WESTINGHOUSE ELECTRIC COMPANY LLC

Document Number	Revision	Total No. Pages
STD-AR-07-2	3	68

Title: Emergency Response Guideline Development

Author(s) Name(s)	Signature / Date	For Pages
Dr. G. D. Storrick, P.E.	[Electronic Approval in EDMS]	ALL
Reviewer(s) Name(s)	**Signature / Date**	**For Pages**
Dr. A. Maioli	[Electronic Approval in EDMS]	ALL
Manager Name	**Signature / Date**	**For Pages**
Dr. M.D. Carelli	[Electronic Approval in EDMS]	ALL

REVISION HISTORY

Revision Number	Changes	Date
0	Report Created	1/2007
1	Added Emergency Response Details	3/2007
2	Added Emergency Response Details	6/2007
3	Final Report	9/2007

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1. INTRODUCTION

1.1. OVERVIEW

Task five of the collaborative effort between ORNL, Brazil, and Westinghouse for the International Nuclear Energy Research Initiative entitled "Development of Advanced Instrumentation and Control for an Integrated Primary System Reactor" focuses on operator control and protection system interaction, with particular emphasis on developing emergency response guidelines (ERGs). As in the earlier tasks, we will use the IRIS plant as a specific example of an integrated primary system reactor (IPSR) design. The present state of the IRIS plant design – specifically, the lack of a detailed secondary system design – precludes establishing detailed emergency procedures at this time; however, we can create a structure for their eventual development.

This report summarizes our progress to date. Section 1.2 describes the scope of this effort. Section 2 compares IPSR ERG development to the recent AP1000 effort, and identifies three key plant differences that affect the ERGs and control room designs. The next three sections investigate these differences in more detail. Section 3 reviews the IRIS Safety-by-Design™ philosophy and its impact on the ERGs. Section 4 looks at differences between the IRIS and traditional loop PWR I&C Systems, and considers their implications for both control room design and ERG development. Section 5 examines the implications of having one operating staff control multiple reactor units. Section 6 provides sample IRIS emergency operating procedures (EOPs). Section 7 summarizes our conclusions.

1.2. SCOPE

The INERI contract scope of work task description for task 5, "operator control and protection system interaction," is as follows:

> "Task Description
>
> > "IPSRs are being designed as "hands-off" plants, with the control and protection systems designed to respond to all anticipated and accidental conditions postulated to occur during the plant lifetime. The main difference to current plants is that the operator will not be "required" to perform any function for the plant to initiate the automatic mitigation features. However, operator actions may improve the plant response, and a close monitoring of the plant systems operation will be vital to give the operator the option to take manual actions should the plant systems not perform as designed. Therefore, operator actions are credited in the plant

probabilistic safety assessment, and the Human Reliability Analysis (HRA) is a critical component of the overall plant safety for IPSRs.

"The differences in design characteristics and overall design philosophy between IPSRs and current LWRs makes the direct application of current LWR control room design features and emergency procedures guidelines (EPGs), the two being strongly connected, not optimal for IPSRs designs. The objective of this task is to develop a novel approach for IPSR control room design and emergency procedure guidelines development."

The following section taken from the original proposal (Reference 1) provides additional insight into the original intent of this task:

"Operator interaction with control and protection systems

"Part of this program aims at developing a methodology for defining both the plant emergency procedures and control room design issues at the design stage, using the Human Reliability Analysis developed for the probabilistic safety assessment. The methodology can make use of a recursive approach, which has a strong impact on HRA as well: every time new information about EPGs and Control Room design features are assumed, HRA results are updated and revised. This activity will be an important step in any new reactor development since a methodology able to define adequate emergency procedure guidance and Control Room features at an early design stage could be generally applicable. Thus, the EPGs, which will adopt a symptomatic approach common to other LWRs in the post-TMI environment, will be developed concurrently with the definition of the control room design, using the HRA as a common base. The plant emergency procedure guidelines will be developed using IRIS as a practical case study. Control Room requirements specific to IPSRs will be an explicit issue within this program. Although a complete design of the control room goes well beyond the scope of this program, a set of functional requirements for the control room will be developed. The overall process will provide the technical community with a possible approach for optimizing the operator interaction with the plant for advanced reactor concepts that present significant differences from the existing LWRs."

The second year of the project focused on “establishing the main features of the EPGs and the control room for IPSRs, with particular emphasis on identifying differences and similarities with existing PWRs. The deliverable is a status report on the progress of this task at the end of the second year.” Revision 0 of this report serves as that deliverable. This year’s effort was to complete “the EPGs and control room characterization for IPSRs, including functional requirements, high level conceptual design, and design approach.” This revision provides the additional information.

2. EMERGENCY RESPONSE GUIDELINE DEVELOPMENT

The recent ERG development effort for the AP1000 provides a view of the current state of the art. Reference 2 summarizes the AP1000 process as follows:

> "The Emergency Response Guidelines (ERGs) have been developed for the AP1000. The generic ERGs for the low pressure[1] reference PWR plant were used as the basic documents to develop the AP1000 ERGs. The AP1000 design differences from the reference plant were reviewed and reflected in the process of developing operational steps in each ERG. The AP1000 used PRA[2] in both design and licensing. The provisions of the AP1000 PRA were also reviewed and incorporated into the ERGs.
>
> "Although the AP1000 design does not require operator action for the first 72 hours after accidents, the operator actions with both safety-related and nonsafety-related equipment have an important role to mitigate the consequences of accidents."

Although the AP1000 featured passive safety systems while the reference plant did not, Reference 2 established functional correspondences between the AP1000 and reference plant systems. This had a significant effect on the AP1000 ERG development process; specifically, reference 2 included the following observation:

> "Based on the comparison of the reference plant systems and the AP1000 systems, the plants have similar functions, although in several cases the functions are performed by different systems. Since the reference plant and the AP1000 have similar basic system functions, the basic framework and recovery strategies contained in the reference plant ERGs generally apply to the AP1000."

The AP1000 ERG development process was an evolutionary one rather than a revolutionary one in the sense that the AP1000 ERGs relied heavily on those developed for the reference plant. Since most IPSRs in general (and IRIS specifically) are pressurized water reactors featuring passive safety systems, we might consider using the AP1000 as a reference plant for developing ERGs; however, the differences between IPSRs and AP1000 are greater than those between AP1000 and its reference plant. The weaker correspondence could

---

[1] In this context, "low pressure" means that the shutoff head of the reference plant's safety injection system was lower than the normal primary system operating pressure. This term does not apply to either the AP1000 or the IRIS designs.

[2] PRA=probabilistic risk assessment.

require different recovery strategies for IPSRs, and perhaps even a different framework for presenting these strategies.

In this paper, we use IRIS as a representative IPSR. IRIS employs a unique Safety-by-Design™ approach that makes it the most advanced of the current IPSR designs. Some of IRIS' characteristics are proprietary, but there is sufficient information available in the public domain to explore the design impacts on the ERGs. Here we consider the following three major differences between IRIS and AP1000:

1. IRIS uses "a '[S]afety-by-[D]esign[™]' approach, which physically eliminates some accident sequences (e.g., large LOCA) and reduces the probability of occurrence or consequences of other serious design basis accidents. The IRIS safety-by-design approach can eliminate or reduce the probability or consequences of ANS 18.2 [Reference 3] design basis accidents" (Reference 4, p. 1-9).

2. IRIS features a hierarchical control system with a supervisory controller that oversees primary and secondary plant operations (much like the Temelín plant), while the AP1000 will use a flat control architecture similar to the one used on traditional Westinghouse PWRs.

3. The vision for IRIS is for more than just a single-unit electric power generating station: it includes an expectation for multiple units on one site. Our vision for the IRIS control room is that barring regulatory or labor requirements to the contrary, one control room operating staff should be able to control multiple IRIS units.

The vision for IRIS includes the possibility of coupling the plant with desalination, district heating, and industrial steam co-generation modules. Although this would require appropriate adjustments to the plant's normal operating procedures, we foresee little impact on the nuclear ERGs.

3. COMPARISON OF IRIS AND AP1000 DESIGN-BASIS EVENTS

The IRIS approach to safety focuses on achieving a design with innovative safety characteristics and multiple levels of defense for accident mitigation (defense-in-depth), resulting in extremely low core damage probabilities while minimizing the occurrences of containment flooding, pressurization, and heat-up situations.

The first line of defense in the IRIS defense-in-depth approach is to eliminate initiators that could eventually lead to core damage. This concept follows the Safety-by-Design™ approach, which involves designing the plant in such a way to prevent the accidents from occurring, rather than coping with their consequences. If it is not possible to eliminate the accidents altogether, then the design should inherently limit their consequences and/or their probability of occurring. The key difference from previous practice is that the integral reactor design is intrinsically conducive to eliminating accidents to a degree impossible in conventional loop-type reactors. The most easily visible of the safety potential characteristics of integral reactors is the elimination of the large LOCAs, since no large primary penetrations of the reactor vessel or large loop piping exist. Many others are possible by an appropriate design process that focuses on selecting the design characteristics that are most amenable to eliminating initiating events. The IRIS designers strived to achieve that focus.

Like the AP1000, the IRIS design includes multiple levels of defense for a very wide range of plant events. The IRIS design provides for defense-in-depth (i.e., multiple barriers to radiation release) along with a multitude of individual plant features capable of providing ensuring plant safety. Some features follow practices common to older reactors, others bear similarities to the AP1000 advanced designs, and some are exclusive features of IRIS. In all cases, the design goal is to always keep the core covered with water and avoid fuel damage.

The U. S. Nuclear Regulatory Commission (NRC) defines the accident analyses needed in light water reactor Safety Analysis Reports (Reference 5). The NRC made their last revision in 1978. Since there is no a-priori reason to believe that the specific accidents appropriate for 1970s-era designs remain appropriate, we reviewed the list to determine if it is necessary and sufficient for IRIS, and drew the following conclusions:

1. The traditional high-level accident classification appears to be sufficient for defining IRIS accident categories. Reference 5 defines the following categories: increase in heat removal from the primary system, decrease in heat removal by the secondary system, decrease in reactor coolant flow rate, reactivity and power distribution anomalies, increase in reactor coolant inventory,

decrease in reactor coolant inventory, and radioactivity release from a system or component.

2. The IRIS design does not appear to introduce any significant new accident categories beyond those listed item 1, but there are some new accidents to consider (e.g., inadvertent operation of the passive core cooling system during operation does not apply to traditional plants that lack this system).

3. The NRC's list of specific accidents has some hidden assumptions on the types of accidents that could result from a single failure; for example, it assumes that a single failure cannot lead to simultaneous opening of the feedwater and turbine bypass valves. The IRIS design basis should include specific requirements to ensure that any assumptions limiting the list of candidate accidents remain valid[3].

4. The IRIS design eliminates the possibility of some of the specific accidents listed in Reference 5. For example, IRIS uses shaftless reactor coolant pumps, so a reactor coolant pump shaft break cannot occur.

Table 1 illustrates how specific IRIS design features influence the plant response to traditional PWR Condition IV events. Reference 6 provides additional details, as well as similar information for condition II and III events. That document also identified "those events for which a significant difference exists in IRIS versus passive PWRs." Without repeating the details here, we found that IRIS is significantly different for the following:

1. 13 out of 20 condition II events.

2. 3 out of 10 condition III events. One of the unaffected events postulates an improperly loaded fuel assembly, and four of the remaining six involve auxiliary systems only, not the NSSS.

3. 7 of 8 condition IV events. The IRIS design eliminates three of the events. The IRIS design does not affect the design basis fuel handling accident.

Even without reviewing each event in detail, it is clear that there might be significant differences between the ERGs for IRIS and traditional passive loop-type PWRs. This likely holds for other IPSRs as well. Table 2 lists the Emergency

[3] For example, "No credible single failure shall result in simultaneous occurrence of more than one of the following: (a) sustained control rod withdrawal, (b) sustained boron dilution, (c) excessive axial offset bank withdrawal or insertion, (d) sustained opening of any turbine bypass valve, (e) sustained excessive feedwater to any feedwater line, (f) sustained excessive opening of the turbine throttle valve."

Operating Procedures (EOPs) developed for the AP1000 Simulator and then provides a preliminary assessment of how well each procedure might apply to IRIS. We can group the assessments into three broad categories:

1. For 14 out of the 34 procedures, IRIS might have similar procedures that might differ in minor details, but essentially follow the same general approach.

2. For 16 out of the 34 procedures, IRIS might have a procedure to accomplish similar goals but differences in the IRIS plant would require significantly different approaches than taken in the AP1000 procedures.

3. For 4 of the 34 procedures, the IRIS design eliminates the need for a corresponding IRIS procedure.

This breakdown is somewhat misleading, since the 17 procedures in the second category account for roughly three-quarters of the total page count in the 34 procedures, while the 13 procedures in the first category are generally quite short. We conclude that Emergency Response Guidelines and Emergency Operating Procedures for an IPSR such as IRIS would significantly differ in details from those existing for conventional loop-type PWRs.

Table 1: IRIS response to PWR Condition IV Events

#	Condition IV Design Basis Events	IRIS Design Characteristic	Results of IRIS Safety-by-Design
1	Large Break LOCA	Integral RV Layout – No loop piping	Eliminated by design
2	Steam Generator Tube Rupture	High design pressure once-through SGs, EHRS, piping, and isolation valves	Reduced consequences, simplified mitigation
3	Steam System Piping Failure	High design pressure SGs, piping, and isolation valves. SGs have small water inventory.	Reduced probability, reduced consequences (limited containment effect, limited cooldown) or eliminated (no potential for return to power)
4	Feedwater System Pipe Break	High design pressure SGs, piping, and isolation valves. Integral RV has large primary water heat capacity.	Reduced probability, reduced consequences
5	Reactor Coolant Pump Shaft Break	Spool pumps have no shaft	Eliminated by design
6	Reactor Coolant Pump Seizure	No DNB for failure of 1 out of 8 RCPs, even without Reactor Trip.	Reduced consequences
7	Spectrum of RCCA ejection accidents	With internal CRDMs there is no ejection driving force	Eliminated by design
8	Design Basis Fuel Handling Accidents	No IRIS specific design feature	No impact

Table 2: AP1000 Emergency Operation Procedures: Application to IRIS

#	Title	Summary	IRIS Implications
1	Reactor Trip or Safety Injection	This procedure provides instructions to verify proper response of the automatic protection systems following manual or automatic actuation of a reactor trip or safety injection, to assess plant conditions, and to identify the appropriate recovery procedure.	IRIS could have a similar procedure but the details would need to be quite different to reflect the differences in the Engineered Safeguard Features and protection systems.
2	Loss of Reactor or Secondary Coolant	This procedure provides instructions to recover from a loss of reactor or secondary coolant.	IRIS could have a similar procedure but the details would need to be different to reflect the differences in the fluid systems (especially on the secondary side).
3	Faulted SG Isolation	This procedure provides instructions to identify and isolate a faulted steam generator.	IRIS could have a similar procedure but the details would need to be different to reflect the differences in the steam generator designs.
4	SG Tube Rupture	This procedure provides instructions to terminate leakage of reactor coolant into the secondary system following a steam generator tube rupture (SGTR).	IRIS could have a similar procedure but the details would need to be quite different to reflect the differences in the steam generator and secondary system designs. The procedure for Faulted SG Isolation (see item 4) may be sufficient.
5	LOCA Outside Containment	This procedure provides instructions to isolate a LOCA outside containment.	IRIS could have a similar procedure.
6	Reactor Trip Response	This procedure provides instructions to stabilize and control the plant following a reactor trip without a safety injection.	IRIS could have a similar procedure.
7	Natural Circulation Cooldown	This procedure provides instructions to perform a natural circulation RCS cooldown and depressurization to cold shutdown, with no accident in progress, under requirements that will preclude any upper head void formation.	IRIS could have a procedure for natural circulation cooldown but because of differences in the primary coolant loop and in the steam generators, the details would be rather different.

#	Title	Summary	IRIS Implications
8	Passive Safety System Termination	This procedure provides instructions to terminate safety injection and stabilize plant conditions.	IRIS could have a procedure to terminate passive safety systems operations (including termination following an inadvertent actuation), but because of the differences in the passive systems, the details would be quite different.
9	Post LOCA Cooldown & Depressurization	This procedure provides instructions to cool down and depressurize the RCS to cold shutdown conditions following a loss of reactor coolant inventory.	IRIS could have a post-LOCA procedure but the details would be quite different.
10	Response to Inadequate Core Cooling	This procedure provides instructions to restore core cooling.	IRIS could have a similar procedure but the differences in the steam generators and Engineered Safeguard Features systems ensure that the details would be quite different.
11	Response to Degraded Core Cooling	This procedure provides instructions to restore adequate core cooling.	IRIS could have a similar procedure but the differences in the steam generators and Engineered Safeguard Features systems ensure that the details would be quite different.
12	Response to Saturated Core Cooling	This procedure provides instructions to restore subcooled core cooling.	IRIS could have a similar procedure.
13	Response to Loss of Heat Sink	This procedure provides instructions to respond to a loss of heat sink in all steam generators.	IRIS could have a similar procedure but the differences in the steam generators and Engineered Safeguard Features systems ensure that the details would be quite different.
14	Response to SG Overpressure	This procedure provides instructions to respond to an overpressure condition affecting either steam generator where pressure has increased above the highest safety valve set point.	This IRIS design eliminates this possibility.

#	Title	Summary	IRIS Implications
15	Response to SG High Level	This procedure provides instructions to respond to a steam generator high-level condition and to address the steam generator overfill concern.	IRIS could have a procedure to address steam generator overfilling, but the differences in the steam generators ensure that the details would be rather different.
16	Response to Loss of Normal Steam Release Capabilities	This procedure provides instructions to respond to a failure of the steam generator power operated relief valves (PORVs) and condenser steam dump valves.	IRIS does not rely on steam release, so this procedure does not apply.
17	Response to SG Low Level	This procedure provides instructions to respond to a steam generator low-level condition.	Because of differences in the steam generators, this procedure does not apply to IRIS. A "Response to Loss of Heat Sink" procedure (see item 13) is probably sufficient for IRIS.
18	Response to High Pressurizer Level	This procedure provides instructions to respond to a high pressurizer level.	IRIS could have a similar procedure
19	Response to Low Pressurizer Level	This procedure provides instructions to respond to a low pressurizer level.	IRIS could have a similar procedure
20	Response to Voids in Reactor Vessel	This procedure provides instructions to respond to voids in the reactor vessel head.	This event does not apply to IRIS because the pressurizer lies within the reactor vessel. A "Response to Low Pressurizer Level" procedure (see item 19) would be sufficient.
21	Response to Imminent PTS [pressurized thermal shock] Conditions	This procedure provides instructions to avoid, or limit, thermal shock or pressurized thermal shock to the reactor pressure vessel, or overpressure conditions at low temperature.	IRIS could have a similar procedure but the differences in the steam generators and Engineered Safeguard Features systems ensure that the details would be quite different.
22	Response to Anticipated PTS [pressurized thermal shock] Conditions	This procedure provides instructions to respond to a limited overcooling condition or to an overpressure condition at low temperature.	IRIS could have a similar procedure but the differences in the steam generators and Engineered Safeguard Features systems ensure that the details would be quite different.

#	Title	Summary	IRIS Implications
23	Response to Nuclear Power Generation – ATWS [anticipated transients without scram]	This procedure provides instructions to add negative reactivity to a core which is observed to be critical when expected to be shut down.	IRIS could have a similar procedure but the differences in the steam generators and Engineered Safeguard Features systems ensure that the details would be quite different.
24	Response to Loss of Core Shutdown	This procedure provides instructions to restore the core to an adequate shutdown condition.	IRIS could have a similar procedure but the details would need to be different to reflect the differences in the protection systems.
25	Response to High Containment Pressure	This procedure provides instructions to respond to a high containment pressure.	IRIS could have a similar procedure
26	Response to Containment Flooding	This procedure provides instructions to respond to containment flooding.	IRIS could have a similar procedure
27	Response to High Containment Radiation	This procedure provides instructions to respond to high containment radiation level.	IRIS could have a similar procedure
28	Response to Low Containment Pressure	This procedure provides instructions to respond to a low containment pressure.	IRIS could have a similar procedure
29	Response to Loss of RCS Inventory During Shutdown	This procedure provides instructions to maintain core cooling and protecting the reactor core in the event that PRZR level is lost during shutdown operations when the RCS is intact or RCS level is too low to support operation of the RNS pumps during operation in reduced inventory conditions in the RCS.	IRIS could have a similar procedure but the details would need to be quite different to reflect the differences in the containment and Engineered Safeguard Features systems.
30	Response to Loss of RNS [residual heat removal system] During Shutdown	This procedure provides instructions for maintaining core cooling and protecting the reactor core in the event that residual heat removal system cooling is lost.	IRIS could have a similar procedure.
31	Response to High Containment Radiation During Shutdown	This procedure provides instructions to respond to high radiation in containment.	IRIS could have a similar procedure

#	Title	Summary	IRIS Implications
32	Response to Increasing Nuclear Flux During Shutdown	This procedure provides instructions to respond to increasing nuclear flux during shutdown.	IRIS could have a similar procedure
33	Response to Cold Overpressure During Shutdown	This procedure provides instructions to respond to an overpressure condition at low temperature.	IRIS could have a similar procedure
34	Response to Unexpected RCS Temperature Changes During Shutdown	This procedure provides instructions to respond to unexpected changes in RCS temperature.	IRIS could have a similar procedure

4. IRIS I&C SYSTEM ARCHITECTURE

4.1. CONTROL SYSTEMS

Although nuclear power plants must be able to handle safely emergency conditions, they exist to generate electricity, and most of the control room actions taken over plant life will focus on normal operations. The control room design must not focus solely on emergency operations; instead, it must facilitate normal operations as well. This requires coordinating the normal control system and control room designs.

Although one can only speculate[4] on what the final control system upgrade in the last operating IRIS plant may be a century or more from today, we can make some reasonable assumptions about what the initial architecture in the first IRIS unit will be a few years from now. Every indication is that the first IRIS units will use a distributed digital system networked to the control room, and that the control room will feature smart workstations. We will assume such an architecture in the remainder of this section.

Reference 8 notes that "Early nuclear units had separate control systems for each control loop, and limited signal interaction between the loops. This simplified the design of each loop, particularly with analog control systems where each interconnection added hardware expense. The current trend is for more integrated systems that can take advantage of coordinating the different control loops." The Temelín units in the Czech Republic are operating examples of power plants that utilize highly integrated control systems. The Temelín control systems provided the following features

1. A "Control Coordinator" performs the supervisory control functions of (1) establishing the major plant reference signals (power, temperatures, pressures) during normal operation, and (2) establishing the operating mode for reactor and turbine control systems in response to operator requests and/or plant conditions (including upsets). Reference 8 describes a Control Coordinator for IRIS.

2. A "Turbostep" function coordinates startup and shutdown of most secondary-side systems. The secondary-side systems, in turn, have their own sequential startup and shutdown algorithms. (Several

[4] Consider, for example, the possibility of developing intelligent, organic computers. This is not necessarily science fiction: reference 7 describes how the University of Florida is testing this technology by flying flight simulators on a laboratory scale.

primary auxiliary systems have sequential startup and shutdown algorithms as well).

3. The Temelín control room provides online computerized procedure displays that (1) include live status information on the relevant plant variables for each step, and (2) in the case of normal (but not emergency) operating procedures, allow taking direct action from the procedures workstations. Reference 9 describes the system.

The Temelín experience shows that, even in the past millennium, the technology existed to automate most if not all plant control operations, at least in the absence of equipment failure. Naturally, no utility would want to automate to the point of eliminating the entire operating staff, but it is clear that automation (1) can ease operator workload, and (2) should lead to more predictable actions than relying on manual control (particularly in timing, but one hopes also through reduction in error probability). The following list gives some of the items that one would probably not want to automate:

1. Taking the reactor critical

   This is a simple operation with little associated risk of plant damage, so any benefits may not outweigh the cost. Forcing the operator to start the reactor manually forces him or her to monitor the plant during this time. Automating this task may be unacceptable to regulatory authorities.

2. Issuing the command to synchronize to the grid

   Although one would want to automate the actual synchronization process, there needs to be an operator action to confirm that the grid dispatchers approve and expect the synchronization.

3. Occasional simple tasks

   Some tasks do not warrant the added complexity of automation; for example, the Temelín system does not automate warming the moisture separator reheaters because the process takes several hours and requires very few manual actions.

4. Long term accident recovery

   Because of the low probability of occurrence for severe accidents coupled with the low workload required for their long-term mitigation, long-term accident recovery actions probably do not warrant automation.

4.2. SAFETY SYSTEMS

For better or worse, separating I&C systems into safety and non-safety systems is so ingrained in the regulatory process that we consider it unlikely that anyone would make the effort to propose, develop, and attempt to license a different approach. Separating safety systems from non-safety systems simplifies the rules for analyzing post-accident response, but sometimes fosters the belief that non-safety systems have no importance. Additional regulatory categories (e.g., systems important to safety) partially address this issue while adding ambiguity. From our perspective, we do not see a pressing need to deviate from existing regulatory practice.

Separating I&C equipment into safety and non-safety systems presents an interface problem when the two systems have to communicate. The industry and its regulatory agencies have allowed sending isolated signals from the safety systems to non-safety systems for decades. With the advent of digital systems, the problem of integrating safety and non-safety systems onto common control room hardware arose. Control room designers have developed and licensed architectures that prevent failures in non-safety control room components from propagating to the safety systems, solving the problem. We hope that additional experience with digital systems will eventually allow complete elimination of all dedicated, hard-wired controls from the control room.

4.3. CONTROL ROOM

The control room equipment performs two basic functions. First, it provides the plant status information needed to let the operators make decisions on plant operations. Second, it provides a mechanism for executing the operator commands resulting from those decisions. In the old analog designs, the information displays consisted of hundreds of dedicated meters, lights, recorders, and similar devices, while the command entry mechanism consisted of hundreds of dedicated switches, potentiometers, and similar devices. Digital technology eliminated the need for large panels filled with dedicated presentations and controls, and replaced these with programmed displays that present the information in a synthesized, consistent, and more user friendly manner. We see no reason to avoid this technology.

Our vision for an IRIS control room incorporates many ideas found in current advanced control room designs such as the AP1000 design. Nuclear suppliers developed and tested these ideas over several decades. Briefly, we see each operator having a work area that includes the following features:

1. Information displays

   Current display technology has size limits, so the current practice is to provide multiple displays for each user. We suggest the following minimum display set:

   A. A dedicated overview display

      Some current designs use a separate wall-mounted display for this purpose, but there is no need to separate the overview from the user's work place[5]. The overview should provide high-level information on the area under the operators control and its major interfaces.

   B. Safety parameters display

      In principal, the overview display should provide this information, but regulatory requirements make it difficult or impossible to combine safety parameters with an operational overview.

   C. Alarm status display

      Modern alarm displays mimic traditional alarm windows, eliminating the old, user-hostile multi-page alarm lists.

   D. Procedure displays

      A key component of our vision is an on-line computerized procedure system that has the capability to suggest and execute commands. As noted earlier, these have existed for many years.

   E. Monitoring and command displays

      Modern I&C displays provide plant information in a graphical format. These graphics include on-screen buttons and controls. The operator can navigate through the display set to focus on the displays that best relate to his or her current attention. We recommend providing at least two displays for monitoring and command.

[5] Large wall mounted displays appear to be good choices for providing overview information to larger groups, but the idea that two operators cannot discuss plant status without using a separate wall mounted system is untenable. We see an application for wall-mounted displays in places such as the technical support center.

The user should have the ability to customize the display arrangement by determining which display serves each display function.

2. Information entry devices

   We suggest a keyboard and a pointing device such as a mouse or trackball.

3. Printer

   The operator should have a printer or similar device. Considering today's prices, we see no need to share printers between operators.

4. Communications

   Power plant operators do not have the high-volume communication requirements that one finds in, for example, air traffic controllers or railroad dispatchers, but at times, they need to communicate with others outside the control room. The operators should have a telephone/intercom system available. We do not recommend integrating this with the plant I&C System, although the analogous integration is common in other industries.

Each connection between the plant I&C system and the general public creates a potential security risk, so we recommend limiting inputs to the plant I&C system to those directly related to plant operation (e.g., dispatcher requests). In particular, we recommend excluding email, web access, and other similar and perhaps important functions from the control room I&C displays, networks, and systems. The control room should have a separate system to provide these functions.

The operator work area outlined here is a robust configuration suitable for several approaches to plant operation. In the traditional approach, plant operators control one unit (reactor, turbine, generator, and switchyard). A more restricted approach separates the nuclear unit control and the turbine/generator/switchyard control into separate operating staffs. A third possibility, discussed in Section 5, is to have one operating staff responsible for all nuclear units on the site. Regardless of the arrangement, the work area described here can accommodate the needs if the designers program the workstation computers accordingly.

The control room's location is another issue. In older units incorporating analog controls, technical limits required placing the control room near the controlled equipment. These limits do not apply to modern digital systems. Technology allows locating the control room anywhere (worldwide), but security and practical considerations suggest locating the control room in a protected area on

site[6]. If one dedicates an operating staff to each reactor, then collocation makes sense, but if one combines functions in a site operating staff, then having a common room for controlling all units on site makes more sense.

Current regulations require some form of emergency shutdown facility. The technology exists to locate this anywhere as well. Although the regulations require only limited capability, it may be cheaper to duplicate the control room functionality than to develop a special, restricted-capability system. Duplicating the control room displays in the emergency shutdown facility has human factors advantages as well. The analog of the switchover from the main control room to the emergency shutdown facility is easily and commonly solved in other industries; however, the current regulations in the nuclear industry have not kept pace with the latest technology in this area.

[6] One should immediately not rule out the possibility of providing for off-site control, since it might offer some advantages in certain emergency conditions (e.g., nearby transportation accident with toxic chemical release). Security, not technology would be the limiting consideration.

5. MULTI-UNIT OPERATION

Before developing procedures, we need to establish the characteristics of the operating staff expected to execute those procedures. The IRIS program considers allowing one operating crew to monitor multiple units. Traditionally, each commercial nuclear reactor had its own operating staff. Multi-unit operation by a single operating staff is common practice in many other industries, including non-nuclear electric power plant. We know of no technical reason why the normal practice cannot extend to nuclear power plant operations.

This section develops example requirements to define the operating staff and some of their constraints. To provide specifics, we followed the approach given in Reference 10, which also served as a source for AP1000 staffing requirements.

5.1. OPERATING STAFF REQUIREMENTS FOR MULTI-UNIT OPERATION

This section establishes preliminary staffing constraints for operating a multi-unit IRIS plant. The individuals identified in these requirements will carry out plant operations during normal and emergency operations. These requirements establish constraints on individual qualifications and define the locations within which each individual may act. These requirements provide for augmenting the minimum staffing to ensure that an adequate staff is available for emergencies and to ensure routine and administrative tasks do not distract the operators at the plant controls from the plant operation. The staffing requirements presented here may exceed those in current regulatory requirements in the sense that they may specify plant operability with a smaller crew than some regulatory agencies might allow. For example, the staffing specified for design purposes follows trends in other industries and may result in less than one operator per reactor.

[IRIS.OpStaff.1] The normal shift operational staff for IRIS plants consisting of no more than three IRIS units shall not exceed the following:

Normal	Position	License
1	Shift Supervisor	SRO
1	Senior Reactor Operator	SRO
3	Reactor Operators	RO
1	Technical Advisor	-
2	Equipment Operators	-
1	Administrative Assistant	-

Basis: This is equivalent to the operating staff for one AP1000 unit. We chose to write this requirement for three IRIS units because three IRIS units provide roughly the same electric power output as one AP1000. As a goal, we would like to have one operating staff operate up to six IRIS units. A utility may choose to use a larger staff (e.g., dedicating at least one Reactor Operator per unit), but our intent is that the workload imposed by the I&C System should not be the limiting factor leading to additional staffing.

Guidance: One shift supervisor will be responsible for overall plant operation. This individual's normal station will be the shift supervisor's office; however, at any time the shift supervisor may be anywhere within the plant boundary. If so, the individual will be available (via voice communication) to respond immediately to the control room operators and if necessary, can be available in the controlling area of the main control room (MCR) within ten minutes.

One Senior Reactor Operator will be responsible for the direct supervision of the operators in the MCR. This individual's normal station will be in the main controlling area of the MCR; however, at any time the individual may be anywhere in the MCR.

Two Reactor Operators will be responsible for operating the controls in the MCR. These individuals will normally be located at the controls in the main controlling area of the MCR. One of these individuals (or another individual with an SRO or RO license) will be at the controls at all times. The other individual will be in the MCR at all times.

A third Reactor Operator will be responsible to assist the operators in the controlling area of the MCR by interfacing with other members of the plant staff. This individual's normal location will be in an area immediately adjacent to the controlling area of the MCR; however, the individual may be anywhere within the plant boundary. If so, the individual will be available (via voice communication) to respond immediately to the control room operators and if necessary, can be available in the controlling area of the MCR within ten minutes.

One Shift Technical Advisor qualified to provide engineering support will normally be located in an office immediately adjacent to the main controlling area of the MCR; however, the individual may be anywhere within the plant boundary. If

so, the individual will be available (via voice communication) to respond immediately to the control room operators and if necessary, can be available in the controlling area of the MCR within ten minutes.

Two equipment operators will be qualified as necessary to operate equipment in the plant at local stations. These individuals will normally be at various locations throughout the plant as operations require. The equipment operators will be available via voice communication to respond immediately to commands from the control room operators.

One Administrative Assistant will assist the shift supervisor with administrative details, e.g., obtaining references, handling correspondence, etc. This individual's normal location will be in or adjacent to the shift supervisor's office; however, the individual may be anywhere within the plant boundary.

[IRIS.OpStaff.2] The control room design (e.g., layout, number, and design of workstations) shall support operation during emergencies by the following maximum crew complement in the main controlling area of the MCR:

Normal	Position	License
1	Shift Supervisor	SRO
1	Senior Reactor Operator	SRO
3	Reactor Operators	RO
1	Technical Advisor	-
2	Equipment Operators	-

Guidance: These people are a subset of the personnel listed in requirement [IRIS.OpStaff.1].

[IRIS.OpStaff.3] In addition to the maximum crew complement, the main controlling area of the MCR shall have provisions for three active observers and assistants.

Guidance: The intent is that one individual is from the regulatory authority, one is from the plant owner's management, and one is to handle communications.

5.2. OPERATOR ACTION REQUIREMENTS

Automating plant operation is a primary I&C System function, and the required degree of automation depends on the constraints imposed on manual actions.

This section establishes preliminary operator action constraints for operating a multiunit IRIS plant. These requirements recognize that utilities normally perform advance planning for unit startups, so they allow for augmenting the staff for those activities. On the other hand, unit shutdowns can occur unexpectedly, so the design must allow a normal operating crew to handle these events without exceeding a reasonable workload for any member of the crew. Additional crew restrictions apply for shutdowns from outside the main control room.

Requirements that state, "...a single licensed operator to adequately perform the control and monitoring functions..." only mean that one operator can perform all the control actions needed at the control workstations. When interpreting these requirements, assume that the remaining members of the plant operating staff are available for other duties (e.g., the Equipment Operators are available to assist at local control stations).

[IRIS.OpActions.1] The I&C system shall allow performing all defined normal and emergency operations with the defined plant operating staff.

[IRIS.OpActions.1.1] The I&C System shall provide the necessary control and monitoring functions so that a normal shift crew can accomplish a single unit startup from cold shutdown to hot standby while monitoring the remaining units under their supervision.

[IRIS.OpActions.1.2] The I&C System shall provide the necessary control and monitoring functions so that a normal control room crew can accomplish multiple simultaneous unit startups from cold shutdown to hot standby while monitoring the remaining units under their control.

Basis: Since one normally plans for startup from cold shutdown to hot standby in advance, it seems reasonable to allow for additional equipment operators so that each unit has a full complement.

[IRIS.OpActions.1.3] The I&C system shall provide for a single licensed operator to adequately perform the monitoring and control functions needed to bring one unit from a hot standby condition to full power.

Basis: This allows one operator to devote attention to synchronization and power escalation.

[IRIS.OpActions.1.4] The I&C system shall provide for a single licensed operator to adequately perform the control and monitoring functions needed to maintain power operation of all units under his or her control.

[IRIS.OpActions.1.5] The I&C system shall provide for a single licensed operator to adequately perform the monitoring and control functions needed to take one or more of the plant units under his or her control from power operation to hot standby, while monitoring the remaining units under his or her control.

Exception: Remote shutdown operations for bringing the reactor from power operation to hot standby.

[IRIS.OpActions.1.6] The I&C System shall provide the necessary control and monitoring functions to allow two licensed operators (SRO or RO) and two EOs (only) to take any or all plant units under their control from power operation to hot standby from outside the main control room.

Guidance: For subsequent operations, assume that a normal crew will be available.

[IRIS.OpActions.1.7] The I&C System shall provide the necessary control and monitoring functions such that startup from the practical low-temperature limit of cold shutdown (i.e., “cold iron”) to hot standby, and for shutdown from hot standby to “cold iron”, can be accomplished by the normal shift crew.

[IRIS.OpActions.2] The I&C system design shall allow adequate time for the plant operating staff to perform their required duties.

[IRIS.OpActions.2.1] The IRIS plant I&C System designer shall perform the analyses of plant transients and emergencies as part of the I&C System design process based on the following assumptions:

(a) At least one licensed operator will be in the controlling area of the MCR at all times during normal power operations, and will be available at the controls immediately to respond to any off-normal situation,

(b) Two additional licensed operators (at least one of which is an SRO) will be available in the controlling area of the MCR within one minute when called upon,

(c) Two equipment operators will be available via voice communication to respond immediately to commands from the control room operators,

(d) The shift supervisor, the shift technical advisor, and an additional RO will be available via voice communication to respond immediately to the control room operators and can be available in the controlling area of the MCR within ten minutes.

[IRIS.OpActions.2.2] The IRIS plant shall require no credit for operator action to meet regulatory limits for at least 72 hours following the initiating events.

[IRIS.OpActions.2.3] The time required before an operator must act in an emergency to meet non-regulatory limits shall not be less than 30 minutes.

[IRIS.OpActions.2.4] The IRIS plant I&C system shall not preclude operator actions during the 30-minute time.

Guidance: The intent is that the I&C System must not lock out operator actions in a general sense. Locking out specific actions for

specific times and reasons (e.g., for a fixed time delay to allow an action to go to completion) is allowed.

5.3. MULTI-UNIT ACCIDENTS

Allowing one control room operating staff to control multiple IRIS units introduces the possibility that they would have to deal with simultaneous emergencies. The IRIS design does not require any operator action to meet regulatory limits for at least 72 hours following any initiating events, so there would be ample time to call in additional staff before exceeding regulatory limits. On the other hand, there may be desirable non-regulatory actions that would burden the operators, particularly if there were simultaneous events. To simplify the problem, we assume that the following combinations are sufficiently improbable that we can forego some or all non-regulatory actions until after calling in additional staff:

1. A condition III or IV event combined with one or more additional condition II, III, or IV events.

2. Simultaneous condition II events unless either (1) the event originates in shared equipment or (2) the events are causally connected (this includes any credible common mode failures).

The design should consider the potential for taking non-regulatory action with certain failures, but there is no need to apply the stringent failure assumptions normally associated with plant safety analyses. If we review the events listed in References 6 and 5 and assume that the only relevant shared equipment is in the plant electrical system, we can make the following observations:

1. Loss of offsite power would affect all units on the site.

2. Loss of external electrical load could affect all units on the site simultaneously.

3. Any condition II event in one unit that leads to a turbine trip could potentially introduce a switchyard electrical transient that would cause a loss of offsite power.

4. Any condition II event in one unit that leads to a turbine trip could potentially introduce a switchyard electrical transient that would cause turbine-generator trips in the remaining units.

5. Grid islanding would affect all units equally. It could also cause a loss of offsite power.

6. Grid and switchyard transients will affect all units on the site. They could also cause a loss of offsite power.

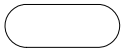
Under these assumptions, if one unit faces any of the design events, the remaining units will not face any event worse than a normal turbine trip with loss of offsite power. Designers should determine whether this assumption continues to apply as detailed design progresses. The designers should consider having the normal plant operating staff take non-regulatory actions to restore power in each of these cases, followed by bringing appropriate units back on line.

6. IRIS EMERGENCY OPERATING PROCEDURES

Table 2 listed the current AP1000 Simulator Emergency Operation Procedures and provided a preliminary summary of how they might apply to IRIS. The next step was to examine these procedures in detail. We looked at each of the corresponding AP1000 procedures and suggested modifications that might make them apply to IRIS. Figure 2 through Figure 36 summarize the results, with Figure 1 providing a legend. We retained the AP1000 numbering scheme for procedures as a convenience, but used our own numbering scheme for Critical Safety Function Status Trees.

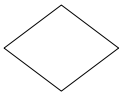
An emergency condition begins whenever a reactor trip condition, reactor trip, or S signal condition occurs. At this time, EOP E-0 takes effect. The operator's first responsibility is to verify that the reactor is tripped; if not, then the plant is in a beyond design basis condition (Anticipated Transient Without SCRAM) and procedure FR-S1 (Figure 11) applies. If the reactor tripped, then the operators begin monitoring the Critical Safety Function Status Trees. The AP1000 Simulator has trees for subcriticality (CSF 1, Figure 10), core cooling (CSF-2, Figure 13), heat sink (CSF-3, Figure 17), reactor coolant system integrity (CSF-4, Figure 20), containment (CSF-5, Figure 23), reactor coolant system inventory (CSF-6, Figure 28), emergency recirculation (does not apply to IRIS), and radiation (covered by other procedures). The Critical Safety Function Status Trees guide the operator to take specific actions when certain prioritized adverse conditions occur. The trees operate concurrently; meanwhile, EOP E-0 guides the operator through a systematic sequence of assessments and verifications that lead to identifying the probable event and the appropriate procedures for responding to that event.

The procedures outlined in Figure 2 through Figure 36 are preliminary and undoubtedly will require significant modification as the IRIS design evolves, as accident analyses continue, and especially when an IRIS simulator becomes available for human factors testing. Two defects are readily apparent: the procedures are too abstract and too ambiguous for implementation in a computerized procedure system. To a large degree, this reflects the current state of the IRIS design. Computer implementation will require identifying specific signals and thresholds for each decision in the process, and identifying failure (i.e., response not obtained) actions for every step.

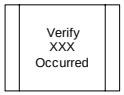


Entry or termination point

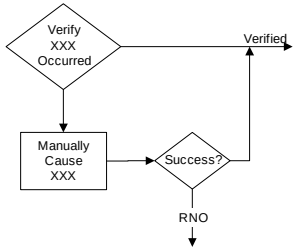
Action with one outcome



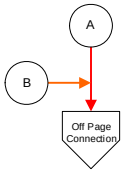
Action with multiple possible outcomes (e.g., a decision).
For “YES”/”NO” decisions, “YES” leaves on the right and “NO” leaves on the bottom.
For “Success”/”Failure” actions, “Success” leaves on the right and “Failure” leaves on the bottom



Shorthand for logic shown at right:
The verified branch leaves on the right and the RNO branch leaves on the bottom. Omitting the RNO branch implies that manual action is always successful



RNO = Response Not Obtained



Round circles A and B are on-page connectors.

Home plate pentagon is an off-page connector.

In Critical Safety Function Status Trees, A leaves page in a “RED” condition and B leaves in an “ORANGE” condition (even though the orange arrow hits a red line).

Figure 1: Legend

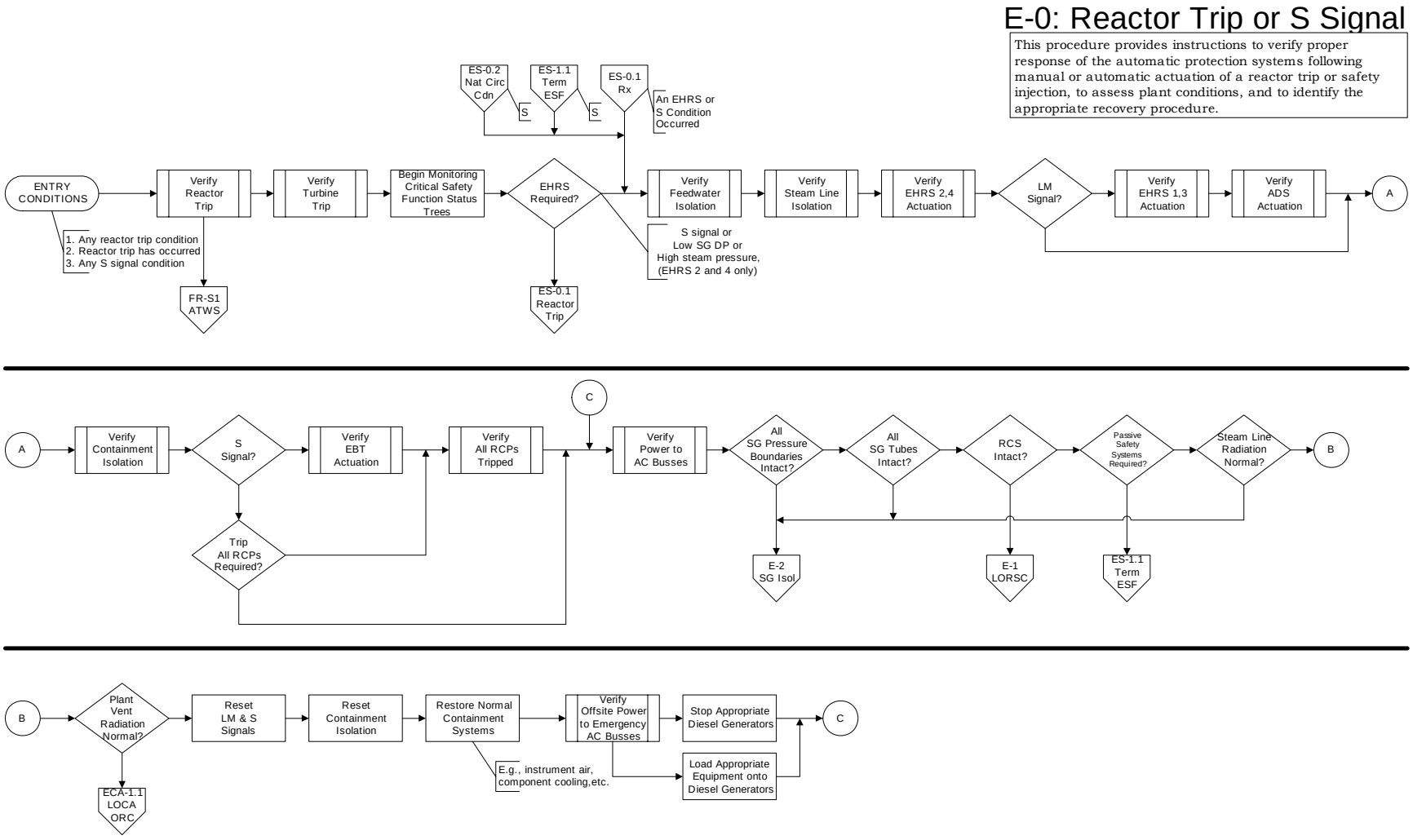


Figure 2: E-0, Reactor Trip or S Signal

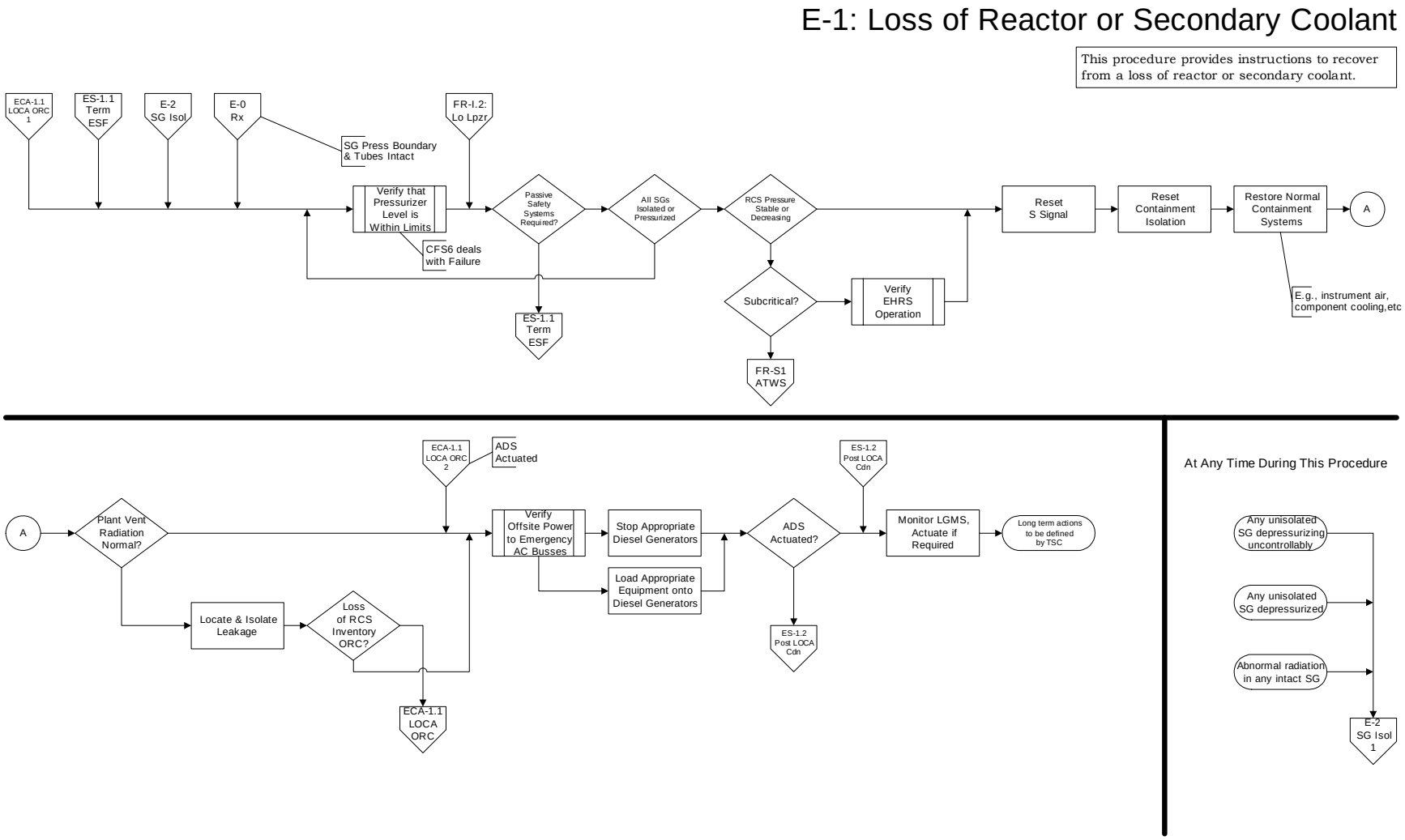


Figure 3: E-1, Loss of Reactor or Secondary Coolant

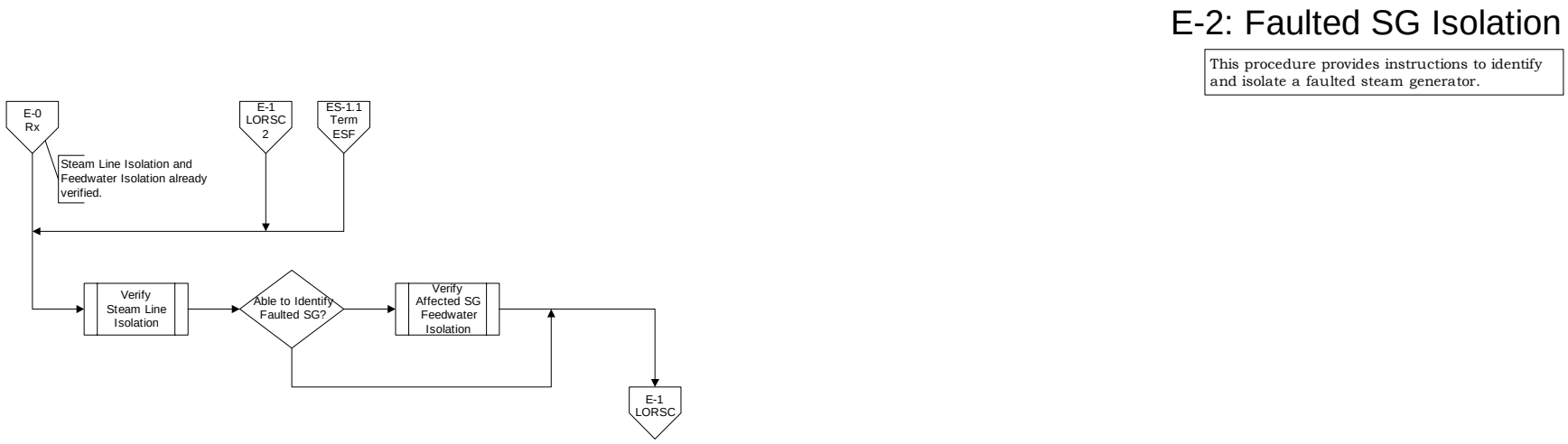


Figure 4: E-2, Faulted SG Isolation

This procedure provides instructions to isolate a LOCA outside containment.

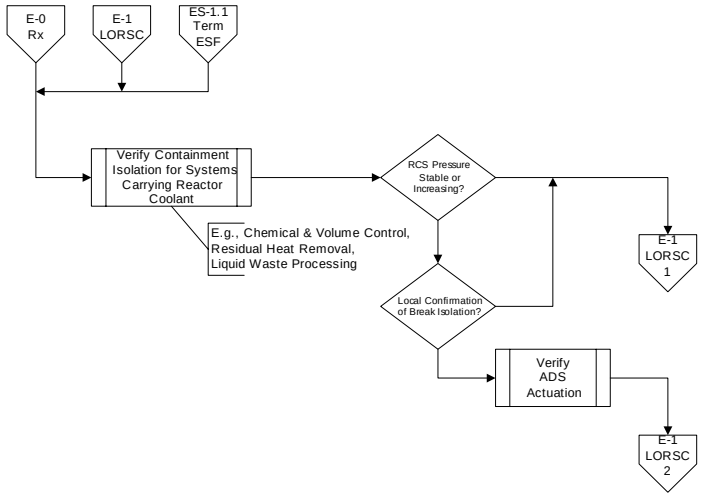


Figure 5: ECA-1.1, Loss of Reactor Coolant Outside Containment

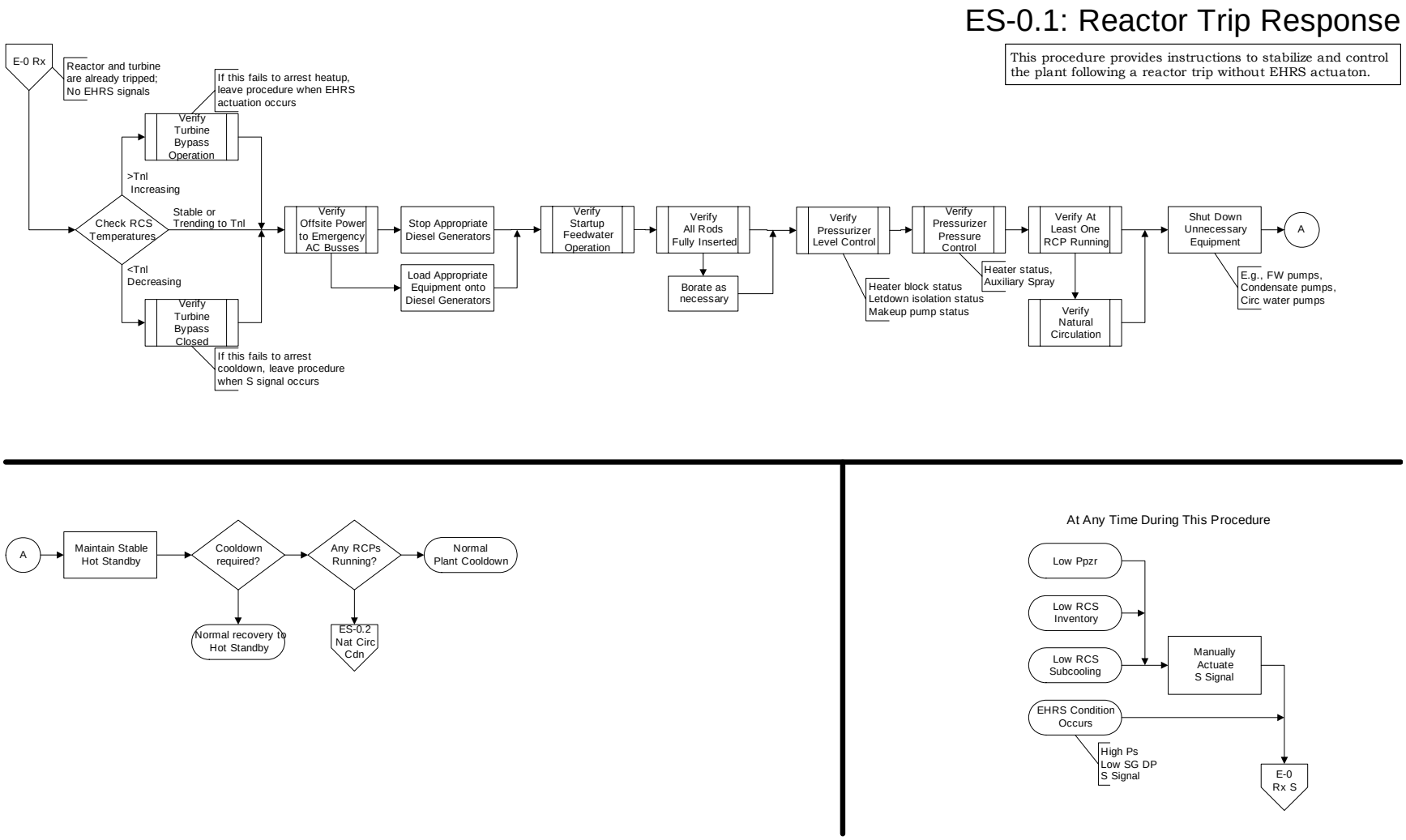


Figure 6: ES-0.1, Reactor Trip Response

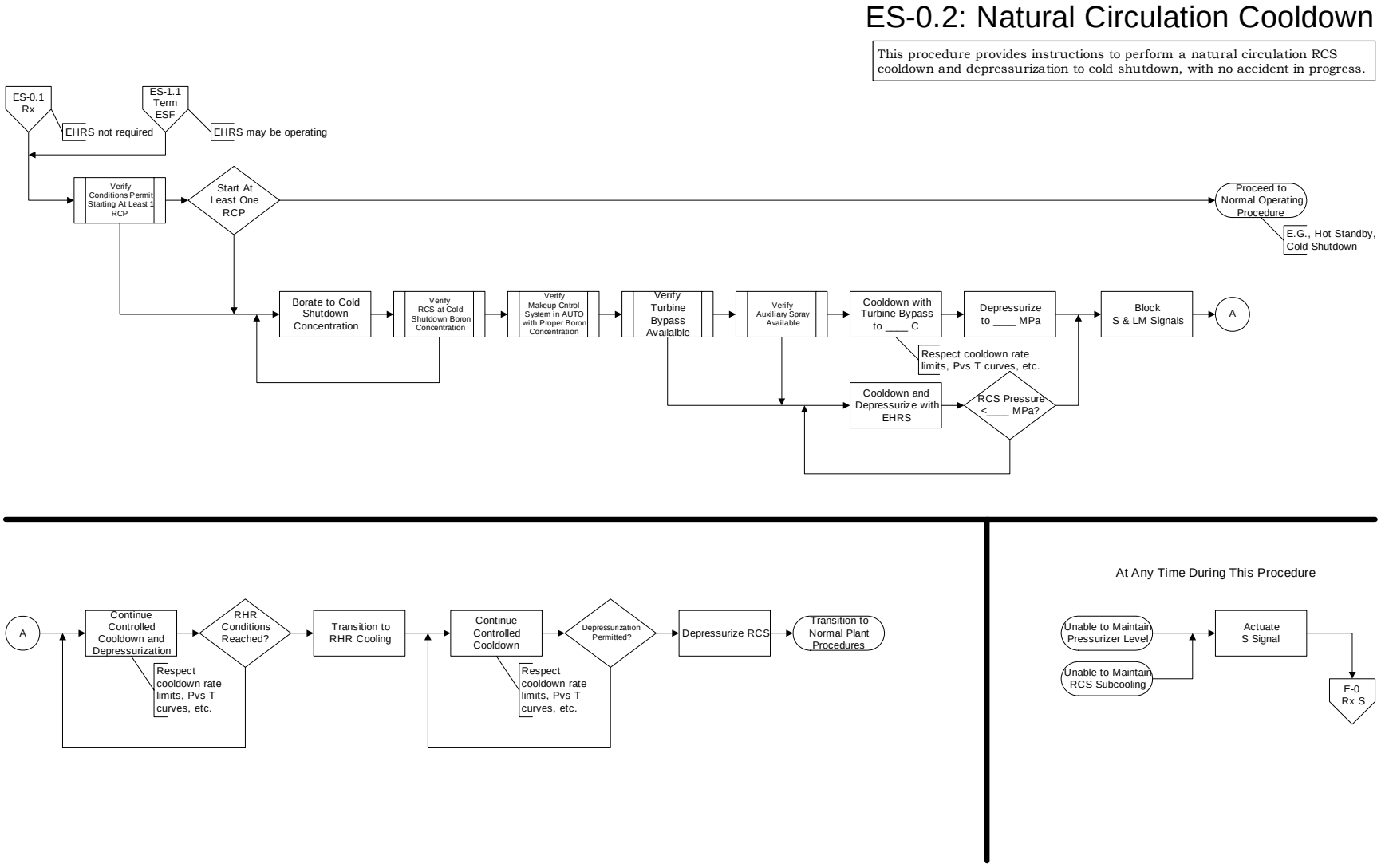


Figure 7: ES-0.2, Natural Circulation Cooldown

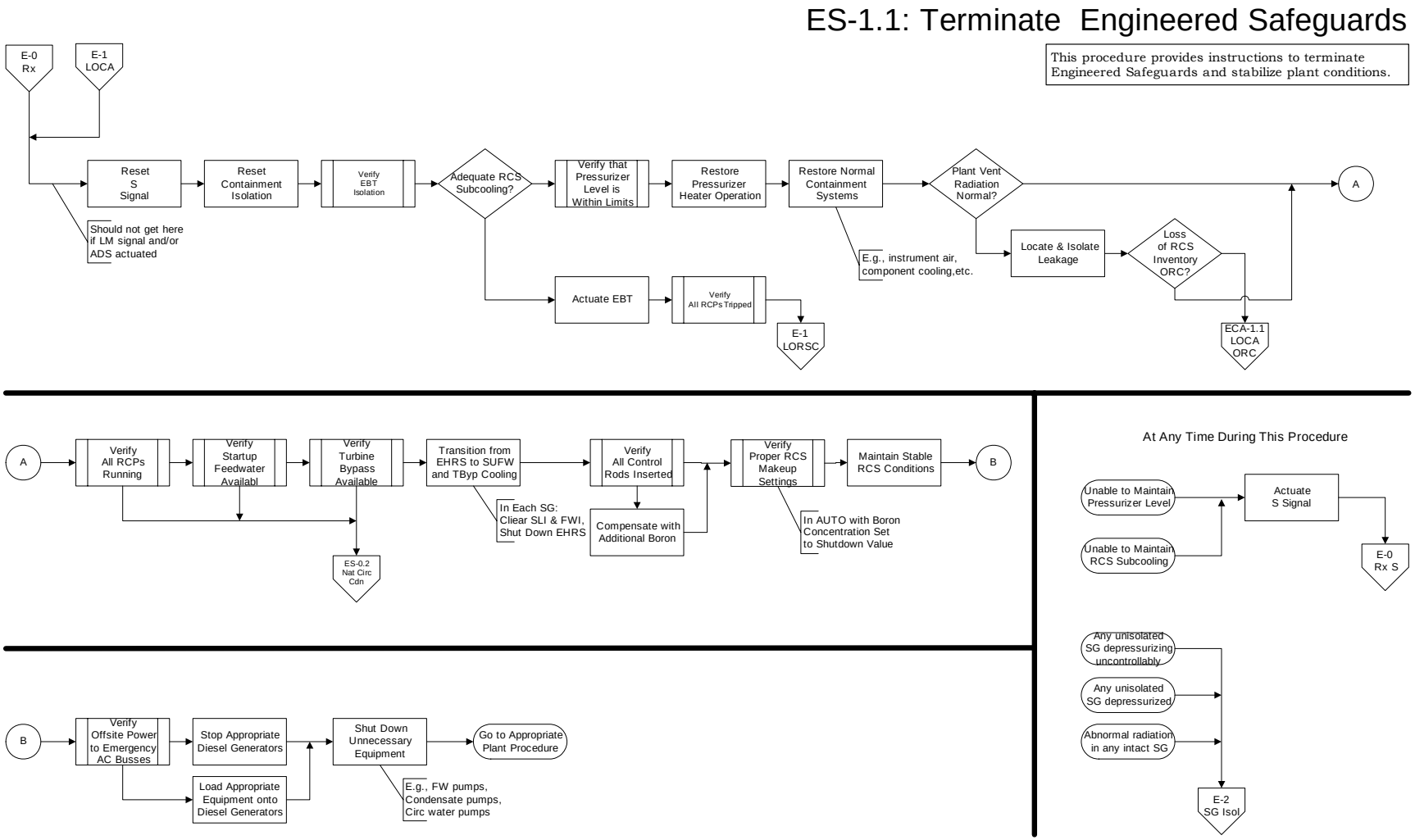


Figure 8: ES-1.1, Terminate Engineered Safeguards

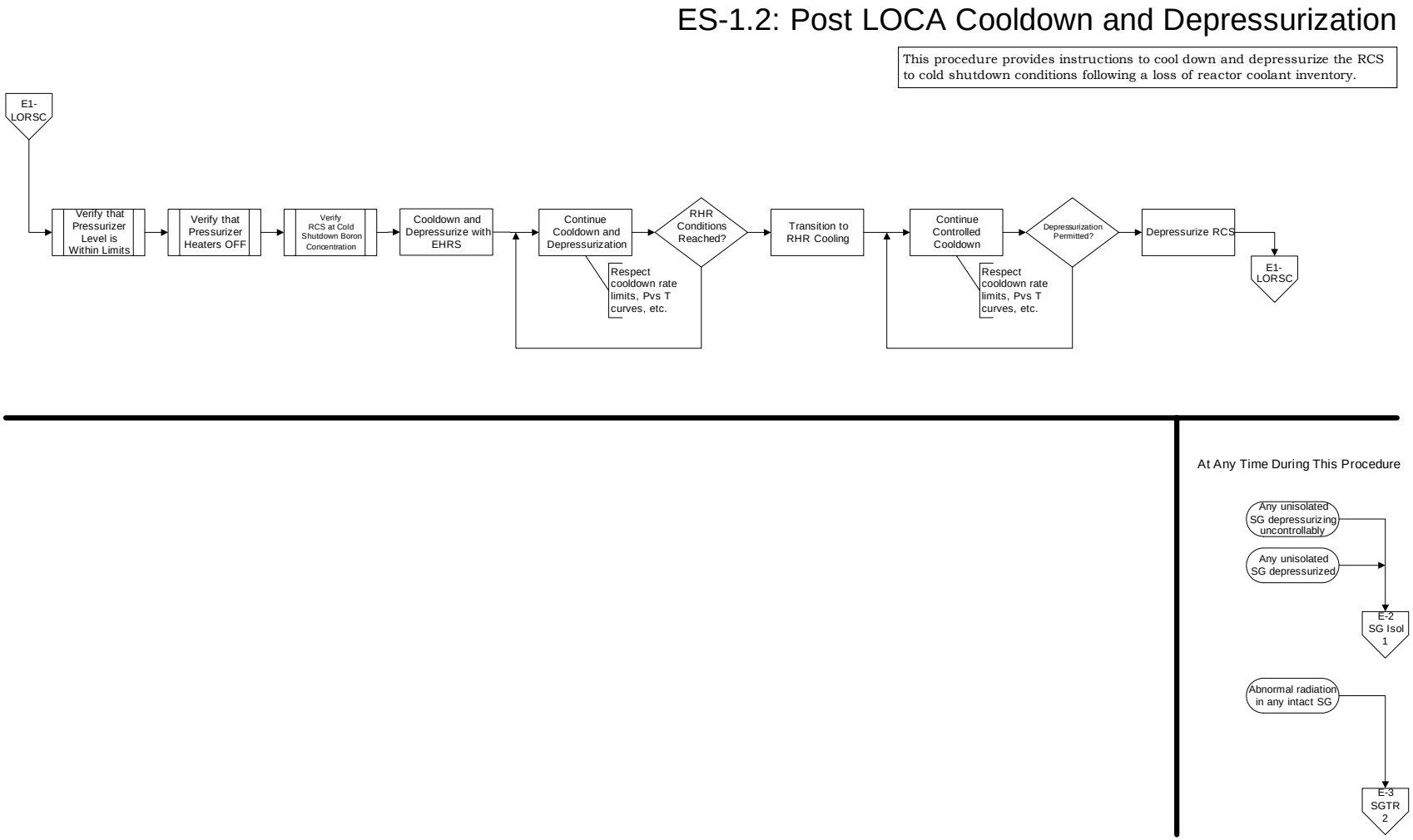


Figure 9: ES-1.2, Post LOCA Cooldown and Depressurization

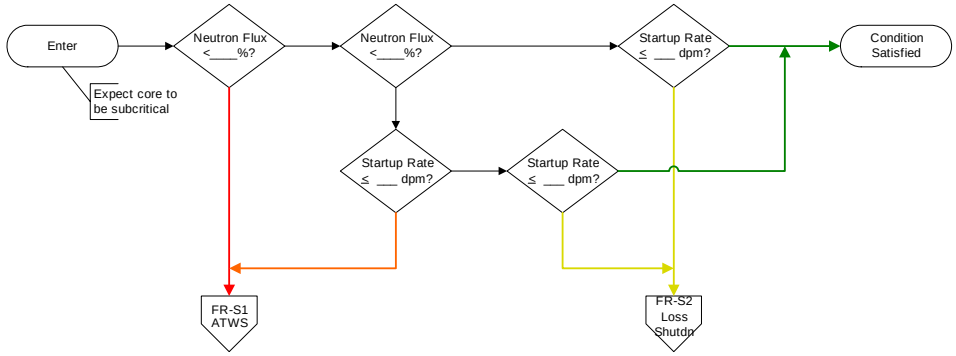


Figure 10: CSF-1, Subcriticality Critical Safety Function Status Tree

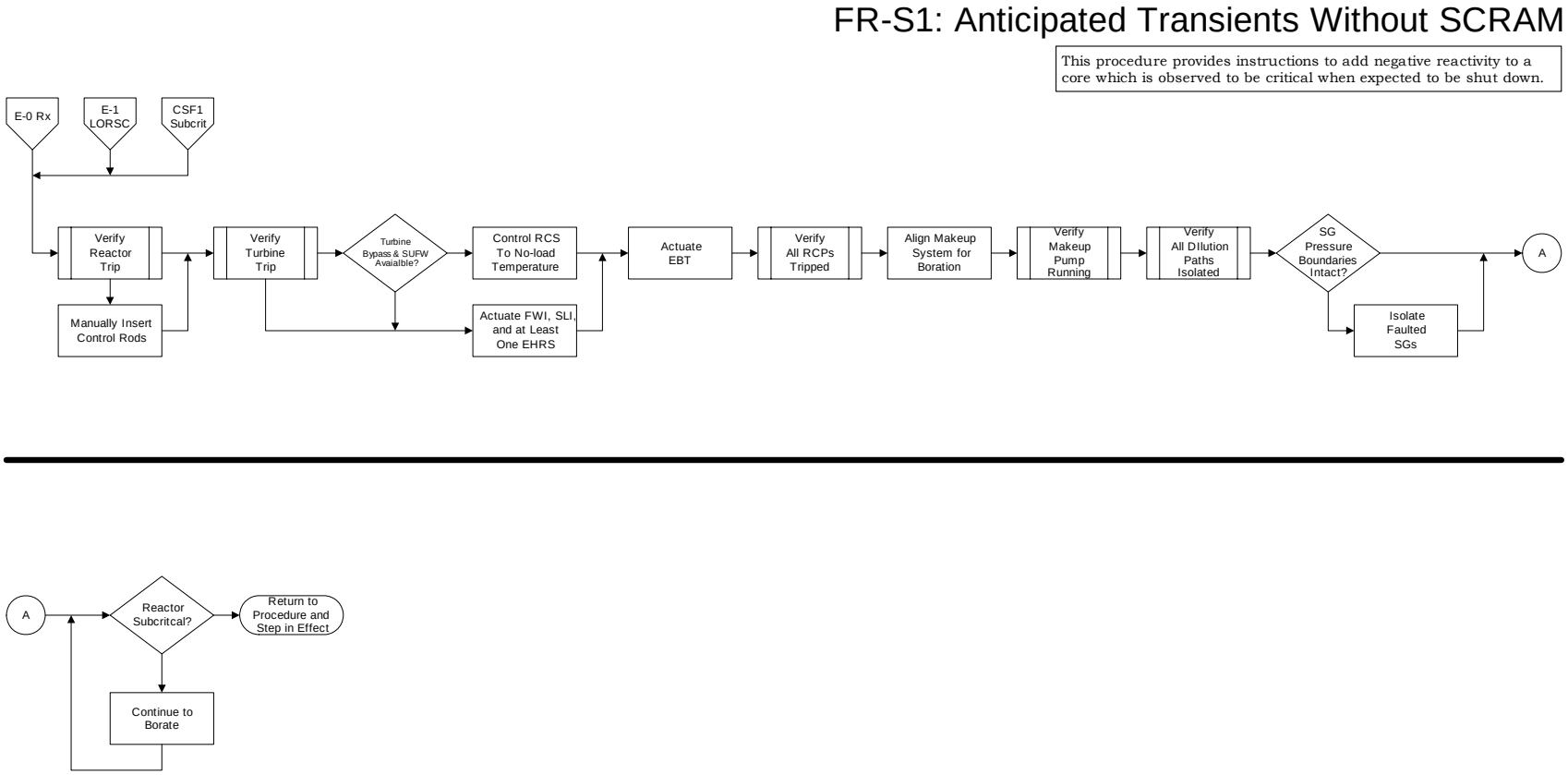


Figure 11: FR-S1, Anticipated Transients Without SCRAM

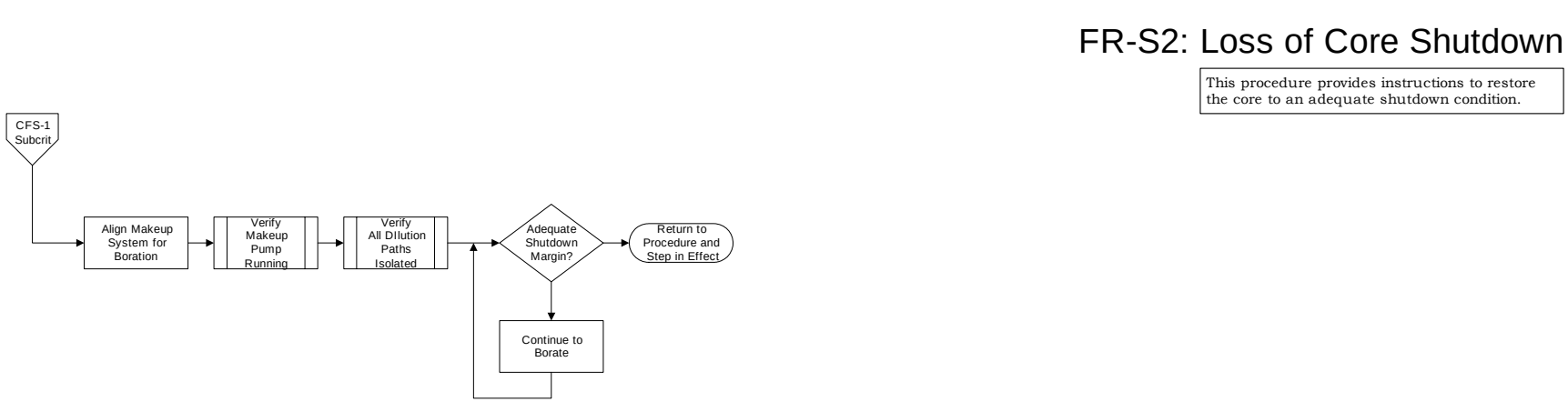


Figure 12: FR-S2, Loss of Core Shutdown

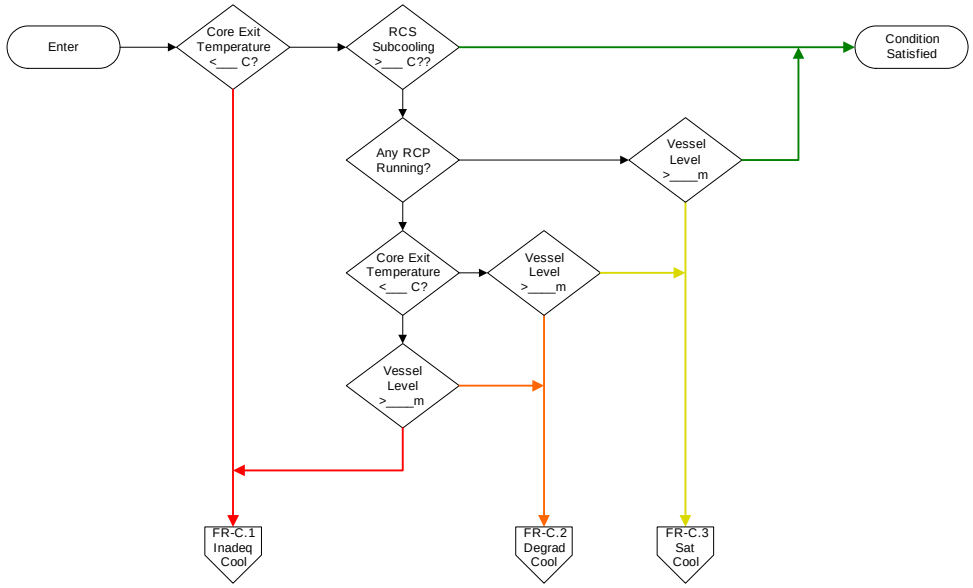


Figure 13: CSF-2, Core Cooling Critical Safety Function Status Tree

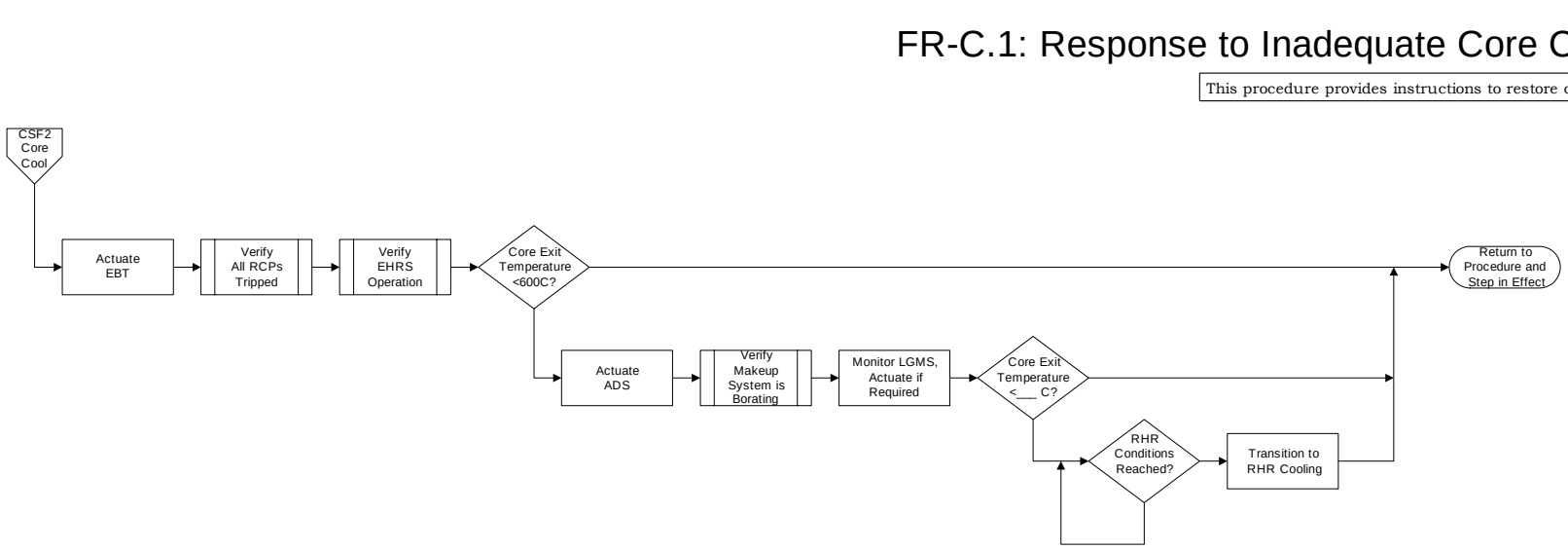


Figure 14: FR-C.1, Response to Inadequate Core Cooling

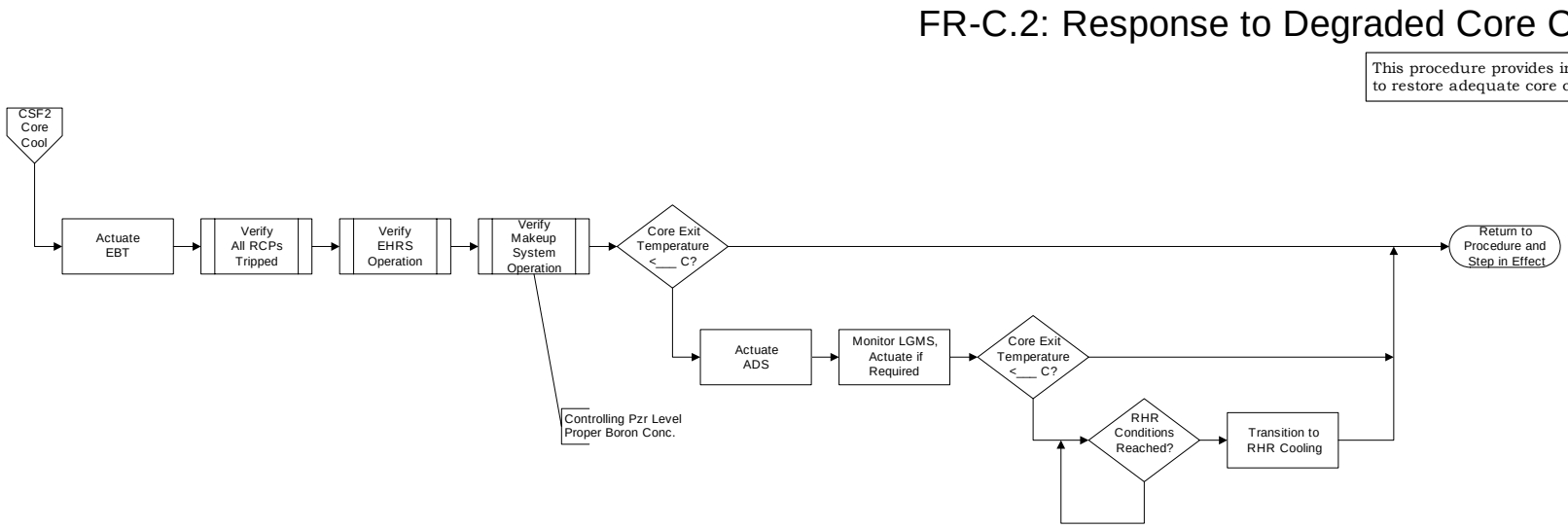


Figure 15: FR-C.2, Response to Degraded Core Cooling

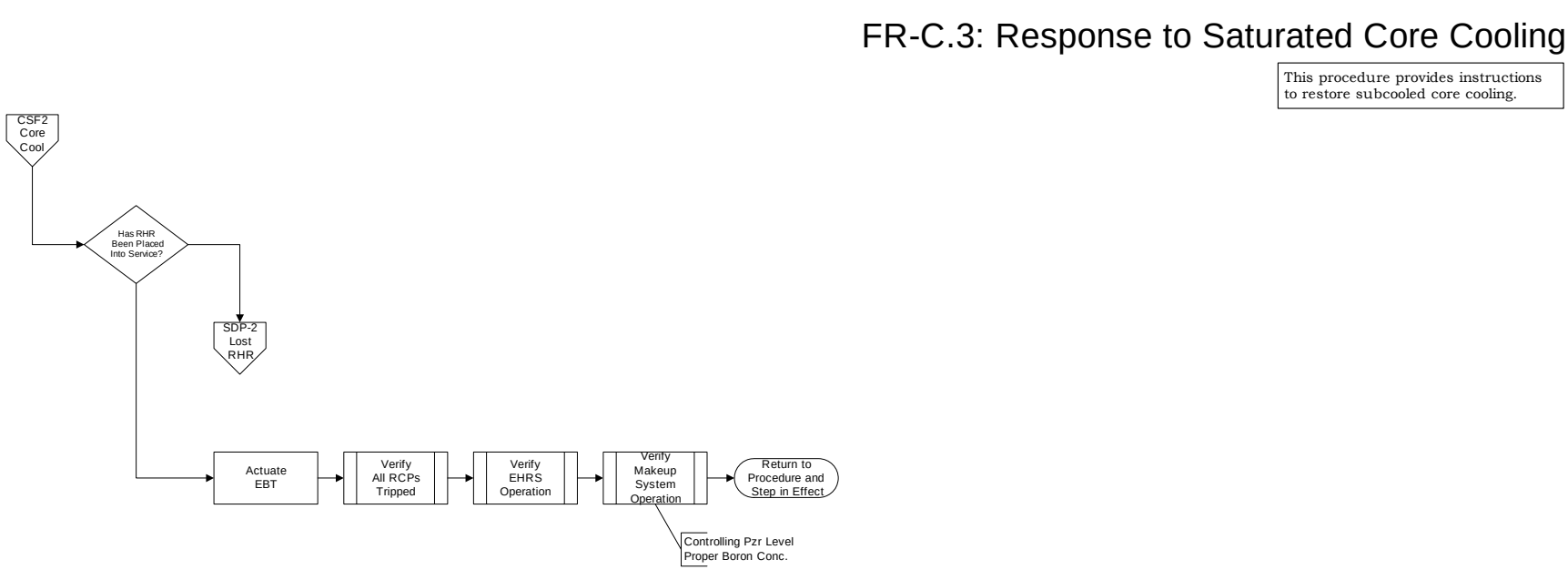


Figure 16: FR-C.3, Response to Saturated Core Cooling

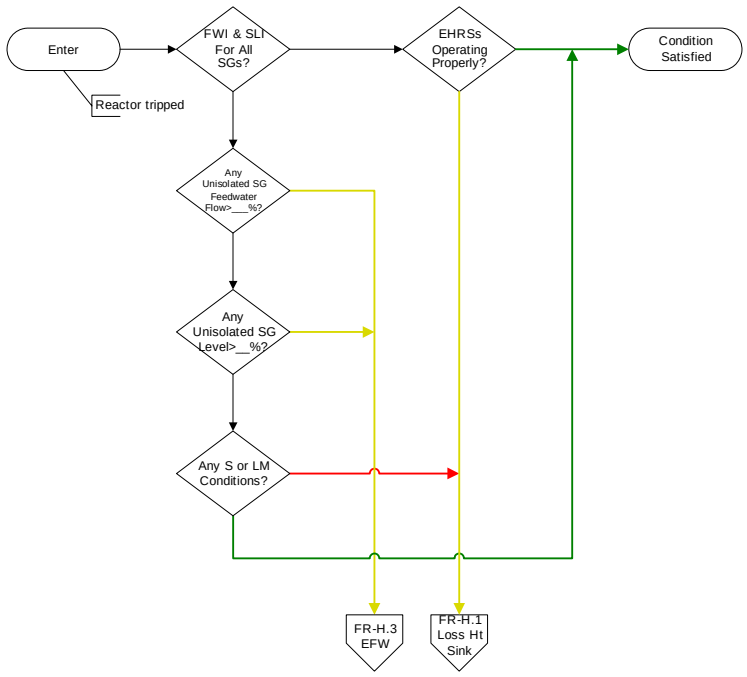


Figure 17: CSF-3, Heat Sink Critical Safety Function Status Tree

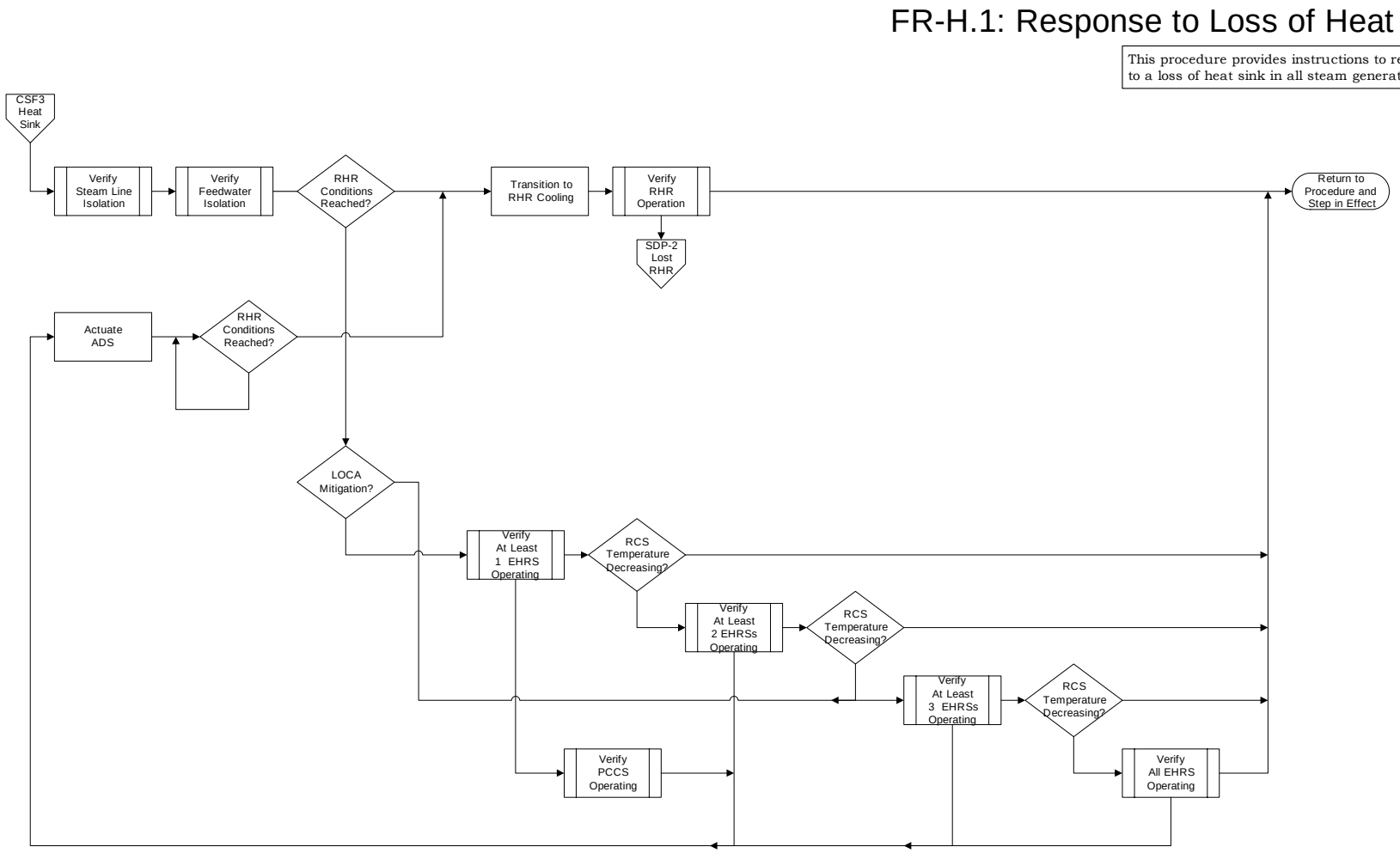


Figure 18: FR-H.1, Response to Loss of Heat Sink

This procedure provides instructions to respond to a steam generator high-level condition and to address the steam generator overfill concern.

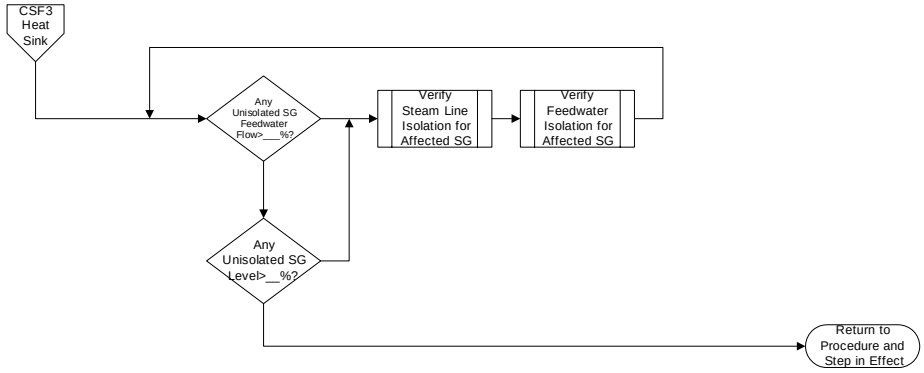


Figure 19: FR-H.3, Response to Excessive Feedwater

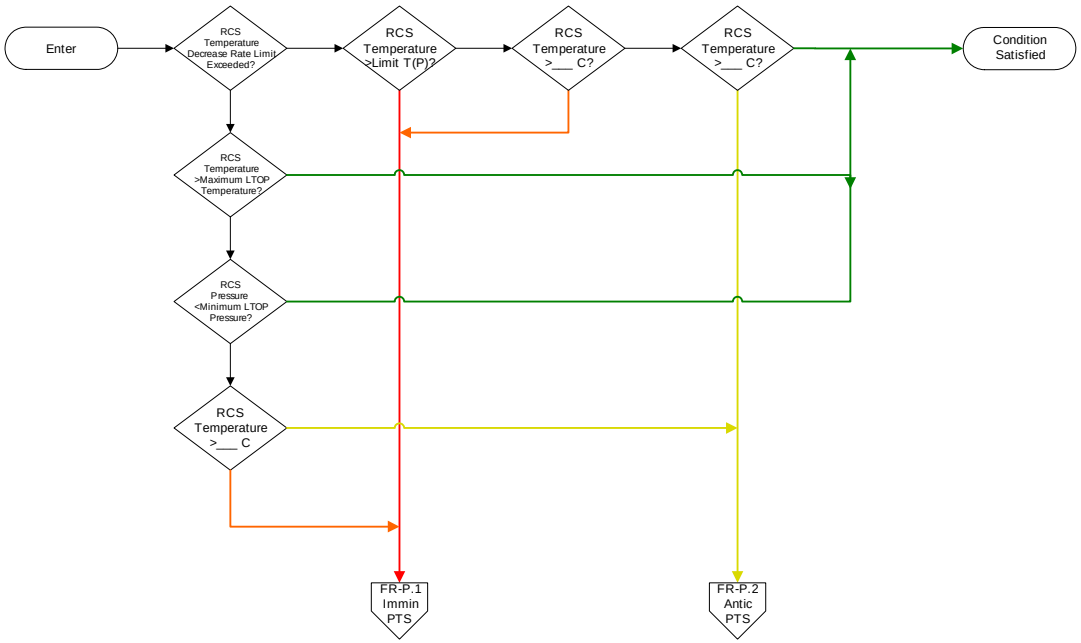


Figure 20: CSF-4, Integrity Critical Safety Function Status Tree

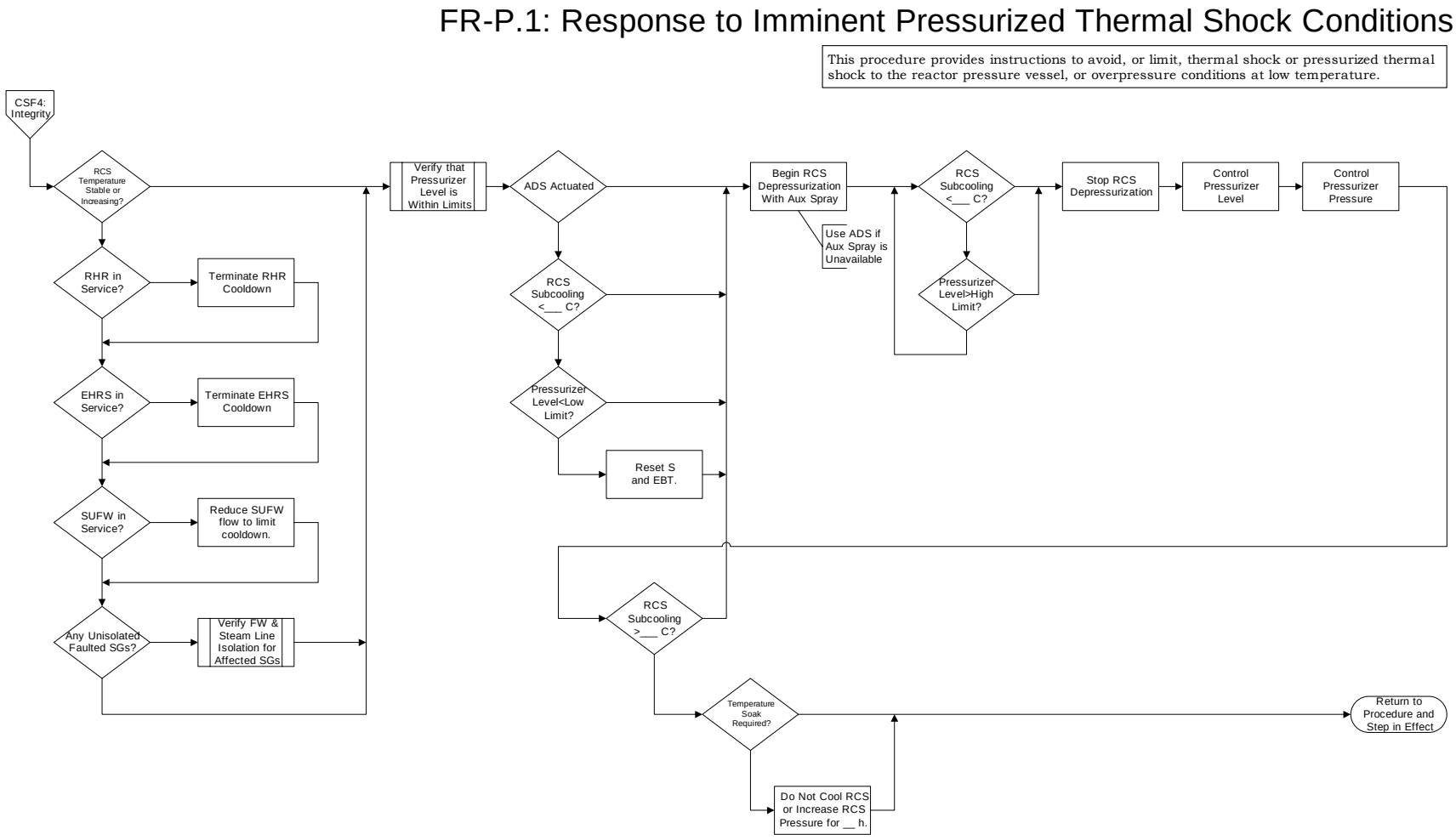


Figure 21: FR-P.1, Response to Imminent Pressurized Thermal Shock Conditions

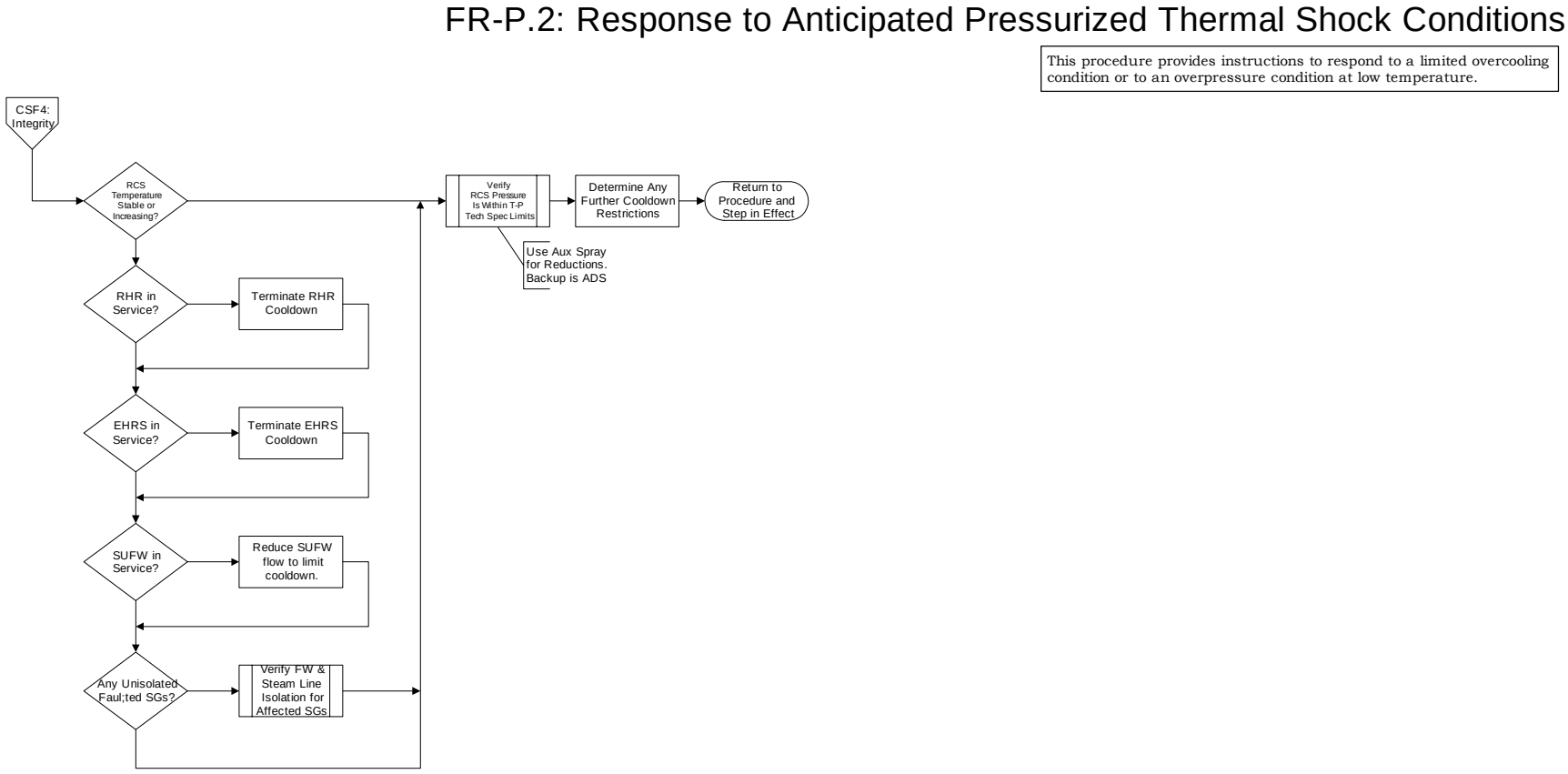


Figure 22: FR-P.2, Response to Anticipated Pressurized Thermal Shock Conditions

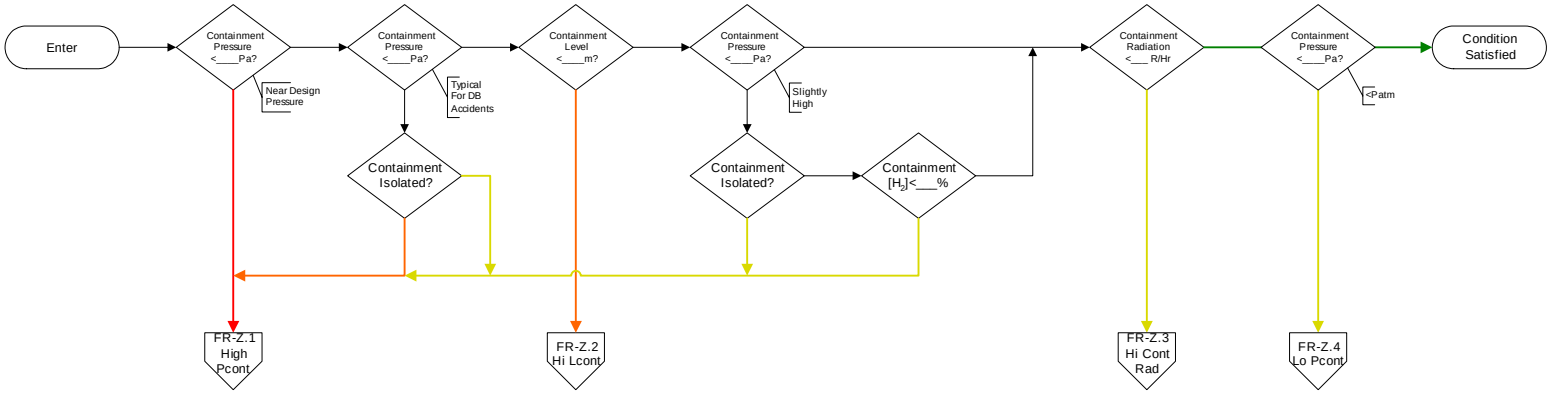


Figure 23: CSF-5, Containment Critical Safety Function Status Tree

FR-Z.1: Response to High Containment Pressure

This procedure provides instructions to respond to a high containment pressure.

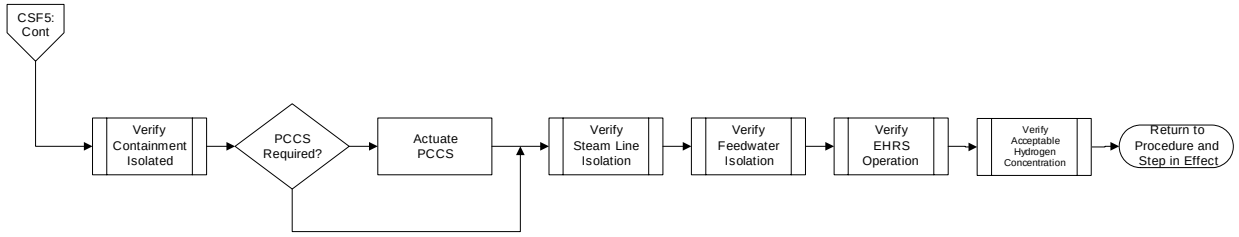


Figure 24: FR-Z.1, Response to High Containment Pressure

FR-Z.2: Response to Containment Flooding

This procedure provides instructions to respond to containment flooding.

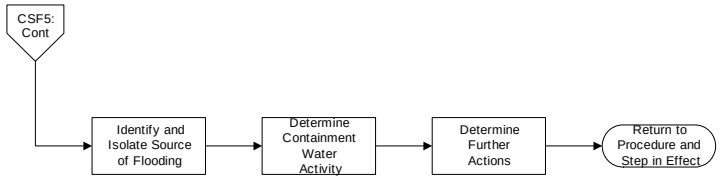


Figure 25: FR-Z.2, Response to Containment Flooding

FR-Z.3: Response to High Containment Radiation

This procedure provides instructions to respond to high containment radiation.

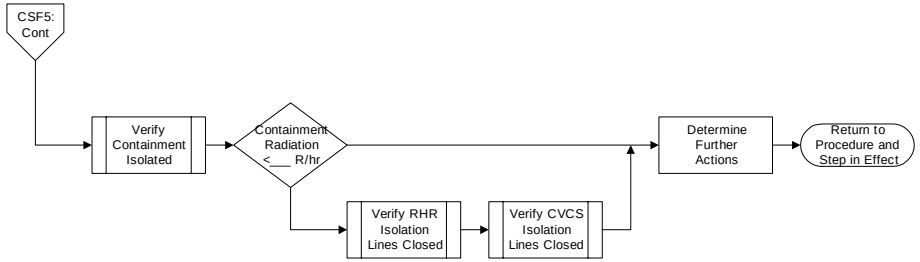


Figure 26: FR-Z.3, Response to High Containment Radiation

FR-Z.4: Response to Low Containment Pressure

This procedure provides instructions to respond to a low containment pressure.

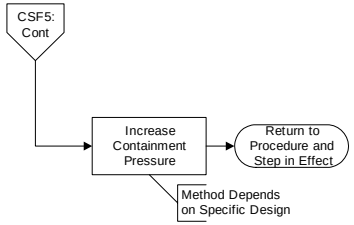


Figure 27: FR-Z.4, Response to Low Containment Pressure

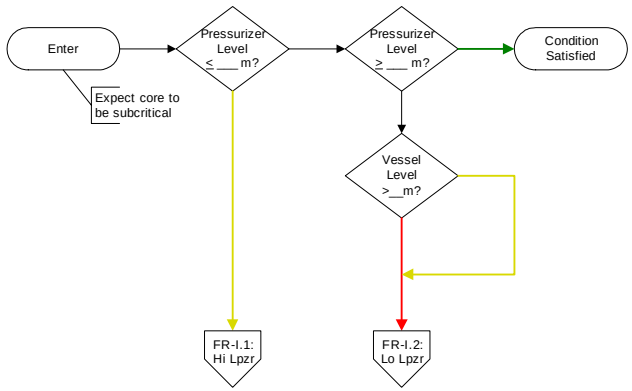


Figure 28: CSF-6, Inventory Critical Safety Function Status Tree

This procedure provides instructions to respond to a high pressurizer level.

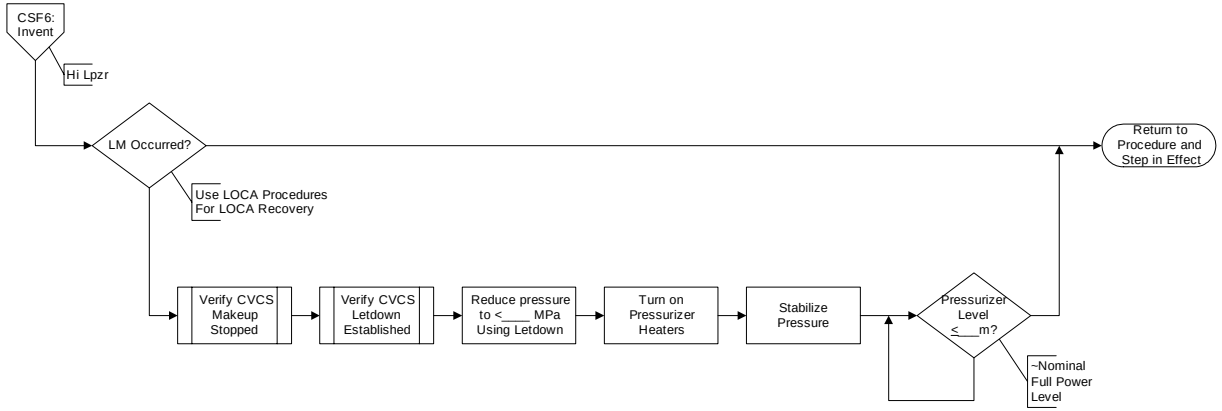


Figure 29: FR-I.1, Response to High Pressurizer Level

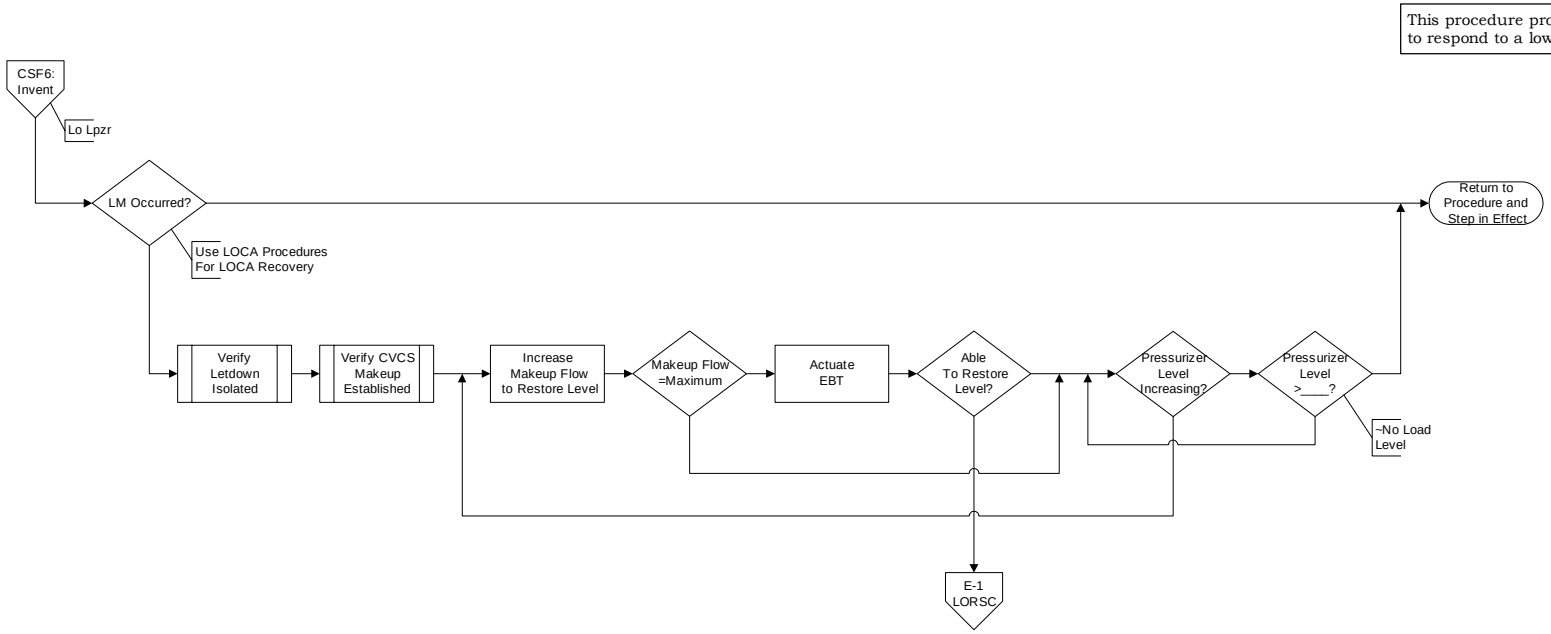


Figure 30: FR-I.2, Response to Low Pressurizer Level

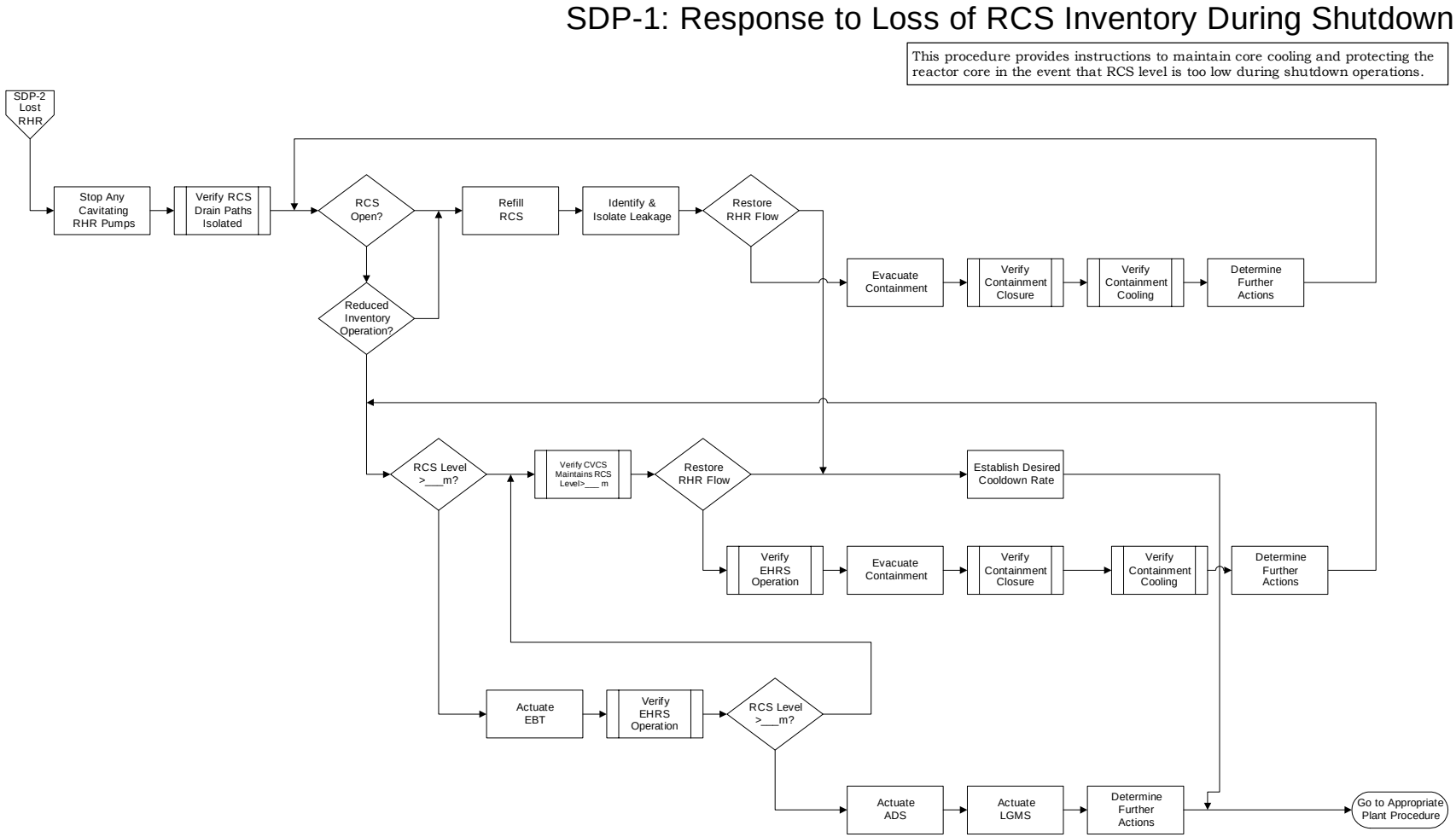


Figure 31: SDP-1, Response to Loss of RCS Inventory During Shutdown

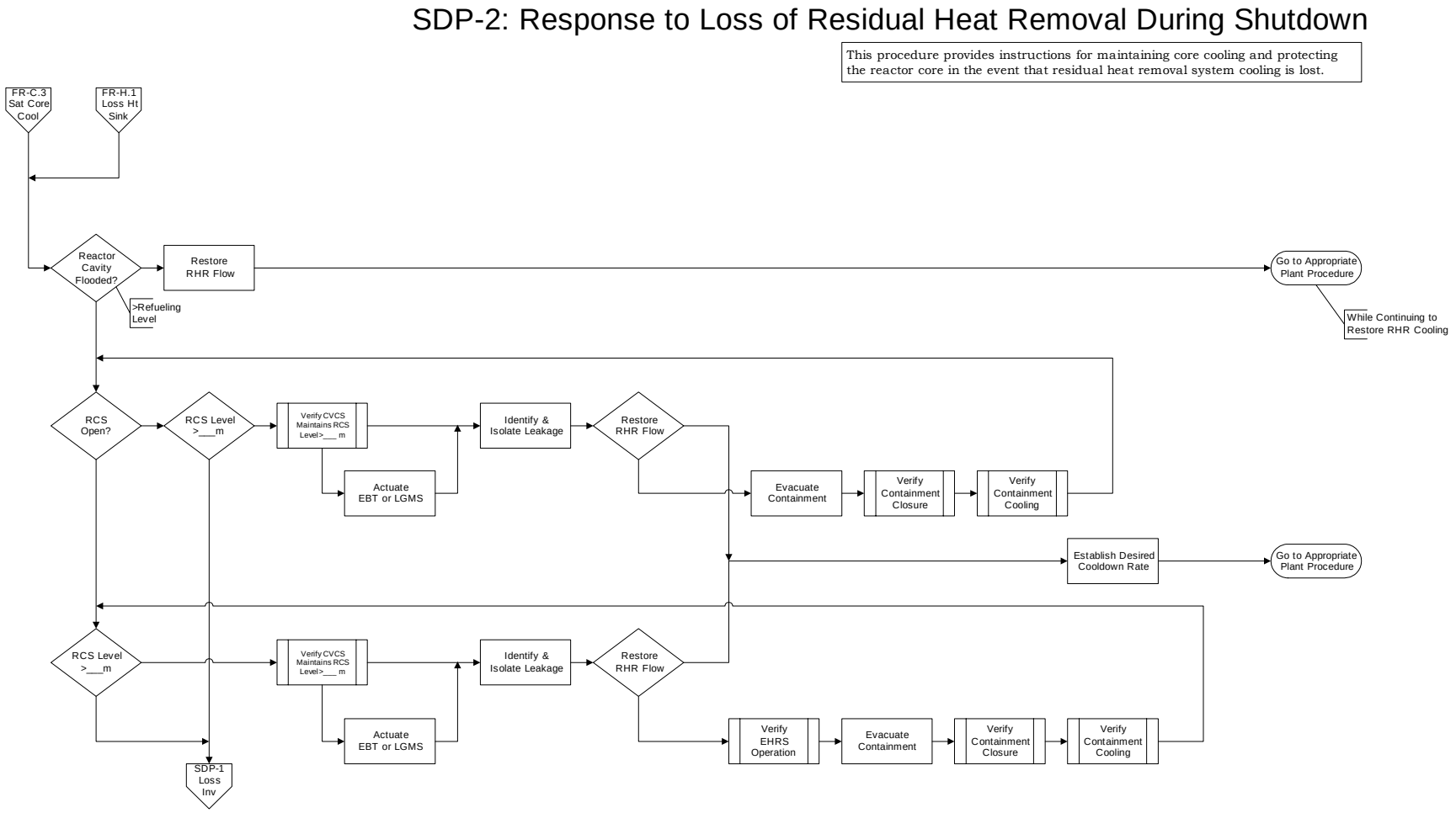


Figure 32: SDP-2, Response to Loss of Residual Heat Removal During Shutdown

SDP-3: Response to High Containment Radiation During Shutdown

This procedure provides instructions to respond to high radiation in containment.

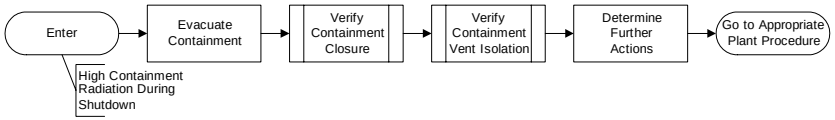


Figure 33: SDP-3, Response to High Containment Radiation During Shutdown

SDP-4: Response to Increasing Nuclear Flux During Shutdown

This procedure provides instructions to respond to increasing nuclear flux during shutdown.

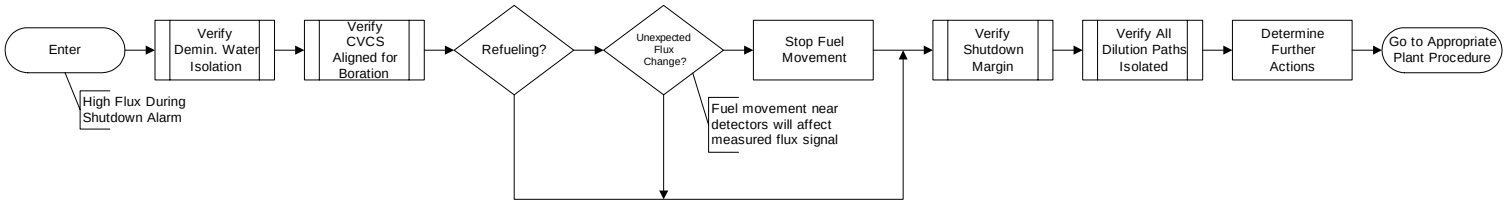


Figure 34: SDP-4, Response to Increasing Nuclear Flux During Shutdown

SDP-5: Response to Cold Overpressure During Shut

This procedure provides instructions to
to an overpressure condition at low tem

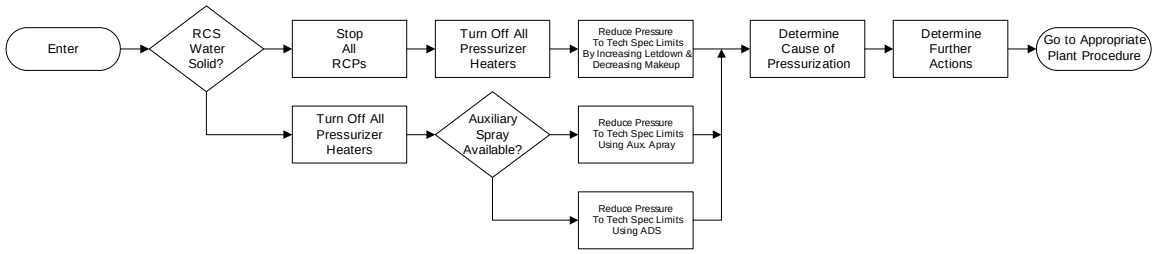


Figure 35: SDP-5, Response to Cold Overpressure During Shutdown

SDP-6: Response to Unexpected RCS Temperature Changes During Shutdown

This procedure provides instructions to respond
to unexpected changes in RCS temperature.

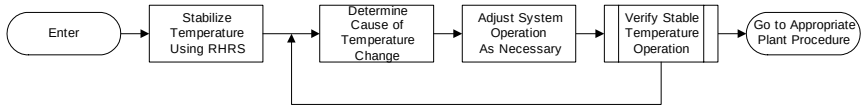


Figure 36: SDP-6, Response to Unexpected RCS Temperature Changes During Shutdown

7. CONCLUSIONS

This report focused the main features of the EPGs and the control room for IPSRs, with particular emphasis on identifying differences and similarities with existing PWRs. In particular, we established the following:

1. The traditional accident categories defined in Reference 5 seem adequate for IRIS. They would probably serve for other IPSRs as well, but the IPSR designers should confirm this.

2. Although the accident categories listed in Reference 5 may serve for IRIS and other IPSRs, the specific accident lists must address the particular characteristics of individual plant designs. The IRIS design eliminates several accidents and reduces the consequences of several others.

3. We looked at the AP1000 ERG development process to determine whether we could use it for IRIS. This process was evolutionary one rather than a revolutionary in the sense that the AP1000 ERGs relied heavily on those developed for the reference plant. We demonstrated that we can use the AP1000 ERGs as a starting point for developing IRIS ERGs; however, the design differences naturally led to ERG differences. In particular, the IRIS Safety-By-Design™ approach eliminated the need for several procedures that would be required for the AP1000 and older type plants.

4. We assume that first IRIS units will use a distributed digital system networked to the control room, and that the control room will feature smart workstations. Existing technology would allow automating operations to a much greater extent than envisioned for AP1000. The decisions to automate particular actions would normally come from economic considerations rather than technological limitations.

5. Normal and emergency operating procedures must reflect the plant design (including multiple units on one site), the size of the site operating staff, and the degree of I&C automation. Traditionally, each reactor has its own operating staff, in part because of the limitations of traditional hard-wired controls. Modern I&C technology removes the technological constraints that lead to dedicated control rooms and operating staffs for each unit, so sharing these becomes technologically feasible.

6. Allowing one control room operating staff to control multiple IRIS units introduces the possibility that they would have to deal with simultaneous emergencies, but passive protections systems that do not require operator actions simplify the staff's response to simultaneous events. Designers should define the credible limits for simultaneous emergencies and design the plant and I&C systems to maintain acceptable operating staff workloads in all cases.

7. We developed EPGs for IRIS, using the AP1000 EPGs as a starting point. These established the major sequences for operator actions[7].

8. Current computer technology provides an excellent base for designing advanced control rooms, and it is difficult to see disadvantages to extending the current advanced control room design philosophy to IRIS.

Although there will be considerable work involved in translating these ideas into detailed designs, we foresee no conceptual difficulties in applying these concepts to IRIS or other IPSRs.

[7] The current state of the IRIS design does not allow including specific component tag numbers in the procedures.

8. REFERENCES

1. Holcomb, D. E. and A. C. Barroso, December 15, 2004. "Collaborative Proposal for the International Nuclear Energy Research Initiative, "Development of Advanced Instrumentation and Control for an Integrated Primary System Reactor."

2. Hayashi, Y., G. Saiu, and R. F. Wright, June 4-8, 2006. "Development of Emergency Response Guidelines (ERPs) for AP1000," Proceedings of ICAAP '06, 61-70.

3. American National Standard Institute, 1973. "Nuclear Safety Criteria for the Design of Stationary PWR Plants," N18.2.

4. Westinghouse Electric Company, March 21, 2003. " IRIS Plant Description Document," WCAP-16062-NP.

5. U.S. Nuclear Regulatory Commission, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)," Regulatory Guide 1.70.

6. Westinghouse Electric Company, July 15, 2003. "IRIS Preliminary Safety Assessment," WCAP-16082-NP.

7. University of Florida, "Flight Control Systems," July 31, 2006. Retrieved from http://www.bme.ufl.edu/research/projects /detail_researchproject.php?RP_id=5 on January 3 2007.

8. Storrick, G. D. and F. Schiavo, STD-ES-04-34, "IRIS Control Systems Conceptual Design," Sep. 2004.

9. Lipner, M. H., R. A. Dudics, J. W. Willis and R. A. Mundy, "Supervisory Sequential Controller Interface system," 2000 ANS/ENS International Meeting, Washington, D.C., November 12-16, 2000.

10. Electric Power Research Institute, March 1999. "Advanced Light Water Reactor Utility Requirements Document," vol. 3 ("ALWR Passive plant"), rev. 8.