# IIoT: New Industrial Security Solution for Secure Modbus Protocol Communication available from Rohde & Schwarz Cybersecurity

**SCADA, CIS, ICS and similar Modbus protocol communication based industrial systems become much more vulnerable due to their increasing connection to the Internet. The protocol lacks built-in security measures, which makes it easy for cybercriminals to exploit industrial systems and networks and take full control of critical infrastructure. Rohde & Schwarz Cybersecurity now provides a critical IT security solution for secure Modbus protocol communication that protects the Industrial Internet of Things (IIoT) against cyberattacks and espionage.**

Leipzig, Germany – April 20, 2017 – Rohde & Schwarz Cybersecurity, a leading German cybersecurity company, today announced the availability of its new Modbus protocol detection and extraction capabilities provided by the deep packet inspection (DPI) engine R&S PACE 2. The DPI engine delivers Modbus content and metadata extraction and enables IT security equipment vendors to gain full visibility of Modbus protocol communication in order to detect vulnerabilities and provide protection for the IIoT.

Modbus is an application layer protocol that provides a client/server communication between devices connected on different types of buses or networks. For instance, supervisory control and data acquisition (SCADA) systems or industrial control systems (ICS) measure temperature and humidity and communicate the results to a computer with the help of Modbus protocol.

Because Modbus-based industrial systems were designed for isolated environments, their development centers on reliability, availability, and speed – not security. Therefore, the Modbus protocol is lacking common security mechanisms such as authentication, confidentiality and integrity. This makes it inherently insecure and vulnerable to attacks.

Today's modern conveniences such as electricity, transportation and water systems are powered by SCADA, ICS or ICS. This means that the weakness of Modbus protocol communication must be addressed. An attack on such systems and networks not only has the potential to shut down an entire region's power grid and disrupt critical systems and production lines, but also can cost lives.

With the new Modbus content and metadata extraction functionality, vendors of security products, such as firewalls or gateways, gain granular visibility and control of the Modbus protocol communication. This enables them to detect threats in the SCADA or ICS environment and enhance their IT security solutions by adding a further layer of security in their products.

"Firewall vendors can embed the deep packet inspection engine in their protection products to inspect the content contained in the industrial protocol communication," says Dirk Czepluch, VP of the business units Network Analytics and Network Protection at Rohde & Schwarz Cybersecurity. "The Modbus content and metadata extraction functionality enables them to apply more detailed rules, filters on individual fields and values that matter to IT administrators using such firewalls," adds Czepluch. "They can now control who can communicate with the device, what communication is allowed and provide protection against malicious commands."

Find out more about how IT security equipment vendors use the DPI engine R&S PACE 2 to enhance their network protection products and add value for their customers: http://ipoque.com/solutions/

**Rohde & Schwarz Cybersecurity GmbH**
**cybersecurity.rohde-schwarz.com**
**R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG.**

Press Contact:
Christine Lorenz, Phone: +49 34159403062, Email: christine.lorenz@rohde-schwarz.com

**Rohde & Schwarz Cybersecurity**

**Rohde & Schwarz Cybersecurity is an IT security company that protects companies and public institutions around the world against cyberattacks. The company develops and produces technologically leading solutions for information and network security, including highly secure encryption solutions, next generation firewalls and software for network analysis and endpoint security. The award-winning and certified IT security solutions range from compact, all-in-one products to customized solutions for critical infrastructures. To prevent cyberattacks proactively, rather than reactively, our trusted IT solutions are developed following the security-by-design approach. Around 450 people are employed at the current locations in Germany, France and Denmark. As a result of the acquisition of DenyAll, the portfolio now includes vulnerability scanners and firewalls for business-critical web applications.**

**Rohde & Schwarz**

**The Rohde & Schwarz technologies group offers innovative solutions in all fields of wireless communications as well as in IT security. Founded more than 80 years ago, the independent company has an extensive sales and service network with subsidiaries and representatives in more than 70 countries. On June 30, 2016, Rohde & Schwarz had approximately 10,000 employees. The group achieved a net revenue of approximately EUR 1.92 billion in the 2015/2016 fiscal year (July to June). The company is headquartered in Munich, Germany, and also has strong regional hubs in Asia and the USA.**

R&S ® is a registered trademark of Rohde & Schwarz GmbH & Co. KG.

**Rohde & Schwarz Cybersecurity GmbH**
**cybersecurity.rohde-schwarz.com**
**R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG.**