



混凝土预制板生产网络中的过程控制系统、生产控制系统和楼宇自动化系统采用了分散式配置的网络方式构成一个整体，并由各自的防火墙防止计算机病毒的入侵

安全

分散式控制系统 确保生产过程的可靠性

生产网络往往是非常复杂的一套系统，因此也往往非常容易出现故障。为了可靠地把机床设备连接成为一个生产网络，奥地利的一家企业采用了封闭的分散式控制系统，从而避免了计算机病毒的侵入。

文 | Herbert Dimberger 和 Martin Ortgies

奥地利 Amstetten 市的 Umdasch 公司安装了 30 台新的焊接机器人，并把这些设备纳入到企业生产网络中。在这些焊接机器人的安装工程中，有必要考虑一些战略性问题，采取必要的措施和方法。因为生产网络发展很快，并且变得越来越复杂，这就要求企业在监督管理方面更具有前瞻性。

复杂自动化工程中的 信息安全解决方案

正确的分析处理方法，例如防止工业计算机因病毒的危害造

成生产线瘫痪，就必须要为生产、加工和楼宇自动化系统采取相应的信息、数据保护措施，制定相应的安全方案。该公司的电子和自动化技术部门及信息技术部门与合作伙伴共同开发了一个创新性的生产和辅助过程的支持平台：Umdasch 解决方案。

方案核心是小型、 分散式控制系统

当前对生产过程信息安全性的要求是：生产指挥网络与生产网络之间畅通无阻、安全可靠的通讯；扁平化网络结构、最低的复杂程度；

很高的新设备集成灵活性和远程登录可靠性，例如在远程维护保养时登录生产网络的可靠性。这一利用公司名称命名的解决方案的核心是小型、分散式控制系统。整个混凝土预制板的生产过程可分为切割下料，孔加工，铣削加工，焊接和其他加工等部分；这些不同的生产过程分割成多个生产单元并用工业防火墙组成安全防护网。这样的生产单元共有 40 多个，它们构成了生产设备与信息网络之间的过渡。这样，信息流在各个生产网络平台之间传递，并受到行政管理系统的监督和管理（图 1）。新的自动化系统和新的控制系统能够相对简单、方便地集成到这一方案之中，快速地与 Umdasch 公司的网络连接起来。

分散式的防火墙是最重要的 安全保护措施

使用分散式配置的防火墙是这一解决方案中最重要的安全保护措施。尽管这家奥地利公司的生产网络中有很多不同的生产设备和系统，但在信息管理方面却十分有效，整个流程一目了然。除了分散式配置的防火墙以外，及时的数据备份、数据恢复以及临时性地提供替代仪器设备等属于次要的安全防护措施。除了这些措施以外还采用了系统强化的措施：防止恶意软件的保护措施、登录时的安全确认和授权确认以及物理地址的保护和系统的防护。在选择合适的安全防护技术时，他们选择了 Innominate 公

司研发的 Mguard-Security-Appliance 技术。这是因为该技术有着很好的技术服务支持，在工业生产环境中非常稳定，系统简单，采用的是 Linux 操作平台。由于这家公司拥有一条很受欢迎的技术服务热线，因此在相关仪器设备的购置时立足于国内即可。

在各个系统之间构成安全的过渡区

由于采用了 Mguard 技术，从而可靠的在各个系统之间构筑了安全的过渡区；因为网络间数据交流的封包过滤和进程都受到所谓最小特权的限制：它只传输绝对必要传输的数据，信息在各个系统之间传递和交换。对于 Umdasch 公司的计算机安全专家们来讲，登录授权功能是必要的安全防护措施（图 2）。因为网络是动态的，随时随地都在发生变化；经常会在网络中添加新的网络用户或者对设计网络中的错误加以纠正；因此要对所设计的网

络非常细心地加以监控。

被拒绝的登录申请或者被接受的数据连接都集中存放在日志服务器中，连续不断地受到监控。所出现的变化都会自动的、有目的的利用脚本过滤出来，加以分析。

防火墙的配置不再是一项繁琐的任务

首先，利用专门的防火墙配置方式，使得防火墙的设置不再是一项繁琐的工作。接受一次培训，做几次练习，掌握一点专业技术人员所掌握的最佳实践经验就可以迅速学会程式化的防火墙配置方法。随后，所有的防火墙都是按照这些步骤一步步设置完成的。一次学会的配置方法可以在 80% 左右的生产加工单元中使用。

在防火墙系统的维护中，Umdasch 公司考虑到未来发展的需要：使用 IDM（身份驱动管理）技术，这样可以明显减少系统调整或者系统维护时的工作量。

一般情况下，在更换文件服

务器或者修改文件服务器地址时都会有很大的维护工作量。由于此时要在所有的防火墙中进行相同的更改，则利用 IDM 技术可以实现自动的更新配置：利用所谓的模板进行匹配调整。它大大简化了安全防护和复杂系统的配置。据 Umdasch 公司估计：当生产加工单元的数量超过 15 个时，采用这一技术就非常合算了。

Umdasch 公司对防火墙在自动化和系统技术方面给出了很高的评价。系统工作非常稳定，各个加工单元在生产过程中无需更改、变动。就是在利用外部技术服务人员远程遥控时，Mguard 技术也是一个受控的、可靠的安全防护技术。

杜绝了黑客从系统后门的入侵

现在，Umdasch 公司的网络技术人员能够准确地知道是哪个加工单元有登录请求。外部黑客想通过网络系统中的后门进入网络已经成为历史：只有当网络服务技术人员点击按钮允许登录之后，登录请求才被批准、才有可能进入网络。只有在这种情况下，生产加工单元的内部网络与办公管理层之间的网络防火墙才被打开；而此时办公平台与生产单元的两道防火墙却有着非常密切的安全防护配合。

根据 Umdasch 公司的使用经验，网络中的异常事件是常有的事情。但这些意外带来的损害都被限制在最小的范围之内：因为整个生产系统都得到了最好的安全保护。这种分散式配置的工业防火墙的最大优势就是：整个网络的复杂程度大大降低，更加易于控制和监控，网络的使用性能明显提高。[MM]

