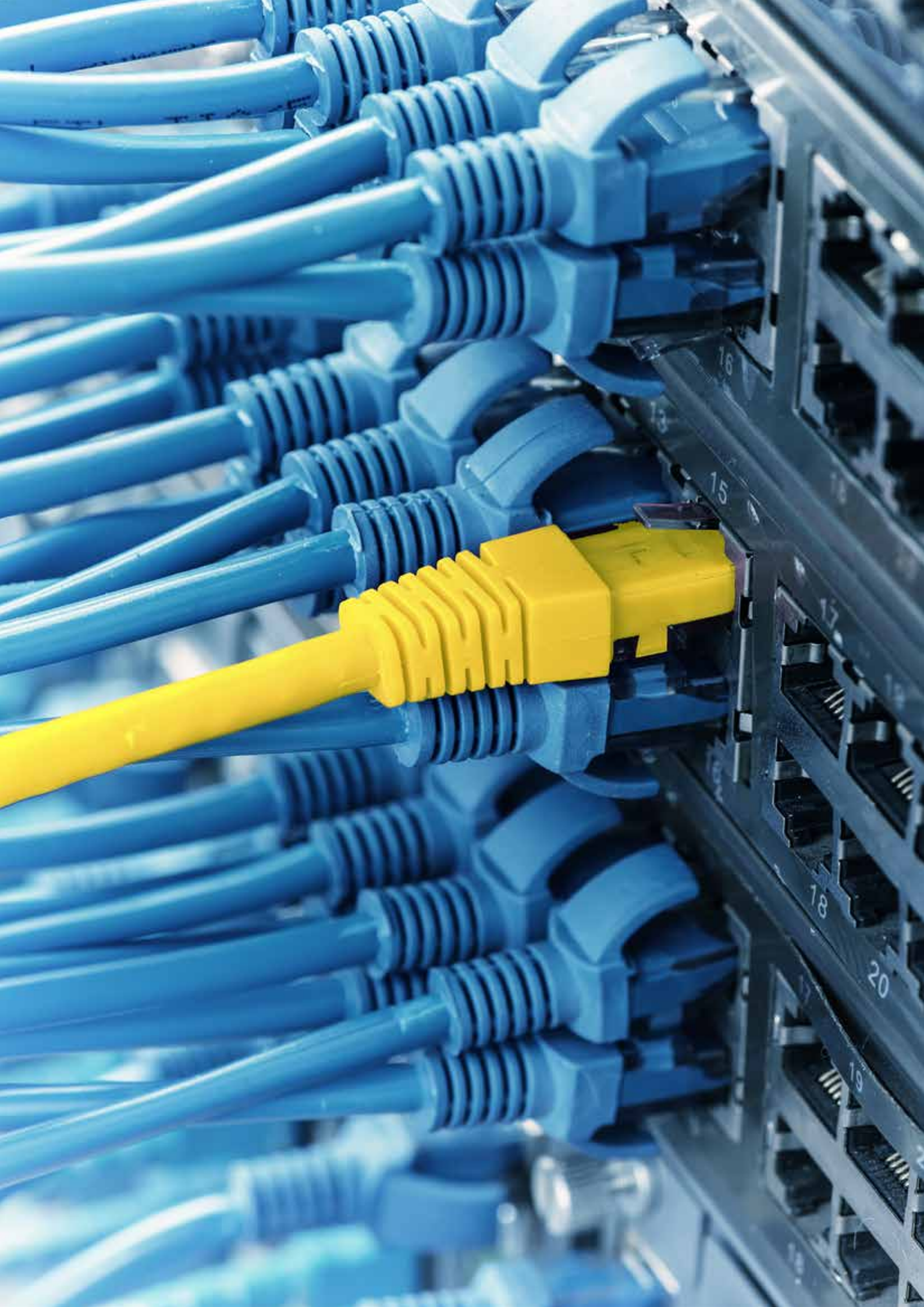
automation solutions

bachmann.

Security

Layer-basiertes Sicherheitskonzept schützt Maschinen und Anlagen.

energy.industry.maritime.



Den entscheidenden Schritt voraus

Security

Im internationalen Wettbewerb des Maschinen- und Anlagenbauers verschieben sich die Alleinstellungsmerkmale in Richtung Software. Den Unterschied machen Erfahrung und Wissen über den Prozess aus. Know-how steckt immer mehr in Anwendungen und Daten, zum Beispiel in Form von Algorithmen, Regelparametern und Rezepten. Neue Chancen mit Dienstleistungsangeboten, wie Online-Überwachung und -Wartung, verlangen nach sicheren Kommunikationswegen, strikt getrennten Zugriffsbereichen und manipulationssicherer Protokollierung.

Anwendungssektoren wie Energie- und Wasserversorgung sowie die Funktionale Sicherheit sind, getrieben durch Gesetze und Normen, bereits seit geraumer Zeit gezwungen konkrete Maßnahmen umzusetzen. Unterschiedliche Schutzmaßnahmen, wie abgesicherte Netzwerkverbindungen, Benutzer- und Zugriffskontrolle und Security-Protokollierung sind schon seit Jahren fixe Bestandteile jeder Steuerung von Bachmann. Das bestehende Sicherheitskonzept wird stetig anhand aktueller Normen und Vorschriften überprüft und gemeinsam mit unseren Kunden weiterentwickelt, nicht erst seit Stuxnet.

FEATURES

- *Layer-basiertes Schutzkonzept*
- *Ethernet-Lastbegrenzung*
- *Absicherung von Netzwerkdiensten und -protokollen durch Authentifizierung und End-to-End Verschlüsselung (SSL/TLS)*
- *Zugriffskontrolle und -protokollierung durch Access Control*
- *Schutzfunktionen auf Systemebene*
- *Offene Schnittstellen zu Access Control und kryptografischen Verfahren zur Anwendung in Benutzerprogrammen*
- *Durchgängiges, eigenständiges Sicherheitsprotokoll*
- *Vordefinierte Sicherheitsstufen zum Basisschutz*
- *Integrierter Bestandteil der M-Base*
- *SCEP, LDAP und syslog*

Kommunikations- und Informationssicherheit

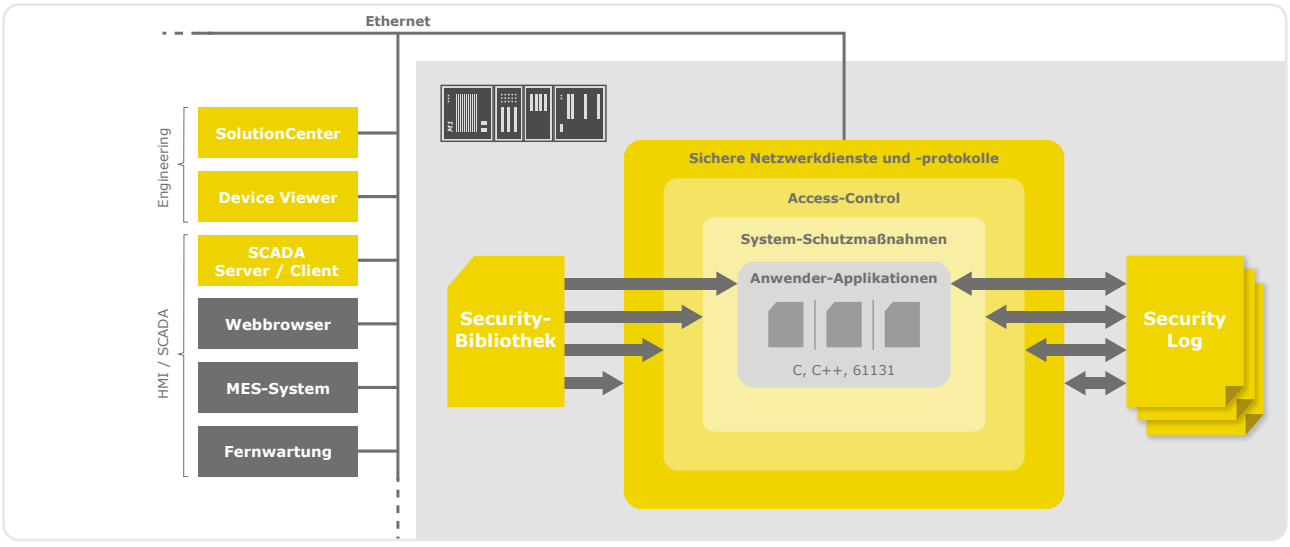
Mit layerbasierter Sicherheitsarchitektur

Direkte Folge eines gezielten zerstörerischen Zugriffs auf eine Maschinensteuerung oder einer unbewussten Fehlbedienung sind dieselben: Stillstand oder gar Zerstörung einer Maschine oder Anlage und somit Produktionsausfall, Verlust von Reputation und Geld. Die Sicherstellung der Robustheit gegenüber Störungen ist somit oberstes Ziel. Absicherung von Daten und Kommunikation und das Protokollieren von Zugriffen sind vorbeugende Maßnahmen, die den nicht autorisierten Zugriff erschweren und Auffälligkeiten ans Licht bringen.

Gezielter Zugriff

Exponierte Maschinen und Anlagen unterliegen nicht dem gleichwertigen Perimeterschutz wie geschlossene Fabrikationsanlagen. So sind Windkraftanlagen oder Biogasanlagen verhältnismäßig einfach zugänglich, die Reaktionszeiten bei einem detektierten Einbruch sind hoch. Hohes Risiko in Produktionsanlagen geht hauptsächlich von legitimierten Personen aus. Servicepersonal vom externen Dienstleister oder der gekündigte Mitarbeiter, der sich in Frustration zu einem gezielten Versuch der Sachbeschädigung hinreißen lässt, sind zwei klassische Beispiele. Ziele sind dabei Switches, Router und Controller mit freien Ports. Diese lassen sich zum unauffälligen Stören oder zum gezielten Abhören der Kommunikation nutzen.

Die layerbasierte Sicherheitsarchitektur bildet einen mehrstufigen Sicherheitswall um Anwender-Applikationen.
Jede Stufe beinhaltet spezifische Sicherungsmaßnahmen die auch in benutzerspezifischen Anwendungen genutzt werden können.

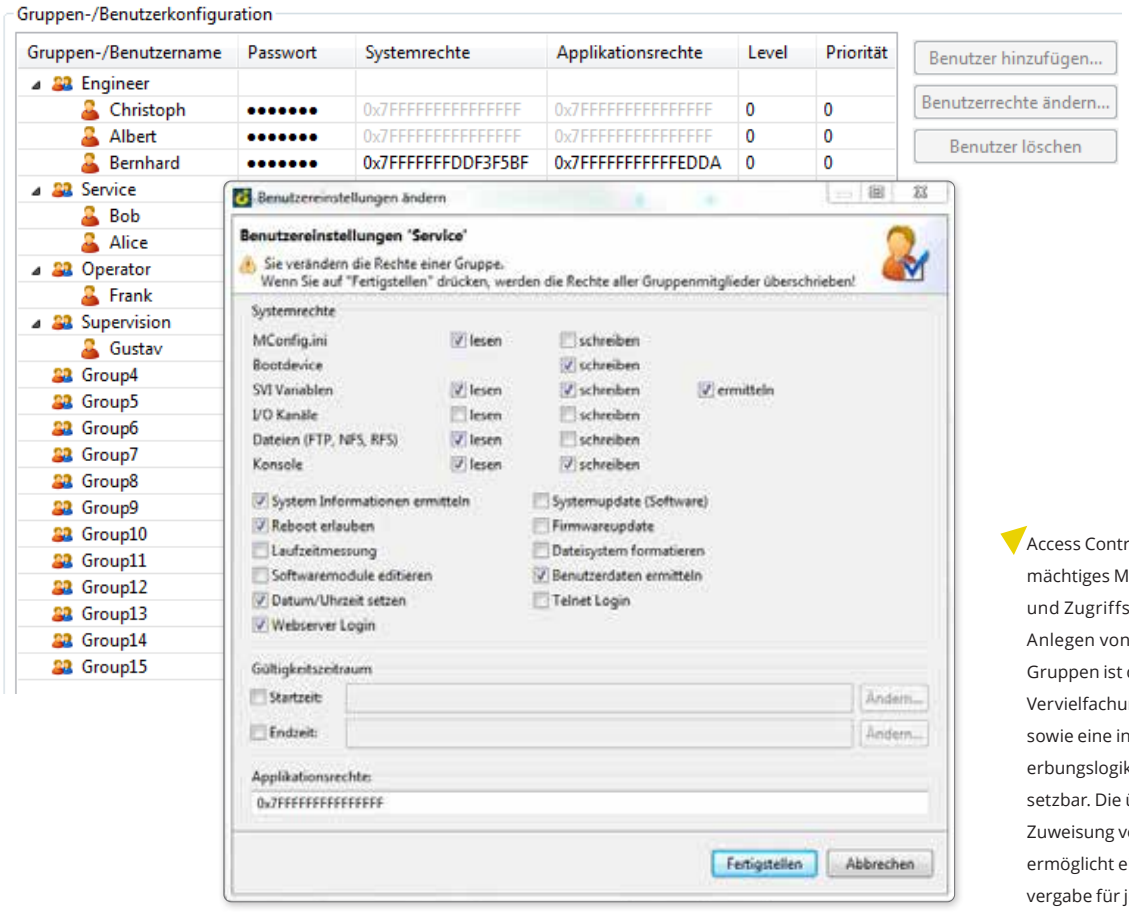


Dem gezielten Zugriff haben Steuerungskomponenten von Bachmann unterschiedliche Maßnahmen entgegenzusetzen. Es bestehen wirksame Mechanismen zum Schutz vor Netzwerk-Überlast die bei Denial of Service Angriffen die Stabilität der Anwendung sicherstellen. Das Mithorchen wird durch konsequente Umsetzung von End-to-End Verschlüsselung der Kommunikation durch SSL/TLS wirkungslos. Anwenderprogramme nutzen Schnittstellen zu aktuellen kryptografischen Verfahren um Daten zu verschlüsseln.

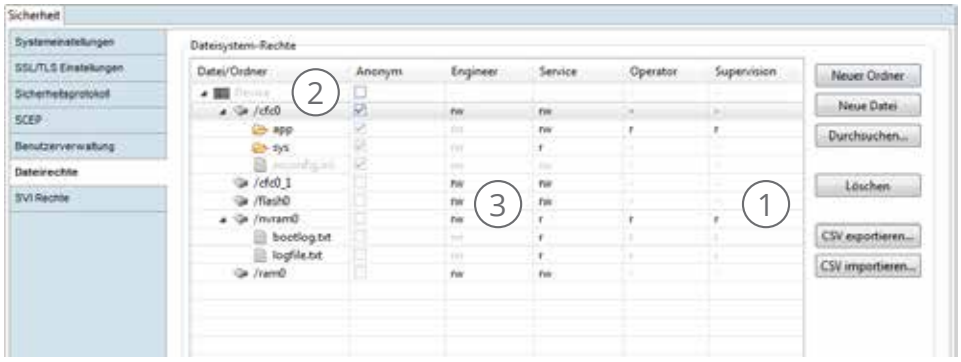
Kritische Infrastrukturen

Angeleitet durch nationale und internationale Vorschriften sind Versorgungsunternehmen besonders auf Sicherheit sensibilisiert und verpflichtet, ihre Anlagen entsprechend zu schützen. Eingebettet in detaillierte Sicherheitskonzepte in allen organisatorischen Ebenen sind umfangreiche Maßnahmen seit langem etabliert. Schutzzäune, eigenes Überwachungspersonal und durchgängige Zugriffskontrollen sind in kritischen Teilen dieser Anlagen vorzufinden. Steuerungsnetzwerke und Bedienkonsolen waren früher strikt abgeschottet. Moderne Geschäfts- und Servicemodelle erfordern inzwischen den gezielten Zugriff von anderen Organisationsteilen via Intranet und sogar von außen via Internet.

Das effiziente Management einer großen Anzahl an Steuerungen in kritischen Infrastrukturen setzt die Möglichkeit der zentralen und serverbasierten Verwaltung von Nutzern und deren Zugriffsrechten, SSL/TLS-Zeritfikaten sowie der zentralen Erfassung von Systemmeldungen voraus. Aus diesem Grund unterstützt das M1-Steuerungssystem die Protokolle LDAP für die zentrale Benutzerverwaltung, SCEP für das zentralisierte Roll-out von SSL/TLS-Zertifikaten sowie syslog für das Erfassen von Systemmeldungen.



Access Control beinhaltet ein mächtiges Modul zur Benutzer- und Zugriffskontrolle. Das Anlegen von Benutzern und Gruppen ist durch einfache Vervielfachung via Copy&Paste sowie eine integrierte Vererbungslogik zeitsparend umsetzbar. Die übersichtliche Zuweisung von Systemrechten ermöglicht eine gezielte Rechtevergabe für jeden Benutzer.



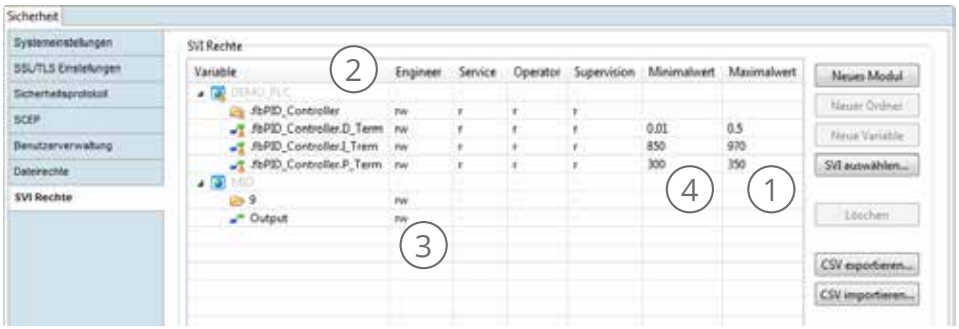
Verwaltung von Datei- und Variablenrechten:

(1) Per Browser werden einzelne Dateien und Variablen oder ganze Ordner zur Rechteverwaltung ausgewählt.

(2) Die Darstellung erfolgt in übersichtlicher Baumstruktur.

(3) Benutzerbezogen können Lese- und Schreibrechte feingranular per Inline-Editing direkt in der Liste zugewiesen werden.

(4) Variablen können zusätzlich im Wertebereich eingeschränkt werden.



Defekte und Fehlbedienung

Gezieltes Sicherheitsmanagement hilft nicht nur bei unerwünschten und potenziell zerstörerischen Zugriffen. Gerade im geschützten Umfeld von Produktionsanlagen sind versehentliches Verändern von Maschinenparametern, Ausfälle von Netzwerkkomponenten oder Fehlkonfigurationen des Maschinennetzwerks weitaus häufiger, aber in den Symptomen und Auswirkungen gleichwertig zu Security-Bedrohungen. Beispielsweise belastet ein Broadcast-Storm in Folge eines Switch-Defekts angeschlossene Netzwerk-Clients in gleicher Art wie eine gezielte Denial of Service Attacke.

Im Gegensatz zu anderen Sicherheitsmaßnahmen kann der Mehrwert zur Aufdeckung von Defekten nur dann erreicht werden, wenn entsprechende Schutzmaßnahmen direkt auf der Steuerung wirken. Bachmann stattet seine Steuerungen mit Funktionen zur Bandbreitenbegrenzung des Netzwerks aus, um die Robustheit gegen absichtliche und unabsichtliche Netzwerkstörungen zu erhöhen. Echtzeitprozesse werden durch Überlastung der Netzwerkschnittstelle nicht gestört.

Das Einrichten einer Benutzer- und Zugriffsverwaltung via Access Control empfiehlt sich für jeden Anwender. Damit werden Manipulationsmöglichkeiten zentral nach dem Least Privilege Prinzip eingegrenzt und eine eigenständige Sicherheits-Protokollierung ermöglicht die Zuordnung von Änderungen zu einzelnen Anwendern. Fehlbedienungen können damit aufgedeckt und Garantiefälle rasch abgewickelt werden.

Safety und Security

Die funktionale Sicherheit verpflichtet zu einem hohen Maß an Security-Maßnahmen zur Vermeidung von Fehlbedienungen und gezielter Manipulation. Unbemerkte Änderungen an der Sicherheitsprogrammierung sowie gefährliche Eingriffe während des sicheren Betriebes müssen verhindert und protokolliert werden. Safety Control von Bachmann alarmiert bereits am Projektierungsrechner vor böswillig manipuliertem Code und schützt vor versehentlichen Änderungen mittels Funktionen zum Einfrieren von Entwicklungsständen. Ein eigenes Login-System auf jeder Sicherheitssteuerung ermöglicht den individuell einschränkbaren Zugriff.

Die lückenlose Protokollierung ist manipulationssicher und redundant realisiert, so dass sogar bei teilweiser Zerstörung der Baugruppe mit hoher Wahrscheinlichkeit die Ereigniskette bis zum Ausfall nachvollzogen werden kann.

Einfach sicher

Sicherheitsmaßnahmen sind nur dann wirksam, wenn diese auch angewendet werden. Bachmann sieht es als Aufgabe, die flächendeckende Anwendung und Verbreitung von Security-Funktionen zu fördern, selbst wenn noch keine durchgängigen Sicherheitskonzepte bestehen und das Personal noch keine Sicherheitsexperten sind. Durch einfache Aktivierung und Bedienung der umfangreichen Schutzmaßnahmen wird bereits in diesem frühen Stadium sichergestellt, dass die Gefahren unachtsamen Bedienens und einfacher Angriffe minimiert werden.

Zentralen Teil bilden vier vordefinierte Sicherheitsstufen, die im Sicherheits-Konfigurator auszuwählen sind. Dahinter stehen Vorlagen, welche automatisch die Einstellungen innerhalb des Controllers so setzen, dass bestimmte Protokolle und Funktionen aktiviert oder auch verboten werden, abhängig von der Stufe.

Basisschutz in drei Schritten:

1

System und Netzwerk absichern
- Sicherheitsstufe einstellen
- nicht benötigte Dienste deaktivieren
- Logging aktivieren

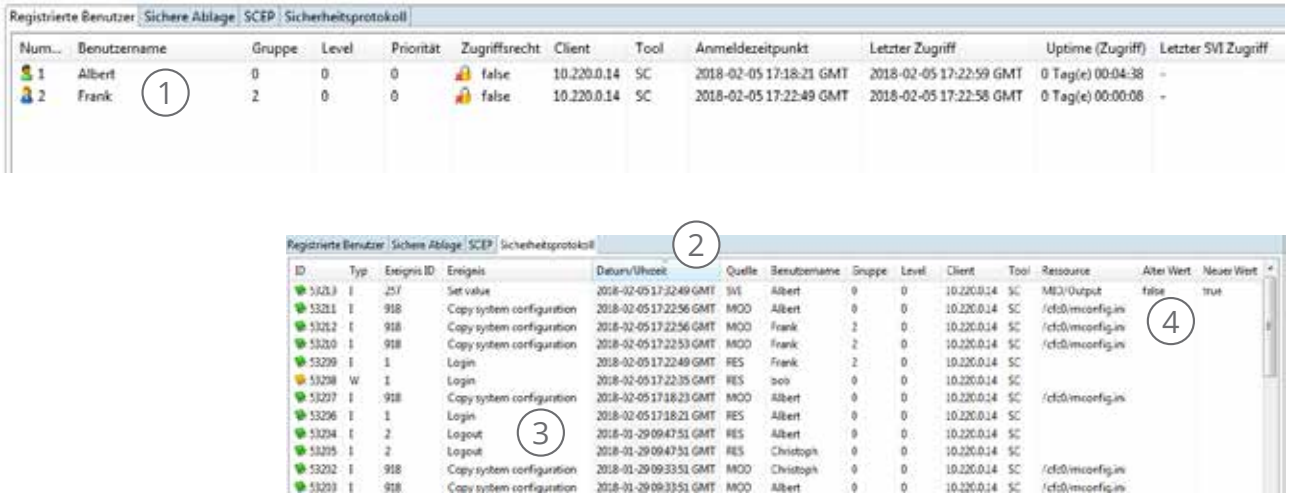
2

Zugriffe eingrenzen
- Gruppenrechte definieren
- Benutzer anlegen
- Dateirechte setzen

3

Anwenderprogramme absichern
- Applikationen unter Berücksichtigung genereller Sicherheitsaspekte umsetzen

Empfohlene Vorgehensweise zur Absicherung der Steuerung



Der Sicherheitsmonitor bietet eine komfortable Online-Übersicht:

(1) Detailinformationen zu eingeloggten Benutzern sowie zum Status des Zugriffsrechts (Token)

(2) Die aktuellsten Einträge im Sicherheitsprotokoll zeigen Details zu Verbindungen und Kommunikationsabläufen, wie z. B. Login/Logout (3) oder Veränderungen an Systemdateien (4)

Übersicht

Ethernet	
Lastbegrenzung	Für jede Ethernetschnittstelle gesondert einstellbare Limitierung der Lese- und Schreibauslastung; Schützt die Maschinenapplikation vor DDoS-Attacken (Distributed Denial of Service), Broadcast Storms und Defekten in der Netzwerkinfrastruktur.
Firewall *)	Konfigurierbare und zur Laufzeit programmierbare IP- und MAC-Filter schützen vor DoS-Attacken und ermöglichen das gezielte Ausblenden von potentiell gefährlichen Services oder defekten Geräten.

Netzwerkdienste und -protokolle	
SSL/TLS basierte Netzwerkkommunikation	Sicherheitsstandard zur Etablierung eines abgesicherten Kommunikationskanals auf IP-Ebene. Unterstützung (Auswahl): *Bachmann-Produkte:* Konfigurations- und Programmiertool SolutionCenter, WebMI Pro, M1COM, MJCOM *Herstellerneutrale:* OPC UA, Webserver, Filetransfer
Server- und Client-Authentifizierung	Die M1-Steuerung kann sowohl SSL-Server als auch Client sein. Zusätzlich wird die Client-Authentifizierung im Server-Modus unterstützt. Diese dient zur zertifikatsbasierten Authentifizierung von Rechern, Diensten und Benutzern an der M1.
Protokollunterstützung für das Management von SSL-Zertifikaten	Die M1-Steuerung unterstützt das Small Certificate Enrollment Protokoll (SCEP) für die zentrale Verwaltung und Verteilung von SSL-Zertifikaten durch einen SCEP-Server.
Abgesicherte und deaktivierbare Services (Webserver, OPC-Server, FTP, NTP, SMTP usw.)	Nicht benötigte Protokolle können per Konfiguration deaktiviert werden. Dadurch sind ausschließlich benutzte Ports erreichbar und verringern somit die Angriffsfläche.
Zentrale Verwaltung von User-Credentials	Die M1-Steuerung unterstützt das Lightweight Directory Access Protocol (LDAP) für die zentrale Verwaltung von User-Zugangsdaten und Role Base Access Control durch einen LDAP-Server.
Zentrales Management von Systemmeldungen	Das syslog-Protokoll der M1-Steuerung ermöglicht das zentrale Sammeln von Systemmeldungen in einem Netzwerk durch einen syslog-Server.

Access Control	
Benutzerverwaltung	Auf Gruppen- und Anwenderbasis werden passwortgeschützte Einschränkungen für Systemzugriffe und Applikationsrechte konfiguriert. Zeitlich eingeschränkte Zugriffe sind vorgesehen.
Token basierter Schreibzugriffsschutz	Der spezielle Mechanismus garantiert, dass dem Token-Besitzer ein exklusives Schreibrecht eingeräumt wird. Zusätzlich kann eine Priorisierung auf Basis der Benutzer-Rolle erfolgen. Unterschiedliche Prioritätsstufen können auf Benutzer- und Gruppenebene vergeben werden.
Dateizugriff	Dateizugriffe, also die Berechtigung zum Lese- oder Schreibvorgang sowie die Sichtbarkeit bei Browser-Anfragen lassen sich auf Gruppenebene einstellen. Die Konfiguration ermöglicht individuelle Rechtezuordnung auf Verzeichnis- und Dateiebene und erleichtert diese durch die verfügbare Vererbungslogik.
Variablenschutz	Online verfügbare Prozessvariablen können in ihrer Sichtbarkeit, Lese- und Schreibzugriffen den Zugriffsrechten des einzelnen Benutzer zugeordnet werden. Mechanismus und Konfiguration wie bei den Dateirechten.
Benutzerspezifische Erweiterungen vorgesehen	Benutzer- und Zugriffsverwaltungssystem sowie der Token-Mechanismus sind durch anwenderspezifische Applikationen ersetzbar. Damit sind spezielle Policies und Funktionen umsetzbar und die Steuerungen nahtlos in bereits bestehende Systeme integrierbar.

System	
Applikationsentwicklung erlauben/sperren	Schutz vor Installation von nicht autorisierten Programmen.
Speicherschutz	Applikationsprogramme werden auf Speicherebene vor Schreibzugriffen aus anderen Applikationen geschützt. Schutz vor Schadprogrammen die Daten auf Betriebssystemebene aushorchen und manipulieren wollen. Schutz vor Buffer Overflows.
Nullpointerschutz	Spezieller Schutz um Manipulationen via Null-Pointer Ausnahmebehandlungen zu verhindern.
Sicherheitsprotokoll mit Archivierungsfunktion	Login und Logout von Benutzern sowie Schreibzugriffe werden auf Variablenebene protokolliert, sicherheitsrelevante Modifikationen vermerkt. Zeitstempel, Benutzer, Gruppe, alter und neuer Wert, sowie weitere Details werden in fortlaufend erzeugten Dateiarchiven gespeichert. Zugriff ist offline, z. B. durch zentrales Archivierungssystem aber auch online durch Anwendungsprogramme oder SCADA-Systeme möglich.
Vordefinierte Sicherheitsstufen	Vier Vorlagen zur Vereinfachung und Verkürzung der Sicherheitskonfiguration.
Partitionsverschlüsselung *)	Transparente Verschlüsselung via SolutionCenter (wahlweise AES128/192/256); Schutz bei Diebstahl des Datenträgers (CF-/CFast-Karte) vor unerlaubtem Datenzugriff und -manipulation.

Anwender-Applikation		
Access Control	Auf die Informationen zu eingeloggten Benutzern, deren Session-Status und die Sicherheitsprotokolle kann aus Anwenderprogrammen zugegriffen werden.	
Security-Bibliothek	Symmetrische, asymmetrische Verschlüsselungsverfahren, Signatur- und Autentifizierungsverfahren, Block- und Stromchiffren, SSL/TLS stehen mittels openssl-Bibliothek den Anwenderprogrammen zur Verfügung. Diese Funktionen können in Form von Bibliotheksfunktionen in PLC verwendet werden.	
Beispiele wichtiger kryptografischer Verfahren und sicherer Methoden zur Netzwerkkommunikation	Symmetrische Verschlüsselung:	AES, 3DES
	Asymmetrische Verschlüsselung:	RSA
	Hash-Funktionen:	SHA, RIPEMD, MD5
	MAC-Funktionen:	CBC-MAC, HMAC
	Signaturalgorithmen:	RSA-PSS, ECDSA
	Schlüssel-Austauschverfahren:	SSL/TLS (TLS 1.2, TLS 1.1, TLS 1.0, SSL 3.0)
	Zertifikatsvarianten, Daten-Encoding:	PKS7, PKS12, x509

Normen, Vorschriften und Empfehlungen	
Security in Control Systems	Die Sicherheitsmaßnahmen wurden unter Berücksichtigung folgender Normen, Vorschriften und Empfehlungen umgesetzt: IEC 62351, IEC 62443, ISA 99, VDI/VDE 2182, FIPS 140, NIST 800 Serie
Herausgeber	BSI, BDEW, NERC

Systemvoraussetzungen	
Automatisierungsgeräte	M1 CPUs der MX200-Serie oder besser
Engineering-PC	Systemvorraussetzungen siehe SolutionCenter
Laufzeit-Software	M-Sys / MxCCore ≥V3.80
Engineering-Software	M-Base ≥3.80
Installationsmedium	In M-Base enthalten (Laufzeit- und Engineeringkomponenten)

*) ab M-Base / M-Sys / MxCCore ≥ V3.95

bachmann.

www.bachmann.info

Security DE | Technische Änderungen vorbehalten