

The Lost Intent of TSRs and Violations

**Charles M. Voldness
Washington Savannah River Site**

Technical and Quality Services

Nuclear Safety

PURPOSE AND SCOPE

SRS noted an increase in Technical Safety Requirement (TSR) violations in CY2004. A causal analysis indicated that the violations were generally the result of human errors, inadequate communications and management issues. However, a review of these and other TSR violations was performed which identified additional, more subtle issues associated with these events. For example, a lack of consistency was noted in the thresholds applied to the determination of whether a TSR violation had occurred, particularly when applied to programmatic administrative controls.

These observations resulted in conduct of a review for the purpose of improving the understanding of the intent of TSRs and applying this understanding to the TSR development process. This understanding could also assist in the development of guidelines for determining when a TSR violation has occurred. The review included an examination of the definition and intent of TSRs as specified in DOE Orders, Guides and Standards, and facility safety basis documents (e.g., DSAs, TSRs). Particular attention was applied toward programmatic administrative control TSRs and determining when declaration of their violation is appropriate.

THE INTENT AND DEFINITION OF A TSR

Safe operation of a DOE nuclear facility is accomplished by imposing limits, such as Technical Safety Requirements (TSRs), on facility operations. 10CFR830 defines Technical Safety Requirements (TSRs) as "the limits, controls, and related actions that establish the specific parameters and requisite actions for the safe operation of a nuclear facility." A recently issued DOE Standard (1186) is somewhat more definitive in stating that TSRs are intended to define the outer bounds of the safety envelope as identified in the Documented Safety Analysis (DSA).

The limits of safe operations are determined through the analysis of operations and accidents. This analysis identifies the level of performance required of safety class and safety significant structures systems and components (SSCs), and describes any ACs or procedures that are necessary to meet the specific safety criteria for the facility.

Although TSR values are based upon the DSA values, there is often a margin built into the TSR values such that the TSR value is more conservative than the DSA Safety Analysis Value (SAV). This provides an additional level of protection to the safety boundary as defined in the DSA and accounts for variables such as instrument uncertainty, drift, etc.. As such, a TSR should be considered as "that which defines the safety envelope boundary, as defined by DOE." In other words, a TSR defines the level of risk DOE is willing to accept.

In other instances, the argument becomes a time-at-risk issue (i.e., how long may a facility continue to operate in its present mode or condition with degraded equipment; how often do we need to check credited equipment to ensure its continued operability, etc.). In the event of malfunction of credited equipment, DOE accepts facility operation with a degraded safety posture for a specified period of time assuming they have implemented the necessary compensatory measures (required actions) that are specified in the TSRs.

THE INTENT AND DEFINITION OF A TSR VIOLATION

A TSR violation would be expected to indicate that a facility has operated outside of the outer bounds of the safety envelope as defined by the TSRs. It is important to note that this definition would not include events in which the facility could have potentially or unknowingly operated outside of the safety basis due to circumstances such as inoperable equipment (e.g., due to setpoints which may have drifted outside of limits within calibration frequencies) or discrepant field conditions. Such events are accepted risks as evidenced by DOE approval of the TSRs and which can be addressed using the DOE-approved Unreviewed Safety Question process.

It may also be argued that a TSR violation must be the result of human error. The declaration of a TSR violation has a very negative connotation on contractor performance and may subject the contractor to fines and other penalties. One would not anticipate that events caused by factors outside of the contractor's control (e.g., unanticipated events or DOE approved risks) would be subject to fines and penalties. This principal is best illustrated by the following examples:

- Failure of a design feature would not be considered a TSR violation if the preventive controls on that feature (e.g., surveillances) had been met and the mitigative controls associated with the event had been properly implemented. This is because the risk of failure was accepted by DOE (assuming the controls were properly implemented) as evidenced by their approval of the safety basis.
- Failure of a design feature as the result of an unanticipated initiator would not be considered a TSR violation, but rather, a Potential Inadequacy in the Safety Basis (PISA). PISAs are considered to be an anticipated event, or risk, with DOE-approved actions required to be taken upon their discovery. As such, they would not be considered a TSR violation, unless appropriate actions were not taken.

It is therefore postulated that a TSR violation is defined as *“a human-based event which results in a facility operating outside of the outer bounds of the safety envelope, as defined by the TSRs.”*

TYPES OF TSRs

TSRs are comprised of the following:

- Safety limits and associated limiting control system settings
- Limiting conditions for operation and associated surveillance requirements
- Credited design features.
- Administrative controls (programmatic and/or specific)

These are discussed in more detail below.

- Safety Limits

Safety Limits provided in the DSA are limits on process variables associated with those safety-class physical barriers, generally passive, that are necessary for the intended facility functions which are required to guard against the uncontrolled release of radioactive materials. DOE-STD-3009-94, states that “S(afety) L(imits)...are reserved for a small set of extremely significant features that prevent potentially major offsite impact.” The significance of a Safety Limit-based TSR is demonstrated in that “Facilities are required to immediately initiate actions to place the facility in a safe condition, which may include a total shutdown of the facility, if such a violation occurs.” Currently, there are no facilities at SRS which have safety limits (and therefore limiting control system settings) specified in their TSRs; therefore, safety-limit TSRs will not be discussed further in this document.

- Limiting Conditions for Operation

Limiting conditions for operation are defined as the limits that represent the lowest functional capability or performance level of safety-related structures, systems, and components required for safe operations. In practice, LCOs may either specify limits on process parameters or operability requirements for credited equipment. In either case, if the specified limit is not met, required compensatory actions and associated completion times are specified in the LCO. In order to verify operability of credited equipment, surveillance tests are periodically performed on the equipment.

- Credited Design Features

Vital, passive components such as piping, vessels, supports, structures, and containers would typically be considered design features. These components are discussed in the Design Features Section of the TSR document. For example, a glovebox is an obvious barrier to uncontrolled material release. The windows, gloves, and cable/piping connectors are all necessary to maintain the barrier, but do not specifically require operational limits or administrative controls as contributors to defense in depth.

- Administrative Controls

Administrative Control TSRs may consist of commitments to sitewide safety management programs, commitments to facility-specific programs or process controls. These TSRs do not typically provide the equivalent of “Required Actions” which are provided in LCO-based TSRs. TSR administrative programs do not specify what may constitute the violation of a particular TSR.

There are two kinds of administrative controls. These are:

Programmatic - Most TSR ACs are designed to provide broad programmatic support for sitewide safety management programs or facility specific programs supporting defense-in-depth, or worker safety. A programmatic AC does not provide specific limits or discernible operator actions relating to specific hazard or accident analysis conditions. Rather, they are intended to define those basic program elements or features that constitute the viability of the program to support safe operations. Programmatic ACs are typically implemented as

performance requirements contained in organizational or company-level procedures. Examples of a Programmatic Administrative Control would be the Radiation Protection, Nuclear Criticality or Quality Assurance programs.

Specific - A Specific Administrative Control (SAC) may be designated if (1) it is identified in the DSA as a control needed to prevent or mitigate an accident scenario, and (2) it has a safety function that would be Safety Significant or Safety Class if the function were provided by an SSC. Based on the Standards/Requirements Identification Document, SACs typically include ACs that are credited as part of the primary control set (e.g., primary Level of Control).] An example of a Specific Administrative Control which could qualify as a TSR would be a specific combustible loading limit (e.g., 5,000 wood lbs equivalent).

In addition to providing the main mechanisms for hazard control, an SAC may also be designated to protect important initial conditions and assumptions of the hazard or accident analysis.

SRS APPLICATION OF TSRS

As previously noted, a TSR is intended to define and/or protect the operating envelope defined by the DSA. A “buffer” to this envelope may be included when developing the TSR by inclusion of a safety margin. However, in some cases, the level and basis for this margin has been applied overconservatively. This may be manifested in the actual limits associated with LCOs and SACs being unnecessarily high (or low) and can result in TSR violations which are of minimal safety consequence (i.e., no challenge to the safety basis boundary or facility safety). Although a level of conservatism is considered good practice in the development of limits and controls, overconservatism which result in declaration of TSR violations for insignificant control failures can result in development of an insensitive attitude to TSR failures and/or an unwarranted negative perception of the contractor, thereby undermining the intent of these high-level controls.

An overconservative TSR is demonstrated by the following example:

An administrative control TSR for the Solid Waste Management Facility (SWMF) (TSR 5.5.2.7) limits the 55-gallon drum content to 485 FGE Pu-239. Several TSR violations have been declared due to legacy drums exceeding this amount of fissile material. However, an analysis demonstrated that several waste drums in an array remain subcritical with high fissile content (up to 730 grams ²³⁹Pu) under optimum conditions of moderation, reflection, geometry, and interaction. Based on engineering judgment, an array of legacy drums with at least 485 FGE Pu-239 under optimal reflection, moderation, etc. is Beyond Extremely Unlikely (BEU) for the following reasons:

- Very few drums with more than 485 FGE Pu-239 have been discovered. These have consisted of a very small percentage of the total number of drums and the likelihood of several such drums together in an array is remote.

- The possibility that any these drums would be optimally moderated, reflected, etc. is negligible.
- A criticality under less than optimum conditions would require kilogram quantities of fissile material. For example, the maximum subcritical mass for a drum in the IQ3 unit (near ideal reflection) increases to 20 kilograms plutonium (100% ²³⁹Pu) when the moderator volume decreases to 5.7 liters.

In summary, there is no challenge to safety if a drum, or even several drums, are determined to have 485 grams Pu-239.

SRS APPLICATION AND TSR VIOLATIONS

The violation of a TSR is easily determined for an LCO. Operation outside the LCO, in addition to the failure to perform the Required Action within the specified time constraints defines such a violation.

A violation is also relatively simple to ascertain for Specific Administrative Controls (SAC). For these, some specifically credited control in the DSA is not met (e.g., Material at Risk limit). SACs sometimes provide a Required Action (or equivalent) or allow some accepted amount of time at risk which must be exceeded before a TSR violation is declared. If a SAC is written in the format of an LCO, a TSR violation is defined the same as it is for a non-SAC LCO. If the SAC is written in the format of a programmatic AC, a violation is immediate upon discovery of the discrepant condition, provided an action is not included in the SAC.

A programmatic AC TSR violation is not as clearly discernable for those controls in which an administrative program is credited as a TSR in a generic manner (e.g., radiation protection or criticality safety program). Determination of a violation can be very subjective. In an attempt to provide some definition to what would constitute the violation of such a TSR, the facilities at SRS have incorporated definitions of a violation into the TSR documents themselves. For example:

- FB- and HB Lines - failing to comply with a programmatic requirement. NOTE: Violations of this nature are characterized by repeated deviations of noncompliance or neglect for a program. *Individual deviations are not considered to be TSR violations.*
- F& H Canyon - Failing to comply with an Administrative Control programmatic requirement. NOTE: Violations of this nature are typically characterized by programmatic noncompliance or neglect for observance of Administrative Controls. *Deviations within the implementing programs for Administrative Controls are not considered to be TSR violations.*
- DWPF/CST - Failure to comply with an Administrative Control statement is a TSR violation when either the Administrative Control is directly violated, as would be the case

with not meeting minimum staffing requirements for example, or the intent of a referenced program is not fulfilled. *To qualify as a TSR violation, the failure to meet the intent of the referenced program would need to be significant enough to render the DSA summary invalid.*

- Tritium, K/L, 235-F - *Programmatic noncompliance or repeated neglect* for observance of the Administrative Controls.

It is apparent that these definitions, which are all taken directly from DOE-approved safety basis documents, are not consistent. Several, but not all of the TSR violation definitions explicitly state that an administrative control TSR violation cannot be claimed for any single deviation from program requirements. The Concentration, Storage and Transfer (CST) definition of a TSR violation does not make this claim. This has allowed them to be subject to a declaration of a TSR violation for a single program deviation which at least partially accounted for some of the increase seen in TSR violations during CY2004. It is probable that a similar deviation in other site facilities would not have been classified as a TSR violation.

Examples

Guidance, Application and Implementation

As a result of the aforementioned observations, an effort was undertaken to identify and assess applicable DOE Orders, Standards and Guides with the goal of developing guidance and direction for use in the determination of whether a TSR violation had occurred. Findings are discussed below.

The DOE “Implementation Guide for Use in Developing Technical Safety Requirements (TSRs)” states that a TSR violation is considered to have occurred as a result of the following four circumstances.

- Exceeding a Safety Limit (SL).
- Failure to complete an ACTION statement within the required time limit following exceeding a Limiting Control Setting (LCS) or failing to comply with a Limiting Condition for Operations (LCO)
- Failure to perform surveillances within the required time limit.
- Failure to comply with an Administrative Control (AC) statement.

As previously discussed, the application of the first three definitions of a TSR violation are straightforward. These apply to Safety Limits/LCOs and Specific Administrative Controls (SACs) which have some specific limit (e.g., setpoint) or requirement (e.g., amount of fissile material) which either has or has not been exceeded. These types of violations will not be discussed further in this document.

- Programmatic AC TSR Violations

The remaining TSR violation definition (i.e., Failure to comply with an Administrative Control (AC) statement) applies to violation of programmatic administrative controls. This definition is can be very subjective, require significant judgment, and has been inconsistently applied. DOE Standards and Guides were examined to assess whether there was additional guidance which could be used to determine when an AC TSR violation had occurred. The following statements were noted:

1. The DOE TSR Development Guide states that a failure to comply with an AC statement is “a TSR violation ... when the intent of the program is not fulfilled”. It goes on to state that “to qualify as a TSR violation, the failure to meet the intent of the referenced program would need to be significant enough to render the DSA summary invalid.”
2. The DOE-Standard on DSA preparation states that “discrepancies in a program would not constitute violation of the safety basis unless the discrepancies were so gross as to render premises of the summary invalid.”
3. The recently issued DOE Standard on Specific Administrative Controls (1189) provides some additional insight by stating that “a TSR violation of a safety management program can only result from a gross program failure, significant enough to render the DSA summary invalid”.

The above definitions appear to be the entire summation of guidance on programmatic administrative control violations. Inadequacies noted in the guidelines are as follows:

- The intent of a TSR programmatic AC as specified in the first “bullet” is not often defined in a clear and concise manner.
- Interviews have indicated that the term “(DSA) summary” used in all of the above definitions is not a defined or understood term.

As such, the statements allow a significant degree of subjectivity in the assessment of events. However, the statements are sufficient to demonstrate that a broad-based, or “gross program failure” is required for a legitimate violation. It would not be expected that a single deviation be considered to invalidate an entire program or to be a “gross program failure”. Therefore, a single failure would not constitute a TSR violation. However, some of the TSR violations at SRS consisted of relatively minor procedure non-compliances. For example, a TSR violation was declared when steps in a procedure being used to verify hydrogen concentration were performed incorrectly. This is contrary to the three statements/definitions provided above.

Based on the aforementioned arguments, it is logical to assume that declaration of a programmatic AC TSR violation should be significant enough to judge that remaining programmatic controls could be inadequate to prevent a significant hazardous event. Conversely, if an administrative control failure were to occur with no immediate action required and

negligible potential for a significant hazardous event, a programmatic AC TSR violation should not be considered to have occurred. However, programmatic AC TSR violations are being declared even though the event has little or no impact on safety margin and immediate actions are not warranted, or even required.

The inconsistent application of the intent of TSRs is demonstrated by an event at SRS in which a legacy drum had been relocated to a condition in which it was “more safe” than that in which it was found and yet, a TSR violation was declared. In this event, a legacy waste drum was removed from an array, segregated (increased level of criticality safety) and moved to a Hazard Category (HC) 3 facility. The drum was then assayed and found to contain HC 2 levels of fissile material. A TSR violation was declared based on exceeding the HC3 limit. However, there was no challenge to safety, no increase in risk, no program failure, etc. In fact, the risk had been reduced by removing the drum from the array and segregating it. In addition, several other controls remained in place which provided additional barriers to any possible challenge to safety.

It is also worth noting that this event would not have qualified as a violation at the Idaho Completion Project, Radioactive Waste Management Complex, or RWMC (the equivalent of the Solid Waste Facility at SRS). The TSRs at RWMC consist of a 380 gram limit on individual drums which if exceeded, only requires that the drum be segregated and evaluated. This may indicate a potential deficiency in the wording and basis of the SRS TSR. (Note: 11/06 – SWMF TSRS have been revised to incorporate this principal).

Further investigation of SRS administrative control TSRs noted that most, if not all of the programmatic controls credit the entire program in a generic manner. However, it appears that some degree of program specificity is expected when defining these programmatic controls. DOE Guidance states the following;

- DOE-STD-3009-94 - “descriptions should be sufficiently detailed that a basic understanding is provided of what is controlled and why”.
- DOE Guide 423.1 - “It is expected that the ACs will be tailored to the facility activities and the hazards identified in the DSA.”

An example of this potential inadequacy is demonstrated by the common practice of crediting an entire, “generic” TSR programmatic control. For example, every aspect of the Site Fire Protection program is not relied upon to meet the intent of this commonly credited control. Alarms and testing or the combustible loading program would probably be credited program elements while the budget or administration aspects of the program would not. However, the credited elements of the program are not typically defined in the Hazard Analysis nor in the TSRs. The failure to identify the specific credited elements creates the potential for the failure of a relatively trivial or irrelevant program aspect to be ruled a TSR violation. This appears to be contrary to DOE guidance.

SUMMARY AND CONCLUSIONS

The review identified several issues which have resulted in the subjective declaration of TSR violations. The following weaknesses were noted:

- The concept and definition of a TSR are not clearly defined, understood or consistently applied. While DOE guidance states that TSRs are intended to define the outer bounds of the safety envelope as identified in the Documented Safety Analysis (DSA), the bases for TSRs is often inadequate and overconservative safety margins are sometimes incorporated into a TSR.
- The basis for declaring a TSR violation is not adequately defined in DOE guidelines. This results in personal interpretation and the declaration of several TSR violations which, in all likelihood, were not violations.
- The definition of a programmatic administrative control TSR violation is inadequately defined in DOE guidelines. Terms used in defining a violation are not defined or understood (e.g., DSA summary). Once again, this allows declaration of a violation to be applied in a highly subjective and personality-driven manner.
- Some TSR programmatic administrative control violations which have been declared at SRS do not appear to meet the intent of DOE guidance. Rather than indicate a significant programmatic breakdown warranting immediate response to regain a safe posture, some violations are declared based on a single non-compliance issue of a very limited scope, which has minimal impact on overall facility safety. This should never be the case. If a single non-compliance is significant enough to warrant a TSR violation, that particular element should be elevated to a SAC.
- Definitions of administrative control TSR violation contained in SRS facility TSRs are not consistent. Some definitions are explicit in that single deviations do not constitute a violation, while others are more subjective.
- Administrative controls are not adequately derived or written. If specific program elements are credited, they are often not identified in the hazards analysis and/or carried through in a forward manner to the DSA and TSR documents as SACs. Required actions are not provided and criteria for more clearly defining a violation are not defined
 - Some administrative TSR controls appear to be overconservative. TSR violations are declared when multiple additional controls (i.e., defense in depth) remain in place and there is no significant challenge to safety, or to the safety basis boundary.

Based on the forgoing, it appears that there have been several unnecessary declarations of TSR violations at SRS. These declarations have negative consequences in that the perception of the site and/or facility in the eyes of the public and the regulator is negatively impacted, in addition to the potential development of insensitivity to the intended significance of a TSR violation.