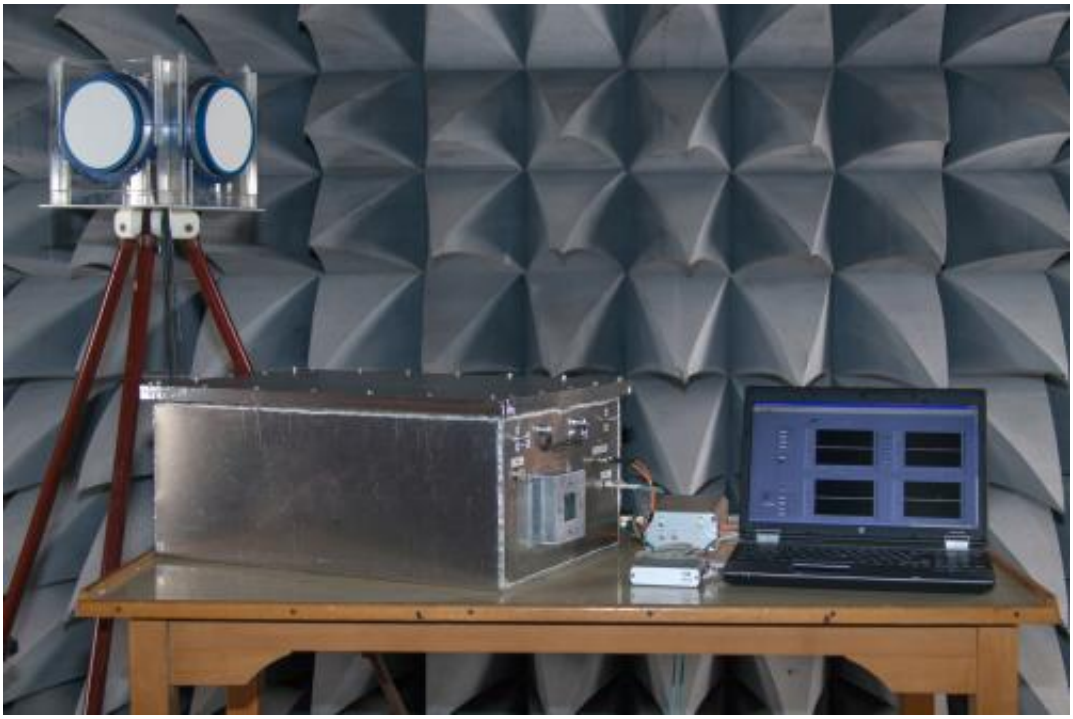
# Defense against electromagnetic fields

December 2 2013



Tools for defending against electromagnetic attack (right to left): an antenna set (on tripod) for sensing the environment, a RF measuring device for conditioning the signals and a computer that calculates the relevant data. Credit: Fraunhofer INT

Electromagnetic fields can interfere with or damage electronic devices. Electromagnetic radiation is invisible to people. A new measuring instrument can now determine the strength, frequency, and direction of the attack.

We are all familiar with the power of electromagnetic attacks from the movies: in *Ocean's Eleven*, George Clooney's gang disables Las Vegas' power grid, and Keanu Reeves' henchmen hold off the enemy robot fighters from their spaceship in the *Matrix* Trilogy. The heroes in the films succeed by sending out a very strong electromagnetic pulse. This changes the voltage in the vicinity so that regulators, switches, and circuit boards in electronic equipment go crazy. You cannot smell, taste, or feel this radiation. Those affected by it do not know why computers or machines breakdown or from which direction the attack comes.

"What works on the silver screen is also conceivable in reality," confirms Michael Jöster from the Fraunhofer Institute for Technological Trend Analysis INT in Euskirchen, just south of Cologne, Germany. The researchers there are concentrating on the question of how these attacks can be detected. They have developed a measurement instrument for this purpose that is capable of determining the strength, frequency, and direction of electromagnetic attacks. The engineering requirements are steep: the detector must measure very high field strengths from very short pulses, yet not be destroyed or damaged itself.

## Identifying the type, location, and duration of the attacks

Four specialized antennas make up the INT demonstration instrument that sample the environment around the subject device to be protected. Each of these covers a quadrant of 90 degrees and detects all types of electromagnetic sources. A high-frequency module preconditions the signals for measurement and determines when the electromagnetic pulse started and stopped. A computer in a monitoring station connected via an optical conductor then calculates the values for the signal and presents them on a screen. "We identify the type and location of the source of the invisible attack as well as its duration as though we had a sixth sense.

Those affected by the attack can use this information to mount a rapid and appropriate protective response," explains Jöster. The threat scenarios are real: criminals disrupt computer networks of banks, exchanges, and companies. They cause confusion in order to bypass monitoring points or overcome alarm systems, enabling them to penetrate into secure areas. Individual cases of these kinds of attacks have already been documented: thieves used electromagnetic waves to crack the security sys- tems of limousines in Berlin. Their weapons are no larger than a suitcase. High-power microwave sources are suitable for those kinds of attacks, for example. Depending on the field strength, the attacker using these high-power microwaves can be located several meters from the target of the attack. "Located In the right position, it is enough to press a button to trigger the pulse. Just like in *Ocean's Eleven* or *The Matrix*, the electronic systems nearby can fail or be damaged," says Jöster.

Electronic devices can withstand a certain amount of radiation. This is measured in volts per meter (V/m) – called the electromagnetic compatibility (EMC). Otherwise, they would not operate reliably. Every device could interfere with others in its immediate vicinity. Depending on the category of usage, they therefore have to fulfill specific EMC requirements. These are significantly higher for industrial applications than for common things like Smartphones, televisions, or stereo equipment. One example where safety is important is automotive engineering. "The importance of electronic components will continue to increase in the future. Completely shielding individual devices from electromagnetic radiation would certainly be theoretically possible, but much too expensive though. Systems are needed that can detect these kinds of attacks. If you know what is attacking, you can also react correctly to it," says Jöster.

Provided by Fraunhofer-Gesellschaft