

# Stealing Cars Will Get Tougher

Texas Instruments' new vehicle immobilizers will make it more difficult for owners to conspire to cheat insurance companies.

July 3, 2002 -- Some people think that RFID will one day eliminate, or at least drastically reduce, theft. That day may not be far off ? at least as far as automobiles are concerned.

Texas Instruments has introduced a new version of its RFID vehicle immobilizer, which aims to stop not just theft but also fraud.

Insurers in Europe are finding that fraud is becoming a problem precisely because of the success of vehicle immobilizers, which were introduced in 1993 in response to the rapid rise in auto theft that followed the opening of Eastern Europe.

A study by Allianz AG, one of the world's largest insurers, revealed that between 1993 and 2000, vehicle theft in Europe dropped by 50 percent, largely because of the use of immobilizers. The first units required a unique serial number stored in an RFID tag in the key to match the number stored in a reader in the steering column. If the key didn't match, the car wouldn't start.

The current technology, which was introduced in 1997, uses an electronic signature for additional safety. The unit in the steering column generates a random number, which is transmitted to the key. The key combines the random number with its own unique serial number. The new number is encrypted and sent back to the unit in the steering column. If the numbers don't match, the car doesn't start.

Allianz and other insurers in Europe found that some criminals had figured out a way around the system -- use the key. Instead of hot-wiring cars, the criminals were conspiring with owners. The criminal pays the owner for a copy of the key and takes the car away, perhaps reselling the parts in Eastern Europe. The owner tells the insurance company that the car was stolen and gets reimbursed.

When the insurer asks to see the keys, the owner turns over the original keys and any copies, but doesn't tell the insurer that there was an extra copy, which was given to the co-conspirator.

To prevent this kind of fraud, Texas Instruments worked out an enhancement to its immobilizers, which it calls Digital Signature Transponder Plus, or DST+. The system allows data to be stored on individual keys and in the car, so that both the vehicle and the car know how many new keys have been made and even when they are used.

Here's how it works. A customer buys a new car and is given two keys. He wants to make two copies. Depending on the car manufacturer, he may have to go to the dealer, or he may be able to get them from a qualified locksmith. Each key has a unique serial number.

When the new key is used in the car, the unit in the steering column records the existence of a new key. The next time the original keys are used, the steering column unit writes data to the keys, so all keys have

information on the existence of all other keys. The system can also store date stamps, so the insurer can check when each key was last used.

The system doesn't stop conspirators from making a copy and using it to get rid of the car before the existence of a new key can be recorded on the existing keys. But the unit in the car will know a new key has been used, so if the car is recovered, the insurer will uncover the fraud.

DST+ will be available on some 2004 models. "We feel we are first to market with this enhancement," says Tony Sabetti, global business unit manager for Texas Instruments RFID Systems. "The technology is backward compatible, so car companies that have used our first and second generation systems will find this to be an easy upgrade."

Texas Instruments has also developed the 3D Analog Front-End RF chip, which automakers can use to allow passive entry. A reader in the car senses the presence of a transponder in a key fob or other form factor and automatically unlocks the doors. The car can even be programmed to start the engine and adjust the seats to a specific driver automatically. The feature will be installed on some 2003 vehicles.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved