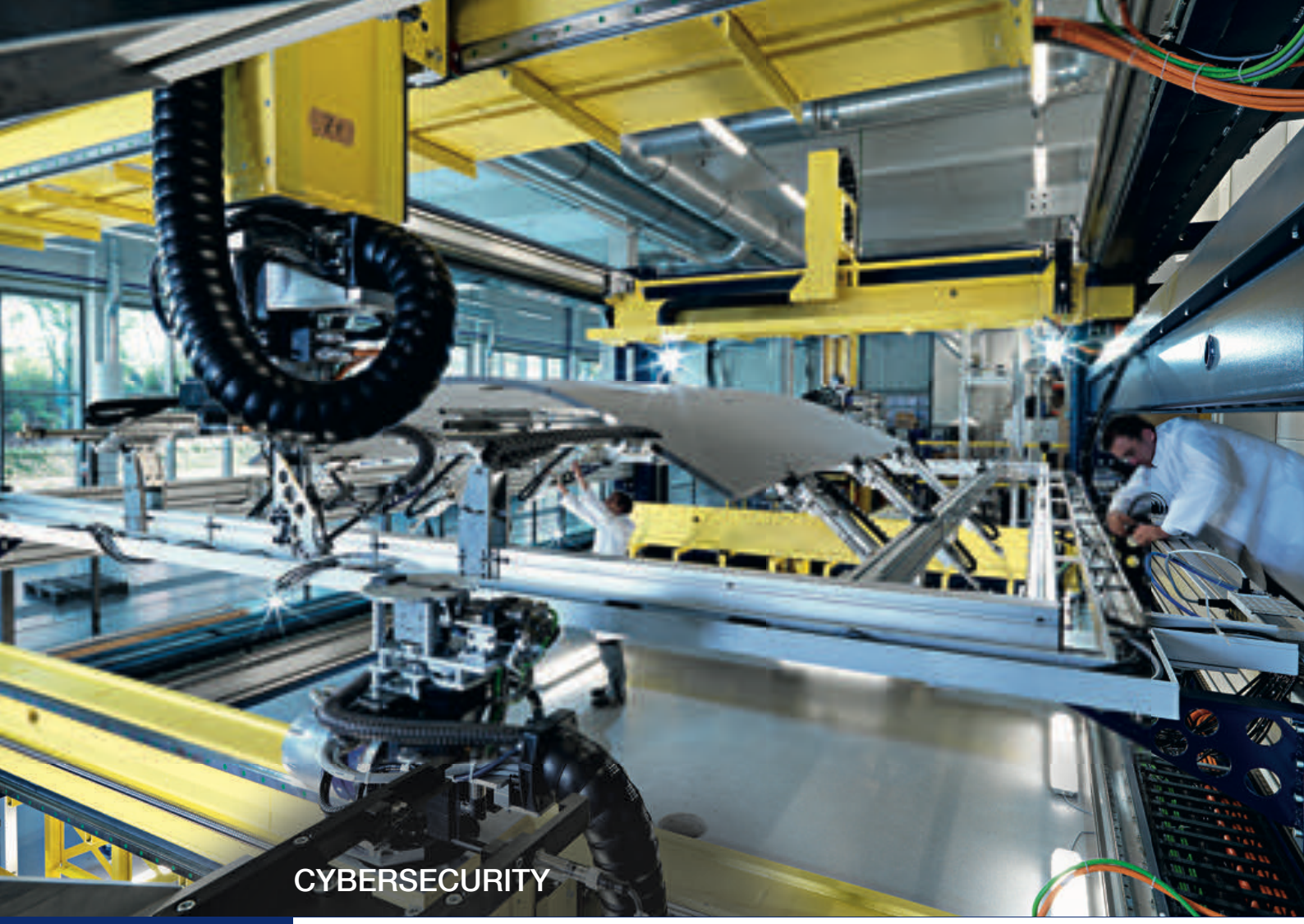

CYBERSECURITY

OT Security Services and Solutions

We help you better secure your OT environment and reduce complexity so that you can focus on your core tasks!

Digitalisation is increasing the efficiency of production and control systems by driving direct communication between areas that were historically unconnected. We now see increasing levels of network connectivity on automated industrial production and control systems throughout the supply chain. This can lead to significant cost reductions and competitive advantages.

However, OT systems are exposed to the threat of cyber attacks. OT industrial networks and ICS components are increasingly the focus of attackers, as they are inherently less protected than IT systems.

Based on our experience, we at Airbus CyberSecurity are convinced that a secure environment is key to efficient production and innovation. We offer various modular services and solutions to better protect critical infrastructures and industrial equipment; these services and solutions have proven themselves in our own activities.

We divide these solutions into three areas:

- **Analyse:** Development of concrete OT security measures for your requirements based on an efficient vulnerability and risk analysis
- **Protect:** Development and implementation of a tailor-made OT cyber security solution
- **Manage:** Continuous monitoring and updating of your security measures through our Managed Security Services.

AIRBUS

Our OT Cyber Security Services and solutions at a glance:

Phase	Service	What the service offers
Analyse	OT Asset Discovery & Analysis	• Passive, technical observation and analysis of industrial networks ✓ Overview of the components in the production network and their communications with each other ✓ Identification of anomalies and vulnerabilities ✓ Creation of a database for comprehensive risk analysis
	OT Security Maturity Check	• Compact overview of the safety level of your production systems ✓ Understanding of the current maturity level, best practice and selected standards such as IEC 62443 ✓ Creation of a database for risk analysis ✓ Identification of prioritised areas for action
	OT Security Pentesting	• Vulnerability analysis and active security testing of your industrial networks (where possible in the OT environment) ✓ Increasing awareness of the current state of protection ✓ Gaining understanding of existing vulnerabilities ✓ Verification of the measures implemented
	OT Security Risk Assessment	• Comprehensive risk assessments of industrial systems based on the likelihood of threats and their potential impact on critical business processes ✓ Comprehensive risk assessment with analysis of the impact on production and business operations ✓ Suggestions for risk reduction / treatment based on prioritisation of the identified risks ✓ Creation of a basis for decision-making based on the implementation of measures
Protect	OT Security Design	• Development of a comprehensive cyber security solution. The typical areas of focus are: · Securing and segmenting industrial networks · Securing terminals, monitoring design · OT Cyber Security Technology Evaluation (Scouting) ✓ Development of a security solution based on your customer-specific requirements, our industry-specific expertise, best practices and national / international standards
	OT Security Integration	• Implementation of OT Security solutions. The typical areas of focus are: · Carrying out a «proof of concept» with possible evaluation of 3rd party technologies · Configuration, integration, testing and validation · Operations manual & training ✓ Turnkey solution implemented for the OT area by experienced experts with current special knowledge about security solutions and technologies
	OT Security Training	• Training to establish a security organisation and increase cyber security skills. The typical areas of focus are: · Awareness Trainings · CyberRange und War Game Trainings · Presentations and live hacking ✓ Knowledge and overall understanding of security threats and possible solutions
Manage	SOC4OT	• Managed service for solution development, planning, implementation and operation of an OT Security Monitoring solution ✓ Comprehensive cyber security solution for the OT infrastructure ✓ Continuous adaptation of the solution to new safety requirements ✓ Long-term calculable costs with reduced effort
	OT Secure Remote Management	• Managed service for the acquisition, installation and operation of a remote maintenance infrastructure for your systems (including access logging, availability monitoring and reporting). Optionally with security monitoringring ✓ State of (European) technology protection according to BSI requirement / recommendation BSI CS 108 ✓ Local control by production staff without IT skills is sufficient; no specialised knowledge is required

What distinguishes us:

- Many years of experience in the implementation and operation of security solutions in sensitive areas with an agnostic approach based on best practices
- Industry-specific know-how for critical and complex infrastructures and production environments
- Comprehensive and integrated service and technology solutions from Airbus and Airbus partners, flexibly adaptable to your requirements

Our solutions are modular and can be ideally integrated into existing campaigns and ongoing measures. We would be happy to assist you with the development of new campaigns and solutions. Contact us for more information.

AIRBUS

// 1118 E 0694_1

Airbus CyberSecurity
Metapole 1, boulevard Jean Moulin / CS 40001 / 78996 Elancourt Cedex / France
Willy-Messerschmitt-Str. 1 / 82024 Taufkirchen / Germany
Quadrant House / Celtic Springs / Coedkernew / South Wales NP10 8FZ / United Kingdom
Etihad Towers T3 / Corniche Road, 19th floor / P.O.Box: 72186 / Abu Dhabi / United Arab Emirates
www.airbus-cyber-security.com / contact.cybersecurity@airbus.com