NUCLEAR ENERGY INSTITUTE

Peter LeBlond
NEI 96-07 Appendix D Team
Nuclear Energy Institute

October 11, 2017

ILLUSTRATIONS FOR ADDRESSING 10 CFR 50.59 CRITERION 6 "DIFFERENT RESULT"

PURPOSE TODAY

Illustrate the meaning of “create a possibility of a different result” used within 10 CFR 50.59 criterion 6:

1. Review the conclusions of August 1, 2017 NEI/NRC public meeting.
2. Illustrate the application of Criterion 6 for a non-digital example.
3. Extend the illustration in #2 above to a variety of digital-related applications.

OUTLINE FOR TODAY

- Brief review of major conclusions from August 1, 2017, NEI/NRC meeting
  - Involved sequential application of definitions from NEI 96-07, Revision 1, endorsed in Regulatory Guide 1.187
- A non-digital modification to the jacket water surge tank level control system will be described
  - The approach required to answer Criterion 6 will be illustrated in detail
  - The definitions cited above will be utilized

OUTLINE FOR TODAY
CONT.

- The framework established will be applied to a closely-related digital modification
- This framework will be graphically summarized to aid in evaluating any modification
- Additional examples may be presented in an overview fashion

CONCLUSIONS FROM 8/1/2017

- Questions being posed today are not new issues
  - These questions were among the 24 separate issues that were eventually resolved by issuance of the current regulation
- The issues were fundamentally resolved by focusing on functions, not UFSAR descriptions
  - Definition of “facility” and “change” established the required regulatory foundation
- The presentation did not describe a new regulatory position
  - Simply applied existing regulatory definitions

NEI

SUMMARY OF
AUGUST 1, 2017 PRESENTATION

A "malfunction" is a failure to perform a Design Function

A Design Function is either:
- A Design Basis Function
- Supports or impacts a Design Basis Function

A Design Basis Function is:
- Credited in the safety analysis
- Defined in Regulatory Guide 1.186

Regulatory Guide 1.186 states that Design Basis Functions are:
- Linked to GDCs
- Functionally far above individual SSCs
- Safety Analyses provide context

The safety analysis is distinct from descriptive material as defined in 10 CFR 50.34(b).

All of the information on this slide is directly quoted from approved Regulatory Guides or the regulation itself.

Non-Digital Example

Manual D/G Jacket Water Surge Tank Level Control to Automatic

Description of Change:

The current Manual Control of EDG Jacket Water Surge Tank Level is being replaced with pneumatic controller and air-operated valves.

UFSAR Content:

- Chapter 15 contains a standard set of safety analyses that assume single failure. (One train operates)
- The D/G's ability to supply the required emergency loads is described.
- The surge tank is described as having a manual-operated supply and drain, along with various alarms and a high temperature EDG trip.

FUNCTIONAL LEVELS INVOLVED

Safety Analyses:

- Credits the availability of AC power
- Assume a single failure

- Credits the DBF.
- **Evaluates the EDG's Malfunction** (Failure of one train.)

The Emergency Diesel System shall be capable of automatically starting and have sufficient capacity to provide AC power to the emergency buses to power the required emergency loads…

EDG Design Basis Function from RG 1.186 based upon GDC 17. Each site's language may vary slightly.

Surge Tank Itself
Surge Tank Level Control

Part of "facility" because of "design and performance requirements…"
Performs a Design Function because:

- Supports or impacts…
- Credited in the safety analyses

ANSWERING CRITERION 6

- Create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the final safety analysis report (as updated);
- Two pieces to the criterion
  - Malfunction of an SSC important to safety with a different result than any previously evaluated in the final safety analysis report (as updated);
  - Create a possibility

➢ Malfunction previously evaluated…

➢Create a possibility

- NEI 96-07, definition 3.9 results in identification of the single failure-based safety analysis
  - Has the single failure assumption (one train operates) become invalid due to cross-connection, installation of common devices, etc.?
  - The postulated presence of lower level UFSAR descriptions of possible reliance on alarms does not alter this conclusion.
- Hardware Common Cause Failure is not credible
- Criterion 6 answer would be “No”

Digital Example

Manual D/G Jacket Water Surge Tank Level Control to Automatic

Description of Change:

The current Manual Control of EDG Jacket Water Surge Tank Level is being replaced with **digital controllers** and air-operated valves.

UFSAR Content:

- No change from Non-digital Example.

Technical Information:

- The low level alarm actuates at 200 gallons remaining in a 450 gallon surge tank.
- The drain line averages 5 GPM.

No Change in Functional Levels Involved

Safety Analyses:

- Credit the availability of AC power
- Assume a single failure

- Credits the DBF.
- **Evaluates the EDG's Malfunction** (Failure of one train.)

The Emergency Diesel System shall be capable of automatically starting and have sufficient capacity to provide AC power to the emergency buses to power the required emergency loads…

EDG Design Basis Function from RG 1.186 based upon GDC 17. Each site's language may vary slightly.

Surge Tank Itself
Surge Tank Level Control

Part of "facility" because of "design and performance requirements…"
Performs a Design Function because:

- Supports or impacts…
- Credited in the safety analyses

NEI

CRITERION 6 IS UNCHANGED

- Create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the final safety analysis report (as updated);
- Two pieces to the criterion
  - Malfunction of an SSC important to safety with a different result than any previously evaluated in the final safety analysis report (as updated);
  - Create a possibility

➢ Malfunction previously evaluated…
➢ Create a possibility

- Software Common Cause Failure likelihood is not sufficiently low
  - Illustration for today's discussion
- NEI 96-07, definition 3.9 results in identification of the single failure-based safety analysis
  - Has the single failure assumption (one train operates) become invalid due to the SCCF?
  - We cannot simply rely on the previous absence of cross-connections.
- A "New FMEA" is needed to determine if the SCCF will propagate to the higher functional level

NEI

USE OF FMEAs

- Use of the acronym “FMEA” within NEI 96-07
  - Does not refer to any IEEE standard
  - No guidance regarding content or structure was developed in 1997-1999
    - Their use is discussed in NPRM, SOC, and NEI 96-07
  - Might be summarized with “What will happen when the failure occurs?”
- NEI Task Force Discussions have resulted in a simplistic format for FMEAs
  - **Presumes compliance with pre-existing procedures and any “interdependent,” modification-related procedures**

GENERATION OF AN FMEA FOR THE EDG SURGE TANK CONTROLLER

- Procedures already exist for:
  - Local operator monitoring of EDG operation
  - Response to Low Surge Tank Level alarms
    - MCR Trouble alarm typically points to a Local Panel
  - Operator manipulation of surge tank supply and drain valves
    - These will be modified due to new reliance upon automatic level control

GENERATION OF AN FMEA FOR THE EDG SURGE TANK CONTROLLER CONT.

- In this situation, 40 minutes (200 gallons being drained at 5 GPM) are available after alarm generation.
- Operator complies with procedural guidance
- Surge Tank Function is preserved
- Answer to Criterion 6 is “No”

- Summarize the overall approach by revisiting the “Functional Level” slide

SUMMARY OF EVALUATION

Safety Analyses:

- Credit the availability of AC power
- Assume a single failure

- No change in the Evaluation of the EDG's "Malfunction"
- Results remain the same

The Emergency Diesel System shall be capable of automatically starting and have sufficient capacity to provide AC power to the emergency buses to power the required emergency loads…

- Effect of SCCF will be manifest over a period of time.
- Procedure compliance will detect and respond to SCCF and preserve the DBF.

Surge Tank Itself
Surge Tank Level Control

- SCCF is:
  - ➢classed as "create a possibility."
  - ➢Induces effects across trains
  - ➢FMEA is needed

NEI

STANDARDIZED APPROACH CAN BE GRAPHICALLY EXPRESSED

- The previous slide can be generalized to describe this approach

Graphical Summary of Approach

Identify all Safety Analyses that credit directly or indirectly the DBF identified below.

(If no Safety Analysis apparently exists, specialized evaluations may be required.)

- Do all assumptions remain valid?
- Does the Safety Analysis remain valid?

Identify the DBF(s) involved and classify its relationship with the identified functions below using NEI 96-07, definition 3.3.

(If no DBF apparently exists, specialized evaluations may be required.)

- Is the DBF preserved?
- Was a FMEA needed to assess the propagation of effects?

- Describe the activity
- Identify **any functions** involved

- Determine if SCCF:

➢Is classed as "create a possibility."

➢Induces effects across trains

➢FMEA is needed?

NEI

CONCLUSION

- The graphical summary introduced on slide #8 is entirely based upon unambiguous use of approved definitions.
- The characteristics of an FMEA developed for 10 CFR 50.59 use was introduced on slide #15
  - This guidance is not from NEI 96-07.
  - Reflects a basic requirement that personnel will follow their procedures.
- The graphical summary of the overall approach was introduced on slide #20
  - May be used to guide personnel in future Evaluations
  - Task Force Members are prepared to discuss any example utilizing that graphical approach.

This Functional Level provides the Evaluation of the D/G's "Malfunction"

- NPRM states:

  However, the Commission recognizes that in its reviews, equipment malfunctions are generally postulated as potential single failures to evaluate plant performance; thus, the focus of the NRC review was on the result, rather than the cause/type of malfunction. Unless the equipment would fail in a way not already evaluated in the safety analysis, there is no need for NRC review of the change that led to the new type of malfunction.

This Functional Level provides the Evaluation of the D/G's "Malfunction"

- NEI 96-07, section 4.3.6 states:

  Malfunctions of SSCs are generally postulated as potential single failures to evaluate plant performance with the focus being on the result of the malfunction rather than the cause or type of malfunction.

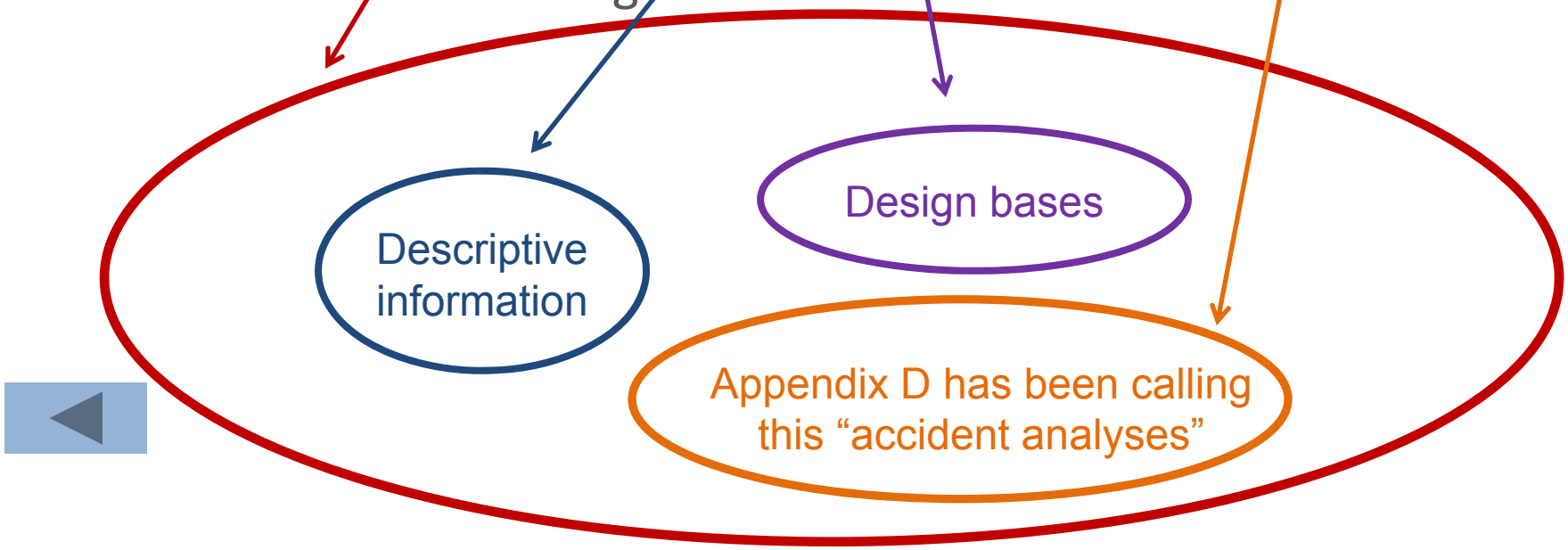
Definition 3.3 from NEI 96-07

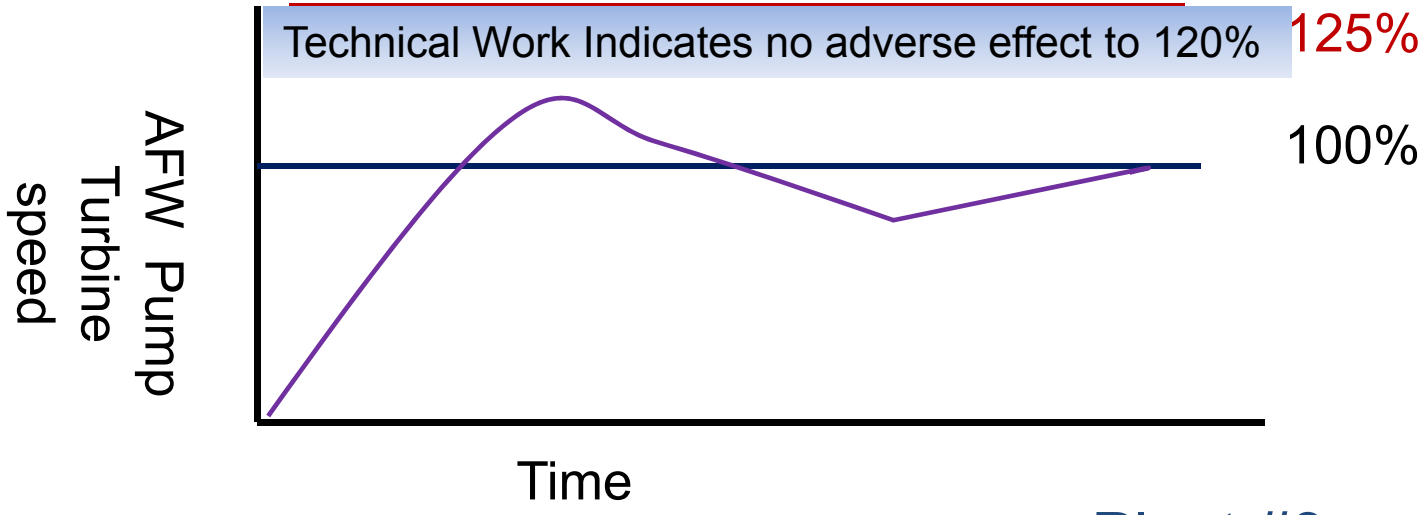
As used above, **"credited in the safety analyses"** means that, if the SSC were not to perform its design bases function in the manner described, the assumed initial conditions, mitigative actions or other information in the analyses would no longer be within the range evaluated **(i.e., the analysis results would be called into question).** The phrase "support or impact design bases functions" refers both to **those SSCs needed to support design bases functions (cooling, power, environmental control, etc.)** and to SSCs whose operation or malfunction could adversely affect the performance of design bases functions (for instance, control systems and physical arrangements). Thus, both safety-related and nonsafety-related SSCs may perform design functions.

FSAR-RELATED TERMINOLOGY

FROM 10 CFR 50.34b

Final safety analysis report. Each application for an operating license shall include a **final safety analysis report**. The final safety analysis report shall include **information that describes the facility**, **presents the design bases and the limits on its operation**, and **presents a safety analysis of the structures, systems, and components and of the facility as a whole**, and shall include the following:





Plant #1
UFSAR is 7 Volumes

Plant #2
UFSAR is 12 Volumes

Plant #3
UFSAR is 17 Volumes

The Design Function is on the bottom line.

The requirement to update the UFSAR is unrelated to the screening decision.

120%
125%

Overspeed trip exists

Overspeed trip exists

Pump works to remove heat
Delivers flow when required

Pump works to remove heat
Delivers flow when required

Pump works to remove heat
Delivers flow when required

NPRM Discussion of "FMEAs"

The staff **has provided guidance on this issue in Generic Letter (GL) 95–02**, concerning replacement of analog systems with digital instrumentation. The GL states that in considering whether new types of failures are created, this must be done at the level of equipment being replaced—not at the overall system level. Further, it is not sufficient for a licensee to state that since failure of a system or train was postulated in the SAR, any other equipment failure is bounded by this assumption, **unless there is some assurance that the mode of failure can be detected and that there are no consequential effects (electrical interference, materials interactions, etc), such that it can be reasonably concluded that the SAR analysis was truly bounding and applicable**.

SOC Also Reinforces Possible Use of "FMEA"

The proposed rule discussion further stated that this determination should be made either at the component level, or consistent with the failure modes and effects analyses (FMEA), **taking into account single failure assumptions**, and the level of the change being made. Several commenters stated that this guidance **should be revised to refer only to the failure modes and effects analysis in the FSAR, and not to specify the component level**. The Commission agrees that this criterion should be considered with respect to the FMEA, **but also notes that certain changes may require a new FMEA**, which would then need to be evaluated as to whether the effects of the malfunctions are bounding.

NEI 96-07 Repeats the SOC wording

…In evaluating a proposed activity against this criterion, the types and **results of failure modes of SSCs** that have previously been evaluated in the UFSAR and that are affected by the proposed activity should be identified. This evaluation should be performed consistent with any failure modes and effects analysis (FMEA) described in the UFSAR, **recognizing that certain proposed activities may require a new FMEA to be performed.**