

APC InfraStruXure

전력 시스템의 안정성 분석

Stephen Fairfax
Neal Dowling
Dan Healey

백서 #111

MTechnology, Inc.

APC[®]

by Schneider Electric

APC InfraStruXure 구성은 중앙 집중식 **UPS**를 대체할 수 있는 설계 및 구조를 제공한다.

MTechnology에서는 확률적 위험도 평가(**Probabilistic Risk Assessment: PRA**) 방법을 이용하여 스태틱 바이패스(**Static Bypass**)가 있는 **40 kW InfraStruXure UPS** 및 **PDU**의 안정성을 평가했다. 이 테스트에서는 이상적 조건과 현실적 조건 모두에서 **InfraStruXure**의 성능을 고찰했다. 또한 이 연구에서는 데이터센터 환경에서 **500 kW**의 임계 부하를 가정하여 **InfraStruXure** 아키텍처의 성능과 중앙식 **UPS**의 성능을 비교했다. 평가 결과 **InfraStruXure** 아키텍처의 경우는 전체 부하의 장애 가능성이 현저히 낮은 반면 개별 **IT** 장비의 장애 가능성은 약간 낮았다. 이 글은 **MTechnology**의 정량적 위험 평가의 주요 결과를 요약하고 그것이 시설 관리자와 설계자에게 어떤 의미가 있는지 논의하고 있다. 글의 구성은, 분석 결과를 가장 먼저 제시하고 제품 분석에 사용된 방법론을 설명한 다음, 분석 결과를 더 자세히 논의하는 순서로 진행된다.

연구 결과 요약

1. APC 제품의 안정성 평가는 대규모 중앙 집중식 UPS 설계 공급업체가 발표한 데이터와 비교 가능하다.
2. 데이터센터의 전력 공급에 500 kW UPS 한 대를 이용하는 경우와 14대의 InfraStruXure UPS를 이용하는 경우를 비교한 결과, APC쪽의 방식이 전체 시스템 장애 가능성이 현저히 낮았다. 양쪽 방식에서 모두 쓰이는 공통 장비(예를 들어, ATS)에 발생하는 장애가 시스템 장애의 가장 중요한 원인이었다.
3. InfraStruXure의 리덕턴트 방식이 안정성을 향상시켜 준다는 점은 명확하다.
4. Mtech은 전력 모듈 장애의 원인과 영향을 분석했는데, 전력 모듈 장애가 더 자주 관찰되는 반면, 그 증가 횟수는 리덕턴스 가 제공하는 상쇄 효과보다 크다는 결론을 내렸다.
5. 일반적인 원인의 고장과 잠재적인 장애 모드의 원인을 상세히 분석해 보면 UPS의 안정적인 리덕턴스 구성으로 발생한 결과와는 거리가 멀다.
6. 유틸리티 고장율에 고장율에 매우 작은 부분을 차지하는 결과를 도출한다. 이것은 InfraStruXure가 의도된 기능을 수행한다는 것, 그리고 고객의 장비가 유틸리티 이전 및 운전 정지의 영향을 받지 않는다는 것을 의미한다.
7. Mtechnology는 APC의 제품 또는 구성요소가 장애율 감소에 기여한다고 말하지는 않았지만, APC 제품이 모듈식 설계로 되어 있고 관련된 제품 수가 많다는 점은 저렴하면서도 결함이 거의 없는 제품을 만드는 전용 생산 시설을 운영할 수 있게 한다. 동일한 전력 등급의 비모듈식 설계방식으로는 전력 모듈을 하나 제조하는 반면, APC는 5개의 전력 모듈을 제조한다. 덕분에 제품의 안정성 향상이 더욱 가속화된다.
8. InfraStruXure 아키텍처의 사전 제작식 분배 배선 방식은 중앙집중식 UPS 제품의 현장 배선식 분배 시스템에 비해 상당한 이점이 있다. 분배 배선 방식은 결과적으로 핵심 장비에 대한 전력 공급 손실을 야기할 수 있는 배선 결함 가능성이 높다. 현장 배선 프로세스와 사전 제작 배선 프로세스에 대한 분석 결과, 현장 제작 시스템의 결함 확률이 그와 동급의 사전 제작 시스템에 비해 1,500배가 높았다. 그러나 Mtechnology는 이 분석에서 APC가 고장률을 낮춘다거나 중앙식 UPS가 고장율을 높인다는 결론을 내리지 않았다.

개요

APC(American Power Conversion Corp.)는 MTech(MTechnology, Inc.)에 스태틱 바이패스(static bypass)가 있는 InfraStruXure 40 kW UPS 및 PDU의 안정성 분석을 의뢰했다. APC의 목적은 제품의 안정성 파악, 잠재적 장애 원천 규명, 제품 안정성 및 가용성의 향상 가능성 평가 등에 확률론적 위험 평가(PRA) 기법이 유용한지 여부를 확인하는 것이었다. InfraStruXure는 안정성을 높이기 위해 여러 구성요소에 이중화를 적용하고 가용성을 높이기 위해 '핫스왑' 기술을 적용한 제품이다. 또한 APC는 InfraStruXure 제품 라인을, 하나 또는 여러 열의 장비 랙에 맞도록 사후 증설이 가능한 제품으로 시판하고 있다. 이러한 방식은 중앙집중식의 대형 UPS 하나로 데이터센터 전체를 담당하는 방식에 대한 대안이 된다.

Mtech은 1997년부터 상시 운영 시설에 대한 공식적인 정량적 안정성 분석 기법을 적용해 온 회사다. Mtech은 미국의 핵발전 산업의 안정성 향상에 투자한 수백만 달러의 자금과 수십 년 간의 경험을 토대로, 상시 운영 시설의 높은 안정성과 가용성을 달성하는 연구에 PRA 기법을 채택해 왔다. MTech의 고객으로는 전력회사, 제조업체, 설계 회사, 기간 설비 관리 및 운영 업체 등이 있다.

Mtech은 스태틱 바이패스를 갖춘 InfraStruXure 40 kW UPS 및 PDU에 대한 세밀한 분석을 실시했다. 오류 트리 분석(fault tree analysis)을 1차적 기법으로 사용하고 이벤트 트리 분석을 통해 보완했으며 베이지언(Bayesian) 업데이트를 통해 빈약한 데이터로부터 구성요소 장애율을 파악해냈다.

본 연구에는 분리 상태의 제품에 대한 분석, 전형적인 데이터센터 환경에서의 분석, 데이터센터의 일반적인 중앙집중식 UPS 구성을 대상으로 하는 안정성 비교 분석 등이 포함되어 있다. 분석 내용에는 전기적 설계 및 기계적 설계, 엔지니어링 확인 및 검증 테스트, 제조 기법, 실제 작동 상태에서의 장치 성능 등에 대한 상세 검토가 포함되어 있다. Mtech은 APC의 설계 엔지니어링팀, 제품 지원팀, 판매 및 서비스 데이터베이스 담당자, 고위 경영진 등과 인터뷰 조사를 수행했다.

MTech의 일부 엔지니어들은 본 제품의 안정성 및 가용성을 평가하기 위해 구성된 수학적 모델을 확인 및 확장하기 위해 덴마크 콜딩(Kolding)에 위치한 APC 설계 센터를 방문하여 제품 설계 담당자 및 지원 엔지니어 등과 함께 작업했다.

서론

24시간 중단 없이 작동해야 하는 정보 시스템의 필요성이 커지면서 이와 같이 비교적 새로운 시장을 대상으로 제품과 서비스를 공급하는 산업이 급속히 생겨나서 성장해 왔다. 주문형(on-demand) 정보 서비스의 활용과 그에 대한 수요가 대형 메인프레임 컴퓨터 기반 기업 데이터베이스(예를 들어 항공 예약 시스템)나 대형 금융 기관을 중심으로 자리잡게 된 후, 현재는 전세계 모든 기업과 사무실에 그 영향을 미치고 있다.

그런데 이와 같은 주문형 서비스에는 전력 공급의 안정성이 필수적이다. 전력망(Electric utility network)만으로는 전력 공급의 안정성 및 품질 요건을 충족하지 못한다. 일반적으로 전력망 보호 시스템은 전기가 흐르는 전도체에 접촉했을 때 인명과 장비를 보호하거나 장비 장애를 방지하기 위해 전원을 차단하도록 설계되어 있다.

전력의 안정성 향상을 위해 선택할 수 있는 제품으로는 비상용 무정전 전력공급장치(Uninterruptible Power Supply), 일명 UPS가 있다. UPS는 보호대상이 되는 장비에 기본적으로 완벽한 전압과 전류가 공급되도록 전력회사가 공급하는 상용전력(Utility Power)을 조절한다. 또한 UPS에는 배터리 등의 전력 저장 장치가 포함되어 있어, 상용전력 공급이 중단되더라도 지속적으로 장비에 전력을 공급할 수 있다. UPS는 수십 년간 생산되어 왔으며 APC의 경우 1984년부터 이를 생산해오고 있다.

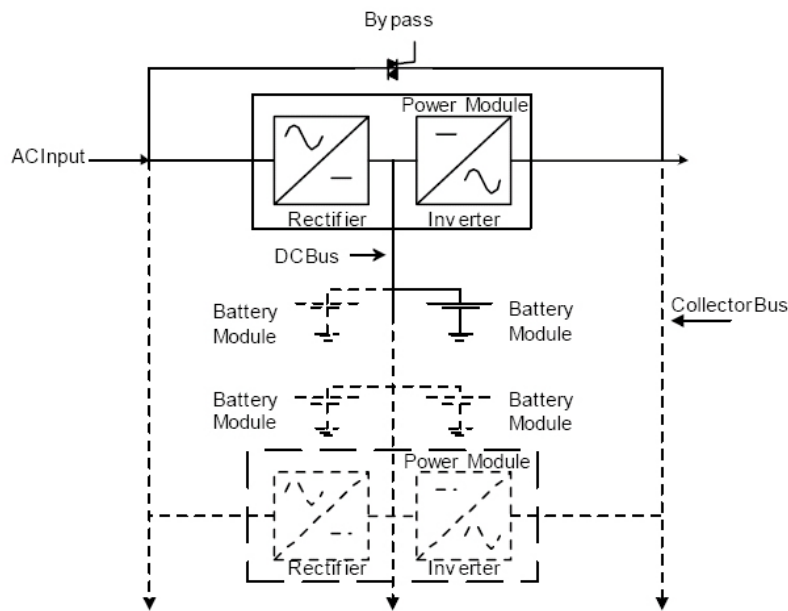
UPS에는 그동안 여러 가지 다양한 설계가 있었지만, InfraStruXure를 비롯하여 데이터센터 시장을 겨냥한 대부분의 제품들은 <그림 1>과 같은 이중 변환 아키텍처를 활용하고 있다. AC 전력은 DC로 정류되고, DC 버스는 정류기를 배터리 및 인버터로 연결한다(그림에는 보이지 않지만 일반적으로 다수의 직렬 및 병렬 스트링으로 구성되어 있음). 인버터는 스파이크(spike), 새그(sag), 고조파(harmonic) 및 짧은 정전이 없도록 AC 전압을 합성한다.

인버터 출력은 정적 바이패스 스위치의 출력과 병렬로 연결된다. 정류기 또는 인버터에 장애가 발생하거나 장비의 전기적 오류로 인해 UPS가 공급할 수 있는 전류보다 많은 전류가 필요한 경우에는 바이패스가 닫힌다.

컬렉터 버스(Collector Bus)는 이 바이패스와 하나 또는 다수의 인버터 출력을 연결한다. 일부 UPS는 높은 전력 등급 또는 이중화를 위해 다수의 인버터를 사용하기도 한다. 인버터가 여러 개 있는 시스템에는 정류기도 여럿인 경우가 일반적이다. 정류기와 인버터를 묶어 조립한 것을 전력 모듈이라 한다.

<그림 1>에서 점선으로 그려진 품목들은 선택 사항이다. 예를 들어, UPS를 설치할 때 병렬 배터리 스트링 또는 다수의 전력 모듈을 이용하는 경우도 있다.

<그림 1> 이중 변환식 UPS



이중 변환식 UPS 아키텍처는 양쪽의 변환 과정에서 손실이 발생하기 때문에 효율성이 다소 떨어지는 단점이 있다. 그러나 이러한 설계 방식은 전력 공급이 중단되더라도 액티브 스위칭(active switching) 등의 적극적인 조치가 필요 없기 때문에 널리 이용되어 왔다. DC 버스 전압이 떨어지는 즉시 배터리는 방전을 시작하고 인버터는 전원이 공급되었을 때처럼 동작하게 되는 것이다.

이러한 UPS는 대단히 효과적으로 작동했으며, 불과 몇 가지 표준 설계 방식이 현장에서 지배적인 방식으로 자리잡았다. 어떤 시장이든 새로운 제품을 소개할 때는 기존 솔루션만큼 또는 그 이상 효과적으로 작동한다는 것을 고객에게 증명하는 것이 문제가 된다. UPS 시장에서는 이 문제가 특히 심하다. 거의 모든 시스템 설치가 외부 장비나 운영 방식 면에서 독자적인 설계로 되어 있기 때문에, 서로 다른 설치 환경끼리 성능을 비교하기가 어려운 것이다. UPS 솔루션의 성공은 또 다른 장애 요소로 작용한다. 고장이 비교적 드문 편인 데다 장애가 발생할 경우 다양한 모델 사이에서 신뢰할 수 있는 데이터 소스가 드물거나 전혀 존재하지 않기 때문이다. 주요 UPS 업체들 대부분이 100년 동안 장애 발생 건수가 채 1회도 안 되는 수준의 안정성을 제공한다고 주장하지만, 사실 20~30년 이상 운영되는 데이터센터나 UPS는 거의 없다.

일단 새로운 제품을 도입한 후 장애 횟수를 관찰하여 안정성을 파악하는 것도 한 가지 방법이 될 수는 있다. 그러나 이 방식에는 여러 단점이 있다. 첫째, 고객이 실험 대상이 된다는 점이다. 둘째, 잘못 설계되거나 잘못 제작된 장치일지라도 자주 장애를 일으키지 않기 때문에 통계적으로 유의미한 차이를 증명하려면 여러 달 또는 보다 현실적으로 여러 해 동안 관찰이 필요할 수 있다. 셋째, (항공기, ABS 제동 장치, 전화 교환기 등의) 중요 시스템에서 안정성을 달성하려면 기본적으로 동일한 수많은 구성요소들을 장기간 관찰해야 한다. 현재의 UPS 시장은 특별 설계된 데이터센터가 상당수 존재할 정도로 발전했다. 각 데이터센터가 고유한 방식으로 설계되어 있으므로 그곳에서 사용되는 UPS는 고유한 운영 환경과 관리 방식에 부응해야 한다. 따라서 향후 구축될 독자적인 데이터센터에 대해 생각할 수 있는 모든 설계 규격을 충족시키는 맞춤형 또는 맞춤 구성이 가능한 솔루션을 지속적으로 제공하는 것이 UPS 업체들에게는 자연스러운 일이었다.

안정성을 저해하는 잠재적인 오류에 수천 여 고객이 노출되기 전에 새로운 제품의 안정성을 미리 파악할 수 있는 수단을 확보할 수 있다면 훨씬 효율적이고 경제적인 것이다. 나아가 여러 방안 중에 어느 것이 최소의 비용으로 최고의 안정성을 제공하는지 알 수 있다면 더욱 유익할 것이다. 제품 설계자들은 어느 구성요소와 서브시스템이 제품의 전체적 안정성에 가장 중요한지 파악하고 싶어한다. 제품의 실제 성능을 확인하고 결함 또는 결점의 수정에 필요한 변경 작업을 파악해 수행해야 하는 제품 지원 엔지니어들은 장애 가능성이 높은 구성요소를 식별해 내는 로드맵을 통해 큰 도움을 받을 수 있을 것이다. 이 로드맵의 예측을 벗어나는 상황이 발생할 경우, 더욱 강도 높은 조사와 조치가 필요한 할 새로운 영역을 파악하는 데 도움이 될 것이다.

확률론적 위험 평가, 즉 PRA는 로켓 시험이 매번 다른 이유로 끊임없이 실패하면서 낙담해 하던 초기 로켓 엔지니어들의 대응 과정에서 처음 개발되었다. 수학적 분석 결과, 로켓이나 데이터센터처럼 각 요소 간의 상관성이 매우 높은 시스템에서는, '사슬의 강도는 가장 약한 고리에 의해 결정된다'는 오랜 속담이 적용되지 않는다는 사실이 바로 드러났다. 여기서 사슬은 한 영역을 다른 영역과 이어주는 드러나지 않은 실마리와 약한 연결 고리를 다수 가진 일종의 그물망과 유사한 모양을 띤다. 그러한 그물망에서 어느 한 부분이 장애를 일으키면 다른 부분에 전과 다른 새로운 긴장이 발생하여 그 다른 부분에서도 장애가 발생할 가능성이 높아지는 것이다. 따라서 극히 사소한 문제가 일련의 장애를 촉발하여 결국 시스템 전체의

고장을 유발하는 것이다.

애초 안전과 관련된 일반의 우려를 해소하기 위해 미국 핵에너지 산업에 대규모로 도입된 것이 PRA였다. 스리마일섬(TMI; Three Mile Island) 원전 사고로 인해 수십억 달러 규모의 핵에너지 산업 전체의 존속 가능성이 의문시된 이후, 이 기법이 설계 선택 문제 뿐만 아니라 운영 및 유지 관리상의 결정 문제와 관리 방식의 효과성 평가에까지 확대 적용된 것이다. 결과는 만족스러웠다. 스리마일섬과 유사한 사건이 더 이상 발생하지 않았을 뿐만 아니라, 103개의 발전소가 생산해 내는 전력량이 스리마일섬 사건 이전보다 20% 증가된 것이다. 연료 재보급에 필요한 경우를 제외하고 단 1회의 강제 중단도 없이 18개월 또는 24개월 동안 발전소가 계속 가동되는 것이 평범한 일이 된 것이다. PRA는 또한 유지 보수 방식에 대한 정보도 제공했으며 다수의 소위 '모범 방식(best practices)'이 실제로는 구성요소 장애 및 사고의 위험성을 오히려 높인다는 사실을 보여주었다.

PRA는 신중하게 활용하면 매우 강력한 도구다. 논리적 모델 구축 프로세스를 활용하면 제품을 규정하는 기본 가정과 특징, 의사 결정 등을 광범위하게 검토할 수 있다. 또한 계산 방식이 수학적이므로, 안정성에 대한 정성적 분석에 영향을 미치기 쉬운 여러 가지 논리적 오류(예를 들어, '경험에 호소하는 오류(appeal to experience)' 등)를 제거할 수 있다. 소위 '20년간의 경험'이라는 것이 학습 경험 1년에 나머지 19년 동안은 동일한 작업을 계속 반복한 것에 지나지 않는 경우가 흔하다.

MTech의 PRA 계산은, 특히 고객이 생각했던 시스템의 안정성보다 PRA 계산 결과가 훨씬 낮게 나오는 경우에 이의를 제기 받는 경우가 흔하다. 그러나 실제로 어떠한 오류가 있는지 아니면 시스템의 기능적 작동과 관련해 어느 한 측에서 오해한 것인지는 수학적 모델의 논리를 검토하면 드러나게 된다. 의뢰 고객이 선호하는 값으로 구성요소 장애율을 변경하는 것이 최종 결과에 의미 있는 변화를 주는 경우는 거의 없다. 거의 모든 UPS가 바이패스 스위치 같은 이중화 경로를 포함하고 있기 때문이다. 이중화 설계에서는 시스템 안정성이 구성요소 장애율에 크게 영향 받지 않는다.

PRA의 가치는 정량적 분석 결과를 낼 수 있다는 점, 그리고 각 구성요소가 장애에 미치는 영향력의 상대적 비중을 파악할 수 있다는 점에 있다. 각 구성요소가 시스템의 가동 또는 장애 발생에서 차지하는 역할을 재현 가능한 방식으로 정량적으로 계산할 수 없다면 최적은 아니더라도 합리적으로 자원을 할당하는 것도 완전히 불가능해진다. 이중화로 시스템 안정성을 규정하는 기존의 방식은 이 점을 잘 보여준다. 많은 데이터센터 설계가 "N+1" 또는 "N+2", 심지어 "2N" 또는 "2N+1" 설계 등으로 규정된다. 이러한 표현의 의미는 필요한 구성요소가 N개인 시스템에 실제로는 1개 또는 2개, 심지어는 2배 또는 2배+1개의 장치를 구성한다는 것이다. 그러나 모든 이중화가 안정성에 동일한 기여를 하는 것은 아니다. 발전기의 장애 확률이 1%인 반면, 변압기의 장애 확률은 매우 낮아 변압기 이중화를 위해 쓸 비용을 다른 용도로 쓰는 것이 거의 언제나 더 효율적이라면, 발전기의 이중화가 안정성에 미치는 영향이 훨씬 클 것이다. 이중화 여부에 관계 없이, 각 구성요소가 안정성에 미치는 영향의 크기를 정량화할 수 없다면 설계자와 구매자는 자금 등 여러 가지 한정된 자원의 최적 활용을 위한 합리적인 결정을 내릴 수 없다. PRA는 이러한 문제에 대한 매우 강력한 해결책이다.

이중화 설계에는 근본적인 문제점들이 있다. 원칙적으로 이중화는 개별 구성요소 또는 부품이 고장을 일으키더라도 시스템 전체의 장애를 야기하지 않게 함으로써 안정성을 높이지만 상당한 비용이 필요하며 잠재적으로 심각한 단점이 있다. 이중화 시스템에는 구성요소 수가 많은데 일반적으로 구성요소 수가 많은 시스템은 장애를 경험할 가능성도 많다. (엔진이 두 개인 쌍발 비행기는 엔진이 하나인 단발 비행기보다 가동 시간당 엔진 장애 횟수가 대략 두 배다.) 장애를

일으킨 구성요소를 파악하여 시스템으로부터 격리할 수 있는 매우 안정성 있는 메커니즘이 반드시 갖춰져 있어야 한다. 그렇지 않으면 구성요소 장애 수가 증가하면서 이중화의 이점은 사라지게 될 것이다.

일부 장애 상황은 여러 구성요소에 동시에 영향을 미칠 수 있으며, 이와 같은 장애로 인해 이중화의 이점이 크게 저하된다. 예를 들어, 설계 결함, 제조 결함을 비롯하여 설치, 유지 관리 또는 수리 작업 중에 발생한 결함 등은 모두 독립적인 것으로 생각했던 여러 장치에 동시에 장애를 일으킬 수 있으며, 이로 인해 전체 시스템 장애가 발생하는 경우가 많아지는 것이다. 또한 일부 구성요소에서 발생한 최악의 장애가 그와 연결되어 있거나 가까이 배치된 장비를 손상시켜 시스템 전체의 장애를 야기할 수 있는 것이다. 이들 모두 이중화 설계를 무색하게 만드는 상황들이다.

MTech에서는 핵 발전 산업에서 이용되는 PRA 기법과 소프트웨어를 적절히 수정하여 InfraStruXure 제품 라인을 분석하고 그 성능을 기존 시스템과 비교했다. 그 결과 도출된 수학적 모델은 몇 가지 주요 의문 사항에 해답을 제공하는 데 사용되었다. InfraStruXure는 높은 안정성을 달성하기 위해 거의 모든 구성요소에 이중화 기법을 활용했다. MTech의 분석은 이중화에는 비용과 효과가 모두 존재하며, 일부 서브시스템은 다른 서브시스템에 비해 이중화의 효과가 적다는 점을 보여주고 있다.

안정성과 가용성

이 연구는 주로 제품의 안정성 문제를 다뤘다. 많은 업체들은 가용성에 관해 논의하는 것을 선호한다. 그 차이는 미세하지만 매우 중요한 의미를 갖는다. 안정성이란, 주어진 시간 동안 시스템이 의도대로 작동할 확률을 말한다. 따라서 미션(mission)이라고도 불리는 ‘그 주어진 시간’이 반드시 명시되어야 한다. 747 항공기는 이륙한 이후 안정성이 극히 높은 수준이다. 14시간 이내의 비행인 경우에는 장비 또는 승객에 피해를 주지 않고 안전하게 착륙할 확률은 99.99%보다 훨씬 높다. 그러나 비행 시간이 36시간에 이르면 747기의 안정성은 영(0)으로 떨어진다. 미션이 완료되기 전에 연료가 고갈될 것이기 때문이다.

가용성이란 시스템이 작동하는 짧은 시간(fraction of time)을 말한다. 그렇지만 가용성은 미션 시간과 관련될 수 있으며, 장기 가용성(즉 가용성의 점근선)으로 표현될 수도 있다. 가용성은 장애 후 시스템 수리에 필요한 시간에 관한 정보를 필요로 한다. 장애율이 동일하다면, 신속히 수리되는 시스템은 수리 작업이 오래 걸리는 시스템에 비해 가동 상태 유지 시간이 더 길며 따라서 가용성이 높다.

가용성과 안정성 모두 각기 계산하고 파악해야 할 타당한 이유가 있다. 그러나 Mtech은 안정성, 좀더 명확히 말하자면 불안정성(unreliability), 즉 미션 진행 도중 장애를 일으킬 확률을 데이터센터 담당자와 운영자에게 더 중요한 측정 기준으로 보고 있다. 안정성은 매우 높지만 수리하는 데 많은 시간이 걸리는 시스템은 장애는 자주 발생하지만 신속히 서비스에 복귀할 수 있는 시스템과 가용성이 같거나 오히려 더 낮을 수도 있다. 그러나 데이터센터 전원 장애의 경우 전원이 아무리 빨리 복구되더라도 경제적 손실 및 기타 손실이 매우 크다. 따라서 대부분의 기업들은 합리적인 선택에 필요한 충분한 정보가 확보된다면 안정성이 높은 시스템을 더 선호할 것이다.

장애 확률(불안정성)을 측정 기준으로 이용하는 가장 중요한 이유는 최종 사용자인 고객이 그것을 가장 유용한 측정 기준이라 보기 때문이다. 확률론적 위험 평가에서 사용되는 수학적 기법에 풍부한 경험을 가진 기업은 사실 거의 없지만, 기업의 경영진과 관리자들은 위험 수준이 서로 다른 여러 가지 방안들을 다루고 처리하는 일을 일상적으로 수행하고 있다. 위험은 확률과 결과의 함수이다. 많은 기업들은 위험에 대한 자신들의 평가, 즉 손실을 입을 확률에 그 손실로부터 예상되는 손해의 크기를 곱한 값에 근거하여 보험 또는 재해복구 프로그램과 같은 상품을 구입한다. 대부분의 기업들은 단 한 차례의 정전으로도 상당한 손실을 입게 된다. 그런데 기업이 추가 투자 또는 기타 위험 완화 방안과 관련하여 합리적인 결정을 내릴 수 있기 위해서는 그러한 사태가 발생할 가능성을 알고 있어야 한다.

장애 확률이라는 기준을 사용하는 두 번째 이유는 그 측정 기준이 해당 기업 전체에 걸쳐 일정하기 때문이다. APC는 일반적인 기업 내 다양한 시스템의 상호 작용을 보여주는 4단계 계층 구조를 개발했다. 최상위 계층은 사람, 그 다음 계층은 프로세스, 세 번째 계층은 정보기술(IT), 마지막 최하위 계층은 전력을 포함한 인프라에 해당한다. 장애가 발생하면 각 계층의 가용성에는 크게 다른 결과를 야기될 것이다.

어느 기업의 UPS 시스템이 가동 10년 만에 한 차례 중단을 경험했다고 가정해보자.

- 인프라 계층은 10분만에 전력을 복구한다. 이 경우 가용성을 다음과 같이 계산할 수 있다.
 $A = 87599.8 / 87600 = 99.9998\%$. 이 인프라 계층은 “9 다섯 자리(five nines)” 수준의 가용성을 갖는다고 할 수 있다.
- 정보기술(IT)에서 애플리케이션을 12시간 만에 복구한다면 그 가용성은 다음과 같다.
 $A = 87588 / 87600 = 99.99\%$, 즉 가용성 수준은 “9 네 자리(four nines)”라 할 수 있다.
- 프로세스 또는 애플리케이션 관리자가 데이터베이스 손상을 수리하고 정상적인 업무 흐름을 복구하는 데 2일이 걸렸다면 가용성은 다음과 같다.
 $A = 87552 / 87600 = 99.95\%$, 즉 “9 세 자리(three nines)” 수준의 가용성을 주장할 수 있다.

고객을 달래고 SEC 보고서를 제출하고 중단 사태와 관련된 부하 직원을 해고하고 신규 대체 인력을 고용해서 교육하느라 두 달을 소비하는 중역들은 자신들의 가용성을 계산하지는 않겠지만 만일 그렇게 한다면 그 계산은 $A = 86160 / 87600 = 98.4\%$ 가 되며, 자신의 가용성 수준이 ‘9 두 자리(two nines)’에 불과하다는 데 불쾌감을 느낄 것이다.

위에서 사용된 수치는 어느 시설 내부의 다양한 지점에서 일반적으로 소요되는 복구 시간이며, 이를 통해 가용성 수준이 관찰 지점에 따라 달라진다는 것을 알 수 있다. 그러나 그 회사 전체의 장애 확률은 10년에 1회이며, 이는 관찰 지점과 관계없이 동일하다. 그리고 시스템의 안정성이 비교적 높다면 장애가 다수 발생할 확률은 낮을 것이므로 첫 번째 장애 확률만 고려하면 된다.

연구 수행

본 연구는 먼저 InfraStruXure 제품 라인을 이해하고, 매사추세츠주 빌레리카와 로드아일랜드주 이스트프로비던스에 위치한 APC 지사의 UPS와 PDU를 세밀하게 파악하는 작업부터 시작했다. APC는 엔지니어링 문서를 제공했으며 MTech가 현장 작업 내역을 검토할 수 있도록 현장 서비스 직원과 면담할 수 있도록 했다.

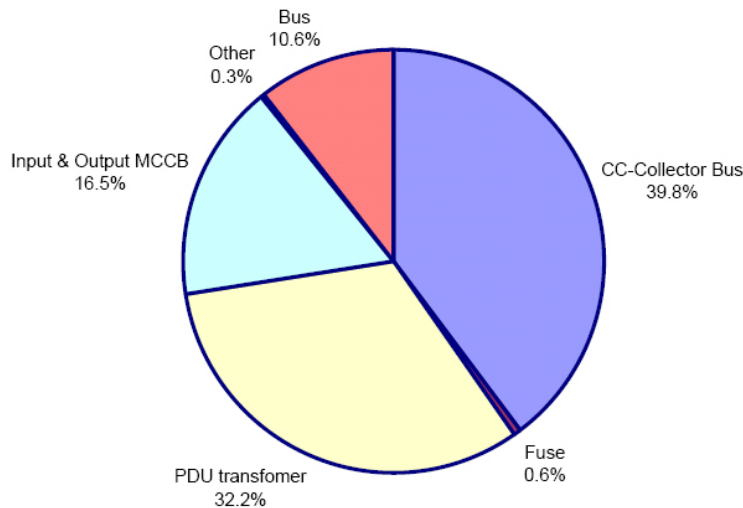
Mtech은 조사 대상 시스템의 오류 트리 모델을 작성했다. 오류 트리 모델링 기법에 대해서는 문서 자료가 많이 나와 있으므로 이 글에서는 자세히 다루지 않는다. 첫번째 모델에서는 APC 제품을 다른 요인과 분리된 상태에서 고찰했다. 상용 전력(utility power) 입력은 완벽한 것으로 가정했으며 고객의 장비 역시 완벽한 것으로 가정했다. 이 모델에서는 UPS 및 PDU 내부적인 장애가 핵심 장비의 손실을 야기하는 빈도가 얼마나 되는지 알아보았다.

모든 UPS는 새로운 구성요소의 추가를 의미하고 따라서 핵심 장비를 담당하는 회선에 최소한 하나의 새로운 장애 모드의 추가를 의미한다는 사실을 인정하는 UPS 공급업체나 구매자는 거의 없다. 모든 조치는 안정성에 긍정적 영향과 부정적 영향을 함께 미친다. 따라서 목표는 긍정적 영향을 극대화하고 부정적 영향은 최소화하는 것이다. 첫번째 오류 트리 모델은 시스템 안정성에 큰 영향을 미치는 구성요소와 부품을 파악하는 데 유의했다. Mtech은 이 구성요소에 대해 더욱 집중적인 조사를 시작했다.

이 글을 작성한 우리 필자들은 덴마크 콜딩에 위치한 APC의 설계 시설을 방문, 제품 설계자들과 집중적인 인터뷰와 토론을 일주일 동안 실시했다. 우리(이 글을 쓴 필자들을 말함=편집자주)는 제품 개발 프로세스, 설계 규칙, 검증 및 인증 테스트, 검토 및 QA 작업, 현장 서비스 기록 등을 살펴보았다. 또한 InfraStruXure 제품과 이전 제품, 그리고 유사 제품에 대한 광범위한 조사를 실시했다. 우리는 첫번째 오류 트리 분석 결과를 APC에 제출하여 검토하도록 한 후 의견을 청취하여, 우리가 잘못 이해한 부분을 수정하고 장애(특히 공통의 원인에 의한 장애) 원인에 관해 더 자세한 정보를 추가했다.

일부 구성요소는 하나 이상의 장애 모드를 갖는다. 컬렉터 버스, 배터리, 제어장치, 전원 모듈 등은 일반 장애와 치명적 장애의 두 가지 장애 모드로 모델링되었다. 이들 구성요소에서 발생한 치명적 장애는 UPS의 장애를 야기하는 반면, 일반 장애는 이중화로 인해 UPS 장애를 일으키지 않는다. 치명적 장애의 한 형태로는 구성요소가 장애를 일으켰음에도 장애로 확인되지 않는 경우가 있다. 이 경우 장애가 발생한 구성요소는 다른 구성요소의 오작동을 유발하거나, 아니면 계속 악화되어 더 심각한 장애를 일으킬 수도 있다. 한편, 물리적으로 UPS 내부에 플라즈마가 유입되어 여러 전원 회로 및 제어 회로를 단락시켜 로드 드롭(load drop)을 야기하는 치명적 장애들도 있다. 어떤 구성요소에서 치명적 장애가 차지하는 비율은 매우 중요한 매개변수다. 우리는 충분한 정보에 근거하여 모든 구성요소에서 발생하는 장애 가운데 약 1%가 치명적 장애라는 판단을 내리고 연구를 시작했다. 첫번째 모델링 작업과 APC 엔지니어들과의 모델 검토 작업을 완료한 후, 우리는 실제 현장 데이터를 반영하여 이 치명적 장애 비율을 조정했다. 그 결과, 일반 장애에 대한 치명적 장애의 비율이 1%라는 것은 상당히 정확한 수준이었다. <그림 2>는 이 단계의 연구 결과를 요약한 것이다.

<그림 2> 구성요소의 장애 비중: InfraStruXure에 한정, 상용전력 장애는 제외



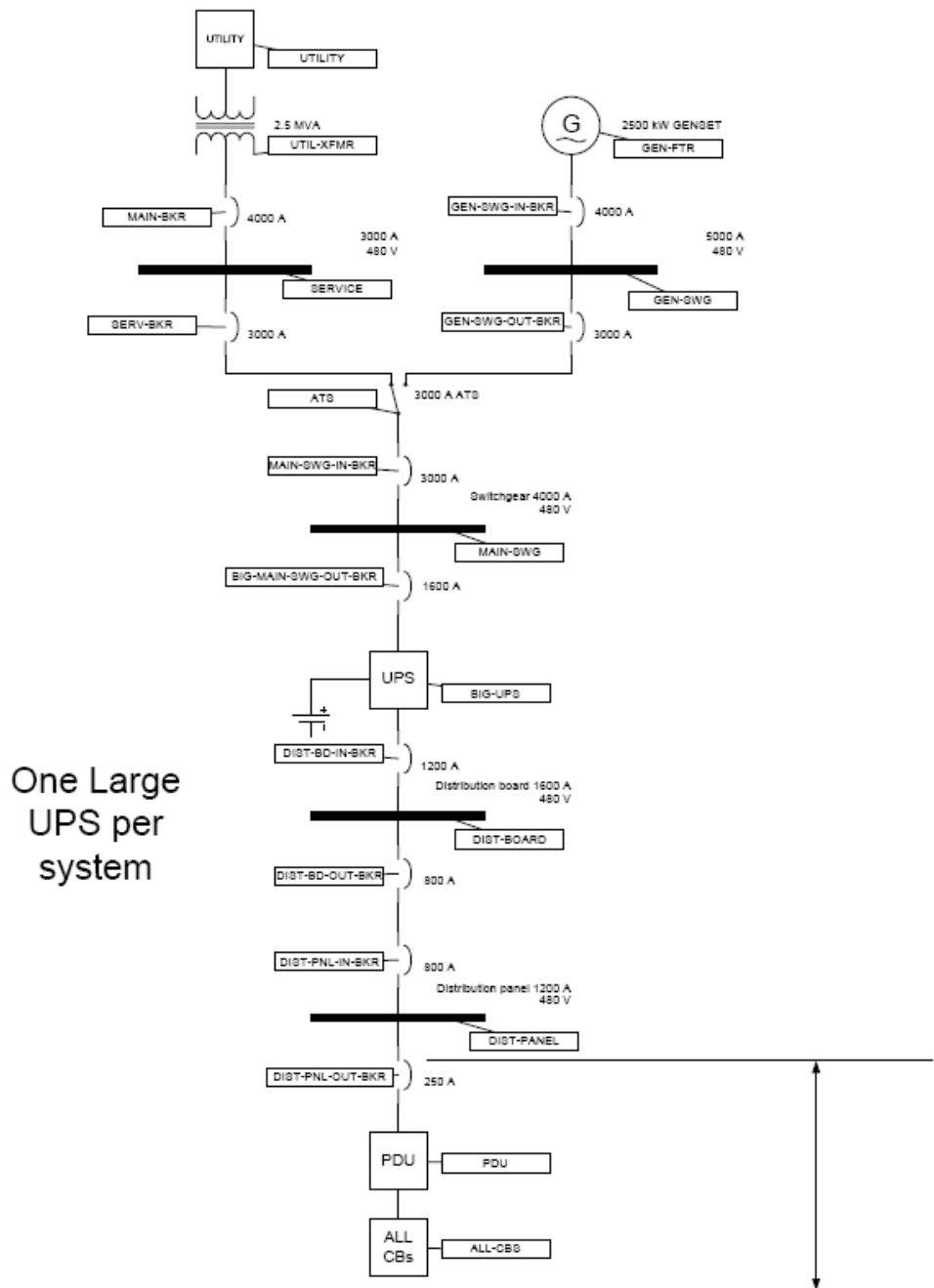
컬렉터 버스(전원 모듈과 바이패스 스위치 사이의 병렬 연결 지점)의 치명적 장애와 PDU 변압기의 장애는 예상되는 모든 장애의 72%를 차지했다. 830만 시간의 MTTF(Mean Time To Failure)에 해당하는 시간당 1.2×10^{-7} 의 구성요소 장애율에도 불구하고, 입출력 몰드 케이스 회로 차단기(MCCB; Molded Case Circuit Breaker)는 거의 17%를 차지했다.

우리는 APC 엔지니어들과 함께 처음의 모델과 예비 작업 결과를 검토한 후, 그에 따라 오류 트리 모델을 수정했으며, 제품의 실제 작동 환경을 설명할 수 있도록 이를 확장했다. 우리는 상용전력 장애, 발전기 기동 장애, 그리고 상용전력과 자체 발전기를 선택하는 전환 스위치(transfer switch) 장애 등을 포함시켰다. 또한 고객 장비에서 발생한 전기적 오류의 영향도 조사했다.

이러한 '현실적인' 제품 분석은 몇 가지 새로운 의문을 낳았다. 분기 회로 차단기 하나의 장애를 제품 전체의 장애로 계산해야 하는가? 몰드 케이스 회로 차단기(MCCB)는 오작동 발생(spurious trips)의 MTTF가 800만 시간이 넘어 안정성이 매우 높지만, 신중한 데이터센터에서조차 회로 차단기 장애가 예상 장애의 큰 부분을 차지하는 경우가 허다하다.

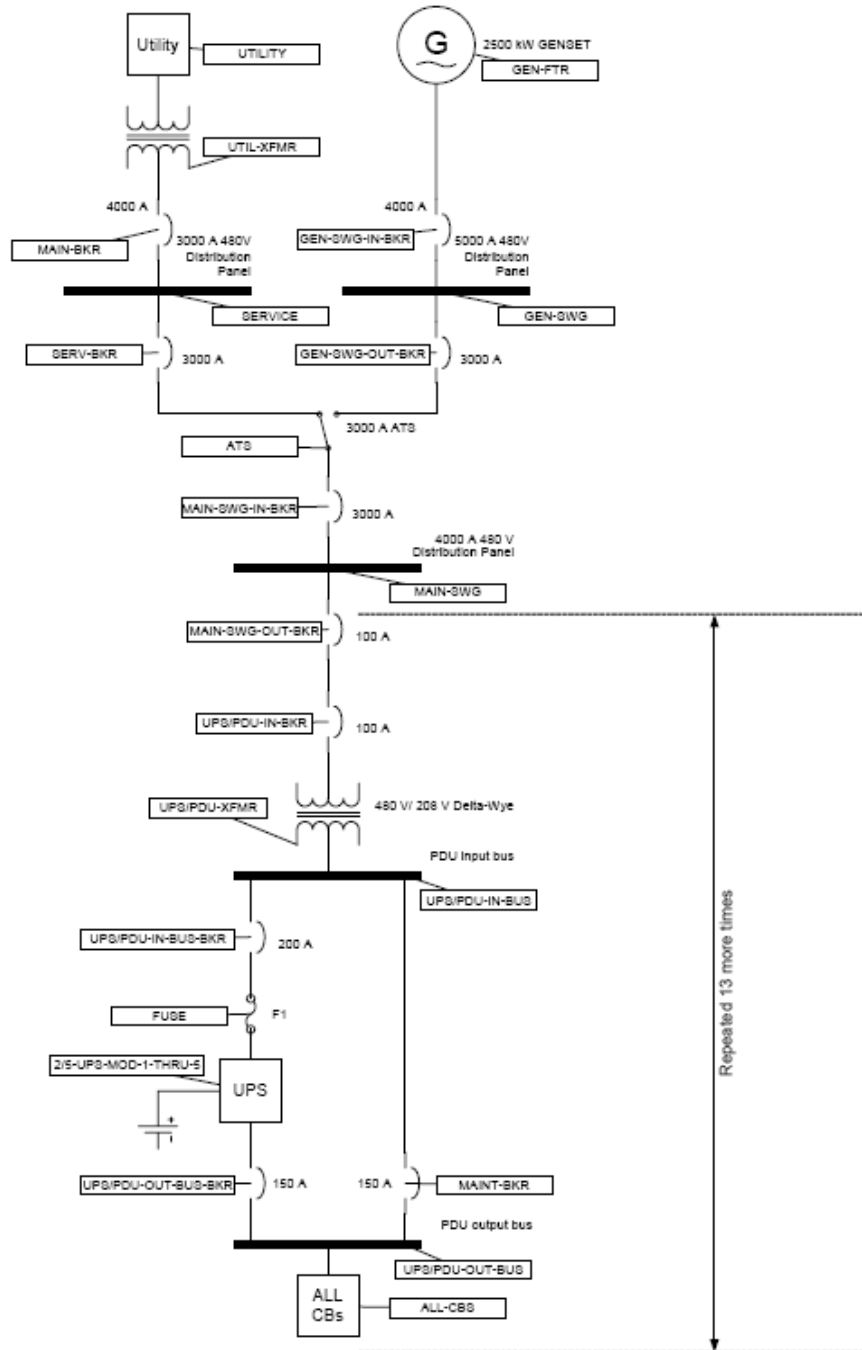
우리는 실제 데이터센터를 대상으로 한 이전의 연구 결과를 활용하여 '전형적인' 데이터센터 배전 시스템의 오류 트리 모델을 구성했다. '전형적'이라는 용어는 데이터센터 설계에 적용하기에 그리 좋은 용어는 아니다. 데이터센터 설계에는 표준화가 거의 이루어져 있지 않으므로 우리가 선택한 사례를 평균 또는 평균 이상이나 이하라고 확인할 수는 없다. 우리는 단지 우리의 모델이 최근 만들어진 실제 데이터센터를 기반으로 하고 있다고 말할 수 있을 뿐이다. <그림 3>은 하나의 중앙식 500kW UPS를 사용한 '전형적인' 데이터센터의 다이어그램이고, <그림 4>는 14개의 APC InfraStruXure UPS로 구성된 데이터센터의 다이어그램이다. 두 경우 모두 소스 시스템과 배전 시스템은 동일하다.

<그림 3> 500kW 데이터센터의 대형 UPS



<그림 4> 500kW 데이터센터의 APC InfraStruXure UPS

APC
InfraStruXure
40 kW
480 Volt



우리는 양쪽 공급업체(즉, 대형 UPS 공급업체와 APC)의 간행물과 제3의 기관이 발행한 전력 시스템 구성요소 장애율 관련 문서로부터 대형 UPS의 장애에 관한 데이터를 수집했다. 우리는 성공과 실패를 가름하는 기준에 있어 공정성을 기하기 위해 공통된 가정을 이용했다. 하나 이상의 전원 모듈이 장애를 일으키더라도 바이패스로의 전송이 제대로 이루어지면 성공으로 간주된다. 배터리 소진으로 인한 장애는 규격보다 훨씬 더 빠르게 소진되거나 상용전력 공급 중단 시 함께 장애를 일으키는 경우가 아니면 장애로 간주되지 않는다. 분기별로 배터리 테스트가 시행되는 것으로 가정했고, 이러한 테스트를 통해 장애를 일으킨 전지셀 또는 접속을 거의 100% 식별할 수 있다는 낙관적 가정을 전제로 했다. 운영자의 실수로 인해 핵심 장비에 대한 전력 공급이 중단되는 경우도 장애로 보지 않았다. 다만 또 다른 별도의 분석에서는, 운영자의 실수 중 최소한 몇 가지는 인체공학적 배려가 잘못되어 있거나 기기의 지시 내용에 오해의 소지가 있어 발생했을 수 있다는 결론이 도출됐다.

우리는 표준적인 통계 기법을 이용해서 개별적인 장애율을 하나의 추정 장애율로 통합하여 비교 대상인 '중앙식 UPS'에 적용했다. 그 결과, 때때로 임계 버스로 식별되는 컬렉터 버스의 대형 UPS의 장애율은 거의 정확히 시간당 1×10^{-6} 으로 나타났다. 이것은 장애율을 불변으로 가정할 경우 100만 시간의 MTTF에 해당된다. 우리의 연구에는 Liebert에서 자사의 600 시리즈 UPS 제품에 대해 수행한 분석 데이터가 포함되어 있으며 우리의 연구 결과 역시 Liebert의 결과와 상당히 일치한다. [<http://www.liebert.com/support/whitepapers/documents/techmtbf.asp>, 2004년 2월 19일 확인]

대형 UPS에서는 장애 보고가 거의 없는 편이다. Liebert 보고서는 2억 시간 동안 80건의 장애가 있었다고 밝히고 있으며, 타사에서 서비스하는 장치에서는 장애가 보고되지 않았을 수도 있음을 정확히 지적하고 있다. 보고된 장애 수가 적기 때문에, 단지 몇 건만 누락되어도 결과가 크게 왜곡될 수 있다. 우리는 MTBF 보고 기준을 '100만 시간 초과'로 한정된 Liebert의 신중한 방법론에 동의한다. 아래 결과에 나타난 바와 같이, UPS 장애율 개선은 최종 로드 드롭(load drop) 확률의 민감도에 큰 영향을 미치지 않을 것이다.

한편, 우리는 APC 제품에서와 같은 자세한 수준으로 대형 UPS를 분석 또는 모델링하지 않았다는 사실을 분명히 밝혀 두고자 한다. 우리는 양자 간의 비교를 위해 전체 UPS 장애율을 구하고자 했을 뿐이다. 우리는 여타 업체들이 발표한 모듈 장애율을, 우리가 APC 전원 모듈에서 파악한 장애율과 대략 비교할 수 있다는 사실을 확인했다. 또한 제어 시스템 장애 및 재해로 인한 구성요소 장애 등 일반적 원인에 의한 장애가 UPS 장애를 초래하는 가장 흔한 원인이라는 사실을 확인했다. 이것은 APC 현장 데이터에 대한 우리의 상세한 분석과 재해 장애 모드에 대한 우리의 모델링에 부합되는 결과였다.

우리는 두 개의 데이터센터를 가정하고 그에 대한 오류 트리를 구성했다. 한 데이터센터는 500kW UPS 1개를 사용하고 다른 데이터센터는 14개의 APC InfraStruXure 제품을 사용하는 것으로 가정했다. 냉각 시스템은 모델링하지 않았으며, UPS 출력의 부분적 로딩(partial loading) 효과도 고려하지 않았다.

InfraStruXure 아키텍처의 결과는 <그림 5>에, 중앙집중식 UPS 아키텍처의 결과는 <그림 6>에 요약되어 있다. InfraStruXure 시스템의 장애율(단, 데이터센터의 모든 핵심 장비가 전력을 공급 받지 못하는 경우를 장애로 정의)은 중앙식 UPS 시스템의 장애율보다 대략 40% 정도 낮았다.

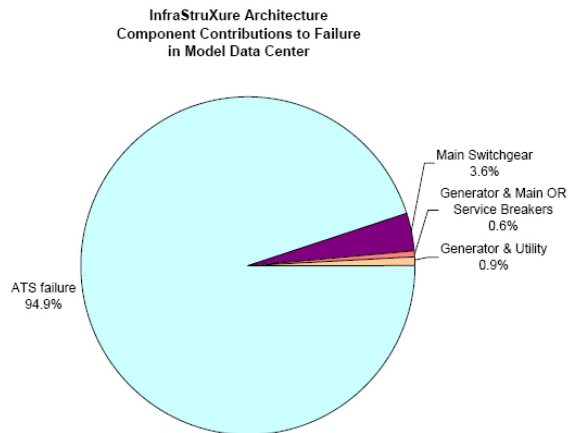
중앙집중식 UPS 시스템에서는 배터리 장애가 큰 영향을 미치지만 InfraStruXure에는 무시할 만한 수준이다. 우리는 양쪽 시스템에 동일한 배터리 장애율을 적용했다. 그런데도 위와 같은 차이가 발생한 이유는 중앙집중식 UPS가 하나의 스트링으로 구성된 VRLA 배터리를 갖춘

것으로 모델링했기 때문이다. 반면 **InfraStruXure**는 8개 직병렬 스트링을 사용하므로 여러 스트링이 장애를 일으키더라도 정상적으로 작동할 수 있다. **InfraStruXure**의 스트링은 196 VDC인 반면, 일반적인 중앙집중식 **UPS** 스트링은 정격 400 VDC 이상이다. 다수의 셀이 직렬로 배치된 높은 전압의 스트링은 전압이 낮은 스트링보다 안정성이 다소 떨어진다. 중앙집중식 **UPS** 아키텍처에서 배터리가 둘 이상의 병렬 스트링으로 구성된다면 배터리 장애가 핵심 장비의 장애로까지 이어지는 경우는 크게 줄어들 것이다. 배터리 장애율을 계산에서 제외하더라도 **InfraStruXure** 시스템의 장애율(단, 데이터센터의 모든 핵심 장비가 전력을 공급 받지 못하는 경우를 장애로 정의)은 중앙집중식 **UPS** 아키텍처의 장애율보다 대략 18% 정도 낮다. 이 차이는 구성요소 장애율의 차이가 아니라 각 시스템의 아키텍처에 기인한다.

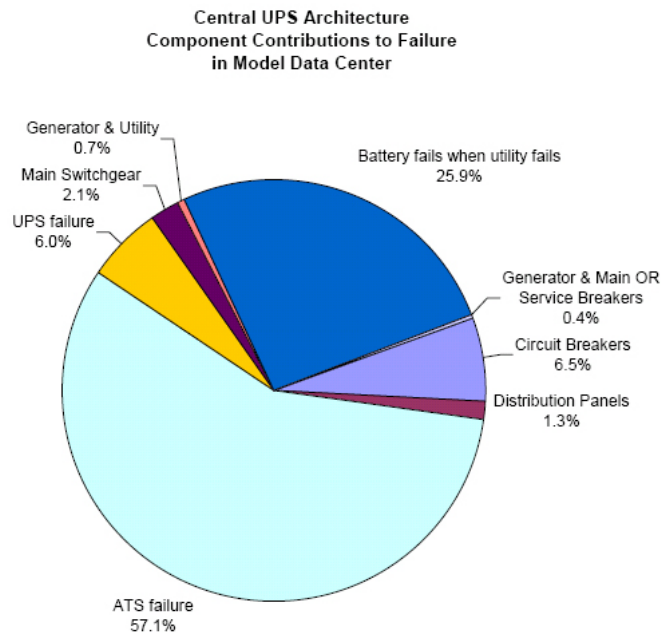
InfraStruXure와 중앙집중식 **UPS** 설계는 모두 그림(<그림 3> 및 <그림 4>)에서 보는 바와 같이 상용전원장치 및 발전기에서 전환 스위치에 이르는 장비에 있어 공통적인 취약성을 갖는다. 그러나 **InfraStruXure** 방식에서 모든 장비에 대한 전원 공급이 중단되는 경우는, 예를 들어 주 전력 유입 버스(main entrance bus) 장애를 일으키거나 전환 스위치가 개방되지 않는 경우처럼 공통의 전력 인프라에서 장애가 발생하는 경우뿐이다. 따라서 내부 장애로 인해 14개의 **InfraStruXure** 유닛이 모두 동시에 장애를 일으킬 확률은 극히 적다. 반면 중앙집중식 **UPS**와 바이패스는 일단 장애가 발생하면 모든 장비가 중단된다. 이것은 **InfraStruXure** 아키텍처에는 존재하지 않는 또 다른 장애 원인이기도 하다. 한편 장애의 정의가 변경되어 PDU 하나의 손실도 장애로 본다면 두 가지 방식의 안정성 차이가 감소될 것이라는 점에 유의해야 한다. **InfraStruXure**의 입력 또는 출력 회로 차단기 장애는 중앙집중식 **UPS** 시스템의 PDU 입력 회로 차단기 장애가 부분적 로드 장애를 야기하는 것처럼 부분적 로드 장애를 야기할 것이다.

아키텍처상의 두번째 차이점은 **UPS** 전력의 공급을 방해하여 **UPS** 전력이 모든 로드에도달하지 못하게 할 수 있는 회로 차단기 수가 적다는 점이다. 중앙집중식 **UPS**에는 전환 스위치 뒤에 5개의 회로 차단기가 있는데 그 중 2개는 **UPS** 입력에 3개는 출력에 있다. 출력 회로 차단기의 장애는 핵심 장비의 즉각적 장애로 이어질 수 있다. 입력 회로 차단기의 장애는 **UPS** 배터리가 소진된 이후 장비의 장애를 야기할 수 있다. 배터리 탱크에서 일반적으로 가능한 것처럼 10~45분간 정격 전류 미만으로 **UPS**를 자체 가동하는 동안, 전력 공급에 지장을 주는 회로 차단기를 수리하는 것도 이론적으로는 가능하지만 다른 장애를 야기하지 않고 그와 같이 할 수 있는 확률은 매우 낮다. **InfraStruXure** 아키텍처의 경우, 전환 스위치 뒤에 모든 핵심 장비의 장애를 유발할 수 있는 회로 차단기가 하나뿐이다.

<그림 5> 구성요소의 장애 비중: **InfraStruXure** 아키텍처



<그림 6> 구성요소의 장애 비중: 중앙집중식 UPS 아키텍처



우리는 운영자의 실수가 UPS 장애에 미치는 영향을 검토했으며 이 경우 APC 제품과 여타 대형 UPS 사이에 유의미한 차이가 없다는 결론을 내렸다. 이 가정상의 데이터센터에서 운영자들은 대형 UPS보다 InfraStruXure UPS에 대해서는 어떠한 조작이든 14배 더 많이 수행하게 될 것이다. 일반적인 성능 형성 요소 분석에서는 이를 어떠한 조작 상황에서든 실수 확률이 크게 감소하는 것으로 기록할 것이다. 실수가 야기하는 피해(즉시 명백히 드러나는 피해) 역시 APC 방식에서는 감소할 것이다.

우리는 이 결과가 배전 시스템 장애율에 상당히 민감하다는 사실을 발견했다. 배전 시스템에는 UPS의 출력과 핵심 장비 사이의 배선 및 보호 장치가 포함된다. 이 문제는 APC 방식과 중앙집중식 UPS 방식 모두에 공통적이다. 이 때문에 우리는 APC의 배전 시스템 생산 기법을 자세히 조사하게 되었다. 우리는 APC가 사전 배선식(factory-wired) 배전 시스템 생산 과정에서 사용하는 공정 제어 및 품질 보증 방식을 검토하고 이것을 중앙집중식 UPS가 있는 데이터센터의 현장 배선에 사용되는 일반적인 방식과 비교했다. 우리의 분석에서는 사전 배선식 배전 시스템의 경우 배선 결함이 크게 감소하는 것으로 나타났지만 이 글에서는 그 효과에 관해 설명하지 않았다. 이 글의 의도는 특정 제품의 경쟁력을 분석하는 것이 아니라 아키텍처 간의 차이를 일대일 비교하는 것이기 때문이다.

결과 및 논의의 확장

Mtech은 InfraStruXure 아키텍처를 채택한 데이터센터가 단일 배터리 스트링과 함께 단일 모듈 UPS를 채택한 데이터센터에 비해 안정성이 훨씬 더 높다는 사실을 발견했다. InfraStruXure 내부의 이중화된 하부시스템들이 UPS 고장 확률은 성공적으로 줄이는 반면, 각 접근 방법들에 공통적인 외부 시스템의 영향은 유의미한 차이를 보이지 않는 것으로 나타났다. PRA는

중앙집중식 UPS에서 이중화된 배터리 스트링을 병렬로 활용할 경우 이와 같은 안정성의 차이를 줄일 수는 있지만 완전히 없애지는 못한다는 사실을 보여주었다. 대부분의 UPS가 배터리 전력만으로는 단 몇 분밖에 중요 장비를 지원하지 못한다. 장시간 보호를 위해서는 비상 발전기 또는 기타 전원이 필요하며 비상 전원과 상용전력 선택을 위한 자동전환스위치(ATS)가 필요하다. MTech의 분석에 따르면 ATS의 성능은 안정성 향상을 제한하는 요소의 하나인 경우가 많은 것으로 나타났다.

수치 결과를 보면 InfraStruXure 아키텍처를 이용한 모델 데이터센터가 중앙집중식 UPS를 이용하는 데이터센터보다 모든 중요 장비의 장애 확률이 대략 40% 정도 낮다는 것을 알 수 있다. 중앙집중식 UPS를 위해 이중화된 배터리 스트링을 추가할 경우 안정성이 크게 향상되지만 작동 1년간 장애를 일으킬 확률은 여전히 InfraStruXure 아키텍처쪽이 18% 더 낮다. 장애의 정의가 바뀔 경우 이러한 결과도 바뀌게 될 것이다. 장애(failure)에 대한 정의를 UPS 고장이 아니라 분기 회로 고장으로 인해 단 하나의 로드 손실마저도 포함하는 것으로 정의한다면 InfraStruXure의 장애 확률은 중앙집중식 UPS에 비해 6% 더 낮다. 18%에서 6%로 감소한 것은 오로지 두 접근 방법 모두의 안정성을 떨어뜨리는 몰드 케이스 회로 차단기의 오작동으로 인한 것이다. 입력 데이터의 불확실성과 현장 설치의 품질 차이 그리고 경쟁 제품들 사이의 편차 등은 이와 같은 약간의 이점을 상쇄해버릴 만큼 폭이 크다.

공정성을 기하기 위하여 InfraStruXure를 기존의 UPS와 비교한 모형들은 모든 구성요소에 대해 동일한 고장율을 적용했다. 경쟁 우위를 확보하기 위해 APC는 MTech의 분석으로 파악된 주요 구성요소의 안정성을 향상시키기 위한 프로그램에 착수했다. APC는 몇 가지 일반적인 고장 유형을 제거하기 위해 PDU 변압기의 설계를 변경했다. 컬렉터 버스를 강화하고 모듈과의 연결성을 개선했다. APC는 이미 InfraStruXure 시스템에 설치하기 전에 모든 회로 차단기를 100% 시험했고, 전체는 아니지만 일부 데이터센터의 경우에는 설치 전에 분기 회로 차단기를 시험했다. 그러나 Mtech은 이번 비교 분석에서 양쪽 시스템에 동일한 회로 차단기 고장율을 사용했다. 회로 차단기 고장 형태에 대한 MTech의 분석을 바탕으로, APC는 회로 차단기 고장 원인을 조사 중이며 가장 고장에 취약한 장비를 식별해내기 위한 새로운 시험을 구상 중이다.

MTech의 분석은 구성요소 수의 차이나 구성요소 안정성의 차이가 아니라 아키텍처의 차이가 InfraStruXure를 중앙집중식 UPS와 차별화시킨다는 것을 분명히 보여준다. 고객들은 UPS 제품이 데이터센터의 물리적 환경에서 사용될 때 그 안정성을 체험하게 된다. 이러한 환경에서 InfraStruXure의 안정성은 중앙 UPS 아키텍처의 안정성보다 우수하지만 고장에 대한 정의를 전체 데이터센터의 손실에서 단일 분기 회로의 손실로 바꿀 경우 그 차이는 통계적인 유의성을 잃게 된다. 결과를 보면 두 가지 아키텍처에서 구성요소 선택이나 사용의 변화가 상당한 안정성 향상을 가져오는 부분이 어디인지 알 수 있다. 참고로, 이 글은 UPS 제품의 개발 및 제조 활동에 지침을 제공하기 위해 공식적, 정량적 PRA 기법을 사용한 최초의 공개 발표 자료다.

APC는 문헌 자료를 통해 InfraStruXure 아키텍처가 제공하는 비용 및 유연성 측면의 이점이 매우 크기 때문에 충분한 정보를 입수한 고객이라면 비록 경쟁 제품에 비해 안정성이 크게 더 나을 게 없다 하더라도 이 제품을 선택할 것이라고 밝히고 있다. 총소유비용 및 관련 문제에 대한 분석은 APC 백서에서 확인할 수 있으며 본 문서에서는 더 이상 논의하지 않을 것이다. 좀 더 자세한 정보는 APC 백서 #37, “데이터센터 및 네트워크룸 인프라 초과설계로 인한 초과 비용 해결 방안(Avoiding Costs From Oversizing Data Center and Network Room Infrastructure)”(APC eNewsletter vol.2 참조) 및 APC 백서 #6 “데이터센터 및 네트워크룸 인프라의 총소유비용 결정(Determining Total Cost of Ownership for Data Center and Network Room

Infrastructure)”(APC eNewsletter vol.14 참조)을 참조하기 바란다.

Mtech은 InfraStruXure에 사용된 제조 기법을 분석하고 기존 제품에 사용된 기법들과 비교했다. InfraStruXure와 중앙집중식 UPS 시스템 사이의 가장 중요한 차이는 모든 InfraStruXure 제품에 사용되는 배전 시스템이 공장 배선(factory wiring) 방식으로 제작된다는 점이다. UPS는 상용전력 공급이 중단될 때 전력이 중요 장비로 계속 흐르도록 하는 “완전완비제품(whole product)”의 한 부분에 불과하다. 기존의 데이터센터에서 UPS는 이중마루의 가장자리에 또는 완전히 다른 방에 위치하며 주문제작 도관 및 전선 어레이가 컴퓨터 및 기타 중요 장비가 탑재된 랙으로 전력을 끌어온다. 전기기사 등이 이러한 주문제작 시스템을 현장에서 설치해야 한다. InfraStruXure에서는 배전 시스템 배선이 완전히 공장에서 이루어진다. Mtech은 양쪽 공장에서의 생산 과정과 현장 설치를 분석했다. APC 공장의 제작 과정에서는 눈금조정, 품질 관리, 전문화된 설비와 도구 및 모든 제품의 자동 검사가 이루어지기 때문에 Mtech은 공장 배선 및 현장 배선 시스템에서 예상되는 결함의 수에 있어 상당한 차이를 발견했다.

단일 분기 회로 설치를 위해서는 적절한 와이어나 케이블의 선택에서부터 도관에 설치(현장-배선 어셈블리)하고, 와이어 피복을 벗겨내고, 파워스트립이나 회로차단기와 같은 중단 장치로 연결하고, 마감된 연결부를 표시하는 등 많은 단계가 필요하다. Mtech은 공장제작 및 현장제작 시스템 두 가지 모두에 대해 설치 과정 각 단계의 오류 발생 확률을 분석했다. 이 분석에서는 군 및 핵 관련 시설의 안정성 분석에 사용되는 데이터와 방법을 사용했다. 현장 연결에서 결함이 발생할 확률은 공장 배선 시스템보다 약 1,500배 더 높았지만, 이러한 차이는 본 안정성 비교 분석에 포함되지 않았다.

모든 결함이 장비 장애로 이어지는 것은 아니고 라벨링이 잘못된 스위치나 와이어와 같은 결함은 시스템 사용연한 내내 발견되지 않은 채 지나칠 수도 있다. 라벨링이 잘못된 구성요소는 종종 IT 설비 변경 중에, 분기 회로 차단기를 열었을 때 엉뚱한 장치에 예상치 못한 로드 손실이 일어나면서 발견되곤 한다. 이것은 종종 '운영자 실수'로 간주되지만 실제로는 현장 배선 중 잠재적 결함이 발생한 결과다. 공장 및 현장 배선 고장율의 이와 같은 큰 차이는 모든 고객에게 유용한 중요한 시사점을 제공해 준다. 즉, 표준화된 제품과 표준화된 공장 제조 기법들이 최고 수준의 안정성을 갖춘 시스템을 만든다는 것이다. 주문제작 제품, 맞춤형 현장 배선 및 비표준적인 고유 조작 절차는 의심의 여지없이 일반적 오류와 특정한 문제가 발생할 확률을 모두 증가시킬 것이다.

Mtech은 APC의 제조 과정을 조사하고 안정성 증진 관리 기법의 효과를 평가했다. 한 개의 전원 모듈을 가진 중앙집중식 UPS 시스템과 비교해 다섯 개의 전원 모듈을 가진 InfraStruXure의 설계와 관련해 제기될 수 있는 당연한 의문점이 있다. InfraStruXure가 다섯 개 모듈 중 하나에 고장이 발생하더라도 작동이 가능하도록 설계되기는 했지만 모듈이 다섯 개면 단일 모듈 시스템에 비해 다섯 배 더 자주 고장을 경험할 것이라고 주장할 수도 있다. 과연 그럴까?

Mtech은 전원 모듈 장애의 원인과 영향을 분석하여, 전원 모듈 장애의 빈도가 더 높더라도 그 증가량은 이중화로 인해 상쇄되고도 남는다는 결론을 내렸다.

다수의 모듈 사용에 따른 이점 중에서 본 연구에서는 정량화되지 않은 사항이 있다. 일단 한 제품의 매출액이 전용 제조 시설의 비용을 정당화할 수 있게 되면, 제조 결함의 발생 비율은 대폭 감소한다. 전담 인력, 시험 설비, 그리고 경험이 결합해 결함이 생길 가능성을 없애는 것이다. 이러한 전용 제조 시설은 대부분의 일반적인 오류가 발생이 불가능할 정도로 빠르게 발전할 것이고, 설사 일반적인 오류가 발생했다고 하더라도 조립부품이 공장에서 출하되기

전에 신속하고 일관성 있게 검출되어 수정될 것이다.

InfraStruXure의 모듈식 설계는 다수의 전원 모듈이 모든 유닛과 함께 배송된다는 것을 의미한다. 따라서 APC는 다른 단일 모듈 제품을 생산하는 경쟁업체에 비해 전용 전원 모듈 제작 시설로 좀 더 빠르게 전환할 수 있다. 단일 모듈 시스템에 비해 유지보수 서비스가 제공되는 모듈이 더 많기 때문에 APC는 출하되는 제품에서 구성요소 결함 및 그와 유사한 오류를 더 빨리 발견할 수 있다. 마지막으로 APC는 모듈 고장의 원인을 좀 더 정확하게 판단할 수 있는데, 고객이 고장난 모듈을 신속 간편하게 교체한 다음 진단 및 수리를 위해 APC로 돌려 보낼 수 있기 때문이다. 대부분의 단일 모듈 설계는 현장에서 수리해야 하기 때문에 문제의 근본 원인을 파악해 내는 과정이 훨씬 더 어렵다.

현장 수리 문제는 잠재적으로 또 다른 고장의 원인이 될 수도 있지만 본 연구에서는 이를 검토하지 않았다. 현장 수리는 공장 수리보다 새로운 결함을 초래할 가능성이 훨씬 더 높다. 모든 UPS 제조업체가 고가능성 테스트(high potential testing), 특정한 극한 환경에서의 기능 테스트 등을 포함해 모든 생산 유닛에 일련의 테스트를 실시한다. 하지만 현장 수리는 그 정도의 엄격하고 포괄적인 테스트가 거의 불가능하다.

결론

Mtech이 InfraStruXure 아키텍처에 대해 PRA 분석을 수행한 결과, 중앙집중식 UPS에 비해 안정성이 우수하다는 점이 증명되었다. 운용 연수에 따른 장애 확률의 차이는 장애의 정의와 중앙집중식 UPS 배터리 뱅크의 설계에 큰 영향을 받는다. 그러나 우리가 검토한 각 사례에서 InfraStruXure의 안정성이 더 높은 것으로 나타났다. 데이터센터의 장비에서 발생하는 장애는 양쪽 UPS의 장애보다 항상 더 심각했다.

APC는 InfraStruXure 제품이 모든 경우에서 확실한 안정성 우위를 보여주지는 않았더라도 본 연구가 나름의 가치를 지니고 있다는 사실을 발견했다. 원래의 연구 동기는 장애의 원인을 더 정확히 파악하고, 추가 투자로 기대할 수 있는 안정성 향상 폭이 가장 큰 구성요소 또는 프로세스를 규명하는 것이었다. 이러한 기준으로 볼 때 본 연구는 대단한 성공이었다.

본 PRA 연구는 InfraStruXure의 안정성을 크게 높이려면 더 우수한 구성요소와 테스트에 어떤 방식으로 투자하는 것이 최선인지 APC에게 보여주었다. 단 3가지 구성요소에 대한 투자만으로 장애의 빈도를 10%까지 줄일 수 있다. 일반적인 부품으로 제작된 InfraStruXure는 동등한 구성요소로 제작된 경쟁업체의 제품보다 안정성이 크게 높지는 않다. 본 연구 결과, APC는 PRA 분석에 따라 대다수 제품 장애의 원인으로 규명된 영역의 주요 구성요소에 주목하고 더 많은 자원을 투입했다.

본 연구는 또한 배전 시스템 배선의 사전 제작 및 테스트에서도 상당한 이점이 발생한다는 사실을 입증했다. APC 공장에서 사전 제작되는 배전 배선은 현장에서 제작되는 맞춤형 배전 시스템보다 잠재적 결함이 존재할 가능성이 1,500배 이상 낮았다. 모듈식 설계의 이점 역시 중요하며, APC는 이를 통해 가장 현대적이고 우수한 품질의 제조 기법을 활용할 수 있게 되어 비용을 낮추는 동시에 제품 안정성은 높이고 있다.

APC와 Mtech은 본 연구를 수행하는 동안 매우 많은 것들을 깨달았다. 다양한 설계 및 제조

기법의 역할과 효과에 대한 가정에 의문을 제기하고, 수학적 분석과 논리적인 논의를 거쳐 이를 수정했다. PRA는 설계 엔지니어와 현장 엔지니어의 기법과 제작 공정에 큰 도움이 된다. 일관되게 철저하게 적용된다면 PRA에 대한 투자는 제품의 안정성을 더욱 높여줄 것이다. 핵발전소의 안정성 계산에 사용된 기법이 급속히 발전하고 있는 전력 산업에도 매우 중요한 수단이 되고 있는 것이다. 이 분야에서도 장애로 인한 경제적 비용 및 인적 비용 또한 빠르게 늘어나고 있기 때문이다.

PRA는 서로 다른 제품과 시스템 아키텍처를 편향 없이 비교할 수 있는 방법이 되고 있다. 신중하게 수행된 PRA 연구 결과는 특정 응용 분야에 가장 적합한 제품 또는 아키텍처가 어느 것인가에 관해 합리적인 결정을 내릴 수 있게 해준다. 고객들이 충분한 정보에 입각하여 제품을 선택한다면 관련 업계에서도 제품의 안정성과 비용, 성능 등을 급속히 향상시킬 것이며 고객의 필요에 맞게 안정성과 기능을 조정할 수 있게 될 것이다. PRA는 제조업체, 데이터센터 설계자, 고객 등이 충분한 정보에 입각하여 합리적인 결정을 내리는 데 유용한 수단이 되고 있다.

참고 문헌

1. IEEE, Inc. IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear-Power Generating Stations. New York: IEEE Press, c1977. [IEEE Nuclear Reliability Data Manual.]
2. IEEE, Inc. IEEE Recommended Practice for Design of Reliable Industrial and Commercial Power Systems. New York: IEEE Press, 1988. [IEEE Gold Book: Power Systems Reliability.]
3. Hale, Peyton and Arno, Robert "Survey of Reliability Information for Power Distribution, Power Generation, & HVAC Components for Commercial, Industrial, & Utility Installations", IEEE Industrial and Commercial Power Systems Technical Conference, 2000.
4. Kumamoto, Hiromitsu, and Henley, Ernest J. Probabilistic Risk Assessment and Management for Engineers and Scientists. 2nd Ed. New York: IEEE Press, 1996.
5. Kusko, Alexander. Emergency/Standby Power Systems. New York: McGraw-Hill, 1989.
6. Military Handbook: Reliability Prediction of Electronic Equipment. MIL-HDBK-217F, Wash., DC: U.S. Dept. of Defense, January 1990.
7. Ramakumar, Ramachandra. Engineering Reliability: Fundamentals and Applications. Upper Saddle River: Prentice Hall, 1993.
8. Sanders, Mark S., and McCormick, Ernest J. Human Factors in Engineering and Design. 6th Ed. New York: McGraw-Hill, 1987.
9. Snevely, Rob. Enterprise Data Center Design and Methodology. Palo Alto: Sun Microsystems Press, A Prentice Hall Title, 2002.
10. Swain, A.D., and Guttman, H.E. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (THERP) Final Report. NUREG/CR-1278-F, Wash., DC: U.S. Nuclear Regulatory Commission, August 1983.

스티브 페어팩스(Steve Fairfax)는 MTechnology의 사장이다. 1997년에 MTech에 입사했지만 MIT 재학 시절부터 멀티-메가와트 전력 시스템을 연구해 왔는데, 재학 시절 토카막(tokamak) 핵융합로용 200 MW 전력 시스템의 구축 및 운전을 도왔다. 그는 Failure Analysis Associates에서 매니징 엔지니어로 일하는 동안 전력 시스템의 안정성에 대한 연구를 시작했다. 그는 MIT 플라즈마 퓨전 센터에서 Alcator C-MOD 핵융합로 설계 및 운전 책임자로, 그리고 보스턴 지역의 여러 회사에서 책임 엔지니어로 일했다. 그는 MIT에서 물리학 및 전자공학 석사 학위를 받았다.

널 다운링(Neal Dowling)은 MTechnology의 수석 엔지니어다. 그는 오류 트리 분석(fault tree analysis)과 관련 모델링 및 시뮬레이션을 실시하고 새로운 전원장치와 스위치 기술을 개발 및 시험하고 MTech의 400 kW 연료전지 발전설비의 운전 및 유지보수를 감독한다. 그는 MTech에 들어오기 전에는 보스턴 지역의 여러 의료 기구 제조업체에서 일했다. 그의 전문 분야는 여러 핵심 기능, FDA 규정 준수 및 아날로그 및 디지털 설계를 위한 펌웨어와 소프트웨어의 개발 및 유지보수다. MIT 전자공학 학사 및 석사 학위를 소지하고 있다.

덴 힐리(Dan Healey)는 MTechnology의 수석 엔지니어다. 그는 인적 요소의 분석과 운전 및 유지보수 활동에 PRA 기법의 응용을 전문으로 하고 있다. 덴은 보스턴의 여러 회사에서 엔지니어링 책임자로 일하며 반도체 처리, 의료 장비, 로봇공학 및 전자광학 시스템을 위한 제품 개발을 감독했다. 그는 로체스터 대학에서 전자공학 학사 학위를 받았으며 대학원에서는 광학 및 프로그램을 연구했다. 현재 하버드대학에서 청강생(special student)으로 기술 및 소프트웨어 개발 관리를 공부하고 있다.

MTechnology는 21세기를 위한 전력 시스템 엔지니어링 기술을 제공하는 컨설팅, 시험, 제품 개발 및 프로토타입 제작 서비스 기업이다.

Mtech은 전력 시스템의 확률론적 위험 평가, 설계 검토, 고장 근원 분석을 실시하고 규정 및 소송 상황에서 감정인 증언을 제공한다. Mtech은 위험도 정보를 활용한 시스템 설계, 운전, 유지보수, 업그레이드 및 안정성 증진 관리에 관해 자문한다. Mtech의 고객들은 종종 투자 및 운영비는 크게 절감되는 동시에 안정성은 크게 증가한다는 것을 깨닫게 된다. 한편 MTech은 500 kW의 연속 로드와 멀티-메가와트 펄스 로드를 운전할 수 있는 능력을 갖춘 5000 제곱피트 규모의 시험 및 실험실 시설을 갖추고 있다. Mtech은 왕복기관 엔진 기술에서 연료 전지 기술에 이르는 고안정성 분산 발전 프로젝트를 진행해 왔다. Mtech의 고객들로는 보유한 설비를 24시간 상시 운영해야 하는 전력 회사, 설계자 및 엔지니어, 주요 설비 관리 및 운영 업체 및 제조업체들이 포함된다.