Two Full Capacity Generators – Why is the Calculated Emergency Power System PFD so High?

Arthur M. (Art) Dowell, III, PE
Process Improvement Institute, Inc.
2437 Bay Area Blvd, PMB 260
Houston, TX 77058-1519
Adowell@piii.com

Prepared for Presentation at
American Institute of Chemical Engineers
2020 Spring Meeting and 16th Global Congress on Process Safety
Houston, TX
August 19, 2020

Two Full Capacity Generators – Why is the Calculated Emergency Power System PFD so High?

Arthur M. (Art) Dowell, III, PE
Process Improvement Institute, Inc.
2437 Bay Area Blvd, PMB 260
Houston, TX 77058-1519
Adowell@piii.com

Keywords: backup generator, fault tree analysis, common cause, LOPA, protection layer, probability of failure on demand (PFD), integrity management

Abstract

The probability of failure on demand (PFD) for an emergency generator system is important when electrical power is needed to protect humans from harm or to prevent equipment damage. Emergency lighting is needed for emergency responders during a power outage. Pumps, compressors, and blowers need to operate during the power outage to safely shut down the facility.

To evaluate the PFD for an emergency power system, we must consider more than just two generators. We must also consider all the components for the generator fuel, the generator controls, the transfer switches, and the circuit breakers in the feeders to the emergency load. In addition, it is important to consider the capability of the weekly, monthly, semiannual, annual, and four-year inspections and proof test to detect all the failure modes that can prevent the generator system from operating correctly. There may be many common cause events that can prevent both generators from starting or running. For example, the fuel storage system, the generator control system including over-voltage and overload protection, the downstream electrical system including the transfer switches and circuit breakers may have single points of failure affecting the power supply from both generators. In addition, human action during maintenance and testing introduce points of failure, such as leaving the transfer switches in test mode instead of automatic. While the emergency power system may be designed and operated according to NFPA 110, it is critical to evaluate and eliminate single points of failure. The paper will suggest opportunities to provide redundancy, to manage human error, and to improve inspections and proof testing to detect more failure modes.

1 Introduction

For some facilities, emergency backup electrical power is needed to protect humans from harm or to prevent equipment damage during a power outage. Emergency lighting is needed for emergency responders during a power outage. Pumps, compressors, and blowers need to operate during the power outage to shut down the facility safely. A facility may begin to use LOPA (layer of protection analysis) to evaluate scenarios with power failure as an initiating cause and with consequences of human harm or equipment damage. Emergency backup electrical power may be considered as part of a protection layer in these two LOPA scenarios. Note that each protection layer in a LOPA scenario must be independent of the initiating cause and independent of any other protection layers [1].

For illustrative purposes, consider a facility where emergency backup electrical power is needed to protect personnel from harm (NFPA Level 1) [2]. The facility had two diesel driven generators (A and B), each capable of the full emergency backup power load.

Each generator had its own day fuel tank. Both generator day tanks were supplied from a large common storage tank. There were two independent electrically driven fuel pumps, each supplying the day tank for each generator engine. However, both fuel pumps were supplied by a single circuit from a single UPS system.

Each generator had two batteries for starting, two starters, and one fuel pump.

The control logic to start each generator and to detect various failures for each generator consisted of a cabinet with physical relays.

The generators were tested by running weekly. A full functional test of the generator control system was conducted every four years with an artificial load.

At first glance, it might appear the PFD for emergency power should be fairly low because of the redundant generators, the redundant batteries and starters. But a review of the emergency power system (EPS) quickly found a number of devices and systems that were common to both the A and the B generator systems. It was not possible to use a generic PFD value from industry data sources, such as [1, 3]. It was necessary to conduct a fault tree analysis to determine the PFD.

2 Fault Tree Analysis

The top event for the fault tree was EPS (emergency power system) Power to Users for the Required Time (fails). The gates to the top event included Fuel, Generator Power (Gen A AND Gen B), or Tie between Gen A and Gen B (Figure 1). Each generator was then modeled as Starting Issues OR Electrical Issues (Figure 2 and Figure 3). The tie model includes the applicable circuit breakers, coils, and relays to switch the load between Gen A and Gen B, if required by a problem on either generator. Industry guidance documents were used for the techniques to develop the tree [3, 4].

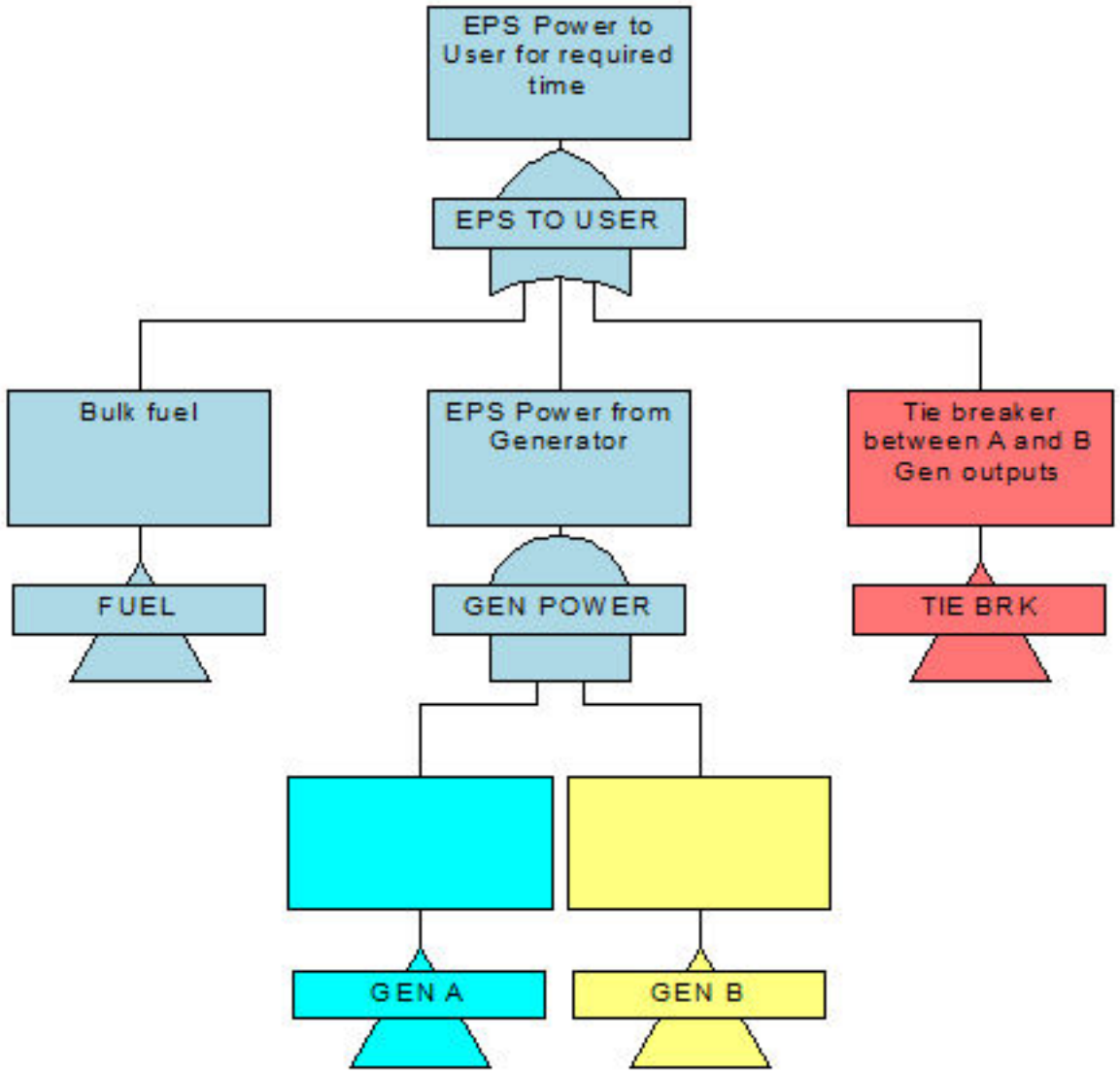

Figure 1: Top Level Fault Tree

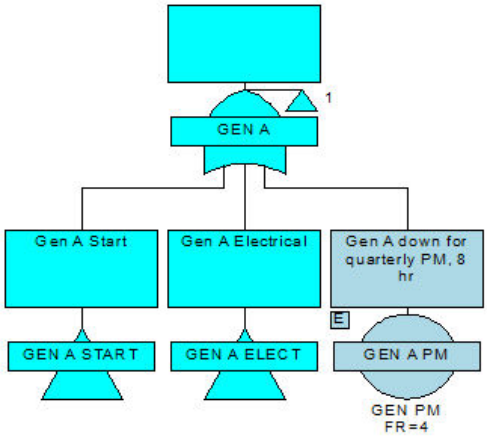

Figure 2: Generator A Sub-Tree

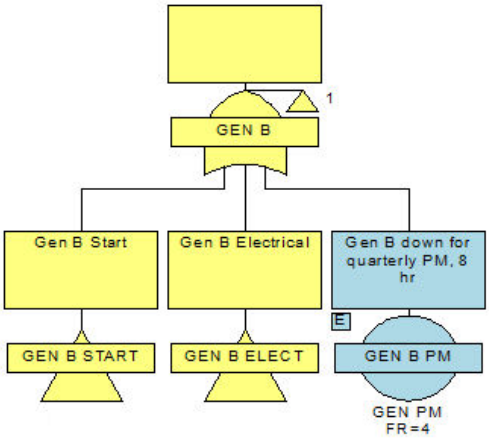

Figure 3: Generator B Sub-Tree

The probability of failure on demand for the system described above is $3x10^{-1}$ (0.3) for a four-year proof test interval. For a one-year proof test interval, the PFD would be $1x10^{-1}$ (0.1). To put these numbers in perspective, 3 times out of 10 power failures, the EPS would fail to provide power (four-year test interval). For a one-year test interval, 1 time out of 10 power failures the EPS would fail. Surely a system with redundancy, weekly test runs, and annual proof tests should give a lower PFD. Why not?

The culprits are common cause, weekly test run coverage, a large number of relays in the control circuits, and a four-year full functional proof test interval.

2.1 Common Cause

There are many common cause events that affect both the Generator A and Generator B systems. That is, a single event disables electrical power to users from both generators.

When building the fault tree, as when doing LOPA, it is critical to identify common causes that can affect multiple branches of the tree; common cause events (or "multiple occurring events" [3]) must be shown with the same label wherever they occur in the tree. Examples of common cause events include components of redundant systems made by the same manufacturer and serviced by the same technicians, such as batteries, engines, generators, alternators, starters, fuel pumps.

When evaluating the minimum cut sets for the fault tree, it is also critical to ensure that common cause events are correctly identified. When calculating the PFD, it is also critical to ensure that the hand calculation or the software calculation includes each common cause event failure rate correctly.

2.1.1 Bulk Fuel System

The bulk fuel system supplies both generators. If the bulk fuel tank is contaminated – for example, with water or gasoline – both generator diesel engines will be unable to run. If the bulk tank runs out of fuel (caused by not ordered, not delivered, level indicator reading higher than actual,

operator error reading level), both generators go down. Typical cross checks of the tank level depend on the same devices and people that caused the problem. Thus, the bulk fuel system is shown as an input to the top event in Figure 1.

2.1.2 Transfer Switches

In this illustrative system, there are six transfer switches to switch portions of the load from maintenance supplied to the EPS. If any transfer switch fails, the full load is not supplied from the EPS and potential human harm is possible during the shutdown.

2.1.3 Human Errors

There are several timers and voltage sensors that must be adjusted by technicians. These devices are electromechanical in design and require calibration against an external timer or a voltage source. EPS power failures have been observed from the timer or voltage sensor left in an incorrect position.

Additionally, there are the well-known human errors of leaving the EPS switch in "Test" or "Mains" instead of "Auto" position.

2.1.4 Common Cause Failures of Redundant Equipment

Even though each generator has redundant batteries and redundant starters (and there are redundant engines/generators) the redundant equipment is subject to common cause failures due to manufacturing defects, environmental damage, mis-calibration, or incorrect maintenance or repair. Various equipment items for Gen A are probably made by the same manufacturers that made the same equipment items on Gen B. The two gensets are in the same environment and are maintained by the same technicians.

In this fault tree, based on the author's experience, the failure rate for common cause events for redundant devices was estimated at 10% (β factor) of the failure rate for one device.

2.2 Weekly Test Run Coverage

While the weekly test run of each genset can detect a number of failure causes (which then can be repaired), the weekly test run cannot detect all the failures of the redundant equipment, such as batteries and starters. If the engine starts, at least one of the two batteries is functional, but we don't know the status of the other battery. Likewise, if the engine starts, at least one starter is functional, but we don't know the status of the other starter. More time-consuming, detailed tests -- potentially requiring lifting wires -- would be required, introducing errors for wires not reconnected.

2.3 Large Number of Relays in the Control Circuit

There are a large number of physical relays in the control circuit. The bane of relays is the potential for loose wires which can cause spurious trips in de-energize to trip circuits. The author has witnessed trips caused by opening or closing the cabinet door on a relay system.

The practice of many facilities is to tighten relay wiring connections during turnarounds or shutdowns. It is reported that a number of loose connections are found in the first turnaround and a reduced number of loose connections (not the same ones) are found in the following turnarounds.

2.4 "Safe" Failures of Protective Equipment

The protective features of the control circuit include detection of electrical faults, bus failure, and voltage failure, generator trip, and engine failure. The associated sensors and relays can fail in such a way to detect falsely a condition requiring a trip or to act falsely when there is no trip condition. Such failures cause a generator trip.

Additionally, the downstream EPS circuits have several circuit breakers that can cause failures of the EPS power to the users.

3 Recommendations to Reduce PFD

The recommendations to reduce probability of failure on demand for the generator system focus on reducing common cause failures where possible, improving weekly and monthly test coverage, increasing the frequency of full functional proof tests, replacing the obsolete relay cabinet with a safety-rated PLC, and minimizing the effect of "safe" failures of protective equipment.

3.1 Reduce or Eliminate Common Cause and Single Points of Failure

3.1.1 Bulk Fuel System

Evaluate the procedures for receiving fuel deliveries to ensure that the correct fuel is delivered. Evaluate the procedures for checking the fuel level in the bulk fuel tank to avoid human error in ordering fuel delivery. Provide redundant measurement of the bulk fuel tank level with cross check.

Supply EPS power to each fuel transfer pump from separate UPS systems (with battery backup).

3.1.2 Transfer Switches

Evaluate how to reduce the PFD of the transfer switches, for example, by more frequent testing if possible. Consider if diagnostics can be developed to assess the health of the transfer switches between tests.

3.1.3 Human Errors

Reduce human errors during adjustments and calibration by replacing the electromechanical timers with a safety-rated PLC control system. Stagger maintenance and calibration between the two generator systems [5].

Provide procedures, cross checks, and alarms to avoid the well-known human errors of leaving the EPS switch in "Test" or "Mains" instead of "Auto" position.

3.1.4 Common Cause Failures of Redundant Equipment

Evaluate potential common cause failures that can disable similar devices on each of the two generator systems. Where possible, eliminate those common cause failures due to manufacturing defects, or environmental damage. To reduce common cause failures from maintenance, repair, or mis-calibration, stagger the maintenance and calibration between the two generator systems [4].

3.2 Weekly Test Run Coverage

Evaluate options to improve the weekly test run coverage of detecting failure causes which can then be repaired. For example, evaluate options to improve diagnostic capability for the redundant batteries and redundant starters during the weekly test.

3.3 Large Number of Relays in the Control Circuit

Replace the large number of physical relays in the control circuit cabinet with a safety-rated PLC system to reduce the number of wiring connections.

The reduction in PFD by replacement of the obsolete control circuit cabinet with a safety rated PLC has not yet been calculated.

3.4 "Safe" Failures of Protective Equipment

Evaluate the design of protective features of the control circuit to reduce the frequency of spurious (safe) trips.

Evaluate the reliability of the circuit breakers in the downstream EPS circuits to determine if the reliability can be improved at reasonable cost.

3.5 Increase the Frequency of the Full Functional Test of the Generator System

Increase the frequency of the full functional test of the generator system and its controls from the current once every four years to annual. This change reduces the PFD by a factor of three.

Design the equipment and the test procedures to avoid the use of jumpers and to avoid lifting wires during the tests. Using jumpers and lifting wires during the test has the potential to leave the equipment in a degraded mode where it fails to operate on demand.

4 Maintaining EPS Integrity

As the recommendations for the EPS are analyzed, designed, installed, commissioned, maintained, and eventually decommissioned, it is vital that the PFD (average) is maintained below the value calculated by the FTA. To accomplish this goal, the facility must use a management system to ensure that the integrity of the EPS is maintained throughout its life cycle. The management system ensures the organization is committed to process safety, including process safety culture, compliance with standards, process safety competency, and workforce involvement [6].

The facility undertook hazard identification and risk analysis (LOPA, FTA). As the recommendations are analyzed and designed, hazard identification and risk analysis are required to ensure that unexpected hazards are not introduced by the recommendations. As the recommendations continue through the design process, management of change is essential to ensure that the intent of the recommendations is achieved by the installation. Training and performance assurance are required for unit management, supervision, operations, technical support, and maintenance personnel. This assurance requires operating procedures, maintenance procedures, and safe work practices. The facility must be committed to the weekly run checks and the annual full functional tests. The results of the checks and tests should be analyzed and deviant trends should be addressed. All the activities of the management system described in this section should be audited to ensure that the management system is functioning as designed [7].

5 Conclusion

The facility was aware that the performance of the backup emergency power supply from the two generators was less than desirable. The facility was somewhat surprised that the fault tree analysis showed a relatively large number of device failures that could prevent both generators from operating correctly. The fault tree analysis provided the basis for recommendations for investigating to improve the PFD of the emergency power system. A management system should be used to ensure that the integrity of the EPS is managed throughout its lifecycle

6 References

[1] CCPS. *Layer of Protection Analysis, Simplified Process Risk Assessment*. Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2001.

[2] NFPA® 110, Standard for Emergency and Standby Power Systems Handbook 2016, Third Edition, National Fire Protection Association®, Quincy, Massachusetts.

[3] CCPS. *Guidelines for Chemical Process Quantitative Risk Analysis, 2nd Edition*. Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 1999

[4] Ericson, Clifton A., II. *Fault Tree Analysis Primer.* CreateSpace Inc., Charleston, NC, 2011.

[5] Dowell, A., Bridges, W., Massello, M., Thomas, H., "SIL-3, SIL-2, and Unicorns (There Is a High Probability Your SIL 2 and SIL 3 SIFs Have No Better Performance Than SIL 1)", 2019 Spring Meeting and 15th Global Congress on Process Safety, New Orleans, LA. American Institute of Chemical Engineers, March 31 – April 3, 2019.

[6] CCPS. *Guidelines for Risk Based Process Safety. Center for Chemical Process Safety*, American Institute of Chemical Engineers, New York, NY, 2007

[7] CCPS. *Guidelines for Implementing Process Safety Management, 2nd Edition*. Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2016