Reliability Assessment of Integrated Flywheel UPS versus Double-Conversion UPS with Batteries

White Paper 103

2128 W. Braker Lane, BK12

Austin, Texas 78758-4028

www.activepower.com

Objective

This paper provides a quantitative analysis of the in-service reliability of Active Power's flywheel-based CleanSource® UPS (uninterruptible power supply) system versus a battery-based double-conversion UPS system using probabilistic risk assessment (PRA).

Key Findings

- MTechnology found CleanSource UPS is approximately seven times less likely to fail versus a double-conversion UPS with batteries during a short utility outage.

- MTechnology found “demand failures of the flywheel energy storage system are extremely unlikely. If the flywheel is operational at the moment an outage occurs, the flywheel will almost certainly function.”

- Common to both systems, the automatic transfer switch (ATS) represents the single most likely cause of a system failure, accounting for 95 percent of anticipated system failures closely followed by main switchgear and generator fail to start.

- The most likely failure mode of a double-conversion UPS with batteries is due to undetected battery failures (demand failures)

- The study used an optimistic non-detectable battery failure rate of 1 percent of detectable battery failures which is conservative and assumes effective maintenance and testing. MTechnology’s experience strongly suggests that it would be difficult to make the battery more reliable than what this model predicts.

- Using a non-detectable battery failure rate of 10 percent, CleanSource UPS is more than 52 times less likely to fail versus a double conversion UPS during a short outage of less than 10 seconds.

- The second most likely failure of a double conversion UPS with batteries is due to detected battery failures while system is on bypass.

Overview

Active Power, Inc. retained Mass.-based MTechnology, Inc. (MTech) to perform a reliability analysis of its expandable CleanSource UPS 300kVA/240kW versus double conversion UPS with batteries.

MTechnology, Inc. (MTech) has been applying the science of probabilistic risk assessment (PRA) to the problem of high-availability electric power suitable for computers, Internet industries, and other mission-critical facilities since 1996. MTech clients include manufacturers, engineering firms, owners, and users of mission-critical facilities. MTech serves clients across a wide range of industries including corporate data centers, nuclear power, LNG production, biomedical research, proton beam cancer therapy, and fuel cell development.

The study included two classes of utility failure:

- Long utility outages lasting longer than 10 seconds where the AC source is transferred to generator requiring the ATS to operate and the generator start and run.

- Short utility outages lasting less than 10 seconds where the UPS energy storage is sufficient to support the load until utility service is restored and transfer to generator is not considered. This amplifies the core reliability differences of the two UPS systems.

MTech developed a fault tree model for both systems. The fault tree model combines the knowledge of what combinations of utility and UPS component failures result in system failure with knowledge of the frequency of component failures and duration of anticipated repairs. Data regarding component failures was obtained from industry standard including published sources such as the IEEE Gold Book, augmented by Active Power's CleanSource UPS fleet experience when possible.

SYSTEM DESCRIPTIONS

CleanSource UPS

The CleanSource UPS 300 Series is a three-phase UPS system utilizing flywheel technology for energy storage. The system provides power conditioning features including voltage regulation and harmonic cancellation. Coupling the CleanSource UPS with a standby generator creates a continuous power system that protects sensitive, mission critical loads from both short power disturbances and extended power outages.

Figure 1: CleanSource UPS 300 Series

The flywheel stores kinetic energy in the form of a rotating mass. During normal operation, the flywheel rotates at a constant speed. The system delivers power from a utility to the protected load. When power from the utility is interrupted, the system converts the kinetic energy stored in the flywheel to electrical power. When the power from the utility is available again, the system transfers the load back to the utility. Refer to white paper #108 ("Operation and Performance of a Flywheel-Based UPS System") for further information.

Flywheel Technology

Active Power produces the integrated UPS and DC power system with flywheel technology serving as an alternative to chemical batteries. The CleanSource fleet has more than 40 million hours of runtime in applications around the world.

Figure 2: Production flywheel for UPS application

The flywheel rotor is supported by Active Power's magnetic bearing technology. This technology unloads a majority of the flywheel's weight from the field replaceable mechanical bearing cartridge. A vacuum pump evacuates the chamber, reducing the drag on the spinning flywheel. The flywheel's speed decreases as power is transferred to the load. Regulated current is supplied to the field coils to maintain constant voltage output throughout the discharge.

The system provides power conditioning and ensures ride-through power during voltage sags and surges. It also bridges the gap between a power outage and the time required to switch to generator power. The one line schematic of the CleanSource UPS simplified for the fault tree model is illustrated in Figure 3.

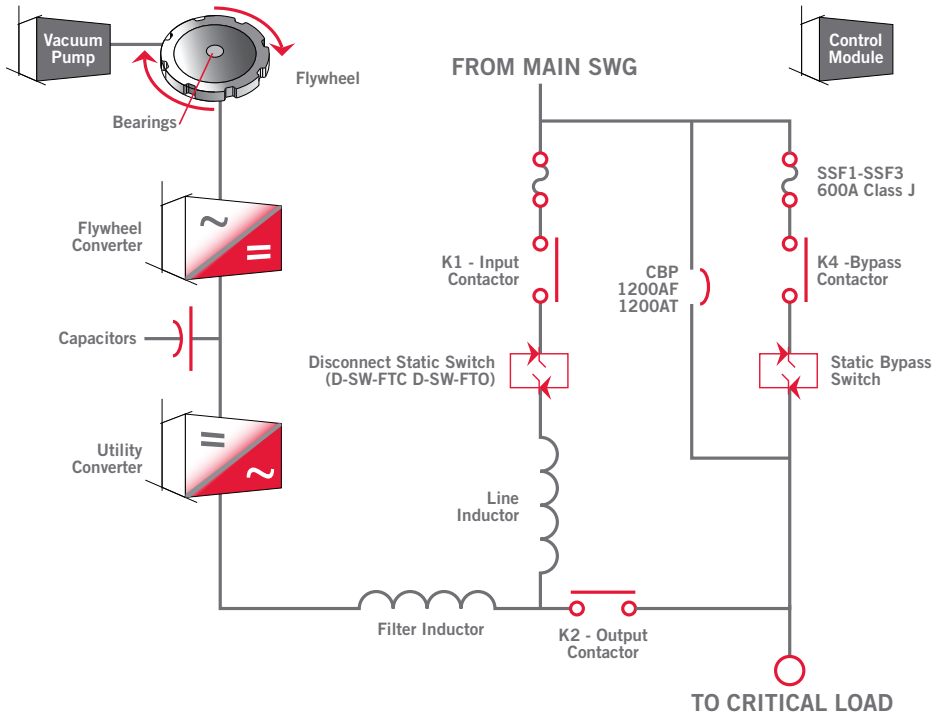

Figure 3: One line schematic of CleanSource UPS

Double Conversion UPS

The double-conversion UPS system utilizes a rectifier and an inverter with energy storage via chemical batteries or other means on the DC link between the two conversion stages. In a traditional double-conversion UPS system, the rectifier charges the battery and supplies the inverter with DC power. The inverter supplies the load with continuous AC power. During an outage at the main input of the UPS, energy is taken from the battery until input power is restored. The rectifier then recharges the battery while simultaneously supplying the inverter with DC power. When the system works as intended, this takes place without interruption of the output of the UPS.

While effective, the drawbacks of a double-conversion system include lower operating efficiencies due to the two-step process of converting utility power from AC to DC, and then from DC to AC. Lead acid batteries are large and heavy, filled with corrosive chemicals and hazardous materials that must be disposed of carefully. Batteries generally require controlled environments. In a typical situation, a 10 degrees Celsius increase in ambient temperature cuts the anticipated lifetime of the battery in half.

Careful engineering is required to prevent adverse reactions between UPS input filters with diesel generators, particularly with a lightly loaded double-conversion UPS system. Generators have limited leading power factor ratings compared to their lagging power factor capabilities. A generator connected to an excessively large leading power factor load can experience self excitation with the generator output voltage increasing even with field current reduced to minimum. This dangerous condition requires a rapid shutdown of the generator and prime mover and generally results in loss of the critical load. The models used for the study did not account for this failure mode – as it was assumed it was engineered out of the system by informed review of the possible loads placed on the generator.

Demand failures in conventional battery systems are another disadvantage. The battery consists of a large number of two volt cells connected in series. Failure of any cell or the connection between cells can cause the battery to fail. These failures have proven difficult to detect in advance of the demand placed on the battery during an actual utility failure. The model of the battery assumed monthly testing with a high probability of detecting failed cells so that they could be repaired. The one line schematic of the double-conversion UPS simplified for the fault tree model is illustrated in Figure 4.

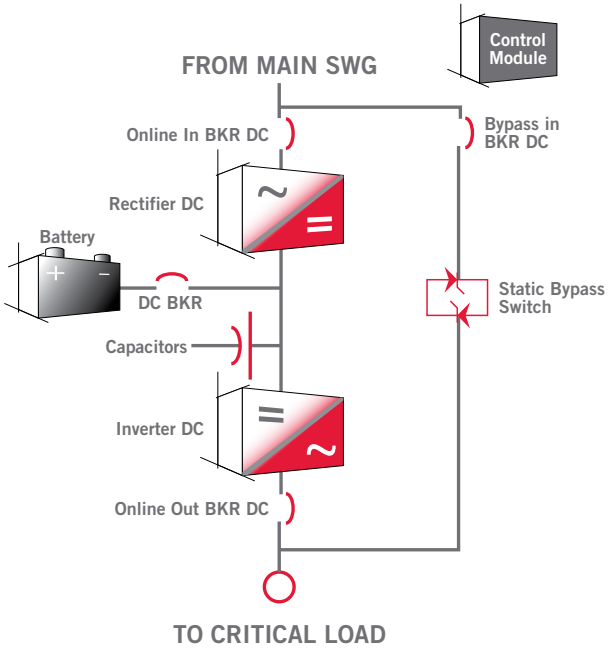

Figure 4: One line schematic for double-conversion UPS

Utility and Generator

Common to both systems is a single incoming utility feed and standby generator connected through switchgear and the ATS to the UPS inputs. The one line schematic of the utility, generator, ATS and main switchgear connected to the input of the UPS is illustrated in Figure 5.

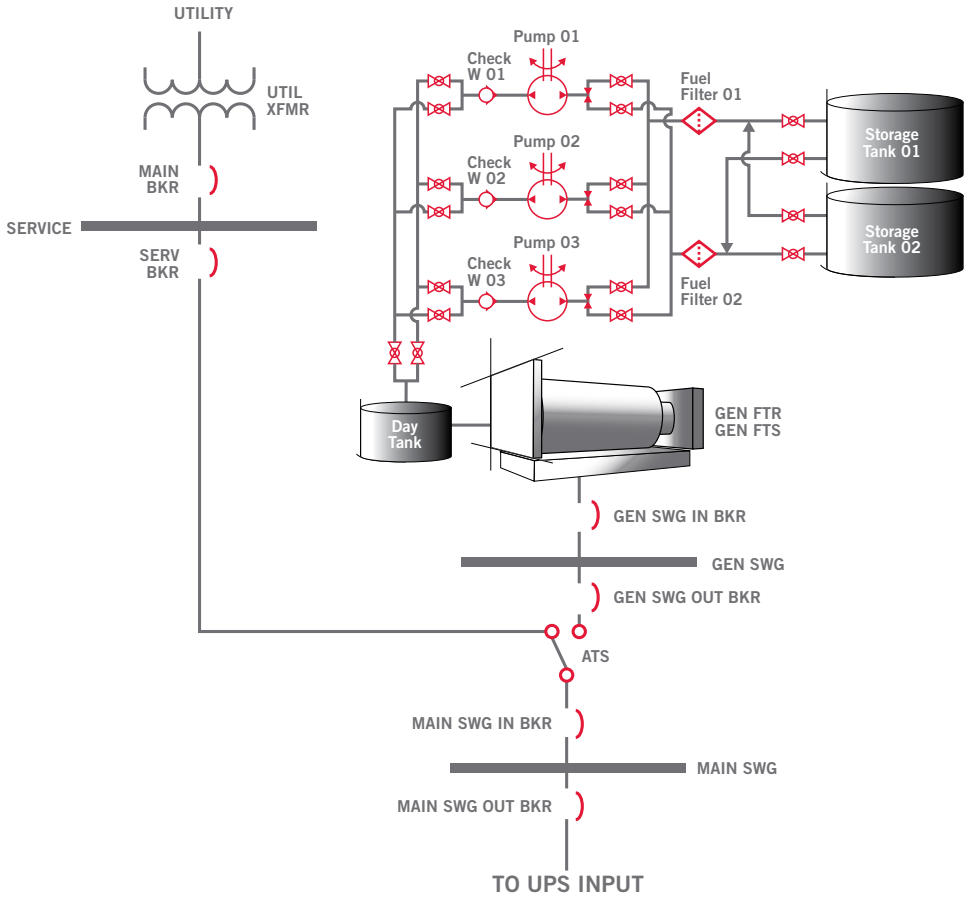

Figure 5: One line schematic of the utility, emergency generator, ATS and main switchgear used in system for fault tree model

Probabilistic Risk Assessment (PRA)

Probabilistic risk assessment is a collection of formal techniques used to assess the reliability and availability of complex systems. There are two important reasons to use PRA to study highly reliable systems:

- The fundamental limitations of learning about reliability by observing system failures
- The necessity of quantifying risk for rational and effective allocation of scarce resources.

Claims of “six nines” availability, shorthand for 99.9999 percent average uptime, are rampant in this field. A brief mathematical analysis can show that such claims are equivalent to a mean time to failure (MTTF) of over 1,200 years. It is impossible to verify or falsify such a claim by observation of a facility with an economic lifetime of a few decades. Neither designer nor owner will live long enough to learn the truth. Similarly, claims of “30 years experience” may be equivalent to saying the same mistakes have been repeated for the entire career of the designer.

PRA techniques allow for the development of credible, defensible estimates of system reliability by combining known data on simpler component failure rates in a formal mathematical model. There is a great deal of component failure rate data available for most electrical, electronic and mechanical components. PRA calculations allow that data, combined with an expert’s knowledge of how the components in a particular system interact, to produce useful estimates of complex system failure rates before the first system is built.

The ability of PRA to estimate system failure rates allows designers and manufacturers to evaluate the reliability of competing designs before building the first prototype. The ability to predict the effects of proposed improvements is also a powerful tool. Highly reliable systems invariably utilize redundant components, backup systems and other techniques. These techniques result in complex designs that defy traditional engineering intuition and judgment.

PRA is required to establish the reliability of systems that fail so rarely that direct measurement is impractical. It is also useful when failure is to be avoided to the maximum extent possible as is the case with nuclear plants. The second, and arguably more important, reason to utilize PRA is its implications for management as an aid in decision making.

The results of a good PRA analysis are much richer than a simple number such as MTTF or availability. Results are presented both as a probability of failure (discussed below) and as a quantitative ranking of the contribution of each component to the overall risk of failure. It is this quantification of risk that is the most powerful reason to utilize PRA in support of highly reliable systems.

Results for CleanSource UPS and double-conversion UPS are consistent both with earlier studies of corporate data centers and with competitors’ UPS products. Models with dozens or even thousands of components invariably show the majority of the risk of failure can be attributed to just a few components. Without this knowledge of the relative contributions to failure, designers and their managers cannot possibly allocate scarce resources most effectively. Armed with the knowledge that only a few components cause most system failures, resources can be allocated to those components. Resources can be removed from components, maintenance practices and other efforts that can be shown to make little or no contribution to the reliability of the system.

In summary, PRA provides information regarding the reliability of a system that is difficult or impossible to obtain by other means. That information enables the rational, defensible allocation of resources for enhancing reliability during all phases of design, operations, maintenance and improvement.

Availability and Probability of Failure

MTech reports results primarily in terms of probability of failure instead of availability. Availability is technically the correct metric for repairable systems, but it is not necessarily the one that is most useful for understanding the risks or the differences between competing systems.

The primary reason to use probability of failure is that customers find it the most useful metric. Few firms have substantial experience in the mathematical techniques of probabilistic risk assessment, but executives and managers routinely juggle competing proposals that have various degrees of risk. Many purchase products such as insurance or disaster recovery programs based upon their assessment of risk, which is the probability of suffering a loss multiplied by the amount of damage they anticipate from such a loss. Most firms that operate data centers will suffer substantial losses in the event of a single outage and they need to know the probability of such an event in order to make informed decisions regarding additional investment or other means of mitigating the risk.

A secondary reason to use probability of failure rather than availability is that the probability of failure is a function of time. Analysis methods such as Markov chains and network reduction are limited to constant failure rates and the results are often quoted as MTTF, obtained from a constant failure rate, 1, by inversion:

$MTTF = 1/\lambda$.

While this is true for a component or system with constant failure rates, redundant elements with constant failure rates result in a system with variable failure rate and it can be misleading to characterize systems with redundant elements with a constant failure rate.

Fault Tree Modeling

Fault Tree Analysis is a technique used to trace the effects of component or subsystem failure. The analysis starts with system failure. The analysis determines which subsystems must fail in order to cause the system to fail. Each subsystem is similarly evaluated, until eventually the analysis stops with a number of well-defined failures, called initiating events. Fault tree models are logical models of system failure, combined with the failure and repair rates for the initiating events. Combinations of component failures that are sufficient to cause a system failure are known as minimal cut sets.

Fault trees, and their accompanying analysis tools, are the prime modeling technique for determining system minimal cut sets. Failure and repair rates for each considered event are used to determine the relative contribution of each event to overall system failure. The product of this analysis is a listing of minimal cut sets and their contribution to the overall probability of system failure. Since even simple models typically have thousands of minimal cut sets, but nearly all failures are caused by a few cut sets, MTech does not report the contributions of every cut set. CleanSource UPS and the double-conversion UPS were modeled for comparison using the SAPHIRE fault tree analysis tool.

System failure is defined as failure to get power from the online or the standby path to the critical load. Utility and the standby generator are AC sources. The model has both UPS systems to be compared – CleanSource UPS/bypass module, and the double-conversion UPS/bypass module. Failure occurs if either type UPS fails. This approach enables the common elements of the fault trees (i.e., utility, generator, etc.) to be shared. The fault tree model can select either CleanSource or double-conversion UPS for analysis by setting the probability of the other system failure to zero.

Fault Tree Analysis

MTech utilized component failure rates from many sources including standard nuclear power plant reliability databases, manufacturers' data and MTech's experience with the UPS industry. In cases where Active Power provided field experience data, such as experience with the CleanSource fleet, that data was used to inform estimates of the component failure rates and failure modes.

MTech constructed the CleanSource UPS fault trees based upon the one line schematic diagrams with clarifications from Active Power as required. System failure is defined as failure of the load to get power from the online or the standby path, which is the "top event" of the combined fault tree models. Template events representing similar basic events were introduced to efficiently handle the basic events of component failure.

Utility Failure Classes

For the purpose of this study, two classes of utility failures were considered.

- Long utility outages lasting longer than 10 seconds where the AC source is transferred to generator requiring the ATS to operate and the generator to start and run.

- Short utility outages lasting less than 10 seconds where the UPS energy storage is sufficient to support the load until utility service is restored and transfer to generator is not considered. This amplifies the core reliability differences of the two UPS systems.

Long Outages: > 10 Seconds with Transfer to Generator

In a long outage scenario, the energy storage in the UPS provides power to the critical load for a short amount of time until the standby generator fires up and assumes the load through transfer of the ATS. It should be noted long outages of greater than 10 seconds are relatively infrequent in developed countries. In fact, the Electric Power Research Institute (EPRI) estimates customers are 10 times more likely to experience voltage sags than a complete power outage. Of complete outages, less than 4 percent are longer than 10 seconds.

The top 18 cut sets for a double-conversion UPS with batteries and CleanSource UPS are reproduced in Figure 6. Each of the line items represents a specific failure within the architecture leading to a loss of power to the critical equipment. Each of the events is weighted and has individual probabilities or frequency of failures as determined by available industry data, IEEE Gold Book or augmented by field experience from UPS manufacturers.

CleanSource UPS

TOP-POWER-FAILURE				
Cut #	Cut Set %	Prob/Freq	Event	Probability
1	94.7	8.20E-02	AUTOMATIC TRANSFER SWITCH FAILURE	8.20E-02
2	1.2	1.10E-03	MAIN SWITCHGEAR INPUT CIRCUIT BREAKER	1.10E-03
3	1.2	1.10E-03	MAIN SWITCHGEAR OUTPUT CIRCUIT BREAKER	1.10E-03
4	1.2	1.00E-03	MAIN SWITCHGEAR BUS FAILURE	1.00E-03
5	1.2	1.00E-03	GENERATOR FAILS TO START	1.20E-03
			LONG UTILITY FAILURE	8.40E-02
6	0.5	4.30E-04	GENERATOR FAILS TO RUN NON-FUEL RELATED	5.10E-03
			LONG UTILITY FAILURE	8.40E-02
7	0.1	8.80E-05	COMMON CAUSE FAILURE OF CONTROL MODULE	8.80E-05
8	0.1	8.40E-05	ATS FAILS TO SWITCH	1.00E-03
			LONG UTILITY FAILURE	8.40E-02
9	0.1	4.70E-05	CAPACITOR FAILURE	5.60E-04
			LONG UTILITY FAILURE	8.40E-02
10	0	3.90E-05	CAPACITOR FAILURE	5.60E-04
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
11	0	3.80E-05	FLYWHEEL CONVERTER FAILS	4.50E-04
			LONG UTILTY FAILURE	8.40E-02
12	0	3.80E-05	UTILITY CONVERTER FAILS	4.50E-04
			LONG UTILTY FAILURE	8.40E-02
13	0	3.10E-05	FLYWHEEL CONVERTER FAILS	4.50E-04
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
14	0	3.10E-05	UTILITY CONVERTER FAILS	4.50E-04
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
15	0	1.80E-05	DAY-TANK FAILS	2.20E-04
			LONG UTILTY FAILURE	8.40E-02
16	0	6.00E-06	VACUUM PUMP FAILS	7.20E-05
			LONG UTILTY FAILURE	8.40E-02
17	0	5.90E-06	GENERATOR FAILS TO START	1.20E-02
			UTILITY TRANSFORMER FAILS	4.90E-04
18	0	5.00E-06	SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
			VACUUM PUMP FAILS	7.20E-05

Double-Conversion UPS

TOP-POWER-FAILURE				
Cut #	Cut Set %	Prob/Freq	Event	Probability
1	93.8	8.20E-02	AUTOMATIC TRANSFER SWITCH FAILURE	8.20E-02
2	1.2	1.10E-03	MAIN SWITCHGEAR INPUT CIRCUIT BREAKER	1.10E-03
3	1.2	1.10E-03	MAIN SWITCHGEAR OUTPUT CIRCUIT BREAKER	1.10E-03
4	1.2	1.00E-03	MAIN SWITCHGEAR BUS FAILURE	1.00E-03
5	1.2	1.00E-03	GENERATOR FAILS TO START	1.20E-03
			LONG UTILITY FAILURE	8.40E-02
6	0.7	5.90E-04	BATTERY FAILURE NON-DETECTABLE	5.80E-04
			SHORT UTILITY FAILURE NON-REPAIRABLE	1.00E+00
7	0.5	4.30E-04	GENERATOR FAILS TO RUN NON-FUEL RELATED	5.10E-03
			LONG UTILITY FAILURE	8.40E-02
8	0.2	2.00E-04	BATTERY FAILS - DETECTABLE	2.40E-03
			LONG UTILITY FAILURE	8.40E-02
9	0.2	1.70E-04	BATTERY FAILS - DETECTABLE	2.40E-03
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
10	0.1	8.80E-05	COMMON CAUSE FAILURE OF CONTROL MODULE	8.80E-05
11	0.1	8.40E-05	ATS FAILS TO SWITCH	1.00E-03
			LONG UTILITY FAILURE	8.40E-02
12	0.1	4.90E-05	BATTERY FAILURE – NON-DETACTABLE	5.80E-04
			LONG UTILITY FAILURE	8.40E-02
13	0.1	4.70E-05	CAPACITOR FAILURE	5.60E-04
			LONG UTILITY FAILURE	8.40E-02
14	0.1	4.10E-05	BATTERY FAILURE – NON-DETECTABLE	5.80E-04
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
15	0	3.90E-05	CAPACITOR FAILURE	5.60E-04
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
16	0	3.10E-05	INVERTER FAILS IN THE ONLINE PATH – DOUBLE-CONVERSION	4.50E-04
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
17	0	1.80E-05	DAY TANK FAILS	2.20E-04
			LONG UTILITY FAILURE	8.40E-02
18	0	5.90E-06	GENERATOR FAILS TO START	1.20E-02
			UTILITY TRANSFORMER FAILS	4.90E-04

Figure 6: Top 18 cut sets for CleanSource UPS (top table) double-conversion UPS with batteries (bottom table)

The fault tree analysis shows ATS failure is the most significant cause of backup power system failure. ATS failures in service participate in about 95 percent of the expected system failures. The ATS is common to the CleanSource UPS and the double-conversion UPS models so there is very little difference in the reliability of the two systems as shown in Figure 7.

The result is not an indictment of ATS. The IEEE Gold Book data used in the model reports a failure rate of approximately 10-5 per hour, or over 100,000 hours (11+ years) mean time between failures. This represents good performance from a complex electromechanical component in continuous service. The ATS participates in a majority of system failures because it is a single point of failure. The consequence of ATS failures is almost invariably system failure.

System Architecture System Power Failure	Probability of System Failure*	Relative Probability
CleanSource UPS w/ Flywheel	8.69E-02	1.00
Double-Conversion UPS w/ Batteries	8.77E-02	1.01

*System failure is defined as failure to provide power to the critical load.

Figure 7: Reliability of Systems

Data shows the system including CleanSource UPS is less likely to fail by a narrow margin due to the dominating failure rates of the ATS, main switchgear and generator failure rates. Short outages were modeled as 100 times more frequent than long outages. Increasing the short outage failure rate will significantly influence the results above.

Short Outages: < 10 Seconds with Transfer to Generator

In a short outage scenario, the energy storage provides sufficient time to ride-through any power disturbance. Given that 96 percent of all sags and outages are 10 seconds or less, this metric is very significant in determining reliability of the individual UPS architectures. This fault tree analysis does not take ATS, switchgear and generator into account. Figure 8 shows probabilities of failure events for the two UPS systems with summary data in Figure 9.

CleanSource UPS

UPS Failure During Short Outage <10 Seconds				
Cut #	Cut Set %	Prob/Freq	Event	Probability
1	31.5	3.90E-05	CAPACITOR FAILURE	5.60E-04
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
2	25.3	3.10E-05	FLYWHEEL CONVERTER FAILS	4.50E-04
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
3	25.3	3.10E-05	UTILITY CONVERTER FAILS	4.50E-04
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
4	4.1	5.00E-06	VACUUM PUMP FAILS	7.20E-05
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
5	3.2	4.00E-06	FILTER INDUCTOR FAILURE	5.80E-05
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
6	3.2	4.00E-06	LINE INDUCTOR FAILURE	5.80E-05
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
7	2	2.50E-06	INPUT CONTACTOR K1 FAILURE	3.60E-05
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
8	2	2.50E-06	OUTPUT CONTACTOR K2 FAILURE	3.60E-05
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
9	1.9	2.40E-06	FUSE (F1-F3) FAILURE	3.40E-05
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
10	0.5	6.70E-07	DISCONNECT SWITCH FAIL TO OPEN	1.50E-04
			INPUT CONTACTOR K1 FAILS TO OPEN	4.40E-03
			SHORT UTILITY FAILURE NON-REPAIRABLE	1.00E+00
11	0.4	5.00E-07	BEARING FAILURE	7.20E-06
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
12	0.4	5.00E-07	FLYWHEEL FAILURE	7.20E-06
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
13	0.1	8.80E-08	DISCONNECT STATIC SWITCH FAILS TO CLOSE	1.30E-06
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02

Double-Conversion UPS

UPS Failure During Short Outage <10 Seconds				
Cut #	Cut Set %	Prob/Freq	Event	Probability
1	66.9	5.90e-04	BATTERY FAILURE – NON-DETECTABLE	5.80E-04
			SHORT UTILITY FAILURE NON-REPAIRABLE	1.00E+00
2	19.4	1.70E-04	BATTERY FAILURE – DETECTABLE	2.40E-03
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
3	4.7	4.10E-05	BATTERY FAILURE – NON-DETECTABLE	5.80E-04
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
4	4.4	3.90E-05	CAPACITOR FAILURE	5.60E-04
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
5	3.6	3.10E-05	INVERTER FAILS IN THE ONLINE PATH – DOUBLE-CONVERSION	4.50E-04
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
6	0.4	3.00E-06	DC DISCONNECT CIRCUIT BREAKER FAILS	4.40E-05
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
7	0.3	2.60E-06	RECTIFIER FAILS IN THE ONLINE PATH – DOUBLE-CONVERSION	3.70E-05
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
8	0.2	2.00E-06	INPUT BREAKER IN THE ONLINE PATH FAILS – DOUBLE-CONVERSION	2.80E-05
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02
9	0.2	2.00E-06	OUTPUT BREAKER IN THE ONLINE PATH FAILS – DOUBLE-CONVERSION	2.80E-05
			SHORT UTILITY OUTAGE DURING BYPASS	6.90E-02

Figure 8: Probabilities of failure events for UPS systems

The fault tree analysis shows that non-detectable and detectable battery failures account for more than 90 percent of all failures in a double-conversion UPS architecture. The assumed failure rate for batteries is based on well-maintained batteries, the maintenance and testing is effective, resulting in a low battery failure rate. According to MTech, experience suggests it would be difficult to make the batteries more reliable than the model predicts.

System	Probability of UPS Failure During Short Outage	Relative Probability of Failure
Flywheel CleanSource UPS	1.24E-04	1.0
Double-Conversion UPS with Batteries	8.74E-04	7.0

Figure 9: Summary Data

The analysis shows CleanSource UPS is seven times less likely to fail compared to a double-conversion UPS.

> ***"One benefit of the CleanSource system is that demand failures of the flywheel energy storage system are extremely unlikely; if the flywheel is operational at the moment an outage occurs, the flywheel will almost certainly function."***

Sensitivity Analysis of Non-Detectable Battery Failures

The non-detectable battery failure rate is an important parameter in the analysis of the double-conversion UPS for short outages. The base case is estimated to be 1% failure rate of the detectable battery failures. MTech calculated additional cases with different estimations of this failure rate: 10 and 20 percent.

Non-Detectable Battery Failure	Probability of System Failure	Probability of UPS Failure During Short Outages	% System Failure **	% UPS Failure During Short Outages **
1% *	8.76E-02	8.74E-04	100%	100%
10%	9.32E-02	6.48E-03	106%	741%
20%	9.94E-02	1.27E-02	113%	1453%

*Base Case: This represents the non-detectable battery failure rate is estimated to be 1 percent of the detectable battery failures.
**This represents the percentage of each case compared with the Base Case.

Figure 10

Where CleanSource UPS is seven times less likely to fail during a short outage compared to the double-conversion UPS at a very optimistic 1 percent non-detectable battery failures of the detectable battery failures, this is widened to 52 times less likely to fail if 10 percent non-detectable battery failures are considered.

System Architecture	Non-Detectable Battery Failures	Probability of System Failure	Relative Probability	Probability of UPS Failure During Short Outage	Relative Probability
CleanSource UPS with Flywheel	N/A	8.69E-02	1.00	1.24E-04	1.0
Double-Conversion UPS with Batteries	1%	8.77E-02	1.01	8.74E-04	7.0
Double-Conversion UPS with Batteries	10%	9.32E-02	1.07	6.48E-03	52.3
Double-Conversion UPS with Batteries	20%	9.94E-02	1.14	1.27E-02	102.4

Figure 11

Similarly, when employed as part of a system designed to protect against both short and long outages, CleanSource UPS is marginally less likely to fail compared to the double-conversion UPS at an optimistic 1 percent non-detectable battery failure rate, but the performance improvement widens at higher battery failure rates.

Conclusion

The fault tree models considered two different classes of utility failures – short outages lasting less than 10 seconds and long outages lasting more than 10 seconds.

The generator must start and run and the transfer switch must operate for success in long outages. According to the PRA, the probability of a CleanSource UPS failure is only 1/7 of the failure probability of the double-conversion UPS during a short outage of 10 seconds or less. EPRI reports 96 percent of all sags and outages occur within this time period. This scenario is 100 times more frequent than long outages meaning that facilities are at significantly higher risk from this class of outage. This elevates the importance of the short outage UPS failure rate.

When employed as part of a system considering long outages of 10 seconds or more, there is essentially no difference in the reliability of the two systems. Failures in the ATS, generators and switchgear account for more than 90 percent of all anticipated failures. In this case, the runtime difference between batteries and flywheel is inconsequential as the ATS, generator and switchgear failures represent either:

1. single points of failure with no possibility of repair (i.e., instantaneous loss of load, etc.), or

2. reparable failures with expected repair times exceeding either the flywheel or the battery runtime.

In the double-conversion UPS with batteries, the most likely failure mode is due to undetected battery failures. Detecting battery cells that will fail on the next demand has proven to be extremely difficult. Even with optimistic assumptions that monthly tests of the double-conversion UPS battery string find the majority of battery failures, CleanSource UPS is more reliable. Realistic estimates of undetectable battery failures results in a clear advantage for the CleanSource UPS.

The most likely failure mode of a CleanSource UPS is a utility outage when the UPS is on bypass, awaiting repairs or scheduled maintenance. However, reducing the MTTR and the time the UPS is on bypass, to a third further improves the reliability by a factor of almost 10.

The key benefit of a dynamic electromechanical system like that of the CleanSource UPS is that demand failures highly unlikely. The normal state of the CleanSource UPS is with the flywheel spinning constantly, storing kinetic energy. Changes in values that determine the health of the system are immediate and provide an accurate status prior to an outage occurring. Conversely, a battery based system is an electrochemical process that, even with monitoring and recommended maintenance, exhibits a high level of non-detectable failures.

Supporting Cases Appendix

Case 1

On May 23, 2008, the hosting service Host Dime published the following description of an outage that occurred at their facility. Root cause determination of the outage was attributed to battery failure. In this case, a failure-on-demand as described in the MTechnology study. Key findings are highlighted.

To our clients and business partners,

There are no words to describe how deeply we apologize about the downtime which occurred on Friday, May 23, 2008. The incident has created immense discontentment to our organization mentally and emotionally because of the love and dedication our team has to our entire community. Moreover, because we realize the level of damage this incident has potentially caused you. We know there is neither money nor words which will replace the losses that may have been experienced by each one of you. Our organization is forever in debt to you all for the frustration and grief endured. It is never easy in disasters, but many of you showed your support as we worked non-stop to get things back to normal. We want to thank all of you for your patience, understanding and support during such a difficult time. In any case, a formal incident report of our investigation is what we wish to rightfully deliver to you. Below is the detailed summary of events as they occurred. Please note some of you may have not experienced any outage during this, not all clients were affected, but we wanted to keep everyone updated.

What happened:

At approximately 8 A.M. EST our data center experienced a surge followed by a power outage which lasted several minutes from our electrical utility provider Progress Energy. The surge tripped our facility's main breaker; this main breaker is designed to have a certain level of sensitivity and to trip in the event of a severe surge in order to protect the load (servers and critical equipment) from being burned. Immediately after this occurred, our generator automatically started up within a few seconds. Meanwhile, power to our load (servers and equipment) was automatically transitioned from unavailable raw power to generator power by the automatic transfer switch (ATS), our uninterruptible power system (UPS) in conjunction with our battery set supply is supposed to automatically sustain continuous power to the load. However, it appeared this did not happen. In any case, generator power was indeed immediately available within the minute of the outage.

Immediately post the outage our engineers and electricians came on site. **The diagnosis conducted revealed there was a fault within a battery string which is connected to the UPS. It is this fault that disabled the UPS from being able to fully sustain continuous power to the load** meanwhile the ATS transitioned the facility to the generator power lines from the raw power lines. During this time a great portion of the data center experienced a sudden power loss which caused a myriad of servers to power cycle. Unfortunately, at times when some systems experience sudden power loss some require manual administrator intervention to get full function restored. Post the outage, our team immediately started working on checking systems and all servers that may have been adversely affected by the sudden power loss these experienced.

What was done to correct the problem:

Our on call UPS maintenance technician along with our electricians and engineers immediately came together on site to conduct a thorough diagnosis and put together a plan of action to correct any and all possible issues.

While the age of the battery supply being employed was well within the manufacturer's life span expectancy, the entire battery supply was replaced with a new set. In addition, our UPS underwent a thorough in depth inspection and all critical components were individually inspected and reconditioned as necessary. Lastly, the batteries and UPS were load tested before being re-employed to the overall power back up system to ensure 100% reliability. All this was completed within several hours of the incident.

Who was affected:

The power outage experienced was intermittent. However, once power was fully restored to the facility many servers required file system checks (FSCK), some power supply replacements, and a few others hard drive replacements due to excessive I/O errors. Unfortunately, depending on the space on the drive the system occupies a FSCK run time can range from 30 minutes to a nine hours plus (approximately 200 servers counted). Those that were worst affected are the systems that were having excessive I/O errors and needed hard drive replacements (approximately 12 servers total counted). Again, unfortunately, hard drive replacements may take 4-12 hours plus to complete depending on the space being occupied on the drive. Those that were least affected were servers that only required a power supply replacement (approximately 60 servers counted).

For those servers that experienced the greatest downtime was not due directly to power unavailability, but rather due to post sudden power loss adverse effects described above.

What preventative measures are being taken:

All critical power systems in our data center and loads were previously and are regularly inspected and maintained. This includes generator, UPS, breakers, etc. In fact, our UPS underwent an inspection and a maintenance service on the week of the 12th of May 2008. The service report came back showing the UPS was in good working condition as well as the battery supply set. The only advice made was to consider replacement of the battery set supply as these were approaching the last year of the manufacturer's life span expectancy. Pro actively following up on the advice made by the maintenance engineer, a new battery supply set was ordered right away and scheduled to be installed this Tuesday May 27, 2008.

Unfortunately, the battery supply set is what ended up being the fault and ironically this is what was already schedule for routine replacement maintenance. It is difficult to state that more could have been done as the batteries were within their life expectancy limits, but failed short during this situation. Something of this magnitude, unfortunately, could not be predicted and was already being addressed with a new battery supply set replacement as a proactive measure. Nonetheless, a new standard has now been adopted as we will be increasing the battery reliability tests schedule to be completed monthly. This will allow us to intercept any and all types of possible issues with any battery sooner and overall highly reducing the probability of a failure encounter during critical times.

Our data center employs a 500KVA UPS and a 500KW generator. This is a statement that can be further proven by the recent pictures and videos taken yesterday afternoon. If you are in any kind of doubt whatsoever with regards to this, we would like to kindly ask for the opportunity to disprove your doubt. The pictures and videos below are of our backup systems in place which have protected us from several past outages to the entire data center. We uncover what maybe some of you didn't know was in place in our facility since day one so you can see that your services with us are secure.

We have been in the industry close to 8 years now and we have always tried our best to ensure 100% uptime to all of you. This is the first outage we experienced with this level of severity in our entire existence. It is not only our job, but our passion to give you the best level of service possible. We do not want to use the misfortune of this unpredictable situation to be an excuse for the downtime experienced. Despite the nature of the situation, we accept full responsibility for the outage and we are ready to compensate you in anyway we can. We value your business relationship and the level of trust you put in us. We know many of you will have a desire to cancel with us due to the losses you have incurred and question our systems' integrity. We ask you to please talk to someone in management before you make your decision as we do understand the level of importance this means to each one of you. We work in high a high volatile environment where anything can happen just like with any of our competitors; however, we will always, no matter what, promise to be here whenever any issue occurs with an open hand to help resolve it as fast as humanly possible. Misfortunes will always happen to the best of us, how they are handled and treated makes the difference. If there is anything at all we can do to help you minimize your losses please just ask and consider it done. Our awareness and commitment level has tripled as a company and you can ensure this has only made us stronger and more experienced as a company. It is not everyday people or companies can overcome such issues and have the support and loyalty that many of you have given us. If you wish to reach out to me personally with any concerns, recommendations, suggestions, venting, or ways we can compensate you, please email me personally at e.v.@ hostdime.com. I will be happy to talk to you in person.

(Source: http://www.hostdime.com/about/5232008/)

Discussion

Power disruptions as described above are disastrous and they happen more often than most companies like to admit to. Despite the fact that the actual utility outage lasted only a few minutes, the system downtime ranged from 30 minutes to several hours. Data centers like to talk about the availability of their facilities (ratio of uptime divided by uptime plus downtime), but it is clear from this analysis the availability has different definitions depending on whether you talk to the power company or to the clients to whom this note is addressed. MTechnology contends probability of failure is a better metric by which to judge data centers as it represents the likelihood of events as described here.

Host Dime states “Something of this magnitude, unfortunately, could not be predicted…” In fact, the study by MTechnology predicts exactly this failure scenario and shows it to be one of the more likely causes of failure next to ATS, main switchgear and generator failure. Given there is no mention of a redundant UPS, one can presume the power system architecture at Host Dime is a Tier I or II which is in line with the architecture analyzed in the MTechnology study. System reliability is only as good as the weakest link and in this case that link turned out to be the demand response of the battery.

Host Dime’s approach to improving power system reliability is to increase the frequency of battery testing to once a month. This is generally accepted as good practice, but has two caveats:

- Lead-acid batteries have finite cycle life. By increasing the test frequency, they are potentially increasing the preventative maintenance (PM) replacement interval – a costly proposition. MTechnology has presented in formation on PM optimization based on reliability analysis at their course titled ‘Real Availability.’

- Monthly testing still leaves 12x 730 hour windows of opportunity for undetected failure. There simply is no reliable way to detect battery failure in between load tests and these windows of uncertainty pose risk for data center operators. Flywheels are different. If power is being absorbed by the flywheel to keep it spinning, there is extremely high probability that it will be able to revert to generation mode on demand. For this reason, there is little reason to perform periodic load testing with flywheels and the need for attention is readily displayed by system monitoring signals such as flywheel speed, etc.

Case 2

On June 24, 2008, the hosting service Adhost published the following description of an outage that occurred at their facility. Root cause determination of the outage was tentatively attributed to battery failure that initiated a UPS fault. This then resulted in common cause failure of a redundant UPS system. Key findings are highlighted.

Adhost Plaza East UPS Event Update
Posted in Company News (Posted by Will R 9:50 pm June 24, 2008)

At approximately 4:35 AM (PDT) on Saturday morning, June 21, 2008, an uninterruptible power supply (UPS) that provides service to approximately 20% of the servers in our Plaza East Data center experienced a significant failure. This UPS unit is in a suite which is dedicated to this purpose and is separate from the Adhost Plaza East Data Center. **Very early indications suggest that the underlying nature of this failure was a significant drop in amperage from the battery strings** which might have caused, for an as yet unknown reason, the unit to go into an uncontrolled over-voltage situation to compensate. Full analysis of this event will likely take at least several weeks. In any case, the end result was significant heat and smoke damage to the UPS unit.

The heroes at the Seattle Fire department were dispatched based on a smoke alarm and with assistance of on-site engineers, were able to get the electrical service to this UPS and the one next to it shut down without injury or other damage to the facility. This caused the “A & B” circuits that are fed from these two UPSs, and which serve the above mentioned portion of our Plaza East Data Center, to go dark at approximately 4:52 AM PDT. No other UPS systems on the floor or anywhere else in Plaza East were affected by this shutdown (including the UPS

systems located within the Adhost Plaza East Data Center and other UPS systems owned and operated by Fisher Plaza on the floor).

Adhost and the Fisher Plaza engineering team were able to restore bypass power to the affected circuits in the Adhost Plaza East Data Center (and to other portions of Fisher Plaza East) by approximately 6:15 AM PDT. Adhost personnel then began the process of powering systems back up and working with affected customers to get their systems back to full operation.

Why did both UPSs get shut down? These two units are in close proximity in a suite dedicated to this function. The second, originally unaffected UPS drew in a significant amount of smoke and other possible foreign material through its intake/cooling fans during the event. It was also probably subject to significant heat which may have compromised the components in the device. At this point, the engineers and the manufacturer are unwilling to certify its operation.

In our initial release to customers, we termed this as a fire, as that is what we initially had to work with. Although there was significant heat and smoke, there were no actual flames and, aside from the two UPSs, there appears to be no long term damage that is not easily redressed. The building has had a restoration company in the building around the clock to address the issue of the smoke and odor which resulted from this event. We are also going through not only our data center in this building, but also our offices which are located on this floor and we find little or no remaining evidence of damage, with the obvious exception of the power status.

So, where are we now? The loads that are affected are currently only backed up by generator power. This means that, in the event of interruption of service from Seattle City Light, the load will drop for 30-60 seconds until power is restored by the generators. Our engineers have been in close contact with Seattle City Light and they are well aware of our situation and have agreed to do whatever they can to minimize or eliminate any work on their power distribution plant that might have an adverse impact on our service. Our thanks go out to them for their understanding and cooperation.

Now, there is some good news. Normally, replacing UPS units like these is a question of several weeks or months. However, two new UPS units were recently installed on the floor which are available for us to use. We are working with the building and our vendors to map out a plan for getting the load moved onto these UPSs as quickly as possible. We do not have an exact timeframe for this because there are several components that are currently hard to predict (exact availability of materials, permitting and inspections, etc.) but we are pushing this process as fast as it is safe (and legal) to do so. We're hoping to set a target date of this weekend. We will make a formal announcement to the affected customers when we have that exact timing. We will, of course, work with our customers to minimize any impact that this transfer may have on their service.

We apologize for any impact this event may have caused to our customers or to their customers. We thank our customers for their understanding as we work through this situation. We also would like to thank the multitude of players for true excellence during this trying time including, the Fisher Communications engineering team, the Egis engineering team, the Adhost engineering and systems administration teams, Prime Electric, the Seattle Fire Department and Seattle City Light. With their collective effort and knowledge, this potentially very bad situation was made considerably better.

We also are very thankful that no one was injured during this event.

(Ref: http://www.adhost.com/blog/2008/06/24/plaza-east-ups-event-update/)

Discussion

In this particular situation, the final findings have not been published. However, based on the preliminary assessment, we can surmise the impedance of the battery circuit (internal or external) was compromised leading to initiation of the secondary fault in the UPS. Adhost does not state why the UPS had gone to battery (possibly from an outage or load test), but only implies the batteries were under load and that the amperage from the batteries dropped suddenly. Internally, plate sulfation can lead to increased internal impedance and loss of capacity, but this usually increases gradually. A more likely internal failure scenario is full or partial loss of interconnection between plates. Battery strings consist of numerous 2-volt cells in series. For a typical three-phase UPS with 480v nominal DC bus, there are 240 cells in series any one of which can fail open rendering failure of the entire string. Externally, battery strings consist of numerous interconnecting cables any one of which can have loose contact with the battery terminals sufficient to allow low amperage charging, but insufficient to carry full load.

MTechnology discusses common cause failures in their course 'Real Availability' periodically held at conferences on data center reliability. The fact that failure of the first UPS affected the redundant system is one of those insidious circumstances that are very difficult to predict without extensive experience. As an example, many companies presume that having dual utility feeds leads to negligible probability of input failure. While it is true that this does mitigate risk due to equipment failure on a single feed, it is only reliable up to the point of common interconnection and will not typically protect against regional outages which have a mean time to failure of approximately every ten years.

In this case, a demand failure on the battery was the likely root cause of this outage compounded by failure of the UPS that initiated a common cause failure of the redundant UPS. For the purpose of this paper, the takeaway from this discussion is that battery demand failures do occur with enough regularity that one is able to document two cases within the period of a month.

References

» IEEE Gold Book
- IEEE 493-2007 (Gold Book) Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems, 2007

» NRC
- Houghton, et al, Review of Operational Experience with Molded Case Circuit Breakers in US Commercial Nuclear Power Plants, AEOD/S92-03, Nuclear Regulatory Commission, 1992

» Grant
- Grant, et al, Emergency Diesel Generator Power System Reliability 1987 – 1993

» RIAC
- RIAC 217Plus™ Integrated Circuit and Inductor Failure Rate Models, J Reliability Information Analysis Center, 2007

» OREDA
- OREDA 2002, Offshore Reliability Data Handbook, 4th ed, SINTEF, Norway, 2002

» JET/TLK
- Pinna, et al, Collection of data related to JET and TLK operational experience and component failure, http://nuclear.inl.gov/fusionsafety/meetings/iea-task-5-2003/docs/pinna_pppl-jet_data.pdf