Security

Security

Communication and information security

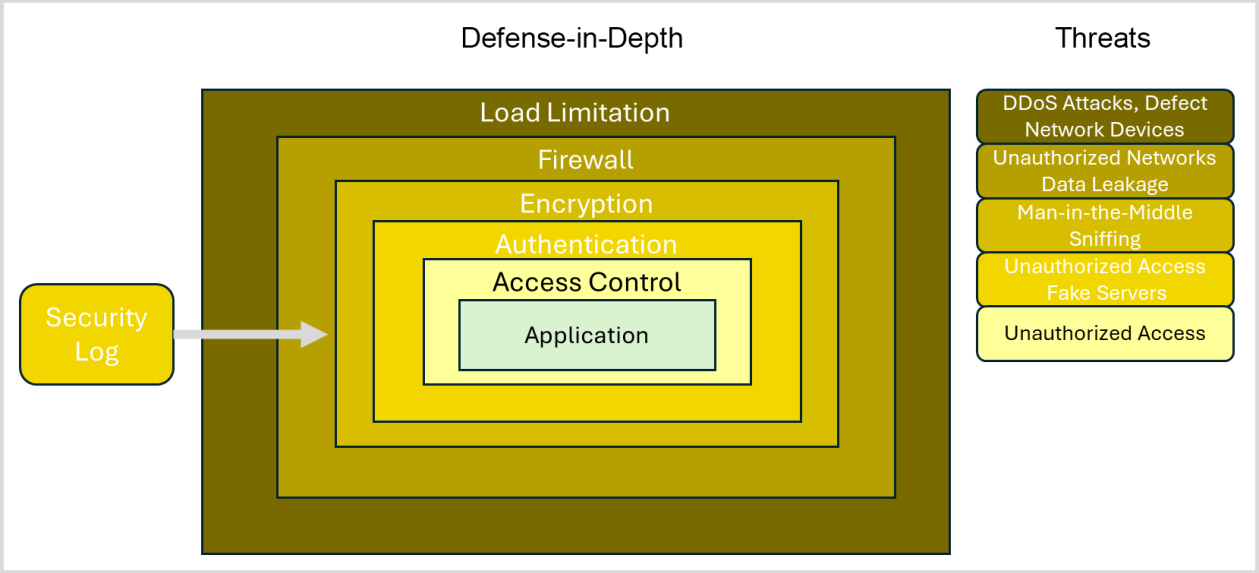
Targeted attacks on industrial control systems are increasing worldwide and can have serious consequences: standstill or even destruction of a machine or plant – resulting in production downtime, reputational damage, and financial loss. Protection against cyberattacks has therefore become a key factor for the safe and continuous operation of industrial facilities.

Securing data and communications, as well as audit logs, are essential measures to prevent unauthorized interventions and to detect security-relevant irregularities at an early stage.

As modern machines and production systems are increasingly integrated into IT and communication networks, for example for remote maintenance, new requirements for information security arise, posing challenges for both plant manufacturers and operators.

Certified security

Bachmann's security solution meets the highest standards of cybersecurity and reliability. It is certified according to IEC 62443-4-2 and thus fulfills all relevant requirements for secure industrial automation and control systems. In addition, it is approved for maritime use in accordance with IACS UR E27. This makes our solution suitable for deployment both in critical infrastructures on land and on ships or offshore installations, where robust, standards-compliant IT security and system availability are essential.



The layer-based security architecture forms multiple security walls around user application programs. Each level includes specific security measures that can also be used in user-specific applications.

Security through Defense-in-Depth

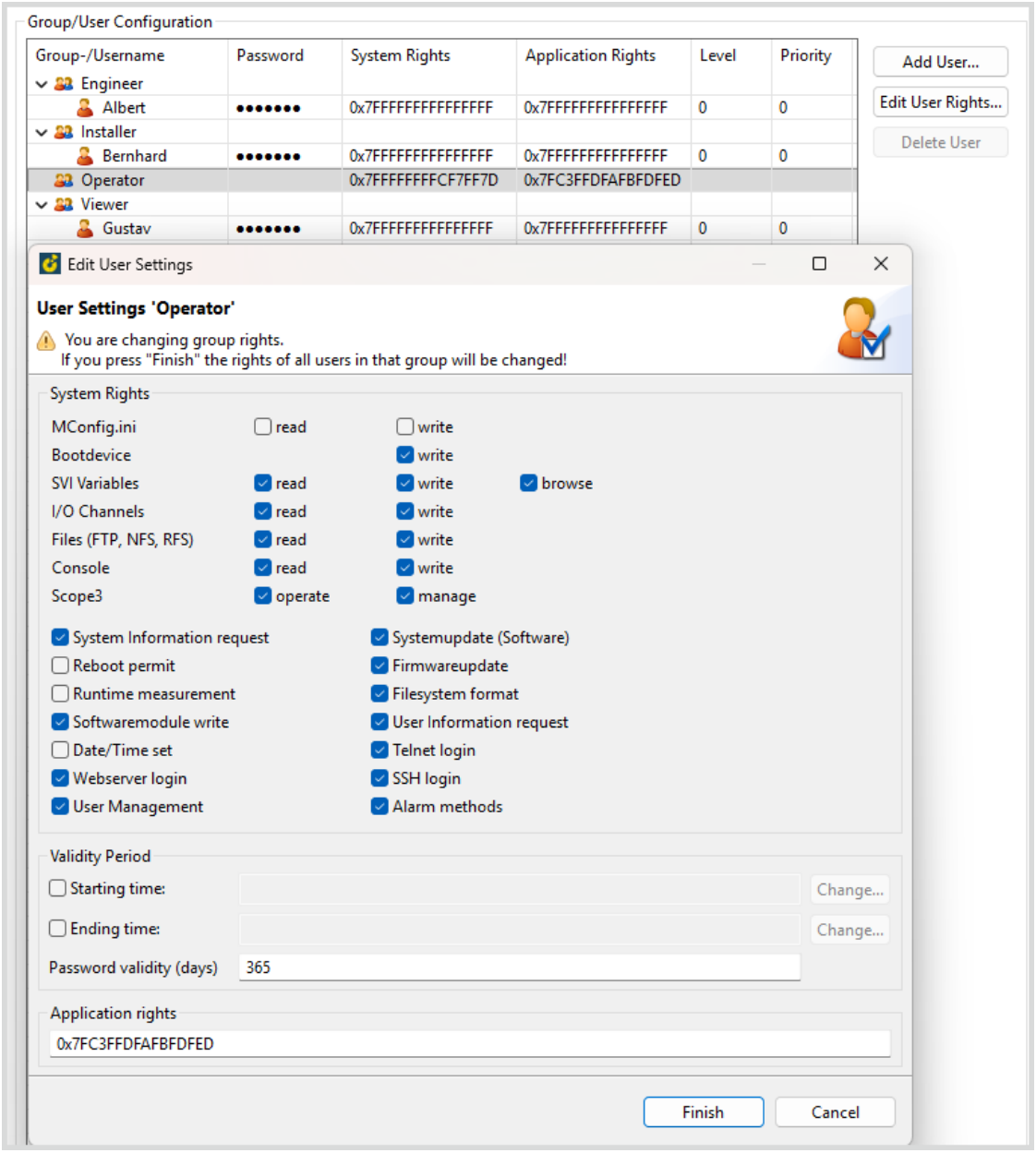
The Defense-in-Depth principle combines multiple interlocking protection mechanisms to ensure that systems remain secure even if one line of defense fails. Bachmann consistently applies this concept to comprehensively safeguard industrial control systems and enhance their resilience against cyber threats.

- Protection against Denial-of-Service attacks ensures the availability of critical functions even under heavy load, network device failures, or targeted attacks.
- Encrypted communication via TLS guarantees data integrity and confidentiality, while server and client certificates restrict access to trusted systems only.
- Access Control and role-based authorization ensure that only authorized users can access critical functions, data, and process variables.
- Regular integrity checks using hash values for critical system components protect system integrity and prevent unauthorized modifications.
- System hardening, such as minimizing the attack surface and consistent patch management, enhances overall stability.
- Security logging provides traceability of all security-relevant events and enables early detection of attack patterns or anomalies.

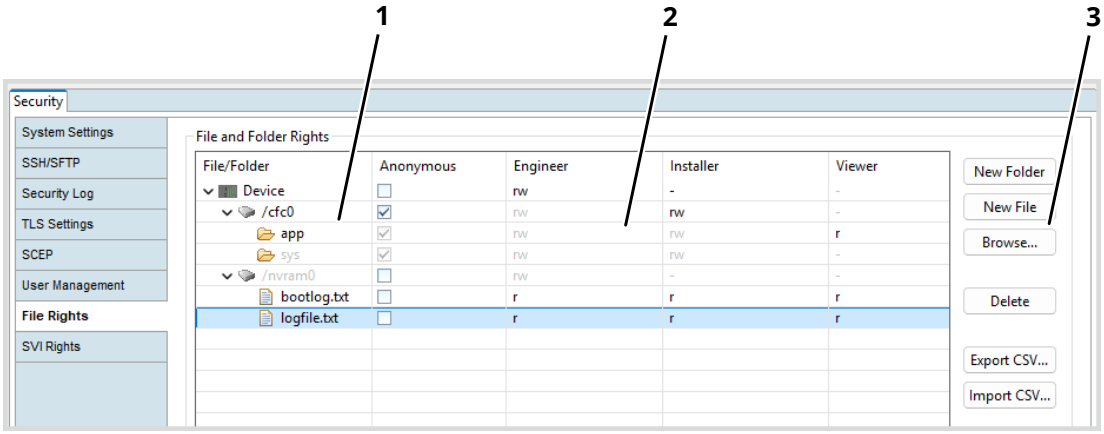
Efficient management

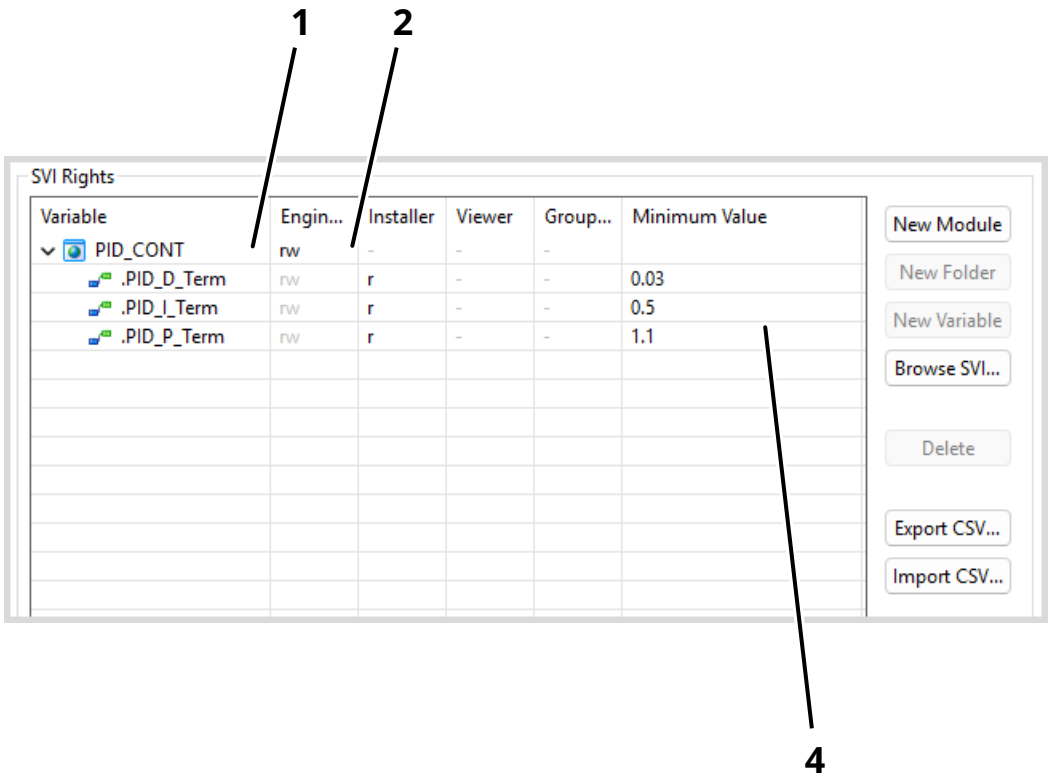
The efficient management of a large number of controllers in critical infrastructures requires the ability of centralized and server-based administration of users and their access rights, SSL certificates and the central logging of system messages.

For this reason, the M200 control system supports the LDAP protocol for central user management, SCEP for the centralized rollout of SSL certificates, and syslog for the logging of system messages. This ensures that administration, security, and traceability remain efficient and transparent at all times.



Access Control includes a powerful module for user and access control. Users and groups can be created by simple copy and paste as well as by integrated inheritance logic thus saving a great deal of time. The clear assignment of system rights allows the specific assignment of rights for each user.





1 Presentation in a clear tree view
2 Finely grained read and write permissions can be assigned user-related directly in the list using the Inline-Editing function
3 Individual files and variables or entire folders are selectable for the rights management using a browser
4 Additionally variables can be limited in the value range

Management of file and variable rights

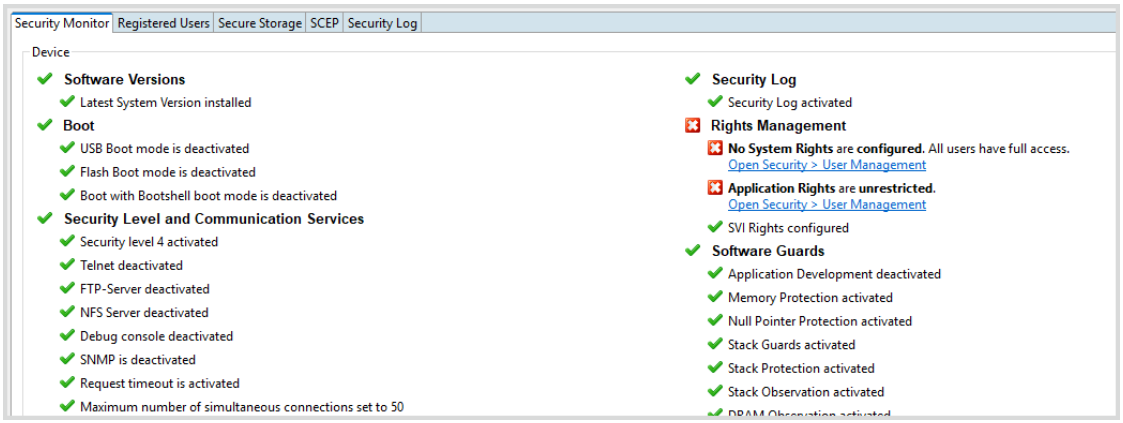
Security Monitor

The Security Monitor consolidates all security-relevant settings of a controller in one clearly structured, central interface. Since modern industrial systems include numerous parameters and aspects related to security, it is easy to lose track. The Security Monitor offers an intuitive, well-organized overview that allows users to quickly assess the current security status and ensure that no important settings are overlooked. It thus supports operators and integrators in consistently implementing security policies and maintaining the integrity and protection of the system over the long term.

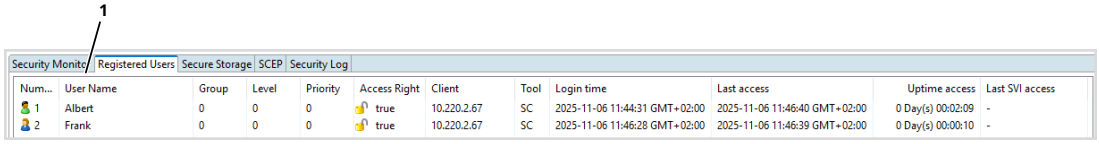
Safety and security

The Bachmann Safety Controller SLC 284 protects against manipulation and misuse, ensuring the integrity of safety-critical programs. Malicious modifications are detected already at the engineering stage, while functions for freezing development states prevent unintentional changes. A customizable login system controls access for each safety controller, and tamper-proof, redundant logging ensures that all events can be fully traced.

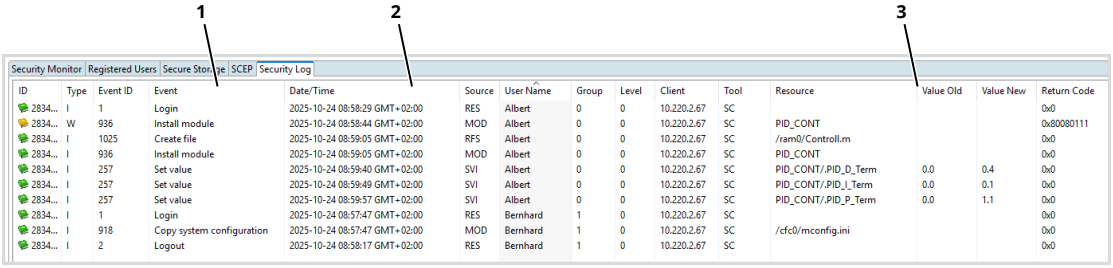
The online security monitor gives comfortable overview:



Security Monitor tab



1 Details to logged in users and the status of the access permission (token)



1 Login/Logout
2 Details to connections and communication status
3 Changes to system files

Information about logged-in users, as well as a detailed security log, provide an overview of security-relevant events.

Security

Ethernet	
Load limitation	Protection against DDoS attacks (distributed denial of service) and defects in the network infrastructure (broadcast storms)
Firewall [1)]	Configurable and during runtime programmable IP- and MAC-filters protect against DoS attacks and enable the targeted hiding of potentially harmful services or defective devices.

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

Network services and protocols	
TLS based network communication	Security standard for the establishment of a secured communication channel at IP level. Support (selection): Bachmann products: Configuration and programming tool SolutionCenter, WebMI Pro, M1COM, MJCOM Manufacturer neutral: OPC UA, web server, file transfer
Server and client authentication	The M200 controller can be an SSL server as well as a client. The client authentication is also supported in server mode. This is used for certificate-based authentication of computers, services and users on the M200.
Protocol support for managing SSL certificates	The M200 controller supports the Small Certificate Enrollment Protocol (SCEP) for the central management and distribution of SSL certificates by an SCEP server.
Secured and deactivatable services (web server, OPC-Server, FTP, NTP, SMTP, etc.)	Unnecessary protocols can be deactivated by configuration. This ensures that only used ports are accessible thus reducing the area for attack.
Central management of user credentials	The M200 controller supports the Lightweight Directory Access Protocol (LDAP) for the central management of user access data and Role Base Access Control via an LDAP server.
Central management of system messages	The syslog protocol of the M200 controller enables system messages in a network to be collected centrally via a syslog server.

Access Control	
User management	Password protected restrictions are configured on a group and user basis for system access and application rights. Specification of password complexity and time-restricted access are supported.
Token-based write access protection	The special mechanism guarantees that the token owner is granted exclusive write permission. Additionally, prioritization can be assigned based on the user role. Various degrees of priority can be assigned at user and group level.
File access	File access, i.e. authorization for the read or write operation as well as the visibility for browser requests can be set at group level. The configuration allows individual assignment of rights at directory and file level and facilitates this by means of the available inheritance logic.
Variable protection	The visibility, read and write access of online available process variables can be allocated to access rights of the individual user. Mechanism and configuration as with file permissions.
User specific extensions provided	The user and access management system as well as the token mechanism can be replaced by user-specific application programs. Thus, special policies and functions can be implemented and the controllers can be integrated smoothly into existing systems.

System		
Permit/disable application development	Protection against installation of unauthorized programs.	
Memory protection	Application programs are protected at memory level against write access from other application programs. Protection against malware that want to eavesdrop and manipulate data at operating system level. Protection against buffer overflows.	
Null pointer protection	Special protection to prevent manipulations via null pointer exception handling.	
Security log with archiving function	Login and logout of users as well as write access are logged at variable level, security relevant modifications are noted. Time stamp, user, group, old and new value as well as further details are stored in continuously generated file archives. Access is offline, e.g. via a central archiving system, but online is also possible via application programs or SCADA systems.	
Predefined security levels	Four templates for simplifying and shortening the security configuration.	
Encrypted containers	Protection against unauthorized data access and manipulation in case of data media theft (CF/CFast card).	
Asset owner root of trust	Cryptographic protection of symmetric and private keys using a master key.	
Application program		
Access Control	The information for logged in users, their session status and security protocols can be accessed from application programs.	
Security library	Symmetric, asymmetric encryption procedures, signature and authentication procedures, block and stream ciphers, SSL/TLS are available to the application programs by means of openSSL library. These functions can be used in PLC in the form of library functions.	
Examples of important cryptographic procedures and secure methods for network communication	Symmetric encryption:	AES-256-GCM, AES-256-XTS, ChaCha20-Poly1305
	Asymmetric encryption:	RSA-4096, Ed25519; X25519 for ECDH key exchange
	Hash functions:	SHA-256, SHA-384, SHA-512
	MAC functions:	HMAC-SHA-256, HMAC-SHA-384, POLY1305
	Signature algorithms:	Ed25519, RSA-PSS, ECDSA P-384
	Key transfer process:	TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0
	Certificate variants, data encoding:	PKCS#7, PKCS#12, X.509v3, PEM, DER
	Elliptic curves:	Ed25519, X25519, P-384, P-521
Standards, regulations and recommendations		
Security in control systems	Certified in accordance with IEC 62443-4-2 and IEC 62443-4-1	
Cyber resilience of onboard systems and equipment	Certified according to IACS UR E27 by Bureau Veritas and DNV, compliant with DNV Rules for Classification – Ships Pt.6 Ch.5 Sec.21 Cyber Security	