FlowChief

WAS FLOWCHIEF FÜR SIE BEWEGT

Sicher mit FlowChief

TÜVRheinland CERTIFIED ISO 50001

www.flowchief.de

ISO/IEC 27001 www.isocert.de zertifiziert

Sicher mit FlowChief

In zahlreichen Betrieben unterstützen wir die Digitalisierung von Anlagen, Maschinen und Prozessen im Bereich der Leittechnik und des Monitorings. Wir sind uns der Verantwortung bewusst, die wir gegenüber unseren Kunden tragen, die zum Großteil im Bereich der **Kritischen Infrastrukturen (KRITIS)** tätig sind. Daher legen wir besonderen Wert auf deren Sicherheitsbedürfnisse.

Wir verpflichten uns dazu, in unserem Handeln und unserem Portfolio höchste Ansprüche an Informationssicherheit, IT-Sicherheit und Ausfallsicherheit zu setzen.

Seit 2022 sind wir als Unternehmen vollumfänglich nach ISO 27001 zertifiziert. Diese gilt für **alle Abteilungen, unseren (digitalen) Dienstleistungen und unsere IT-Systeme inkl. deren Infrastrukturen und Cloud-Diensten**.

Mit der Zertifizierung zahlen wir auf das Versprechen ein, unseren Kunden ein durchgehend sicheres Produkt auf Basis einer auf Sicherheit ausgelegten Firma bieten zu können.

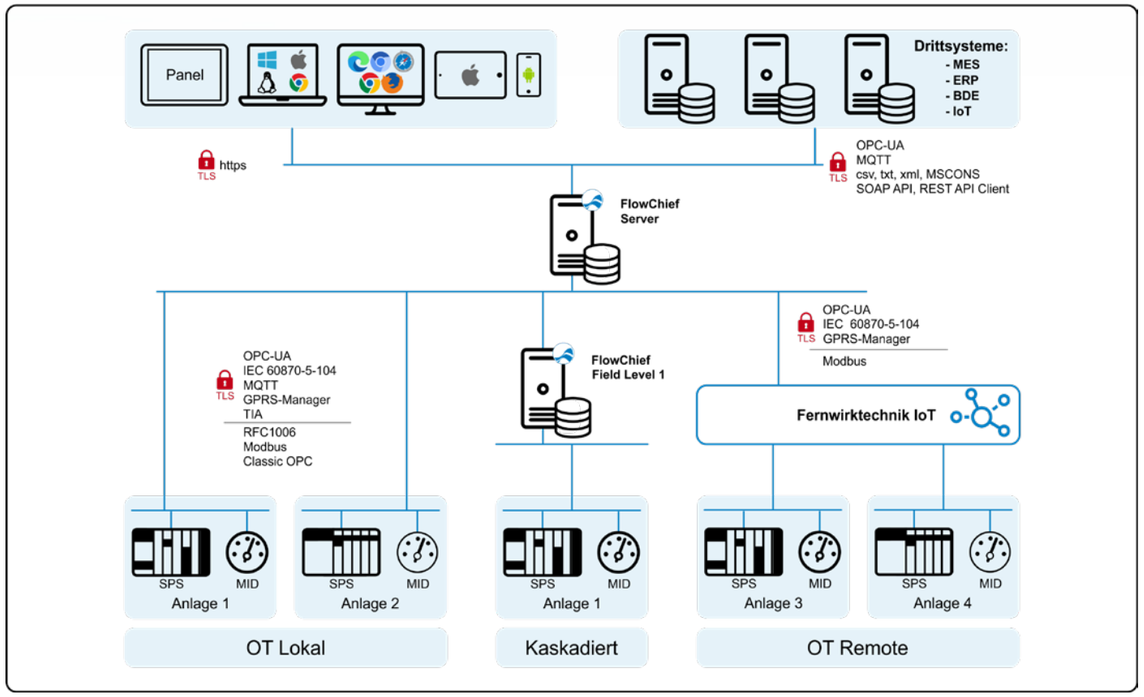
COMPLIANCE & STANDARDS

Die Normung und Compliance Vorgaben im Bereich der IT-Sicherheit nehmen stetig zu. Aufgrund der ebenfalls stetig steigenden Bedrohungslage unterstützen wir die Bestrebungen des Gesetzgebers, Sicherheitsstandards abgestimmt auf die Anforderungen der unterschiedlichen Sektoren zu etablieren.

Als Unternehmen handeln wir entsprechend den aktuellen und zukünftigen Gesetzen (u.a. **ITSig 2.0, BSI-Gesetz, KRITIS-Dachgesetz**). Unser Portfolio weist einen hohen Eignungsgrad für die Nutzung in **KRITIS-Sektoren** auf und ermöglicht die Umsetzung von Kunden-ISMS-Anforderungen oder geltenden Branchenvorgaben wie **DWA-M 1060, B3S Wasser, LSI Checkliste und Handlungsempfehlung Wasser** oder dem **BDEW-Whitepaper**.

ROBUSTE SYSTEMTOPOLOGIE FÜR JEDEN SICHERHEITSANSPRUCH UND JEDES KUNDENPROFIL

Durch eine simple und skalierbare Systemarchitektur ermöglichen wir vielfältige Lösungsansätze für verschiedenste Topologien. Dadurch gewährleisten wir eine nahtlose Integration in jede IT-Infrastruktur und eine optimale Abstimmung mit Netzwerk- und Sicherheitsinfrastrukturen wie Virtualisierung, Firewalls, VPN und Active Directory. Der Client ist der Browser – die TLS-verschlüsselte Kommunikation ist optimal für Netzübergänge geeignet und auch überwachbar. Windows-Installationen und Updates für Engineering-Arbeitsplätze und Ferneinwahlsoftware entfallen vollständig.



Sichere Kommunikation zur OT
Wir setzen auf Standards und unterstützen dabei alle gängigen Methoden der Absicherung der Verbindung. Dabei verzichten wir auf das Risiko der Zentralisierung durch Cloud Vermittlungsdiensten, und setzen auf direkte Kommunikation, Autorisierung, Verschlüsselung und VPN-Flankierung.

Ausfallsicherheit
Mit FlowChief stehen Ihnen zahlreiche Wege zur Sicherstellung eines hochverfügbaren Betriebs zur Verfügung. Von der Verteilung der Aufgaben auf verschiedene Systeme, über Applikations- und Kommunikationsredundanz bis hin zum Failover-Cluster.

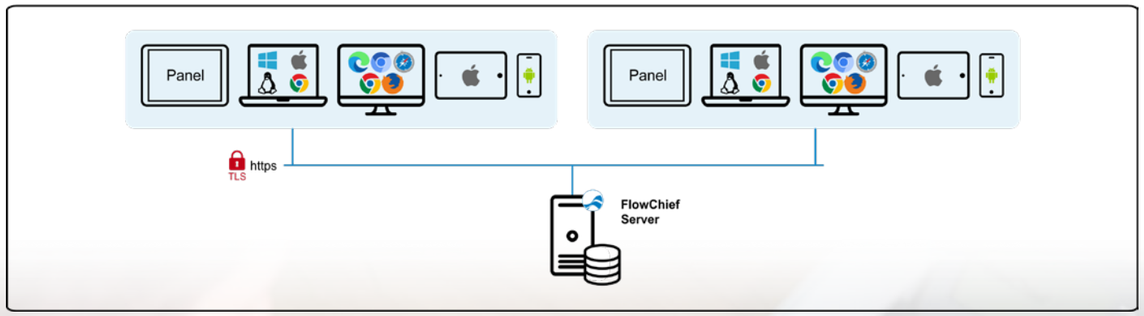
IT-OT Integration
Durch die Nutzung von Standardprotokollen wie https, OPC UA oder MQTT weist FlowChief eine hervorragende Architektur für eine harmonische IT-OT-Vernetzung auf. Wir bieten durchdachte Lösungen für ganzheitliche Netzwerksicherheit

Flexible Software-Bereitstellung
FlowChief kann in der Infrastruktur des Kunden installiert werden oder auch als Hosting-Lösung ohne eigene IT bereitgestellt werden. Zudem stehen verschiedene SaaS (-Portal) Dienste für unsere Kunden zur Verfügung.

WEBAPPLIKATION BIETEN SICHERHEITSVORTEILE GEGENÜBER PROPRIETÄREN WINDOWS APPLIKATIONEN

Webanwendungen sind einfacher zu handhaben als verteilte Windows-Installationen. Die zentralisierte Bereitstellung und die sichere Integration des HTTPS-Protokolls bilden die Grundlage für zahlreiche Vorteile:

- ***Einfache zentrale Updates***
  Webapplikationen ermöglichen eine unkomplizierte zentrale Aktualisierung, um potenzielle Schwachstellen schnell zu beseitigen
- ***Regelmäßige Sicherheitsupdates für Webbrowser***
  Durch regelmäßige Sicherheitsupdates für Webbrowser werden bekannte Schwachstellen rasch behoben, was die Sicherheit der Benutzer erheblich verbessert
- ***HTTPS-Verschlüsselung für Vertraulichkeit und Integrität***
  Die Verwendung von HTTPS-Verschlüsselung sichert die Verbindung zwischen Browser und Server ab und gewährleistet ein Höchstmaß an Vertraulichkeit und Integrität der Daten.
- ***Firewall-freundliche HTTPS-Verbindungen***
  HTTPS-Verbindungen sind Firewall-freundlich und ermöglichen eine einfache Handhabung von Zonensegmentierungen, Netzübergängen und Fernzugriffen. Verdächtige Aktivitäten können leicht per IDS, IPS oder Angriffserkennung erkannt oder verhindert werden.
- ***Skalierbarkeit ohne Sicherheitsvernachlässigung***
  Die Skalierbarkeit von Webapplikationen ermöglicht es, sich flexibel ansteigenden Benutzerzahlen anzupassen, ohne dabei die Sicherheit zu vernachlässigen.

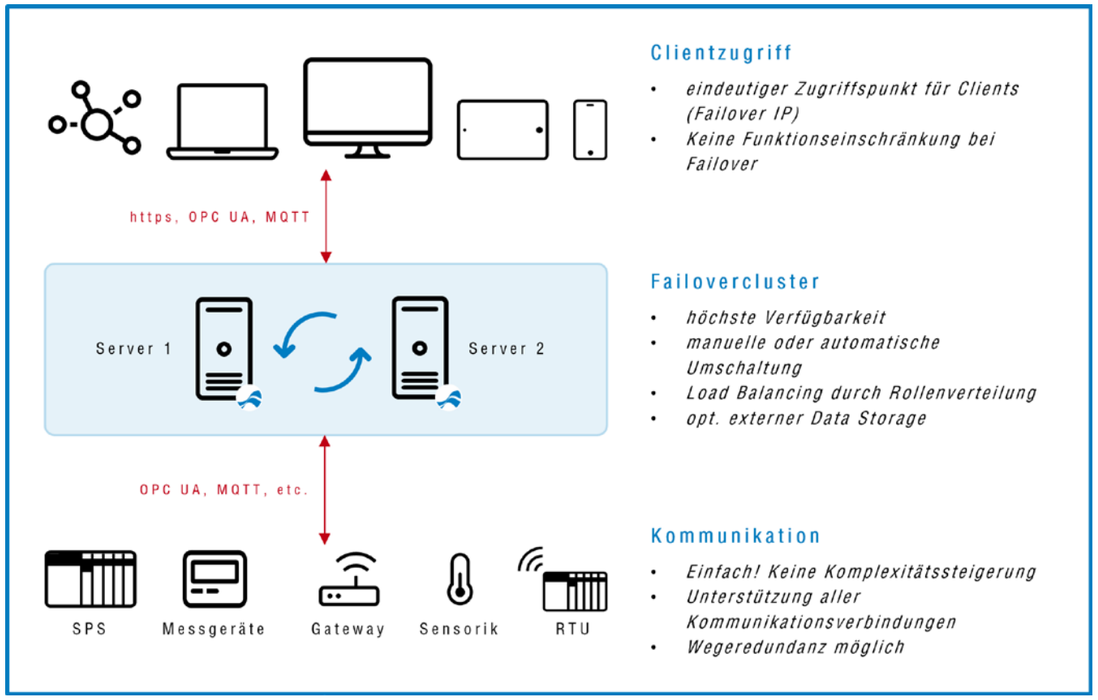


Ausfallsicherheit | Hochverfügbarkeit

FlowChief bietet eine Vielzahl von Optionen, um die Verfügbarkeit zu maximieren und Ausfallzeiten zu vermeiden oder zu minimieren:

- ***Integrierte Backup- und Recovery-Prozeduren, die an individuelle Anforderungen angepasst werden können***
- ***Regelmäßiges Sichern von Befehlen und Sollwerten in Ringpuffern mit der Möglichkeit zur Reaktivierung gespeicherter Sollwertsätze***
- ***Diverse Möglichkeiten zur Nutzung redundanter Kommunikationswege***
- ***Separierung der FlowChief-Services auf verschiedene Systeme, z.B. zentraler Datensammler und dezentrale Visualisierung***
- ***Parallele Infrastrukturen (HMI vor Ort für die ausfallsichere Bedienung zusätzlich zur zentralen Leittechnik)***
- ***Umfangreiche Eigenüberwachungsmöglichkeiten des Systems***

Mit FlowChief Redundanz werden sämtliche potenzielle Ausfallpunkte abgedeckt, sei es Netzwerk, Hardware, Betriebssystem oder FlowChief Laufzeit. Dadurch gewährleisten wir den kontinuierlichen Betrieb der gesamten Applikation, einschließlich Visualisierung, Archivierung und Alarmierung. Unsere Redundanzlösungen können als Cold- oder Hot-Standby implementiert werden, um die Verfügbarkeit der Systeme sicherzustellen. Standardisierte Microsoft-Funktionen wie Failover-Clustering, SQL-Hochverfügbarkeit oder Failover-IP sind einfach in Umsetzung und in der Anwendung. Zudem lassen sie sich optimal für jede Anlagengröße skalieren.



GESICHERTE ANBINDUNG DEZENTRALER ANLAGEN

Flexibilität: *Wir unterstützen sämtliche gängigen Übertragungsmedien (kabelgebunden und drahtlos) sowie Übertragungsprotokolle und sind kompatibel mit allen standardisierten Protokollen. Zudem ermöglichen unsere Lösungen die Interaktion mit Leittechnik von Drittanbietern.*

Kein Cloud-Vermittlungsdienst: *Unsere Lösungen funktionieren autonom, ohne die Notwendigkeit eines Cloud-Dienstes und somit ohne die damit verbundenen Risiken.*

Keine eingehenden und ausgehenden Verbindungen: *Die größte Gefahr für Netzwerke geht oft von internen Quellen aus, wie beispielsweise durch Phishing-Mails. Eine wirksame Maßnahme zur Eindämmung der Ausbreitung von Angriffen besteht darin, den aktiven Verbindungsaufbau aus dem Leitsystemnetzwerk zu blockieren. Eingehende Verbindungen können durch VPN-Flankierung vermieden werden.*

Umfassende Sicherheitsfeatures: *Wir integrieren alle gängigen Sicherheitsmechanismen in den Übertragungsprotokollen, einschließlich TLS-Verschlüsselung und Autorisierung.*

FlowChief Security Gateway: *Das FlowChief-System für dezentrale Anlagen befindet sich in einer separaten Sicherheitszone, getrennt vom zentralen Prozessleitsystem.*

FERNZUGRIFF OHNE FERNEINWAHLSOFTWARE

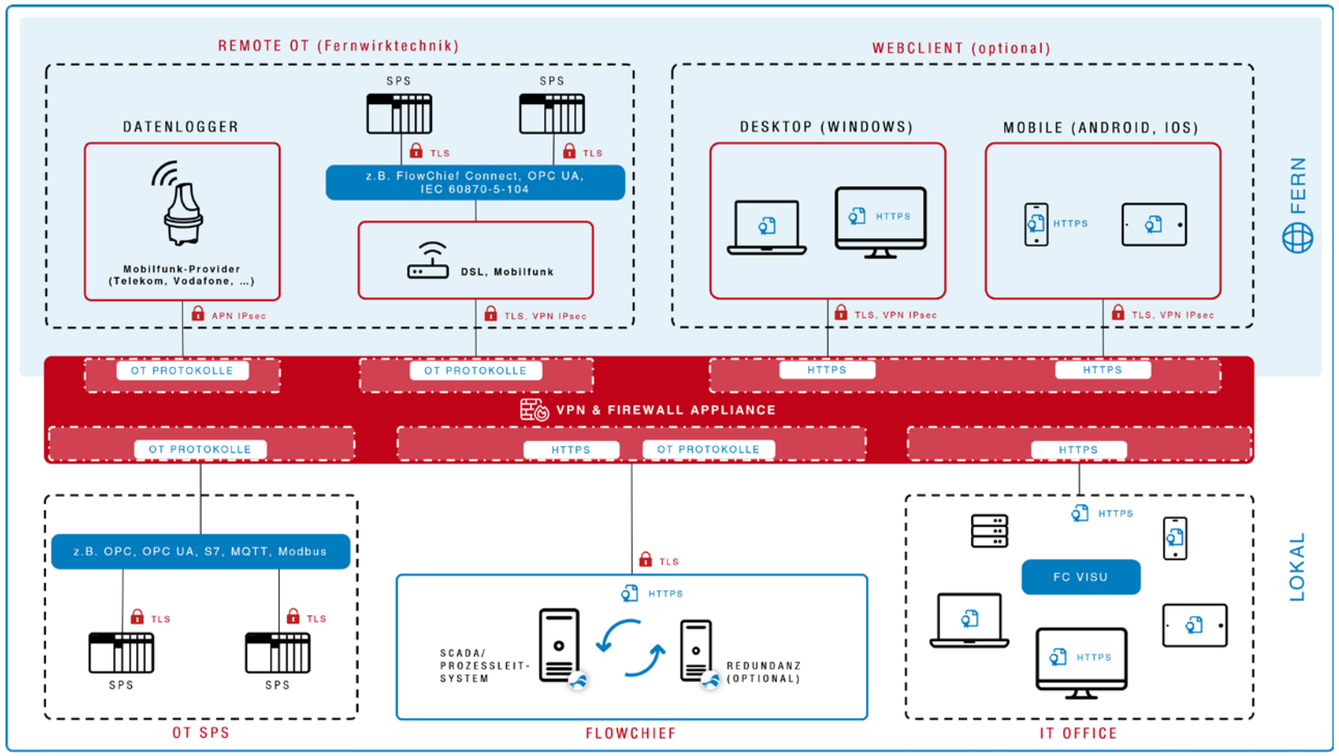
Ferneinwahlsoftware wie Remote Desktop birgt zahlreichen Folgerisiken, da Benutzer direkten Zugriff aufs Leitsystem Netz oder gar auf den Server erhalten. Mit FlowChief benötigen Sie keine Ferneinwahlsoftware, weder für die Überwachung noch fürs Engineering. Sie verbinden sich sicher mit dem Browser mit Ihrem FlowChief System. Sie haben dabei keine Einsicht auf das Host-System oder die damit verknüpften Netzwerke.

- ***Abschottung der Windows- und Netzwerkumgebung, da die Einwahl nicht direkt auf dem Windows-System erfolgt, wodurch das Risiko minimiert wird***
- ***Kein zusätzlicher Aufwand durch Installation & Updates***
- ***Verringerung der Komplexität***
- ***Bessere Skalierbarkeit durch parallelen gleichzeitigen Zugriff auf die Anwendung***
- ***Nutzung der integrierten Sicherheitsfunktionen wie Benutzerberechtigungen mit granularer Kontrolle über die einzelnen Funktionen***
- ***Fernzugriff per Browser oder App optional mit VPN-Flankierung***

SICHERE OT-KOMMUNIKATION

FlowChief kommuniziert auf der Anlage mit bis zu 500 Teilnehmern wie SPS-Steuerungen oder Messgeräten und bis zu 1 Mio. Datenpunkten. Wir setzen dabei auf eine direkte Kommunikation zwischen SPS und FlowChief. Durch die standardisierte Kommunikation ist es möglich, das SPS-Netz und das Leitsystem-Netz einfach zu trennen und durch eine Firewall zu segmentieren. Auch die Autorisierung und Verschlüsselung zwischen Feldgeräten (SPS) und FlowChief ist möglich.

- ***Unterstützung der Siemens Secure-PG-PC Kommunikation (TLS Verschlüsselung) und des Passwortschutzes***
- ***Unterstützung von Autorisierung und TLS Verschlüsselung bei OPC UA, MQTT, FlowChief Connect und IEC 60870-5-104 Kommunikation***
- ***OPC UA oder S7TIA Kommunikation bieten zahlreiche Sicherheitsfeatures wie z.B. die Definition von Rechten (lesen, schreiben) auf Signalebene***
- ***Möglichkeit zur Generierung individueller Gerätezertifikate***
- ***Diverse Optionen zur Verbesserung der Verbindungsresilienz (redundante Steuerungen) und zur Selbstüberwachung der Verbindung (Watchdog)***



VERTIKALE UND HORIZONTALE SEGMENTIERUNG

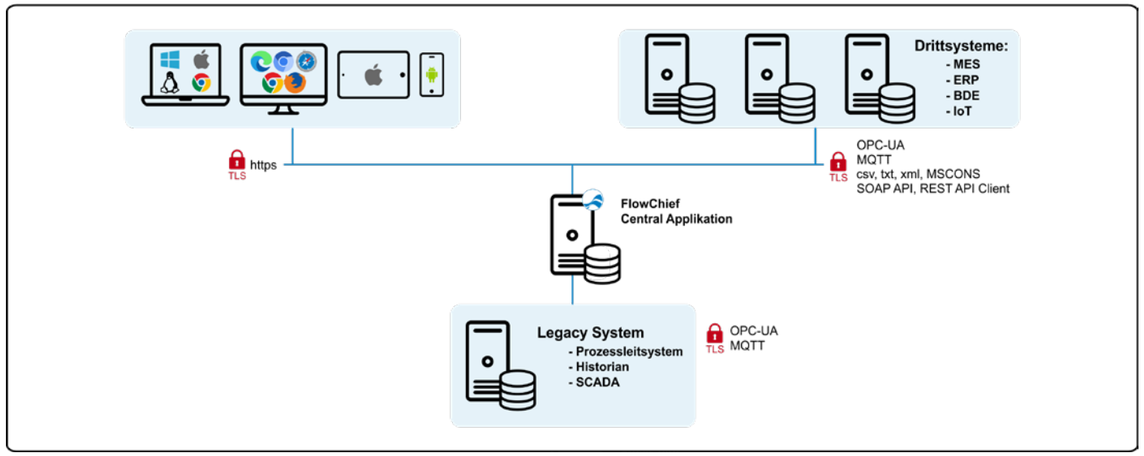
Eine klare Netzwerktrennung (IT, Leittechnik, OT Remote, OT SPS, Fernzugriff) ist entscheidend für eine sichere Integration von Leittechnik. Sie gewährleistet ein hohes Sicherheitsniveau und minimiert potenzielle Angriffsrisiken sowie deren Folgen. Angesichts der Tatsache, dass Angriffe hauptsächlich aus dem internen Netzwerk stammen, beispielsweise durch Social-Engineering und Phishing, wird deutlich, dass eine Firewall nicht nur an der Schnittstelle Öffentlich-Privat wichtig ist, sondern auch innerhalb des Netzwerks.

- ***Die Zonensegmentierung ermöglicht eine effektive Eindämmung von Angriffen. Sollte beispielsweise ein Mailclient im IT-Netz eine Ransomware-Attacke erleiden, stellt die Zonenbildung eine wirksame Barriere zwischen Leittechnik und Büronetz dar***
- ***Sicherer Fernzugriff über Browser oder App ohne Fernwartungssoftware***
- ***Definition verschiedener Sicherheitszonen – Für jede Zone kann eine eigene Risikobewertung mit entsprechenden Maßnahmen durchgeführt werden***
- ***Erhöhte Transparenz und Überwachung: Die Segmentierung erleichtert die Überwachung und Erkennung von Anomalien (IDS, IPS, Angriffserkennung)***

LEGACY IT-INTEGRATION

Die steigenden Anforderungen in Unternehmen, Daten und Funktionen aus der Prozessleittechnik einem breiteren Nutzerkreis oder anderen Diensten zugänglich zu machen, stehen oft im Kontrast zur mangelnden IT-Kompatibilität der bestehenden Prozessleitsysteme. FlowChief bietet eine Lösung, um veraltete Systeme oder Prozessleitsystem-Monolithen anzukoppeln, Informationen zu erfassen und verschiedene Funktionen wie Dashboards, Reporting, Monitoring oder Alarmierung unternehmensweit bereitzustellen. Die vorhandenen Systeme können abgeschottet vom restlichen Netz weiter eingesetzt werden.

- ***Höhere Sicherheit durch gehärteten Benutzerzugriff und niedrigere Risikokategorisierung im Vergleich zu Legacy-Systemen***
- ***Einfache Anbindung bestehender Prozessleitsysteme/SCADA-Infrastruktur, z.B. per OPC UA***
- ***Wahlweise nur lesender oder auch schreibender Zugriff***
- ***Abbildung von Objektstrukturen und einfaches Engineering***
- ***Nutzung der feingranularen und mandantenfähigen FlowChief-Rechteverwaltung zur Bereitstellung von Funktionen im Unternehmen***
- ***Vielfältige Anwendungsfälle von Monitoring, Historisierung, Datendrehscheibe bis hin zur zentralen OT-Datenplattform im Unternehmen***

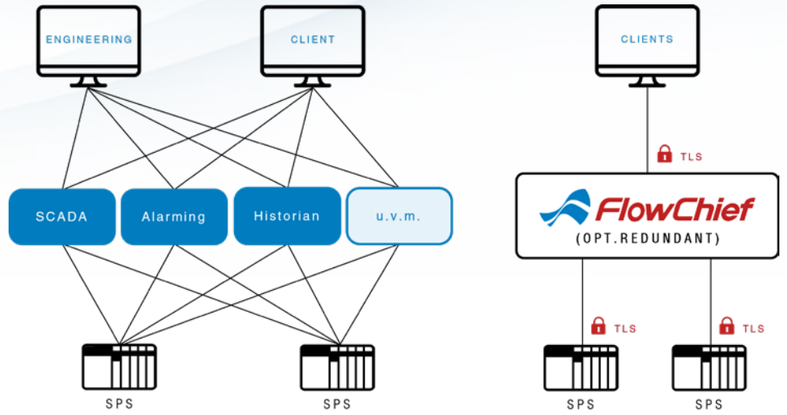


SICHERE IT-ANBINDUNG

Die Qualität einer Software kann noch so gut sein – ist diese nicht im Stande, sich in Systemlandschaften bzw. Ökosysteme zu integrieren, ist sie nicht brauchbar. Wichtig dabei, dass Schnittstellen auch Möglichkeiten zur sicheren Integration unterstützen.

- ***Anbindung an Active-Directory (zentrale Benutzerverwaltung) per LDAPS***
- ***Anmeldung über Drittanbieter-Anwendung per OAuth 2.0***
- ***Anbindung an Mailserver per SMTPS***
- ***Anbindung von FTP Servern per FTPS***
- ***Anbindung von Posteingangsservern per POP3S und S/MIME***
- ***Sichere Bereitstellung von Stammdaten, Online- und Archivdaten per OPC UA, MQTT, API***
- ***Bereitstellung von Dateien per HTTPS und WebDAV***

SCHLUSS MIT KOMPLEXEN SYSTEMLANDSCHAFTEN

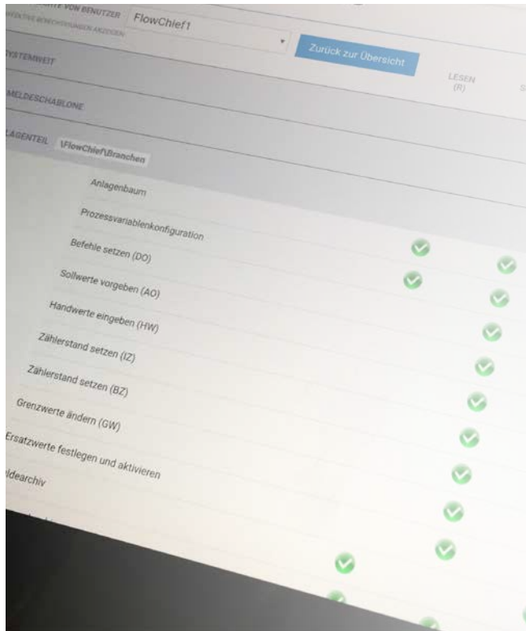


In Leittechnikumgebungen finden sich häufig diverse Produkte unterschiedlicher Hersteller (z.B. SCADA, Alarmierung, Historian, Energiemanagement). FlowChief bietet eine umfassende Lösung, die dieses Spektrum in einer einzigen Plattform vereint. Weniger Systeme bedeuten weniger Kommunikationsverbindungen, was wiederum den Aufwand für Sicherheitsbewertungen reduziert und die Überwachung vereinfacht.

- ***Weniger zu überwachende Hard- und Softwaresysteme***
- ***Weniger Kommunikationsverbindungen***
- ***Standardisierung auf wenige definierte Kommunikationsprotokolle***

IHR NUTZEN

- ***Einfache Umsetzung von Netzwerksicherheit (Firewall, Zonensegmentierung, IDS, Monitoring)***
- ***Softwarearchitektur ist entscheidender Faktor für Komplexität, Beherrschbarkeit und Kosten in Beschaffung und Betrieb***



FEINGRANULARE RECHTEVERWALTUNG

FlowChief verfügt über ein leistungsfähiges und feingranular aufgebautes Rechtemanagement, das Benutzern die Zuordnung zu Gruppen ermöglicht und die Rechtevergabe über Benutzer und Gruppen erfolgen kann. Jedes FlowChief-System wird gemäß der realen Applikation strukturiert. Dabei können anlagenteilspezifische Rechte auf das Lesen, Schreiben oder die Konfiguration. Zusätzlich können spezifische Rechte für Systemfunktionen wie Quittierung, Wertkorrektur und zahlreiche andere Funktionen festgelegt werden.

Das FlowChief IAM (Identify-Access-Management) ist durchgehend mandantenfähig konzipiert, sodass auf einer FlowChief-Plattform mehrere Mandanten (Anwendungen) bereitgestellt werden können.

Die Integration in vorhandene IAM-Lösungen wie Active Directory (per LDAPs) oder andere zentrale Benutzerverwaltungen per OAuth 2.0 wird unterstützt.

VERDÄCHTIGE AKTIVITÄTEN JEDERZEIT IM BLICK

FlowChief verfügt über ein umfangreiches Logging von Ereignissen und Benutzeraktivitäten, um den Administratoren umfangreiche Anlalyse- und Überwachungsmöglichkeiten zur Verfügung zu stellen.

- ***Erfassung von erfolgreichen und erfolglosen Benutzeranmeldungen***
- ***Auslösung von Reaktionen bei fehlgeschlagenen Anmeldeversuchen***
- ***Logging und Alarmierung bei Leistungsdaten und Systemzustandsvariablen***
- ***Protokollierung von steuernden Aktionen, Konfigurationsänderungen und Quittierungen***
- ***Bereitstellung von Ereignissen an zentrale Überwachungs- und Monitoring-Software***

SICHERE DATEIABLAGE

Prozessbilder, Laufzettel, Berichte und weitere Dateien sind unverzichtbare Bestandteile jedes Leitsystems. Doch wie steht es um die Sicherheit dieser Dateien? Bei FlowChief werden Dateien sicher in der Datenbank gespeichert, was zahlreiche Vorteile für den Nutzer bietet:

- ***Zugriffskontrolle***
  Visualisierungen und andere Dateien können mit individuellen Lese- und Schreibrechten versehen werden, um eine effektive Sicherheit zu gewährleisten
- ***Protokollierung***
  Zugriffe und Konfigurationsänderungen an Dateien werden protokolliert
- ***Einfache Integration ohne Fernzugriff***
  Dateien lassen sich bequem über den Dateimanager verwalten. Auch für das Engineering ist kein direkter Zugriff auf den Server erforderlich
- ***Reduzierung der Fragmentierung***
  Durch die Speicherung in der Datenbank wird Fragmentierung vermieden, was die Sicherheit der Applikation, redundante Strukturen und das Backup vereinfacht

SICHERER HOST

Wir zielen darauf ab, ganzheitliche Lösungen für einen sicheren Betrieb der gesamten Infrastruktur zu bieten. Dazu gehört auch der Host – die Komponente auf dem FlowChief installiert bzw. betrieben wird. Einige Schlüsselmerkmale für eine sichere Integration sind:

- ***Freigabe aller aktuellen Windows-Betriebssysteme entsprechend unserer Systemvoraussetzungen***
- ***Unterstützung von Virtualisierung***
- ***Sicherer Betrieb bereits mit der Installation***
- ***Minimalitätsprinzip – Auf dem Server laufen ausschließlich die Dienste für FlowChief, Datenbank und Webserver***
- ***Unterstützung von Applikation Whitelisting***
- ***Kompatibel zu SQL-Clustern und externen Datenbanken***
- ***Keine Windows App – ein Dienst, der unabhängig und stabil läuft***
- ***Keine Backdoors – wir garantieren, dass in unserer Software keine Hintertüren vorhanden sind um unbefugten Zugriff zu verhindern***
- ***SQL-Datenbank nach aktuellen Sicherheitsrichtlinien***
- ***Grundhärtung der Applikation***
- ***Härtungs-Guide zur zusätzlichen Härtung der Applikation***
- ***Kompatibilität mit gängigen Anitvirus/Anti-Malware Schutzprogrammen***

Betriebsmodelle für jede Sicherheitsanforderung

	Lokale Installation auf eigenem Server (On-Prem)	Hosting-Bereitstellung der Software auf FlowChief Server (PaaS)	Cloud–Bereitstellung der Software als Service (SaaS)
FlowChief Software			
	Konfiguration	Konfiguration	Konfiguration
	Daten	Daten	Daten
	Kommunikation	Kommunikation	Kommunikation
	Laufzeitumgebung	Laufzeitumgebung	Laufzeitumgebung
Infrastruktur			
	Betriebssystem	Betriebssystem	Betriebssystem
	Virtualisierung	Virtualisierung	Virtualisierung
	Server	Server	Server
	Speicher	Speicher	Speicher
	Netzwerk	Netzwerk	Netzwerk
	Höchste Flexibilität durch Installation im Kundennetzwerk	***Sichere Bereitstellung einer eigenen FlowChief Umgebung in einem zertifizierten Rechenzentrums (keine eigene Hardware)***	***Bereitstellung FlowChief als Service – keine eigene FlowChief Umgebung – sichere Bereitstellung aus einem zertifizierten Rechenzentrum***
	Firewall- und VPN-Portfolio zur Gewährleistung der Netzwerksicherheit	***Hohe Netzwerksicherheit durch Firewall-Überwachung und VPN-Flankierung***	***Hohe Netzwerksicherheit durch Firewall-Überwachung und VPN***
	Optional Security Quick Check durch FlowChief		

Für alle drei Varianten bieten wir zahlreiche Service Dienstleistungen, vom Monitoring, über Patching, bis hin zum 24/7/365 SLA.

Eigene Verantwortung | FlowChief Verantwortung

Sicherer FlowChief Login

Wie stellen wir sicher, dass sich ausschließlich berechtigte Benutzer mit dem System verbinden?

Bei FlowChief verbindet sich der Benutzer per Browser oder App ausschließlich sicher und verschlüsselt per HTTPS mit dem zentralen Server. Es erfolgt sowohl in der Anwendersitzung als auch im Engineering keine weitere proprietäre Netzwerk-Kommunikation zwischen den Arbeitsplätzen und dem Server. Um die Usersitzungen aus Intranet und außerhalb bestmöglich abzusichern, bieten wir zahlreiche Security-Features und Lösungen zur Absicherungen dieser Verbindungen.

- ***Absichern der Zugänge durch definierbare Passwortrichtlinien (Komplexität und Länge) und Zwei-Faktor-Authentifizierung (TOTP-App, SMS TAN)***
- ***Anbindung an ein unternehmensweites Benutzermanagement wie OAuth oder Active Directory (LDAPS)***
- ***Begrenzung der Anzahl von Login-Versuchen innerhalb einer bestimmten Zeit zum Schutz vor Brute-Force-Attacken***
- ***Möglichkeit zur Überwachung verdächtiger Aktivitäten durch weitreichende Protokollierung von Nutzeraktionen (u.a. Login, Konfiguration, Quittierung)***
- ***Feingranulares Rechtemanagement mit der Möglichkeit, eines ausschließlich lesenden Zugriffs von außerhalb des Server-Netzwerks***
- ***Umfangreiche integrierte Härtungsmaßnahmen sowie ein zusätzlicher Härtungsleitfaden zur weiteren Verbesserung der Zugriffssicherheit***
- ***Sicherheitsfeatures sowie die Zwei-Faktor-Authentifizierung sind in jedem System enthalten und müssen nicht explizit bezahlt werden***
- ***Passwörter werden ausschließlich sicher verschlüsselt übertragen und auch rücklesesicher mit SHA-512 Hash in der Datenbank abgelegt***

SECURITY QUICK CHECK FÜR IHRE ANLAGE

Unser Security Quick Check bietet eine gründliche Überprüfung des Istzustands Ihrer Leittechnik. Anhand einer Checkliste analysieren wir die zentralen Komponenten Ihrer Leittechnikinfrastruktur, darunter:

- ***Prüfung der Softwarestände auf dem Server (Betriebssystem, Datenbank, FlowChief)***
- ***Status der Sicherheitseinstellungen des Leitsystem-Servers***
- ***Prüfung der Backup- und Wiederherstellungsprozeduren sowie deren Inhalt***
- ***Prüfung der aktuellen Netzwerkstruktur bezüglich Absicherung und Segmentierung***
- ***Prüfung der Kommunikationsverbindungen zur OT***
- ***Prüfung der fernwirktechnischen Anbindung von Anlagen***

Basierend auf den Ergebnissen erstellen wir einen Prüfbericht, der als Grundlage für eine Ersteinschätzung des Sicherheitsniveaus dient. Dies ermöglicht die Ableitung der nächsten Schritte zur Sicherheitsverbesserung.

FlowChief GmbH
Alte Salzstraße 9
D-90530 Wendelstein

Tel.: +49 (0)9129 14722-0
Fax: +49 (0)9129 14722-99
E-Mail: info@flowchief.de

www.flowchief.de