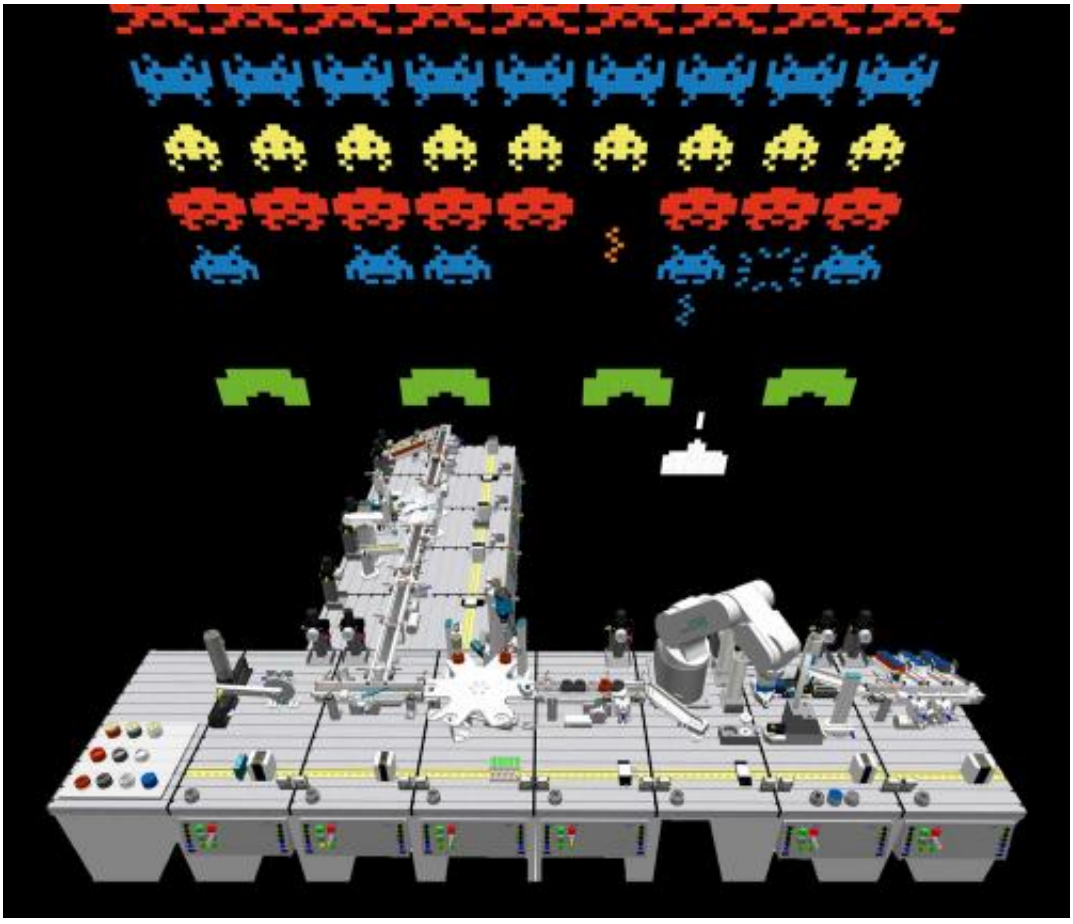
Safe production in Industry 4.0

February 2 2015



Space invaders haven't got a chance: Production networks of the future will be attack-proof -- with the aid of the IT security laboratory found at Fraunhofer IOSB. Credit: Fraunhofer IOSB

Production facilities and components of Industry 4.0 are linked to the Internet, networked with each other, and thus open to attack. Using an IT

security laboratory, Fraunhofer researchers offer a test environment in order to simulate attacks on this network and to detect any gaps. They will unveil the possibilities at this year's Hannover Mess.

Beautiful new production world: For value-creation chains that span multiple locations, equipment, robotics, systems components, minicomputers in components and sensors are all networked with each other in Industry 4.0. They exchange data, retrieve the status of equipment and components, calculate the optimal sequence of work processes, schedule equipment usage and much more. Yet with the entry of communications into factories via Internet technologies, the safety risk also increases. Beside the known viruses, there are new, custom-tailored malware programs threatening the networked production plants. They can spy out system parameters, remotely control machinery, manipulate controls or paralyze processes. Industry 4.0 networks therefore require particular protective measures, sophisticated network technology and effective test methods that detect security gaps and close them reliably. With an IT security laboratory specially equipped for production and automation technology, the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB in Karlsruhe provides a secured test environment in order to readjust potential attacks on production networks, to study the effects and thus, to deduce new strategies and suitable defense measures. It also enables researchers to assess the security functions of conventional communications standards and protocols for industrial automation systems. These regulate, among other things, the data encryption to counter product piracy, espionage and sabotage.

Different framework conditions than in office IT

"IT security in industrial production must take into account entirely different framework conditions that do not exist accordingly in Office IT," says Birger Krägelin, project manager at IOSB's IT Security

Laboratory. The control of production facilities entails real time requirements that make changes to the systems difficult. Downloading available software patches onto the systems and installing surveillance software, malware scanners, and antivirus programs influence the stability of meticulously coordinated processes. By the same token, production processes affect conditions when updates can be realized. Firewalls within the network and encrypted connection between systems can diminish real-time conditions. "For example, it is possible that the built-in of known security measures from the office environment can delay the dispatch of messages between computers. That can lead to conveyor belts running slower, valves or outlets closing with a delay, light barriers are triggered incorrectly, the rotational speed of motors increases, or control components break down," Krägelin explains. Even the relatively long usage period of hardware and software in production is markedly different from other areas where IT is deployed.

In order to find and establish appropriate IT security mechanisms for the production environment, the research team of specialists in automation technology and IT security equipped the laboratory accordingly. It features its own model factory with real auto mation components that control a simulated production facility, complete with conveyor belts, electric motors, robots, and lifting equipment. All network levels of a factory are equipped with typical components, including firewalls, circuits, and components for wireless parts. Having its own private cloud means it is possible for the IOSB experts to flexibly arrange various configurations and set up the model factory for a variety of scenarios.

"In the cloud, we can patch in virtual firewalls, PCs, add additional client computers and modify entire network structures with just one mouse-click. This makes it possible for us to install a virtual firewall or even analytical systems between two components, such as a machine and an overarching MES system (Manufacturing Execution System). From the cloud, we can start malware detection and for example text controls and

systems visualizations for infections," the master of information science (MIS) explains. "We are capable of building other factory situations and simulate cyber attacks - without having to buy components and configure circuitry."

The researchers from IOSB will be demonstrating which attack scenarios could happen to networked production facilities at the Fraunhofer joint exhibition booth at this year's Hannover Messe, in Hall 2, Booth C16 from April 13 to 17. Companies can use the laboratory so they can consult on the planning and operational launch of secure industrial network structures. In addition, they benefit from the know-how of the IOSB experts when it comes to the analysis of their already existing network and components. Furthermore, the researchers want to offer the laboratory in the future as an education and learning platform for training measures. "The one thing that engineers often don't have is the knowledge of how to deal with cyber threats," Krägelin points out.

Provided by Fraunhofer-Gesellschaft