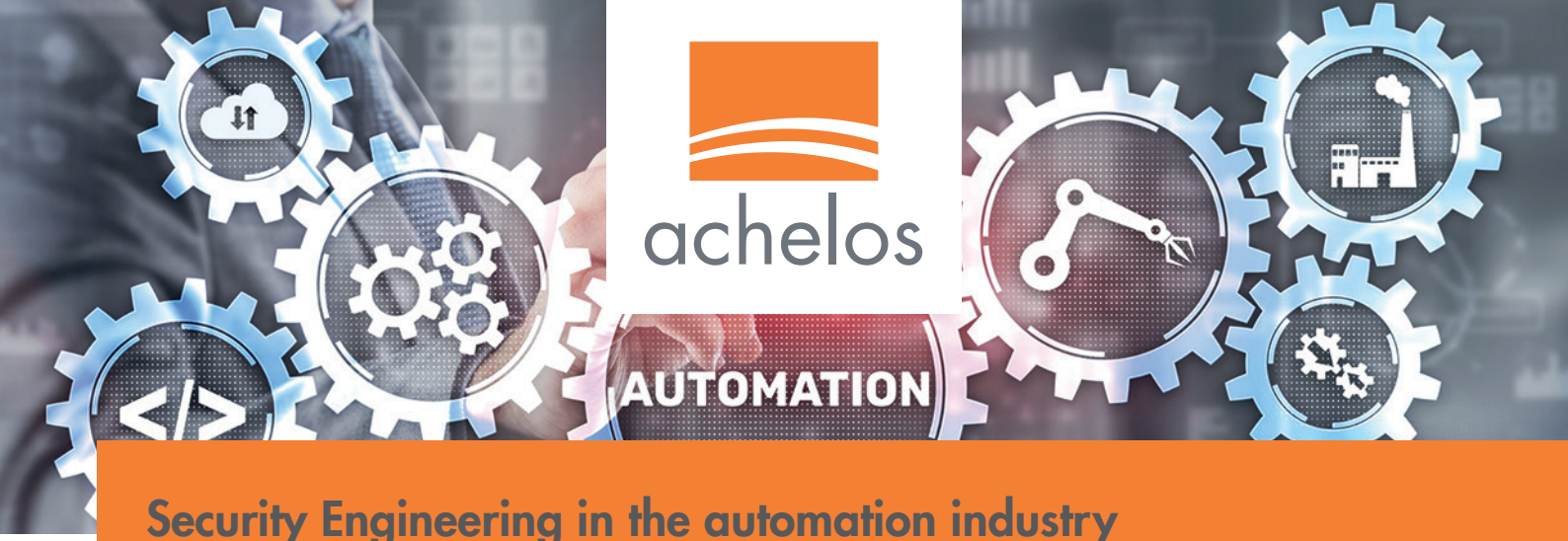


Security Engineering in the automation industry
Successfully develop secure ICS Products

Security Engineering by achelos

Increasing connectivity requires secure solutions

Commercial enterprises are today in the process of implementing digitalisation and Industry 4.0, so cyber security is currently right at the top of their agenda. Cyber attacks are currently considered the greatest business risk being faced by companies throughout the world.

Digital, connected manufacturing and cyber security come together at a whole new security level in the automation industry. The market is demanding secure products and solutions that can reliably fend off hacker attacks and come with verified security, for example in the form of safety certification according to IEC 62443.

achelos has many years of experience in the development and evaluation of secure software. We have profound cryptographic expertise and specialist knowledge of embedded systems for all project phases. Our clients benefit from significant time and money savings here, helping them avoid high costs for subsequent modifications.

The team of experts at achelos provides you with professional and efficient support throughout the entire evaluation and development process.

Secure software from the outset

1. Security Requirements Engineering / TARA

Developing secure software starts with a risk assessment. Our security engineers support you in performing this risk assessment and also a threat analysis, thereby facilitating proactive specification of security requirements for your product.

For this, we organise security workshops, to identify and evaluate potential threats to the components of industrial control systems (ICS). Based on the results of the workshops, we then define security objectives and requirements for ongoing project work.

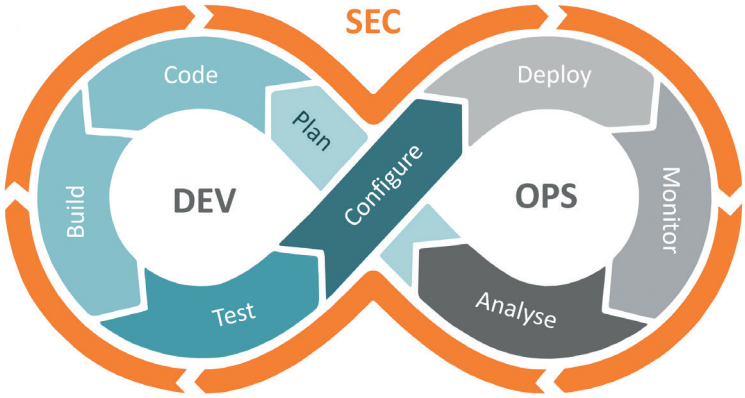
2. Security Architecture Engineering

Our security engineers accompany you throughout the entire development process. They examine security requirements, work with you to develop security architectures and are the central contacts for any product security-related issues and questions your team of developers may have. Relevant standards such as IEC 62443 are obviously observed here.

3. Embedded Security Engineering

Would you like to make the update and boot processes of your ICS components more secure? As your development partner, we support you in implementing cyber security and cryptographic functions, in particular in embedded Secure Elements (eSE) and hardware security modules (HSM). This ensures that the ICS components you produce are protected from cyber attacks and are certifiable under IEC 62443.

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

Security Engineering by achelos

4. Security Testing

achelos offers individual testing services, as well as high performance testing tools for manufacturer-independent testing of your new ICS products for security and conformity with IEC 62443, as well as individual security requirements.

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

5. Security Evaluation & Certification Support

As your competent partner, we use all the experience we have gained from collaborating with both testing centres and manufacturers on Common Criteria evaluations and other established safety standards for high-security products.

Benefit from our expertise: When performing product evaluations as per IEC 62443, achelos helps save you both time and money, as well as avoid the high costs associated with subsequent adaptations.

Your benefits

Secure products – Develop and provision of secure products without vulnerabilities that are resistant to attacks and other security threats.

Future-proof – Efficient integration of cyber security into your development process.

Risk minimisation – Secure software development from the outset, suitable for meeting the requirements of the German Federal Office for Information Security (BSI) and, where applicable, also for certification.

Efficiency – Avoid high costs and time spent on subsequent identification and elimination of vulnerabilities.

Secure products	Risk minimization
Future-proof	Efficiency

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

Integriertes Managementsystem ISO 9001 ISO/IEC 27001

Allianz für Cyber-Sicherheit Partner

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