Industrial Security Engineering
Successfully develop secure ICS products

Increasing connectivity requires secure solutions

The automation industry is increasingly vulnerable to cyber attacks due to the rising digitisation and connectivity in the industrial sector. Hackers possess the capability to manipulate systems and processes, disrupt production or even cause catastrophic accidents.

Moreover, the EU law on cyber resilience, the Cyber Resilience Act (CRA), requires manufacturers to have a secure product and development life cycle, fulfil cyber security requirements and continuous vulnerability management.

Our Industrial Security Engineering services offer comprehensive solutions to protect your control units and systems from cyber attacks and to develop them in compliance with the CRA. We provide you with professional and efficient support on the path to CRA compliance for your Industrial Control Systems (ICS) products, taking into account industrial security standards in accordance with IEC 62443. This allows you to avoid additional costs from the very beginning resulting from subsequent modifications.

achelos has many years of experience in the development and evaluation of secure software. With the assistance of our specialists, you can guarantee the integrity, availability and confidentiality of your critical data and systems.

Secure software right from the start

1. Security Requirements Engineering / TARA

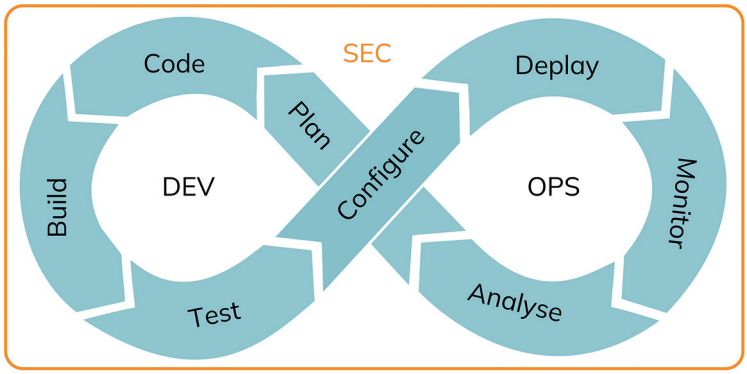
The process of developing secure software commences with a thorough risk assessment. With the aid of our security engineers, you can undertake a comprehensive threat analysis and risk assessment to proactively establish security requirements for your product. To facilitate this, we arrange and oversee security workshops, during which we identify and evaluate potential threats to the components of Industrial Control Systems (ICS). Building upon the outcomes of these workshops, we formulate security objectives and requirements for subsequent stages of the project.

2. Security Architecture Engineering

Our security engineers are with you every step of the development process. They delineate security requirements and work alongside you to construct security architectures, serving as the primary liaison for your development team. Naturally, relevant standards such as IEC 62443 are considered throughout.

3. Embedded Security Engineering

Would you like to ensure the security of the update and boot processes for your ICS components? We work with you as a development partner to integrate cybersecurity and cryptographic functions, particularly within embedded Secure Elements (eSE) and Hardware Security Modules (HSM). This ensures that your manufactured ICS components are safeguarded against cyber attacks and can attain certification in accordance with IEC 62443.



Security Engineering by achelos

Plan
- Security Requirements Engineering / TARA
- Security Architecture Engineering

Code & Build
- Embedded Security Engineering

Test
- TLS Inspector for ICS
- Security Testing for ICS

Configure
- Security Evaluation & Certification Support

4. Security Testing

achelos provides tailored testing services and robust testing tools to assess your new ICS products for security and compliance with IEC 62443 and individual security requirements, irrespective of the manufacturer.

achelos offers support in the following areas:
- Functional check & conformity tests
- Robustness tests of security functions
- Code analysis
- Vulnerability analysis
- Penetration tests

5. Security Evaluation & Certification Support

Drawing upon our extensive experience in evaluating high-security products in alignment with Common Criteria and other established security standards for test centres and manufacturers.
We offer our expertise to your advantage: achelos assists you in saving time and money on product evaluations conforming to IEC 62443 while circumventing the substantial costs associated with subsequent customisation.

Your benefits

Secure products – Develop and provide secure products devoid of vulnerabilities, resilient against attacks and other security threats.

Future-proof – Seamless integration of cybersecurity into your development process.

Risk minimisation – Secure software development from inception, aligning with BSI requirements and ready for certification if required.

Efficiency – Prevent high costs and time spent on subsequent vulnerability mitigation.

Secure products	Risk minimisation
Future-proof	Efficiency

achelos GmbH Vattmannstraße 1 33100 Paderborn Deutschland T +49 5251 14212-0 info@achelos.de www.achelos.de