Securing Automation Systems – a Step by Step Approach

Prof. Dr. Frithjof Klasen

The big problem when it comes to security for automation systems: there are no simple solutions. This makes it all the more helpful when communication technology experts from organizations like PROFIBUS & PROFINET International (PI) give users a hand by providing guidelines. PI also offers specific tests for testing and improving the robustness of devices to withstand denial-of-service attacks, for example.

A system is only safe if the threats are known. Typical security threats in production include infection by malware, unauthorized use (both intentional and unintentional), manipulation of data, espionage and related know-how loss, and denial of service. The consequences can be loss of production, reduced product quality, and endangerment of humans and machines.

In order to evaluate threats, the properties and possible weak points of devices and systems must be known. After all, a property that is useful from the automation perspective – for example, the ability for a programming device to access a controller without authentication – is seen as a possible weak point from the security perspective. It is necessary to distinguish these weak points in order to assess risks, develop security solutions, and take appropriate measures:

• Weak points that arise due to incorrect implementation (for example, faulty device behavior).

• Conceptually planned and accepted properties. These include all features that can also be exploited for attack purposes. An example here would be an integrated web server in an automation device.

• Weak points that are caused by organizational measures or lack thereof.

Field devices not only contain communication technologies for transmission of process signals (real-time communication) but also standard IT technologies, such as FTP services. In addition, field devices also operate as

network infrastructure components (switches) and therefore have services and protocols that are needed for network management and diagnostic purposes. The fact of the matter is that most communication protocols at the field level have no integrated security mechanisms. Devices and data are not authenticated and, consequently, within the scope of a possible attack, systems at the field level can be expanded at will and communications can be imported. Even the transferring of PLC programs often takes place without use of security measures such as user authentication and integrity protection.

There is no panacea

Ideally, users would like to have a tool, certification, or system that promises them long-term security. The difficulty, however, is that such solutions don't provide lasting security. In order to develop secure systems, users must not only implement technical measures but also conceptual and organizational measures. And everyone will know from their own experience that processes can be implemented in technologies much faster than in the minds of people.

However, conceptual and organizational weak points can be more easily overcome when they are described in guideline documents. For example, PI developed a Security Guideline for PROFINET in 2006 and published a completely revised version of this guideline at the end of 2013. This guideline specifies ideas and concepts on how security solutions can be implemented and which security solutions should be implemented. The subject of risk analysis is covered, for example. This analysis estimates the probability of a damage event and its possible consequences, based on protection goals, weak points, and possible threats. Only on the basis of an analysis of this type can appropriate security measures be derived that are also economically feasible. A series of proven best practices are also given, such as the cell protection concept.

Making devices more secure

Another measure concerns the device security. After all, robust devices are the basis for stable processes and systems. They are a basic prerequisite for

security in automation. Weak points due to incorrect implementation can be eliminated only through appropriate quality assurance measures and certifications. In large networks, system availability matters the most. To achieve this, devices must respond reliably to various network load scenarios. In systems with many devices, an unintended elevated broadcast load can occur on the network during commissioning, for example, when the master attempts repeatedly to access all devices even though only a few devices are connected. The available devices must be able to handle this abnormal load. It is difficult for operators to predict such scenarios since the probability of a high data volume is dependent on the system. The reason is that the data traffic is determined by cyclic and acyclic data exchange as well as the event-driven data volume.

With the help of the Security Level 1 Tester developed by PI for certification of PROFINET devices and free-of-charge to member companies, such network load scenarios up to and including denial of service can be simulated already in advance. The field devices are tested under stress conditions to simulate an unpredictable load and, thus, to reduce device failures. Uniform test specifications have been defined for this, which can be systematically applied by the test tool. In addition, various network load-related scenarios have been developed that take into account various frame types and sizes as well as the repetition period and number of frames per unit of time, among other things. The network load-related test is already being required by various end users such as the automotive industry. This test is already integrated in the device certification testing according to the latest PROFINET 2.3 specification and must therefore be passed in order for a device to be certified. Users that purchase such a certified device can rely on having a correspondingly robust device.

By no means are all problems solved

Only those who know their devices can protect them. Still, not all manufacturers provide comprehensive information about the utilized protocols and services and communication properties of their devices. Another problem: in spite of security, users must still be able to handle and

operate systems. No maintenance technician wants to be looking for a certification key for a failed device at 2 AM in order to bring a system back online. Future-oriented concepts therefore master the tightrope walk between usability and security.

PI has been dealing with the issue of security for years. For example, one PI Working Group is concentrating continuously on security concepts. A product of this is the PROFINET Security Guideline, which can also be downloaded free of charge by non-members. Moreover, further development of the Security Level 1 Tester is being advanced here. In so doing, it is important to all participants that the described and recommended procedures are sustainable and practicable and ultimately also accepted by users. Only in this way can protection concepts be truly successful.

End (1,076 words)

Author:

Prof. Dr. Frithjof Klasen

is a member of the Managing Board of the PROFIBUS Nutzerorganisation e.V. (PNO), Director of the Institute for Automation & Industrial IT (AIT) at FH Köln, and Director of AIT Solutions GmbH in Gummersbach.

Lead Graphic: