DIGITAL INDUSTRIES SOFTWARE

데이터 보안
SoC(Systems on chip)에 대한 혁신적인 검증 능력을 제공

Richard Pugh
Siemens EDA

SIEMENS

서론

사람이 컴퓨터와 주고받는 상호작용이 엄청나게 확대되면서, 기업과 비즈니스에서는 데이터 보호와 무결성이 중대한 과제로 대두되었습니다. 이 때문에 엄청난 양의 정보가 생겨나고 "빅 데이터"의 시대가 도래하면서 대량의 데이터 세트를 수집하고 분석하여 여러 분야에서 지식과 발전을 도모하게 되었습니다. 그리고 바로 이 데이터의 보안이 중대한 요구 사항으로 떠올랐습니다.

Identity Theft Resource Center의 2021년 데이터 침해 보고서에 따르면 2021년 한 해 동안 발생한 데이터 침해 사건은 1,862건으로, 2020년 대비 68%나 증가하여 역대 최고치를 기록했습니다.

데이터 보안에서는 다양한 암호화 형식, 키 관리와 인증을 통해 인증되지 않은 사용자가 무단으로 데이터에 접근할 수 없도록 보호하는 것이 관건입니다. 이렇게 해서 다음과 같은 보안 주체와 관련된 중대한 자산을 보호를 제공하게 됩니다.

- 소비자: 데이터 무결성과 기밀 보장
- 비즈니스: 평판, 매출원과 지적 자산
- 정부: 국가 안보, 국방, 주요 인프라

보호를 통해 공급망, 물리적 공격, 지속적 공격과 악성 구성요소로부터 들어오는 공격을 차단해야 합니다.

중점은 데이터 보안 공격에 취약한 소프트웨어를 노리는 공격에 맞선 보호에 대체로 맞춰져 있는 편이지만, 하드웨어도 점점 취약해지고 있습니다. 예를 들어 최신 전자제품과 부품에 쓰이는 반도체 칩도 공격의 표적입니다.

그림 1. 데이터 침해는 대기업에 약 1,800만 달러를 들여 해결해야 하는 글로벌 위협으로 점차 규모가 커지고 있습니다.

하드웨어 인터페이스는 SoC 데이터 취약성의 근원입니다

복잡한 장치, 즉 시스템온칩(SoC)은 보통 다양한 프로토콜 하드웨어 인터페이스를 사용합니다. 예를 들어 이더넷, 동영상, 오디오, 메모리와 PCI Express 등은 여러 애플리케이션에서 보편적으로 쓰입니다.

이런 인터페이스는 잠재적인 공격자가 보안을 침해할 수 있는 SoC 설계 취약점이 될 수 있습니다.

공격자에 맞서 시스템을 보호하려면 프로토콜마다 데이터 보안 메커니즘을 기본 내장해야 합니다. 칩 설계와 그와 연관된 애플리케이션은 워낙 종류가 광범위하고, 이런 칩 중 대부분은 여러 업종에서 PCI Express 프로토콜을 사용하고 있습니다. 따라서 PCI Express는 잠재적인 공격자에게 아주 손쉬운 표적이 됩니다.

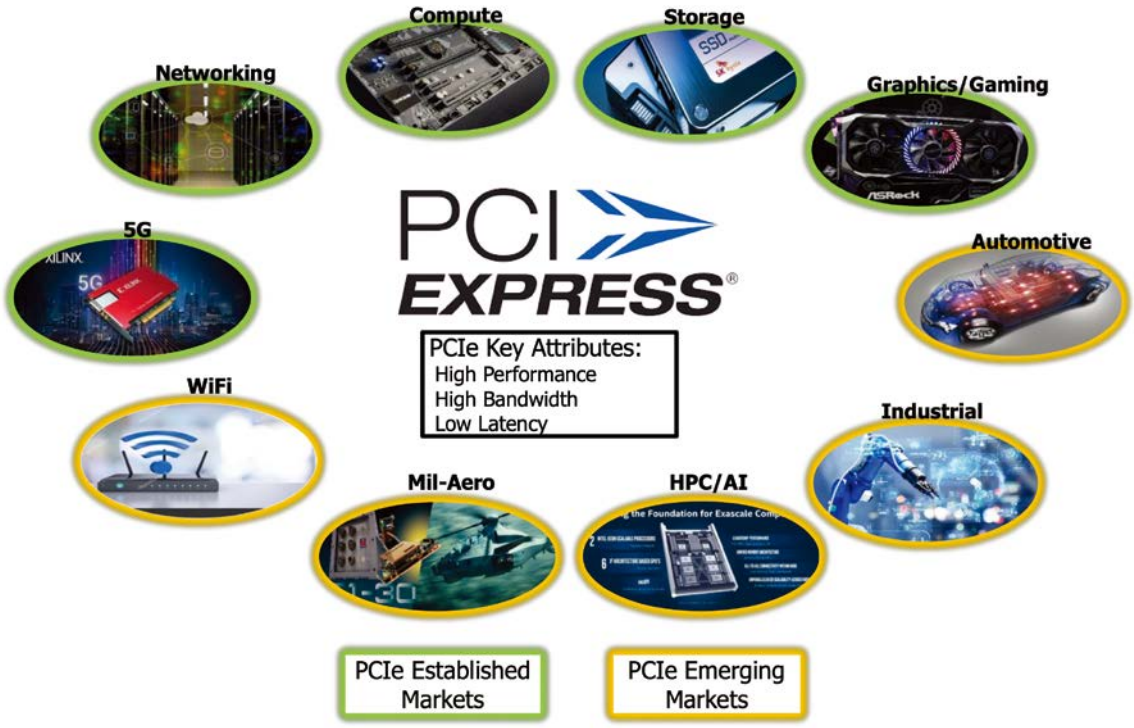

그림 2. PCI Express는 SoC의 가장 보편적인 인터페이스 프로토콜입니다.

PCI Express Data의 보안 확보 – 무결성 및 데이터 암호화(IDE)

PCI Express 프로토콜의 데이터 보안에 대한 늘어나는 요구 사항에 부응하기 위해, 지난 2020년 12월 Peripheral Component Interface Special Interest Group(PCI-SIG)에서는 PCI Express 버전 5.0에 추가 기능을 통해 무결성 및 데이터 암호화(IDE)를 추가하였습니다. 이러한 IDE 기능은 최근 출시된 PCI Express 6.0 version에 포함되어 있습니다.

PCI Express 상의 IDE 보안 메커니즘은 PCI Express 트랜잭션 레이어 패킷(TLP)에 대한 기밀성, 무결성, 재생 보호를 제공합니다. IDE는 광범위한 PCI Express 사용 모드를 지원하며, 데이터 보안에 관한 업계 모범 사례와 일맥상통하는 확장 가능한 솔루션입니다. 또한 PCI Express 링크를 노리는 물리적 공격, 기밀 데이터 읽기, TLP 콘텐츠 변경, 그리고 다음과 같은 경로를 통한 TLP 순서 다시 매기기 및/또는 삭제 등의 공격에 맞서 보안을 확보합니다.

- 연구실 장비
- 특수 제작 인터포저
- 악성 확장 장치

그림 3은 PCI Express TLP 패킷에 암호화를 적용하여 PCI Express 장치끼리 데이터를 교환할 때 보안을 제공하는 방법을 나타냅니다. IDE 기능은 업계 표준 AES-GCM[1] 암호화 보호를 활용하여 TLP 전체에 인증 무결성 보호를 제공합니다. 그런 다음 이처럼 암호화된 TLP 패킷은 표준 링크를 통해 TLP 데이터를 복호화하는 PCI Express 수신 장치로 전송됩니다. 마지막으로, 보안 TLP 데이터를 시스템 나머지 부분에 안전하게 전달합니다.

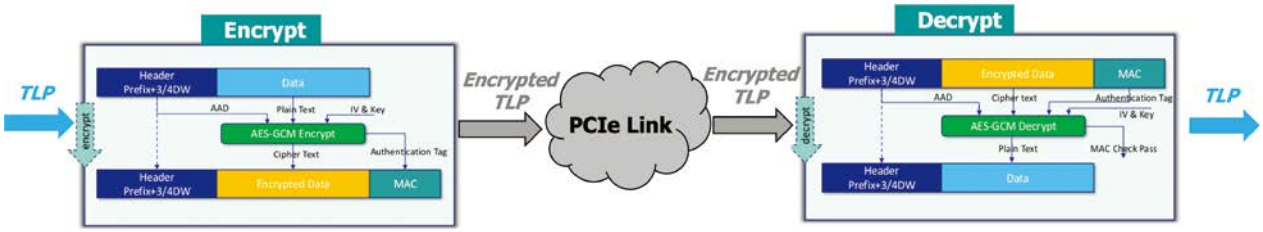

그림 3. PCI Express TLP 패킷의 IDE 암호화/복호화 플로우. 출처: PCI-SIG.

PCI Express 기반 SoC 설계에서 verification 솔루션의 역할

Verification 솔루션이란 전자 부품 시스템 개발 플로우에 사용되는 확립된 방법입니다. 이는 SoC의 프리 실리콘(pre-silicon) verification에 광범위하게 사용되며, PCI Express와 같은 업계 표준 프로토콜의 동작을 모델링하는 데도 쓰여 verification 엔지니어가 RTL에서 실리콘 전 설계를 실제 환경의 실제 칩과 아주 유사한 환경에서 현실적인 벡터를 사용해 자극할 수 있게 해줍니다.

요즘은 verification 솔루션이 여러 가지 형식으로 나와 있습니다. 일반적인 컴퓨터에서 실행하는 시뮬레이션 기반 소프트웨어 솔루션, 일명 verification IP부터 전용 하드웨어에서 실행하는 하드웨어 기반 솔루션, 즉 인-서킷 솔루션(ICE)까지 다양합니다. 이러한 ICE 솔루션의 경우, 사용자의 설계를 실행 중인 하드웨어 지원 verification 플랫폼에 연결하여 순전히 소프트웨어 시뮬레이션만으로 가능한 것보다 최대 수천 배까지 verification 성능을 끌어올려 줍니다.

지난 십 년 사이 회로 내 솔루션의 성능과 비견할 수 있는 선구적인 솔루션이 개발되었지만, 이런 솔루션은 전용 하드웨어를 통해 제공하지 않고 소프트웨어 전용 verification 구성요소 형태, 즉 *가상 ICE 솔루션*이라는 형식으로 제공되었습니다. 그림 4는 프리 실리콘 verification 작업을 담당하는 디지털 엔지니어가 현재 구할 수 있는 시중의 솔루션 유형을 나타냅니다.

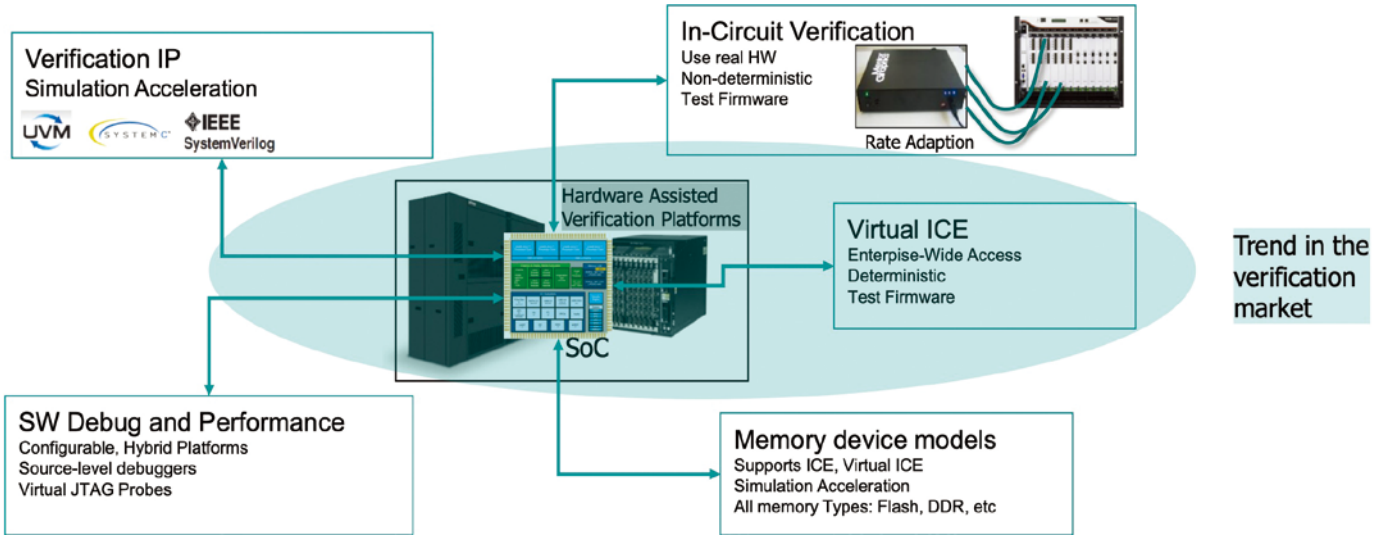

그림 4. verification 솔루션은 디지털 설계의 초석입니다.

verification 솔루션 유형마다 디지털 엔지니어가 verification 프로세스에 사용할 수 있는 "최고 장점"이 각기 다릅니다. 이는 환경, 기능, SoC 설계의 전반적인 verification 목표에 따라 다릅니다.

지난 십 년 동안은 가상 ICE 솔루션으로 이동하는 추세가 두드러졌습니다. 이 솔루션이 verification 작업에서 성능, 디버깅과 사용자 경험 면에서 가장 유연성이 뛰어났기 때문입니다.

이와 같은 가상 추세의 최전방에 선 Siemens EDA에서는 자사 VirtuaLAB의 일부분으로 가상 솔루션 포트폴리오를 만들어 SoC 프리 실리콘 verification을 지원하기로 했습니다. VirtuaLAB의 몇 가지 명확한 장점 덕분에, 지난 30년간의 verification 솔루션 역사상 가장 혁명적인 변화를 불러왔다 해도 과언이 아닙니다.

VirtuaLAB은 다음과 같은 본질적인 장점으로 하드웨어 지원 verification이라는 분야를 완전히 변혁했습니다.

- 전용 하드웨어가 필요하지 않으면서 ICE와 기능은 같음
- 빠르고 간편한 구성
- 여러 사용자 이용 가능, 전사적 액세스 가능
- 저비용에 안정성이 매우 뛰어남
- 결정론적, 반복 가능한 verification 결과
- 데이터 센터와 호환됨

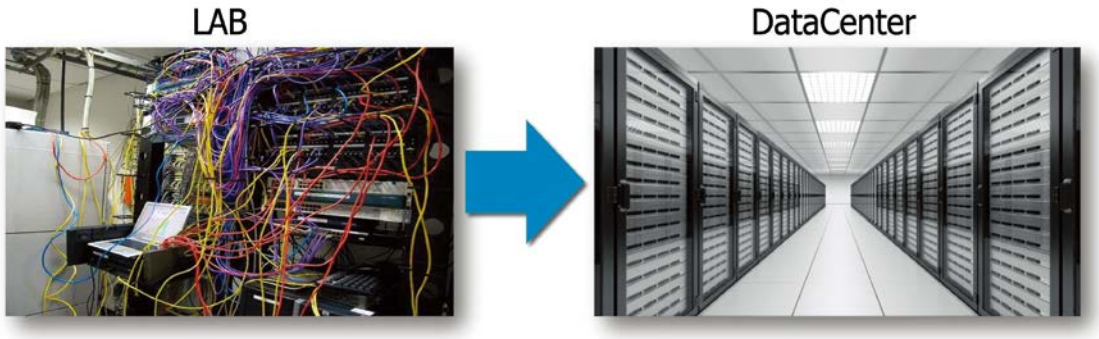

그림 5. 검증을 LAB에서 DataCenter로 전환하는 VirtuaLAB 혁명.

SoC 프리 실리콘 verification을 위한 VirtuaLAB PCI Express

Siemens EDA에서는 VirtuaLAB의 강점을 PCI Express에 도입하기 위해 VirtuaLAB PCI Express를 만들어 SoC 프리 실리콘 verification의 요구 사항을 해결하고자 했습니다.

VirtuaLAB PCI Express 솔루션은 pre-silicon system level 검증의 PCI Express 엔드포인트 및 switch를 위해 실제 PCI Express root complex를 모델링 하였습니다. 이 솔루션은 가상머신(VM)을 사용하여 모델링한 PCI Express 호스트 시스템으로 구동되고 운영됩니다. VM에서 실행되는 게스트 운영 체제 소프트웨어는 사용자의 DUT(Design-under-test)를 PCI Express 버스 계층 구조의 업스트림 PCI Express 장치로 간주합니다. 이렇게 하면 사용자의 애플리케이션 소프트웨어가 실제 하드웨어와 상호작용하듯이 DUT와 상호작용을 주고받을 수 있습니다.

또한, VirtuaLAB solution은 그래픽 상호적인 protocol analyzer라는 tool을 제공하여 PCI Express 프로토콜에 대한 풀 스택 visibility와 분석을 제공합니다. 이것이 여러 레이어에서 PCIe 프로토콜 패킷을 모니터링, 추적, 디코딩, 시각화하는 것입니다. 또한 DUT와 교환되는 PCI Express 패킷 전체에 대하여 런타임 가시성을 제공하면서 강력한 디버깅과 분석 기능이 보장되므로 사용자가 verification 실행 중에 PCI Express 프로토콜 문제를 디버깅하고 분석하는 데 도움이 됩니다.

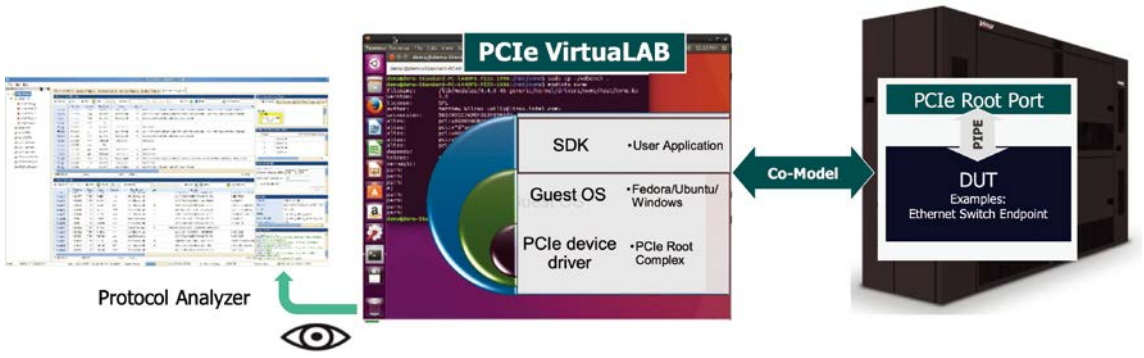

그림 6. PCIe SoC의 Hardware-assisted verification을 위한 Virtual PCI Express solution.

프리 실리콘 단계에 PCI Express 무결성 및 데이터 암호화 제공

VirtuaLAB PCI Express는 PCI Express root complex 안에서 IDE를 구현하므로 프리 실리콘 환경에서 장치 드라이버를 개발함과 동시에 사용자의 엔드포인트 IDE 설계를 verification할 수 있습니다.

VirtuaLAB 솔루션은 소프트웨어에서 IDE를 구현하면서 하드웨어에서 함수를 복잡하게 모델링할 필요를 줄여주므로, 결과적으로 하드웨어 verification 플랫폼의 리소스 요구 사항이 완화됩니다.

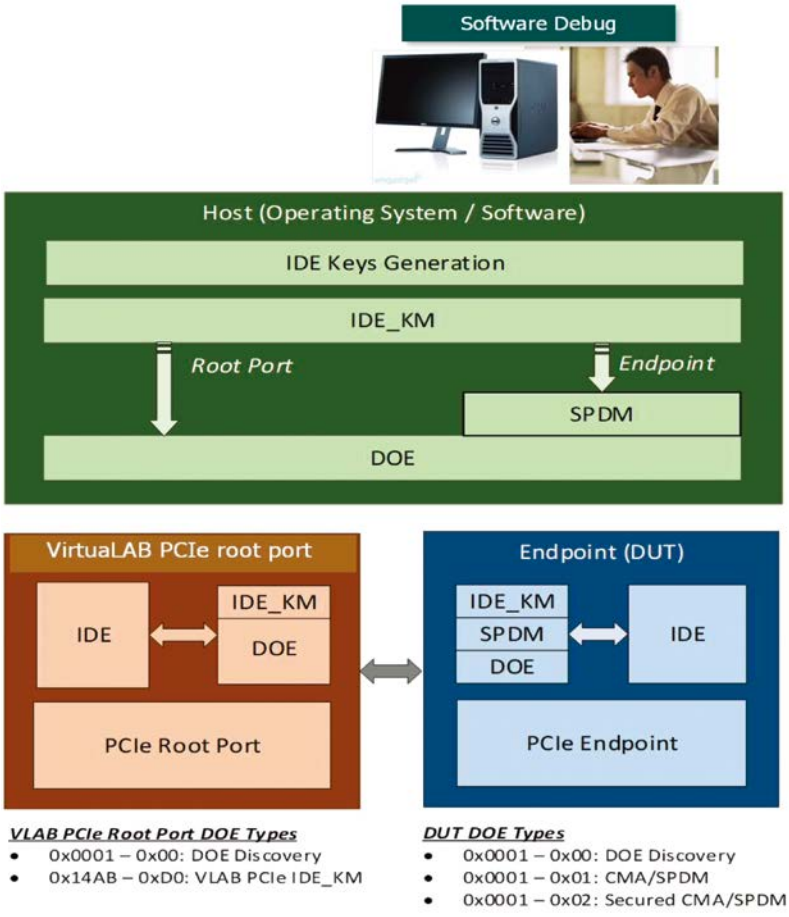

그림 7. VirtuaLAB PCI Express: IDE 구현.

IDE 주요 프로그래밍은 PCI Express 루트 포트와 엔드포인트 장치 양쪽 모두 호스트 운영 체제와 장치 드라이버가 수행합니다.

VirtuaLAB PCI Express 솔루션에서 루트 포트는 보안 프로토콜 및 데이터 모델(SPDM)을 우회하여 데이터 개체 교환(DOE)과 직접 바인딩될 수 있으므로 verification 프로세스에서 사용하기 간편합니다. 사용자의 PCI Express 엔드포인트 DUT 장치의 경우, IDE 주요 프로그래밍은 SPDM을 통해서나 DUT가 지원하는 여타 모든 메커니즘을 통해 수행될 수 있습니다. VirtuaLAB PCI Express 솔루션은 사용자 환경에서 배포하기 쉽도록 메모리 엔드포인트 예시 design도 제공합니다.

또한 VirtuaLAB PCI Express 솔루션은 통합형 프로토콜 분석 장치 툴을 제공하여 가시성과 분석을 보강하므로, 디지털 verification 엔지니어의 DUT 디버깅 작업에 도움이 됩니다.

- 프로토콜의 다양한 레벨에서의 가시성 (PHY, 트랜잭션, 애플리케이션 레이어)
- 실시간, 오프라인 운영 모드
- 시뮬레이션, 에뮬레이션 및 프로토타이핑 지원
- 안정적이고 강력한 분석 및 디버깅 기능 제공

Siemens의 VirtuaLAB PCI Express는 PCI Express 기반 SoC 설계를 verification하는 방식에 일대 혁명을 일으키고 있습니다. IDE 기능을 추가하여 사용자에게 PCI Express 호스트 모델과 그 엔드포인트 장치 사이에 이루어지는 보안 데이터 교환을 표준 PCI Express 환경에서 verification할 수 있는 솔루션을 제공하게 되었습니다.

verification의 구동력은 Veloce™ 에뮬레이션 및 프로토타이핑 플랫폼의 하드웨어 기반 verification을 사용하여 제공됩니다. 이러한 하드웨어 기반 플랫폼은 실리콘 칩의 *하드웨어* 모델에서 verification 제품군을 실행할 수 있는 슈퍼컴퓨터입니다. 이는 일반적인 시뮬레이션보다 수천 배는 빠르므로, 경쟁이 치열한 시장에 경쟁력 있는 설계를 내놓기 위해 필요한 시간 안에 완전한 verification을 마칠 수 있게 해줍니다.

Siemens 하드웨어 기반 verification 툴, 애플리케이션과 함께 사용하면 VirtuaLAB PCI Express 솔루션을 통해 다음과 같은 장점을 누릴 수 있습니다.

- 완전한 functional verification
- 강력한 디버깅 기능과 더불어 내부 회로에 대한 가시성 100% 확보
- 칩 및 소프트웨어 verification 툴과 완벽한 상호운용성 확보, 포스트 실리콘 하드웨어 체크아웃과도 호환됨
- 하드웨어/소프트웨어 공동 verification 및 풀칩 성능, 대역폭과 전력 메트릭 추출

따라서 새롭고 혁신적인 방식으로 PCI Express 설계를 verification할 수 있습니다. 여기에는 일반적인 PCI Express 환경에서의 보안 데이터 교환도 포함하며, 높은 수준의 성능까지 겸비하여 개발한 기술을 시장에 훨씬 효율적으로, 짧은 기간 안에 출시할 수 있습니다.

참조

1. Advanced Encryption Standard with Galois Counter Mode.

Siemens Digital Industries Software

미주 지역: 1 800 498 5351

유럽, 중동, 아프리카 지역: 00 800 70002222

아시아 태평양 지역: 001 800 03061910

다른 지역 번호는 여기를 클릭하십시오.

Siemens Digital Industries Software 소개

Siemens Digital Industries Software는 엔지니어링, 제조 및 전자 설계가 미래와 만나는 디지털 엔터프라이즈를 실현하기 위한 혁신에 박차를 가하고 있습니다. Siemens Digital Industries Software의 포괄적인 소프트웨어 및 서비스 통합 포트폴리오인 Xcelerator는 규모를 막론하고 모든 기업이 조직에 혁신을 촉진할 새로운 인사이트, 기회, 자동화 수준을 제공하는 포괄적 디지털 트윈을 생성하고 활용할 수 있도록 지원합니다. Siemens Digital Industries Software 제품과 서비스에 대한 자세한 사항은 sw.siemens.com을 방문하시거나 LinkedIn, Twitter, Facebook 및 Instagram 계정 팔로우를 통해 확인하실 수 있습니다. Siemens Digital Industries Software – Where today meets tomorrow.

siemens.com/software

84594-D4-KO 11/22 in-c