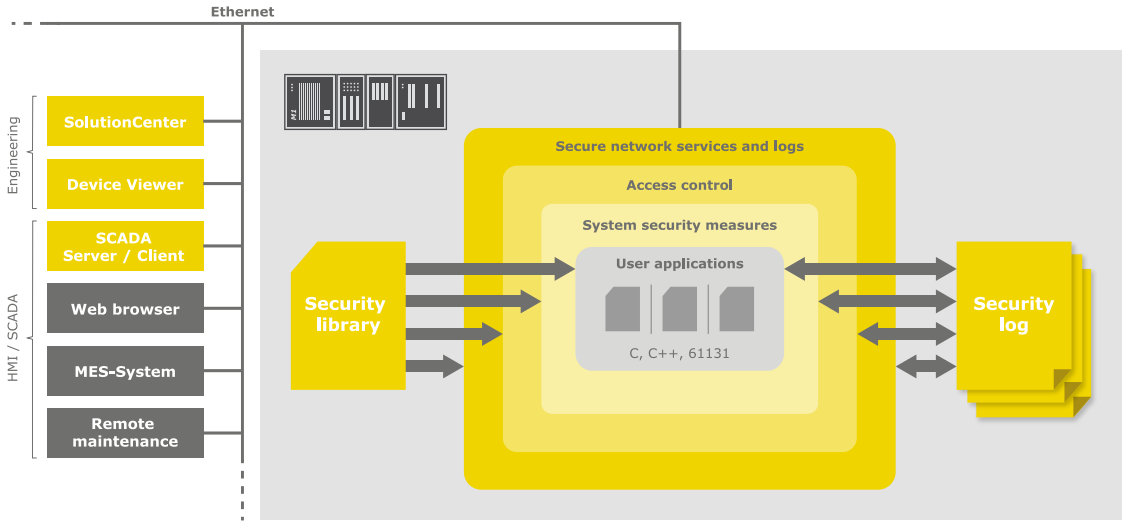
Security
Communication and Information Security

The direct consequences of targeted, destructive access to a machine controller or an unintentional operating error are the same: standstill or even destruction of a machine or plant and thus production stoppage, loss of reputation and money. Ensuring robustness against disturbance is therefore the top priority. Securing data and communication and logging access are preventive measures that make unauthorized access more difficult and bring anomalies to light.

Targeted access

Exposed machines and plants are not subject to the same perimeter protection as enclosed industrial plants. Hence, wind turbines or biogas plants are relatively easy to access and the response times in the event of a detected break-in are high. High risk in production plants mainly emanates from legitimized persons. Service staff from the external service provider or a dismissed employee who in frustration succumbs to the temptation of a targeted act of damage to property are two classical examples. The targets here are switches, routers and controllers with free ports. These can be used for inconspicuous disruption or for targeted interception of communications.



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.

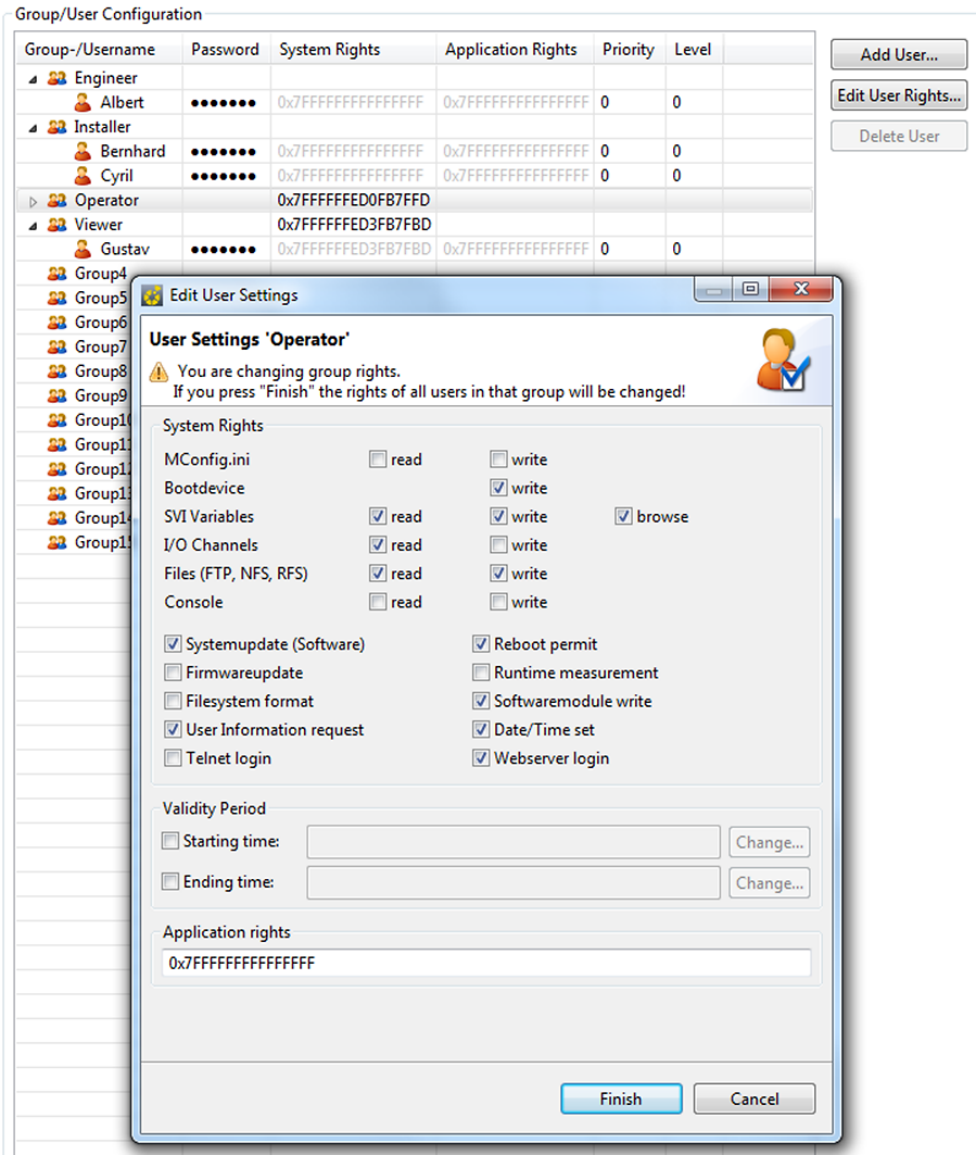
Hardware components of Bachmann have various measures for counteracting targeted access. Effective mechanisms are in place for protecting against network overload which ensure stability of the application in the event of denial of service attacks. Vigorous implementation of end-to-end encryption of the communication by SSL renders eavesdropping ineffective. Application programs use interfaces to current cryptographic procedures to encrypt data.

Critical infrastructures

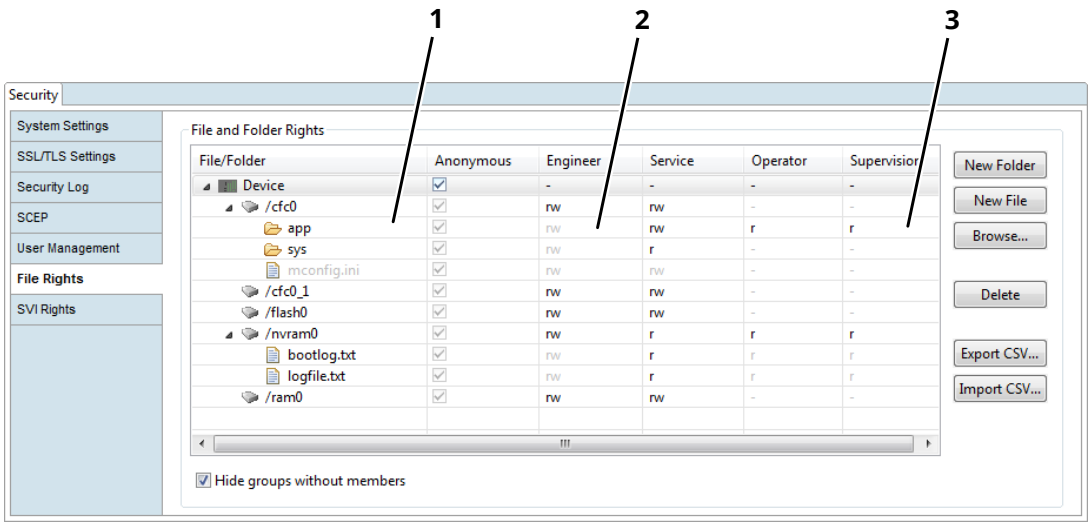
Guided by national and international regulations, public utility companies are particularly sensitized in matters of security and are obligated to protect their plants accordingly. Comprehensive measures embedded in detailed security concepts at all organizational levels have long been established.

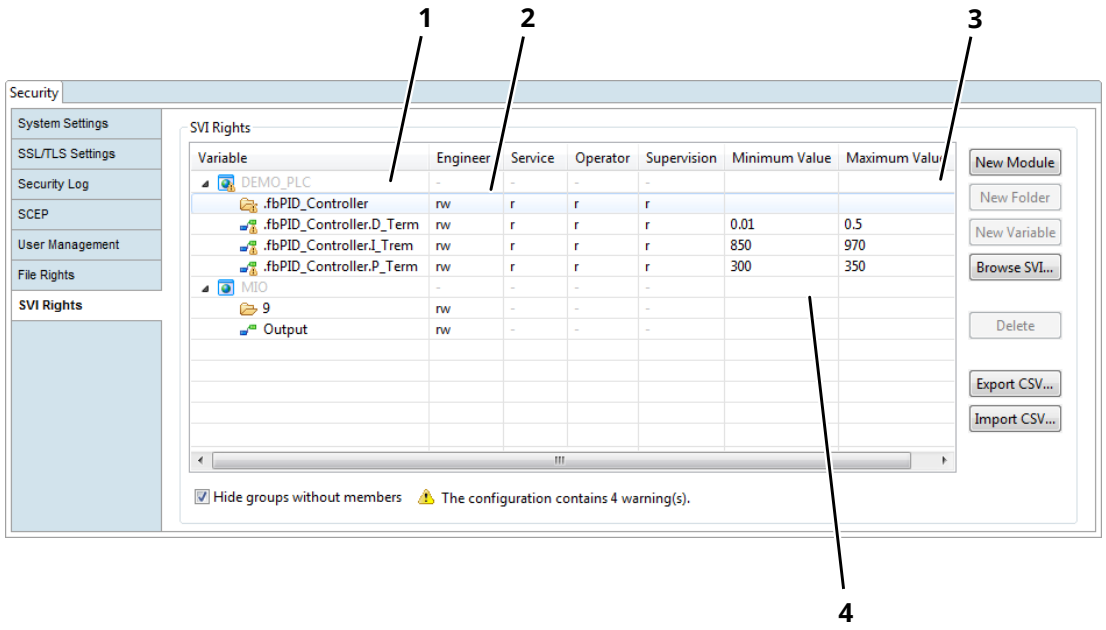
Protective fencing, own surveillance staff and continuous access controls have been found in critical parts of these plants. Control networks and operating panels were strictly sealed off previously. In the meantime, modern business and service models require targeted access of other organizational components via intranet and even externally via internet.

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.



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

Defects and operating errors

Targeted security management not only helps in the case of undesirable and potentially destructive access. Accidental changes to machine parameters, failures of network components or misconfigurations of the machine network are far more common, especially in the protected environment of production plants, but pose the same security threats in terms of symptoms and effects. For example, a broadcast storm as a result of a faulty network switch, overloads connected network clients in the same way as a targeted denial of service attack.

Unlike other security measures, the added value of revealing defects can only be achieved if appropriate protective measures directly affect the controller.

Basic protection in three steps:

1. **Safeguarding the system and network**
   - setting the **security level**
   - deactivating unnecessary services
   - activating **logging**
2. **Limiting access**
   - **defining group rights**
   - **creating users**
   - **setting file rights**
3. **Securing application programs**
   - implementing **applications** while taking general security aspects into account

Recommended procedure for safeguarding the controller

Bachmann provides its controllers with functions for limiting the bandwidth of the networks in order to increase the robustness against intentional and unintentional network disturbances. Real time processes are not disturbed by overloading of the network interface.

It is advisable to set up a user and access management system for each user via Access Control. This limits any possibilities of manipulation centrally according to the least privilege principle, and independent security logging allows changes to be allocated to individual users. Operating errors can thus be detected and warranty cases processed quickly.

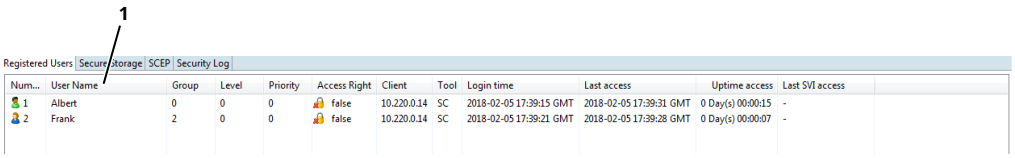
Safety und Security

Functional safety requires a high degree of security measures to prevent operating errors and targeted manipulation. Unnoticed changes to the safety programming as well as dangerous interferences during safe operation must be prevented and logged. Safety Control of Bachmann already warns about any malicious, manipulated code on the configuration computer and protects against inadvertent changes by means of functions for pinning software versions. A separate login system on each safety controller allows individually restrictable access. The continual logging is tamper-proof and implemented redundantly, so that even in the case of partial destruction of the module, it will be possible to reproduce the chain of events up to the failure with a high degree of probability.

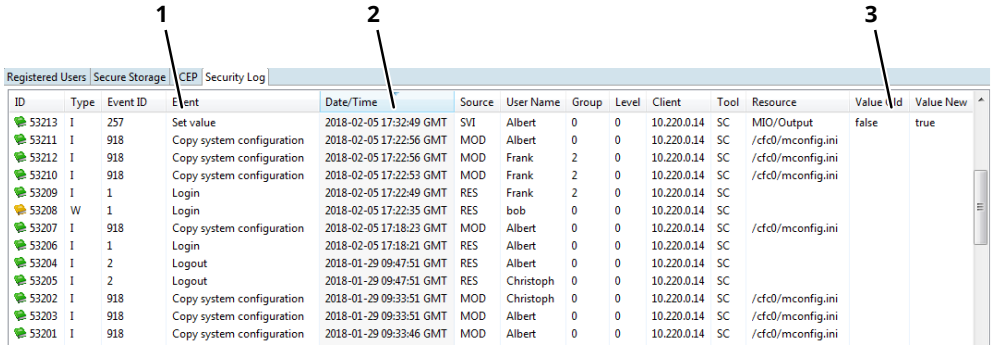
Simply secure

Security measures are only effective if they are also applied. Bachmann sees it as its task to promote the comprehensive application and dissemination of security functions even if consistent security concepts do not yet exist and the staff are not yet security experts. Simple activation and operation of the extensive protective measures ensure that the dangers of careless operation and simple attacks are minimized even at this early stage. The central part is composed of four predefined security levels that can be selected in the security configurator. Behind this are templates which automatically set the settings within the controller so that certain protocols and functions are activated or even forbidden depending on the level.

The online security monitor gives comfortable overview:



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

Security

Ethernet	
Load limitation	Separately adjustable limitation of the read and write workload for each Ethernet interface; Protects the machine application against DDoS attacks (Distributed Denial of Service), Broadcast Storms and defects in the network infrastructure.
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	
SSL/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. Time-restricted access is provided.
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	User and access management system as well as the token mechanism can be replaced by customized 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.
Partition encryption [1)]	Transparent encryption (AES128/192/256) via SolutionCenter. Protection against unauthorized data access and manipulation in case of data media theft (CF-/CFast).

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

User 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, 3DES
	Asymmetric encryption:	RSA
	Hash functions:	SHA, RIPEMD, MD5
	MAC functions:	CBC-MAC, HMAC
	Signature algorithms:	RSA-PSS, ECDSA
	Key transfer process:	SSL/TLS (TLS 1.2, TLS 1.1, TLS 1.0, SSL 3.0)
	Certificate variants, data encoding:	PKS7, PKS12, x509

Standards, regulations and recommendations	
Security in Control Systems	The security measures were implemented while taking the following standards, regulations and recommendations into account: IEC 62351, IEC 62443, ISA 99, VDI/VDE 2182, FIPS 140, NIST 800 series
Publisher	BSI, BDEW, NERC
System requirements	
Automation devices	M200 CPUs of the MX200 series or better
Engineering PC	For system prerequisites see SolutionCenter
Runtime software	M-Sys / MxCCore ≥V3.80
Engineering software	M-Base ≥3.80
Installation medium	Included in M-Base (runtime and engineering components)