Contact person:

Barbara Weber

Barbara.Weber@profibus.com

 +49 721 9658-549

**P R E S S R E L E A S E**

# Additional security measures supplement the proven IT security concept for PROFINET

**Karlsruhe, Germany – September 17, 2020:** Already very early – in parallel with the first PROFINET specifications – PI published an extensive security concept, which was further refined and adapted in multiple steps. It is not sufficient simply to protect plant networks and automation components, rather the used protective mechanisms and concepts must not interfere with the running production operation. Moreover, the protection concepts must be easy to implement and remain affordable. The most important aspect, however, is that the concepts must be adapted time and again to current developments. PI has now expanded its IT security concept.

The IT security concept used for PROFINET employs a defense-in-depth approach. With this method, the production plant is protected against attacks – particularly from the outside – by means of a multi-layer perimeter (including, among other things, firewalls). In addition, further safeguarding within the plant is possible by dividing into zones through the use of firewalls. Furthermore, a security component test ensures the ability of the PROFINET components to withstand overloading in a defined scope. This concept is supported by organizational measures in the production plant within the framework of a security management system.

Security is, however, a topic that must be continuously adapted to the current development and, as a result, is never finished. This applies in particular with respect to the increasing networking of production plants. The use of PROFINET components with added value, e.g., web or OPC communication, thereby ensures increased, direct communication with higher-level systems outside of the security zone. At the same time, it is becoming increasingly difficult to separate PROFINET networks.

Moreover, the networks are becoming larger, meaning that more and more components are connected together to form a network and interact with one another. A successful attack on a single (PC) system within such a cell therefore bypasses upfront security measures. Widely distributed plants also hinder the physical protection of networks and access points. Unauthorized persons can thereby gain access to the PROFINET network.

For this reason, previous concepts, which rely primarily on isolating the production plants, must be supplemented with new concepts that enable protection within the cell. PI therefore expanded the previous measures with further-reaching protective measures. This includes a credential management system, e.g., for authentication of the devices and an end-to-end security expansion for PROFINET communication as a configuration option. As not every application has the same security requirements, three security classes were defined for PROFINET.

Further technical details and practical examples can be found in the Industry 4.0 Highlight "Security" at <https://www.profibus.com/technology/industrie-40/>. In this campaign on the PI website, current topics, issues and trends from Industry 4.0 applications are addressed so that the user can easily implement and realize them in practical work.

\*\*\*

**Graphic:** PI has expanded its IT security concept for PROFINET.

****

**Press contact:**

PI (PROFIBUS & PROFINET International)

PROFIBUS Nutzerorganisation e. V.

Barbara Weber

#### Haid-und-Neu-Str. 7

#### D-76131 Karlsruhe, Germany

Phone: +49 7 21/96 58 - 5 49

#### Fax: +49 7 21/96 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](http://www.profibus.com).