WECC

Risk Assessment Concepts for Internal Controls

Harold Sherrill

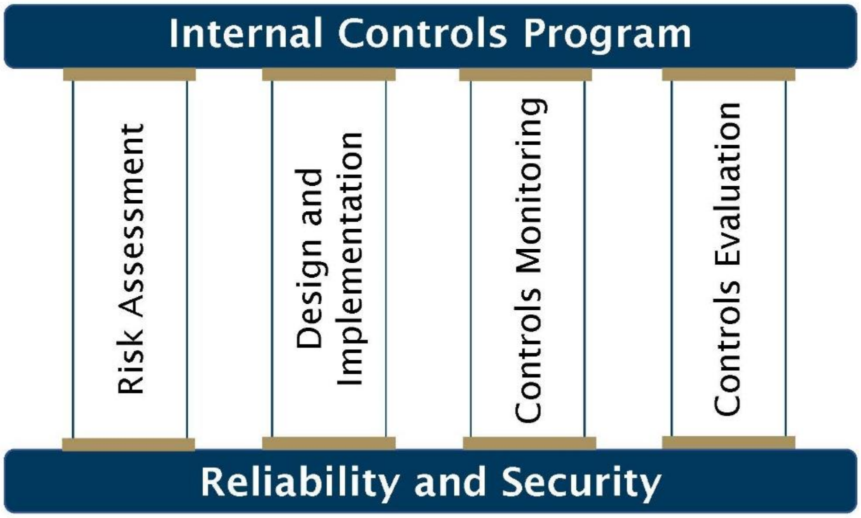
Table of Contents

Introduction

To have an effective internal controls program, you, as an entity, must define how you develop and manage the parts of your program. Specifically, you must explain how you design effective controls, consolidate processes, verify implementation, and evaluate risk. Internal controls programs are made up of four parts: Risk Assessment, Design and Implementation, Controls Monitoring, and Controls Evaluation. A good program continuously matures in all these areas.

This paper focuses on Risk Assessment.

Figure 1



Risk Assessment

Risk assessment is an organization’s approach to discovering risks to its business, governance, and operations. Organizations use risk assessment to create controls that mitigate those risks. You must evaluate the potential failure points[1] related to each requirement. When you understand the risks of your activities and processes, you can create controls that help you achieve reliability and security. The point of risk assessment is to look for all types of potential failures to get a clear picture of the risks you may face.

Risk/Controls Relationship Defined

While the primary goals of internal controls programs are reliability and security, your internal controls must also comply with controls reporting requirements. Your internal controls program

[1] Potential failure points are risks that may lead to noncompliance with NERC Reliability Standards and Requirements and, in turn, to potential risks to the bulk power system.

should include processes to develop requirement-level controls in two areas: control design and control implementation.

Control Design

Effective controls must meet the following requirements:

- Design your controls to meet risk objectives (e.g., potential failure points);
- Document your controls in formal processes and procedures to promote consistent performance of control activities; and
- Create documentation that describes control activities in enough detail to enable you to monitor and evaluate internal controls.

The more detailed you are in assessing risks, the more effective your controls design will be. General, high-level risk identification makes it difficult to see gaps in controls at the activity and process levels. You should document your risk in enough detail to allow for effective controls design.

Control Implementation

Once you have identified the risks and mapped existing controls to them, you must make sure that the controls are working (i.e., mitigating risks).

Implemented controls must meet the following requirements:

- See it in operation and confirm that it mitigates risk as designed; and
- Apply activities or processes that cover all the identified risks.

The better your controls cover the risks, the more "in control" you can consider your process. When identifying risks, keep in mind that your goal is to prevent failures; essentially making your processes "mistake proof."

Mistake-Proofing

Mistake-proofing is about *awareness, detection,* and *prevention* of mistakes that adversely affect process outcomes (i.e., reliability and security) and compliance.

- **Awareness** means communicating the potential for mistakes and designing the process to detect or prevent mistakes.
- **Detection** means allowing the mistake to happen but providing a way to uncover the mistake.
- **Prevention** means keeping process mistakes from occurring.

Risk Identification

The key to creating a successful controls program is understanding risks. In the utility sector and throughout the Interconnection, entities use different methods to identify areas of risk. Unfortunately, these methods are usually reactionary, relying on the industry's past performance, instead of being proactive and preventative. It is important to consider *potential* failure points; otherwise, risk identification is just a representation of past process failures.

Process Failure Mode Evaluation and Analysis (PFMEA) is a tool to help with risk assessment. In PFMEA, the first step is to brainstorm the "ways" in which a process can fail. After listing as many "ways" as possible, the next step is to list possible "causes" for the failures. When you apply this concept to the requirement-specific language of the NERC Standards, you can more easily see the risks that come from failing to meet the Standard or requirement. In essence, you get an activity- and process-level risk assessment.

Once you have identified activity- and process-level risks, you can assess how your controls mitigate those low-level risks. The benefit of using PFMEA is that the process can show risk not yet realized by you or the industry. This is a proactive approach designed to *prevent* process failures, not just react to them.

Assurance is based on adequately identifying and mitigating risk. In the case of the utility sector, consider possible failure points that might lead to a reliability event or noncompliance with a Standard.

You do not need to identify *all* possible failure points during this process. The goal is to get a reasonable assurance, not an absolute assurance, that you will meet the control objective. The list of potential failure points may grow over time as the process matures and you discover more risks.

Application of PFMEA in Identifying Risk

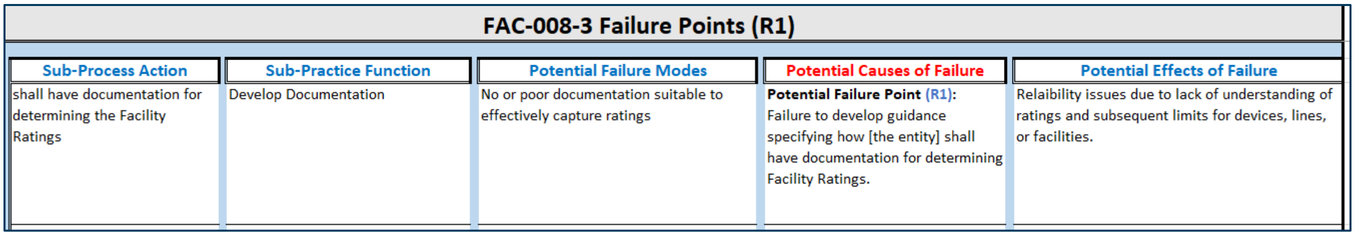
The following example shows the steps in the PFMEA process. Use these steps to identify risks related to specific reliability requirements. In this process, we consider the language in FAC-008-3 R1, which states:

> Each Generator Owner shall have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main step up transformer if the Generator Owner does not own the main step up transformer and the high side terminals of the main step up transformer if the Generator Owner owns the main step up transformer.

In this example, we use only part of the language of the requirement. The part we will use is a call to action or "Sub-Process Action" for the entity to achieve a sub-process objective of "have documentation". This objective is established by the clause, "…shall have documentation for determining the Facility Ratings."

Begin by using the clause "…shall have documentation for determining the Facility Ratings" in the steps below to produce a result in the Potential Causes of Failure column. This column is the possible risk for not achieving the objective in the Sub-Process Action column.

Figure 2



FAC-008-3 Failure Points (R1)

Sub-Process Action	Sub-Practice Function	Potential Failure Modes	Potential Causes of Failure	Potential Effects of Failure
shall have documentation for determining the Facility Ratings	Develop Documentation	No or poor documentation suitable to effectively capture ratings	**Potential Failure Point** (R1): Failure to develop guidance specifying how [the entity] shall have documentation for determining Facility Ratings.	Relaibility issues due to lack of understanding of ratings and subsequent limits for devices, lines, or facilities.

Step 1) Create an action statement from the language of the requirement and place it in the Sub-Process Action column. For instance, "…shall have documentation for determining the Facility Ratings"

Step 2) Determine what the requirement is asking you to do. In this example, you are required to document how you determine facility ratings. So, the Sub-Practice Function is to "develop documentation."

Step 3) Detail the "way" in which you might fail to meet the requirement in the Potential Failure Mode column. In this example, you might fail by having "No or poor documentation suitable to effectively capture ratings."

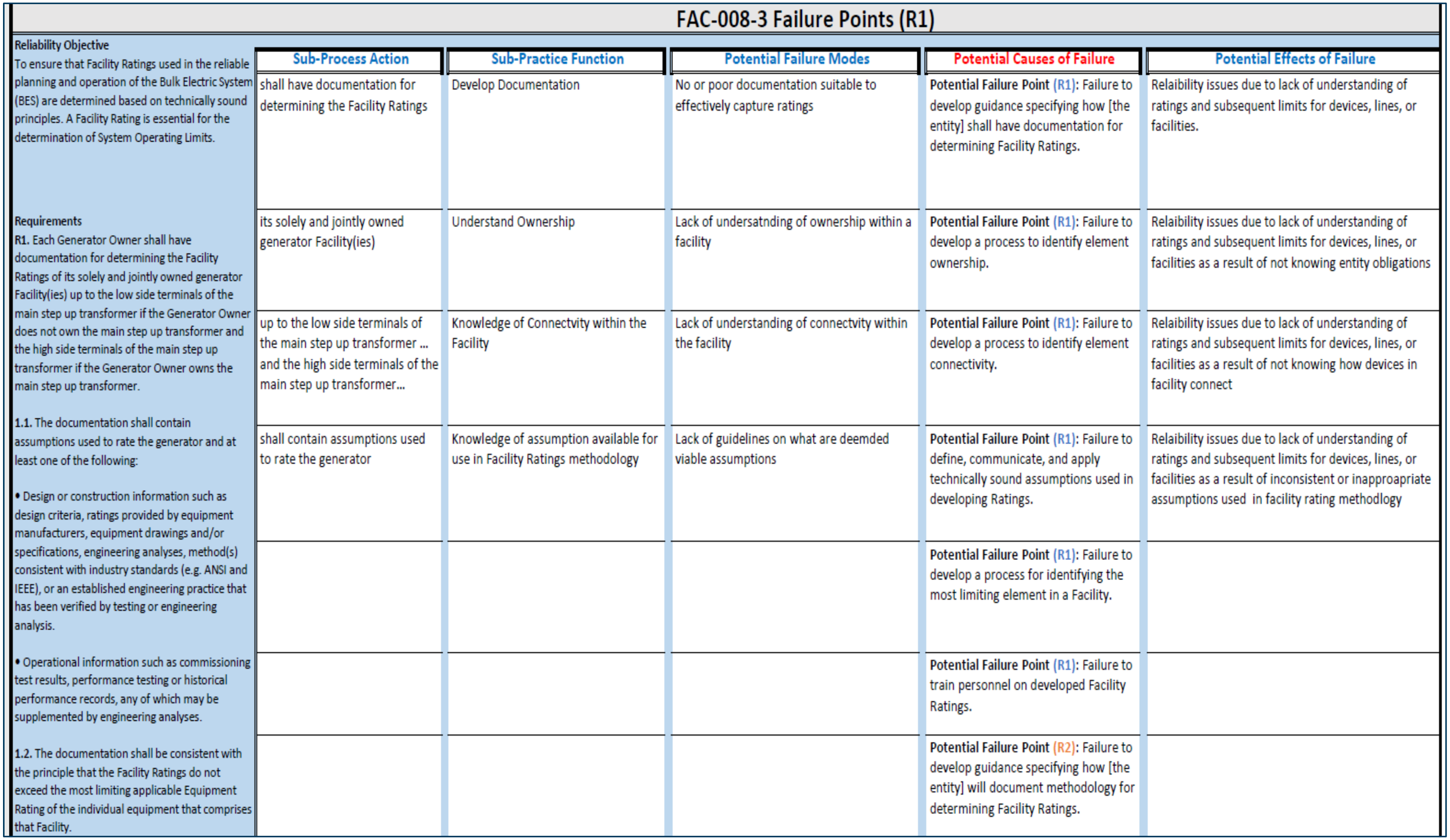
Step 4) Now find the "cause" of this potential failure**.** One cause might be that you did not include guidance on how exactly you will produce and maintain documentation. In this example, the Potential Causes of Failure might be "Failure to develop guidance specifying how [the entity] shall have documentation for determining Facility Ratings."

Step 5) Finally, you must state the "effect" if you fail to mitigate the Potential Causes of Failure. In this example, the effect statement might be "Reliability issues due to lack of understanding of facility ratings and subsequent limits for devices, lines, and facilities."

Conclusion

Effective internal controls that prevent, detect, or correct noncompliance give reasonable assurance to WECC that an entity will comply with the Reliability Standards. Concepts taken from existing quality management and internal controls frameworks, like "mistake-proofing" and PFMEA, can aid in doing a complete, process-level risk assessment that reveals potential failure points. After identifying the potential failure points, the entity can address risk by designing and implementing effective internal controls.

Appendix A



FAC-008-3 Failure Points (R1)

	Sub-Process Action	Sub-Practice Function	Potential Failure Modes	Potential Causes of Failure	Potential Effects of Failure
Reliability Objective To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on technically sound principles. A Facility Rating is essential for the determination of System Operating Limits. **Requirements** **R1.** Each Generator Owner shall have documentation for determining the Facility Ratings of its solely and jointly owned generator Facility(ies) up to the low side terminals of the main step up transformer if the Generator Owner does not own the main step up transformer and the high side terminals of the main step up transformer if the Generator Owner owns the main step up transformer. **1.1.** The documentation shall contain assumptions used to rate the generator and at least one of the following: • Design or construction information such as design criteria, ratings provided by equipment manufacturers, equipment drawings and/or specifications, engineering analyses, method(s) consistent with industry standards (e.g. ANSI and IEEE), or an established engineering practice that has been verified by testing or engineering analysis. • Operational information such as commissioning test results, performance testing or historical performance records, any of which may be supplemented by engineering analyses. **1.2.** The documentation shall be consistent with the principle that the Facility Ratings do not exceed the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.	shall have documentation for determining the Facility Ratings	Develop Documentation	No or poor documentation suitable to effectively capture ratings	**Potential Failure Point** (R1): Failure to develop guidance specifying how [the entity] shall have documentation for determining Facility Ratings.	Relaibility issues due to lack of understanding of ratings and subsequent limits for devices, lines, or facilities.
	its solely and jointly owned generator Facility(ies)	Understand Ownership	Lack of undersatnding of ownership within a facility	**Potential Failure Point** (R1): Failure to develop a process to identify element ownership.	Relaibility issues due to lack of understanding of ratings and subsequent limits for devices, lines, or facilities as a result of not knowing entity obligations
	up to the low side terminals of the main step up transformer ... and the high side terminals of the main step up transformer...	Knowledge of Connectvity within the Facility	Lack of understanding of connectvity within the facility	**Potential Failure Point** (R1): Failure to develop a process to identify element connectivity.	Relaibility issues due to lack of understanding of ratings and subsequent limits for devices, lines, or facilities as a result of not knowing how devices in facility connect
	shall contain assumptions used to rate the generator	Knowledge of assumption available for use in Facility Ratings methodology	Lack of guidelines on what are deemded viable assumptions	**Potential Failure Point** (R1): Failure to define, communicate, and apply technically sound assumptions used in developing Ratings.	Relaibility issues due to lack of understanding of ratings and subsequent limits for devices, lines, or facilities as a result of inconsistent or inappropraite assumptions used in facility rating methodlogy
				Potential Failure Point (R1): Failure to develop a process for identifying the most limiting element in a Facility.	
				Potential Failure Point (R1): Failure to train personnel on developed Facility Ratings.	
				Potential Failure Point (R2): Failure to develop guidance specifying how [the entity] will document methodology for determining Facility Ratings.	