



OT-Cyber-Security-Review: The key to secure system operation

The security and availability of an industrial plant should be a top priority, especially as the threat situation, regulations, directives and international and national security standards are constantly evolving. When a new plant is built, the security systems are designed and commissioned by specialists. However, over the course of their life cycle, these systems are constantly optimized, updated and expanded. The status of OT security is not always well documented or known.

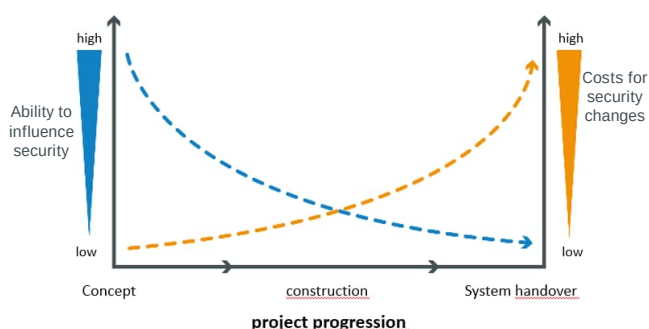
Overview of the status of OT security and the establishment of lifecycle management

Every change or modification in the plant context not only requires a review of OT security with regard to the applicable standards and norms, but also represents the practical possibility of enforcing modernization cycles. HIMA helps you to obtain an overview of the status of your OT security and all necessary measures prior to a conversion, expansion or modernization project. This enables you to adapt security processes at an early stage and avoid unexpected and expensive rework. In order to determine conformity with the applicable standards and norms, we carry out an evaluation of your OT security measures and the associated documentation as part of the OT cyber security review. Due to the shorter update intervals and threat potentials required in the security sector, the OT cyber security review is also a valuable contribution to the development or expansion of your security lifecycle management.

Advantages

- Independent overview of the current status of OT security in terms of modification, conversion, expansion or modernization
- Independent overview of the impact of changes with regard to OT security
- Determine the current degree of conformity with applicable standards, norms and best practices
- Checking the competence level of those involved in the security lifecycle
- Identification of potential cost savings and avoidance of expensive rework in later project phases
- Guidance for future activities in OT security through to the establishment of lifecycle management

Options for influencing security aspects and expenditure during the course of the project



Objective of OT Cyber Security Review

Based on the available documentation and contacts, the OT cyber security review determines whether correct and suitable processes and systems are in place in accordance with the requirements of any existing security program for operators of industrial control and automation systems (IACS). The OT cyber security consultant uses a structured procedure with questions and checkpoints as the basis for the assessment. This determines the level of maturity and identifies what needs to be done to ensure compliance with the applicable standards and guidelines and to operate the system with the lowest possible risk profile. Following the review, a summary report is prepared to discuss the findings and recommendations in a meeting and develop a concrete plan for implementation. A separate offer will be prepared to suit your budget to follow up on any necessary measures and rectify any deviations identified

Scope OT Cyber Security Review

During the OT cyber security review, the OT cyber security consultant reviews and records the following content:

- The original OT security risk assessments and specification of security requirements are in line with current standards.
- The information security policy, the risk management policy and the associated process (associated with a crisis management (manual)/policy) are up to date and have been properly maintained
- A strategy for updating security assessments and documentation is available to ensure that the required security level (SL) is defined and can be achieved on a regular basis.
- Documentation is up to date and properly maintained.
- Management, including ongoing assessment of responsibilities and competencies, is in place.

An OT cyber security review is also helpful in the event of incomplete documentation.

Standards

The OT Cyber Security Review takes into account the requirements of the following standards:

- IEC 62443 - IT security for industrial automation systems
 - Relevant IEC 62443-2-1 Requirements for an IT security program for IACS operators
- National Institute of Standards and Technology (NIST)
 - Special Publication 800-53 and
 - Special Publication 800-82
- IEC 61511 - PCT safety devices for the process industry
- IEC 61508 - Functional safety of safety-related electrical/electronic/programmable electronic systems
- Other customer-specific standards, working methods and guidelines provided



Smart Safety Services from HIMA

HIMA offers you services that cover the entire SIS life cycle. Our experience with the management of functional safety, SIS specification as well as the realization, testing and commissioning of safety equipment creates holistic knowledge. This forms the basis for the efficient implementation of the OT security review.

course of action

The OT cyber security review requires the participation of the relevant plant personnel and extends over a continuous period of time. Due to the variety of topics and the different contact persons involved this service is typically carried out via websession.

- 0.5 day Kick off
- 3-4 days Evaluation of the documentation incl. explanation, preparation of the report
- 0.5 day Final meeting with all relevant employees of the client

During the kick-off meeting, we define the necessary documents together.

Pricing

- Basic fee 9.340 Euro* for the defined scope
- Including preparation, interviews, meetings and reporting
- Excluding travel expenses and accommodation
- Successful processing is based on the availability of customer documentation and the responsible employees; additional time required is charged at the corresponding daily rates.

* The indicated price is only valid within Europe.

Contact us:

E-Mail:
consulting.de@hima.com

or visit us online:
<https://www.hima.com>