자동차 키(Key) 기술

원격 키리스 엔트리는 한동안 저가형 승용차의 표준 기능이었습니다. 새로운 모델에는 자동차를 시동 할 수 있는 근접성이 충분한 잠금 시스템이 점점 더 많이 장착되어 열쇠가 운전자의 주머니에 남아있게 됩니다. 이러한 무선 시스템의 기술도 변화하고 있습니다. 초광대역 (UWB) 기술의 사용이 증가하고 있습니다. 제조업체가 어떤 기술을 사용하든 새로운 테스트 시스템이 이를 모두 처리 할 수 있습니다

자동차는 더 이상 차체, 내부, 섀시, 엔진 및 변속기로 구성된 기술적으로 단순한 운송 수단이 아닙니다. 그 시절은 오랫동안 지났습니다. 전기 이동성이 추진력에 혁명을 일으키고 있다는 사실 외에도, 편안함과 안전을 제공하는 전기 및 전자 부품은 이미 자동차의 구석 구석에 있습니다. 자율 주행에 대한 업계의 비전이 현실이 되려면 차량이 자체 경계를 넘어서서“보는”방법을 배워야 합니다. 이 고성능 센서 기술 및 다른 교통 참여자 또는 인프라 여부를 자동차의 환경과 일정한 무선 접촉을 통해 수행됩니다. 이를 통해 자동차는 항상 다음 곡선 또는 다음 교차로에 있는 것을 알고 사전에 대응할 수 있습니다. 결과적으로 도로 안전이 크게 향상 될 것입니다.

그러나 이 시나리오의 과제는 데이터 보안입니다. 무선 네트워크 자동차는 해커에게 잠재적인 게이트웨이를 제공합니다. 2015년의 유명한 “지프 핵 (Jeep hack)”과 같은 데모 핵은 이 위험이 공중에서 쫓겨 난 것이 아니라는 것을 증명했습니다. 지프 체로키에 충분히 확보 모바일 무선 액세스 스티어링 제동 같은 기본 기능으로 차량 외부 간섭을 허용했습니다. Wi-Fi 및 Bluetooth®와 같은 단거리 무선 서비스는 다른 공격 경로를 열어줍니다. 여기에는 일반적으로 활성화 된 인포테인먼트 시스템을 갖춘 "경고"자동차가 필요하지만, 점화가 꺼지면 다른 무선 인터페이스가 해결되기를 기다리고 있습니다. 흥미롭게도, 대량 생산 차량의 첫 번째 RKE는 고급 모델이 아니라 1982년 르노푸에고 였습니다. 그러나 이 기술이 다른 제조업체의 차량으로 발전한 것은 1990 년대 초반이었습니다. 첫 번째 RKE 모델에서 5~10 미터 범위의 단거리 무선 송신기는 암호화되지 않은 열기 또는 닫기 명령을 자동차 수신기 (보통 북미 315, 유럽 및 아시아 433.92)로 보냈습니다. 신호 수신은 표시등을 통해 시각적으로 또는 경적을 통해 음향 적으로 확인되었습니다.

자동차 도둑은 재머로 폐쇄 명령을 차단하여 자동차가 열린 상태를 유지하거나 제어 신호를 기록하고 차량 소유자가 떠난 후에 다시 보냅니다. 당연히 이 취약점은 오랫동안 숨겨져 있지 않아 시스템이 암호화 방식으로 향상되었습니다. 그러나 최첨단 시스템조차도 침입에 영향을 받지 않습니다. 하는 PEP 시스템은 이미 자동차 원격 키 사이에 두 개의 트랜시버로 구성된 무선 브리지를 설정하여 금이 되었습니다; 이것은 열쇠가 근처에 있다고 생각하여 차를 두들 겼습니다 (릴레이 공격). 다른 경우에는 암호화가 불충분하거나 제대로 구현되지 않은 것으로 판명되었습니다. 그러나 재래식 RKE를 괴롭히는 것은 범죄 행위 만이 아닙니다. 때때로 실패의 원인을 설명하기가 쉽지 않습니다. 북미 지역에서는 쇼핑 센터의 결함이 있는 RFID 시스템이 주변에 신호를 보내 주차 된 차량의 RKE를 차단 한 사례가있었습니다. 이 불행은 단 5분 안에 사라지지 않았을 것입니다.

그림 1 : 일반적인 테스트 시스템
구성 맞춤형 변형이 가능합니다.

UWB는 몇 가지 문제를 해결합니다.

최근까지 RKE 및 PEPS 시스템에는 무선 기술이 혼합되어 사용되었습니다. 구성 요소를 깨우기 위한 신호 신호로 LF (예 : 125 kHz), 암호화 된 통신을 위한 UHF (예 : 433 MHz) 및 차량의 자기 나침반 시스템 키가 내부 또는 외부에 있는지 테스트하기 위한 내부 (예 : 21 kHz). 이러한 시스템은 취약한 것으로 판명 되었기 때문에 다양한 대역이 예약 된 3.1GHz ~ 10.6GHz 범위의 UWB 주파수 범위에서 단일 무선 표준을 갖춘 솔루션이 추세입니다.

UWB는 500 MHz 이상의 넓은 대역폭을 사용하는 매우 짧은 펄스 저에너지 신호의 일반적인 명칭입니다. 대역폭이 넓으면 신호가 짧아지기 때문에 시간과 대역폭 간의 상호 관계가 이 기술을 선택하는 주된 이유입니다. 이것은 여러 가지 이유로 바람직하다. 우선, 나노 초 범위의 펄스 지속 시간 동안, 원래 신호에 반사가 중첩되지 않아서 신호가 모호하지 않습니다. 둘째, 펄스 전파 시간 및 송신기 거리가 정확하게 결정될 수 있어서, 키의 위치 결정을 위한 시간 소모적 인 자기장 측정이 더 이상 필요하지 않다. UWB 무선 기술은 노이즈 플로어 보다 약간 높은 매우 낮은 전송 전력으로 작동하므로 배터리 수명을 연장하고 다른 무선 전송의 방해를 방지하며 범위를 제한하여 해커가 신호를 가로 채기가 더 어렵습니다.

UWB의 장점으로 알 수 있듯이 구체적인 구현에 대한 규제 기관의 사양은 엄격합니다. 예를 들어, FCC는 스펙트럼과의 간섭을 최소화하기 위해 스펙트럼 전력 밀도를 대역폭의 MHz 당 –43 dBm으로 제한합니다 (비교 : 모바일 장치는 MHz 당 최대 +30 dBm으로 전송) . 결과적으로 –45 dBm 보다 훨씬 낮은 레벨에서 약 1 far 폭의 신호를 안정적으로 평가하는 T & M 장비가 필요합니다.

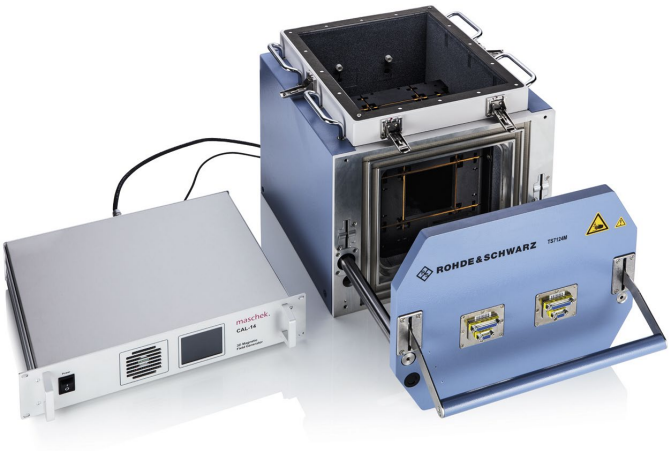

그림 3 : 자기장 센서 용 테스트 설정이 있는 R&S® TS7124 쉴드박스

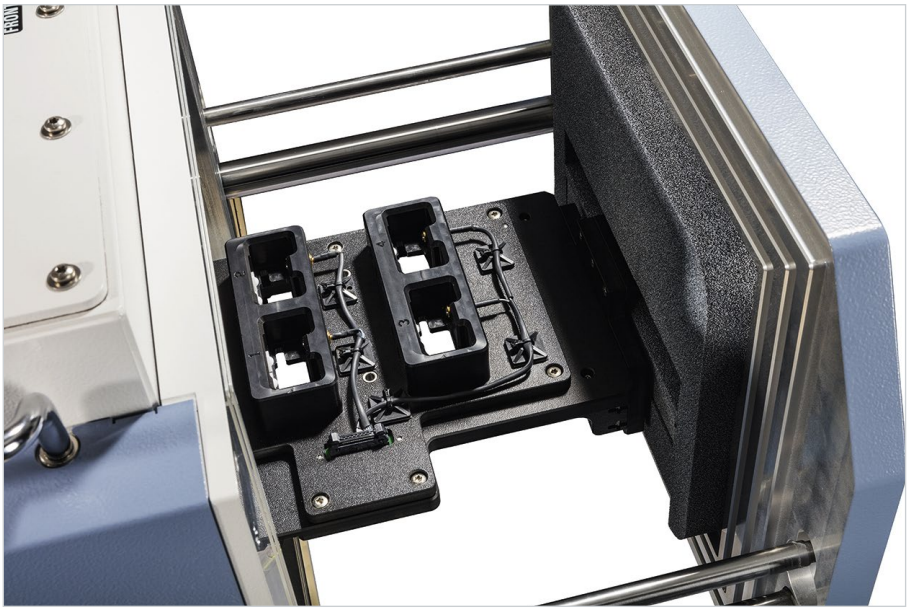

그림 2 : 4 개의 DUT에 대한 테스트 픽스처. 최대 8 개의 DUT를 위한 고정 장치를 사용할 수 있습니다.

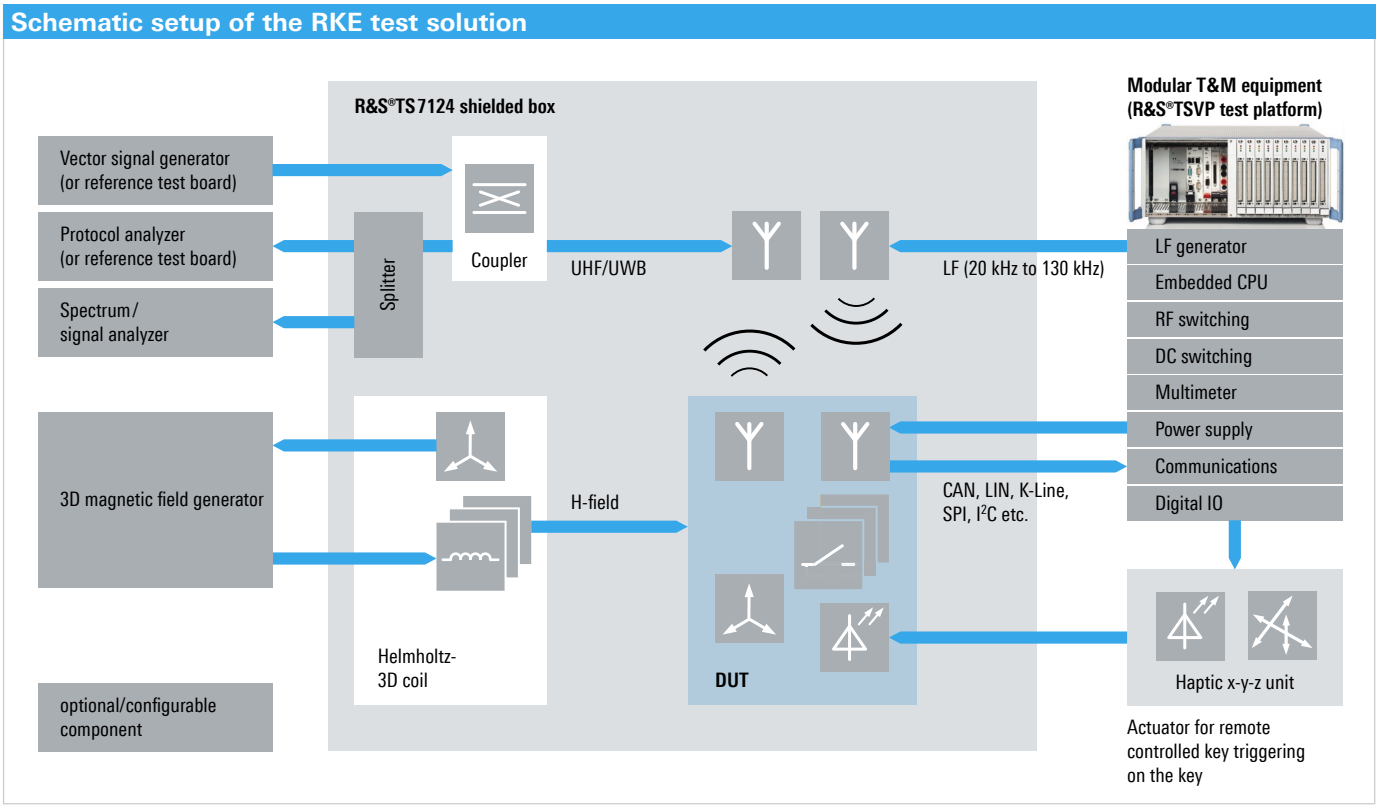

그림4 : 다른 옵션으로 시스템 설정

모든 일반적인 기술을 위한 하나의 솔루션

UWB가 미래의 RKE 및 PEPS 시스템을 위한 유행 기술이더라도 혼합 무선 솔루션을 갖춘 시장에는 여전히 많은 차량 모델이 있습니다. 즉, 구성 요소 테스트 시스템에는 사용 된 모든 기술을 지원할 수 있는 유연성이 있어야 합니다. 로데슈바르즈는 이러한 솔루션을 개발했습니다 (그림 1).

R&S® TS7124 차폐 상자는 응용 분야별 테스트 픽스처 (그림 2) 및 안테나 시스템, 예를 들어 자기장 센서 (Helmholtz 코일, 그림 3)에 대한 테스트 설정을 장착 할 수 있는 테스트 환경으로 작동합니다. 이 상자는 개발 실험실과 생산 현장의 요구 사항을 충족하기 위해 수동 또는 공압식 개구부와 함께 제공됩니다.

생산 최적화 R & S® FPS와 같은 스펙트럼 분석기는 주파수 및 시간 영역에서 전송 신호를 분석합니다. 여기서, 점유 대역폭과 채널 및 인접 채널 전력이 중요하다. 프로그래밍 가능한 신호 지연을 통해 두 UWB DUT 간의 거리 측정을 실현할 수 있습니다.

시스템의 기술 "마음"은 R&S® TSVP PXI 기반 테스트 플랫폼으로, 제어 컴퓨터, 전원 공급 장치 및 인터페이스 (LIN, CAN, I2C, SPI) 및 테스트 모듈 (발전기, 분석기, 멀티 미터, 스위칭)을 수용합니다. 행렬 등). 일반적으로 다양한 작동 모드에서 DUT 전류 드레인은 전송 버스트와 동시에 분석됩니다.

원격 키가 없는 항목이거나 테스트중인 관련 온 보드 장치입니다. DUT의 각 원격 스테이션은 선택적으로 참조 테스트 보드 ("골든 장치")로 테스트 설정에 통합되거나 프로토콜 분석기 및 벡터 신호 생성기와 같은 테스트 장비를 사용하여 시뮬레이션 될 수 있습니다. 강력하고 조작하기 쉬운 테스트 시퀀서인 R&S Quickstep은 테스트 프로그램의 설계 및 워크 플로우 제어를 처리합니다. 이 시스템은 R&S® TSVP PXI 시스템이 장착 된 차폐 상자에서 전용 T&M 기기가 있는 대형랙 솔루션에 이르기까지 고객 요구 사항에 맞게 유연하게 구성 할 수 있습니다 (그림 4).

Rob Short; Volker Bach