What use is the best security technology if hackers intercept the radio signal from the remote control and switch the control unit out of operation? The industry is trying to protect itself with radio signals with "*rolling code*" or "*hopping code*". After each signal transmission, a new code is agreed between the central station and the transmitter.

However, this is not certain and the so-called "*replay attacks*" are increasing. How do you then explain to your insurance company that a burglary occurred even though a burglar alarm system was installed and armed?

Modern developments use digital radio technologies that also meet the highest security requirements. AlarmTab® takes a pioneering position with a complete digitalization of the system and a 4-fold encryption of the radio communication.

These four steps are:

1) AES-128-BIT encryption of all radio signals (AES encryption is still classified as cryptically secure today and serves as secure technology for radio signal transmission in most security-relevant areas).

2) Use of a unique, distinctive MAC address in each sender, this address was previously stored as an authorized address in the headquarters. If someone sends a signal with a foreign transmitter, this will be done with an unknown MAC address and rejected by the control center.

3) Use of a 16-digit password in the "*secret Key*" procedure, with each signal this password is not readable in the data package sent and compared with the control panel.

4) Encryption of all function codes in a process developed and patented by our company. All transmitter settings made by the user during commissioning are translated into a unique machine code in the central unit and then stored on the sensor. This applies to all radio signals such as arming and disarming, alarm signal, installation location, alarm function in the control panel after receiving the alarm signal, etc.

Even if someone intercepts this machine code theoretically, he cannot use it because he cannot recognize which number and which letter stands for which function. As these codes are generated differently in each control centre, our security system is considered to be particularly secure.