Ihr Ansprechpartner:

Barbara Weber

Barbara.Weber@profibus.com

Brief_Phone +49 721 9658-549

**P R E S S E M I T T E I L U N G**

**PROFINET wird um weitere Security-Maßnahmen ergänzt**

**Karlsruhe – 27. November 2019:** Bereits früh hat PI (PROFIBUS & PROFINET International) erkannt, dass Security einer der wichtigsten Bausteine eines industriellen Kommunikationssystems ist. Seit 2006 beschreibt die PROFINET Security Guideline technische und prozedurale Maßnahmen auf Seiten der Hersteller und Anwender von PROFINET-Geräten. Nun erarbeitet PI ergänzende Maßnahmen, um PROFINET auch auf Protokollebene zu schützen.

Im Rahmen der weitreichenden Digitalisierung von Produktionsprozessen rückt die IT-Sicherheit von Produktionsanlagen immer stärker in den Vordergrund. Die durchgängige Vernetzung in Unternehmen, die vertikale Integration und die Tendenz zu flacheren Systemhierarchien erfordern durchgängige Ansätze für die IT-Sicherheit in der Produktion. Bisherige Konzepte, die in der Hauptsache auf eine Abschottung der Produktionsanlagen setzen, müssen durch neue Maßnahmen, die einen Schutz der Komponenten vorsehen, ergänzt werden. Diese sehen einen Schutz von PROFINET auf Protokollebene vor. Die Grundlagen hierzu wurden in diesem Jahr in dem Whitepaper „Security-Erweiterungen für PROFINET“ von PI vorgesellt, welches auf den internationalen Standard IEC 62443 zurückgreift.

Dabei spielen verschiedene Schutzziele für PROFINET eine wesentliche Rolle. Insbesondere die Integrität, also z.B. die Verhinderung bzw. das Erkennen einer Manipulation der Daten, bzw. der Unterdrückung von Alarmen der Geräte, hat eine hohe Priorität. Ebenso muss eine Änderung der Konfiguration von IO Devices im laufenden Betrieb durch Autorisierung abgesichert werden. Aber auch die Robustheit des Systems, und damit die Verfügbarkeit der Anlage, dürfen nicht außer Acht gelassen werden. Aus der Analyse der Schutzziele ergeben sich unterschiedliche Prioritäten, sodass PI nun drei Security Klassen definiert: Robustness, Integrity + Authenticity und Confidentiality. So lässt sich beispielsweise die Authentizität der PROFINET-Teilnehmer durch eine kryptografisch gesicherte digitale Identität, z. B. in Form von Zertifikaten, sicherstellen. Aber auch die Integrität der Kommunikation kann beispielsweise durch kryptografische Prüfsummen gewährleistet werden.

Die notwendigen Spezifikationsaufgaben wurden nun skizziert und erste Maßnahmen zu Security Class 1 (Robustness) definiert. Diese werden in die Spezifikationen von PROFINET und von GSDML eingebracht, wie z. B. die Signierung von GSD-Dateien, Zugriffskontrollen von Network-management Diensten (SNMP) und eine „Nur-Lesen“-Funktion für Konfigurationsinformationen wie den Gerätenamen.

Parallel wird an der Ausarbeitung der weiteren Security-Klassen gearbeitet. Somit wird sichergestellt, dass PROFINET für die Anforderungen von Industrie 4.0 gewappnet ist und als zukunftsorientierte Plattform für das industrielle Internet dient. PI setzt hier die wesentlichen Themen zur Realisierung der Digitalisierung in der industriellen Produktion um. Go digital. Go PROFINET.

\*\*\*

**Graphik:** PROFINET wird zukünftig auch auf Protokollebene sicher. PI hat erste Maßnahmen in die PROFINET-Spezifikation eingebracht.



Copyright: voyager624/shutterstock

**Pressekontakt:**

PI (PROFIBUS & PROFINET International)

PROFIBUS Nutzerorganisation e. V.

Barbara Weber

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

#### D-76131 Karlsruhe

Tel.: 07 21 /96 58 - 5 49

#### Fax: 07 21 / 96 58 - 5 89

Barbara.Weber@profibus.com

<http://www.PROFIBUS.com>

Diese Pressemitteilung liegt unter [www.profibus.com](http://www.profibus.com) zum Download für Sie bereit.