



## SCHRAML Sicherheit

**Rundum sicher:  
IT-Sicherheit  
Informationssicherheit  
Ausfallsicherheit**

SCHRAML digitalisiert die Wasser- und Umweltwirtschaft und das seit jeher mit einem besonderen Augenmerk auf alle relevanten Themen der Informationssicherheit.

Sowohl die Prozessleittechnik als auch die IoT-Fernwirktechnik erfüllen dabei mit zahlreichen Eigenschaften die **strengen Anforderungen**, die heute an die Systeme von **KRITIS Unternehmen** gestellt werden. Wir stehen dabei im Dialog mit allen Akteuren, die sich für die sichere Umsetzung von KRITIS Infrastrukturen einsetzen. Wir begrüßen die Entwicklung von Sicherheitsstandards und die in den Arbeitsgruppen der DWA und DVGW in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnologie (BSI) ausgearbeiteten Operationalisierungsempfehlungen im IT-Sicherheitsleitfaden zum Branchenspezifischen Sicherheitsstandard Wasser/Abwasser (B3S WA 2021).

Auch die neueste Version 2021 3.0 beinhaltet im IT-Sicherheitsleitfaden zahlreiche Ergänzungen um relevante Themen zum Einsatz von z.B. **sicheren IoT Anwendungen** oder dem Thema **Fernkommunikation bzw. Datenverbindungen über externe Netzwerke**. Sicherheitsthemen, die wir sofern möglich bereits in unserer Produktentwicklung erfolgreich adressieren.

Neben technischen Maßnahmen stehen auch **organisatorische Maßnahmen** im Zentrum erfolgreicher IT- und Informationssicherheitsanstrengungen. Natürlich bei den Betreibern, aber auch bei den Herstellern. Daher ist SCHRAML seit 2021 erfolgreich **nach ISO 27001** zertifiziert und ergänzt damit die vorhandenen Zertifizierungen im Bereich des Qualitätsmanagements (ISO 9001), des Energiemanagements (ISO 50001) und des Umweltschutzes (ISO 14001) um den Nachweis für ein **nachhaltig eingerichtetes Informationssicherheits-Management-System**.



SCHRAML  
ISO 27001  
Zertifikat



## System- und Sicherheitsinfrastruktur

Wie passt AQASYs zu Ihren Sicherheitsanforderungen?

Das AQASYs Prozessleitsystem ist für den Betrieb **innerhalb einer gesicherten IT-Infrastruktur** geeignet. Die Software- und Sicherheitsarchitektur des Prozessleitsystems schränkt generelle IT-Sicherheitsmaßnahmen nicht ein.

AQASYs ist mit IT-Sicherheitskomponenten wie **Firewalls, DMZs, IPCs oder Antiviren-Software** kompatibel und bietet verschiedene Sicherheitsmechanismen, die diese Basisschutzmaßnahmen verstärken.

AQASYs kann auch in **virtuellen Umgebungen** eingesetzt werden und ist als **lokal installierte on-premise Lösung** oder als **SaaS/PaaS-Lösung aus der Cloud** verfügbar.



## Ausfallsicherheit | Hochverfügbarkeit

Wie unterstützt AQASYs einen unterbrechungsfreien Betrieb?

Ein redundanter Betrieb des Systems sowohl als **Cold-Standby-, Hot Standby-Lösung oder als Failover-Cluster in virtuellen Umgebungen** ist möglich.

Zur Vermeidung hoher Aufwände für das Einrichten und den Betrieb redundanter Server ist es zugleich möglich, mit dem **Sicherheits-Server MIP 49x/58x** eine hohe Ausfallsicherheit über eine **programmatische und räumliche Trennung des prozesskritischen Echtzeitbetriebs** (inklusive Fernalarmierung und Datenzwischenspeicherung über mehrere Tage) und des Anwendungs- und Datenservers zu realisieren.

Über den **robusten und energieeffizienten MIP Sicherheits-Server** von SCHRAML (ohne bewegte Teile, ohne Fremdsoftware, gehärtetes Linux Betriebssystem, kein Windows) und dessen Software kann sichergestellt werden, dass alle Überwachungs-, Alarmierungs-, Bedien- und Steuerfunktionen des Leitsystems auch dann zuverlässig genutzt werden können, wenn der Prozessleit-Server/Rechner, beispielsweise beim Installieren von Windows Updates oder bei einem Ausfall, nicht zur Verfügung steht.



**Redundanzsystem mit MIP Sicherheits-Server:**  
Einfach einzurichten, äußerst robust und zuverlässig bei Nichtverfügbarkeit des PLS-Rechners

Darüber hinaus sind weitreichende Möglichkeiten zur **Eigenüberwachung des Systems** implementiert, d.h. Systemkennwerte werden aufgezeichnet und überwacht. Das System unterstützt **automatische Backups** und einfache Prozeduren zu seiner vollständigen Wiederherstellung.

Ebenso ist eine **beliebige Kombination aus redundanten Servern und redundanten MIP Sicherheits-Servern** als Hot Standby-Lösung möglich, bei der automatisch der Ausfall der jeweiligen Komponente vom System erkannt und auf die entsprechende Ersatzkomponente übergeben wird.



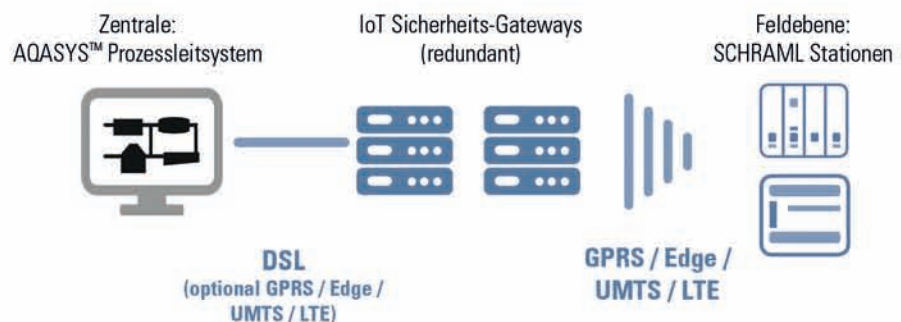
## Sichere Fernwirktechnik: Keine eingehenden Verbindungen am zentralen Netzwerk

Wie kann sicheres Fernwirken realisiert werden?

Für einen optimalen Schutz vor unbefugten Angriffen des Systems und dessen Netzwerk werden **eingehende Verbindungen** für die Fernwirkkommunikation **am zentralen PLS-Netzwerk ausgeschlossen**. Dies ist ein einfacher – aber zugleich mächtiger – Mechanismus, der das Netzwerk in der Zentrale maßgeblich schützt.

Auch bei Fernwirkverbindungen über das Internet oder den Mobilfunk - also z.B. DSL, LTE, GPRS - ermöglicht das SCHRAML System die Einrichtung der Firewall so, dass **alle eingehenden Kommunikationen abgeblockt** werden. Dadurch werden externe Angriffe unterbunden und ein Eindringen von Unbefugten wird verhindert. **Dies ist auch ohne Umsetzung und Konfiguration eines VPN-Netzes möglich**, was einen wichtigen Unterschied des SCHRAML Prozessleit- und Fernwirksystems gegenüber anderen Anbietern darstellt.

DSL- und Mobilfunk- (z.B. LTE/GPRS) Stationen kommunizieren zeit- und ereignisgesteuert **über IoT-Sicherheits-Gateways**, die von SCHRAML an unterschiedlichen Standorten innerhalb Deutschlands betrieben werden. Somit ist eine Portfreigabe für eingehende Daten und für eingehende VPN-Verbindungen von den Fernwirkstationen am zentralen PLS-Netzwerk nicht erforderlich (geschlossenes Einfallstor), womit ein hoher Schutz vor unbefugten Angriffen erzielt wird. Die IoT Sicherheits-Gateways sind **für eine hohe Ausfallsicherheit redundant ausgelegt** und mit allen erforderlichen IT-Schutzmaßnahmen abgesichert. Eine latenzminimierte und volumenreduzierte Fernwirk-Kommunikation ist dabei grundlegende Voraussetzung.



Die SCHRAML Fernwirkstationen sind Embedded IoT-Komponenten **mit gehärtetem Linux und umfangreichen Sicherheitsfeatures**.



## Schutz der Automatisierungsebene: Netzwerktrennung und -segmentierung

Wie kann eine Kompromittierung der Automationssebene verhindert werden?

Zum Schutz der Anlagen-Automatisierung verfügt der MIP Sicherheits-Server über eine **intelligente Netzwerksegmentierung und zwei getrennte Ethernet-Schnittstellen**, die für die netzwerktechnische Trennung von Büro-/PLS-Ebene und Automatisierungs-Ebene sorgen. Durch die strikte Netzwerktrennung des MIP Sicherheits-Servers kann sich Schadsoftware vom Büronetzwerk nicht in das Automatisierungsnetzwerk ausbreiten und die Anlagensteuerung nicht angreifen.

Es gibt **keine direkte Netzwerkverbindung** zwischen den Fernwirkstationsnetzwerken und dem zentralen Automatisierungsnetzwerk, d.h. die Fernwirkstationen sind so nicht Teil des Automatisierungsnetzwerkes, insbesondere auch nicht über VPN-Verbindungen. Somit kann ein unbefugtes Eindringen über kompromittierte Außenstationen in die komplette Anlage verhindert werden.



Zusätzlich sind die Kommunikation und der Datenverkehr zwischen den Leitsystemkomponenten und dem MIP Sicherheits-Server **per Standard verschlüsselt (SSL/TLS) und mit Zertifikaten authentifiziert** – optional mit Anlagen- und Geräte-spezifischen Zertifikaten.



## Sichere Nutzung von Webclient und App

Wie erfolgt der sichere Zugriff aus der Ferne?

Der AQASYS Webclient und die AQASYS App (für Android und iOS) bieten auf Basis modernster Webtechnologie sichere Systemzugriffe – sowohl für den schnellen und mobilen Anlagencheck in der Bereitschaft, als auch für die umfassende Anlagen-Überwachung, -Steuerung und -Analyse.

- Die Verbindungen von Webclient und App zum PLS-Server sind **SSL/TLS verschlüsselt** und nutzen Zertifikate zur Authentifizierung.
- Das Login erfordert eine **hohe Passwortstärke** und kann optional mit reCAPTCHA und **2-Faktor-Authentifizierung** weiter abgesichert werden.
- Es erfolgt eine **automatische Synchronisation der Benutzer- und Rechteverwaltung** über PC, App, Webclient (und HMI) hinweg.
- Nachvollziehbarkeit durch eine vollständige **Dokumentation der Benutzeraktionen** im Webclient und in der App im Leitvorgangarchiv
- Zusätzlich lassen sich **VPN-Verbindungen** nutzen.
- Admins können **aktive Online-Verbindungen überwachen** und managen.
- Der Status des Systems ist überwach- und auslesbar.
- Die Verwendung von **sicherheitskritischen, permanent geöffneten Remote-Desktop-Verbindungen** entfällt.



## Verschlüsselung und Authentifizierung in der Zentrale und im Fernwirknetz

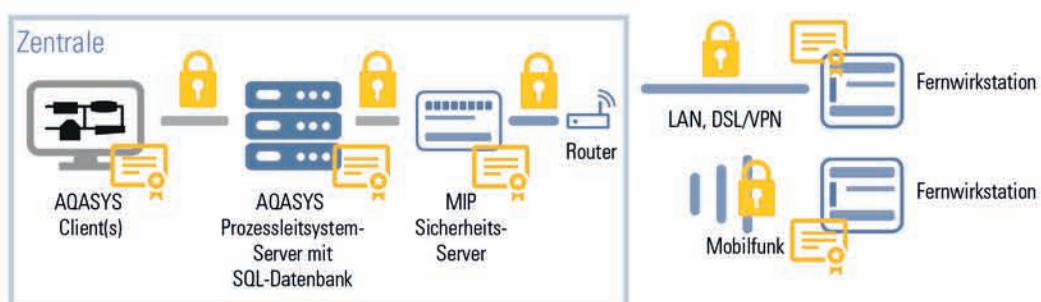
Wie unterstützt AQASYS die Vertraulichkeit von Daten?

AQASYS ermöglicht eine **durchgängige Verschlüsselung mit SSL/TLS und X.509-basierten Zertifikaten der gesamten Datenkommunikation in der Prozessleitzentrale, bis hin zu den Fernwerkstationen.**

Der Datenverkehr in der Anlagenzentrale selbst, d.h. innerhalb des ServerLANs, ist immer SSL/TLS-verschlüsselt und authentifiziert. Darüber hinaus sollte/kann die Kommunikation bis zu den Fernwerkstationen durchgängig SSL/TLS-verschlüsselt und authentifiziert werden.

Das System unterstützt außerdem **SSL/TLS-Verschlüsselung bei der Anmeldung an Mailservern** (SMTPS und POP3) und der Anbindung **externer FTP-Server**.

Zur sicheren Authentifizierung von Sender und Empfänger und damit zur Sicherstellung der Integrität der Fernwirkverbindungen müssen je nach Sicherheitslevel-Anforderung **öffentliche oder Anlagen- und Gerätespezifische Zertifikate** verwendet werden. Die Zertifikate müssen nach Ablauf oder Kompromittierung ausgetauscht werden.





## Betriebssystem und Rechtemanagement

Wie setzt AQASYs Berechtigungen um und was sind die Voraussetzungen auf Betriebssystemebene?

AQASYs setzt voraus, dass **aktuelle Microsoft Serverbetriebssysteme** zum Einsatz kommen. Das Product Lifecycle Management von SCHRAML erfasst auch Software-Patches für ältere Versionen. Die PLS-Anwendung ist auf Betriebssystemebene mit möglichst wenig aktiver Software, offenen Ports, etc. lauffähig. Ein Betrieb des Systems benötigt lediglich die Leitsystem- und Kommunikationssoftware, die Datenbank und Treiber für Hardware-Anbindungen.

Der Leitsystem-Rechner ist auch ohne aktive Windows-Anmeldung im Dienstmodus lauffähig. Das System kann von Clients auch ohne aktive Windows-Anmeldung administriert und bedient werden. AQASYs benötigt zur Ausführbarkeit keine administrativen Rechte und kann daher von einem Nutzer mit Standardrechten sicher konfiguriert und bedient werden. Ebenso ist eine uneingeschränkte Systemnutzung auch dann möglich, wenn der Nutzer aktiv in der Windows-Benutzersteuerung angemeldet ist.

Das Prozessleitsystem verfügt über ein **umfassendes Rechte- und Rollenkonzept**, das eine gruppenweite Rechtevergabe und -pflege und eine Rollenzuweisung auf Benutzerbasis ermöglicht. Lese- und Schreibrechte werden wahlweise auf Konfiguration oder auf komplette Benutzeroberflächen vergeben. Rechte können dedizierten Mandanten bzw. Anlagenteilen zugeordnet werden. **Das Rechtemanagement deckt damit auch die Anforderungen von Cloud-Systemen ab.**

Alle wichtigen Konfigurationsänderungen, Anmeldungen und Schaltvorgänge werden **im Leitvorgangsarchiv archiviert.**



## Systembedienung

Wie erfolgt der sichere Zugriff auf AQASYs für den Anwender?

Als Systemanwender haben Sie die Wahl, über einen **Desktop-Client**, einen **Webclient** oder die **AQASYs App** auf das System zuzugreifen. Die Anlage kann darüber jeweils überwacht, bedient und gesteuert werden (Lizenzoption Webclient/App). Auch Analysetools wie Berichte, Kurven und Grafiken stehen in den drei Varianten uneingeschränkt entsprechend den vergebenen Nutzerrechten zur Verfügung. Der Server unterstützt theoretisch eine unbegrenzte Anzahl an Desktop-Client-, Webclient- und App- Zugriffen.

Der Zugriff über Webclients ist **100% HTML5 konform** und rein über moderne Webbrowser möglich, d.h. ohne zusätzliche Installation oder sicherheitskritische Plugins wie Java oder Flash.

Alle möglichen Eingabedaten werden durchgängig validiert. Das System hat Methoden implementiert, die **mögliche Angriffsvektoren** wie z.B. XSS (Cross Side Scripting) oder SQL Injection **ausschließen.**

Die Berechtigungen der Systemnutzer können für den mobilen App- oder Webzugriff bei Bedarf separat spezifiziert werden.



## Systeminstallation und Datenbank

Welche Sicherheitsaspekte betreffen die Datenbank?

Das System wird mit der Installation für einen sicheren Betrieb eingerichtet. **Hartcodierte aktive Zugänge für Servicezwecke sind nicht erlaubt.** Komponenten mit direkter Internet-Anbindung müssen bereits mit der Installation gehärtet ausgeführt sein.

AQASYS wird in Verbindung mit einer **SQL Datenbank** eingesetzt. Die Datenbank muss nach aktuellen Datenbankmanagement-Sicherheitsrichtlinien betrieben werden. Der Datenzugriff erfolgt direkt auf alle archivierten Daten, ohne dass ein ausgelagerter Datenbankteil dafür wieder eingespielt werden muss.



## Loginverfahren

Wie erfolgt das sichere Login?

Unautorisierte Logins werden über Schutzkonzepte wirkungsvoll vermieden:

Es ist möglich, sich nicht nur durch Login und Passworteingabe, sondern durch **zusätzliche Zwei-Faktor Authentifizierung** (2FA, weiteres erzeugtes Einmal-Passwort) in das System einzuloggen. SCHRAML nutzt hierfür das TOTP-Verfahren – Time-based One-time Password Algorithmus. Dabei wird ein zusätzliches, zweites, temporäres Passwort verwendet, das mit einer beliebigen, kostenlosen Standard-App (Authenticator) generiert werden kann. Die Zwei-Faktor-Authentifizierung ist sowohl für den Zugriff auf den Desktop-Client, als auch auf den Webclient und die App einsetzbar und eine optional zu lizenzierende Funktion.






Zusätzliche Sicherheit über 2-Faktor-Authentifizierung

Nutzerkonten dürfen nicht mit leeren Passwortfeldern angelegt werden. **Eine Mindest-Passwortlänge und -Zeichenzusammensetzung kann festgelegt werden.** Ebenso ist es möglich, einen Passwort-Erneuerungszyklus festzulegen. Für das System-Login erfolgt eine Verschlüsselung mit dem SHA-512 Algorithmus. Die kompletten Authentifizierungsdaten werden damit vom System gehashed abgelegt, so dass kein Zurücklesen oder Kopieren möglich ist. Um sich wirkungsvoll vor Brute-Force-Login-Attacken zu schützen, wird ein Login temporär gesperrt, wenn zu viele Fehlversuche stattgefunden haben (Schutz des Webservers gegen Denial-of-Service-Attacken oder Brute-Force-Attacken). Anmeldungen und Anmeldeversuche werden durchgängig aufgezeichnet.

Die Authentifizierung am System kann auch über **Active Directory** umgesetzt werden.

SCHRAML GmbH  
Herxheimer Straße 7 | D-83620 Vagen  
www.schraml.de

T +49 (0) 8062 7071-0  
E info@schraml.de

 SCHRAML  
 schraml\_team  
 SCHRAML GmbH

# SCHRAML

