SCHRAML

SCHRAML Sicherheit

Informationssicherheit
IT-Sicherheit
Cybersicherheit
Ausfallsicherheit

mehr Informationen:

Sicherheit by Design & by Default für kritische Infrastrukturen

In einer Zeit zunehmender IT-Sicherheits- und Cyberbedrohungen ist es entscheidend, dass sicherheitsrelevante kritische Infrastrukturen auf robuste, verlässliche und überprüfbare Schutzmechanismen setzen.

Genau hier setzen wir an: Auf den folgenden Seiten zeigen wir Ihnen übersichtlich alle IT-Sicherheits- und Cybersicherheits-Features, die ab AQASYS 12 in vollem Umfang zur Verfügung stehen.

Die Systemlösungen von SCHRAML folgen dem konsequenten Prinzip Security by Design und Security by Default. Durch die Umsetzung zentraler Sicherheitsprinzipien – darunter Rechtemanagement nach dem Least-Privilege-Ansatz, Segmentierung von Netzen, stringente Kryptographie sowie Mechanismen für Betriebssicherheit und Kontinuität – unterstützen wir Betreiber von KRITIS-Anlagen und Unternehmen, die unter NIS-2 fallen, wirksam bei der Erfüllung ihrer Informations- und Cybersicherheitsanforderungen.

KRITIS-Betreiber, die ihre Informationssicherheitsstrategie an der ISO 27001:2022 ausrichten oder diese Norm einführen möchten, profitieren ebenfalls:
Dank integrierter Sicherheitsfunktionen wie granularen Berechtigungskonzepten, sicherer Kommunikationsstandards, verschlüsselter Datenübertragung, sicherheitsorientierter Systemhärtung und klar definierten Update- und Backup-Prozessen bieten unsere Produkte eine solide technische Basis, um zentrale Anforderungen der Norm zu unterstützen und verlässlich im täglichen Betrieb umzusetzen. Dabei gilt: Nachhaltige Informationssicherheit entsteht nicht allein durch leistungsfähige Technologien.

Neben den technischen Maßnahmen sind organisatorische Maßnahmen auf Unternehmensebene unverzichtbar – etwa klare Rollen und Verantwortlichkeiten, Richtlinien für den sicheren Betrieb, ein systematisches Risikomanagement, kontinuierliche Sensibilisierung der Mitarbeitenden sowie ein gelebter Verbesserungsprozess.

Gemeinsam schaffen wir ein **ganzheitliches Sicherheitsniveau**, das den steigenden regulatorischen Anforderungen um **NIS-2** und dem **Cyber Resilience Act** (CRA) gerecht wird, resilient gegenüber aktuellen Bedrohungen bleibt und Ihre betrieblichen Abläufe nachhaltig stärkt. Als Hersteller dokumentieren wir unsere Compliance nach **IEC 62443-4-2** und unterhalten ein **ISMS** nach **ISO 27001:2022**.

ARCHITEKTUR & NETZWERKSICHERHEIT

Zero-Trust-Architektur und Zero-Inbound-Prinzip | Fernwirken, IoT via Internet (DSL, Mobilfunk)

- Keine offenen Ports am zentralen Netzwerk erforderlich
- Alle Fernwirkstationen initiieren ausgehende Verbindungen („Call-Home“)
- Internet-Kommunikation ausschließlich über deutsche, redundante IoT-Sicherheits-Gateways
- Vorteil: Externe Angriffsvektoren werden strukturell eliminiert

Netzwerksegmentierung

- MIP Sicherheits-Server mit physisch getrennten Ethernet-Schnittstellen
- Strikte Trennung zwischen Büro-/PLS-Ebene und Automatisierungsebene
- Keine direkte Verbindung zwischen Fernwirkstationen und Kernnetzwerken
- Malware-Barriere: Kompromittierung einer Ebene gefährdet nicht die andere

Verschlüsselung & Authentifizierung

- Web/App Server
  - Zertifikatsbasierte Verschlüsselung
  - Automatische Aktualisierung via Let’s Encrypt Zertifizierungsstelle
- Server & Desktop Client
  - Anlagenspezifische Zertifikate
  - Höchste Sicherheit im internen Netzwerk
- MIP SCHRAML IoT-Sicherheits-Gateways: Durchgängig mit Geräte- und anlagenspezifischem SSL/TLS verschlüsselt
- X.509-Zertifikate für alle Verbindungen zur Fernwirkstation und SPS Steuerung optional umsetzbar
- Unterstützung für SFTP und FTPS

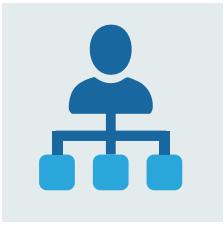
SCHRAML AQASYS und Fernwirk-Lösungen sind flexibel einsetzbar:

Ob als **Cloud- bzw. Cloud-Portal-Lösung**, in einer robusten **Hybrid-Cloud-Architektur** oder vollständig **On-Premise** – wir unterstützen das passende Deployment-Modell für Ihre Sicherheits- und Compliance-Anforderung. Das gilt auch für die Nutzung von **VMs** sowie die Integration in **DMZs** und segmentierte Netzwerkarchitekturen.

ZUGRIFFSKONTROLLE & AUTHENTIFIZIERUNG

Authentifizierung

- Verpflichtende starke Passwortrichtlinien
- Konfigurierbare Passwort-Lebenszyklen
- 2FA/TOTP für alle Zugriffswege (Desktop, Web, Mobile)
- Argon2-Hashverfahren für Passwort-Speicherung



Rechte- und Rollenmanagement

- Granulares Berechtigungskonzept mit Rollenzuweisung
- Named User für Minimalprinzip bei Zugangsberechtigungen
- Mandantenfähigkeit, z.B. für Verbundanlagen oder auch Cloud Deployments
- Active Directory Integration verfügbar

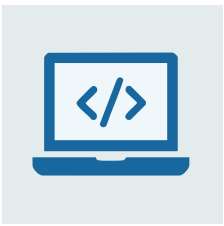
Angriffsprävention

- Brute-Force- und DDoS-Schutz durch differenzierte temporäre Account-Sperrung
- Eingabevalidierung für die Steuerungsebene
- Implementierte Schutzmechanismen gegen XSS und SQL-Injection
- Audit-Logs aller relevanten Zugriffe und Aktionen im Leitvorgangsarchiv

SYSTEM- & BETRIEBSSICHERHEIT

Gehärtete Installation

- Minimaler Software-Footprint (nur essenzielle Komponenten)
- Service-Betrieb ohne aktive Windows-Anmeldung
- Keine administrativen Rechte für Normalbetrieb erforderlich
- Keine hartcodierten Service-Zugänge



Client-Technologie

- 100% HTML5 Webclient - keine unsicheren Plugins (Java, Flash)
- Keine Remote-Desktop-Verbindungen erforderlich
- Apps für iOS und Android mit identischem Sicherheitsniveau
- Named User Lizenzen zur Sicherstellung des Systemzugriffs
  (Verhinderung gegenseitiges Aussperren durch concurrent licenses)
- Paralleler Client-Zugriff auf Desktop, Web und App möglich

MIP Sicherheits-Server (optional)

- Ausfallsicherheit durch Redundanz- und HMI Notbedienebene
- Gehärtetes Linux-System ohne Windows-Abhängigkeiten
- Keine beweglichen Teile, keine Fremdsoftware
- Entkopplung des Echtzeitbetriebs von Windows-Updates
- Robuste Hardware für 24/7-Betrieb

HOCHVERFÜGBARKEIT & DISASTER RECOVERY

Redundanz-Konzepte

- Cold-Standby, Hot-Standby oder Failover-Cluster
- Beliebige Kombination redundanter Server und MIP-Systeme
- Räumliche Trennung kritischer Komponenten möglich

Backup & Recovery

- Automatisierte Backup-Strategien
- Schnelle Wiederherstellung ohne Datenverlust

Monitoring

- Kontinuierliche Systemüberwachung
- Echtzeit-Kennwerte und Alarme
- Admin-Dashboard für das Management aktiver Verbindungen

COMPLIANCE & STANDARDS

Normkonformität

- IEC 62443-4-2 Compliance dokumentiert
- ISO 27001/27002 kompatible Sicherheitsarchitektur
- Vorbereitet für NIS-2 und CRA (Cyber Resilience Act)

Dokumentation & Transparenz

- Vollständige SBOM (Software Bill of Materials) verfügbar
- Kontinuierliche Vulnerability-Analyse
- Durchführung und Dokumentation von Penetrationstests
- Transparente Release Notes nach Typ und Kritikalität

Die SCHRAML **Automations-** und **Konnektivitätslösungen** basieren auf etablierten Standards und nutzen **sichere** Kommunikation – etwa durch verschlüsselte und authentifizierte Datenübertragung via **OPC UA** oder **REST-API**.

Technologie für eine nachhaltige Zukunft des Wassers

SCHRAML hat sich seit über 35 Jahren ganz auf Wasser- und Abwasserbetriebe, auf Umweltwirtschaft und Infrastrukturanlagen spezialisiert. Als familiengeführtes Unternehmen ist es unsere Mission, Lösungen für eine hoch effiziente Trinkwasserversorgung sowie energie- und umweltschonende Abwasserbehandlung zu entwickeln. Damit tragen wir zu einem nachhaltigen Einsatz der kostbaren Ressource Wasser und zum Schutz von Umwelt und Mensch bei.

Mit SCHRAML Technik lassen sich Schlagworte wie "Industrie 4.0" oder "Internet of Things" auf die Wasser- und Abwasserwirtschaft übertragen. Unsere Produkte bieten den Anlagenbetreibern Arbeitserleichterungen und Optimierungsmöglichkeiten in alltäglichen Prozessen - sozusagen "Wasser 4.0". Denn die SCHRAML Systeme erfassen, verdichten und analysieren große Datenmengen aus Anlagen und Wassernetzen und bilden damit die Grundlage für ein intelligentes, energieoptimiertes Wassermanagement und für innovative Steuerungsoptionen für die Wassergewinnung, die Aufbereitung, Reinigung und Verteilung von Wasser- und Abwasserströmen.

Prozessleittechnik | SCADA | IoT Fernwirken | Automation

SCHRAML GmbH

Herxheimer Straße 7
D - 83620 Vagen
+49 (0) 8062 7071-0
info@schraml.de

www.schraml.de

SCHRAML
schraml_team
SCHRAML GmbH