SIEMENS

# 工业安全指导

Industrial Security operational guidelines

**User Guide** **Edition (2012 年 2 月)**

**摘　要** 本内容是涉及工业安全的重要性以及工业安全实施的指导方针。

**关键词** 工业安全　工厂安全　工厂 IT 安全

**Key Words** Industrial Security　Plant Security　Plant IT Security

# 目　　录

1 工业安全介绍 ..... 4
1.1 工业安全概述 ..... 4
1.2 工业安全的重要性 ..... 4
1.3 工业安全与办公安全的不同 ..... 4
1.4 工业安全分级的基本原则 ..... 5
1.5 工业安全国际标准 ..... 6
1.6 工业安全管理 ..... 7
2 工业安全的实施 ..... 8
2.1 安全的组织和安全的策略 ..... 8
2.2 工厂安全 ..... 8
2.3 工厂 IT 安全 ..... 8
2.3.1 网络分段 ..... 9
2.3.3 补丁管理 ..... 12
2.4 访问保护 ..... 14
2.4.1 未授权的操作修改的保护 ..... 14
2.4.2 运行期间操作员站的保护 ..... 14
2.4.3 编程阶段的组态操作保护 ..... 14
2.4.4 对网络的访问保护 ..... 15
3 综述 ..... 15

# 1 工业安全介绍

## 1.1 工业安全概述

由于以太网技术的优越性，使其在工业领域的各个方面得到了广泛的应用，甚至被应用到现场总线技术上，但对于工业领域中的安全的问题也随之而来。毕竟，生产系统的开放通信和网络规模的不断增大带来的不仅是巨大的机遇同时也带来了高的风险。为了提高工业工厂全面的 IT 安全防止被攻击，需要采取相应的措施。西门子向客户提供全面的工业信息安全支持，包括产品、系统、解决方案，以及专业的咨询服务。

工业信息安全不是一个单纯的技术问题，而是一个从意识培养开始，涉及到管理、流程、架构、技术、产品等各方面的系统工程。目前，部署纵深防御是工业领域应对安全挑战的现实方法。工业信息安全是一个动态过程，需要在整个工业基础设施生命周期的各个阶段中持续实施，不断改进。

## 1.2 工业安全的重要性

安全在工业中非常重要，它保护着工厂的生产和工厂的自动化系统。目前对于工厂来说，可能受到的威胁：

- 监听数据, 配方,…
- 破坏工厂的生产
- 由病毒和木马导致工厂停机
- 操纵数据或应用软件
- 未被授权却能使用系统的功能

上面的威胁可能造成下列的安全事件：

- 有人员伤亡和严重伤害的风险
- 环境灾难
- 知识产权的侵犯
- 产品的减量或者质量降低
- 破坏了公司形象和财务的损失

## 1.3 工业安全与办公安全的不同

信息安全有三个重要因素：保密性、完整性、可用性。

保密性：防止未授权的人浏览和使用数据。

完整性：数据是正确的、完全的且直接来源于发送方的。

可用性：网络与参与者必须保证通讯在指定的时间内发生。

从网络安全的角度，传统的办公及 IT 网络对保密性和完整性的要求是非常高的。对于工厂的控制系统来说，安全操作的维护和对人力及固定资产的保护的优先权是最高的。因此过程控制系统中可用性是安全的重要因素。

工业安全的需求必须满足一个工业的环境，具有下列的特点：

- 24/7/365 可用性第一重要
- 持续的操纵性和系统的可访问性
- 系统性能
- 防止无意或有意的的操作
- 知识产权的保护
- 系统和数据的完整性
- 数据的实时传输
- 支持贯穿一个工厂的整个生命周期
- 安全追踪和管理变化

### 1.4 工业安全分级的基本原则

一般可把工业安全分为 3 个级别：工厂安全、工厂 IT 安全、访问保护。如下图 1 所示。

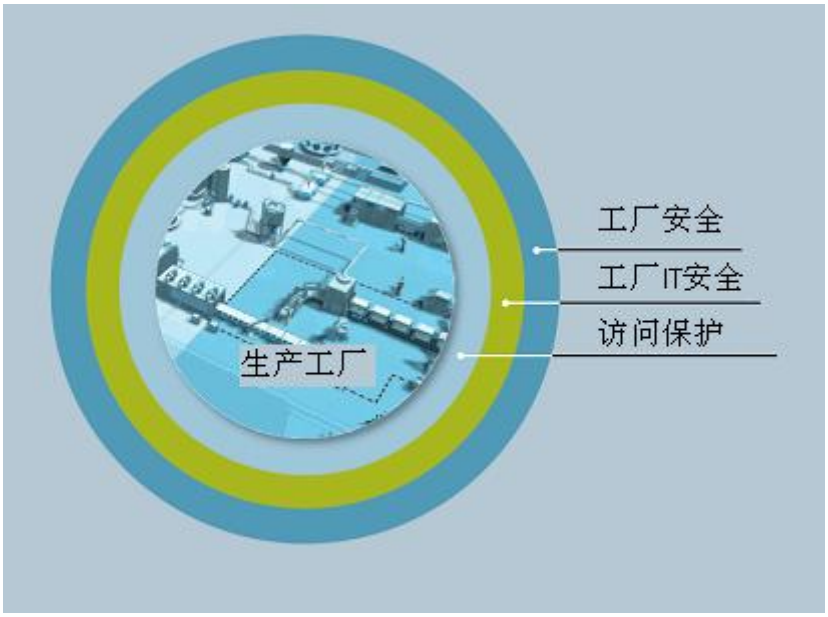


图 1、工厂安全分级

**工厂安全**

- 对未授权人的访问的禁止
- 对关键设备的预防性禁止访问

**工厂 IT 安全**

- 对办公网络与工厂网络之间的接口进行控制。例如：防火墙
- 对办公网络的进一步分割
- 防病毒和白清单软件
- 维护和升级处理

**访问保护**

- 对工厂或者机器操作员的用户验证
- 自动化组件中集成访问保护机制

工业的安全解决方案必须考虑到所有的层级。

## 1.5 工业安全国际标准

工业安全是需要每个人的贡献。IEC62443 标准涉及了工业安全的各个方面。如下图 2 所示。

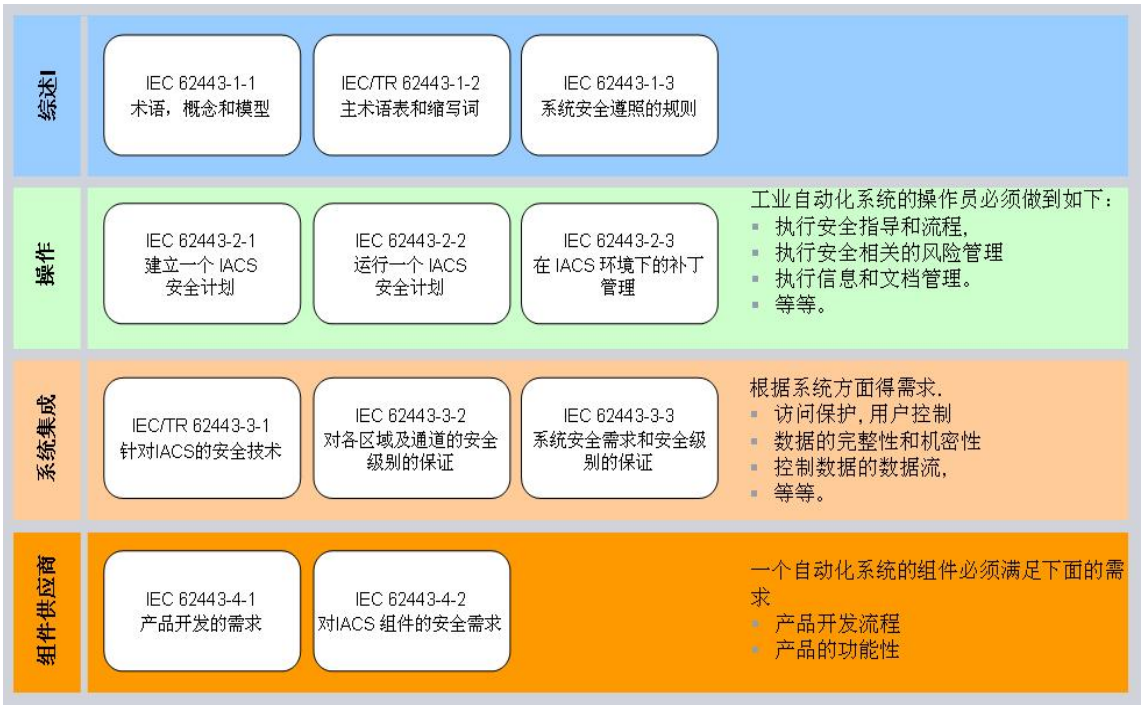


图 2、IEC62443 标准

## 1.6 工业安全管理

工业安全管理流程。如下图 3 所示。


图 3、工业安全管理流程

安全管理是形成工业安全管理概念的重要的一部分。定义安全的措施取决于工厂的危险和风险识别。达到和维持必须得安全级别，需要严格的安全管理流程。包括有风险分析及定义相应的对策使风险减小到可接受的级别、协调组织/技术措施、定期/基于事件的重复。需要生产商，系统集成商和操作员考虑工业安全。

风险分析对于工厂或者机器设备的安全管理是一个非常主要的前提, 主要识别和评估危险及风险。

典型的风险分析内容包括如下方面：

- 鉴定受到威胁的对象
- 分析威胁程度和损害的可能性
- 威胁和弱点的分析
- 认识存在的安全措施
- 风险评估

被评估的且不能接受的风险必须通过某种措施来消减。

那些最终被接受的风险仅能用于特定的应用场合。然而，并不能通过一种措施或者组合的措施来保证 100% 安全。

# 2 工业安全的实施

## 2.1 安全的组织和安全的策略

工业安全不是只通过技术措施行之有效, 而是需要积极应用到公司的相关单位的持续执行的流程中。

工业安全作为一种管理的职责。需要高级管理人员全面支持工业安全；需要清晰的定义工厂的工业安全、IT 安全和常规安全各自的职责；需要建立一个逻辑组织 / 负责工业安全的相关事情 。

加强安全意识。起草并定期举办关于产品生产安全的主题活动；从社会工程角度评估安全。

## 2.2 工厂安全

工厂安全是从物理上保护关键的生产设备。

从如下的方面对关键的生产设备进行风险分析：

- 未被授权的人访问生产设备及生产车间。
- 从物理上破坏或更换生产设备。
- 由于间谍活动，丢失了保密的信息。

公司安全措施如下：

- 对重要的设施加隔离装置或进行监控。
- 对关键的自动化组件的物理访问保护 (例如：加锁控制柜)
- 访问者或外部人员需要有内部员工的陪同。

总之，从工厂安全方面需要考虑如下：

- 相应的措施和流程防止在工厂环境中未被授权用户的访问
- 从物理上分成不同的生产区域，采用不同的访问授权
- 对关键的自动化组件的物理访问保护 (例如：加锁控制柜)

## 2.3 工厂 IT 安全

工厂 IT 安全是对产品生产的特定的 IT 安全措施。像类似防火墙的网络安全机制, 阻止或协调办公网络与工厂网络的通讯；以及对工厂网络的分段来限制和保护子网间的安全通讯 (保护自动化网络) ；可以通过相应的措施减少攻击弱点，应用反病毒和白名单软件防止计算机受木马病毒的攻击； 维护和更新的流程确保自动化系统最新 (例如. 补丁管理, 软件升级等) 。

### 2.3.1 网络分段

网络分段的第一步是严格分离生产网络和其它的公司网络。最简单的情况下，通过单一防火墙系统来控制和协调与其它网络的通讯。最安全的方式连接一个 DMZ （非军事管理区）网络，生产网络与公司网络直接的通讯是被防火墙完全阻止；通信只能间接的通过 DMZ 网络中的服务器。如下图 4 所示。

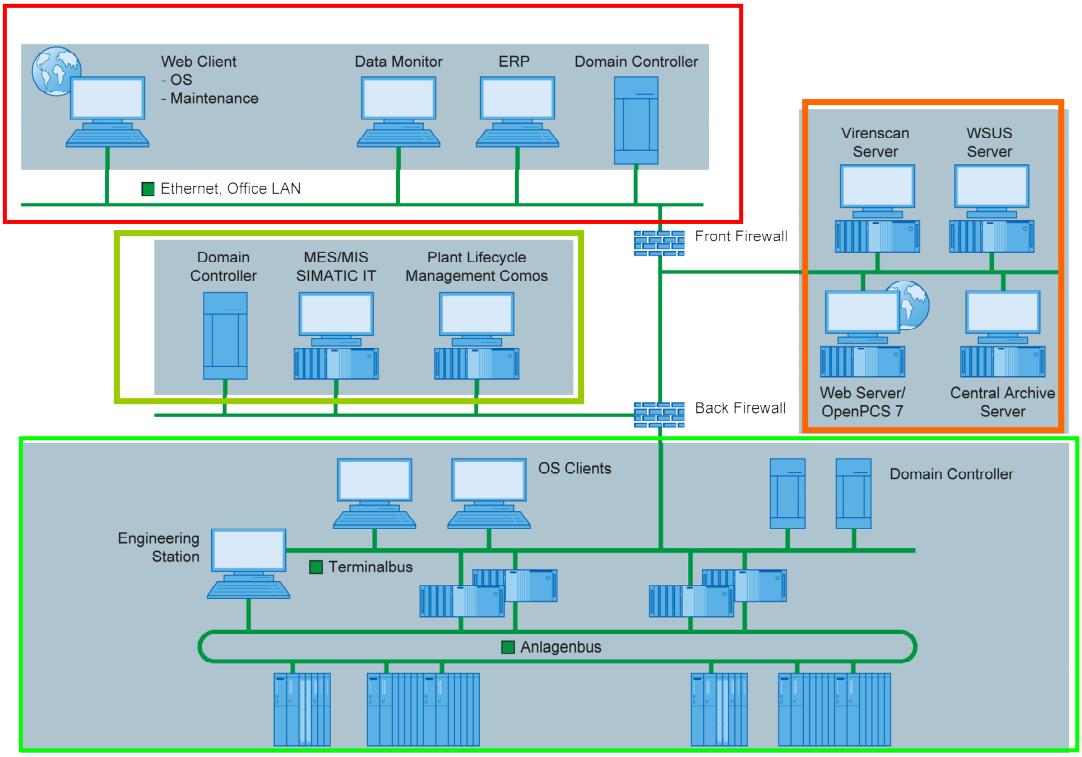


图 4、网络分段

为了实现更好的安全，生产网络也应分 成若干个自动化单元。如下图 5 所示。

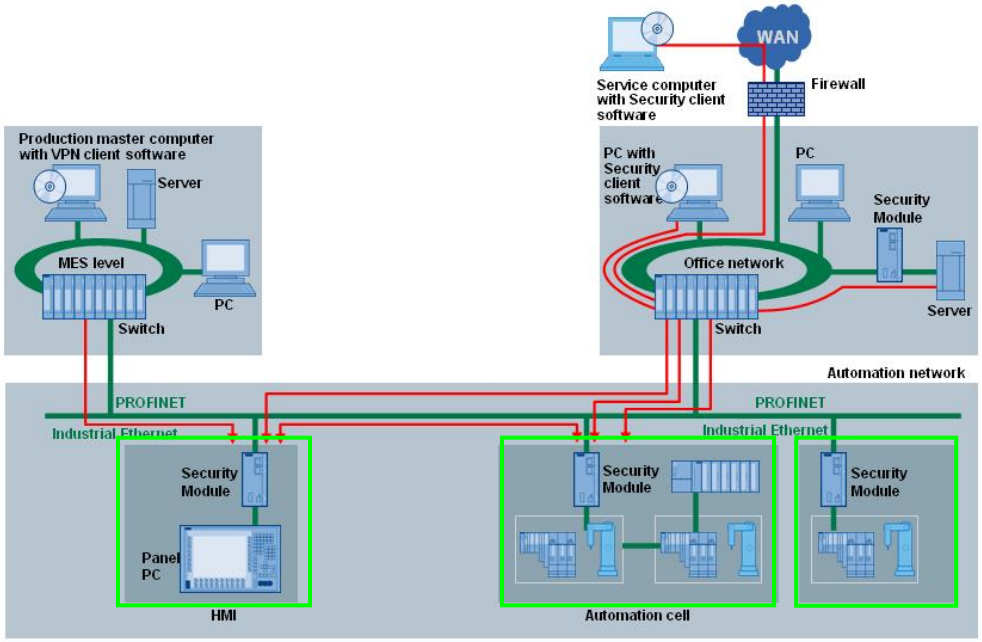


图 5、自动化单元保护

自动化单元保护：

- 一个“单元”是一个处于安全目的的网络段。
- 在“单元的入口”设置网络安全的组件，实现访问控制。
- 没有访问保护机制的设备通过自动化单元来实现安全机制。因此在实际现场中可多样化。
- 单元可以通过限制带宽来保护，不会因数据阻塞而使网络中断。
- 实时通讯在单元中不受任何影响。
- Safety 的 应用也能被保护在单元里而不受任何安全机制的影响。
- 安全的通道（VPN）使得自动化单元通讯的安全。

将来，不仅可以用安全模块实现安全单元，在 PLC 或 PC 的通讯处理器中也集成了安全的机制。如下图 6 所示

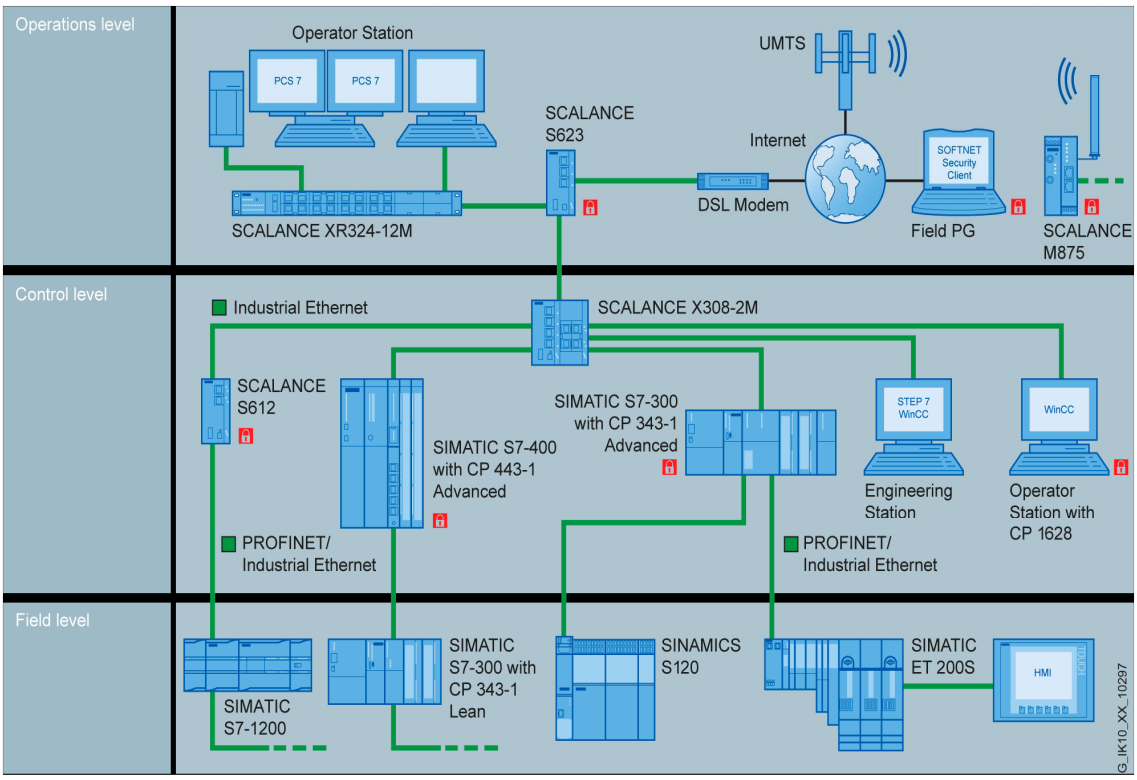


图 6、网络分段及单元保护实例

安全单元的大小取决于保护对象中的组件，一个单元中的组件有可能已经有相同的保护功能。下面是关于网络大小及网络分段的建议，这是从性能方面考虑的：

- 所有的 PROFINET IO 系统属于一个单元
- 设备之间若有大量的通讯应该分在一个单元中
- 设备若仅与一个单元通讯，应该将此设备集成到这个单元中。

在网络分段中的单元保护概念阻止了未被授权的访问。在单元里数据的通讯是不被安全工具控制的，因此在单元中需要考虑其它的保护机制，例如，交换机的端口安全。

### 2.3.2 系统加固

系统加固是对操作系统进行适当有效的配置，减少系统受攻击的弱点。主要可以从如下三个方面考虑：

- 网络服务
- 硬件接口
- 用户账号

1）网络服务

带有弱点的网络服务是一个潜在的危险。为了减小危险，所有自动化的组件的服务仅在必须使用的情况下才启用。被启用的服务（特别是 Web 服务、FTP、远程访问等）应被考虑到安全的理念中。

2）硬件接口

硬件接口成了危险的入口可能当未授权的人通过它去访问设备或系统。不使用的接口应被禁用（Ethernet/Profinet 口；WLAN，Bluetooth；USB 等）。通过禁用或物理隔离达到保护作用；禁止对外部介质的自动引导与自动启动功能。

3）用户账号管理

每个激活的用户账号都形成了一个对系统访问的潜在的危险。配置实际需要的账户。对于存在的用户账号也应采用安全的数据访问机制。需要定期的检查系统的用户帐号，特别是本地配置的用户账号。

除了上述的三个方面外，可以使用合适的防病毒软件来识别木马程序和阻止病毒的进一步传播。然而，在特殊的情况下需要注意下面几个方面。

- 病毒扫描过程降低了系统的性能（例如可以仅自动扫描进入的数据。在系统的维护期间作手动扫描整个系统）
- 定期的更新病毒签名（若可能的话可以从中央服务器上更新）
- 即使是受木马的感染的情况下也必须保证系统的可用性，这意味着病毒扫描器不能作如下的操作：移除文件或作阻止访问；把文件放到隔离区；终止通讯功能；关闭系统。

与西门子产品兼容的杀毒软件有：

Trend Micro Office Scan

Symantec Endpoint Protection

McAfee VirusScan Enterprise

除使用防病毒软件外，为了更加安全可以使用白名单来阻止和识别木马。白名单机制提供了额外的保护，阻止了未知的应用程序或木马的执行。当然也可以阻止对已安装软件的未授权的修改操作。白名单软件创建了可以在计算机上运行的程序和应用列表，不在白名单列表中的不允许执行。与西门子产品兼容的白名单软件：McAfee Application Control。

### 2.3.3 补丁管理

Windows 计算机的补丁管理

迄今为止大多数的安全的攻击是通过已知的弱点。而且这些弱点生产商是有相应的补丁包。只有极少数的攻击是通过零日漏洞（这些弱点仍然不为人所知）。

装载 Windows 补丁是加强安全的重要措施。注意的是对于装有西门子产品（SIMATIC WinCC、PCS 7 、PC-based、SIMOTION 和 SINUMERIK 等）的计算机只能安装经过兼容性测试的安全补丁。这些兼容的补丁的列表会发布在 Newsletter 和 FAQ 中。而且建议作系统的兼容性测试。

补丁的发布是通过放置在 DMZ 区中的 Windows 更新服务器（WSUS）。对于在线的更新需要建立更新组合更新流程（尤其对于冗余系统），如下图 7 所示。

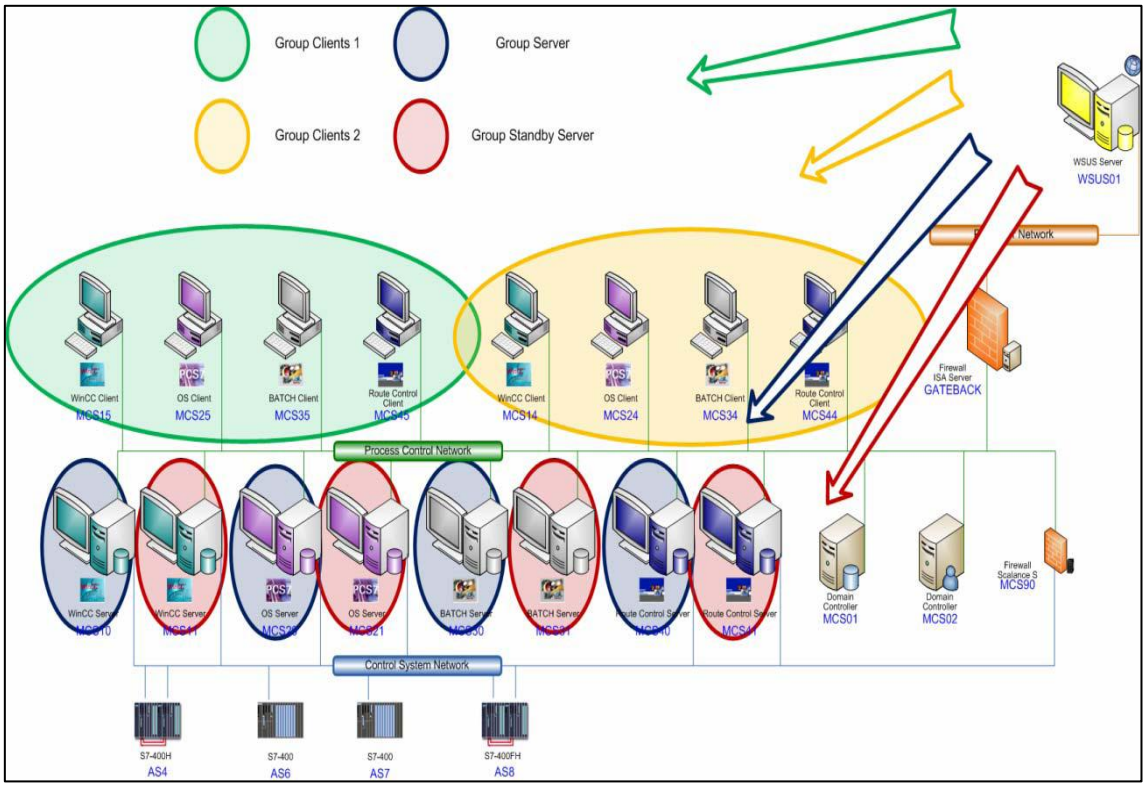


图 7、布置 Windows 更新服务器

自动化设备的版本更新

虽然自动化设备的操作系统不像计算机的操作系统。这并不意味着它没有安全相关的弱点。一但有关于安全相关的弱点信息出现，就应被在其应用环境中被评估这个弱点。是否采用进一步的措施，需要考虑如下几种情况：

- 不需要任何措施，已有的措施保证了足够的安全
- 为了保证安全需要额外的外部措施
- 安装最新的更新版本减小弱点

需注意的是风险的评估是受限于关注点的。

## 2.4 访问保护

访问保护可以分为未授权的操作修改的保护、运行期间操作员站的保护、编程阶段的组态操作保护、对网络中的组件的访问保护。

### 2.4.1 未授权的操作修改的保护

- 对工厂或机器设备的操作员采用集中的用户认证，每个操作站都需要设置独立的访问权限。
- 对自动化组件设置访问保护机制，防止在编程组态或系统维护期间的未授权的访问或修改。
- 对网络层作访问保护，仅允许授权的网络设备使用网络。

### 2.4.2 运行期间操作员站的保护

- 在通常的情况下设备或机器会由不同的人来操作，因此建议作集中的用户管理如下图 8 所示。
- 这种用户管理通常是基于 Windows 的域管理或者是 Windows 的活动目录管理。在使用 SIMATIC (HMI) 运行应用环境时也可以考虑使用 SIMATIC Logon。
- 集中的用户管理可以使常规的访问权限检查简单化。

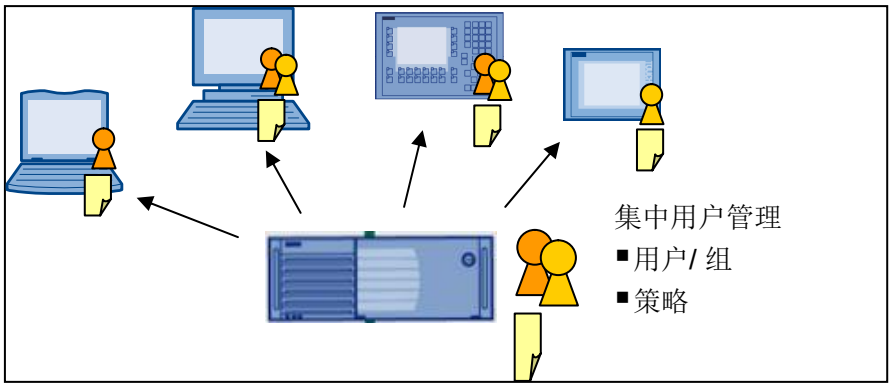


图 8、用户集中管理

### 2.4.3 编程阶段的组态操作保护

为了阻止对自动化组件的未授权的组态修改，强烈建议使用集成的访问保护机制。这包括如下几个方面：

- PLC（保护级别）
- HMI 屏（安全模式）
- 管理型交换机（密码保护）
- 工业无线访问点（密码保护）
- 防火墙（证书保护）

为了安全尽可能的使用不同的密码。根据人的数量的多少，尽量的采用集中的密码管理且对不同的人采用不同的权限及对网络的访问。

### 2.4.4 对网络的访问保护

对网络的访问保护通过如下几种方式：

- 交换机的端口安全：MAC 或者 IP 的访问控制列表。
- 交换机的端口安全：使用 RADIUS 认证（802.1X）的集中用户管理。
- 通过防火墙对不同的网络进行网络分界。

而对于工业无线网络安全可采用如下方式：

- 采用 WPA2 的高级加密方式
- 对数据加密采用高级的加密标准（AES）
- 通过 RADIUS 认证（802.1X），集中管理用户。
- 通过 HTTPS 或安全登录 SSH 实现对 Web 接口的实现安全的组态访问。

## 3 综述

工业安全不仅仅是通过技术来解决的问题。应该是从各级管理层到工厂工人都有很强的工业安全的意识。安全是一个持续执行的流程而且在整个工厂的生命周期内都被考虑。在自动化系统中由于特殊且固有的风险的存在，所以必须采用适当的组织与技术措施并定期的回顾。

西门子工业自动化在提供产品与系统的同时也提供安全的服务，为客户提供全面的工业安全解决方案。

**如果您对该文档有任何建议，请将您的宝贵建议提交至下载中心留言板。**

**该文档的文档编号：A0606**