

# SEU, 고장 및 시스템 레벨 안전

*Martin Cornes, ControlSafe 제품 기획자, 그리고 Dan Weed, 안정성 및 안전 엔지니어*  
2018년 6월

SEU나 싱글 이벤트 업셋은 장치나 시스템 안에서 저장 요소 상태로 변경한 것입니다. 그것은 시스템은 예상대로 계속 작동하기 때문에 수년 동안 알아차릴 수 없을 수 있는 시스템에서 하나의 결함의 사례입니다. 본 논문에서는 SEU 그리고 기능성 안전 시스템에 영향을 미칠 수 있는 기타 잠재적인 결함이 시스템 레벨의 접근방식을 통해서 완화될 수 있는 방법을 요약합니다. 이것은 사용자에게 추가적인 주기 또는 인증 실험 요건 없이도 시스템 수명 이상의 주문으로 기능적 안전 시스템에서 예상되는 위험 고장률을 개선합니다.

기능적 안전 적용을 위해서 시스템을 설계하거나 구매하는 시점을 고려할 것들이 많습니다. 가장 큰 함정들 중 하나는 개별 모듈의 주요 또는 특정 안전 기능에 대한 초점입니다. 이것이 뜻하는 바는, 사람들은 때때로 총 시스템 안전 및 유용성에 대해 더 큰 그림을 볼 수 없다는 것입니다.

수많은 산업별 기능 안전 표준이 있고 이것들 대부분은 IEC 61508에 근거를 두고 있습니다. EN 50129는 IEC 61508에서 파생되어 주로 사용되는 철로 기준입니다. 이 기준들의 주요 기능은 시스템 안전 프로세스를 통해서 안전 제품을 생산하게 하고 필요한 안전 수준을 충족하기 위한 요건을 식별하게 하는 것입니다. IEC 61508 및 EN 50129는 모두 안전 무결성 레벨(SIL)을 통해서 필요한 안전 정도를 분류합니다. 충족하기에 가장 어려우면서도 가장 높은 안전 레벨은 안전 무결성 레벨 4(SIL4)입니다. 모든 기능 안전 증명이 동일하지는 않습니다. 두 개의 제품이 안전 무결성 레벨로 인증을 받았다고 해서 그 제품들이 적용에 동일하게 적합하다는 것을 의미하지는 않습니다. 그것은 제품들이 어떤 안전 기능을 제공하고 운영 제약이 무엇인지에 따라 다릅니다.

또한, 특정 SIL 레벨로 시스템 사용을 인증을 받았다고 해서 그것이 사용자의 수요를 충족한다는 것을 의미하지 않습니다.

## 안전 기능 및 아키텍처

우선 안전 기능과 아키텍처를 봅시다. 최고의 안전 레벨로 인증을 받기 위해 취해야 할 것은? 개요:

- 시스템은 인증 기관으로부터 인증을 받아야 합니다. 인증은 2가지 주요 속성에 초점이 맞춰져 있습니다. 첫째, 시스템 아키텍처는 제품 수명 동안 발생하는 위험스런 고장의 확률에 대한 엄격한 제한을 충족합니다. 그리고 둘째, 제품은 설계 결함의 가능성을 최소화하기 위해 잘 정의된 프로세스를 사용하여 개발되었습니다.
- 시스템이나 모듈은 어떤 안전 기능이 그 시스템이나 모듈에 의해 실행되는지 그리고 사용자에게 의해 실행되어야 할 기능들 명확하게 정의해야 합니다. 예를 들어, 사용자는 주기적 실험을 실행하거나 시스템을 (우리가 '내보낸 제약'이라고 부르고 이것을 안전 사용 설명서에서 확인하는) 특정 방식으로 사용해야 합니다.
- 수많은 아키텍처가 가능하다고 해도 더 높은 SIL 레벨에는 리던던시가 안전-관련 기능에 필수적입니다. 일반적으로 이것에는 리던던트 센서 및 다양성, 그리고 2oo2 비교측정기나 2oo3 보팅 방식으로 알려진 마스터-체커 구성이 포함됩니다.
- 현실적인 이유 때문에, 일부 안전 집중 데이터는 '블랙 채널' 커뮤니케이션으로 알려진 비-안전

인증 네트워크 요소들간에 가끔 전송되어야 합니다. 이 경우에, 시스템의 중점은 일부 형태의 보팅이나 체킹을 갖추고서 중점에서 데이터 거래의 정확도를 인증해야 합니다.

- 리던던트 요소는 실제로 서로간에 독립적이어야 합니다. 즉, 그것들은 전력 같은 공통의 하부시스템을 공유하지 않고, 그것들간 인터페이스는 하나의 결함이 다른 것의 결함을 초래할 수 있는 연속 결함에 대해 보호를 받아야 하고, 그리고 그것들은 진동, 온도, 오염, EMI 등의 다른 공통 요소에 대응하여 튼튼해야 합니다.
- 결함의 탐지가 핵심입니다! 안전 기능에 영향을 미치는 어떠한 결함도 보통 안전 기능이 작동되지 않게 할 수 있는 리던던트 채널에서 안전 기능이 위험한 상황이 일어나지 않도록 충분히 그리고 제 2의 결함이 일어나지 않도록 신속하게 탐지되고 완화되어야 합니다.

## 리던던트 채널

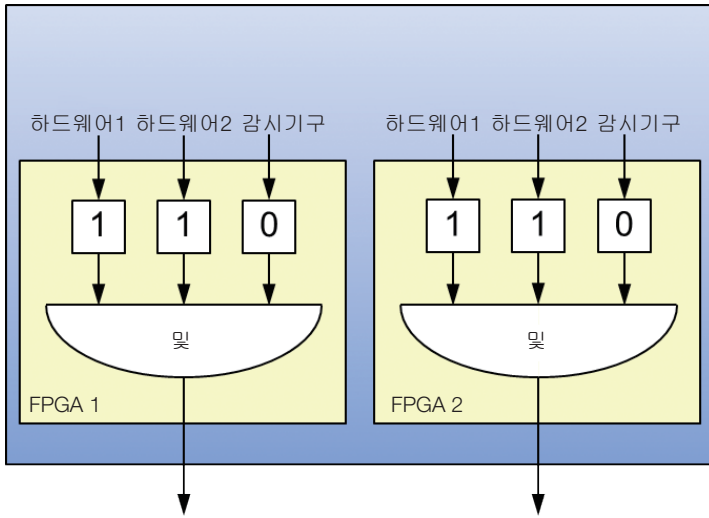
리던던트 채널이 모든 것을 해결하지 않나요? 리던던트는 수많은 문제점들을 해결하지만 그렇다고 모든 것을 해결하지는 않습니다. 간단한 사례를 봅시다.

안전 시스템은 단 하나의 결함도 없이 수주, 수개월 또는 수년 동안 작동할 수 있습니다. 시간이 지남에 따라, 내부 결함이 진전되어 안전 기능이 그것 자체의 결함을 탐지하거나 그것에 대응하지 못할 수 있습니다. 시스템이 장기간 동안 고장이 없을 경우, 우리는 그것이 필요할 때 결함을 탐지하고 그것에 대응할 수도 있는 것을 어떻게 압니까?

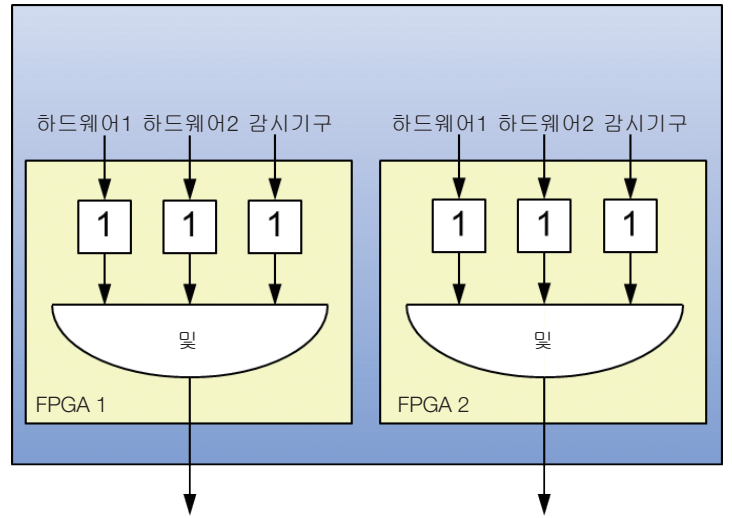
이에 대한 하나의 솔루션은 시스템에 결함을 주입하여 강제로 결함에 대응하게 하는 것입니다. 그러나 이러한 '증명 실험'은 어려울 수 있고, 시간이 소비되고, 일반적으로는 작동하지 못하도록 시스템을 분리해야 합니다.

여기에서 더 깊이 파고들어 리던던트 안전 감시기구 실행의 사례를 봅시다.

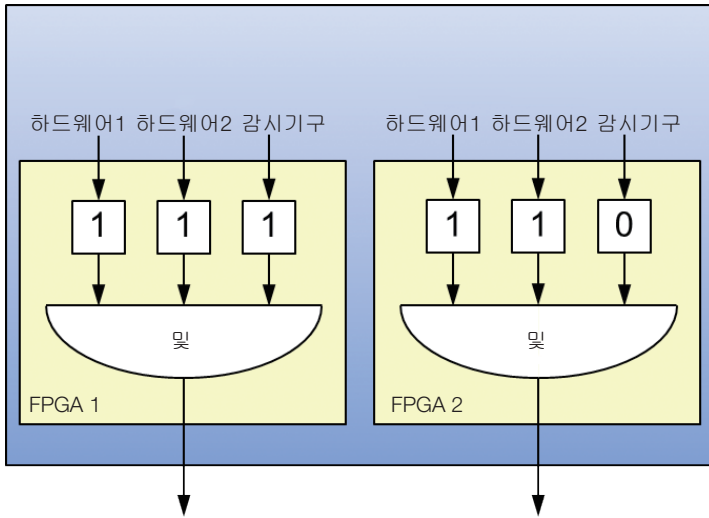
아래의 사례에서, 2개의 FPGA가 각각 3개의 신호들, 즉 하드웨어 소스에서 2개(HW1 및 HW2) 그리고 1개의 소프트웨어 감시기구(WD)를 모니터링하고 있습니다. 이 감시기구는 리던던트 FPGA에 대한 간단한 등록 인터페이스입니다. 소프트웨어 적용이 FPGA를 구별하기 위해 필요한 이 시나리오에서, WD 비트를 1의 일반 요건(소프트웨어 적용에 예상치 못할 중대 오류가 있을 경우, 그것은 감시기구를 재설정하지 않고 하드웨어는 고장에 대해 안전하게 된다)에 설정함으로써 계속 기능이 유지됩니다.



우리의 시나리오를 둘러보면, 소프트웨어는 여러 해 동안 아무 문제 없이 잘 작동하고 있고 스택 비트 결함이나 싱글 이벤트 업셋(SEU) 같은 것들이 WD 신호 자체에 또는 FPGA1 내에 일어납니다. 이제 WD 비트는 소프트웨어에 의해 리프레시되지 않는 경우에도 1에 고정됩니다. 이제 우리의 상황은 아래와 같습니다.



적용이 계속해서 잘 운영되고 있습니다. 수년 이상이 지나가고 적용이 이상한 오류 경로를 보이고 감시시구를 재설정하지 않습니다. 하드웨어가 그것에 무효합니다! 지금 우리에게 잠재적으로 위험한 상황이 있습니다. 드물고 거의 확률이 없지만, 우리는 본 백서에서 나중에 이것에 대해 토론할 것입니다.



우리에게 있는 것은 잠재적 결함으로서 우리는 이 결함을 탐지할 수 없습니다. 그러나 여기서도 여전히 문제가 없습니다. 그에 대한 조건은 적용이 폐쇄되고 FPGA1 WD가 리셋되지 않아 FPGA2가 계속 이것을 감시하고 고장에 안전할 경우입니다. 좋아요, 그것이 리던던시가 추구하는 것이죠?  
어느 정도 이후, 아마도 수년 이후에 유사한 사건이 FPGA2에 일어날 경우 어떨까요? 적용은 계속 아무 문제 없이 잘 운영되고 있지만 이제 우리에게는 아래와 같은 상황이 있습니다.

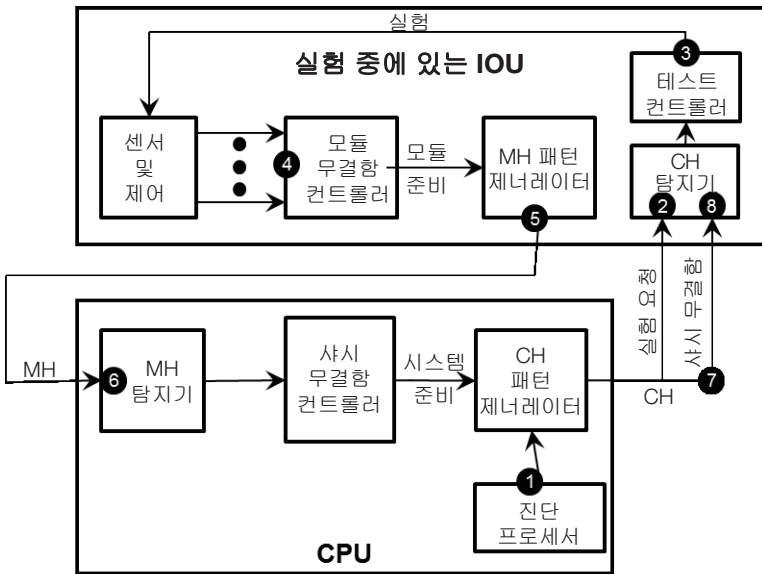
## 예방

그러면 사용자는 이러한 상황이 일어나지 못하도록 어떻게 할 수 있습니까? 위의 시나리오는 일어날 수 있는 하나의 결함 유형 사례에 불과합니다. 일부 결함은 모듈에서 국부적으로 탐지할 수 있지만 일부는 그렇지 않아 최소한 그 비트를 실제로 토글링하지 않고서는 오류를 강제하거나 그것을 탐지하는 방법을 관찰할 수 없습니다. 풀 샷시 레벨 솔루션은 샷시 내의 어떠한 결함도 제어 모듈에 통신할 수 있도록 필요하여, 샷시를 고장에 안전하도록 하면서 다른 무결함 샷시로 제어를 교환하도록 합니다. 이 추가된 보호 레벨은 고도의 유용성을 유지하면서 안전 레벨에 여러 실행을 주문할 수 있습니다.

위에서 언급했듯이, 이것을 실행하는 한 가지 방법은 증거 실험 프로세스를 통해서입니다. 시스템을 오프라인으로 취하고 결함을 주입하여 그것이 탐지되고 완화된다는 사실을 입증합니다. 이것은 복잡하고 값비싸게 될 수 있습니다. 예를 들어, Artesyn의 ControlSafe™ 컴퓨터에서 CPU 안과 밖으로 오는 이더넷 패킷은 비트별로 비교됩니다. 이러한 비교 작업을 입증하기 위해서, 잘못 연결된 패킷은 각 CPU로부터 보내야 합니다. 이것에는 사용자 정의 적용 소프트웨어가 필요합니다.

이러한 오프라인 실험에 대한 요건을 제거하기 위해서, Artesyn은 이러한 종류의 잠재적 결함을 탐지하고 결함 탐지에 시스템 대응을 입증할 수 있는 특허 받은 런타임 진단 프로세스를 실행했습니다.

당사는 결함을 시스템의 다른 모듈로 탐지할 수 있는지를 보기 위해 일시적 결함을 주기적으로 주입하는 시스템을 설계했습니다. 이러한 결함은 시스템 기능에 영향을 미치지 않고 페일오버로 이어지지 않도록 하기 위해 200µs 미만에 대해 주입합니다.

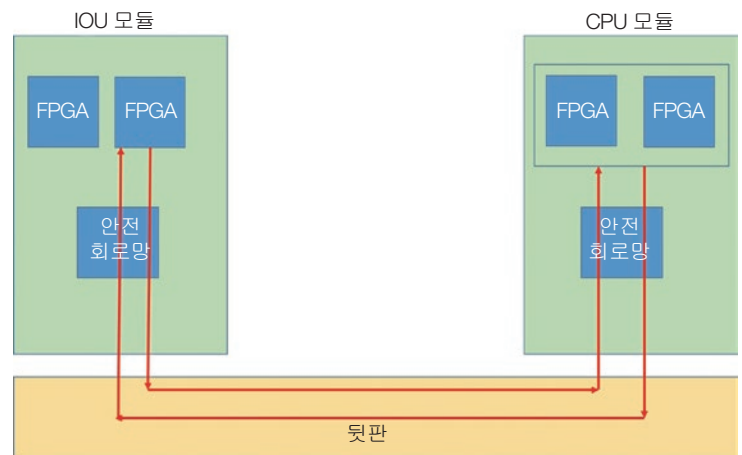


1. 진단 프로세서는 실험 요청을 모듈들의 하나 (그 자체, 동급 CPU 또는 IOU)에 발행합니다
  2. 모든 모듈은 실험 요청을 탐지하여 실험이 끝날 때까지 무결함 신호 상태를 무시합니다
  3. 취급된 모듈은 온보드 로직을 조정하여 결함을 자극합니다
  4. 이것은 모듈의 무결함 제어 등록기에 의해 탐지됩니다
  5. 그리고 이것은 모듈 무결함 신호의 주장 해제로 이어집니다
  6. CPU 모듈은 실험 중에 있는 모듈이 완전하지 않음을 탐지합니다
  7. 이것을 통해 CPU 샴시의 무결함 컨트롤러가 샴시 무결함의 주장을 해제하게 됩니다
  8. 실험 중에 있는 모듈은 주장 해제된 샴시 무결함을 탐지하고 실험이 성공적이었고 일상 운영으로 복구되었다고 결론을 맺습니다
  9. 다음 실험이 실행을 위해 예정되어 있습니다
- 다시, 이 모든 것은 하드웨어에 행해져서 200µs 미만에 실행됩니다. 또한 이 내부 결함 실험은 표준 실험 프로토콜을 통해 ControlSafe™ 샴시 내의 모든 모듈뿐만 아니라 CPU 모듈 내/사이에 실행될 수 있습니다. 일반적으로 완전한 순서의 실험은 24시간 내에 자동으로 실행됩니다.

이러한 유형의 실험이 사용자에게 제공하는 범위를 더욱 자세히 보는 것을 당사는 결함의 출처에 순간적인 결함을 주입함으로써 시작합니다. 예를 들어, 이것은 FPGA가 투표하는 잘못 맞춰진 패킷을 만들거나 온도 센서의 보정을 수정하여 정상적인 온도 범위에서 작동하게 하는 것이 될 수 있습니다. 이후 당사는 결함이 다음과 같이 탐지되고 있음을 실험할 수 있습니다:

- 결함에 대해 대응하는 FPGA,
- 결함에 대해 대응하고 상태를 바꾸는 그 모듈의 안전 회로망,
- 내부적으로 그리고 CPU 모듈의 뒷판에 안전 회로망에 의해 생성되고 있는 신호,
- 결함을 인식하는 CPU 모듈의 안전 회로망,
- 신호를 올바르게 처리하고 적절한 대응을 페일-세이프에 보내기 위한 CPU의 리던던트 FPGA의 능력,
- CPU 모듈 외부 그리고 실험 중에 있는 모듈 뒷판을 따라 보낸 신호,
- 안전 회로망을 통해 페일-세이프 신호가 올바르게 생성되었는지 확인하기 위해 실험 중에 있는 FPGA로 다시 보냄

완전한 엔드-투-엔드 경로가 실험을 거쳤습니다. 이 실험은 글로벌 헬스 테스트 컨트롤러(GHTC)에 의해 ControlSafe™ 샴시를 통해 일어나도록 배열되었습니다. 샴시의 각 모듈은 자체의 로컬 헬스 테스트 컨트롤러(LHTC)를 갖추고 있어서 내부 실험을 GHTC가 명령한 대로 내부 실험을 배열합니다. 실험이 통과하면 GHTC는 다음 실험을 배열하고 각 모듈을 통해 진행합니다. 이것은 시스템의 정상적 작동에 투명한 방식으로 매우 높은 레벨의 안전 진단 범위를 사용자에게 제공합니다.



## 계산

수학으로 봅시다. 우리가 이미 토론했듯이, 결함을 탐지하고 완화하도록 실행하기 위해 안전 기준이 필요로 하는 설계 고려사항이 많지만 특별히 결함이 장치를 정상적으로 작동하고 있는 것처럼 보이도록 만드는 상태에서 고착된 신호로 이어질 때 탐지할 수 있는 실리콘 장치에 하드웨어 결함이나 SEU가 항상 일부 있습니다. 문제는, 첫 결함이 탐지되지 않는다면 무엇이 유사한 결함이 리던던트 채널에서 일어날 수 있는 기회인가 관한 것입니다? 그것이 일어날 경우, 그러한 신호를 사용하고 있는 안전 기능은 작동불능으로 간주될 것이고 아무도 그것을 알지 못합니다.

안전 기준에는 이 문제를 보는 몇 가지 방법이 있습니다. ICE 61508은 시스템의 수명에 걸쳐 위험스런 고장의 전반적 확률을 봅시다. 즉 미탐지 결함의 영향을 포함시켜야 하는 분석, 주기적 실험을 통해 일부 기간(날에서 달까지)에 탐지된 결함 그리고 필수적으로 즉각 탐지된 결함들. 또한 EN 50129는 잠재적 결함이 결함의 확률과 리던던시 양을 기반으로 하여 잠재적 결함이 얼마나 오래 탐지되지 않는 상태로 지속하는가에 대해 수학적으로 제한합니다.

얼마나 내부 진단이 집단 내에서 전반적 위험 고장률에 영향을 미치는가를 보기 위해 하나의 사례를 통해 연구합시다.

FPGA과 그 외 요소에 대한 고장률에는 일반적으로 합리적인 예상치가 있습니다. 이러한 많은 요소는 패키지 부패, 중성자, 외부 EMI 소음, 내부 혼선 그리고 위치, 위도나 고도 같은 그 외 요소가 야기한 소프트 에러 비율(SER)에 의해서도 영향을 받습니다. SER에 불안이 크다면, 매우 보수적인 가정을 사용합니다.

이에 대한 예로, 우리는 10억 시간당 20번의 하드웨어 고장률을 사용합니다. 이것은 FIT(시간당 고장 회수)로도 알려져 있습니다. 그것에다 우리는 SER 고장에 대해 200 FIT를 추가합니다. 이 총 고장률은 2채널 시스템의 일부인 단일 채널의 안전 기능을 나타냅니다.

모든 결함이 위험하고 탐지되지 않는 것은 아닙니다. 일부 결함은 온도가 정상적임에도 불구하고 작동하는 온도 센서 같이 즉시 탐지됩니다. 그것은 동일 온도 센서가 작동할 수 없는 곳에서 우리가 관심을 두고 있는 다른 결함입니다. 이 사례에 대해, 우리는 결함들의 반은 탐지고 나머지 반은 탐지되지 않는다고 추정합니다. 실제적으로 더욱 정교한 분석을 각 요소에 실행합니다. 그러나 이 사례에 대해 우리는 채널당 총 미탐지 및 잠재적 위험 결함을 110 FIT라고 추정합니다.

다음에 25년 이상 작동하는 많은 시스템을 고려하겠습니다. 연간 평균 8,000시간으로 25년 이상 작동하는 5,000대의 열차는 합계 10억 시스템 시간을 제시합니다. 이것은 가장 높은 안전 무결성 레벨에서 목표는 10억 시간당 위험 고장이 한 번 미만이기 때문에 유용한 추정치입니다.

아래의 사례에서는 위의 사례 데이터를 사용하여 10억 작동 시간 동안 싱글 채널과 듀얼 채널 구성에 대해 25년 이후 고장 확률과 예상 고장의 수를 보여줍니다.

	HW FIT	SEU FIT	총 FIT	연간 시간	년수	장치 작동 시간	장치 고장 확률	열차 수	시스템 작동 시간	시스템 고장	25년간 시스템 고장
첫 번째 잠재적 결함	10	100	110	8,000	25	200,000	2.200%	5,000	1,000,000,000	110.0	110.0
두 번째 잠재적 결함	10	100	110	8,000	25	200,000	0.048%	5,000	1,000,000,000	2.42	2.420

두 번째 독립적 채널을 역동적으로 추가하면 예상 위험 고장의 총 숫자가 줄어들지만 그것은 여전히 안전 집중 시스템에 대한 것보다 거의 2.5배나 더 높습니다. 문제는 이러한 고장이 랜덤이고 독립적이며 시스템 수명 동안 언제라도 일어날 수 있다는 점입니다. 하나의 채널에 위험스런 미탐지 고장이 있자마자 전반적 시스템은 듀얼 채널에서 싱글 채널로 효과적으로 되돌아갑니다.

이것을 아래의 사례에 비교합니다. 여기에서 우리는 내부 진단을 분기별로 실행하여 그렇지 않을 경우 미탐지될 내부 결함을 탐지합니다.

	HW FIT	SEU FIT	총 FIT	연간 시간	년수	장치 작동 시간	장치 고장 확률	열차 수	시스템 작동 시간	시스템 고장	25년간 시스템 고장
첫 번째 잠재적 결함	10	100	110	8,000	0.25	2,000	0.022%	5,000	10,000,000	1.1	110.0
두 번째 잠재적 결함	10	100	110	8,000	0.25	2,000	>0.001%	5,000	10,000,000	0.00	0.024



싱글 채널에 25년 동안 총 고장 숫자는 여전히 위와 같음을 주목합니다. 차이는 양 채널의 고장 확률에 있습니다. 하나의 채널이 고장날 경우, 두 번째 채널은 진단을 실행하여 첫 결함이 탐지되기 전에 충분히 오래 살아있어야 합니다. 25년의 수명 동안, 고장나고 미탐지되고 있는 양 채널의 확률은 집단에 대해 25년간에 1개 미만으로 급격하게 떨어집니다. 주목해야 할 것으로는, 이 사례에서 ControlSafe™ 시스템은 24시간 주기로 이 실험을 실행하지만 분기별이 아닙니다.

사용자는 위의 표에서 안전 기준이 왜 결함 탐지를 강력하게 강조하면서 리던던트 채널을 동시에 요구하는가를 볼 수 있습니다. 이를 통해서 모듈은 안전할 수 있도록 필요한 FIT 레벨을 취할 수 있습니다.

듣금 없지만, 그러한 10억 시간은 그렇게 긴 시간이 아닙니다.

## 결론

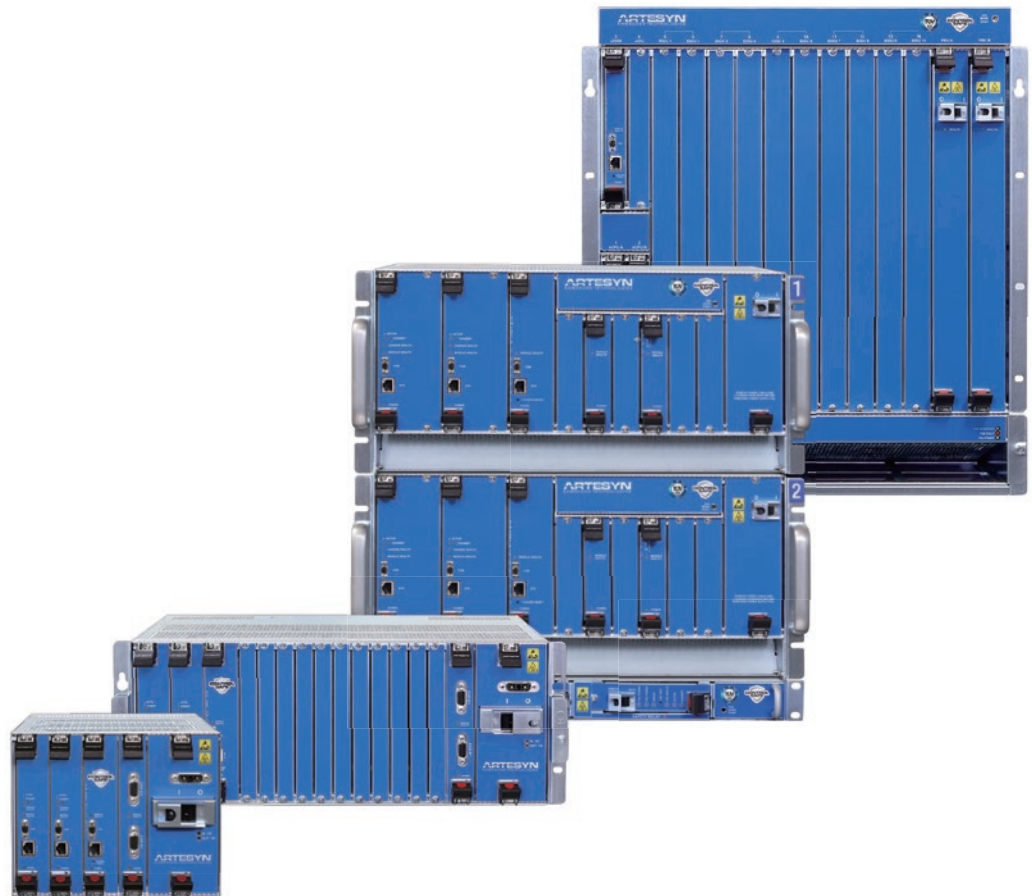
위에서 설명한 때로 샤시 또는 시스템 범위의 실험 프로토콜을 실행하여, 시스템 수명에 걸쳐 예상되는 위험 고장률은 사용자에 대해 추가적으로 주기적 또는 증명 실험 요건 없이 여러 주문을 통해 개선되었습니다. Markov 모델을 사용하여 더욱 복잡한 분석을 통해 개선을 위험 고장 확률에 4배 감소에서부터 안전 기능에 따라 50배 감소까지 다양함을 볼 수 있습니다.

샤시의 모든 모듈은 자동 및 체계적인 내부 실험 시퀀스 일부가 되었습니다. 샤시의 모든 모듈은 자체의 내부 실험을 실행할 수 있지만 이러한 실험을 처리하고 상태를 통신하는 공통의 프로토콜을 통해서 ControlSafe™ 컴퓨터는 전반적 시스템 무결성을 결정하고 무엇인가가 잘못되면 서비스가 중단되지 않도록 대기 컴퓨터로 교체되도록 합니다.

개별 성분이 안전 기준을 충족하고 사람들이 완전한 시스템을 볼 수 있게 하는 것은 매우 중요합니다. 그렇게 할 때, 전체 안전 경로를 실험하는 완전한 샤시나 시스템 레벨 테스트 계획에 대한 수요가 명확해지고 필요해지면서 고객 영향이 최소화된 안전한 시스템이 보장됩니다.

Artesyn의 ControlSafe 플랫폼에 대해 더욱 자세히 알아보려면 다음 사이트를 방문하십시오:

<https://ko.artesyn.com/computing/products/category/controlsafe>



## Artesyn Embedded Technologies 에 대한 설명

Artesyn Embedded Technologies는 통신, 컴퓨팅, 가전제품, 의료, 군, 항공우주 및 산업 등 다양한 산업 용도의 전력 변환 및 임베디드 컴퓨팅 솔루션의 디자인과 제조에 있어서 세계적인 선두 업체입니다.

고도로 안정적이고 유용한 임베디드 컴퓨터 시스템 개발에 30년 이상의 전문성을 활용한 Artesyn은 철로 시스템 통합자들과 철로 애플리케이션 제공자들에게 상업용 기성(COTS) 장애 내성 컴퓨터 시스템을 제공하는 최고의 업체입니다.

그토록 오랜 경험을 통해서, 탁월한 고객 지원과 동시에 적시의 지속적이고 고품질의 제품에 대한 당사 고객들의 요구사항을 깊이 이해하게 됩니다. 당사는 당사 소유의 세계적 수준의 공장 및 숙련된 지원 전문가를 통해서 모든 지원을 아끼지 않습니다.

Artesyn은 고객들의 수익 창출 시간을 단축하고 고객 개발 과정을 가능한 한 쉽게 하도록 노력합니다. 제품 기능은 사용자 일정을 유지할 수 있도록 로컬 시스템 기획자와 현장 적용 엔지니어(FAE)로 전세계적으로 지원을 받습니다.

당사는 매우 유연하고 민첩하게 대처합니다. 당사는 고객에게 자신 고유의 브랜드를 갖추는 시스템이 필요할 수 있다는 사실을 인식하고 있습니다. 문제 없습니다. 당사는 그것에 익숙해져 있습니다. 당사는 고객에게 외관을 정의할 수 있게 하는 서비스를 갖추고 있고 그것은 고객 회사의 브랜드 및 미적 기준과 일치하고 있음을 느낍니다.

당사의 유연성은 외관과 느낌에만 국한되어 있지 않습니다. 통합 서비스, 고유의 지원 요건, 공급의 장기성, 생산자 직송 그리고 수많은 서비스가 우리와 사업하는 것을 더욱 쉽고 만들고 고객이 시장에 진입하여 연락처 하는 것을 빠르게 하도록 설계되어 있습니다.

40년 이상, 고객들은 Artesyn이 출시 시간을 단축할 뿐만 아니라 개발 노력을 통해 새롭고 가치가 부가되는 기능 및 서비스로 이어지는 것을 돕고 있다고 신뢰해 왔습니다.

아리조나 주 템페에 본사를 두고 있는 Artesyn은 여러 곳의 우수한 엔지니어링 센터, 전액 출자한 세계 수준의 제조 시설 그리고 세계 판매 및 지원 사무실에 15,000명 이상의 직원을 두고 있습니다.

## 담당자

전화번호 : +82 2 6004 3266

이메일 : [powersales@artesynt.com](mailto:powersales@artesynt.com)

<https://ko.artesynt.com>

Artesyn Embedded Technologies, Artesyn 및 Artesyn Embedded Technologies 로고는 Artesyn Embedded Technologies, Inc의 상표 및 서비스 마크입니다. 그 외 언급된 모든 이름과 로고는 관련 소유자의 상품명, 상표 또는 등록 상표입니다. 고지 없이도 사양은 변경될 수 있습니다. © 2018 Artesyn Embedded Technologies, Inc. 모든 권한 보유. 약관 전문은 [www.artesynt.com/legal](http://www.artesynt.com/legal)을 방문하여 확인하실 수 있습니다.

주소:  
Artesyn Embedded Technologies  
2900 S. Diablo Way, Suite 190  
Tempe, Arizona 85282