Contact person:
Barbara Weber
Barbara.Weber@profibus.com
☎ +49 (0) 721 9658-549

PRESS RELEASE

New security white paper

Hanover, Germany – April 01, 2019: PI (PROFIBUS & PROFINET International) is publishing a new security white paper documenting the basic concepts for protecting the PROFINET protocol. The purpose of the white paper, dubbed "Security enhancements for PROFINET," is to initiate coordination meetings with users, integrators and manufacturers. The objective of this discussion is a coordinated and viable concept which will make industrial communication with PROFINET fit for the requirements of the Industry 4.0 environment. Implementation will lead to a security specification for PROFINET networks provided as a supplement to the security guideline which has been available for more than 10 years.

Integrated networking within the company, vertical integration and the trend toward flatter system hierarchies require further-reaching approaches for IT security in production. Previous concepts, which relied primarily on isolating production plants, must be supplemented with new concepts which make provision for the protection of components.

The current IT security concept for PROFINET assumes a defense-in-depth approach as described in IEC 62443. The production plant is protected against attacks – particularly from the outside – by means of a multi-layer perimeter (firewalls, among other things). In addition, further safeguarding within the plant is possible by dividing the network into zones. Furthermore, a security component test ensures the ability of the PROFINET components to withstand overloading in a defined scope. This concept is supplemented by organizational measures in the production plant within the framework of a security management system.

The described security measures for PROFINET essentially correspond to current state-of-the-art technology. New requirements from users demand further protection on the component level, which in turn necessitates suitable protective measures on the protocol level, however.

The “Security enhancements for PROFINET” white paper describes the new security requirements, protection goals derived from them and – based on the analyses conducted – the key concepts and protective measures for a PROFINET system. In the next step, the security working group will specify enhancements of the PROFINET protocol and strengthen it with additional cryptographic functions to ensure integrity, authenticity and, if required, the confidentiality of communication on the protocol level. The goal here is to limit the technical expenditure for systems with basic security requirements while at the same time ensuring backwards compatibility with the option of being able to operate the enhanced protocol parallel to the previous protocol on a network.

The white paper can be downloaded from the PI website free of charge: https://www.profibus.com/profinetsecurity

***

Press contact:

PI (PROFIBUS & PROFINET International)
PROFIBUS Nutzerorganisation e. V.
Barbara Weber
Haid-und-Neu-Strasse 7
D-76131 Karlsruhe, Germany
Phone: +49 (0) 721/96 58 - 5 49
Fax: +49 (0) 721/96 58 - 5 89
Barbara.Weber@profibus.com
http://www.PROFIBUS.com

The text of this press release is available for download at www.profibus.com.