Contact person:
Barbara Weber
Barbara.Weber@profibus.com
☎+49 (0) 721 96 58 549

PRESS RELEASE

PROFINET enhanced with further security measures

Karlsruhe – November 27, 2019: PI (PROFIBUS & PROFINET International) recognized at an early stage that security is one of the most vital components of an industrial communication system. Since 2006, the PROFINET Security Guideline has described the technical and procedural measures on the part of the manufacturer and users of PROFINET devices. PI is now developing supplemental measures to also protect PROFINET at the protocol level.

Within the scope of the far-reaching digitization of production processes, the IT security of production plants is gaining in importance. The integrated networking in companies, the vertical integration and the trend toward flatter system hierarchies require comprehensive approaches for IT security in production. Previous concepts, which relied primarily on isolating the production plants, must be supplemented with new measures that make provision for the protection of components. These include the protection of PROFINET at protocol level. The basics for this were presented by PI this year in the white paper "Security Extensions for PROFINET," which draws on international standard IEC 62443.

Various security objectives play a significant role for PROFINET in this process. One of the highest priorities is integrity – e.g. identifying and preventing data manipulation or the suppressing of alarms in devices. Changing the configuration of IO devices in day-to-day operations must also be secured by means of authorization. The robustness of the system, and thus its availability, also cannot be disregarded. The analysis of the security objectives yields various priorities, resulting in PI now having defined three security classes: robustness, integrity and authenticity, and confidentiality. For instance this allows for the authenticity of the PROFINET nodes to be ensured through a cryptographically secured digital identity, e.g. in the form of certificates. But the integrity of the communication can also be ensured, e.g. through cryptographic checksums.

The necessary specification tasks have now been outlined, and initial measures for security class 1 (robustness) have been defined. These will be integrated in the specifications for PROFINET and for GSDML, e.g. the signing of GSD files, access controls of network management services (SNMP), and a read-only function for configuration information such as the device name.

Parallel to this, further development is taking place on the other security classes. This ensures that PROFINET will be equipped to face the demands of Industry 4.0 and will serve as a future-oriented platform for the industrial internet. Here, PI is implementing the key subjects for the realization of digitalization in industrial production. Go digital. Go PROFINET.

***

Graphic: PROFINET will also be protected at the protocol level. PI has integrated initial measures in the PROFINET specification.

Copyright: voyager624/shutterstock

Press contact:

PI (PROFIBUS & PROFINET International)

PROFIBUS Nutzerorganisation e. V.

Barbara Weber

Haid-und-Neu-Str. 7

D-76131 Karlsruhe, Germany

Phone: +49 (0) 721 / 96 58 549

Fax: +49 (0) 721 / 96 58 589

Barbara.Weber@profibus.com

http://www.PROFIBUS.com

This press release is available for download at www.profibus.com.