信息安全 - 通信与信息的保护

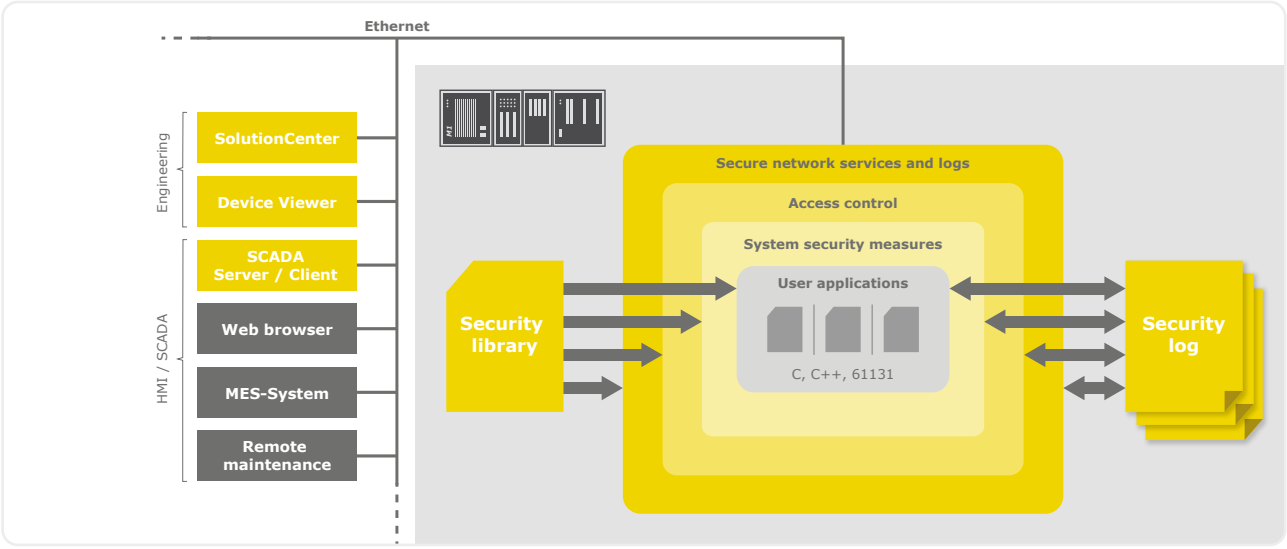
不管是对机器控制器进行以破坏为目的的访问，还是发生了意外的错误操作，它们的直接后果都是相同的：机器/设备停机或损毁，生产中断，名誉扫地还浪费大笔金钱。确保系统具备有效对抗干扰的鲁棒性成为了最高目标。对数据和通信的保护以及对访问的日志记录都属于预防性措施，这些措施能使非法访问更加困难，并且将异常情况大白于天下。

有针对性的访问

就周边保护措施而言，暴露在外的机器和设备与封闭起来的工厂设备肯定是不同的。比如，风能设备或沼气设备就相对比较易于接近，因为在侦测出有人闯入时它们的反应时间很长。

生产设备中的大部分风险都是由合法人员引起的。举两个经典的案例：其一，来自于外部服务商的服务人员发生误操作，其二，已经被解雇的同事在冲动之下以破坏为目的进行访问。

交换机、路由器、带有空闲端口的控制器是最大的目标：可以通过它们进行隐蔽的干扰，或者对通信进行有针对性的监听。



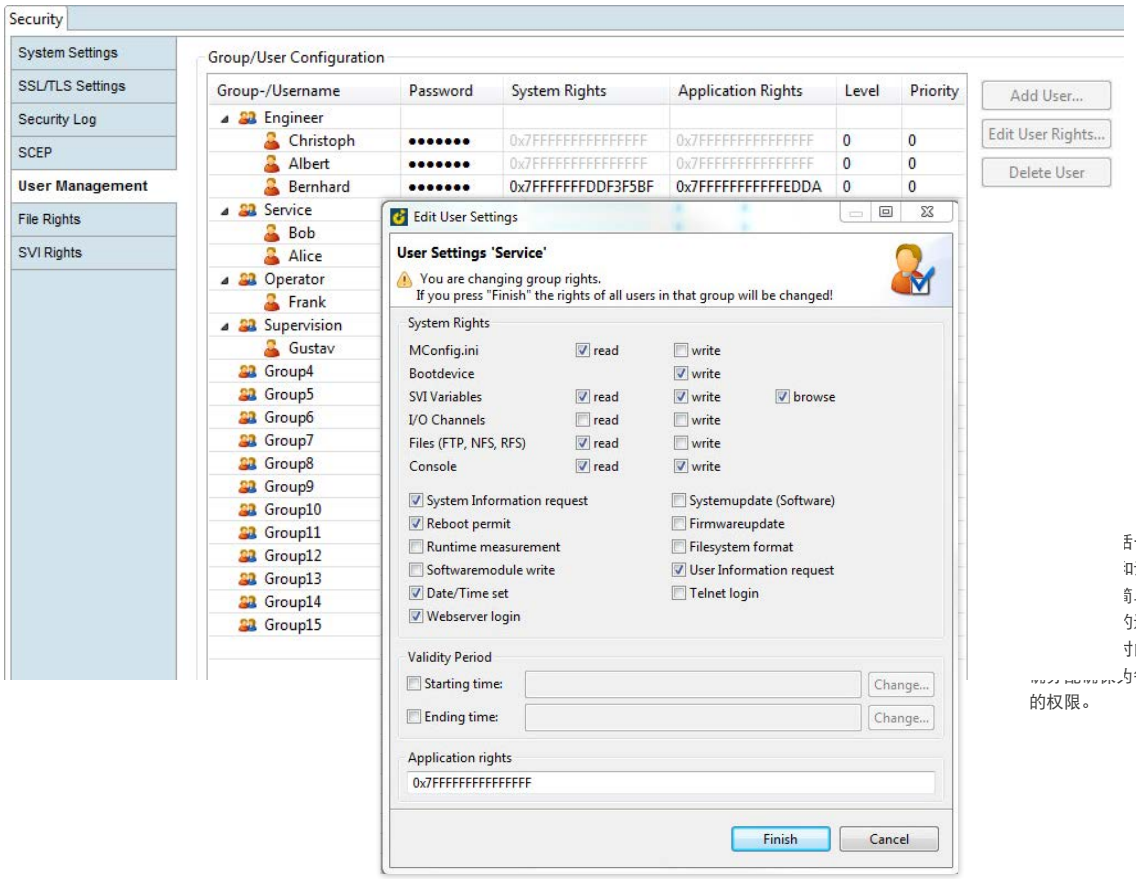
基于层的安全架构围绕用户应用形成了多重安全墙。每个级别都采用特定安全措施，这些措施还可用于用户特定的应用。

巴合曼的控制组件有各种措施对抗有针对性的访问。已建立的有效机制可以防止网络过载，确保在拒绝服务攻击的情况下应用的稳定性。通过 SSL 高效地实现通信的端到端加密，使窃听失效。用户程序利用当前加密程序的接口加密数据。

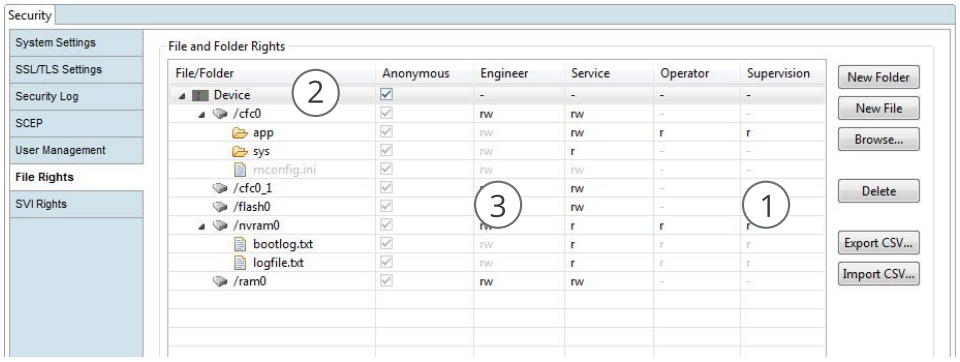
关键基础设施

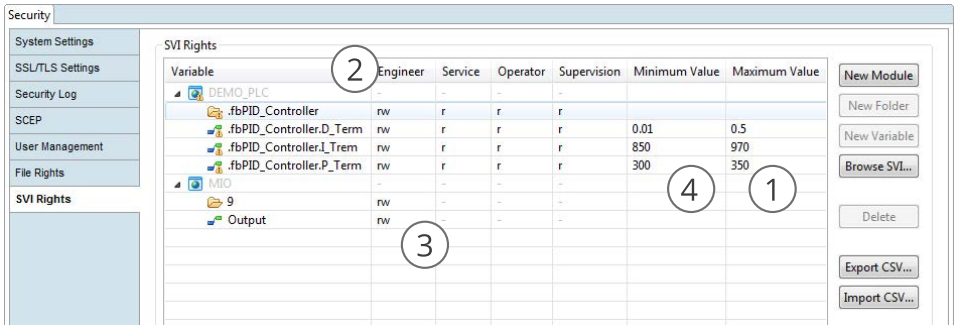
在国内外一系列法规的约束下，供能企业对于安全保护的问题尤为敏感，并且有义务采取相应措施对自己的设备进行保护。长期以来，在所有组织级别的详细安全概念中都已嵌入了全面的措施。这些工厂的关键部分设置了防护围栏、监控专管员和持续的访问控制。控制网络和操作面板很早以前就进行了严格的隔离。与此同时，现代业务和服务模式要求通过内部网、甚至通过互联网从外部访问其他组织组件。

要在关键基础设施中对大量控制器进行高效管理，需要能够管理用户及其访问权限、SSL 证书和系统消息的中央日志记录。因此，M1 控制器系统支持用于集中用户管理的 LDAP 协议、用于集中发布 SSL 证书的 SCEP 以及获取系统消息的系统日志。



括一个面向用户的强
和访问控制。用户和
简单的复制粘贴以及
的逻辑进行创建，从
时间。系统权限的明
为每个用户分配特定
的权限。





文件和变量权限管理：

(1) 使用浏览器进行权限管理，可选择单个文件和变量或整个文件夹。

(2) 一目了然的树状结构呈现。

(3) 使用内联编辑功能，可以在列表中直接分配与用户相关的细分读写权限。

(4) 此外，可以限定变量的范围值。

缺陷和操作错误

有目的性的安全管理不仅仅有助于避免非预期的访问或者存在潜在破坏可能的访问。机器参数的意外变更、网络组件故障或机器网络配置错误的情况要频繁得多，这在生产设备的受保护环境中尤为明显，其状况和后果与外部入侵对安全防范造成的危害性旗鼓相当。例如，由于网络交换机故障而导致的广播风暴，导致连接的网络客户端过载，其方式与有针对性的 Dos 攻击相同。

与其他安全措施不同的是，只有在适当的保护措施直接影响到控制器的情况下，才能查明损坏原因。巴合曼为其控制器提供了限制以太网端口带宽的功能，目的是提高抵御有意和无意网络干扰的鲁棒性。实时过程不会因网络接口过载而受到干扰。

建议通过访问控制功能 (Access Control) 为每位用户建立用户和访问管理。这样，就可以根据最小特权 (Least Privilege) 原理集中限制误操作的可能。同时，独立的安全日志记录还可以对各个用户所做的更改进行归类。错误操作因此大白于天下，可以尽快展开担保索赔程序。

基本保护的三个步骤：

1

保护系统和网络
- 设置**安全级别**
- 禁止不必要的服务
- 启用**日志记录**

2

限制访问
- **定义组权限**
- **创建用户**
- **设置文件权限**

3

保护用户程序
- 在实现**应用程序**的同时考虑到通用的安全方面

用于保护控制的推荐程序

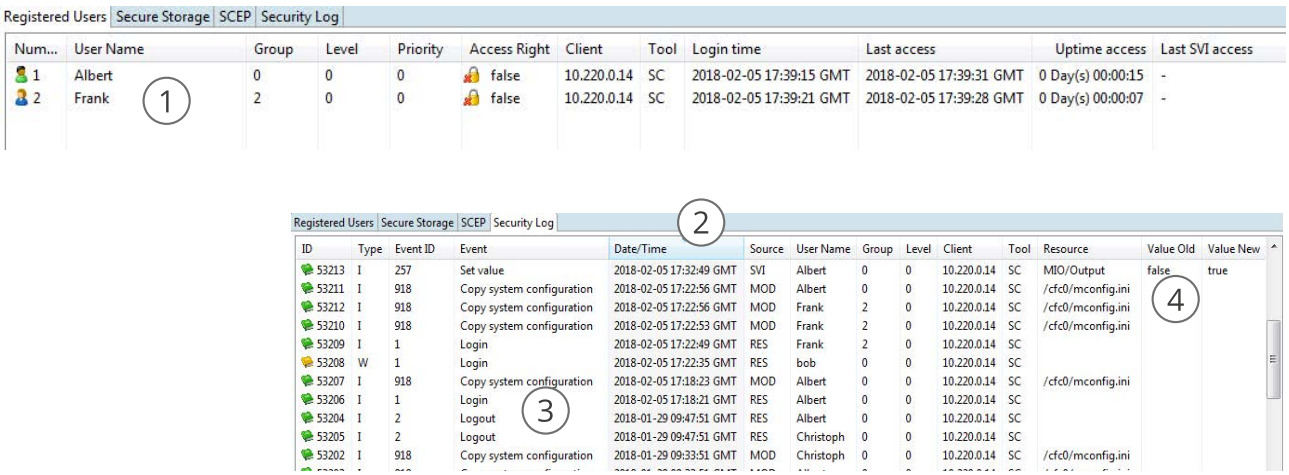
安全保护和安全防范

功能安全有责任使安全防范措施达到最高水平，以避免错误操作和有目的性的误操作。必须防止有人对安全程序进行非常隐秘的更改，以及在安全运行过程中进行危险的干预，一旦发生这种情况，必须将其记录下来。巴合曼的安全控制功能 (Safety Control) 在出现恶意操作代码之前就在组态计算机上发出警报，并通过开发状态冻结功能来避免意外更改。每个安全控制器都有自己独立的登录系统，可以根据个性化的需求对访问进行限制。实现了无缝的日志记录，具有误操作保护和冗余等特点，这样即便是在模块部分损坏时，也很有可能能够追溯包含停机在内的全部事件链。

安全可靠，易如反掌

安全措施只有得到了切实的应用，才能真正确保安全。巴合曼始终将促进安全功能的全面应用和传播视为其重要任务，即使是不存在全面的安全理念，即便没有安全专家，也可以毫不费劲地使用巴合曼的安全措施。简单的启用并操作广泛的保护措施，可以确保操作疏忽和简单攻击的危险在这个早期阶段降到最低水平。

核心部分由四个预定义的安全级别组成，它们可以在安全配置器中进行选择。这背后是在控制其中进行设置的模板 - 根据级别的不同，某些日志和功能会被启用或禁止。



安全监视器提供简洁的在线概览

(1) 基于登录用户和令牌状态的详细信息

(2) 安全日志条目显示连接和通信状态的详细信息，例如：登录/退出(3)或为变量赋值(4)

信息安全	
以太网	
负载限制	可单独调节每个以太网接口的读写工作负载限制； 在发生 DDoS 攻击、广播风暴和网络基础设施故障时保护机器应用免受影响。
防火墙[1)]	可配置以及运行期间可编程的 IP 和 MAC 过滤可防止 DoS 攻击，并允许动态阻断潜在的有害服务或网络设备。
网络服务和日志	
基于 SSLTLS 的网络通信	建立 IP 级安全通信通道的安全标准。 支持（选择）： 巴合曼产品：配置和编程工具 SolutionCenter、WebMI Pro、M1COM 和 MJCOM 跨品牌通用：OPC UA、webserver、file transfer
服务器和客户端身份验证	M1 控制器既可以是 SSL 服务器，也可以是客户端。 在服务器模式下也支持客户端身份验证。这用于 M1 上基于证书的计算机、服务和用户身份验证。
管理 SSL 证书的协议支持	M1 控制器支持小型证书注册协议（SCEP），用于 SCEP 服务器对 SSL 证书的集中管理和分发。
安全且可停用的服务（网页服务器、OPC 服务器、FTP、NTP、SMTP...）	不必要的协议可以通过配置停用。这确保了只能访问使用的端口，从而减少攻击区域。
集中管理用户凭证	M1 控制器支持轻量级目录访问协议 （LDAP），通过 LDAP 服务器集中管理用户访问数据和角色基础访问控制。
系统消息的集中管理	M1 控制器的系统日志协议使网络中的系统消息能够通过系统日志服务器集中收集。
访问控制	
用户管理	密码保护限制是在组和用户基础上进行配置，从而获得系统访问和应用权限。提供限时访问。
基于令牌的写访问保护	专用机制保证令牌所有者获得专属写入权限。此外，还可以根据用户角色分配优先级。可以在用户和组级别分配不同的优先级。
文件访问	文件访问（即读写操作授权）以及浏览请求的可见性可以在组层面进行设置。该配置允许在目录和文件层面上单独分配权限，并通过可用的继承逻辑加以实现。
变量保护	可将在线可用流程变量的可见性、读写访问权分配给单个用户。与文件权限一样的机制和配置。
提供特定于用户的扩展	用户和访问管理系统以及令牌机制可以由特定于用户的应用替代。因此可以执行特殊政策和功能，并将控制措施顺利地集成到现有系统中。

1) M-Base/M-Sys/MxCCore ⩾ V3.95

信息安全	
系统	
启用/禁用应用开发	防止安装未经授权的程序。
存储器保护	应用在存储器级别上受到保护，免受来自其他应用的写访问。 防止恶意软件在操作系统层面窃听和操纵数据。防止缓冲溢出。
空指针保护	特殊保护：通过空指针异常处理来防止发生操作。
具有存档功能的安全日志	用户的登录和注销以及每次写访问都在变量层面进行记录，并注明与安全相关的修改。 时间戳、用户、组、旧值和新值以及更多详细信息都存储在不断生成的文件存档中。 访问是离线进行（例如：通过中央存档系统），但还可以通过应用程序或 SCADA 系统进行在线访问。
预定义的安全级别	四个模板用于简化和缩短安全配置。
分区加密[1)]	通过 SolutionCenter 进行透明的数据加密（AES128/192/256）。数据介质被盗（CF-/CFast）时避免出现未经授权的数据访问和操纵。
用户应用	
访问控制	登录的用户、用户会话状态和安全协议信息可以从用户程序进行访问。
安全库	对称、非对称加密程序、签名和身份验证程序、块和流密码、SSL/TLS 可通过 openSSL 库提供给应用程序。 这些功能可以以库功能的形式在 PLC 中使用。
网络通信重要加密程序和安全方法示例	对称加密：AES，3DES 非对称加密：RSA 散列函数：SHA，RIPEMD，MD5 MAC 函数：CBC-MAC，HMAC 签名算法：RSA-PSS，ECDSA 密钥传输过程：SSL/TLS（TLS 1.2，TLS 1.1，TLS 1.0，SSL 3.0） 证书变体，数据编码：PKS7，PKS12，x509
标准、规定和建议	
控制系统中的安全防范	在实施安全措施的同时，还考虑以下标准、规定和建议： IEC 62351，IEC 62443，ISA 99，VDI/VDE 2182，FIPS 140，NIST 800 系列
发行方	BSI，BDEW，NERC
系统先决条件	
自动化设备	MX200 系列或更高版本的 M1 CPU
工程 PC	系统先决条件参见“SolutionCenter”
运行软件	M-Sys/MxCCore ⩾ V3.80
工程组态软件	M-Base ⩾ 3.80
安装介质	包含在 M-Base（运行和工程组件）中

1) M-Base/M-Sys/MxCCore ⩾ V3.95