



OT Asset Discovery

& Analysis

## A feasible way to understand your OT/ICS environment

Digitalisation increases efficiency in today's industrial work processes. However, it also increases the convergence of IT and OT as well as the integration and connectivity of industrial control systems along the supply chain. Previously air gapped systems now communicate directly with each other. Therefore, in-depth knowledge of OT assets and networks is crucial for sufficient mitigation of this increased attack surface.

Based on our industry experience, we know that the foundation of OT security consists of a comprehensive inventory of all OT/ICS assets and their risks. Our services provide you with this

vital information, building the basis for OT security activities like maturity checks, risk assessments, and other security analysis and improvement measures.

**What we offer:**

- Passive recording of network communications or active scanning at central locations of the industrial network
- Analysis of data by experts with the support of specialised software tools
- Identification and assessment of potential vulnerabilities and anomalies

### Benefits Summary



Scalable analysis of your OT/ICS environment according to your desired process impact



Disclosure of potential vulnerabilities and anomalies



Inventory of assets with visualisation of communication pathways



Prioritised recommendations of measures for improving OT security protection

## OT Asset Discovery & Analysis in detail

### Kick-off

- Outline of the exact scope of investigation
- Identification of organisational and technical requirements for network recording and/or discovery, as well as definition of a time period for execution

### Data collection

- Installation of a recording and/or scanning system provided by Airbus CyberSecurity at a suitable central network node
- Automatic passive recording of network communications and/or active asset/vulnerability scanning over a defined period of time (min. 24 hours, max. 1 working week)

### Analysis of network data

- Analysis of the data by Airbus CyberSecurity experts to detect assets, firmware versions, communication paths and vulnerabilities
- Preparation of a final report with recommended and prioritised actions

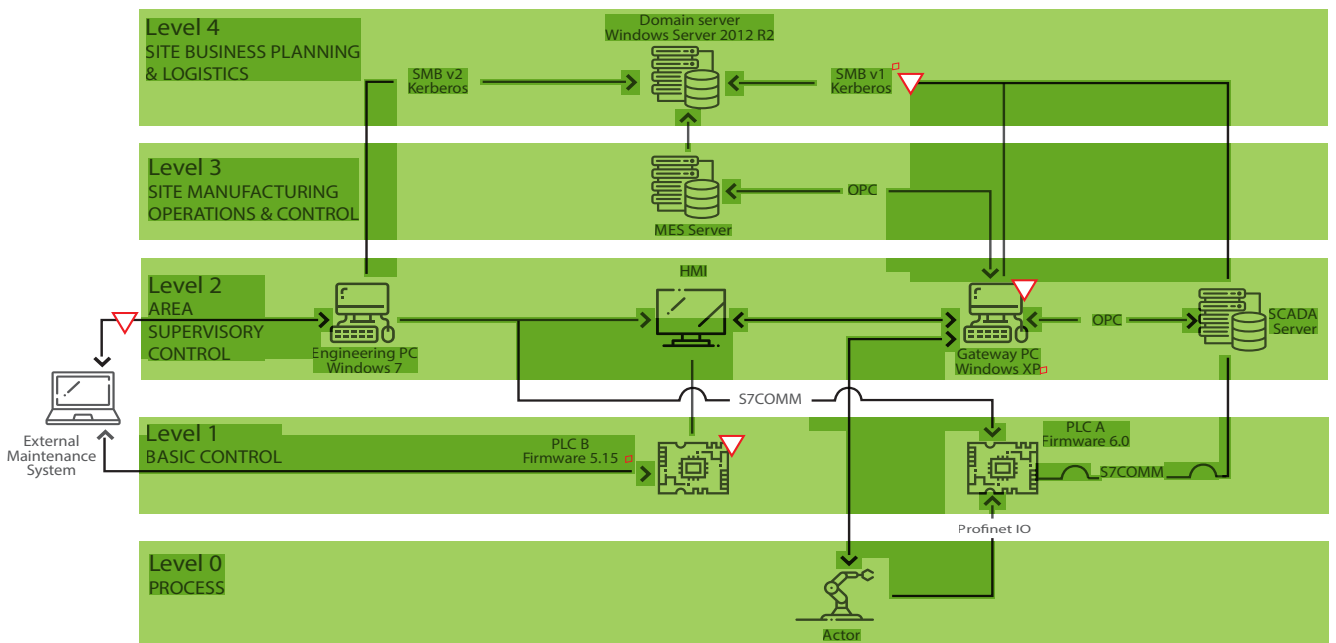
### Feedback workshop

- Clarification of remaining open questions and issues
- Discussion of first recommendations for improving OT security
- Request for additionally required information for the final report

### Final report and presentation

- Delivery, presentation, and discussion of the final report with the customer

## Gain visibility of your assets, communication pathways and potential vulnerabilities



Purdue Model for Control Hierarchy logical framework

△ Identified vulnerabilities

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

This document is not contractual. Subject to change without notice.  
© 2021 Airbus CyberSecurity. AIRBUS, its logo and the product names are registered trademarks. All rights reserved.

[contact.cybersecurity@airbus.com](mailto:contact.cybersecurity@airbus.com)  
[www.airbus-cyber-security.com](http://www.airbus-cyber-security.com)

