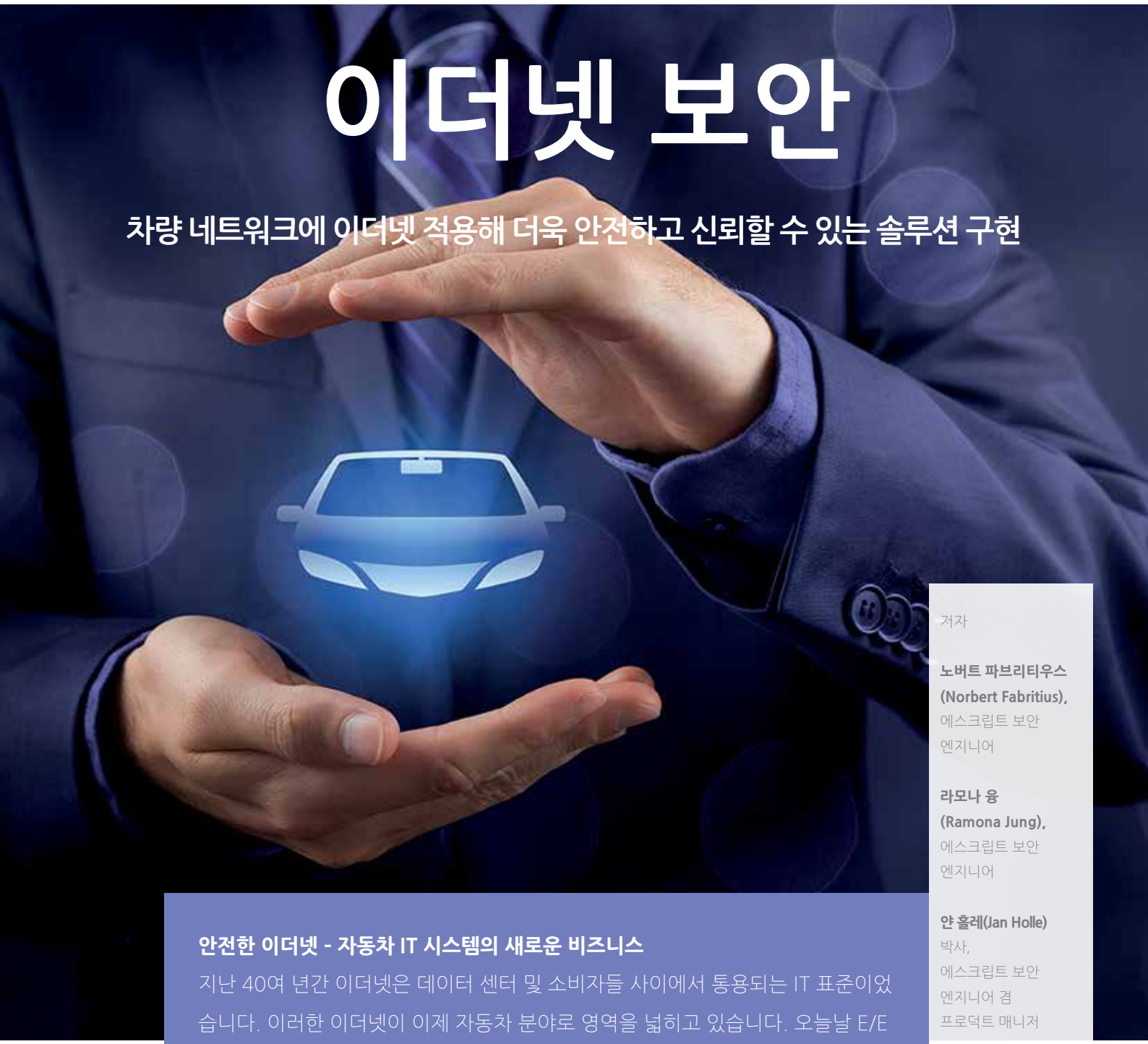
이더넷 보안

차량 네트워크에 이더넷 적용해 더욱 안전하고 신뢰할 수 있는 솔루션 구현



저자

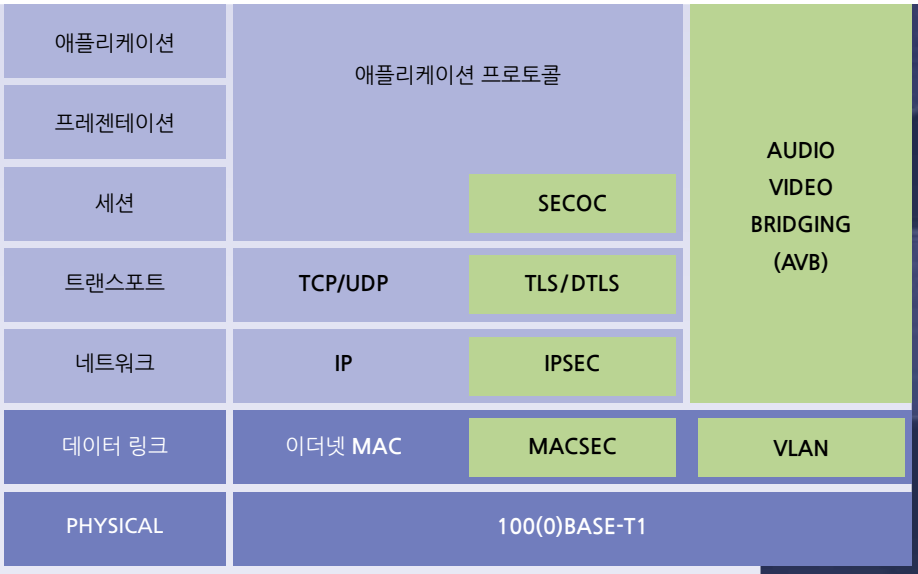
노버트 파브리티우스 (Norbert Fabritius), 에스크립트 보안 엔지니어

라모나 융 (Ramona Jung), 에스크립트 보안 엔지니어

얀 홀레(Jan Holle) 박사, 에스크립트 보안 엔지니어 겸 프로덕트 매니저

안전한 이더넷 - 자동차 IT 시스템의 새로운 비즈니스

지난 40여 년간 이더넷은 데이터 센터 및 소비자들 사이에서 통용되는 IT 표준이었습니다. 이러한 이더넷이 이제 자동차 분야로 영역을 넓히고 있습니다. 오늘날 E/E 아키텍처는 도메인 간 통신이 불가능했던 초기 어플리케이션과 달리 도메인 경계를 넘어 확장되고 있습니다. 이는 보안과 안전, 신뢰할 수 있는 실시간 대응이 필요하다는 것을 의미하며, 이에 대응할 수 있는 효과적인 이더넷 솔루션이 필요합니다.



안전 관련 포로토콜
(연두색 표시)

자동차의 데이터 전송 속도가 급증하면서 CAN과 FlexRay와 같은 전통적인 버스 시스템의 대안으로 이더넷이 도입됐습니다. 인포테인먼트 부문에서 시작된 기술이 이제 차량 도메인 시스템 간 통신에 이용되고 있는 것입니다.

데이터 버스가 안전하면서도 독립적으로 원활한 통신을 하기 위해서는 강력하고 정교한 솔루션이 필요합니다. 이 솔루션은 이더넷 구성요소 간 통신은 물론, 일반 버스와의 원활한 데이터 통신도 지원해야 합니다. 필요 시 이더넷 표준을 차량의 특정 요구사항에 적용시키는 것 역시 매우 중요합니다. 기존 IT 솔루션을 수정해 사용할 수도 있지만, 새로운 개발이 필요한 경우도 있습니다. 이에 대한 결정은 비디오 신호와 같은 대용량 데이터를 처리할 때에도 최대한의 보안, 안전성, 신뢰할 수 있는 응답 시간을 보장하는 방법에 따라 달라질 수 있습니다.

전통적인 IT 시스템의 문제점과 솔루션

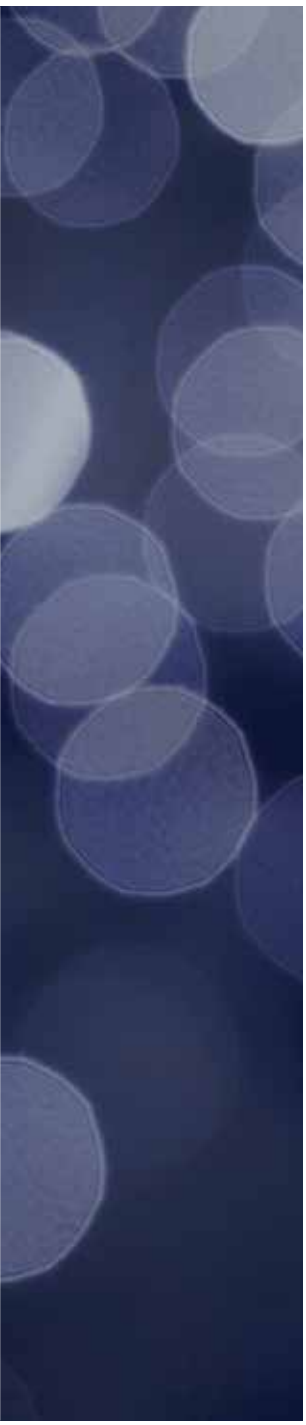
이더넷의 구조는 분산되어 있기 때문에 사전에 설계된 이중화 및 동적 네트워크 경로를 통해 중앙 제어 없이 운영됩니다. 그러나 이 분산 구조는 그 자체로 의심의 여지가 있습니다. 이더넷 네트워크의 모든 구성원이 동등한 권한을 가지고 있다면, 허가되지 않은 네트워크 액세스를 시도할 때 어떻게 탐지하고 막을 수 있을까요? 네트워크 조작을 식별하고 방지하는 방법은 무엇일까요?

먼저 네트워크 트래픽 분할을 위한 가상 네트워크 (VLAN)와 같은 솔루션이 있습니다. 원래 네트워크 포트는 여러 VLAN에 할당되어 있습니다. 이제는 이더넷 프레임과 독립된 포트의 VLAN을 표시(태그)할 수도 있습니다. 이 태깅은 IEEE 802.1Q 표준으로 규정되어 있습니다. 하지만 네트워크 트래픽의 논리적 분리만으로 원치 않는 디바이스의 침입을 막을 수는 없습니다. 조작 및 스파잉으로부터 트래픽을 조건적으로만 차단합니다. 따라서 완전한 보안을 위해서는 암호화 인증 또는 암호화 과정이 필요합니다. 이 문제에 대한 전통적인 IT 솔루션도 존재합니다. 초기 솔루션은 TLS (Transport Layer Security)와 같은 데이터 형식 및 표준을 사용하는 상위 프로토콜 계층에 중점을 뒀습니다. 이에 비해 최신 솔루션은 더 깊은 계층에 대한 추가 보안 메커니즘을 제공합니다. 여기에는 IPSec을 사용하는 IP 패킷 (Layer 3)과 MACsec (IEEE 802.1AE)을 사용하여 이더넷 프레임 (Layer 2)을 암호화하는 작업이 포함됩니다. 이러한 솔루션은 산업 표준에 따라 규제됩니다.

또한 보안 구성요소들이 있습니다. 필터 규칙을 통해 기존 방화벽이 패킷을 다른 네트워크나 엔드포인트 간 전달할지 여부를 통제할 수 있습니다. 최근 방화벽 솔루션은 딥 패킷 검사를 통해 패킷의 페이로드까지 트래픽을 분석하고 평가할 수 있습니다. 침입 탐지 시스템 (IDS, Intrusion Detection Systems) 및 침입 방지 시스템 (IPS, Intrusion Prevention Systems)은 이러한 토대를 기반으로 하여 관리자가 관리에 용이하도록 지원합니다.

최신 차량 네트워크의 보안 요구사항

최신 차량 네트워크 아키텍처는 일반적으로 IT에 사용되는 네트워크 아키텍처와 유사점이 많습니다. 그러나



기술적 기준과 보호 대상에는 큰 차이가 있습니다. 차량은 승객과 재산의 안전을 최우선으로 하기 때문에 일반적인 네트워크 아키텍처에 비해 시스템 가용성과 네트워크 트래픽의 진위 판단이 매우 중요합니다. 또한 네트워크 구성요소들이 지연 없이 결정론적 방식으로 작동되어 차량 작동 관련 실시간 중요 요구사항들이 수행돼야 합니다.

이러한 요구사항은 데이터 패킷의 전송 시간을 보장할 필요가 없는 패킷 기반의 전송 매체인 이더넷 특성과 명백히 모순됩니다. 또한 차량 ECU의 컴퓨팅 능력이 제한되어 있기 때문에 보안과 실시간 요구사항을 충족시키기 어렵습니다.

따라서 이더넷을 차량 네트워크에 적용하기 위해서는 VLAN을 사용해 fail-safe 속성을 향상시키는 것과 같은 수정이 필요합니다. 이를 위해 네트워크는 서로 다른 보호 요구사항을 가진 가상영역들로 나뉘며, 이를 통해 안전 관련 구성요소들의 네트워크 트래픽을 실시간으로 확인할 수 있습니다. 필요한 경우 우선 순위를 정하거나 차단할 수도 있습니다. DoS (Denial-of-Service) 공격 또는 문제가 있는 컴포넌트가 패킷으로 네트워크로 과다하게 보내면, 우선 순위가 지정된 VLAN의 통신을 먼저 제공하기 위해 속도를 제한하는 방법으로 다음 스위치에서 트래픽을 차단할 수 있습니다.

방화벽이나 보다 강력한 IDS/IPS 시스템을 사용하면 서로 다른 보안 요구사항을 가진 인접 IP 네트워크들을 더 엄격하게 분리하고 정확하게 모니터링할 수 있습니다. 반면, 기존 차량 버스 시스템은 추가적으로 물리적 버스가 설치되어 있지 않으면 논리적으로 분리될 수 없습니다.

기존 보안 솔루션과 새로운 보안 솔루션

과거 TLS IT 보안 프로토콜에서는 사용하는 데 제약사항이 있었습니다. TLS는 차량의 실시간 요구사항과 상충될 수 있기 때문에 백엔드 시스템 또는 테스트 장치와의 시간에 영향을 받지 않는 (time-uncritical) 통신을 위해서만 사용될 수 있었습니다. 하지만 TLS 1.3의 사양은 연결 기능에 최적화되어 있기 때문에 (zero-RTT handshakes), TLS 보안 데이터를 핸드셰이크 중 첫 번째 패킷에 적용할 수 있습니다. 더 이상 TLS를 사용할 때 추가 왕복 시간 (RTTs)이 필요하지 않습니다. 사전 공유 키 (TLS-PSK)를 사용하면 비대칭 프로세스가 더 이상 필요하지 않기 때문에 TLS의 오버 헤드 비용도 크게 줄일 수 있습니다. 그러나 현재는 TLS 보안에 대한 약점 발생가능성을 평가하는 데 중점을 두고 있습니다.

차량의 실시간 요구사항은 비대칭 프로세스를 기반으로 하는 암호화 서명 과정에서 문제가 될 수 있습니다. 데이터 패킷의 신뢰성을 보호하기 위해 SecOC (Secure On-Board Communication) 모듈 사양이 2014 년에 AUTOSAR 4.2의 일부로 발표됐습니다. SecOC의 표준은 이더넷/IP 기반 트래픽에도 적합하도록 유연하게 설정되어 있습니다.

Time-critical 비디오 데이터 전송을 위해 개발된 Audio Video Bridging (AVB)를 포함해 Time-Sensitive Networking (TSN) 표준도 동일합니다. 이더넷을 통해 실행되며, 네트워크 리소스의 예약, 시간 신호 동기화 및 데이터 스트림의 우선 순위를 결정하는 자체 메커니즘을 정의합니다. 또한 AVB는 기존 버스 데이터 전송을 허용합니다. 이를 통해 이더넷 환경 내에서 실시간 환경의 요구사항을 고려할 수 있습니다. 최신 버전의 AVB 전송 프로토콜 (2016년 말 출시)은 필요 시 하드웨어 성능 요구사항이 상대적으로 낮은 환경에서도 전송된 페이로드 데이터의 암호화를 지원할 수 있습니다.

차량 이더넷 통신 보안 - 개발 및 통합

차량 네트워크에 이더넷 기반 솔루션이 본격적으로 통합되고 있습니다. 이는 차량의 미래지향적 기능들을 구현할 수 있게 해줍니다. 동시에 개발은 차량의 최신 보안 요구사항을 고려하여 이루어집니다. 보안 전문가가 제공하는 맞춤형 솔루션을 포함한 심층적 지원을 통해 복잡한 이더넷 아키텍처를 완벽히 구현할 수 있습니다.

이를 위해 에스크립트는 이더넷 보안 및 자동차 분야에서 오랜 기간 경험을 쌓아왔습니다. 이러한 노하우를 바탕으로 실질적인 보안 컨셉 개발과 분석에서부터 자동차 산업의 요구에 정확히 부합하는 맞춤형 소프트웨어 및 하드웨어 솔루션 구현까지 이더넷 통합의 모든 단계에서 고객을 지원합니다. 지난 40여 년간 사용되던 이더넷과 달리 이더넷의 새로운 미래는 지능형 보안 솔루션 및 제품과 함께 이어질 것이며, 특히 자동차 산업에서 두드러진 역할을 해나갈 것입니다.