

# Final Precursor Analysis

Accident Sequence Precursor Program --- Office of Nuclear Regulatory Research

Ginna	Automatic Reactor Trip and Loss of Offsite Power Due to the August 14, 2003, Transmission Grid Blackout	
Event Date 8/14/2003	LER: 244/03-002	CCDP <sup>1</sup> = $2 \times 10^{-5}$

December 17, 2004

## Event Summary

At 1611 hours on August 14, 2003, Ginna experienced grid instability and a subsequent reactor trip while operating at approximately 100% power. Offsite power was never completely lost to the buses supplying the power block area; however, the operators determined that the offsite power supply was unreliable and manually started and loaded the plant emergency diesel generators (EDGs) onto the emergency buses. The EDGs supplied power to safety-related plant loads until offsite power was deemed stable. Attachment A is a timeline of significant events. (Refs. 1 and 2).

**Cause.** The reactor trip was caused by grid instability associated with the regional transmission system blackout that occurred on August 14, 2003.

**Other conditions, failures, and unavailable equipment.** Both pressurizer power-operated relief valves (PORVs) lifted and reclosed to limit the pressure transient. (Ref. 1).

**Recovery opportunities.** Offsite power was considered stable at 1700 hours. Power from offsite was first restored to an emergency bus at 2108 hours.

## Analysis Results

### • Conditional Core Damage Probability (CCDP)

The CCDP for this event is  $2 \times 10^{-5}$ . The acceptance threshold for the Accident Sequence Precursor Program is a CCDP of  $1 \times 10^{-6}$ . This event is a precursor.

	Mean	5%	95%
Best estimate	$2 \times 10^{-5}$	$2 \times 10^{-6}$	$6 \times 10^{-5}$

<sup>1</sup> For the initiating event assessment, the parameter of interest is the measure of the CCDP. This is the value obtained when calculating the probability of core damage for an initiating event with subsequent failure of one or more components following the initiating event. The reported value is the estimated mean CCDP.

## ● Dominant Sequences

The dominant core damage sequence for this assessment is loss of offsite power (LOOP)/station blackout (SBO) sequences 18-45 (78.9% of the total CCDP). The LOOP and SBO event trees are shown in Figures 1 and 2.

The events and important component failures in LOOP/SBO Sequence 18-45 are:

- loss of offsite power occurs,
- reactor shutdown succeeds,
- emergency power is unavailable,
- auxiliary feedwater fails to provide sufficient flow,
- offsite power is not recovered in 1 hour, and
- an emergency diesel generator is not recovered in 1 hour.

## ● Results Tables

- The CCDP values for the dominant sequences are shown in Table 1.
- The event tree sequence logic for the dominant sequences is presented in Table 2a.
- Table 2b defines the nomenclature used in Table 2a.
- The most important cut sets for the dominant sequences are listed in Table 3.
- Table 4 presents names, definitions, and probabilities of (1) basic events whose probabilities were changed to update the referenced SPAR model, (2) basic events whose probabilities were changed to model this event, and (3) basic events that are important to the CCDP result.

## Modeling Assumptions

### ● Assessment Summary

Due to the unstable power grid, this event was modeled as a LOOP initiating event. Rev. 3.10 (SAPHIRE 7) of the Ginna SPAR model (Ref. 3) was used for this assessment. The specific model version used as a starting point for this analysis is dated December 10, 2004.

Since this event involves unstable offsite power for a significant duration, probabilities of nonrecovery of offsite power at different times into the event are important factors in the estimation of the CCDP.

**Best estimate:** Stable and useable offsite power was available in the switchyard at 1700 hours, about 1 hour into this event. Failure to recover offsite power to plant safety-related loads (if needed because EDGs fail to supply the loads), given recovery of power to the switchyard, could result from (1) operators failing to restore proper breaker line-ups, (2) breakers failing to close on demand, or (3) a combination of operator and breaker failures. The dominant contributor to failure to recover offsite power to plant safety-related loads in this situation is operators failing to restore proper breaker line-ups. This analysis assumed that at least 30 minutes are necessary to restore power to an emergency bus given that

offsite power is available in the switchyard.<sup>2</sup> The time available for operators to restore proper breaker line-ups to prevent core damage is dependent on specific accident sequences and is modeled as such using the SPAR human reliability model (Ref. 4). Assumptions described below, combined with the assumption of offsite power restoration described above, form the bases for the LOOP nonrecovery probabilities.

## ● Important Assumptions

Important assumptions regarding power recovery modeling include the following:

- No opportunity for the recovery of offsite power to safety-related loads is considered for any time prior to power being available in the switchyard.
- At least 30 minutes are required to restore power to emergency loads after power is available in the switchyard.
- SPAR models do not credit offsite power recovery following battery depletion.

The GEM program used to determine the CCDP for this analysis will calculate probabilities of recovering offsite power at various time points of importance to the analysis based on historical data for grid-related LOOPS. In this analysis, this feature was overridden; offsite power recovery probabilities were based on (1) known information about when power was restored to the switchyard and (2) use of the SPAR human error model to estimate probabilities of failing to realign power to emergency buses for times after power was restored to the switchyard.

Attachment B is a general description of analysis of LOOP events in the Accident Sequence Precursor Program. It includes a description of the approach to estimating offsite power recovery probabilities.

## ● Event Tree and Fault Tree Changes

A rule was developed for LOOP/SBO sequence 18-45. After discussion with INEEL, it has been determined that basic event AFW-XHE-XM-FIREW does not apply to short term core damage sequences. The rule is provided below.

```
if AFW-XHE-XM-FIREW then
  DeleteRoot;
endif
```

## ● Basic Event Probability Changes

Table 4 includes basic events whose probabilities were changed to reflect the event being analyzed. The bases for these changes are as follows:

- **Probability of AFW motor-driven pump (MDP) B fails to run (AFW-MDP-FR-AF01B).** Operators caused AFW MDP '1B' to trip while trying to restore to a normal lineup. Therefore, AFW-MDP-FR-AF01B was set to 1.0. This event has minimal effect on the analysis results.

---

<sup>1</sup> Sensitivity analysis has shown that the difference between 30 and 60 minutes restoration time has minimal effect on the results.

- ***Probability of failure to recover offsite power in 1 hour (OEP-XHE-XL-NR01H).*** During the event, reliable offsite power was available in the switchyard 1 hour into the event. Therefore, the operators did not have sufficient time to recover offsite power to the vital safety buses. Using the SPAR human error model to determine the value (see Attachment C), OEP-XHE-XL-NR01H was set to TRUE.
- ***Probability of failure to recover offsite power prior in 2 hours (OEP-XHE-XL-NR02H).*** During the event, reliable offsite power was available in the switchyard 1 hour into the event. Therefore, the operators had 1 hour to recover offsite power to the vital safety buses. Using the SPAR human error model to determine the value (see Attachment C), OEP-XHE-XL-NR02H was set to  $1.0 \times 10^{-2}$ .
- ***Probability of failure to recover offsite power prior in 3 hours (OEP-XHE-XL-NR03H).*** During the event, reliable offsite power was available in the switchyard 1 hour into the event. Therefore, the operators had 2 hours to recover offsite power to the vital safety buses. Using the SPAR human error model to determine the value (see Attachment C), OEP-XHE-XL-NR03H was set to  $1.0 \times 10^{-2}$ .
- ***Probability of failure to recover offsite power prior in 4 hours (OEP-XHE-XL-NR04H).*** During the event, reliable offsite power was available in the switchyard 1 hour into the event. Therefore, the operators had 3 hours to recover offsite power to the vital safety buses. Using the SPAR human error model to determine the value (see Attachment C), OEP-XHE-XL-NR04H was set to  $1.0 \times 10^{-3}$ .
- ***Probability of failure to recover offsite power prior in 6 hours (OEP-XHE-XL-NR06H).*** During the event, reliable offsite power was available in the switchyard 1 hour into the event. Therefore, the operators had 5 hours to recover offsite power to the vital safety buses. Using the SPAR human error model to determine the value (see Attachment C), OEP-XHE-XL-NR06H was set to  $1.0 \times 10^{-3}$ .
- ***Probability of PORVs/SRVs to open during LOOP (PPR-SRV-CO-L).*** During this event, both of the pressurizer's PORVs lifted to limit the pressure transient. Therefore, PPR-SRV-CO-L was set to TRUE.
- ***Probability of PORVs/SRVs to open during SBO (PPR-SRV-CO-SBO).*** During this event, both of the pressurizer's PORVs lifted to limit the pressure transient. Therefore, PPR-SRV-CO-SBO was set to TRUE.
- ***Probability of diesel generators failing to run (ZT-DGN-FR-L).*** The default diesel generator mission times were changed to reflect the actual time offsite power was restored to the first vital bus (approximately 5 hours). Since the overall fail-to-run is made up of two separate factors, the mission times for the factors were set to the following: ZT-DGN-FR-E = 1 hour (base case value) and ZT-DGN-FR-L = 4 hours.
- ***Probability of auxiliary feedwater turbine-driven pump failing to run (ZT-TDP-FR-L).*** Since the AFW TDP is the only ac-power-independent pump in the AFW system, the AFW TDP mission time was set to the actual time that offsite power was restored to the second vital bus (approximately 5 hours). Since the overall fail-to-run is made up of two separate factors, the mission times for the factors were set

to the following: ZT-TDP-FR-E = 1 hour (base case value) and ZT-TDP-FR-L = 4 hours.

## References

1. Licensee Event Report 244/03-002, Revision 0, *Major Power Grid Disturbance Causes Loss of Electrical Load and Reactor Trip*, event date August 14, 2003 (ADAMS Accession No. ML0328904410).
2. NRC Region 1 Grid Special Report, October 15, 2003 (ADAMS Accession No. ML0324102160).
3. R. F. Buell and J. K. Knudsen , *Standardized Plant Analysis Risk Model for Ginna (ASP PWR B)*, Revision 3.10, December 2004.
4. D. Gertman, et al., *SPAR-H Method*, INEEL/EXT-02-10307, Draft for Comment, November 2002 (ADAMS Accession No. ML0315400840).

**Table 1. Conditional probabilities associated with the highest probability sequences.**

Event tree name	Sequence no.	Conditional core damage probability (CCDP) <sup>1</sup>	Percentage contribution
LOOP/SBO	18-45	$1.5 \times 10^{-5}$	78.9%
<b>Total (all sequences)<sup>2</sup></b>		<b><math>1.9 \times 10^{-5}</math></b>	

1. Values are point estimates. (File name: GEM 244-03-002 12-13-2004.wpd)

2. Total CCDP includes all sequences (including those not shown in this table).

**Table 2a. Event tree sequence logic for the dominant sequences.**

Event tree name	Sequence no.	Logic ("I" denotes success; see Table 2b for top event names)
LOOP/SBO	18-45	/RPS, EPS, AFW-B, OPR-01H, DGR-01H

**Table 2b. Definitions of fault trees listed in Table 2a.**

AFW-B	NO OR INSUFFICIENT AFW FLOW
DGR-01H	OPERATOR FAILS TO RECOVER AN EDG IN 1 HOUR
EPS	EMERGENCY POWER SYSTEM FAILURES
OPR-01H	OFFSITE POWER RECOVERY IN 1 HOUR
RPS	REACTOR FAILS TO TRIP DURING LOOP

**Table 3. Conditional cut sets for dominant sequences.**

CCDP <sup>1</sup>	Percent contribution	Minimal cut sets <sup>2</sup>	
Event Tree: LOOP, Sequence 18-45			
1.4 x 10 <sup>-6</sup>	9.6	EPS-XHE-XL-NR01H EPS-DGN-CF-FRAB	AFW-XHE-XO-TDP
8.6 x 10 <sup>-7</sup>	5.8	EPS-XHE-XL-NR01H EPS-DGN-CF-FRAB	AFW-XHE-XM-HVAC
8.6 x 10 <sup>-7</sup>	5.8	EPS-XHE-XL-NR01H EPS-DGN-CF-FRAB	AFW-TDP-FS-TDP
8.1 x 10 <sup>-5</sup>	Total (all cut sets) <sup>3</sup>		

1. Values are point estimates.

2. See Table 4 for definitions and probabilities for the basic events.

3. Totals include all cut sets (including those not shown in this table).

**Table 4. Definitions and probabilities for modified or dominant basic events.**

Event name	Description	Probability/ frequency	Modified
AFW-MDP-FR-AF01B	AFW MOTOR-DRIVEN PUMP 1B FAILS TO RUN	1.0	Yes <sup>1</sup>
AFW-TDP-FS-TDP	AFW TURBINE-DRIVEN PUMP FAILS TO START	$6.0 \times 10^{-3}$	No
AFW-XHE-XM-HVAC	OPERATOR FAILS TO RESTART AFW VENTILATION	$6.0 \times 10^{-3}$	No
AFW-XHE-XO-TDP	FAILURE TO CONTROL AFW TDP AND ALIGN FW COOLING	$1.0 \times 10^{-2}$	No
EPS-DGN-CF-FRAB	CCF OF DIESEL GENERATORS 'A' AND 'B' TO RUN	$1.7 \times 10^{-4}$	Yes <sup>1</sup>
EPS-XHE-XL-NR01H	OPERATOR FAILS TO RECOVER AN EDG IN 1 HOUR	$8.4 \times 10^{-1}$	No
IE-LOOP	LOSS OF OFFSITE POWER (INITIATING EVENT)	1.0	Yes <sup>2</sup>
OEP-XHE-XL-NR01H	OPERATOR FAILS TO RECOVER OFFSITE POWER WITHIN 1 HOUR	TRUE	Yes <sup>3</sup>
OEP-XHE-XL-NR02H	OPERATOR FAILS TO RECOVER OFFSITE POWER WITHIN 2 HOURS	$1.0 \times 10^{-2}$	Yes <sup>3</sup>
OEP-XHE-XL-NR03H	OPERATOR FAILS TO RECOVER OFFSITE POWER WITHIN 3 HOURS	$1.0 \times 10^{-2}$	Yes <sup>3</sup>
OEP-XHE-XL-NR04H	OPERATOR FAILS TO RECOVER OFFSITE POWER WITHIN 4 HOURS	$1.0 \times 10^{-3}$	Yes <sup>3</sup>
OEP-XHE-XL-NR06H	OPERATOR FAILS TO RECOVER OFFSITE POWER WITHIN 6 HOURS	$1.0 \times 10^{-3}$	Yes <sup>3</sup>
PPR-SRV-CO-L	PORVs/SRVs OPEN DURING LOOP	TRUE	Yes <sup>1</sup>
PPR-SRV-CO-SBO	PORVs OPEN DURING SBO	TRUE	Yes <sup>1</sup>
ZT-DGN-FR-L	EDG FAILS TO RUN (LONG TERM)	$3.2 \times 10^{-3}$	Yes <sup>4</sup>
ZT-DGN-FR-L	AFW TDP FAILS TO RUN (LONG TERM)	$2.0 \times 10^{-4}$	Yes <sup>4</sup>

1. Event changed to reflect the condition being analyzed. See report and Basic Event Probability Changes for further details.

2. Initiating event assessment– all other initiating event frequencies set zero.

3. Evaluated per the SPAR-H method (Ref. 4). See report and Attachment C for further details.

4. Changed mission times to correspond to the time offsite power was restored to the first and second vital busses. See report and Basic Event Probability Changes for further details.

## Attachment A Event Timeline

**Table A.1 Timeline of significant events.**

Time <sup>1</sup>	Event
1611	Reactor trips due to grid instability. Offsite power was not lost, but voltage was unstable
1614	EDGs are manually started and loaded to power the emergency buses
1700	Stable power available in switchyard
2108	First emergency bus is switched to offsite power source
2108	Second emergency bus is switched to offsite power source

1. All times are on August 14, 2003.



## Attachment B

### LOOP Analysis Procedure

This procedure is not intended to stand alone; instead it is intended to augment *ASP Guideline A: Detailed Analysis*<sup>1</sup>. LOOP event analyses are a type of initiating event assessment as described in ASP Guideline A. Specific analysis steps that are unique to ASP analysis of LOOP events are included here.

**1. Determine significant facts associated with the event.**

- 1.1 Determine when the LOOP occurred.
- 1.2 Determine when stable offsite power was first available in the switchyard.
- 1.3 Determine when offsite power was first restored to an emergency bus.
- 1.4 Determine when offsite power was fully restored (all emergency buses powered from offsite, EDGs secured).
- 1.5 Identify any other significant conditions, failures, or unavailabilities that coincided with the LOOP.

**2. Model power recovery factors associated with the best estimate case and any defined sensitivity cases.**

- 2.1 For the best estimate case, the LOOP duration is the time between the occurrence of the LOOP and the time when stable power was available in the switchyard plus the assumed time required to restore power from the switchyard to emergency buses. Attachment C documents the probabilistic analysis of power recovery factors for the best estimate case analysis.
- 2.2 If EDGs successfully start and supply emergency loads, plant operators do not typically rush to restore offsite power to emergency buses, preferring to wait until grid stability is more certain. Therefore, a typical upper bound sensitivity case considers the LOOP duration as the time between the occurrence of the LOOP and the time when offsite power was first restored to an emergency bus. Attachment C documents the probabilistic analysis of power recovery factors for the sensitivity case analysis.

**3. Model event-specific mission durations for critical equipment for the best estimate case and any defined sensitivity cases. (For most equipment, SPAR model failure probabilities are not functions of defined mission durations and are therefore not affected by this analysis step. Notable exceptions include EDGs and, for PWRs, turbine-driven auxiliary feedwater pumps.)**

- 3.1 For the best estimate case, mission durations are set equal to the assumed LOOP duration as defined in Step 2.1 above.
- 3.2 For a typical upper bound sensitivity case, mission durations are set equal to the time between the occurrence of the LOOP and the time when offsite power was fully restored to all emergency buses. (Note these mission durations are longer than the assumed LOOP duration defined in Step 2.2 above; they are intended to represent the longest possible mission duration for any critical equipment item.)

---

<sup>1</sup> ASP Guideline A: Detailed Analysis, U.S. Nuclear Regulatory Commission.

## **Attachment C**

### **Power Recovery Modeling**

- **Background**

The time required to restore offsite power to plant emergency equipment is a significant factor in modeling the CCDDP given a LOOP. SPAR LOOP/SBO models include various sequence-specific ac power recovery factors that are based on the time available to recover power to prevent core damage. For a sequence involving failure of all of the cooling sources, only about 30 minutes would be available to recover power to help avoid core damage. On the other hand, sequences involving successful early inventory control and decay heat removal, but failure of long-term decay heat removal, would accommodate several hours to recover ac power prior to core damage.

In this analysis, offsite power recovery probabilities are based on (1) known information about when power was restored to the switchyard and (2) estimated probabilities of failing to realign power to emergency buses for times after offsite power was restored to the switchyard. Power restoration times were reported by the licensee in the LER and in response to the questionnaire that was conducted by the NRC Regional Office. The time used is the time at which the grid operator informed the plant that power was available to the switchyard (with a load limit). Although the load limit was adequate to energize plant equipment and, if necessary, prevent the occurrence of an SBO sequence, plant operators did not immediately load safety buses onto the grid. This ASP analysis does not consider the possibility that grid power would have been unreliable if that power were immediately used.

Failure to recover offsite power to plant safety-related loads (if needed because EDGs fail to supply the loads), given recovery of power to the switchyard, could result from (1) operators failing to restore proper breaker line-ups, (2) breakers failing to close on demand, or (3) a combination of operator and breaker failures. The dominant contributor to failure to recover offsite power to plant safety-related loads in this situation is operators failing to restore proper breaker line-ups. The SPAR human error model (ref.) was used to estimate nonrecovery probabilities as a function of time following restoration of offsite power to the switchyard. The best estimate analysis assumes that at least 30 minutes are necessary to restore offsite power to emergency buses given offsite power is available in the switchyard.

- **Human Error Modeling**

The SPAR human error model generally considers the following three factors:

- Probability of failure to diagnose the need for action
- Probability of failure to successfully perform the desired action
- Dependency on other operator actions involved in the specific sequence of interest

This analysis assumes no probability of failure to diagnose the need to recover ac power and no dependency between operator performance of the power recovery task and any other task the operators may need to perform. Thus, each estimated ac power nonrecovery probability is based solely on the probability of failure to successfully perform the desired action.

The probability of failure to perform an action is the product of a nominal failure probability ( $1.0 \times 10^{-3}$ ) and the following eight performance shaping factors (PSFs):

- Available time
- Stress
- Complexity
- Experience/training
- Procedures
- Ergonomics
- Fitness for duty
- Work processes

For each ac power nonrecovery probability, the PSF for available time is assigned a value of 10 if the time available to perform the action is approximately equal to the time required to perform the action, 1.0 if the time available is between 2 and 4 times the time required, and 0.1 if the time available is greater than or equal to 5 times the time required. If the time available is inadequate (i.e., less than the time to restoration of power to the switchyard plus 30 minutes for the best estimate), the ac power nonrecovery probability is 1.0 (TRUE).

The PSF for stress is assigned a value of 5 (corresponding to extreme stress) for all ac power nonrecovery probabilities. Factors considered in assigning this PSF include the sudden onset of the LOOP initiating event, the duration of the event, the existence of compounding equipment failures (ac power recovery is needed only if one or more emergency buses are not powered by EDGs), and the existence of a direct threat to the plant.

For all of the ac power nonrecovery probabilities, the PSF for complexity is assigned a value of 2 (corresponding to moderately complex) based on the need for multiple breaker alignments and verifications.

For all of the ac power nonrecovery probabilities, the PSFs for experience/training, procedures, ergonomics, fitness for duty, and work processes are assumed to be nominal (i.e., are assigned values of 1.0).

## ● Results

Table C.1 presents the calculated values for the ac power nonrecovery probabilities used in the best estimate analysis.

**Table C.1 AC Power Nonrecovery Probabilities**

Nonrecovery Factor	Nominal Value	PSF		Nonrecovery Probability
		Time Available	Product of All Others	
OEP-XHE-XL-NR01H	$1.0 \times 10^{-3}$	Inadequate	10	TRUE
OEP-XHE-XL-NR02H	$1.0 \times 10^{-3}$	1	10	$1.0 \times 10^{-2}$
OEP-XHE-XL-NR03H	$1.0 \times 10^{-3}$	1	10	$1.0 \times 10^{-2}$
OEP-XHE-XL-NR04H	$1.0 \times 10^{-3}$	0.1	10	$1.0 \times 10^{-3}$
OEP-XHE-XL-NR06H	$1.0 \times 10^{-3}$	0.1	10	$1.0 \times 10^{-3}$

## Attachment D

## Response to Comments

### 1. **Comment from Bob Clark, Licensing Project Manager for Ginna - Feedwater control system failure (Ref. D.1)**

“There was a failure in the digital feedwater control system at Ginna during the grid event that you may want to consider in the SPAR model. Westinghouse plants have a control signal to close the main feedwater regulating valves (MFRVs) after a reactor trip when the RCS average temperature drops several degrees below the normal value. This MFRV closure failed at Ginna due to voltage fluctuations which caused the digital feedwater control system to switch to manual. Both SGs filled up to the high-high level setpoint. At that point a safety-related signal closed the MFRVs. This is described in the Ginna LER. AFW was available to both SGs. The primary concern would be an overfill of the SGs, increasing the probability of a steam line break (for example, a SG safety valve opens on high SG pressure, and a slug of water gets accelerated through it, causing it to fail open). However, since the high-high level terminated the overfill, and the setpoint is designed to protect against overfill, it may not be that significant in the risk model.”

**Response:** The analysis gave no credit for MFW working (i.e., it was slightly conservative). Overfilling a steam generator is not addressed by the SPAR model. It is probably not risk significant, as stated above in the comment.

### 2. **Comment from Kenneth Kolaczyk, Ginna SRI - Feedwater control system failure**

“The description of the Ginna event as outlined on page two of the forwarding memo, and page five of attachment one, seems to indicate that the ‘B’ Motor Driven Auxiliary Feedwater (MDAFW) pump did not start and operate as designed following the trip. This is incorrect, as the pump did operate as designed. It was damaged only after the operators failed to correctly align the AFW system when they were restoring it to a more “normal” lineup following the trip.

I am not sure if this fact will effect the results of your analysis. If you want additional information regarding the particulars of the error, see NRC inspection report 50-244/2003-006.”

**Response:** Even though the “B” motor-driven AFW pump failed due to operator error, it did fail to complete its mission time, and therefore it is modeled as failed to run. This had a negligible effect on the quantitative result.

### **References:**

1. Ginna feed reg valve failure during 8/14/03 event, e-mail from John P. Boska, Licensing Project Manager (Hope Creek), U.S. Nuclear Regulatory Commission, to Gary Demoss, U.S. Nuclear Regulatory Commission, March 11, 2004.

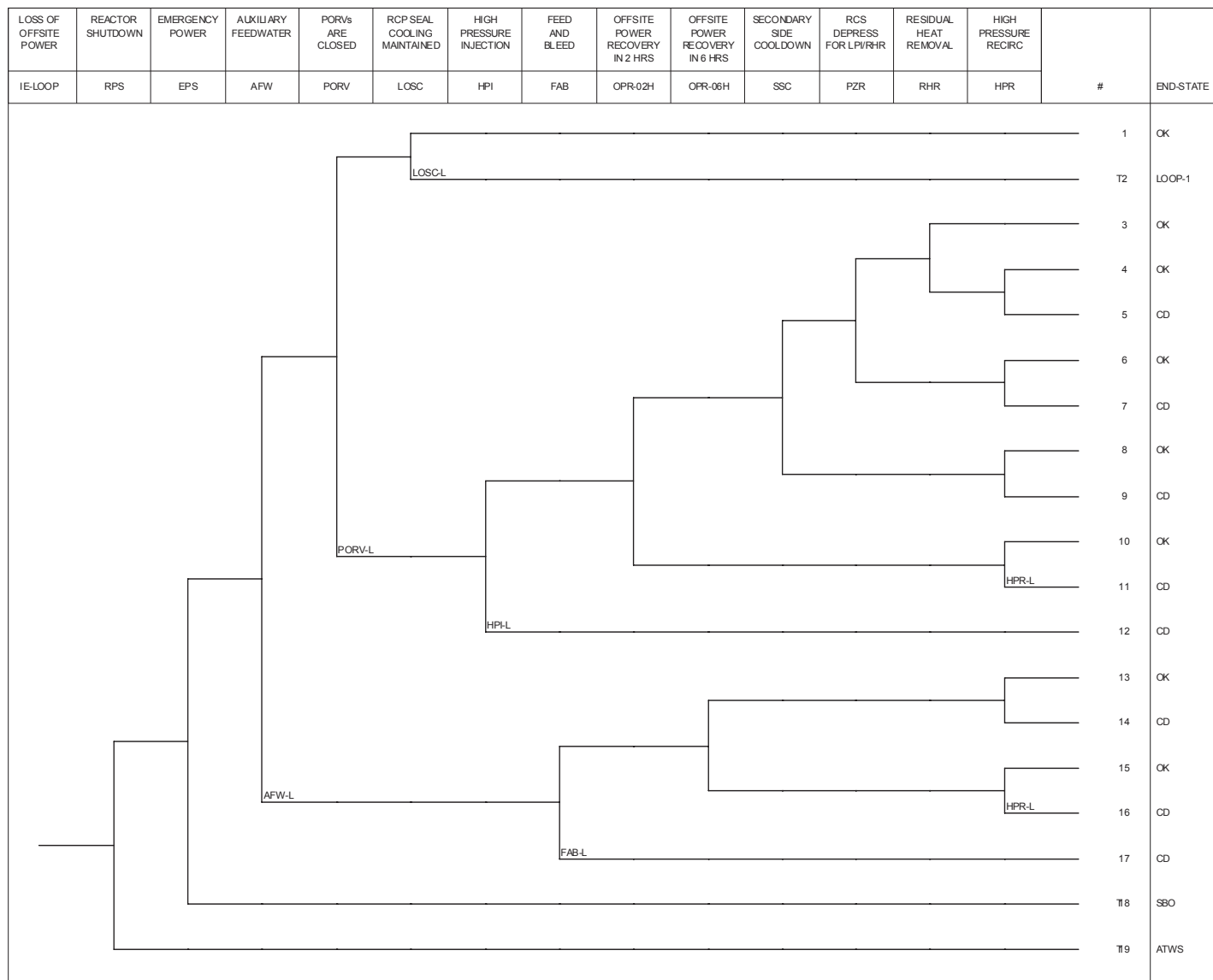


Figure 1: Ginna LOOP event tree.

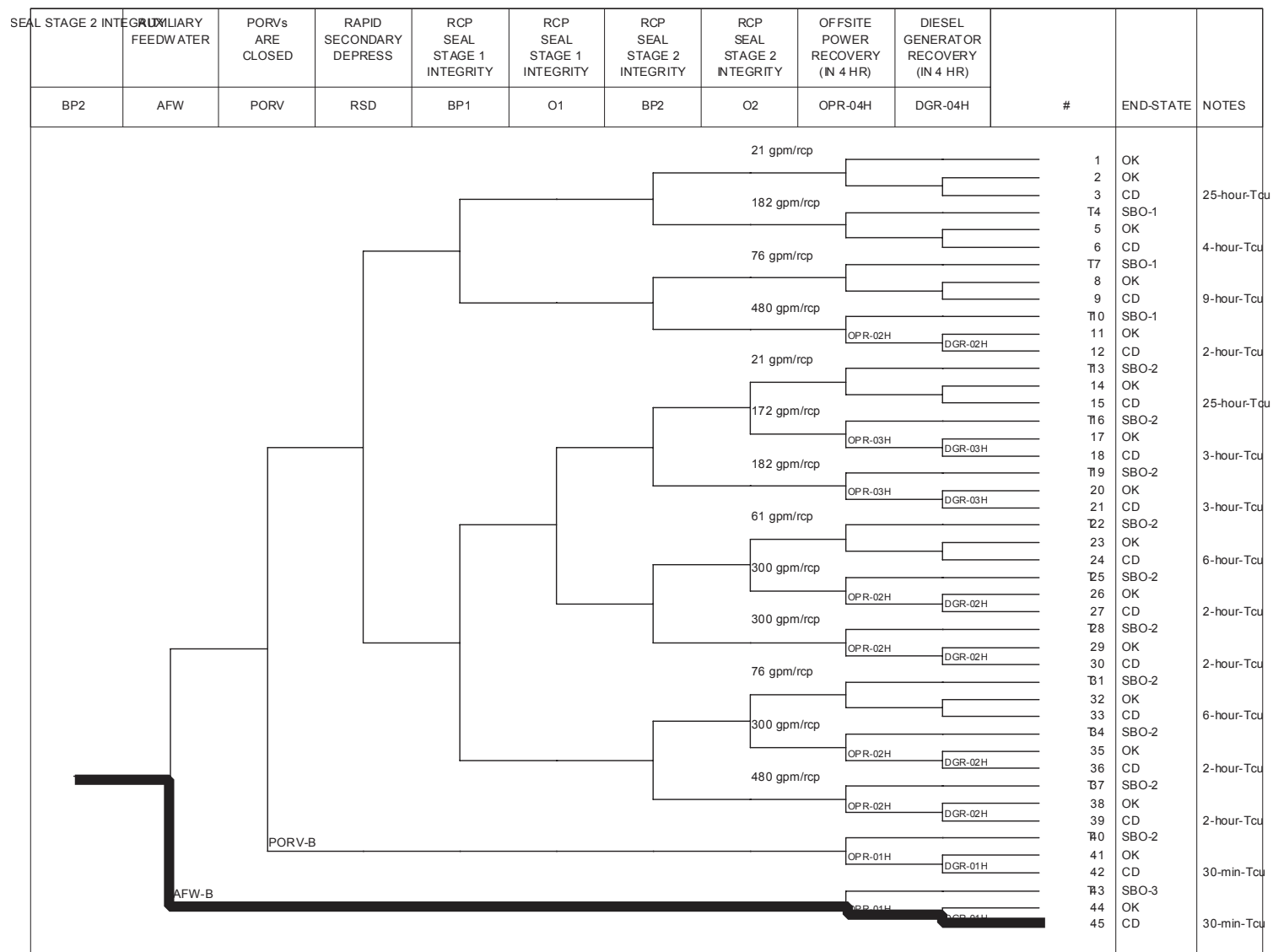


Figure 2: Ginna SBO event tree with dominant sequence highlighted.