

Nuremberg, April 10, 2018

Hannover Messe 2018, Hall 9, Booth D35

Siemens heightens industrial cyber security by detecting anomalies

- **Transparency for industrial plant networks and the software in use**
- **Comprehensive vulnerability insights**
- **Industrial Anomaly Detection to identify threats**
- **Important complementary measure for the Defense-in-Depth security concept**

Siemens will present a solution for detecting anomalies in industrial networks at the Hannover Messe 2018. "Industrial Anomaly Detection" enables security-related incidents, such as unauthorized intrusions and malware, to be identified and countermeasures to be taken. The software is pre-installed on an industrial PC (IPC), and easily integrated into industrial environments. Alternatively, it will be enabled to run on network components from Siemens, such as the multiservice platform Ruggedcom RX1500 with Ruggedcom APE. The solution is especially suitable for companies in the automobile production, aerospace, chemical, pharmaceutical, food and beverage, and water/waste water industries.

Industrial Anomaly Detection begins by establishing transparency regarding the devices integrated into industrial networks (such as controllers and HMI devices) and the software installed on them. Having achieved that, the second step is to identify vulnerabilities within devices on the network by matching assets with known vulnerabilities (Common Vulnerabilities and Exposures/CVEs) and identifying other "network hygiene" configuration issues that need to be closed. The third step is to continuously monitor the devices' communication behavior. The system collects the data passively, so it does not have any effect on production. It supports the products

of all the current automation manufacturers and their protocols. If the solution detects deviations that might indicate unauthorized intrusions or misconfigurations, it automatically sends an alarm to the users. Depending on the criticality, the incidents can be dealt with by on-site experts or external security specialists.

The anomaly detection system also uses artificial intelligence (AI), which configures the system by a process of self-learning: The solution automatically analyzes the data traffic in the network in a "learning phase", so that it can then detect anomalies, which might indicate intrusion or data theft by hackers.

"Industrial Anomaly Detection" is an important complement to the range of industrial security products and services offered by Siemens, which is based on the holistic Defense-in-Depth concept.

Partnerships to heighten cybersecurity

At the Munich Security Conference 2018, Siemens initiated the Charter of Trust for binding rules and standards to build trust in cybersecurity and further advance digitalization. To continuously innovate and adapt cybersecurity measures to new threats it's important to combine domain know how. For this reason Siemens cooperates with numerous different partners and uses for "Industrial Anomaly Detection" technology from leading partners.



Siemens will present a solution for detecting anomalies in industrial networks at the Hannover Messe 2018. "Industrial Anomaly Detection" enables security-related

incidents, such as unauthorized intrusions and malware, to be identified and countermeasures to be taken.

You will find this press release and a press picture at

<http://www.siemens.com/press/PR2018040235DFEN>

Find further information about Siemens at the Hannover Messe 2018 at

www.siemens.com/press/hm18 and www.siemens.com/hannovermesse

Contact for journalists

Dr. David Petry

Phone: +49 (9131) 7-26616; E-mail: david.petry@siemens.com

Follow us on **social media**:

Twitter: [www.twitter.com/MediaServiceInd](https://twitter.com/MediaServiceInd) and [www.twitter.com/siemens_press](https://twitter.com/siemens_press)

Blog: <https://blogs.siemens.com/mediaservice-industries-en>

Siemens AG (Berlin and Munich) is a global technology powerhouse that has stood for engineering excellence, innovation, quality, reliability and internationality for 170 years. The company is active around the globe, focusing on the areas of electrification, automation and digitalization. One of the world's largest producers of energy-efficient, resource-saving technologies, Siemens is a leading supplier of efficient power generation and power transmission solutions and a pioneer in infrastructure solutions as well as automation, drive and software solutions for industry. With its publicly listed subsidiary Siemens Healthineers AG, the company is also a leading provider of medical imaging equipment – such as computed tomography and magnetic resonance imaging systems – and a leader in laboratory diagnostics as well as clinical IT. In fiscal 2017, which ended on September 30, 2017, Siemens generated revenue of €83.0 billion and net income of €6.2 billion. At the end of September 2017, the company had around 377,000 employees worldwide. Further information is available on the Internet at www.siemens.com