P3KI
trust yourself.

Pitfalls of Adapting Security Solutions for OT

P3KI Explained

Version Rev1
November 2024

1 Introduction to Operational Technology and its unique security landscape

Operational Technology (OT) encompasses the hardware and software systems used to monitor and control industrial processes, physical equipment, and infrastructure within sectors like manufacturing, energy, utilities, transportation, and critical infrastructure. Unlike traditional IT, which primarily handles data and information flow, OT systems directly impact the physical world, managing processes such as power generation, chemical production, and water treatment. This close integration with physical processes introduces distinct security and operational challenges that diverge considerably from those encountered in IT environments.

In OT environments, continuity, reliability, and safety are paramount. Systems often need to run continuously, as downtime or disruption can lead not only to financial loss but also to safety hazards or widespread operational failure. Additionally, OT environments tend to feature older, legacy systems that were not originally designed with cybersecurity in mind. These legacy systems may rely on proprietary protocols, lack sufficient processing power for modern encryption, and may not be easily patched or upgraded due to operational constraints. This contrasts with the more rapid, update-friendly nature of IT systems, where regular patching and iterative security measures are typically more feasible. Furthermore, the primary focus in OT is often to ensure operational resilience over data confidentiality, a departure from traditional IT security priorities.

With the convergence of IT and OT environments, many organizations attempt to adapt traditional IT security solutions for OT applications. However, this approach often fails to account for the nuances of OT, leading to pitfalls that can compromise both security and operational stability. For example, intrusion detection systems (IDS) designed for IT may generate excessive noise in an OT setting, where frequent alerts disrupt critical processes. Similarly, endpoint protection software can introduce latency or interfere with system operations, which, in OT, could trigger mechanical faults or safety shutdowns. This whitepaper explores some of the most common but generally overlooked pitfalls, underscoring the importance of OT-specific security considerations and highlighting how organizations can better tailor their security strategies to meet the unique demands of operational technology.

Version Rev1, November 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2 Problem statement

The core issues we regularly observe with our clients in the context of OT Security, IT/OT Convergence, and Industrial IoT generally fall under the problem category of "violation of fundamental security assumptions."

The typical causes here are:

1. Introduction of centrally or online-managed technologies (e.g., IAM)
2. Introduction of technologies that are theoretically applicable but can only be effectively maintained through centralized automation (e.g., PKI)
3. Integration of external optimization systems
4. Modularization of previously monolithic applications
5. Technological category errors
6. Complications in retrofitting

Version Rev1, November 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2.1 Centrally / Online-Managed Technologies

The integration of central services has two major side effects:

- The violation of perimeter security necessitates a fundamental reworking of the threat model as well as retroactive hardening of the control network environment.
- By externalizing the service, a strong dependency is created, which violates the integrity and autonomy of the control network.

2.2 Theoretically Applicable Technologies that Require Automation

A classic example of this category is PKI or technologies that fundamentally rely on PKI in their security model (e.g., OAuth2 / OpenID Connect). Certificates can theoretically be verified offline, but complete verification involves querying a central service (OCSP) or distributing additional data structures (CRL) to exclude the possibility of certificate revocation.

Running a local PKI is possible, but in complex environments with many control networks, the effort escalates significantly, both on the operator and user sides. An effective and controlled interaction between multiple PKI hierarchies cannot be smoothly implemented. As a result, each authorized party requires a separate certificate from the respective hierarchy for each target system.

2.3 External Optimization Systems

The exfiltration of data from a protected environment into a less secure environment (e.g., the cloud) does not present a major challenge. The problem arises with the reintegration of data that influences processes in the control network. In this regard, the NAMUR organization is developing the VOR (Verification of Request) concept, but there are still essential questions open regarding how verification should be carried out.

2.4 Modularization of Monolithic Systems

A subtle error in reasoning can easily slip in here. A monolithic system operates in a defined environment and has a specific state that can be evaluated once.

The reasons for modularization are varied, but the primary drivers are typically the ability to allow different vendors to implement individual elements and to operate individual elements in different environments.

The latter is equivalent to the above category of “external optimization systems.” The former requires an authorization system to be established between the elements and quickly escalates toward a Zero Trust

Version Rev1, November 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

Architecture and systems that fall into the category of "theoretically applicable but only meaningful if centrally managed."

2.5 Technological Category Errors

Last but not least, a common category error we observe is the use of PKI for authorization. At its core, PKI is intended for identification and authentication. Options for implementing authorization are at best rudimentary and inflexible.

2.6 Complications in retrofitting

Retrofitting itself poses significant challenges:

- Loss of certification in industries where OT equipment is required to be certified for operation
- Introduction of new assets which need to be life-cycle managed
- Ability to install additional software on vendor controlled workstations and machines might be difficult to impossible

3 Solution Approach

Our approach, which we have already successfully tested with large international players, is a fully offline-capable authorization and delegation solution.

Based on this solution, control networks as well as field devices can be enhanced with an authorization concept that is highly flexible in addressing the aforementioned complications.

We are happy to assess its applicability in your specific environment using concrete examples. Schedule a first call for free via contact@p3ki.com today.

Version Rev1, November 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com