safety functions (such as reactivity control, reactor pressure control, and decay heat removal). The delivery of high-pressure primary coolant from the reactor water storage tank to the core may be categorized as a high safety-significant function. The pumps, valves, and other SSCs whose proper operation is required to fulfill this function derive their initial categorization from the significance of the function. Therefore, any determination of an SSC's safety significance requires determination of the safety significance of all functions the SSC supports. Similarly, determination of the safety significance of support system functions (which should be later pursued in the support system's evaluation) is best performed by determining the safety significance of the function being supported. …
>
> When basic events are used to characterize the importance of system functions, the relationship between the failure of the basic events and the system functions they support becomes a critical consideration. For example, the risk achievement worth of a common cause failures basic event that fails a set of nominally identical pumps provides a reasonable estimate of the <u>margin of safety</u> the proper operation of the pumps is contributing. If the pumps fulfill only one system function, the risk achievement worth of the common cause failures provides a reasonable estimate of that function's contribution to <u>margin of safety</u>. (emphasis added, p 8)

10 CFR 830, Table 2 lists NRC Regulatory Guide 1.70 as a safe harbor for a DOE reactor. The writers of 10 CFR 830 had RG 1.70 in mind when considering the term margin of safety. RG 1.70, Section 6, Engineered Safety Features discusses the margin between two values of a critical pressure for a safety related SSC, as found in the following text.

> a. The postulated accident conditions and the extent of simultaneous occurrences (e.g., seismic event, loss of offsite power, and single active failures) that determine the containment design pressure requirements (including both internal and external design pressure requirements) should be discussed. The maximum calculated accident pressure should be stated, and the bases for establishing the <u>margin</u> between this pressure and the design pressure should be discussed.
>
> b. The postulated accident conditions and the extent of simultaneous occurrences (e.g., seismic event, loss of offsite power, and single active failures) that determine the design pressure requirements for the containment internal structures (i.e., containment subcompartments with reference to the design evaluation in Section 6.2.1.2) should be discussed. The maximum calculated accident pressures should be stated, and the bases for establishing the <u>margin</u> between this pressure and the design pressure should be discussed. (emphasis added, p 6-4)

The NRC use of MOS is limited to safety related SSCs in Technical Specifications. This could be an appropriate model for use and application by DOE/NNSA and its contractors.

Safety Limits (SL), Limiting Control Settings (LCS), and Limiting Conditions for Operation (LCO)

This section describes how margin of safety is relevant to SSCs controlled by SLs, LCSs, and LCOs. SLs, if used, are reserved for a small set of extremely significant features (safety class SSCs) that prevent potentially major off-site impacts (i.e., ≥ 25 rem to the public). LCSs are developed for any SL for an SSC that is protected by an automatic device with setpoints. LCSs act to keep normal operating conditions below the SLs and are developed for each identified SL, thereby providing a margin of safety. Most LCSs are assigned without an accompanying SL or a margin of safety. Likewise, LCOs are not expected to have an accompanying SL or a margin of safety. (DOE-STD-3009, p 68) (DOE-STD-1189, p I-34)

SLs are applicable only for protection of passive barriers as close to the accident source as possible whose failure, due to the occurrence of a specific event, will result in exceeding safety class (SC) criteria (i.e., the Evaluation Guideline of 25 rem to the public). Mitigation of releases is generally not amenable to useful definition of SLs. For example, a ventilation system directing airflow through HEPA filters to keep offsite radiological dose below the Evaluation Guideline during an accident is mitigative and is more appropriately covered by a LCO. Temporary loss of its function during normal operations does not initiate a significant hazardous material release. An LCO on the system would identify the specific responses necessary to compensate for the loss of safety function. Control of the ventilation system via a SL would be academic for preventing accidents that the ventilation system only mitigates. In contrast, consider a tank that acts as a barrier preventing an uncontrolled release of hazardous material that could exceed the Evaluation Guideline without ventilation mitigation. If that tank could experience a hydrogen explosion and rupture, then the tank hydrogen concentration may warrant coverage by a SL. (DOE-STD-1189, p I-34)

Figure 1 shows the margin of safety between a SL and a LCS for key SC TSR parameter tied to an SSC factor of safety. Normal operations occur below the LCS. The SL is tied to a safety factor and has a defined or explicit margin of safety. However, an abnormal operating transient could occur and the LCS is temporarily approached but not exceeded. The automated system response would correct the key parameter and keep its value below the LCS without ever exceeding the LCS, be within the range of the margin of safety. Thus, all normal operations and abnormal operating transients should always be less than the key SC TSR parameter LCS.

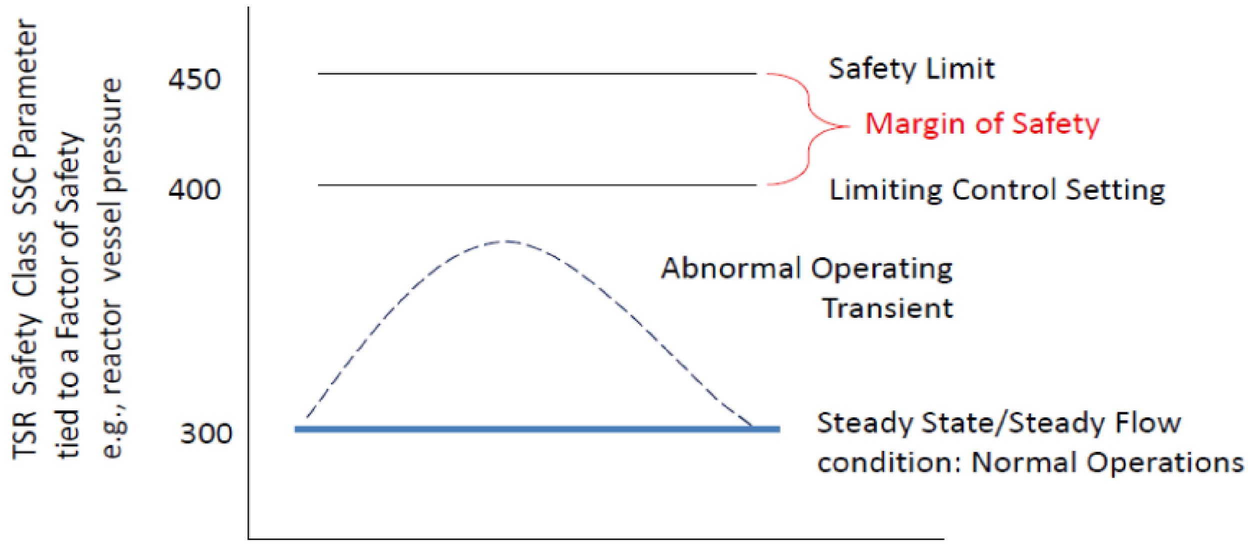


Figure 1

For example, a nuclear power reactor coolant temperature and pressure are controlled to operate at a steady state, steady flow condition for normal operations. For this example the reactor pressure is 300 psi for steady state, steady flow condition for normal operations (solid blue line in Figure 1), the LCS is 400 psi and the safety limit is 450 psi. The automated protection devices (e.g., pressure relief valve, etc.) are designed and set to control the pressure so that the Limiting Control Setting is not exceeded for any abnormal operating transients (dashed blue line in Figure 1). A pressure relief valve could actuate to vent at a pressure above 300 psi but below 400 psi. The design for the pressure relief valve considers all calculation conservatisms and uncertainties to keep the pressure transient below the LCS and preserves the margin of safety (the range between the SL and LCS as indicated in Figure 1).

Let us consider making a change to the credited pressure relief valve and the effect that change may have on the safety basis. The normal operating conditions and expected abnormal operating transients are documented in the safety basis. Changes to the pressure relief valve are evaluated via the USQ process approved for the facility. USQ question 7 asks "Could the proposed change reduce the margin of safety?" Changes to the pressure relief valve that keep the expected abnormal operating transients below the LCS and preserve the margin of safety have a no answer to the margin of safety question.

Figure 2 represents the same nuclear power reactor coolant temperature and pressure given in the above example, but with an USQ that has a Yes answer to USQ question 7, because it has a decreased margin of safety. For example, the pressure relief valve was changed so that it no longer can meet its safety function of keeping the transients pressures below the LCS.

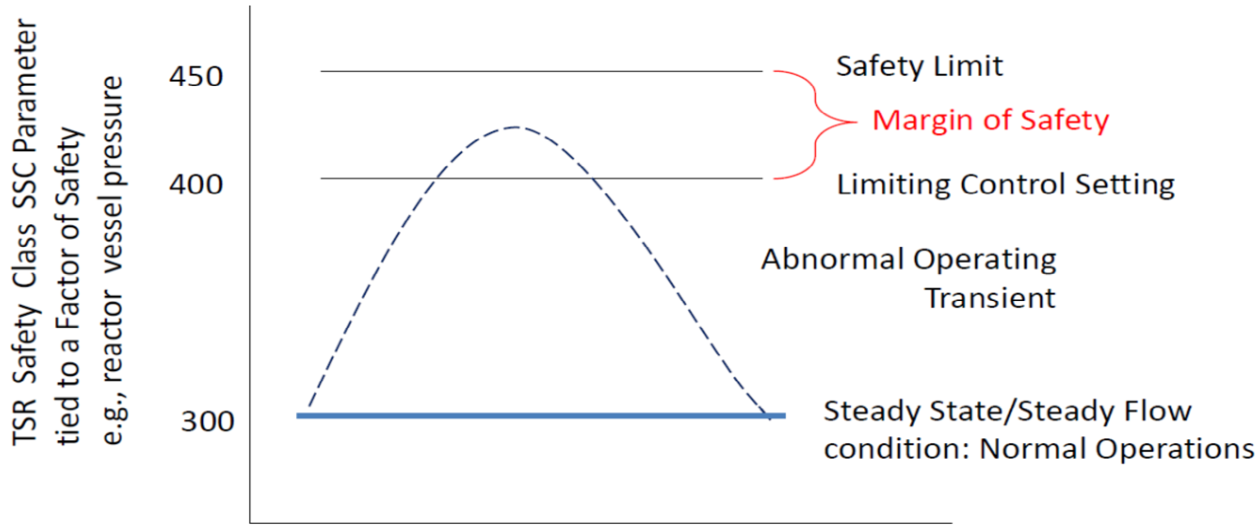


Figure 2

Margin of Safety for Building Structure Blast Design Criteria

Let us consider a safety class SSC, the building structure, designed and built with a design safety factor and a TSR limit on the weight of explosives allowed in that building structure. The pressure created by an explosive detonation inside a building is analogous to the pressure inside a vessel when comparing this example to the NRC application of a pressure inside a reactor vessel or containment building.

An example Nuclear Facility (NF) building structure was designed with a safety factor of 1.5 as described in its design criteria document. The assembly bays, bunkers, and high bays can withstand a blast net explosive weight (NEW) limit times the safety factor of 1.5. The explosive weight limit is a TSR parameter control (MAR limit) documented in the TSR. The range between the TSR NEW limit and the NEW limit times the factor of safety is a margin of safety.

The Blast Analysis is contained in NF design criteria document. The analysis considers an explosion of 423 lb NEW in an assembly cell with a factor of safety of 1.5. The results include the maximum over-pressures and impulses on an acceptor cell walls and roofs from an explosion in an adjacent cell. The range between 635 lbs and 423 lbs NEW is a MOS.

$$\text{Factor of safety} = \text{FS} = \frac{\text{ultimate load}}{\text{allowable load}} \quad \text{or} \quad \frac{635}{423} = 1.5$$

$$\text{Margin of safety} = \text{MOS} = \text{FS} - 1.0 \text{ or } 1.5 - 1.0 = 0.5$$

Thus, the MOS for the SC building structure is 0.5.

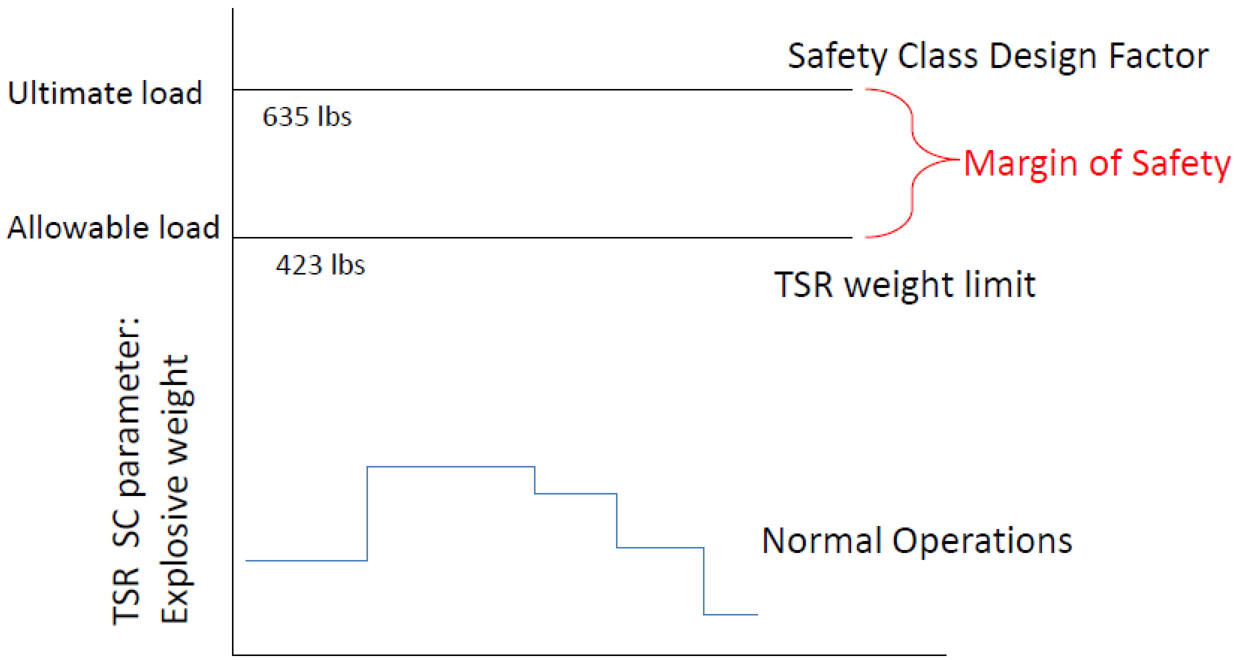


Figure 3

Normal operations (solid blue line) would always have the weight of explosives in a building at an amount less than the TSR limit. Figure 3 depicts the margin of safety between a SC Design Factor and a TSR weight limit.

A catastrophic event (significant offsite consequence) would occur if more than the design factor NEW [423 lbs x 1.5 (635 lbs)] detonated in a building structure; the blast would possibly exceed the design and what the building structural components could contain based upon the estimated calculation. If the explosion involved radioactive material, then the offsite consequences could be more than what was analyzed in the Documented Safety Analysis (DSA).

K_{eff} Parameter Difference Between Values is Not a Margin of Safety

In nuclear criticality safety, one important parameter is k_{eff}. The definition of k_{eff} from ANSI/ANS 8.1 **effective multiplication factor (k_{eff}).**

> ***Physically***, *the ratio of the total number of neutrons produced during a time interval (excluding neutrons produced by sources whose strengths are not a function of fission rate) to the total number of neutrons lost by absorption and leakage during the same interval.*
>
> ***Mathematically*** *(computationally), that eigen value number which, when divided into the actual mean number of neutrons emitted per fission in an assembly of materials, would make the calculated result for the nuclear chain reaction of that assembly critical.*

The overarching regulations in both the DOE and the NRC with respect to nuclear criticality safety are the ANSI/ANS-8 National Consensus Standards. These standards do not anywhere mandate a specific delta-k value as a subcritical margin - for very good reasons. The overriding SHALL statement is: "Before starting a new operation with fissile materials or before an existing operation is changed, it shall be determined that the entire process will be subcritical under both normal and credible abnormal conditions."

Thus, the differences between values of k_{eff} for operations involving fissile material are not margins of safety.

DOE-STD-1066 Hydraulic Design Pressure Parameter Difference is Not a Margin of Safety

DOE-STD-1066, Section 4.2.7 Fire Protection Systems and Equipment, discusses hydraulically designed sprinkler systems. According to DOE-STD-1066:

> 4.2.7.6.2 Hydraulically designed sprinkler systems shall be designed for a supply pressure of at least 10 percent, but not less than 10 pounds per square inch (psi), below the water supply curve to provide a pressure margin to accommodate minor system modifications or degradation of the water supply and sprinkler systems that may occur over time. (p 17)

The 10 percent is a design margin applied to the supply pressure that is expected to decrease over time, but this is not a margin of safety.

Factors in the Selection of a Safety Factor that are Not a Margin of Safety

- Degree about uncertainty about loading
- Degree about uncertainty about material strength
- Uncertainties in relating applied load to material strength via stress analysis
- Conservatisms in calculations
- Rounding up or down of numbers

Margin of Safety Expectation

Margins of safety are not always required to be developed; if development of the DSA derived margins of safety, those margins of safety should be explicitly defined in the DSA as a best management practice. Margins of safety should not be left implicit in a DSA as subsequent USQ processing would be inconsistently applied. A MOS is more likely to apply to hazard category 1 or 2 nuclear facility safety class hazard controls since the bases for these hazard controls have a higher relative likelihood of being influenced by worst-case assumptions of initial conditions, conservative assumptions in computer modeling and codes, allowance for instrument drift and system response time, redundancy and independence of components in safety trains, and plant response during operating transient and accident conditions. Margin of safety is not anticipated or required for most non-reactor nuclear facilities. "A DSA prepared in accordance with this Standard is focused on identifying functional requirements that, in general, are neither absolute **nor subject to fine safety margin resolution** [emphasis added]." (DOE-STD-3009, Ch 4, p 56)

DOE Guide 424.1-1B (DOE G 424.1-1B), including its attachments, provides information to assist in the implementation of Title 10 Code of Federal Regulations (CFR) Section 830.203, "Unreviewed Safety

Question Process," of the Nuclear Safety Management Rules for Category 1, 2, and 3 nuclear facilities owned or operated by the DOE, including the NNSA. However, unclear and conflicting MOS language regarding implicit MOS still exists in the USQ Process guide. According to DOE G 424.1-1B:

> Hazard control documents set forth the minimum acceptable limits for operation under normal and specified failure conditions; they ensure that the available safety equipment and operating conditions meet the assumptions in the existing safety analyses. They distill those aspects of the safety analyses that are required to ensure the performance of safety SSCs and personnel as relied on and defined in the safety analyses.
>
> The bases for a hazard control should define the margin of safety. If the bases of a hazard control do not specifically identify a margin of safety, the DSA and other appropriate safety basis documents should be reviewed to determine whether the proposed change, test or experiment, or new information has or would result in a reduction in a margin of safety. The judgment on whether the margin is reduced should be based on physical parameters or conditions that can be observed or calculated. …
>
> Safety margins generally include worst-case assumptions of initial conditions, conservative assumptions in computer modeling and codes, allowance for instrument drift and system response time, redundancy and independence of components in safety trains, and plant response during operating transient and accident conditions. A change that affects initial conditions, a system response time, or some other parameter that can affect the course of an accident analysis supporting the bases of hazard controls is evaluated to determine whether the change would reduce a margin of safety. (p A-5)

Answering the 7th Question in the USQ Process for MOS and no MOS

Example 1, no decrease in margin of safety for changes related to SSCs.

Could the proposed change reduce the margin of safety? NO

WHY (explain the technical basis for the answer):

The proposed change does not reduce any margin of safety. The DSA and TSR were reviewed and no explicit or implicit margin of safety is associated with the potentially affected SSCs, other affected SSCs, or this proposed change. The proposed activity doesn't affect initial conditions, system response times, or other credited parameters impacting the accident analysis supporting the bases of hazard controls. Hence, no margin of safety is reduced.

Example 2, no decrease in margin of safety for simple changes not related to SSCs.

Could the proposed change reduce the margin of safety? NO

WHY (explain the technical basis for the answer):

The proposed change does not reduce any margin of safety. The DSA and TSR were reviewed and no explicit or implicit margin of safety is associated with this proposed change. The proposed activity doesn't affect initial conditions, system response times, or other credited parameters impacting the accident analysis supporting the bases of hazard controls. Hence, no margin of safety is reduced.

Example 3, no decrease in margin of safety for simple changes not related to SSCs, and is consistent with the DSA.

Could the proposed change reduce the margin of safety? NO

WHY (explain the technical basis for the answer):

The proposed activity does not reduce any margin of safety. The proposed activity is consistent with administrative programs specified in the DSA. Therefore, the proposed activity cannot change the implicit or explicit margin of safety.

Example 4, no decrease in margin of safety for proposed change that does not impact an Equipment Important to Safety (EITS) parameter.

Could the proposed change reduce the margin of safety? NO

NOTE: Since MOS is defined as range between two values of an SC or SS EITS parameter, and this proposed change does not involve any EITS parameter, then no MOS is associated with this proposed change.

WHY (explain the technical basis for the answer):

The proposed activity does not reduce any margin of safety. The approved safety basis was reviewed for a reduction in any implicit or explicit margin of safety. No margin of safety or safety limits are associated with this facility and no EITS parameter is impacted by the proposed activity. Therefore, the proposed activity cannot change any margin of safety.

TSR Bases Example Text for MOS and no MOS

A. The automated activation of ABC equipment at the LCS for SC vessel XYZ protects the SL. The range between the TSR parameter values of the LCS and the SL is a margin of safety.

B. No explicit or implicit margin of safety is associated with the ABC equipment described in LCO 3/4.x.

Summary

Safety basis documents should be reviewed to identify any relevant margins of safety. Not every range between two safety basis values document a margin of safety. The bases of hazard TSRs should identify relevant margins of safety. Only controls for a credited SC or SS SSC could potentially involve a margin of safety. No MOS applies to safety management programs or to specific administrative controls. After a review of the safety basis has been conducted to determine if any margin of safety exists, then the DSA Executive Summary should include a statement documenting the results of this evaluation. Consistent with each DSA change, the statement documenting the results will be evaluated via a Safety Evaluation Report by the DOE approval authority. The USQ Process will become more efficient by decreasing time spent on the margin of safety USQ question.

References

10 CFR 52, *Licenses, Certifications, and Approvals for Nuclear Power Plants*. U.S. Nuclear Regulatory Commission, April 18, 1989.

10 CFR 72, *Licensing Requirements for the Independent Storage of Spent Nuclear Fuel, High-level Radioactive Waste, and Reactor-related Greater than Class C Waste*, U.S. Department of Energy, December 1, 2009.

10 CFR 830, *Nuclear Safety Management*, U.S. Department of Energy, January 10, 2011.

DOE G 421.1-2A, *Implementation Guide for Use in Developing Documented Safety Analyses to Meet Subpart B of 10 CFR 830*, U.S. Department of Energy, December 19, 2011.

DOE G 424.1-1B, *Implementation Guide for Use in Addressing Unreviewed Safety Question Requirements*, U.S. Department of Energy, April 8, 2010.

NRC Regulatory Guide 1.176, *An Approach for Plant-Specific, Risk-Informed Decisionmaking: Graded Quality Assurance*, U.S. Nuclear Regulatory Commission, August 1998.

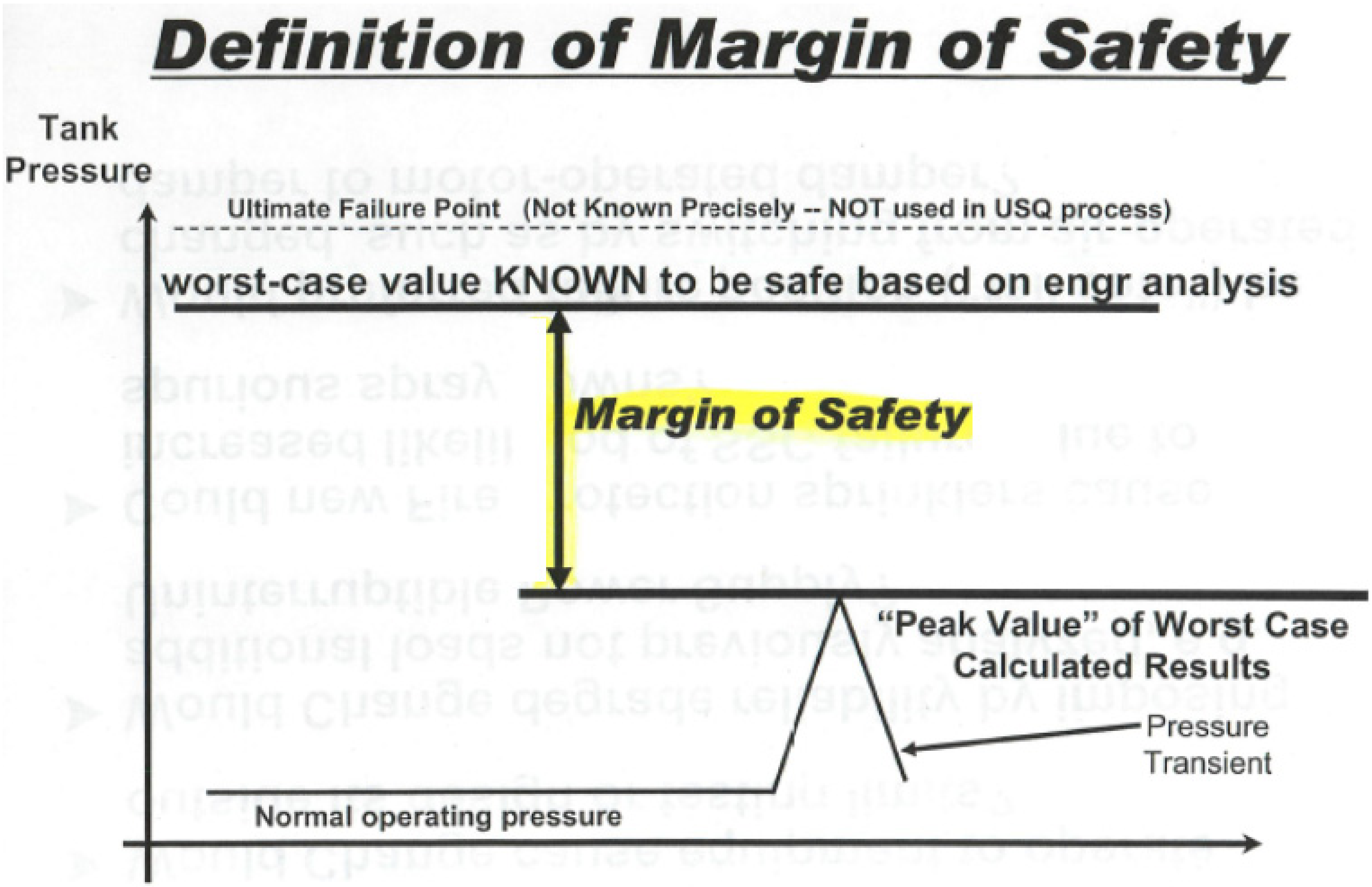
NRC Regulatory Guide 1.70, *Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants*, U.S. Nuclear Regulatory Commission, Revision 3, November 1978.

DOE-STD-1066-2012, *Fire Protection*, U.S. Department of Energy, December 2012.

DOE-STD-1189-2008, *Integration of Safety into the Design Process*, U.S. Department of Energy, March 2008.

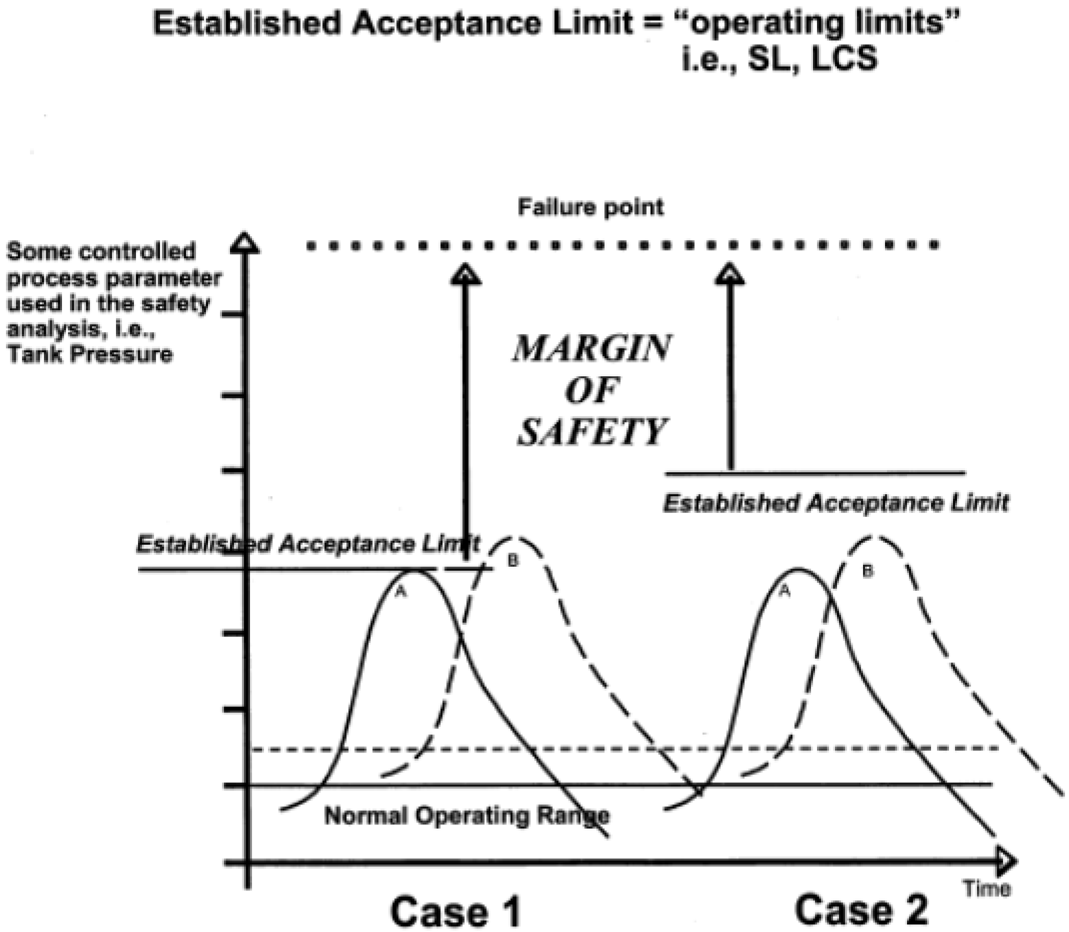
DOE-STD-3009, Change Notice 3, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, U.S. Department of Energy, March 2006.

Comments from the NNSA, Nevada Field Office, Nuclear Safety Team during a meeting on 9-9-13 were incorporated into this document.



Definition of Margin of Safety
Tank
Pressure
Ultimate Failure Point (Not Known Precisely -- NOT used in USQ process)
worst-case value KNOWN to be safe based on engr analysis
Margin of Safety
"Peak Value" of Worst Case
Calculated Results
Pressure
Transient
Normal operating pressure

Figure 4

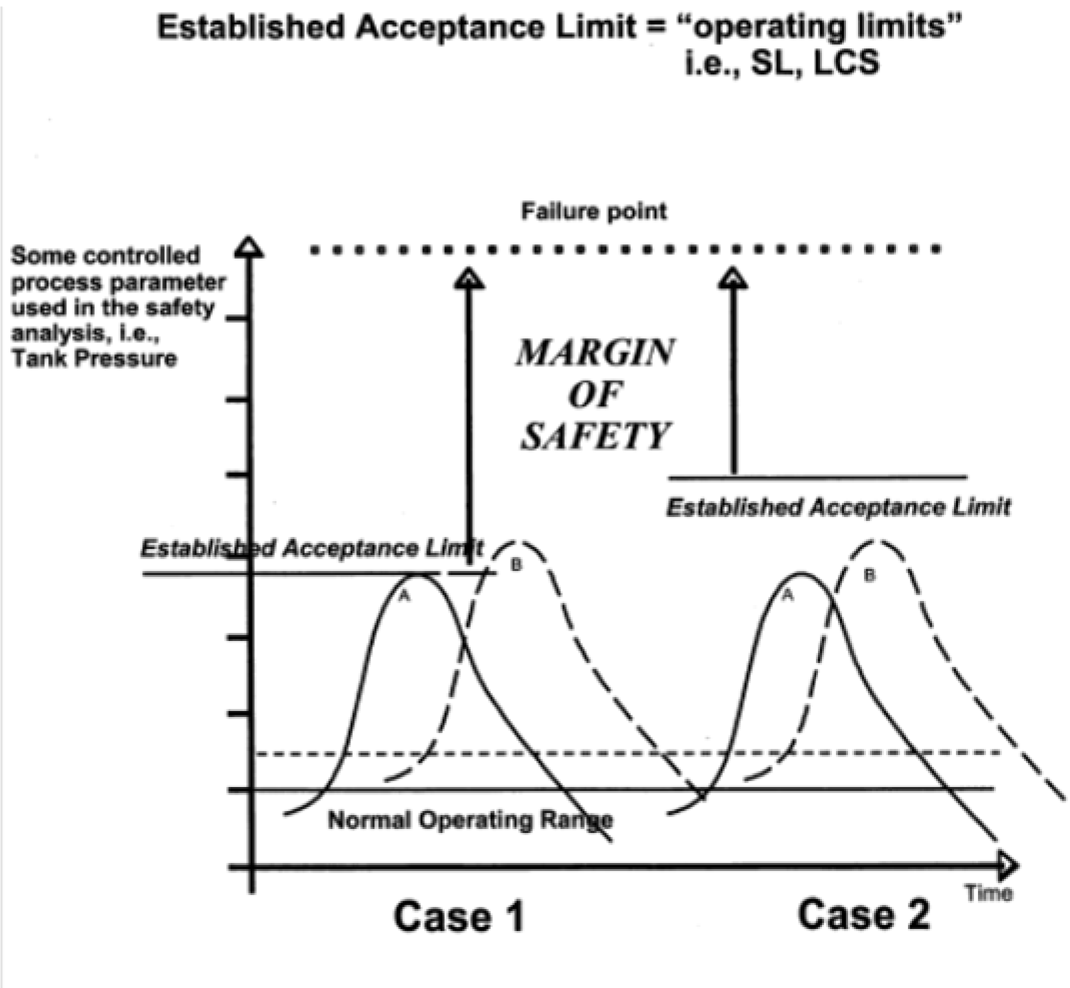


Now consider a proposed activity. The "A" curve in both cases represents a safety-related and controlled (through TSRs) process parameter under normal operations. The "B" curve represents this process parameter after the proposed modification.

In Case 1, the "B" curve depicts the predicted maximum pressure expected from proposed changes to the process. Since this max pressure is greater than the maximum previously established acceptance limit, it represents operation in an unanalyzed state and represents a reduction in the margin of safety. This would require a "Yes" on the question on the USQ determination.

However, in Case 2, the "B" curve is still under the previously established acceptance limit. There is no reduction in the margin of safety and the question would be answered "No".

Figure 5



Now consider a proposed activity. The "A" curve in both cases represents a safety-related and controlled (through TSRs) process parameter under normal operations. The "B" curve represents this process parameter after the proposed modification.

In Case 1, the "B" curve depicts the predicted maximum pressure expected from proposed changes to the process. Since this max pressure is greater than the maximum previously established acceptance limit, it represents operation in an unanalyzed state and represents a reduction in the margin of safety. This would require a "Yes" on the question on the USQ determination.

However, in Case 2, the "B" curve is still under the previously established acceptance limit. There is no reduction in the margin of safety and the question would be answered "No".

Figure 6