



Industrial Security Engineering

Erfolgreich sichere ICS Produkte entwickeln

Zunehmende Vernetzung fordert sichere Lösungen

Die zunehmende Digitalisierung und Vernetzung in der Industrie macht die Automationsindustrie immer anfälliger für Cyberangriffe. Systeme und Prozesse können durch Hacker manipuliert, Produktionen gestoppt oder sogar gefährliche Unfälle verursacht werden.

Zudem verlangt das EU-Gesetz über Cyberresilienz, der Cyber Resilience Act (CRA), von den Herstellern einen sicheren Produkt- und Entwicklungslebenszyklus, die Erfüllung von Cybersicherheitsanforderungen und ein kontinuierliches Schwachstellenmanagement.

Unsere Dienstleistungen im Industrial Security Engineering bieten umfassende Lösungen, um Ihre Steuergeräte und Systeme vor Cyberangriffen zu schützen und konform zum CRA zu entwickeln. Wir begleiten Sie professionell und effizient auf dem Weg zur CRA Compliance Ihrer ICS-Produkte unter Berücksichtigung industrieller Sicherheitsstandards gemäß IEC 62443. Damit vermeiden Sie von Anfang an zusätzliche Aufwände für nachträgliche Anpassungen.

achelos hat langjährige Erfahrung in der Entwicklung und Evaluierung sicherer Software. Unsere Expert:innen unterstützen Sie dabei, die Integrität, Verfügbarkeit und Vertraulichkeit Ihrer kritischen Daten und Systeme sicherzustellen.

Sichere Software von Anfang an

1. Security Requirements Engineering / TARA

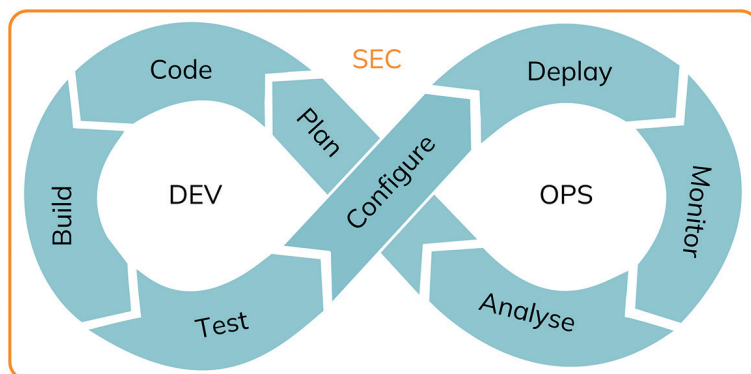
Die Entwicklung einer sicheren Software beginnt bei der Risikobewertung. Unsere Security Engineers unterstützen Sie bei der Bedrohungsanalyse und der Risikobewertung, um Sicherheitsanforderungen für Ihr Produkt spezifizieren zu können. Dazu planen und moderieren wir Sicherheits-Workshops und identifizieren und bewerten mögliche Bedrohungen für Komponenten von Industrial Control Systems (ICS). Auf Basis der Workshop-Ergebnisse definieren wir Sicherheitsziele und -anforderungen für die weitere Projektarbeit.

2. Security Architecture Engineering

Unsere Security Engineers begleiten Sie im gesamten Entwicklungsprozess. Sie nehmen Sicherheitsanforderungen auf, entwickeln mit Ihnen gemeinsam Sicherheitsarchitekturen und sind zentraler Ansprechpartner für Ihr Entwicklungsteam. Relevante Standards wie die IEC 62443 werden dabei selbstverständlich berücksichtigt.

3. Embedded Security Engineering

Sie möchten die Update- und Boot-Prozesse Ihrer ICS-Komponenten sicher gestalten? Als Entwicklungspartner unterstützen wir Sie bei der Implementierung von Cybersicherheit und kryptographischen Funktionen, insbesondere in embedded Secure Elements (eSE) und in Hardware Security Modules (HSM). So sind ihre hergestellten ICS-Komponenten vor Cyberattacken geschützt und im Rahmen von IEC 62443 zertifizierbar.



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 bietet individuelle Testdienstleistungen sowie leistungsfähige Testwerkzeuge, um Ihre neuen ICS-Produkte herstellerunabhängig auf Sicherheit und Konformität mit der IEC 62443 und individuellen Sicherheitsanforderungen zu testen.

Dabei unterstützt achelos in den folgenden Disziplinen:

- Funktionsprüfung & Konformitätstests
- Robustheitstests von Sicherheitsfunktionen
- Code-Analyse
- Schwachstellenanalyse
- Penetrationstests

5. Security Evaluation & Certification Support

Als Ihr kompetenter Partner bringen wir unsere Erfahrungen aus der Mitarbeit an Evaluierungen von Hochsicherheitsprodukten nach Common Criteria und anderen etablierten Sicherheitsstandards für Prüfstellen als auch für Hersteller ein.

Profitieren Sie von unserer Expertise: Bei Produkt-Evaluierungen nach IEC 62443 sparen Sie mit der Hilfe von achelos Kosten und Zeit und vermeiden hohe Aufwände für eine spätere Anpassung.

Ihre Vorteile

Sichere Produkte – Entwicklung und Angebot sicherer Produkte ohne Schwachstellen, die gegen Angriffe und andere Sicherheitsbedrohungen resistent sind.

Zukunftssicher – Effiziente Integration von Cybersicherheit in Ihren Entwicklungsprozess.

Risikominimierung – Sichere Softwareentwicklung von Anfang an, für BSI-Anforderungen geeignet und bei Bedarf zertifizierungsfähig.

Effizienz – Vermeidung von hohen Kosten und Zeitaufwand für die nachträgliche Beseitigung von Schwachstellen.

Sichere Produkte

Risikominimierung

Zukunftssicher

Effizienz