No chance for industrial pirates

February 14 2014

Facilities will use a data network to communicate with one another. For these functions is indispensable: Secure access that keeps industrial pirates and saboteurs out. Credit: © Fraunhofer IPA

In the future, production facilities will be able to communicate and interact with one another, and machinery will often be remote-serviced. But no company boss wants to run the risk of opening the door to

industrial espionage and sabotage with unsecure networks. A new development offers a particularly high level of security. Researchers are presenting the system at the embedded world trade fair from 25 through 27 Feb. in Nuremberg (Hall 5, Booth 5-250).

Though it looks like something straight out of a science-fiction film, it will soon become a reality in the production halls of the future: products along the production lines will know where they are, which steps they have already completed, and what they still need to become a finished product. Production facilities will coordinate their work steps and exchange information with one another. There will be no need for technicians to set foot in the production halls for servicing, with machinery inspections carried out remotely instead. In a word: products and plants will be intelligent. This is also referred to as "Industry 4.0" – meaning industry of the fourth generation, following mechanization, electrification and digitization.

There's one sticking point, though. Facilities will use a data network to communicate with one another, and even the products themselves will have to "log in." Human beings will use this network connection to control and monitor production, too – to keep an eye on plant operation even if they don't happen to be in the production hall. On top of this, there will be remote maintenance and remote software updates. For all these functions, one thing is indispensable: secure access that keeps industrial pirates and saboteurs out. Certainly, businesses can use a normal Internet connection for this form of data traffic, securing it through a "Virtual Private Network," or VPN for short. "But there's something many people don't know: there are VPNs and there are VPNs – and not every VPN access is secure," explains Bartol Filipovic, division director at the Fraunhofer Institute for Applied and Integrated Security (AISEC) in Garching, Germany.

That is why researchers have come up with a router that offers secure

VPN access. Authorization and firewall functionalities provide additional access protection. The necessary security protocols can also be integrated directly in the industrial customer's plants and machinery. "The system is a software kit. We've already developed the basic components, and we can tailor them to fit the customer's specific requirements," Filipovic points out. The process takes around four weeks to complete. The researchers integrate simple systems at the same time, such as sensors in the pharmaceuticals industry that report filling levels or mixing ratios – these, too, should not forward their information to unauthorized parties.

Physical protection: film sounds an alarm

On the one hand, the system protects companies from spies trying to hack their way into the network from off-site locations. On the other hand, it also outwits data thieves trying to coax secrets out of routers and circuit boards on location. A special film affixed to security-relevant casings immediately reports any attempts to unscrew the protective covering to access security-relevant data. Developed at AISEC, the film is affixed to the router casing, or directly onto the circuit boards – the board containing key control elements such as microcontrollers, chips, diodes and other security-critical processing units – and sealed shut at multiple points. If the router is switched off, all of the software it contains is stored in encrypted form. If it is in operation, though, it needs the decrypted program code. Each decryption key is a function of the properties of the protective film. And if these properties are changed – by tearing open or drilling into the film to reach the circuit boards, for instance – the film detects the attack in a few milliseconds and responds immediately: it deletes all of its unencrypted, security-relevant data.

Unauthorized intruders cannot get to the software. Data deletion is no problem for the business, however: all a company has to do is reinstall the software and affix a new protective film. "Combining software and

film gives us an ideal security level," Filipovic says, "and the events of 2013 very clearly taught us just how important that can be." Secure communication software and hardware are fundamental to the evolution of production toward digitization and Industry 4.0; and protection against espionage, sabotage and product piracy is crucial to innovation and a strong competitive position.

Provided by Fraunhofer-Gesellschaft