Security

Security

Kommunikations- und Informationssicherheit

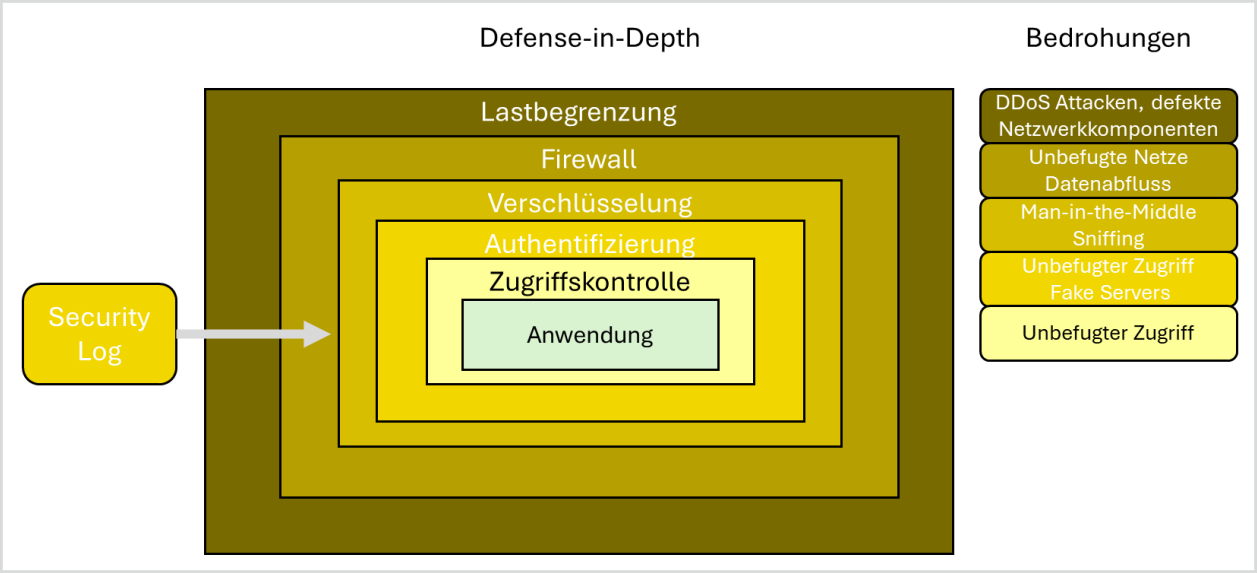
Gezielte Angriffe auf industrielle Steuerungen nehmen weltweit zu und können gravierende Folgen haben: Stillstand oder gar Zerstörung einer Maschine oder Anlage – mit Produktionsausfall, Reputationsschaden und finanziellen Verlusten. Der Schutz vor Cyberangriffen ist daher zu einem zentralen Faktor für den sicheren und kontinuierlichen Betrieb industrieller Anlagen geworden.

Die Absicherung von Daten und Kommunikation sowie das Protokollieren von Zugriffen sind entscheidende Maßnahmen, um unautorisierte Eingriffe zu verhindern und sicherheitsrelevante Auffälligkeiten frühzeitig zu erkennen.

Da moderne Maschinen und Produktionsanlagen zunehmend in IT- und Kommunikationsnetzwerke eingebunden sind, etwa zur Fernwartung, entstehen neue Anforderungen an die Informationssicherheit, die Anlagenbauer und Betreiber gleichermaßen vor Herausforderungen stellen.

Zertifizierte Sicherheit

Die Security-Lösung von Bachmann erfüllt höchste Anforderungen an Cybersicherheit und Zuverlässigkeit. Sie ist nach IEC 62443-4-2 zertifiziert und erfüllt damit alle relevanten Anforderungen an sichere industrielle Automatisierungs- und Steuerungssysteme. Darüber hinaus ist sie gemäß IACS UR E27 für den Einsatz im maritimen Umfeld zugelassen. Damit eignet sich unsere Lösung sowohl für den Einsatz in kritischen Infrastrukturen an Land als auch auf Schiffen und Offshore-Anlagen, wo robuste, normkonforme IT-Sicherheit und Ausfallsicherheit entscheidend sind.



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

Security durch Defense-in-Depth

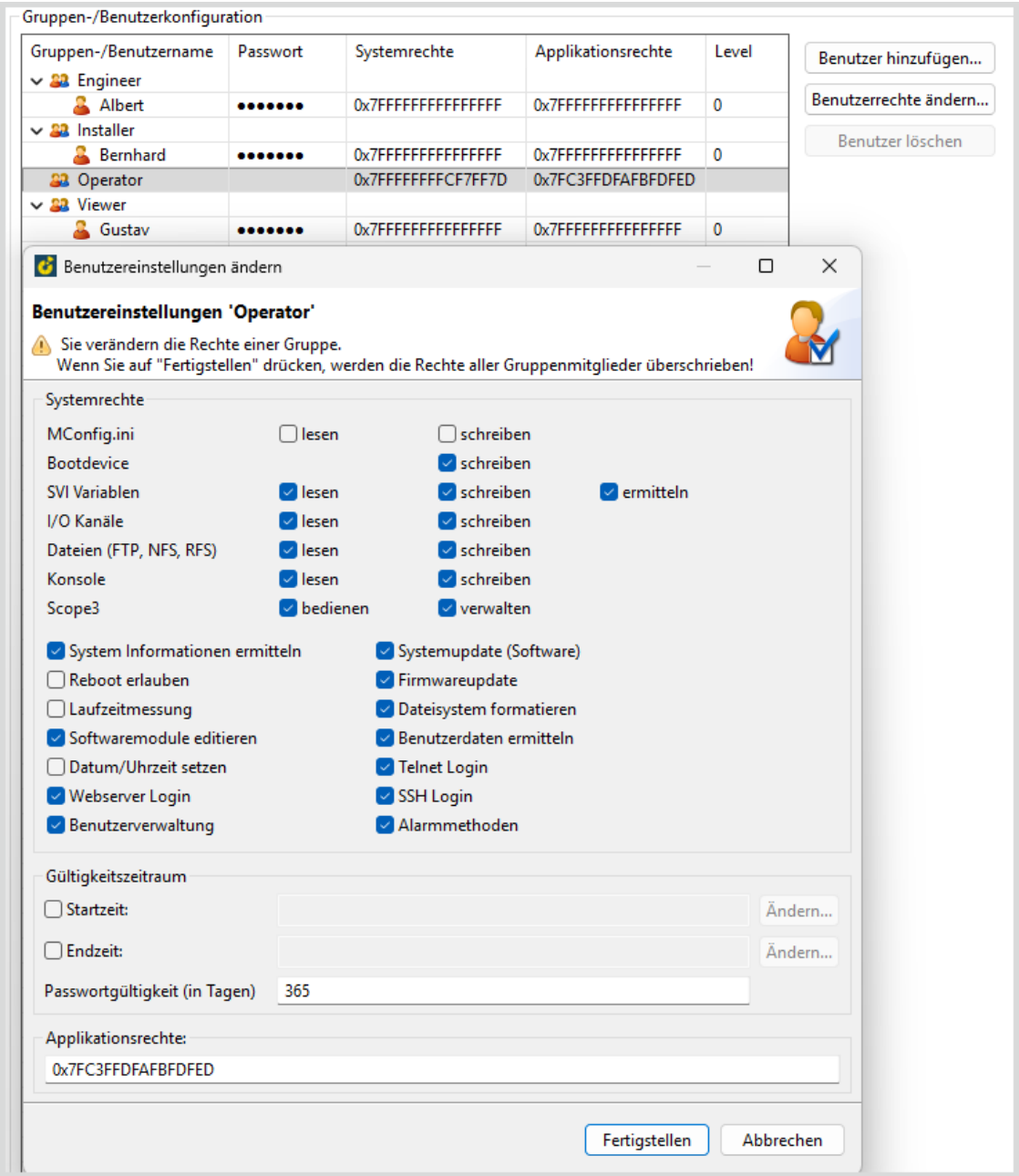
Das Defense-in-Depth-Prinzip kombiniert mehrere ineinandergreifende Schutzmechanismen, um Systeme auch dann zu sichern, wenn eine einzelne Verteidigungslinie versagt. Bachmann setzt dieses Konzept konsequent ein, um industrielle Steuerungssysteme umfassend abzusichern und ihre Resilienz gegenüber Cyberbedrohungen zu erhöhen.

- Ein Schutz vor Denial-of-Service-Angriffen gewährleistet die Verfügbarkeit kritischer Funktionen auch unter hoher Last, bei Defekten anderer Netzwerkgeräte oder gezielten Angriffen.
- Verschlüsselte Kommunikation via TLS sichert die Integrität und Vertraulichkeit der Daten, während Server- und Clientzertifikate nur vertrauenswürdigen Systemen den Zugriff erlauben.
- Access Control und rollenbasierte Autorisierung stellen sicher, dass nur berechtigte Nutzer Zugriff auf kritische Funktionen, Daten und Prozessvariablen haben.
- Die regelmäßige Prüfung von Hashwerten kritischer Systemkomponenten schützt die Systemintegrität und verhindert unautorisierte Änderungen.
- Systemhärtung, etwa durch Reduzierung der Angriffsfläche und konsequentes Patch-Management, erhöht die Stabilität.
- Ergänzend sorgt Security Logging für die Nachvollziehbarkeit aller sicherheitsrelevanten Ereignisse und ermöglicht die frühzeitige Erkennung von Angriffsmustern oder Anomalien.

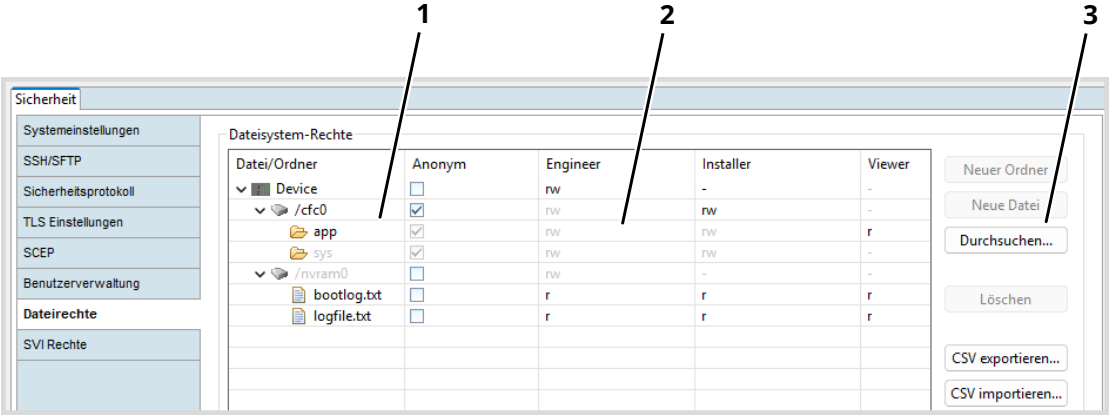
Effizientes Management

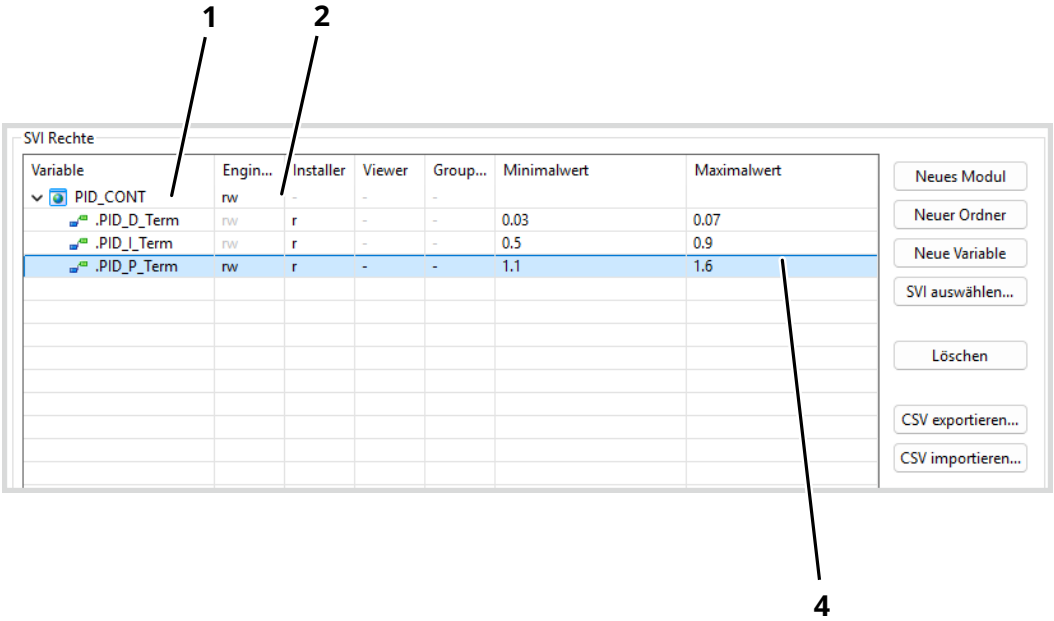
Das effiziente Management einer großen Anzahl an Steuerungen in kritischen Infrastrukturen setzt voraus, dass die Möglichkeit der zentralen und serverbasierten Verwaltung von Nutzern und deren Zugriffsrechten, SSL-Zeritfikaten sowie der zentralen Erfassung von Systemmeldungen besteht.

Aus diesem Grund unterstützt das M200-Steuerungssystem die Protokolle LDAP für die zentrale Benutzerverwaltung, SCEP für das zentralisierte Rollout von SSL-Zertifikaten sowie syslog für das Erfassen von Systemmeldungen. So bleiben Administration, Sicherheit und Nachvollziehbarkeit jederzeit effizient und transparent.



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.





1 Die Darstellung erfolgt in übersichtlicher Baumstruktur
2 Benutzerbezogen können Lese- und Schreibrechte feingranular per Inline-Editing direkt in der Liste zugewiesen werden
3 Per Browser werden einzelne Dateien und Variablen oder ganze Ordner zur Rechteverwaltung ausgewählt
4 Variablen können zusätzlich im Wertebereich eingeschränkt werden

Verwaltung von Datei- und Variablenrechten

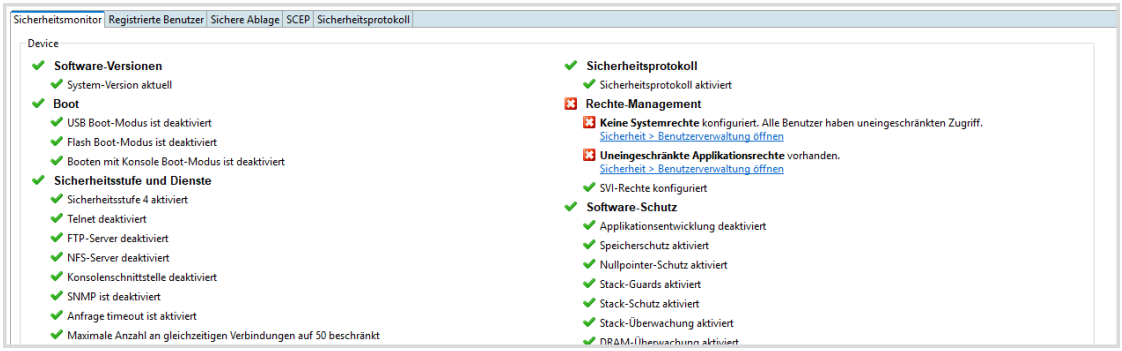
Security Monitor

Der Security Monitor fasst alle sicherheitsrelevanten Einstellungen einer Steuerung übersichtlich an einer zentralen Stelle zusammen. Da moderne industrielle Systeme zahlreiche Parameter und Aspekte zur Absicherung enthalten, kann leicht der Überblick verloren gehen. Der Security Monitor bietet eine klar strukturierte, intuitive Darstellung, die es Anwendern ermöglicht, den aktuellen Sicherheitsstatus auf einen Blick zu erfassen und sicherzustellen, dass keine wichtigen Einstellungen übersehen werden. So unterstützt er Betreiber und Integratoren dabei, Sicherheitsrichtlinien konsequent umzusetzen und die Integrität sowie den Schutz der Anlage dauerhaft zu gewährleisten.

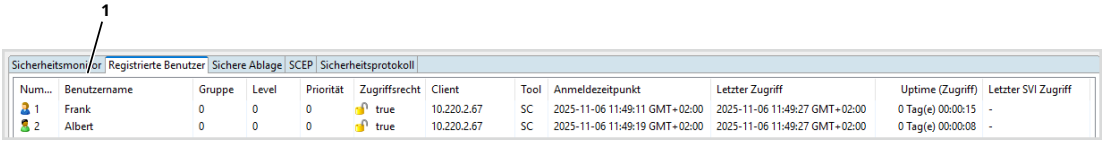
Safety und Security

Der Bachmann Safety Controller SLC 284 schützt vor Manipulationen und Fehlbedienungen und gewährleistet die Integrität sicherheitskritischer Programme. Bereits am Projektierungsrechner werden böswillige Änderungen erkannt, während Funktionen zum Einfrieren von Entwicklungsständen versehentliche Änderungen verhindern. Ein individuell konfigurierbares Login-System regelt den Zugriff auf jeder Sicherheitssteuerung, und die manipulationssichere, redundante Protokollierung stellt sicher, dass alle Ereignisse lückenlos nachvollzogen werden können.

Der Sicherheitsmonitor bietet eine komfortable Online-Übersicht:

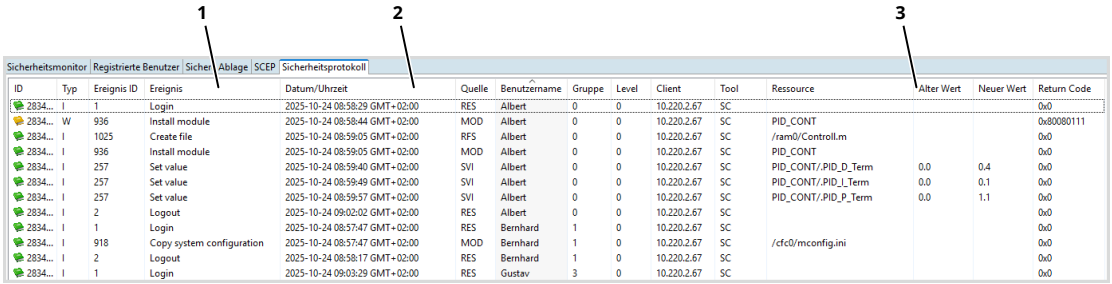


Register Sicherheitsmonitor



Num...	Benutzername	Gruppe	Level	Priorität	Zugriffsrecht	Client	Tool	Anmeldezeitpunkt	Letzter Zugriff	Uptime (Zugriff)	Letzter SVI Zugriff
1	Frank	0	0	0	true	10.220.2.67	SC	2025-11-06 11:49:11 GMT+02:00	2025-11-06 11:49:27 GMT+02:00	0 Tag(e) 00:00:15	-
2	Albert	0	0	0	true	10.220.2.67	SC	2025-11-06 11:49:19 GMT+02:00	2025-11-06 11:49:27 GMT+02:00	0 Tag(e) 00:00:08	-

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



ID	Typ	Ereignis ID	Ereignis	Datum/Uhrzeit	Quelle	Benutzername	Gruppe	Level	Client	Tool	Ressource	Alter Wert	Neuer Wert	Return Code
2834...	I	1	Login	2025-10-24 08:58:29 GMT+02:00	RES	Albert	0	0	10.220.2.67	SC				0x0
2834...	W	936	Install module	2025-10-24 08:58:44 GMT+02:00	MOD	Albert	0	0	10.220.2.67	SC	PID_CONT			0x80080111
2834...	I	1025	Create file	2025-10-24 08:59:05 GMT+02:00	RFS	Albert	0	0	10.220.2.67	SC	/ram0/Controll.m			0x0
2834...	I	936	Install module	2025-10-24 08:59:05 GMT+02:00	MOD	Albert	0	0	10.220.2.67	SC	PID_CONT			0x0
2834...	I	257	Set value	2025-10-24 08:59:40 GMT+02:00	SVI	Albert	0	0	10.220.2.67	SC	PID_CONT/.PID_D_Term	0.0	0.4	0x0
2834...	I	257	Set value	2025-10-24 08:59:49 GMT+02:00	SVI	Albert	0	0	10.220.2.67	SC	PID_CONT/.PID_I_Term	0.0	0.1	0x0
2834...	I	257	Set value	2025-10-24 08:59:57 GMT+02:00	SVI	Albert	0	0	10.220.2.67	SC	PID_CONT/.PID_P_Term	0.0	1.1	0x0
2834...	I	2	Logout	2025-10-24 09:02:02 GMT+02:00	RES	Albert	0	0	10.220.2.67	SC				0x0
2834...	I	1	Login	2025-10-24 08:57:47 GMT+02:00	RES	Bernhard	1	0	10.220.2.67	SC				0x0
2834...	I	918	Copy system configuration	2025-10-24 08:57:47 GMT+02:00	MOD	Bernhard	1	0	10.220.2.67	SC	/cfc0/mconfig.ini			0x0
2834...	I	2	Logout	2025-10-24 08:58:17 GMT+02:00	RES	Bernhard	1	0	10.220.2.67	SC				0x0
2834...	I	1	Login	2025-10-24 09:03:29 GMT+02:00	RES	Gustav	3	0	10.220.2.67	SC				0x0

1 Login/Logout
2 Details zu Verbindungen und Kommunikationsabläufen
3 Veränderungen an Systemdateien

Information zu eingeloggten Benutzern sowie ein detailliertes Sicherheitsprotokoll geben Übersicht über sicherheitsrelevante Ereignisse.

Security

Ethernet	
Lastbegrenzung	Schutz vor DDoS-Attacken (Distributed Denial of Service) und Defekten in der Netzwerkinfrastruktur (Broadcast Storms)
Firewall [1)]	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.

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

Netzwerkdienste und -protokolle	
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 M200-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 M200.
Protokollunterstützung für das Management von SSL-Zertifikaten	Die M200-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 M200-Steuerung unterstützt das Lightweight Directory Access Protocol (LDAP) für die zentrale Verwaltung von Benutzer-Zugangsdaten und Role Base Access Control durch einen LDAP-Server.
Zentrales Management von Systemmeldungen	Das syslog-Protokoll der M200-Steuerung ermöglicht das zentrale Sammeln von Systemmeldungen in einem Netzwerk durch einen syslog-Server.

Access Control	
Benutzerverwaltung	Auf Gruppen- und Benutzerbasis werden passwortgeschützte Einschränkungen für Systemzugriffe und Applikationsrechte konfiguriert. Vorgabe der Passwortkomplexität sowie 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 Browse-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 benutzerspezifische Anwendungsprogramme 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	Anwendungsprogramme werden auf Speicherebene vor Schreibzugriffen aus anderen Anwendungsprogrammen 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.	
Encrypted Containers	Schutz bei Diebstahl des Datenträgers (CF-/CFast-Karte) vor unerlaubtem Datenzugriff und -manipulation.	
Asset Owner Root of Trust	Kryptographischer Schutz von symmetrischen und privaten Schlüsseln durch einen Master Key.	
Anwendungsprogramm		
Access Control	Auf die Informationen zu eingeloggten Benutzern, deren Session-Status und die Sicherheitsprotokolle kann aus Anwendungsprogrammen zugegriffen werden.	
Security-Bibliothek	Symmetrische, asymmetrische Verschlüsselungsverfahren, Signatur- und Autentifizierungsverfahren, Block- und Stromchiffren, SSL/TLS stehen mittels openssl-Bibliothek den Anwendungsprogrammen 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-256-GCM, AES-256-XTS, ChaCha20-Poly1305
	Asymmetrische Verschlüsselung:	RSA-4096, Ed25519; X25519 für ECDH-Schlüsselaustausch
	Hash-Funktionen:	SHA-256, SHA-384, SHA-512
	MAC-Funktionen:	HMAC-SHA-256, HMAC-SHA-384, POLY1305
	Signaturalgorithmen:	Ed25519, RSA-PSS, ECDSA P-384
	Schlüssel-Austauschverfahren:	TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0
	Zertifikatsvarianten, Daten-Encoding:	PKCS#7, PKCS#12, X.509v3, PEM, DER
	Elliptische Kurven:	Ed25519, X25519, P-384, P-521
Normen, Vorschriften und Empfehlungen		
Security in control systems	Zertifiziert nach IEC 62443-4-2 und IEC 62443-4-1	
Cyber resilience of onboard systems and equipment	Zertifiziert nach IACS UR E27 by Bureau Veritas and DNV, DNV Rules for Classification – Ships Pt.6 Ch.5 Sec.21 Cyber Security	