Key technology

Remote keyless entry has been a standard feature in even lower-end passenger cars for a while. New models are increasingly equipped with locking systems where proximity is sufficient to enable the car to be started, allowing the key to remain in the driver's pocket. The technology for these wireless systems is also changing. The use of ultrawideband (UWB) technology is on the rise. No matter what technology a manufacturer uses, a new test system can handle them all.

Cars are no longer a technically simple means of transportation consisting of a body, interior, chassis, engine and transmission; those days are long gone. Aside from the fact that electromobility is revolutionizing propulsion, electrical and electronic components that provide comfort and safety already find themselves in every nook and cranny of our cars. For the industry's vision of autonomous driving to become a reality, vehicles must reach beyond their own boundaries and learn how to "see". This will be accomplished through highly-developed sensor technology and constant wireless contact with the car's surroundings, whether with other traffic participants or the infrastructure. This will allow the car to always know what is beyond the next curve or at the next intersection and respond proactively. The result will be a significant increase in road safety.

A challenge with this scenario, however, is data security. The wirelessly networked car offers a potential gateway for hackers. Demo hacks such as the famous "Jeep hack" of 2015 have proven that this danger is not just something plucked out of the air. An insufficiently secured mobile wireless access in a Jeep Grand Cherokee allowed external intervention into elementary vehicle functions such as steering and braking. Short-range wireless services such as Wi-Fi and Bluetooth® open up other paths for attack. While these generally require an "alert" car with an activated infotainment system, another wireless interface is idly waiting to be addressed when the ignition is switched off: the keyless entry system, which is either realized as a remote keyless entry (RKE) solution where the driver triggers a wireless command on the key or, increasingly, as a passive entry/passive start (PEPS) system where it suffices to have the key in your pocket.

Interestingly, the first RKE in a mass-produced vehicle was not in a high-end model, but rather in the 1982 Renault Fuego. But it was only in the early 1990s that this technology made its way into other manufacturers' vehicles. In the first RKE models, a short-range wireless transmitter with a range of five to ten meters sent an unencrypted open or close command to the car's receiver – in North America normally at 315 MHz, in Europe and Asia at 433.92 MHz. The signal reception was acknowledged visually via the indicator lights or acoustically via the horn.

Car thieves could either block a close command with a jammer so that the car remained open or record the control signals and send them again once the vehicle's owner had left. Naturally, this weak point did not remain concealed for long, resulting in the systems being cryptographically enhanced. But even state-of-the-art systems are not immune

Fig. 1: Typical test system configuration. Customized variants are possible.

to break-ins. PEPS systems have already been cracked by setting up a wireless bridge consisting of two transceivers between the car and the remote key; this duped the car into thinking that the key was nearby (relay attack). In other cases, the encryption proved to be insufficient or poorly implemented.

However, it is not just criminal activities that can put conventional RKEs in distress. Sometimes the cause of a failure is not easy to explain. There was a case in North America where a shopping center's flawed RFID system sent a signal into its surroundings that blocked the RKEs of parked vehicles. This misery was likely not eliminated in just five minutes …

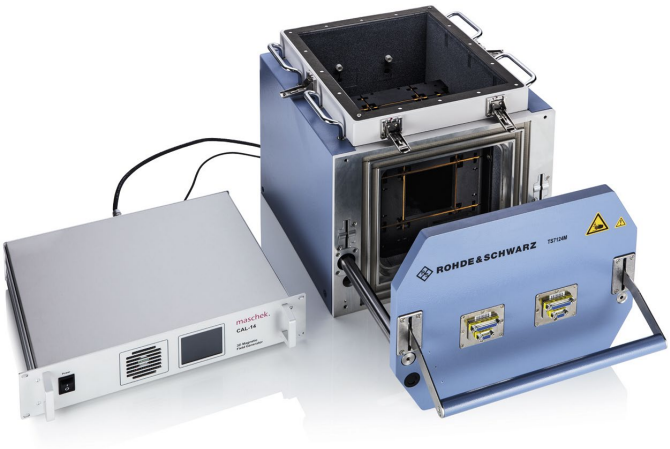

Fig. 3: R&S®TS7124 shielded box with test setup for magnetic field sensors.

UWB solves several problems

Until recently, a mix of wireless technologies was used for RKE and PEPS systems: LF (e.g. 125 kHz) as a beacon signal to wake up the components, UHF (e.g. 433 MHz) for encrypted communications, and a magnetic compass system in the vehicle interior (e.g. 21 kHz) for testing whether the key is inside or outside. Since these systems have proven vulnerable, the trend is toward a solution with a single wireless standard in the UWB frequency range from 3.1 GHz to 10.6 GHz in which various bands have been reserved.

UWB is a general designation for very short, pulsed low-energy signals that use a wide bandwidth of more than 500 MHz. The reciprocal relationship between time and bandwidth is the main reason for selecting this technology, since a wide bandwidth results in short-duration signals. This, in turn, is desirable for several reasons. First of all, for pulse durations in the nanosecond range no reflections are superimposed on the original signal, which guarantees that the signal is unambiguous. Secondly, pulse propagation time and the transmitter distance can be accurately determined, so that the time-consuming magnetic field measurement for the positioning of the key is no longer required. The fact that UWB wireless technology operates with very low transmission power – slightly above the noise floor – extends battery life, prevents jamming of other wireless transmissions and limits the range, which makes it more difficult for hackers to intercept the signal.

As pronounced as the advantages of UWB are, the regulators' specifications with respect to the concrete implementation are just as strict. In order to ensure that there is as little

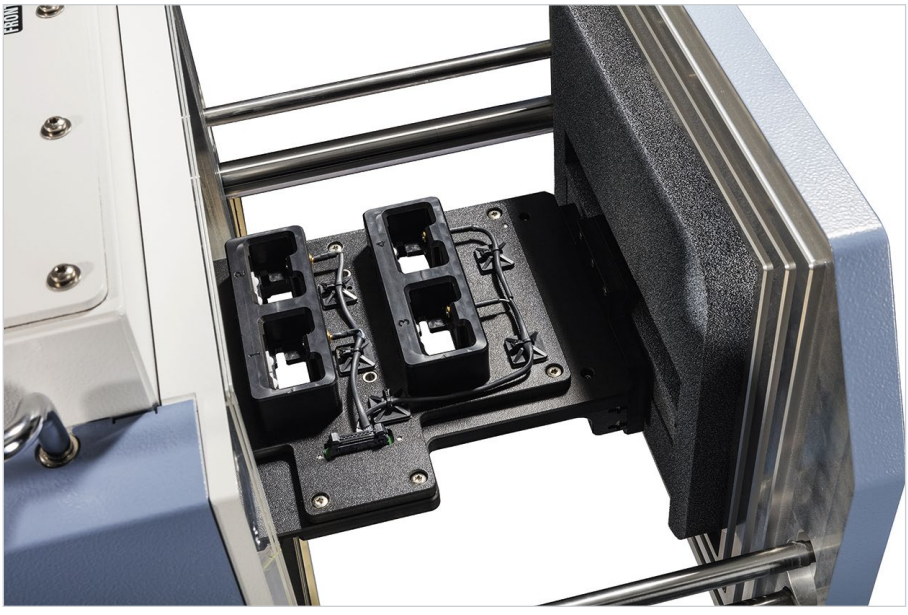

Fig. 2: Test fixture for four DUTs. Fixtures for up to eight DUTs are available.

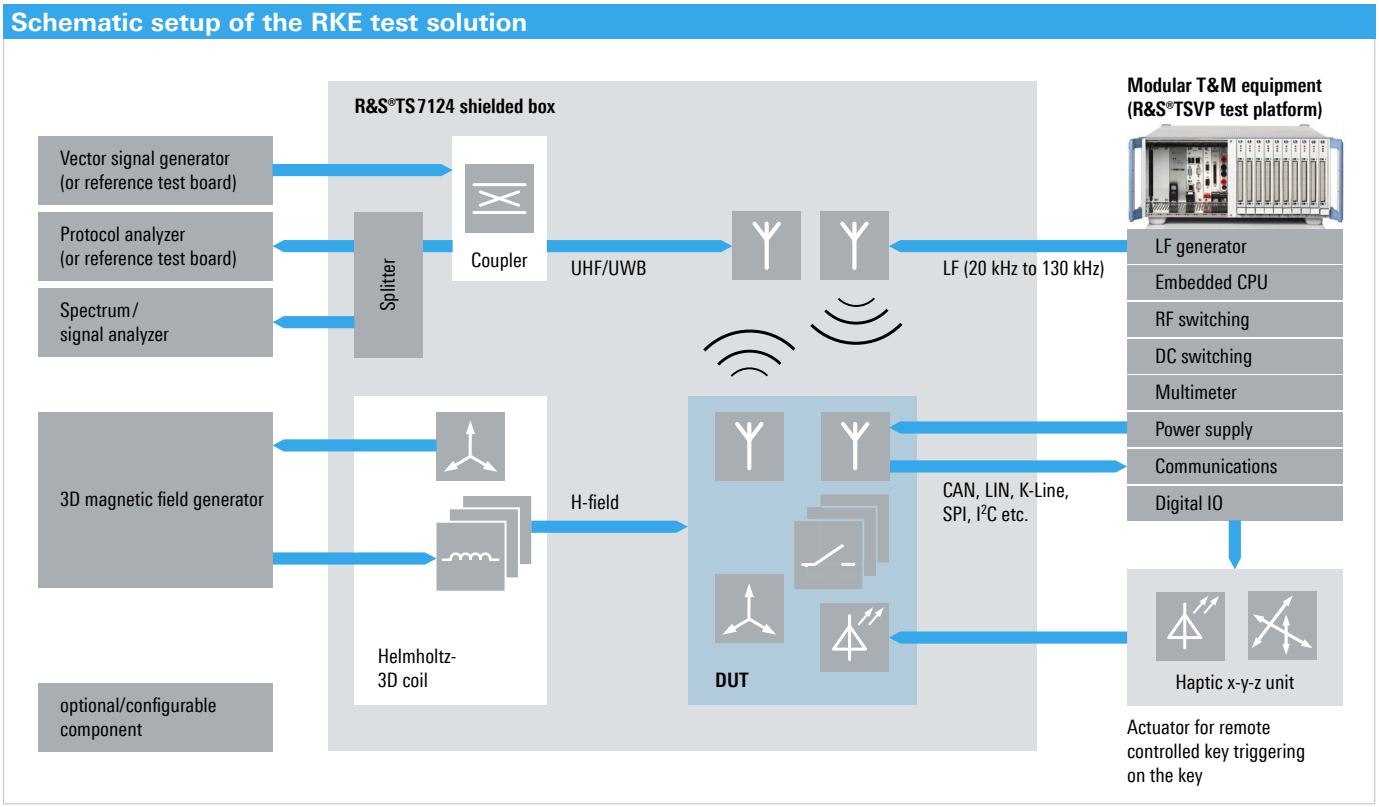

Fig. 4: System setup with different options.

interference with the spectrum as possible, for example, the FCC limits the spectral power density to –43 dBm per MHz of bandwidth (by comparison: mobile devices transmit with up to +30 dBm per MHz). As a result, T&M equipment is required that reliably evaluates a signal that is approximately 1 GHz wide with levels far below –45 dBm.

One solution for all common technologies

Even if UWB is the fashionable technology for future RKE and PEPS systems, there are still many vehicle models on the market with mixed wireless solutions. This means that a component test system should have the flexibility to support all of the technologies used. Rohde&Schwarz has developed such a solution (Fig. 1).

The R&S®TS7124 shielded box functions as a test environment that can be fitted with application-specific test fixtures (Fig. 2) and antenna systems, for example also with a test setup for magnetic field sensors (Helmholtz coil, Fig. 3). The box is available with a manual or pneumatic opening in order to fulfill requirements in the development lab as well as in production.

Spectrum analyzers, for example the production-optimized R&S®FPS, analyze the transmit signal in the frequency and time domain. Here, the occupied bandwidth and the channel and adjacent channel power are of interest. Distance measurements between two UWB DUTs can be realized via programmable signal delays.

The technological "heart" of the system is the R&S®TSVP PXI-based test platform, which accommodates the control computer, power supply as well as the interface (LIN, CAN, I²C, SPI) and test modules (generators, analyzers, multimeters, switching matrices, etc.). Typically, the DUT current drain in the various operating modes is analyzed at the same time as the transmission bursts.

It is either the remote keyless entry or the associated on-board units that are being tested. The respective remote station for the DUT can optionally be integrated into the test setup as a reference test board ("golden device") or simulated using test instruments such as a protocol analyzer and vector signal generator. R&S®Quickstep, the powerful and easy-to-operate test sequencer, handles the design and the workflow control of the test program.

The system can be flexibly configured to customer requirements (Fig. 4) – from an equipped shielded box with the R&S®TSVP PXI system to a big rack solution with dedicated T&M instruments.

Rob Short; Volker Bach