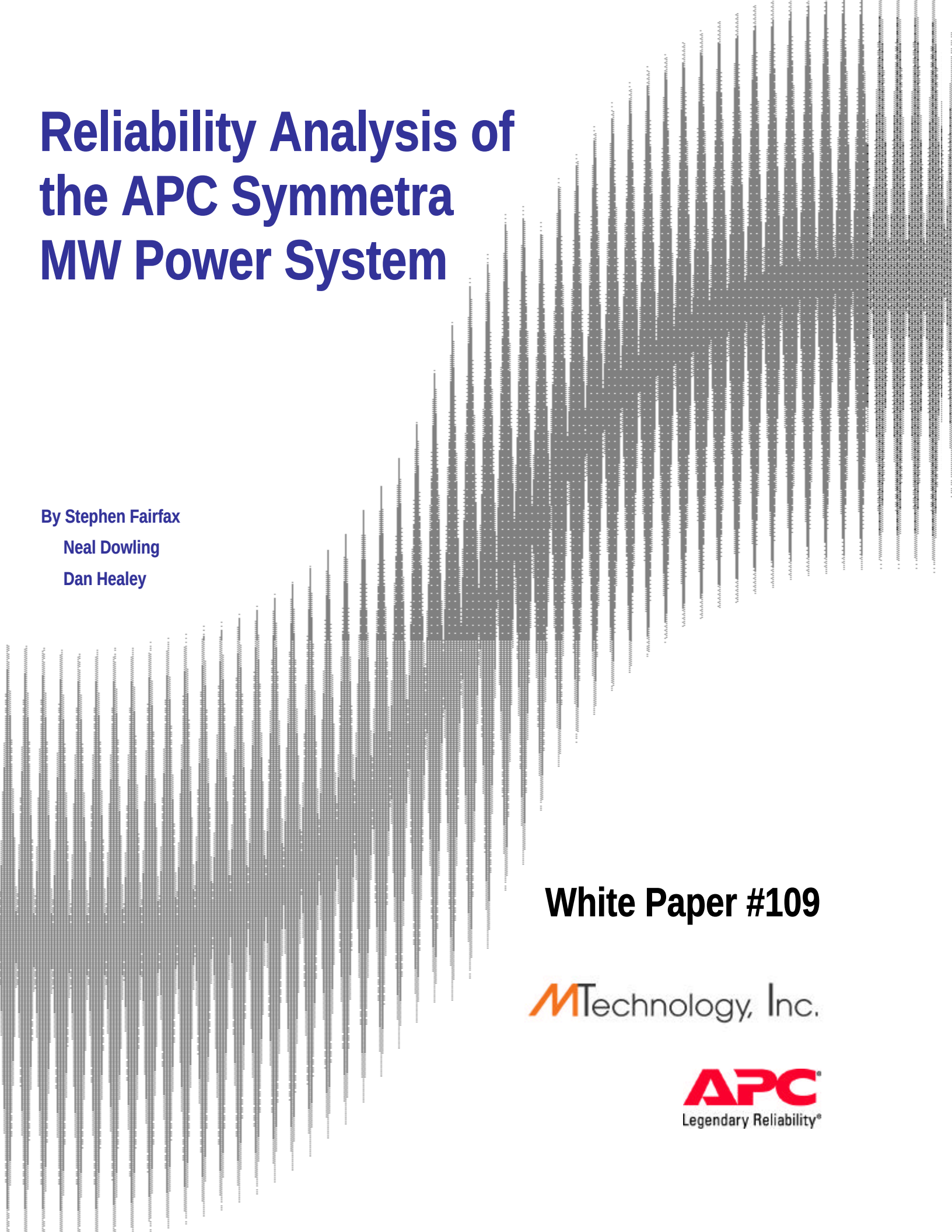
Reliability Analysis of the APC Symmetra MW Power System

By Stephen Fairfax
Neal Dowling
Dan Healey



White Paper #109

MTechnology, Inc.

APC
Legendary Reliability®

Executive Summary

MTechnology, Inc. (MTech) performed a quantitative reliability analysis of the APC Symmetra MW UPS. The study used techniques of Probabilistic Risk Assessment (PRA) to calculate the likelihood of over 680,000 potential failure modes. The mathematical method accounts for uncertainty in failure rates and component performance, and provides detailed guidance as to the contribution of each system component to the overall risk of failure. The results allow APC to focus its engineering, manufacturing, and field service resources where they will be most effective in further improving system reliability. The study included an exhaustive analysis of the system's architecture, component selection, control system, manufacturing practices, and response to internal and external faults. The study also included a detailed review of APC's delta conversion online topology.

The study showed that system mean time between failures (MTBF) can exceed 1 million hours when operated with a redundant power section. This figure includes all equipment failures, including those attributable to causes beyond APC's control, such as failures in the battery plant or electric utility.

Findings

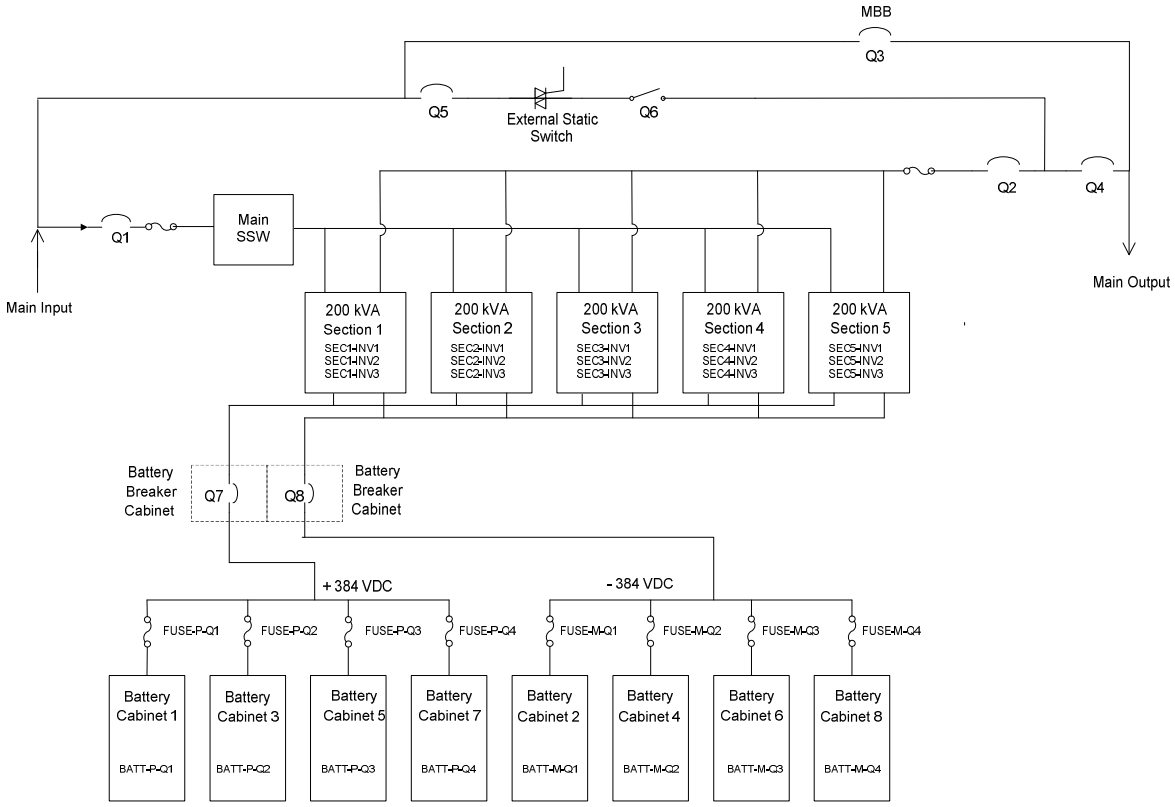
1. The Symmetra MW is at least as reliable as comparable double conversion UPS with similar power ratings, with an expected mean time between failure (MTBF) of about 1 million hours when operated with a redundant power section. This figure includes the effects of UPS, battery, static bypass, and utility failures, even when the ultimate cause was beyond APC's control. MTech's method of calculating MTBF should reflect what a knowledgeable and competent customer will experience when operating a Symmetra MW. Failure as defined in this study encompasses all cases where power to the critical load is lost for any reason.
2. The system is highly redundant and contains no single points of failure except for catastrophic failures of the input bus, output bus, and output circuit breaker. These failure modes are present in any large UPS, although they are often neglected or discounted. The design and testing of the Symmetra significantly reduces the probability of these already rare failure modes.
3. The redundant, modular design improves system reliability and availability. The system is more reliable than its major components. The calculated MTBF of the power modules and other major subassemblies are similar to competitors' claims.
4. In a single Symmetra MW system with one redundant power section, the largest contributions to failure arise from the requirement that most repairs are performed with the system in maintenance bypass, because utility failure during the time the system is in bypass will lead to critical load drop.
5. Reducing repair time, which reduces the time the load is exposed to utility failure, reduces this risk. The modular design allows for rapid, low-risk replacement of nearly all major components.
6. A redundant inverter section (e.g., 1 MW system with less than 800 kW load) significantly reduces the risk of load drop, by roughly a factor of 7, as compared to the non-redundant configuration.
7. A detailed analysis of the objections to delta conversion online reveals that most are without merit, and the remainder are the result of design choices rather than topology. Refer to Appendix A for more information on this topic.
8. The high efficiency of delta conversion online results in less heat generated and significantly reduced component operating temperatures compared to less efficient double conversion designs. Elevated operating temperature significantly reduces the reliability of nearly all components. Our study did not include the effects of this important consideration because we lacked quantitative data about the typical component operating temperature of competing products. This means that our results are probably conservative, and it is quite possible that the MTBF of the Symmetra MW fleet will be significantly higher than our predictions.

System Description

The APC Symmetra MW is a delta conversion online uninterruptible power supply (UPS). Symmetra MW can be configured to support loads from 400 kW to 1.6 MW as a single system, or larger loads if multiple Symmetra MWs are connected in parallel. (Our study did not examine parallel configurations.) The design is highly modular, with power modules, controls, and most major sub-assemblies housed in a standard

modular frame. The modularity provides subtle but important benefits for the economy, reliability, and availability of the system. **Figure 1** presents an elementary one-line diagram of a Symmetra MW system rated 1 MW.

Figure 1 *– One-line diagram of a Symmetra MW rated 1 MW*



Advantages of Small Power Modules

The Symmetra MW differs from comparable products in its use of relatively small (67 kW) single-phase power modules, with three such modules in each 200 kW 3-phase section. Customers have the option of purchasing a unit with unpopulated 200 kW power sections. These sections are populated with power modules as critical loads grow. This practice provides economic benefits to customers who are uncertain about the magnitude of future critical loads, but it has no significant effect on

the reliability of the system, and will not be considered in this report. (The reduction in risk from the simplified upgrade is considerable, but not considered in this study

Many competing UPS utilize parallel units to achieve higher power levels, but typically each unit is based on a “stand alone” product. That is, each parallel unit has all the components and features of a full 3-phase UPS product, including rectifier, inverter, controls, DC bus, protection circuits, and, sometimes, a static bypass circuit. These modules tend to be fairly large. APC’s Silcon product line offers the capability of paralleling modules rated up to 500 kW to achieve higher power levels. The offerings of Liebert, MGE, and Powerware also utilize parallel 3-phase modules rated 100 to 500 kW or more to achieve higher power levels and/or redundancy.

Economic Advantages of Small Modules

There are several economic arguments for the use of smaller modules. Economic analysis is integral to practical, actionable reliability analysis. The goal is not simply to achieve the highest possible reliability, but to find the system that produces the highest reliability within the limits of money, space, and time. The essence of invoking economic arguments in a discussion of reliability is this: If two comparable systems are equally reliable, the lower-cost system should be purchased, freeing scarce funds for further reliability improvements or other purposes. Estimation of “cost” is an imprecise art at best; and individual needs, time preferences, budgetary limits, and risk tolerance will influence any decision to purchase. Sophisticated buyers tend to use discounted future value analysis of the costs of the product over its useful life.

Smaller modules will be produced at higher volume than larger modules, allowing the introduction of automation and other manufacturing techniques that can reduce unit cost while decreasing the incidence of manufacturing defects. A product serving a 100 MW per year market for 1 MW UPS, with each UPS built from two 500 kW modules, will construct 200 such modules, while the Symmetra design results in the production of 1,500 power modules.

A second economic argument applies to redundancy. A system based on 500 kW modules can offer a redundant 1 MW UPS by incorporating 3 modules. The Symmetra MW provides redundancy by incorporating 3 additional power modules in one 200 kW bay, increasing the total from 15 to 18. The Symmetra design affords the same degree of redundancy with a 20% increase in the number of modules while an alternative using 500 kW modules requires a 50% increase.

The Symmetra MW’s 67 kW module is compact and light enough to be safely handled by two qualified people. It can be removed and replaced quickly and it has no user-accessible controls, indicators, or bypass circuits. A 500 kW module is very large and heavy and requires mechanical assistance in handling. Removing and replacing a Symmetra MW power module is a matter of some minutes while replacing large power modules requires hours or days. The time and difficulty of replacing large modules means that, in most cases, large modules are repaired in the field rather than replaced with factory-tested units. Symmetra modules are replaced in the field and are invariably repaired at factory facilities. Both the quality of repairs and the significant disparity in repair time have powerful effects on system reliability.

Reliability Implications of Modularity

Basic considerations of reliability suggest that simplicity is a virtue, i.e., devices with fewer parts have fewer parts to fail. Given two devices that accomplish the same function, one with twice as many parts as the other, many people will use intuition to support a belief that the simpler device is more reliable. Unfortunately, intuition is a very poor guide for understanding low probability events.

Thoughtfully applied complexity can and does improve system reliability. Nearly all modern automobiles have dual braking circuits and computer-controlled anti-lock brakes. These systems are more complex than a single-circuit hydraulic system, but are many times more reliable and much safer in handling emergency stops.

Carelessly adding extra components can reduce system reliability, however, informed design and testing of more complex systems can result in significantly improved reliability. Broad claims regarding the "optimum" number of components or modules do not withstand informed scrutiny. When the arguments offered to support such claims ignore basic redundant features common to modern UPS, they lose credibility.

MTech's exhaustive analysis of the reliability of the Symmetra MW shows that the product should be at least as reliable as competing large UPS products. The definition of failure used in our study encompasses all cases where power to the critical load is lost for any reason. Many published figures exclude "external" causes such as malfunction of the battery plant. Some manufacturers specifically exclude failures that occur during or after preventive maintenance or repairs, thereby obscuring the very significant sources of failure arising from these inherently risky procedures. MTech's conservative definition of failure and analysis means that, given claims of equal reliability, the Symmetra MW will generally be less likely to fail.

APC produces 15 power modules per MW while competing large UPS designs produce 1 or 2. In addition to the economic advantages mentioned earlier, this strategy allows APC be more effective in their reliability growth management process. APC is able to identify any defects in the Symmetra power module roughly 10 times faster than in a comparable large module product line. Ultimately, APC should be able to identify a defect that occurs 10 times less frequently than a competitor can hope to discern.

APC identifies defects and crafts appropriate responses to realize the advantages of higher unit production volumes. APC's commitment to and execution of its reliability growth management program is among the best in the industry and APC makes effective use of this important competitive advantage.

Benefits of Modular Design for Repairs

The reliability implications of larger unit volumes, mass production techniques, and reliability growth management practices are substantial. The effects of modular design on the repair process are much more dramatic and visible. APC's modular design introduces fundamental changes to the process of repairing failed UPS that will be immediately beneficial and readily apparent to informed customers.

Operation, failure, repair, and return to service constitute a cycle whose complexity is rarely acknowledged or scrutinized. A system architecture based on replacement of modules results in profound changes in this cycle. The chart below summarizes the differences in the repair process that results from a modular design versus a typical large or monolithic UPS whose modules are repaired in the field.

Figure 2 *– Repair Process: Comparison of Monolithic vs. Modular Design*

Repair Step	Monolithic Design	Modular Design	Advantage
Detection of failed components or modules	Generally Automated. Parallel operation of independent UPS can complicate detection and isolation	Automated. Modules designed with self-testing and isolation features.	Potential slight advantage for modular design.
Acknowledgement of failure by operator	Operator response	Operator response	No significant difference.
Mobilization of repair personnel.	Highly trained service personnel required. They constitute a scarce resource that is rarely available on-site	Minimally trained personnel can change failed or suspect modules	Significant advantage for modular design: more numerous, less costly personnel, reduced response time.
Confirmation/diagnosis of component failure	Many failures must be traced to individual components. This often requires field test procedures and time.	Failures need to be traced only to the module level. Component failure diagnosis takes place at factory repair facility.	Modular design offers reduced time for diagnoses, decreased opportunity for introduction of latent defects.
Troubleshooting	Field testing and replacement of suspect parts	No troubleshooting performed in field. Factory module repair.	Modular design offers substantially reduced risk of introducing new latent defects and/or misdiagnosis.
Procurement of spare parts	Wide variety of spare parts required	Modules replaced for all component failures	Greatly reduced spare parts inventory for modular design. Higher probability of having required spares on-site.
Installation of new parts	Field work	Replace module for most failures	Significant reduction in potential for introduction of latent defects in modular design.
Testing	Complete testing is generally impossible	Module fully tested at factory. System confirms module operation.	Very significant advantage for modular design. All repairs tested to original factory standards.
Return to Service (RTS)	Procedure depends on nature of repair	Standard procedure and automated RTS	Significant advantage for modular design due to lower potential for operator error.
Demobilization (Removal of test equipment, parts, trash, and service people from the site.)	Procedure depends on nature of repair	Standard procedure after module replacement	Modest advantage for modular design due to reduced probability of introducing latent defects.

The mobilization, troubleshooting, spares procurement, installation, testing, and return to service steps are all significantly faster, less risky, and/or less costly in a modular system design. The risks of ad-hoc troubleshooting procedures, field repairs, and field replacement of suspect parts are quite substantial. They provide multiple opportunities for human error and the introduction of latent defects in the repaired UPS. It is generally impossible to subject a field repaired UPS to the full suite of functional and performance tests performed on every new unit by all manufacturers of high-quality UPS. In contrast, modular design eliminates nearly all field repair and troubleshooting. Modules are replaced and returned to the factory for these procedures. The new (or repaired) modules are fully tested before leaving the factory.

Availability Advantages

The ability to quickly replace failed modules reduces repair times. Availability is a measure of average time the system is operational, so reducing repair time will increase availability. When operated with redundant power modules (e.g., no more than 800 kW load on a Symmetra rated 1 MW) it is possible to reduce repair times to as little as 15 to 30 minutes, with most of the repair steps shown in **Figure 2** completed before the unit is taken off-line. Repair time in this report is defined as the time the critical load is exposed to the utility or generator plant while the UPS is shut down for repairs.

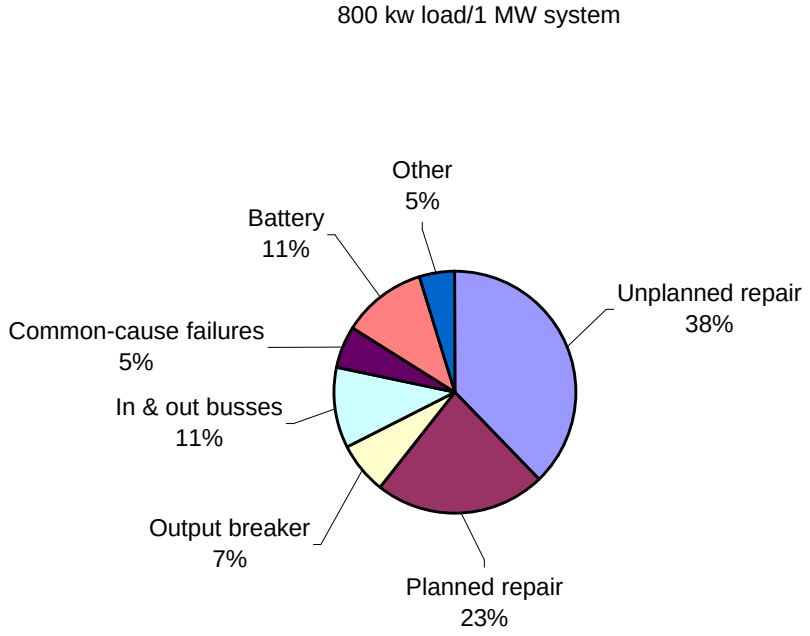
Availability must be defined carefully if it is to provide meaningful and useful guidance to customers. MTech takes the view of the end-users of the equipment protected by the UPS. If the equipment is operating normally, it is available to these users. We define the system as available even when the load is momentarily transferred to utility power in order to replace a module, as long as there is no utility upset during that interval. This does not mean that there will be no module failures during the normal lifetime of the system. Modules can fail and be replaced, but as long as the protected equipment is powered and available, no failure has occurred. Our study predicts that the Symmetra MW MTBF exceeds 1 million hours.

Results of Fault Tree Analysis

Fault tree analysis is conducted by constructing logical models of how combinations of component failures can ultimately result in system failures. The highly redundant design of the Symmetra MW means that single component failures rarely result in system failure, defined as loss of power to the critical load. The “logic of failure” contained in the fault tree is combined with standard component failure rates to produce estimates of system reliability. Fault trees are shown and discussed in the Appendix.

Figure 3 shows the results of our analysis for a 1 MW (5 section) Symmetra protecting a critical load of less than 800 kW. This results in one redundant power section (N+1).

Figure 3 *– Component contributions to system failure rate in Symmetra MW operated with N+1 redundancy in power modules*



The major contributors to failure are (in clockwise order):

- **Unplanned repairs (38%)**: are failures that force the system to static bypass. In this state any failure of the electric utility causes system failure. Unplanned repairs were modeled as lasting an average of 24 hours. APC uses a relatively high utility failure rate of 3.89E-03 failures per hour in their internal calculation of system availability and reliability. This value corresponds to a mean time to utility failure of 257 hours, with more than 34 expected events per year on average. This conservative (pessimistic) utility failure rate serves to highlight the demand failure modes and sensitivity to repair times. In some areas of the US with networked utility distribution networks, the actual failure rate may be 10 times lower. Increasing the utility MTTF to 1000 hours reduces the expected system failure rate by over a factor of 3.

  The ability to plan repairs means that they are no longer random, and probabilistic methods are best applied to random events. In contrast, the "unplanned repair" is a truly random event, as repairs must begin immediately if the system is to be repaired and returned to service in 24 hours. The modeling of unplanned repairs may be somewhat optimistic, as it can be challenging to complete many repairs in 24 hours.

- **Planned repairs (23%)**: are failures in system components (primarily power modules) that do not force the UPS into static bypass because redundant components are available. Planned repairs were modeled as lasting an average of 30 minutes on utility. During this interval, the critical load is subject to utility failures.

Our modeling of the planned repair event is somewhat conservative (pessimistic) in that it assumes the same utility failure rate during the brief repair window. In reality, the operators of the system avoid making repairs during periods where failure is more likely or the consequences of failure are more severe. Large financial firms generally prohibit repairs during trading hours. Repairs are not conducted during storms, heat waves, or other conditions that threaten utility reliability.

- **Output breaker (7%)**: Spurious trip of circuit breakers (tripping when load current is within the rated current of the device) places a significant limit on reliability of all electric power systems. Data gathered in the US nuclear power industry over a population of some 27,000 units in non-radiation environments shows a failure rate of 1.2 x 10-7 per hour, corresponding to a MTTF of 5 million hours, or 57 years.[1]

- **In & out busses (11%)**: Catastrophic failure of an input or output bus (e.g. persistent line-to-line or line-to ground faults) causes the system to fail. While failure of the input bus does not cause immediate failure, it does prevent charging of the UPS batteries, and battery exhaustion is inevitable.
  The input and output bus failures are significant not because they are likely, but because just one such failure will disable the system. These failure modes are common to all large UPS and are not a result of the Symmetra modular design. The only way to eliminate these important failure modes is to utilize a data center architecture based on many smaller UPS rather than one large UPS. Interested readers will find more information in the APC White Paper #111, prepared by MTechnology, that applies PRA analysis to such an architecture.[2]

- **Common-cause failures (5%)**: These are failures that cause multiple components to fail due to a single cause. Common-cause failures place very severe limits on the benefits of redundancy. Sources of common-cause failures are varied: design or manufacturing defects; fires, floods, and other natural disasters; and catastrophic failure of one component so that plasma or shrapnel cause nearby components to fail.

  A very significant source of common-cause failures in data centers is periodic maintenance when improper procedures or failure to return the system to a fully operational state can disable all UPS or generators or batteries simultaneously. Our detailed examination of the Symmetra MW design, test, and manufacturing facilities revealed no particular sources of common-cause failures. The modular design and redundant, fail-safe control system architecture lends itself to simple test and maintenance procedures that are unlikely to result in load drops even after operator error.

[1] "Review of Operational Experience with Molded Case Circuit Breakers in US Commercial Nuclear Power Plants," et al., NRC AEOD/S92-93, 1992.

We use a value of 10-8 failures per hour corresponding to a mean time to failure (MTTF) of 100 million hours, or 11,400 years. The fact that such a rare failure is expected to cause 5% of all failures is testament to both the power of common-cause failures, and the reliability of the Symmetra MW.

- **Battery failures (11%)**: are primarily demand failures that occur when the utility fails and the battery fails to provide sufficient power to protect the load for the specified interval. Our model is based on multiple strings of VRLA batteries, and includes circuit breakers, fuses, connections, and controls. We account for the Symmetra's ability to automatically perform periodic tests of the battery, and for the fact that the test is not 100% accurate in identifying failed battery cells. The tests deplete the battery plant and shorten its lifetime, so we modeled a test scheduled for every 3 months. A large battery plant with many cells and connections offers many opportunities for failure, and the significant contribution from the battery plant arises from both detectable failures that occur between periodic tests and undetectable failures that are revealed only during actual battery operation. The result is also influenced by the large number of demands that follow from APC's very conservative (pessimistic) estimate of the utility failure rate.

- **Other (5%)**: represents all other sources of failure. Despite the fact that the Symmetra MW, and our model, has a very large number of components, only a few components cause 95% of all failures. Note that power module and control module failures do not show up in the top 95%, because the redundant design prevents module failures from causing system failures.

Benefits of Redundancy

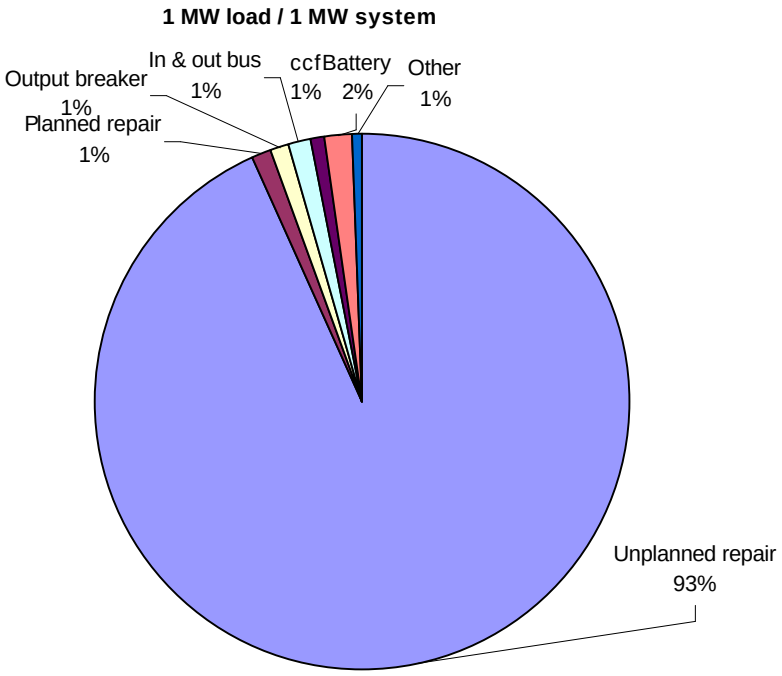
Most customers will operate the Symmetra MW with N+1 redundant power modules. For example, a 1 MW critical load would normally be served by a Symmetra with 6 sections, capable of 1.2 MW. Failure of any power module or section would not force a transfer to bypass.

If the Symmetra is instead configured to operate without redundant power modules, the overall probability of failure per year of operation increases by a factor of 7. The distribution of the causes of failure changes even more dramatically, as shown below.

Figure 4 displays the results of our analysis for a 1 MW (5 section) Symmetra protecting a critical load of 1 MW. There is no redundant power section.

[2] "Reliability Analysis of the APC InfraStruXure Power System," White Paper #111, MTechnology, Inc.

Figure 4 *– Component contributions to system failure rate in Symmetra MW operated with no redundant power sections*



Unplanned repair now accounts for almost all failures. Power module failures force the system to static bypass. The repair is now truly random (operators are as likely to be called at 2 AM as 2 PM). The entire repair process, from acknowledging the failure to mobilization of manpower and spare parts, occurs during this interval, which we modeled as lasting 24 hours. It is generally difficult to gain access and permission to repair critical infrastructure in less than 24 hours in large data centers with well-established change management procedures.

Conclusion

MTech's analysis of the APC Symmetra MW shows that the designers have produced a very reliable, easily maintained and repaired product. The causes of failure are evenly distributed among the UPS and its associated components. This is a sign of thoughtful design. If all the risk arises from just 1 or 2 components, designers should better utilize their resources to reduce the probability of those particular items.

The modular, redundant nature of the Symmetra MW has profound, very beneficial effects on the repair process. Repair quality is greatly improved and repair time is greatly reduced. No machine is perfect, and failures will occur in the fleet of any successful product, no matter how reliable. APC's thoughtful engineering and rigorous testing has produced a UPS that performs as well, and very possibly better, than competing designs based on parallel operation of a few large modules.

About the Authors:

Steve Fairfax is President of MTechnology, Inc. Steve joined MTech in 1997, but he has been working with multi-megawatt power systems since his undergraduate days at MIT, where he helped build and operate a 200 MW power system for a tokamak fusion reactor. He began full-time study of power system reliability while working as Managing Engineer for Failure Analysis Associates. He served as head of engineering and operations for the Alcator C-MOD nuclear fusion reactor during its design and initial operation at the MIT Plasma Fusion Center, and as principal engineer in Boston-area firms. Mr. Fairfax holds Master's Degrees in both Physics and Electrical Engineering from MIT.

Neal Dowling is a senior engineer at MTechnology, Inc. He performs fault tree analysis and related modeling and simulation, develops and tests new power supply and switch technology, and supervises the operation and maintenance of MTech's 400 kW fuel cell power plant facility. Neal worked at several Boston-area medical device manufacturers prior to joining MTech. His expertise includes development and maintenance of firmware and software for critical functions, FDA compliance, and analog and digital design. Neal holds Bachelors and Masters degrees in Electrical Engineering from MIT.

Dan Healey is a senior engineer at MTechnology, Inc. He specializes in human factors analysis and the applications of PRA techniques to operations and maintenance activities. Dan served as Director of Engineering at several Boston-area firms, overseeing product development for semiconductor processing, medical equipment, robotics, and electro-optical systems. Dan holds a Bachelors degree in Electrical Engineering from the University of Rochester with additional graduate work in optics and programming. He is presently a special student at Harvard studying management of technology and software development.

MTechnology, Inc. provides power systems engineering for the 21st century. The firm offers consulting, testing, product development, and prototype fabrication services.
MTech performs probabilistic risk analysis of electric power systems, design reviews, root cause failure analysis, and provides expert testimony in both regulatory and litigation settings. MTech offers consultation on risk-informed system design, operations, maintenance, upgrades, and reliability growth management. Clients frequently realize substantial savings on capital and operating expenses while simultaneously increasing reliability. MTech's facilities include a 5,000 square foot test and laboratory facility with ability to operate 500 kW continuous loads and multi-megawatt pulsed loads. MTech has worked on high-reliability distributed generation projects spanning technologies from reciprocating engines to fuel cells. The firm's clients include electric utilities, designers and engineers, critical facility owners and operators, and manufacturers serving the 7x24 mission critical industry.

Appendices

Appendix A: Delta Conversion OnLine versus Double Conversion UPS

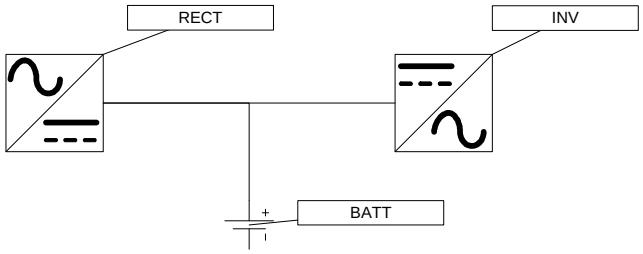
Appendix B: Load Faults and Coordination failures

Appendix C: Fault Tree Models

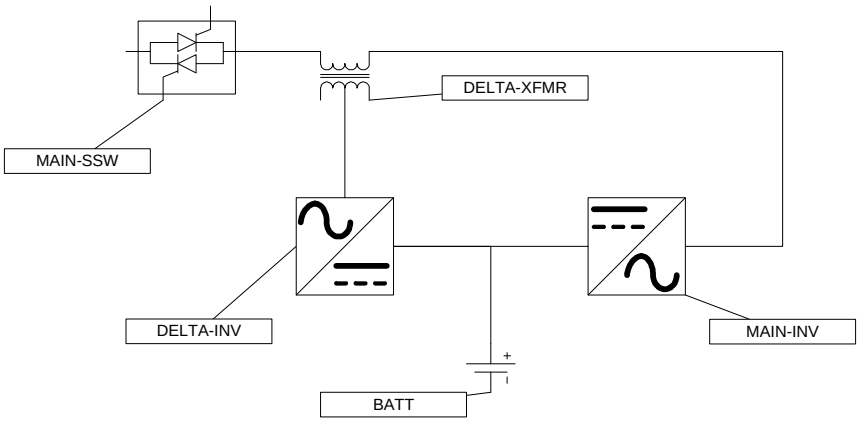
Appendix A: Delta Conversion OnLine versus Double Conversion UPS

The delta conversion online circuit topology is more subtle and, at first, more difficult to understand than the standard double conversion UPS. The delta transformer functions as a current transformer. Most electrical engineers are familiar with voltage transformers, but the few who work with current transformers use them primarily as sensors, not dependent sources.

Comparison of conversion designs: Double conversion vs. Delta Conversion



Double-Conversion UPS



Delta-Conversion UPS

A common criticism of the delta conversion UPS is that it is more complex. This argument states that the double conversion UPS, having fewer components, should be more reliable. This argument was discussed in the body of this report, and found to be flawed. (Dual braking circuits in automobiles are both more complex and more reliable than single-circuit designs.)

If we assume that the following components have approximately equal failure rates (double conversion component first):

- INV and MAIN-INV,
- BATT and BATT,
- RECT and DELTA-INV,

the delta conversion UPS has additional components: MAIN-SSW and DELTA-XFMR. Both static switches and dry-type transformers are relatively reliable components (less than 10-6 failures per hour) so we expect the contributions to failure from these components to be relatively small. Both types of UPS generally have a redundant power path provided by a static bypass switch that will supply utility power to the load if the UPS components should fail. The addition of a static bypass switch will further reduce the difference in reliability between the two types of UPS. Finally, both designs are subject to common-cause failures. Control system failures of large double-redundant UPS cause a significant fraction of all load drops. Reliability in real-world operation is determined by architecture and execution, rather than simple component count.

The reliability of physical products is strongly affected by detailed design choices, whether or not the designers apply appropriately conservative margins to critical components, manufacturing quality, repair quality, operating environment, and the efficacy of the manufacturer's reliability growth management program, if one exists. These factors are much larger than the effects of adding one or two circuit elements.

Some potential customers object to delta conversion. During the course of this study, MTech engineers have encountered the following statements regarding the merits of delta conversion.

It is Line Interactive - not as good as OnLine Double conversion.

"Line interactive" is a term of art that describes a particular UPS configuration. Among other attributes, the single inverter in a line interactive UPS is always connected to the critical load, but generally is not operated when utility power is present, except to charge the batteries. Some models include tap-changing transformers or other means to compensate for high or low utility voltages. The delta on-line topology is distinct from line interactive designs, and its delta inverters normally operate whenever the utility is present, unlike most line interactive designs. The delta conversion on-line UPS interacts with the line, as does any UPS, but it is certainly not a "line interactive" design as the term is routinely applied.

"Not as good" is a value judgment and cannot be supported or refuted by logical, scientific, or engineering arguments. The implication is that "double conversion" UPS designs are inherently superior to all other circuit designs. There is no logical or empirical evidence to support such a broad claim. Certainly modern double conversion UPS are more reliable than 40-year-old line interactive designs, but they are also more reliable than early double conversion products. Our analysis of the delta conversion online circuit topology concluded that the reliability of power modules, inverters, and other major components were essentially identical to their counterparts in double- conversion UPS.

Delta conversion cannot perform frequency conversion, and must be synchronized to the utility.

The statement is true in that the output of a delta conversion UPS is obliged to be at the same frequency as the input. However, the implication that this is a defect is false for two reasons. First, modern computer loads are not frequency sensitive. Nearly all modern switch-mode power supplies are rated to operate at any frequency between 48 and 63 Hz, and many would function over an even greater range.

Second and more importantly, the requirement to keep UPS output synchronized to the input AC waveform comes from the use of a static bypass switch. Nearly all large UPS, whether double conversion or delta conversion or other designs, incorporate a static bypass switch. It provides a parallel path and is essential to achieving high reliability. Without the static bypass, all UPS would be simple series elements and any failure in the UPS would cause failure of the critical load. The bypass switch fundamentally alters this behavior. Typical large UPS power sections have a mean time to failure of approximately 150,000 hours. Only when operated in parallel with a bypass switch does the system MTTF approach or exceed 1 million hours.

UPS input and output waveforms must remain closely synchronized or the static bypass switch will be disabled. Attempting out-of-synchronization transfers in a large UPS carries the near certainty of saturating downstream transformers, resulting in large currents and operation of protective devices. Both double conversion and delta conversion UPS must synchronize input and output waveforms. The loads are not sensitive to frequency, so attempting to operate a double conversion UPS as a frequency changer poses serious risks (loss of static bypass protection) with no benefit.

The delta conversion UPS has a high battery voltage. The large number of batteries in series reduces reliability for the battery and is a safety issue.

Most large double conversion UPS utilizes between 192 and 240 cells in series, for a nominal open-circuit voltage of 384 to 528 volts. The Symmetra MW delta conversion UPS utilizes two strings of 192 cells in a center-tapped configuration, resulting in a total of 384 cells in series, for a nominal open-circuit voltage of 768 volts.

The choice of DC bus voltage is a design parameter, and both delta conversion and double conversion UPS design engineers selected the battery voltage for a variety of reasons. Choosing a lower DC voltage does indeed result in fewer cells in series, but it necessitates the use of input and output transformers. These series devices introduce losses (which can add significantly to operating costs in large systems) and multiple new failure modes. The choice of a +/- 384 volt DC design allows the elimination of all internal transformers, although one can be added if isolation is desirable in a particular application. The reliability of either DC source is of secondary interest to the customer; the reliability of the system is what is more important. System reliability can be determined only in the context of a larger study of system reliability, and must rely on analytical methods (such as this document) or historical field data. Establishing that one DC voltage choice carries noticeable advantages would require much more than a simple count of cells.

The issue is rendered moot if more than one battery string is connected in parallel. Open-circuit failures in a single battery string are the most serious failure mode, as they deprive the inverter of all DC voltage. Since the battery is discharged only when the utility is failed or grossly out of tolerance, an open-circuit cell failure will generally cause a load drop. Parallel strings reduce the importance of this failure mode to negligible values. Open-circuit cell failures in a parallel string bank cause reduction in battery hold-up time, but so long as the remaining string(s) can support the load until standby generators are dispatched, there is no load drop. Whatever merits there are to arguments about the number of cells in series, they are generally rendered insignificant if parallel strings of batteries are utilized.

The issue of safety does not withstand scrutiny. All large battery banks are extremely dangerous, as they cannot be switched off, supply lethal voltages, and are capable of supplying extremely large fault currents. The potential with respect to earth is large enough to injure or kill in both systems. National and international codes and standards make no distinction between these two designs. As long as the potential with respect to earth is maintained at 600 volts or less, the protection, construction, and insulation requirements are identical for both designs.

The battery is center tapped and connected to the AC neutral.

The Symmetra MW battery string(s) are indeed center tapped and connected to the AC neutral, but we have discovered no evidence that this represents a safety hazard or affects reliability in any way. Our analysis of other large UPS systems required basic events (failure modes) arising from a significant number of plausible electrical faults that would cause cascading failures of key components. Our review of the APC design documents showed that designers had anticipated all plausible faults and demonstrated successfully that components would not be subjected to excessive stresses.

Delta conversion is a new unproven topology, and is not as reliable as Double-Conversion.

This criticism is based on the wholly erroneous belief that reliability of products automatically increases as systems age. The lessons of both history and analytic investigations demonstrate that reliability is determined by design, component quality, manufacturing quality, and repair quality. The fact that the reliability of a fleet of similar products sometimes increases over time is due to reliability growth management, where the lessons implicit in field failures are used to remove defects from the existing fleet, and inform new designs. The original equipment's reliability remains unchanged unless and until effective field upgrades are completed.

MTech has studied numerous double conversion UPS, delta conversion, rotary UPS, fuel cells, and other, more exotic designs. We have never encountered a UPS topology that was demonstrably superior to all others. We have learned that system architecture with respect to features like modularity and redundancy play a much greater role in reliability than basic circuit topology. Manufacturing quality, operator interface, and field service policies play an equally important role. The delta conversion online topology itself is not significantly more or less reliable than double conversion.

Delta conversion is more complex than Double conversion, reducing reliability.

This argument is based on the simplistic notion that more parts results in more failures. But if this were true, then an N+1 system would be inferior to a non-redundant alternative. The use of redundancy to achieve high reliability demonstrates that it is how parts are added, not just the number of parts that determines system reliability.

It is true that delta converters have more functional components than double conversion UPS. But all large UPS have a static bypass, which keeps the critical load safely powered during most UPS failures. The operation of the parallel static bypass switch greatly reduces the significance of the number of components in the power circuits. Further, the fault-tolerance achieved with multiple power modules means that component failures need not result in operation of the static bypass. This advantage is not confined to delta conversion; modular designs confer benefits with many circuit topologies.

The delta conversion main inverter does not utilize a transformer, and there is no isolation between load and battery.

An isolation transformer can be added to the system if required or desired. The use of isolation transformers in most competing products is a consequence of choosing a DC voltage too low for direct conversion to appropriate AC levels. This argument attempts to make a virtue out of necessity, but in reality either circuit topology can choose to use isolation transformers, or not.

Delta conversion results in more frequent battery discharge, and higher ripple on DC link due to two inverters, shortening battery lifetime.

Battery lifetime is reduced by each discharge. Deeper discharges are more damaging. The delta conversion online approach automatically provides some ability to operate from out-of-tolerance AC input voltage without discharging the battery. The voltage tolerance is set by the designers when they choose the delta transformer characteristics and DC link voltage. Double conversion UPS designers often employ buck or boost converter functionality in the input rectifier in order to provide the same ability to reduce the frequency of battery discharge. In either case, the designers, who must defend their choices to management and ultimately the market, choose the parameters. Neither topology offers a significant advantage with regard to AC input voltage range and battery discharge. The issue of DC link voltage and current ripple is likewise controlled with inductors, capacitors, and design in both circuits.

Delta conversion is not compatible with generators due to its inability to provide frequency conversion.

As discussed earlier, using a double conversion UPS to provide frequency conversion is a very poor choice from a risk and reliability perspective, because it disables what is probably the most significant protective component in large UPS, the static bypass switch. Modern data center loads are insensitive to any reasonable frequency variation and there is no basis for requiring frequency conversion. The ability of the delta converter to provide unity power factor and low harmonics under nearly all operating conditions provides a significant advantage for operation from generators. Nearly all generators are subject to a very serious failure mode, self excitation, when operated into a leading power factor load. Self excitation results

in loss of the ability to control generator output voltage. Modern data center loads often present a slight leading power factor, and some double conversion UPS operate with substantial leading power factor when under light load. These systems must be carefully integrated with the generators to avoid self-excitation and critical load drop. Systems using delta conversion products need not concern themselves with this particular problem.

The inverter is kW rated and must be oversized to handle actual load.

Design engineers set the real (kW), reactive (kVAR), and apparent (kVA) power capabilities of both kinds of UPS. Both double conversion and delta conversion online systems can be designed with apparent power greater than or equal to real power ratings. A design with kVA rating larger than kW rating generally includes a reactive power source. Operating generators into equipment with reactive power sources can result in self-excitation and loss of voltage control. APC designed the Symmetra MW with equal real and reactive power ratings, but this was a choice, not a necessity associated with delta conversion online.

The claimed high efficiency of delta conversion online is not true; double conversion is more efficient with actual load.

This is a factual statement, and can be proved or disproved by simple testing. The fact that delta conversion only subjects part of the energy flow to conversion by silicon power transistors, while all energy flow is converted twice in double conversion, suggests that the delta conversion topology is inherently more efficient. Certainly the efficiency claims of both APC and their competitors support the higher efficiency of delta- conversion online.

Delta conversion online can't handle non-linear loads, they cause big distortion on output voltage waveform.

Both designs utilize silicon power transistors to synthesize a nearly pure sinusoidal voltage waveform. The power transistors in both designs are rated for continuous operation at maximum rated power. Any differences in the response of either inverter to a non-linear load are determined by the design of the circuits that measure the output and control the transistors. Neither design is fundamentally more or less susceptible to voltage distortion.

Appendix B: Load Faults and Coordination failures

There are a number of possible failure modes that could have been included in the fault tree but were not. Our analysis of other large UPS, particularly those employing a few 3-phase modules operated in parallel, have considered the potential for load faults or component failures within one module to cause system failure. Typically this results from poor coordination between fuses and circuit breakers, so that a short circuit in one module causes the circuit breakers or fuses from several modules, and sometimes the static bypass, to open. We examined the Symmetra MW and found that the engineers had included specific provisions that render these failure modes implausible, with most requiring multiple simultaneous failures, rather than a cascade where one failure causes the next.

Fuse and circuit breaker coordination is technically challenging for UPS in general and large UPS in particular. It can prove difficult or even impossible to guarantee that protective devices coordinate properly when a few large modules are operated in parallel. Coordination means that the device closest to the fault operates first, with upstream devices operating only if the first device fails to clear the fault.

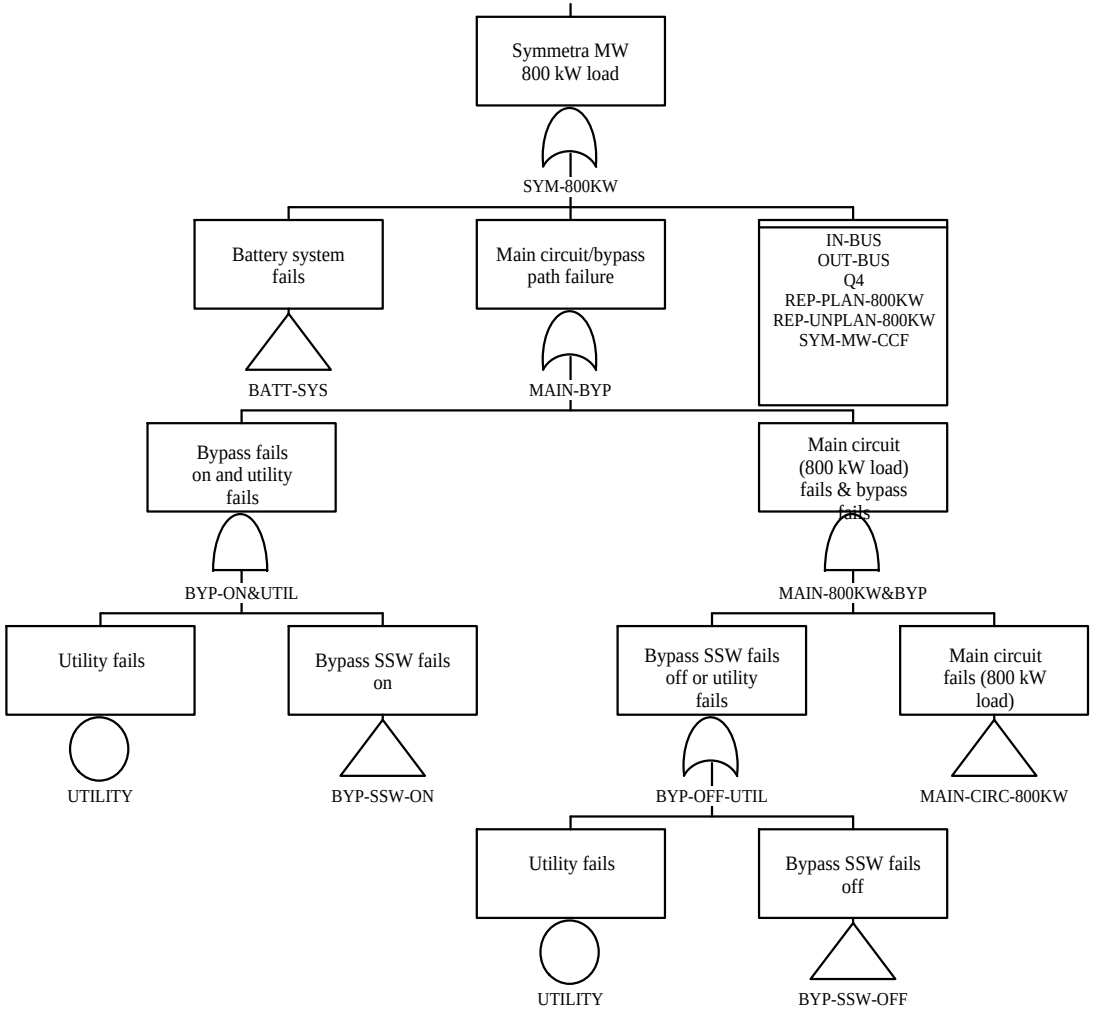
Many large UPS designs are basically multiple complete UPS products operated in parallel. These machines were generally not initially designed for parallel operation. Each UPS includes its own input and output circuit breakers, internal fuses, and other protective functions. The additional requirements for parallel operation, particularly with respect to coordinating the responses of protective devices, can be in conflict with the requirements of a stand-alone UPS.

The Symmetra MW design reduces the probability of coordination failures in two distinct ways. First and most importantly, the designers considered fault current flows and effects in every portion of the system, including input, output, power module, DC bus, AC filter, and external bypass circuits. They adopted a strategy of using high speed fuses that are expected to operate only during short circuits with large fault currents. Each fuse will conduct several times its normal operating current indefinitely. Running fuses in this manner results in very low thermal loses, therefore, long-term temperature-related degradation of the fuses should be negligible. This attention to the details of parallel operation during the design stage eliminated many potential failure modes.

The second aspect of the Symmetra MW design that reduces the probability of fuse and coordination failures is the relatively small size of the power module. A 1 MW system (five sections of 200 kW each) that experiences a fault in a 67-kW module will have 4 modules feeding power to the faulted module. The fuse in the faulted module will conduct four times the current as those in the good modules, and will operate first. In contrast, a 1 MW system composed of two 500 kW modules will have equal currents in the fuse of faulted and working module. There is a distinct possibility that the fuse in the working module will clear before the faulted module. Even if the faulted module's fuse opens first, the fuse in the good module may be degraded and subject to spurious operation in the future as a result of conducting the fault current. It is also much more difficult for the control system to correctly identify which module has failed. Many parallel UPS designs must transfer to bypass on every module failure, and rely on the large fault currents available from the local electric utility to operate the protective devices.

Appendix C: Fault Tree Models

Symmetra MW 800 kW load



Symmetra MW 1 MW load