Protection against cyberattacks: More IT security in port terminals

3 September 2020

Automated straddle carriers at the container terminal in Wilhelmshaven – efficient and secure. Credit: EUROGATE

Ports are critical infrastructures since disruptions and stoppages can have immense impacts. The potential security risks are multifarious, especially in digitalized container terminal operations, which are steadily gaining importance through Industrie 4.0. A new method and tool set developed by research scientists at the Fraunhofer Institute for Factory Operation and Automation IFF and its industry partners enables preventive defense against attacks on automated cyber-physical systems and helps increase security along the entire supply chain, including the IT systems landscape. At the same time, automation projects can be planned and implemented efficiently.

A well-developed port infrastructure is essential to the performance of a seaport's opera-tions. With few exceptions, people still transport the containers at port terminals all over the world from point A to point B with vehicles. The Fraunhofer IFF's project partners EUROGATE, TRANSPORTWERK Magdeburger Hafen GmbH and METOP GmbH want to automate this process. Transporters' movements between ships, trucks and trains during loading and unloading will be automated in the future. This will turn them into cyber-physical systems that respond to their environment with the aid of sensors, track their location at terminals with actuators, and process given transportation orders automatically.

Cyber-physical systems, which could even be forklifts or cranes, are highly complex software systems that interact with mechanical and electronic components. This exposes them to a wide range of risks, such as hacker attacks or physical tampering. Moreover, their complexity makes them susceptible to systems' intrinsic malfunctions that compromise stability. "Simply a software update on one of the vehicles can result in version conflicts and stoppages. Cyberattacks and hacker attacks are also becoming a growing threat to port operators in Germany," says Tobias Kutzler, research scientist at the Fraunhofer IFF in Magdeburg. In close collaboration with the project partners, he is establishing actions that increase the security of cyber-physical systems and the IT infrastructure with his team and project partner METOP GmbH in the joint AUTOSEC project (see box). They will implement them at the port terminals run by consortium coordinator EUROGATE first. They will also assess whether they can be transferred to and implemented at Magdeburg's inland port, which has significantly fewer IT resources.

Digital twins increase critical infrastructures' security and resilience

Automated solutions will also be introduced at the Port of Magdeburg in the future. Credit: Fraunhofer IFF

Newly discovered errors or specific attacks can never be completely eliminated or prevented from the start (stability approach). The research scientists' goal is to find an approach that permits quick, automatic detection of errors or problems and increases resilience (resilience approach). The goal must be to shut down not an entire system but only malfunctioning subcomponents and additionally to make it possible to restart the complete system rapidly by enabling rapid troubleshooting and debugging. This approach can be applied to a wide array of logistical operations. "Using simulations, we build a digital twin of the port and constantly compare the real port infrastructure's operations with the digital twin. If the two do not perform identically, there is a problem," says Kutzler, explaining the idea.

Three-stage plan: identify, localize, rectify

The comparison is made using a specially developed method and tool set based on a three-stage plan: identify, localize, rectify. First, the software detects malfunctions by comparing monitored performance parameters or key indicators. "We detect a disruption when containers are no longer moving at the specified speed, for instance," says the engineer. In the next step, the software localizes the malfunction in the system and identifies the type of problem. Here, the software uses data mining methods to compare the parameters monitored for their progression over time with other context data to identify correlations and pinpoint the malfunction. Then it attempts to localize the cause of the malfunction in order to decide whether the entire system or just part of it (e.g. a vehicle) has to be shut down. "Since there are still no standards for the automation of container terminal operations and the monitoring of cyber-physical systems, we are basically starting from scratch," says Kutzler. "The digital twin additionally enables testing a system's startup with all 'real' IT components and simulated hardware in the simulation, going live only when it functions flawlessly. What's more, we can also use the same method to test it in real operation against the digital twin. This enables us to identify and narrow malfunctions down rapidly and shut off the affected system."

The project partners are evaluating the prototype solution in initial tests at Wilhelmshaven's port terminal and Magdeburg's inland port from July through the end of September. The location, direction of travel and speed of already automated straddle carriers being developed and tested on a test site in EUROGATE'S STRADEGY project will be observed in Wilhelmshaven first. Straddle carriers are very complex vehicles that move and stack containers at terminals. "A successful hacker attack on or other tampering with the logistics system would harm more than just our partner EUROGATE. It would also affect traffic in the respective port city since the trucks being processed would back up for kilometers," says the research scientist. The urgency of the AUTOSEC project was underscored by the hacker attack on the Danish company Maersk, which ships around twenty percent of total global trade in its shipping containers, in 2017. The damage totaled several hundred million dollars.

Provided by Fraunhofer-Gesellschaft