

Safety System Functional Failures
NUREG 1022 & ROP PI
Insights and Guidance

John Thompson

Performance Assessment Branch
Division of Inspection & Regional Support
Office of Nuclear Reactor Regulation

2009 Fall Regional Resident Inspector Counterparts Meeting

Objectives

- To provide a history of why the SSFF has been problematic and what is being done to address it.
- To identify the problematic areas and discuss a path forward.
- To provide additional insight on the current guidance.
- To discuss examples that illustrate the problems.
- Answer any questions and provide points of contact.

Key Reporting Issues

- Not risk-informed, reporting should be based on description and commitments contained in the UFSAR.
- Reportability based on conditions outlined in 50.73(a)(2)(vi).
- Use of reasonable engineering judgment is limited to assessment of whether safety function was lost due to conditions stated under 50.73(a)(2)(vi).
- Crediting use of operator actions is very limited.
- Operator error that contributes to a loss of safety function is a special case.
- Concurrent, unrelated failures in different safety systems may count as an SSFF when the safety function is lost.
- Loss of offsite power is reportable as a separate event; conversely LOOP scenarios, given an initiating event, must be assumed when considering reportability.

Differences Between the PI and 10 CFR 50.73 (a)(2)(v)

- Note that the LER report date (or the revised LER date) that first identifies the SSFF (with the box checked on the LER form) is the date used for the ROP SSFF PI.
- SSFFs that are identified as having occurred during past operation can be reported under 50.73(a)(2)(v) as far back as 3 years from the date of discovery (i.e., this was a new requirement when Revision 2 was issued for NUREG 1022.) See pages 14 and 53.
- If an SSFF was not reported in the original LER, the licensee must revise the LER to check the box for (a)(2)(v) to start the clock for ROP SSFF PI reporting purposes.

50.73(a)(2)(v) Not Risk-Informed

- Systems within scope of the rule are systems that are described by the UFSAR that have a safety function.
- TS-related systems are included within scope of the rule.
- Scoping can include HELB, Appendix R, EQ, and other design issues if their deficiency/degradation impact the safety function.
- Some licensees are using risk arguments to justify that there was no loss of safety function. These risk arguments should not be the basis for excluding an SSFF from being reported.
- Loss of function under (a)(2)(v) is not necessarily a loss of PRA function. It is a loss of function as described by the UFSAR that is needed to satisfy A-D of the rule.

50.73(a)(2)(v) is Based on Loss of UFSAR Safety Function

- Reportability is based on TS **inoperability** of a safety system caused by one or more personnel errors, failures, design/analysis, fabrication, construction, and/or procedural inadequacies that result in loss of UFSAR safety function (see 50.73(a)(2)(vi)).
- Use of “**reasonable**” engineering judgment is applied to assess operability (for TS systems) relative to the above that causes a loss of safety function. Non-TS systems are assessed against the design basis of the UFSAR.
- **Unavailability** is a term associated with train status and is used by MSPI and Maintenance Rule. This term is not defined for 50.73(a)(2)(v).
- Purposeful removal from service of one or more trains of a system for surveillance testing or maintenance, when done in accordance with TS, and appropriate procedures is not reportable.

Use of Engineering Judgment

- Use of engineering judgment is limited to assessing whether the conditions of 50.73(a)(2)(vi) could have, or actually did result in loss of a safety function.
- Engineering judgment is a “reasonable” expectation that a loss of safety function as defined by the UFSAR would or could occur and was caused by any combination of equipment failures, personnel errors, design, analysis, or procedural deficiencies (i.e., 50.73(a)(2)(vi)).
- Degraded conditions should be assessed for operability using IMC 9900 in lieu of GL 91-18.

Credit for Operator Actions

- Crediting operator action in accordance with Part 9900 is a temporary compensatory action to maintain or restore operability. In most cases, it would be a conscious effort on the part of a licensee to re-establish operability after equipment has already been declared inoperable (i.e. the safety function has already been lost). As a result, use of Part 9900 guidance may not alleviate the need for SSFF reporting since the safety function may have already been lost prior to compensatory measures being implemented.
- **When all train(s) are purposefully removed from service for ST or maintenance, through use of approved procedures (which are not deficient) and in accordance with TS, this does not constitute a SSFF event under 50.73(a)(2)(v).**
- Purposeful removal of a system from service may still be reportable if the licensee failed to adhere to regulatory requirements, incurred procedural (or other performance) deficiencies, and/or operator errors. These examples should be handled on a case-by-case basis and should involve discussion with the program office.

Operator Error that Contributes to a Loss of Safety Function is a Special Case

- Operator error(s) that contribute to a loss of safety function are a special case of SSFF.
- When the error **effects or involves** components in more than one train or channel of a safety system, no recovery credit is given.
- The components do not have to be functionally redundant.
- An example would be operator stops the Train A pump correctly, but instead of closing the pump discharge valve in Train A, the operator closes the Train B valve.

Concurrent Unrelated Failures

- Failures that occur in different systems that result in a loss of safety function are reportable under 50.72 and 50.73(a)(2)(v).
- Failures that occur in different systems that **do not result in a loss of safety function** are not reportable under 50.73(a)(2)(v).
- NUREG 1022, rev 2, page 57, “unrelated component failures in several different systems” (generally are not reportable) is interpreted as situations that don't impact loss of safety function.
- Some licensees are confusing this statement with situations that do result in loss of safety function.

Loss of Offsite Power

- Loss of offsite power is reportable under 50.73(a)(2)(v) irrespective of the status of the emergency AC power system.
- Loss of the emergency power system (EDGs, hydro) is reportable under 50.73(a)(2)(v) irrespective of the status of the offsite power supply.
- Many events that should have been reported as SSFFs were not considered reportable because offsite power remained available.
- Loss of power should be determined at the essential switchgear busses.
- Under voltage protection issues may be reportable (separately as an SSFF) if the safety function is described in the UFSAR.

Safety System Functional Failures

General Guidance for Inspectors

- NUREG 1022, rev 2 is the guidance document for compliance with the LER rule. In some instances, NEI 99-02 must be consulted for reporting the PI.
- Some specific guidance differences are contained in NEI 99-02 in the clarifying notes on pages 26 & 27.
- Note that NEI 99-02 SSFF guidance requires licensees to evaluate 50.73(a)(2)(i), or (ii), or (vii) reporting (i.e., TS deviation, seriously degraded conditions, common cause situations) against (a)(2)(v).
- Resolving 50.73(a)(2)(v) compliance is handled through the inspection program, not the FAQ process.

Safety System Functional Failures

General Guidance for Inspectors

- Plant conditions under design basis accident scenarios have to be assumed when evaluating the event or discovered condition, unless otherwise addressed in the guidance.
- Additional single failures do not need to be considered.
- Questions concerning SSFF reporting should be in consultation with IRIB (Aron Lewin, lead for NUREG 1022) or IPAB (Steve Vaughn, lead for the ROP PI Program).

Example 1a

During surveillance testing activities on ECCS Train A, the licensee uses a dedicated operator with approved procedures to compensate for the inoperability of Train A during the ST. Meanwhile, ECCS Train B experienced a demand failure that rendered the auto-start function unavailable, leaving both trains inoperable. TS 3.0.3 was entered as a result of the dual train inoperability.

This is an SSFF because:

1. Loss of the second train (un-intentional TS 3.0.3 entry) due to the discovered condition constituted a loss of function that could have prevented the system from performing its safety function.
2. No credit for recovery can be considered for reporting under this provision once loss of function has occurred.

Example 1b

With Train A inoperable due to a failed surveillance test, the licensee removed Train B from service to conduct a test. This action placed the plant in TS 3.0.3. Train B completed the test without incident and is restored to operable status.

This is not an SSFF because:

1. The licensee purposefully entered TS 3.0.3 with removal of an “operable” train that was not degraded at the time of inoperability.
2. The licensee used approved procedures and were in compliance with their TS, with no other discovered conditions that would have rendered Train B not capable of performing its safety function.

Example 2

Some plant designs do not require certain ECCS equipment to be declared inoperable when its associated EDG is inoperable. However, if there is a problem with the other ECCS train that results in it being inoperable, TS usually requires both ECCS trains to be declared inoperable, with typical TS 3.0.3 entry.

Although TS inoperability is not the sole basis for SSFF reporting (i.e., if the system can still meet FSAR assumptions), some licensees who provide an explanation of why the event was not reportable as an SSFF inappropriately take into account:

- 1) length of time both ECCS trains were inoperable (i.e., length of time is irrelevant).
- 2) If the licensee managed to exit TS 3.0.3 and avoid a plant shutdown.
- 3) credit simple operator recovery actions to maintain availability.

Example 3

Operators identified that Train “A” ESW had been in a faulted condition for 30 days and rendered inoperable due to a relay failure that had occurred during the last month’s ST. ESW provides heat removal to the RHR system. During day 29, the “B” LPI pump was in a quarterly ST that rendered the pump unavailable for two hours. Upon completion of the ST, operators later realized that the “A” LPI had been impacted by the loss of Train “A” ESW. The licensee reasoned that the “A” LPI could still perform its function for the first 30 minutes before heat removal by the RHR system would no longer meet FSAR accident assumptions.

This event constitutes an SSFF because unintentional entry into TS 3.0.3 (and where the function was lost) caused by examples listed under 50.73(a)(2)(vi) is not recoverable by operator actions.

Situations where inoperability doesn’t immediately result in a situation that is not in compliance with assumptions in the UFSAR doesn’t mean the condition is not an SSFF.

Example 4

Operators identified that both trains of safety injection and/or both charging trains could be rendered inoperable due to a common suction void in the piping, depending on what system would receive a start demand. No SSFF was identified because the licensee reasoned that various combinations of safety injection and charging pumps together could have fulfilled the safety function. The licensee did declare both trains of safety injection inoperable.

This event should be reported as an SSFF because during a DBA, safety injection would attempt to perform its function. Further, the event is reportable regardless of whether or not an alternate safety system could have been used to perform the safety function (NUREG 1022, rev 2, page 53).

Example 5

The licensee identified that the Train “A” for the control room air conditioning system was inoperable (and not capable of performing its safety function) for a 3 month period due to an equipment problem. This deficiency was not realized at the time. Over the course of these 3 months, the “B” Train had been removed from service several times for up to 20 hours of unavailability at one time. The licensee did not report this event as an SSFF because they stated the safety function remained intact by crediting operator actions to restore the “B” Train within a 4 hour period if it was needed.

This event should be reported as an SSFF because:

1. The licensee lacked situational awareness of the status of the safety system.
2. Applying credit for operator action in accordance with IMC 9900 would not have restored operability to the B Train, therefore credit does not apply.

Example 6

During operator rounds, a HELB barrier door was found open. This resulted in both divisions of 4 kv switchgear to be declared inoperable due to flooding concerns. Severe flooding would cause a loss of offsite power to both divisions of switchgear. Licensee did not consider this event as an SSFF due to the availability of the EDGs to supply power to maintain at least one division of switchgear.

Although this event is not reportable under the LOOP criterion, both divisions of switchgear could not perform their function. Per NUREG 1022, no credit should be given to an alternate safety system (i.e., EDGs) to restore the safety function. Some licensees are erroneously relying on an alternate safety system (i.e., EDGs) to maintain the safety function intact.

Example 7

In order to conduct a ST or some other evolution, the licensee intentionally removes the capability of a system to perform its intended safety function (e.g., disable auto-start on ESFAS signal). However, the status of all trains in the system is known prior to the evolution (i.e. all trains operable, one train inoperable, etc.)

The event is not reportable if:

- no adverse conditions are discovered, and
- the evolution is conducted in accordance with an approved procedure and the TS.

If an argument can be made that the procedure was deficient (i.e. should not have been in place or authorized, etc.), then an argument can be made that the events are reportable. The determination as to whether or not a procedure is deficient would currently need to be assessed under rules and criterion outside of 50.72 and 50.73.