자동차 산업의 사이버보안 강화

모든 상황에서
신뢰를 확보하는 방법

Contents

자동차 산업의 사이버보안 강화

커넥티드 카 및 자율 주행의 증가는 제조업체와 소비자에게 새로운 중요한 기회를 열어줍니다. 이러한 잠재력을 실현하기 위해 제조업체는 자동차 전기전자(E/E)시스템의 사이버보안에 대해 증가하는 요구를 충족해야 합니다.

빠른 진화

자동차 산업은 급속하게 진화하고 있습니다. 혁신을 향한 포부, 최첨단 기술, 그리고 커넥티드 카에 대한 소비자의 관심이 증가하면서 공급업체, 제조업체, 승객, 그리고 사용자에게 더 많은 기회와 선택지가 생겼습니다.

연결성과 자동화

이러한 진화를 완벽하게 보여주는 것은 바로 동적 환경에서 인공 지능(AI)와 머신러닝(ML)을 사용하여 안전하게 차량을 안내하는 차량 자동화의 수준이 높아졌다는 점입니다. 또한 모바일 앱을 통해 소비자의 차량 연결성 수준이 높아지고 차량의 상태와 기능을 제어할 수 있게 되었습니다.

위협 환경의 확장

이러한 발달과 더불어 위협 환경 역시 끊임없이 변화하며 존재합니다. 이러한 위험을 미리 방지하기 위해 조직은 강력하고 엄격하며 일관된 사이버보안 전략이 필요합니다.

Rob Brown, Global Head of Automotive

“커넥티드 카 시대에서 신뢰를 구축하려면 자동차 사이버보안에 대한 라이프 사이클 접근 방식이 필요합니다. 본 가이드 문서와 파트너십을 통해 BSI는 표준 기반 규정 준수를 지원하여 고객, 파트너 및 이해관계자와의 지속적인 신뢰를 구축할 것입니다.”

규정 준수와 보안을 달성하기 위한 가이드

커넥티드 카는 안전성, 편안함, 그리고 풍부한 여행 경험을 제공합니다. 그러나 설계부터 폐기까지 차량의 전체 수명 주기에 걸쳐 사이버 위협에 취약합니다. 개인 식별 정보(PII), 결제 정보, 여행 기록 및 위치 데이터는 모두 해킹이 가능하고 오용되거나 조작될 수 있습니다. 사용자의 차량이나 시스템에 대한 액세스가 거부될 수도 있습니다.

표준으로의 보안

따라서 전체 제품 수명주기에 걸쳐 사이버보안에 대한 표준 기반 접근 방식을 채택하는 것이 중요합니다. 이를 통해 안전하고 책임감 있는 커넥티드 카 산업의 기반을 마련하고 미래를 준비할 수 있습니다.

BSI에서는 다음을 위한 권장사항을 제공합니다:

- 자동차 생태계 전반에서 디지털 위험을 적극적으로 완화하는 방법;
- 차량 수명주기 동안 신뢰성을 구축하는 방법;
- 공급망 신뢰성과 협력을 강화하는 방법;
- 글로벌 규제를 준수하겠다는 의지를 입증하는 방법

2030년까지 전 세계 판매 신차의 95%가 커넥티드 카가 될 것이며, 서비스 중인 차량 대수는 2023년 1억 9200만대에서 2027년 3억 6700만대로 증가할 것입니다.[1]

[1]Connected vehicles to surpass 367 million globally by 2027, Juniper, 2023

자동화 증가는 더 강력한 사이버보안을 필요로 합니다.

자동차기술자협회(SAE) 자동화 레벨

레벨 0(자동화 없음)에서 레벨 5(완전 자율주행)까지의 SAE Levels of Driving Automation™ 에서 자동차 사이버보안 강화의 맥락을 읽을 수 있습니다.

SAE **J3016**™ LEVELS OF DRIVING AUTOMATION™

Learn more here: sae.org/standards/content/j3016_202104

	SAE LEVEL 0™	SAE LEVEL 1™	SAE LEVEL 2™	SAE LEVEL 3™	SAE LEVEL 4™	SAE LEVEL 5™
운전석에서 사람의 역할은 무엇입니까?	운전자 보조 기능 작동으로 운전자가 페달을 밟지 않고 운전대를 조작하지 않더라도 **운전자가 주행 작업을 수행**합니다			운전자가 운전석'에 앉아 있지만, 자율주행 기능이 작동 중일 때는 **운전을 하지는 않습니다.**		
	운전자가 운전자 보조 기능을 지속하여 감시할 의무가 있으며, 안전을 유지하기 위해 필요 시 운전대 조종, 감속 또는 가속을 해야 합니다			기능이 요구할 경우 운전을 해야 함	자율주행 기능으로 운전자의 운전 수행이 요구되지 않습니다.	
	운전자 보조 기능			**자율주행 기능**		
기능의 역할은 무엇입니까?	경고 제공 및 순간적인 보조 제공으로 제한됩니다.	운전자에게 조종 **또는** 가/감속을 지원합니다.	운전자에게 조종 및 가/감속을 **모두** 지원합니다.	제한된 조건에서 자율주행 기능을 수행하며, 필요한 모든 조건이 충족되어야만 자율주행 기능이 작동됩니다.		모든 조건에서 자율주행 기능이 작동됩니다.
기능 예시	• 자동 긴급 제동 • 사각지대 경고 • 차선 이탈 경고	• 차선 중앙 유지 **또는** • 어댑티브 크루즈 컨트롤 지원	• 차선 중앙 유지 **그리고** • 어댑티브 크루즈 컨트롤 동시 지원	• 교통 체증 시 운전기사 기능	• 무인 택시 • 페달/운전대가 있을 수도, 없을 수도 있음	• 레벨 4와 동일하나, 자율주행 기능이 모든 조건에서 항상 작동

[2]SAE levels of driving automation™ refined for clarity and international audience

자동차 산업 사이버보안 계획을 위한 4가지 기본 원칙

자동차 사이버보안에 대한 종합적인 계획 수립은 파트너 및 고객에게 확신을 주고 신뢰를 구축하는데 도움이 됩니다.
이때 차량, 수명 주기, 공급망, 규제의 네 가지 주요 요소가 있으며, 이들이 서로 연결되어 있다고 생각해야 합니다.

1 커넥티드 카

차량에 대한 정교한 사이버 위협 가능성

OEM 및 공급업체는 진화하는 사이버 위협 증가에 대한 강력한 대책이 있다는 것을 입증해야 합니다. 앱, 블루투스, Wi-Fi, 텔레매틱스 (차량 정보 통신 장치) 및 온보드 진단용 포트 등 다양한 진입점은 모범 사례 표준에 따라 시스템을 보호해야 함을 의미합니다.

2 공급망

공급망 위험 완화

복잡한 공급망은 사이버보안 침해부터 자재 부족까지 다양한 위험에 노출되어 있습니다. 프로토타입부터 소프트웨어 코드까지 민감한 데이터를 공유하려면 신뢰가 필요하며, 이는 표준과 보증을 통해 구축할 수 있습니다.

3 제품 수명 주기

전 수명 주기 사이버보안 보호를 입증하세요

사이버보안 시스템은 설계, 제작, 운영부터 유지 관리 (OTA 업데이트 포함) 및 수명 종료 데이터 삭제에 이르기까지 차량과 연결된 모빌리티 자산의 전체 수명주기를 포함해야 합니다. 표준에 기반한 엄격한 계획은 완벽한 엔드 투 엔드 신뢰성을 제공합니다.

4 규제 및 표준

자동차 규제 및 표준을 선도하세요

OEM 및 공급업체는 2024년 UNECE 규정 R-155 및 R-156와 같은 규정 및 규제 준수 기한에 적응하고 있습니다. 동시에 표준 기관과 업계는 공급업체가 규정 준수를 달성하고 사이버보안 위험을 완화할 수 있도록 모범 사례를 개발하고 있습니다.

신뢰성 확보와 규정 준수를 위한 5가지 필수 도구

BSI는 자동차 산업에서 사이버보안 전문성을 보유한 글로벌 리더로서, 귀사가 규정 준수와 신뢰성을 획득하기 위한 종합적인 모범 사례 솔루션을 내재할 수 있도록 지원합니다. 교육, 심사 및 공인 인증 서비스를 통해 글로벌 규정을 준수하고, 디지털 위험 완화 및 신뢰를 구축하기 위한 귀사의 노력을 지원합니다.

다음 두 페이지는 조직에서 이해하고 모범 사례를 내재하는 데 활용할 수 있는 5가지 필수 표준 및 평가 체계입니다. 이는 귀사의 업계에 적용되는 표준의 일부입니다.

최고 경영진의 **68.5%**는
자동차 공급망 전반에서
표준의 의미와
비즈니스에 미치는
영향에 대한 이해도가
높아져야 한다고 말했습니다.[3]

[3]Automotive threat intelligence on the road to cyber safety, Kaspersky, 2023

신뢰성 확보와 규정 준수를 위한 5가지 필수 도구

1

정보보호경영시스템 (ISO/IEC 27001)

정보 보호 거버넌스를 위해 전세계적에서 확립되고 신뢰할 수 있는 표준입니다. 기초적인 정보보호 경영시스템 표준으로 AI, ML 및 자동화의 책임 있고 안전한 사용의 길을 엽니다.

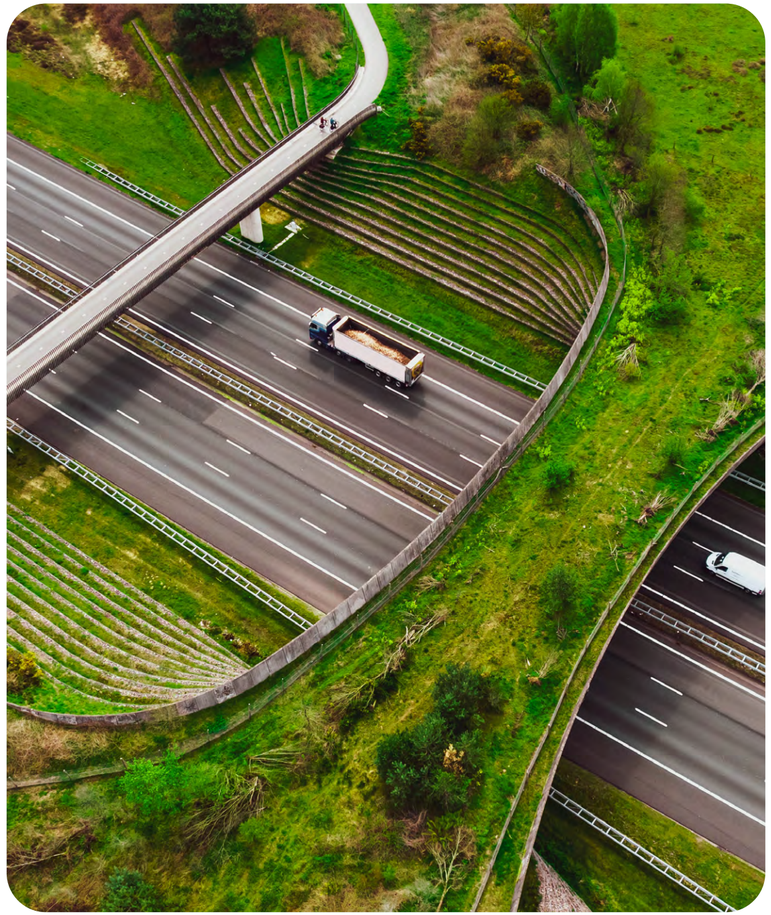
더 자세한 내용 확인하기

2

TISAX 평가

자동차 산업을 위해 자동차 산업에서 개발한 이 정보 보호 평가 체계는 ISO/IEC 27001의 요구 사항에 기반합니다. 세 가지 주요 영역에서 정보 보호를 통합하고 OEM에서 모든 계층의 공급업체까지 공급망 파트너 간의 신뢰할 수 있는 정보 교환 방식을 향상시킵니다.

더 자세한 내용 확인하기



신뢰성 확보와 규정 준수를 위한 5가지 필수 도구

3
차량 사이버보안 요구 사항 (ISO/SAE 21434)

본 표준은 모든 구성 요소와 인터페이스를 포함하여 도로 차량의 자동차 전기전자(E/E)시스템의 전체 수명주기 동안 사이버보안 위험 관리에 대한 요구사항을 명시합니다. 이 표준을 효과적으로 구현하면 UNECE 규정 R-155 (사이버보안 경영시스템 구현) 및 R-156 (소프트웨어 업데이트 경영시스템 구현)을 충족하는 데 도움이 됩니다.

더 자세한 내용 확인하기

4
ENX 차량 사이버보안 (VCS) 심사 체계

2024년 신규 도입된 이 체계는 도로 차량용 E/E 시스템을 개발, 생산 또는 유지 관리하는 자동차 공급업체를 지원합니다. ISO/SAE 21434 및 UNECE R-155의 맥락에서 사이버보안 엔지니어링 심사 지침(ISO/PAS 5112)을 구현하여 표준화된 사이버보안 경영시스템(CSMS) 심사를 제공합니다. 심사를 성공적으로 마치면 공급망 파트너 사이에 신뢰와 협력의 기반을 조성합니다.

더 자세한 내용 확인하기

5
BSI Kitemark™ 보안 디지털 애플리케이션 인증

BSI Kitemark™ 인증은 귀사가 차량에 내장되거나 원격으로 연결된 디지털 애플리케이션에 대해 엄격하고 독립적인 테스트를 거쳤음을 입증합니다. 강력한 통제력이 오픈 웹 애플리케이션 보안 프로젝트 (OWASP), 웹 애플리케이션용 보안 검증 표준 (The Application Security Verification Standard), 모바일 애플리케이션 보안 검증 표준(MASVS)을 포함한 업계 표준을 충족하여 신뢰성을 높입니다.

더 자세한 내용 확인하기

강력한 사이버보안 생태계 구축하기

다음 페이지에 나오는 BSI의 그래픽을 활용하여 귀사의 공급망 역할 및 제품 수명주기에 관련된 표준, 프레임워크, 솔루션을 탐색하세요. 본 가이드 문서에서 요약된 5가지 모범 사례, 관련 추가 표준이 나와 있으며, 디지털 신뢰를 강화하기 위한 종합적인 툴킷을 구축하도록 도와드립니다.

자동차 업계에서
문제를 인지하고 있지만
무엇을 해야 할지 파악하는 데
어려움을 겪고 있습니다.[4]

[4]Automotive threat intelligence on the road to cyber safety, Kaspersky, 2023

Automotive Cybersecurity Ecosystem

제품 수명 주기	**설계 및 구축**				**운영 및 유지 관리**			**재사용 및 재활용**	
공급망	**Tier 3** Part/ HW/SW supplier	**Tier 2** Component supplier	**Tier 1** System supplier	**OEM** Auto maker	**Developer** Embedded SW, SaaS	**Processor** Data storage & processing	**Developer** Software update	**Processor** Factory reset/ data deletion	**Recycler** Recover and reuse
제품	Chips	PCBs	SatNav, ALKS, EMS	Vehicles User apps Dealer tools	Embedded software apps	Cloud storage	Patches, versions, security updates	Data in vehicle, apps, cloud	Chips, PCBs, systems, precious materials
규제사항		<<<	UN R155	>>>	UN 156		>>>	GDPR	>>>
OEM Flow Down		<<<	ISO/IEC 27001, TISAX 및 ENX VCS에 대한 OEM 플로우다운 요구 사항						>>>
공급자 목표		<<<	규정 및 고객 요구 사항 준수 OEM 및 고객으로부터 원치 않는 점검 제거 기술 발전을 위한 견고한 플랫폼 구축 사이버 위험(멀웨어)및 무단 액세스(해킹)에 대한 대응 완화						>>>
		<<<	**Standards, training, assessment, and certification supporting:** ISO/IEC 27001 – 정보보호 경영시스템 ISO/SAE 21434 – 차량 사이버보안 경영 TISAX 평가 및 ENX VCS 감사 제도						>>>
BSI 솔루션	ISO/IEC 24089- Software Update for Vehicles BSI Kitemark™ for Secure Digital Applications				ISO/IEC 24089- Software Update for Vehicles BSI Kitemark™ for Secure Digital Applications	ISO/IEC 27017 - Infosec for Cloud Services ISO/IEC 27018 - PII in Public Clouds	ISO/IEC 24089- Software Update for Vehicles BSI Kitemark™ for Secure Digital Applications	ISO/IEC 27017 - Infosec for Cloud Services ISO/IEC 27018 - PII in Public Clouds	
이점		<<<	이해관계자 신뢰 구축: 소비자, 공급망 파트너, 규제 기관						>>>

안전한 디지털 미래를 향해

본 가이드 문서는 강력한 전체 수명주기에 대한 사이버보안 접근 방식 구축을 도와, 다음을 지원합니다:

1. 디지털 위험을 적극적으로 예측하고 완화합니다.
2. 공급망 파트너와의 협력을 강화합니다.
3. 규정 및 OEM 요구 사항 준수를 입증합니다.
4. AI, ML 및 자동화 기술의 채택을 가속화합니다.

이러한 원칙을 염두에 두면 진화하는 디지털 위험에 앞서 대응할 수 있습니다. 결과적으로 긍정적인 영향을 미치고 비즈니스 성장을 가속화하는 데 필수 원칙이 될 것입니다.

"자동차 사이버보안 시장은 **2030년까지 97억 USD에** 이를 것으로 예상됩니다.[5]"

[5]'Cybersecurity in automotive: Mastering the challenge', McKinsey & Company

Your partner in progress

BSI의 표준, 교육, 감사 및 인증 서비스에 대해
자세히 알아보려면 우리의 웹사이트를 방문하세요.