CYBERSECURITY

OT Asset Maturity Check

Accurately determine the security maturity level of your company OT environment and receive prioritised recommendations to be actioned

Digitalisation has helped increase the efficiency of production and control systems, resulting in reduced costs and improved competitive advantages.

In order to take full advantage of this potential, industrial production and control systems are increasingly connected to each other. However, this means that OT and ICS in particular, are exposed to the threat of cyber-attacks.

Based on our experience, we are convinced that a secure environment is key to efficient production and innovation.

A detailed analysis of your security systems and processes will show you how secure and mature your production environment is in regards to OT Security.

We offer an efficient customised service to determine the maturity level of protection of critical infrastructure and industrial facilities: the OT Security Maturity Check.

What we offer:

- Analysis and validation of implemented security measures, including an on-site visit and expert interviews
- Assessment of the security measures implemented according to international Standard (IEC 62443) and best practices (BSI ICS Security Compendium)
- Creation and reporting of a prioritised list of OT security measures to increase the security maturity level

Benefits Summary

Gain a fast overview about the maturity level of implemented security controls

Gain prioritised actionable recommendations considering all dimensions people, process and technology

Analysis based on international standards (e.g. IEC 62443) and best practices (BSI ICS Compendium)

Report and presentation tailored to management

AIRBUS

OT Security Maturity Check in

Kick-off

- Determination of the automation systems to be checked based on their criticality
- Definition of the documents to be analysed
- Identification of key personnel for the on-site visit and interviews
- Scheduling of appointments
- Identification of target security level

Document analysis

- Analysis of the documents provided in regards to architecture as well as technical, organisational and personal security measures
- Preparation of interviews and inspection

Interviews and inspection

- Inventory of the organisational framework, guidelines and processes
- Interview of the implemented and documented security measures
- Sample-based validation of the documented organisational security measures such as roles, rights, patch management, as well as backup and restore procedures

Evaluation

- Comparison of the information collected with the documented requirements, IEC standard and BSI best practices

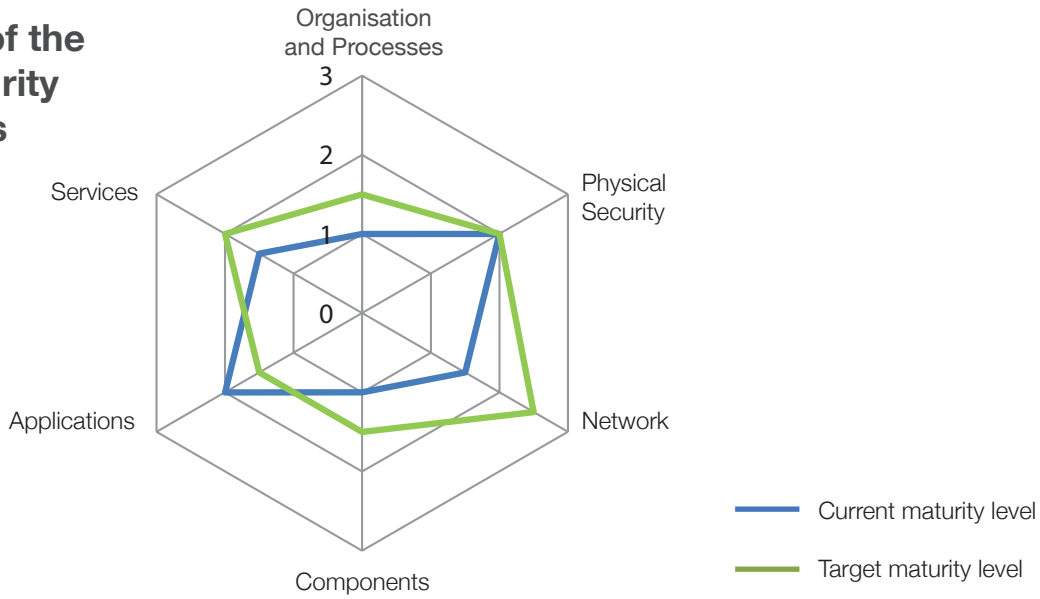
Consolidation of results

- Clarification of remaining issues with all participants
- Definition of content of the final report
- Request for missing information for the final report
- Identification of critical assets, systems and applications

Final report and presentation

- Management summary
- Subject matter, procedure and scope
- Results of the evaluation
- Recommendations for prioritised actions including quick wins

Simplified presentation of the analysed security maturity levels



Contact us for more information.

AIRBUS

FRANCE
Metapole 1, boulevard Jean Moulin
CS 40001 / 78996 Elancourt Cedex
France

GERMANY
Willy-Messerschmitt-Str. 1
82024 Taufkirchen
Germany

UNITED KINGDOM
Quadrant House / Celtic Springs
Coedkernew / South Wales
NP10 8FZ / United Kingdom

contact.cybersecurity@airbus.com
www.airbus-cyber-security.com