

安全分区解决方案

智能生命周期管理能够保证过程自动化的最大安全性——流程企业越来越关注网络安全的话题。长期以来，仅靠杀毒软件、防火墙和密码已经不足以防止网络黑客的攻击了，企业需要定制化的安全保护方案来保障网络安全。因此，B&R 公司重新修改了自己研发的生命周期管理软件 Apröl 过程控制系统。

文 /Sabine Mühlkamp

流程工业网络安全面临的
最大风险来自不安全的
保护密码、没有进行软件
更新或者被病毒污染的 U 盘。
合适的保护对策能减少这类事件
的发生，但也增加了一些风险。
因为现代化的工业控制系统广泛
使用的是标准软件，即 CTOS 现
场的商品软件，这种软件提高了
受到网络攻击的风险。因此，企
业必须采取适当的防护措施来大
程度降低这种风险。

虽然杀毒软件、防火墙和密码一直是流程工业日常工作的一部分，但这些不足以保护过程控制系统免受网络攻击。更重要的是，企业要在流程设备规划设计的早期阶段就进行风险评估，并制定全面的安全防护方案。这一安全保护方案与流程设备的工艺流程、基础设施、当地的安全条件等因素有着密切的关联。此时，没有一套现成的标准型网络安全保护方案成为了最大的挑战。另外，安全保护系统还必须定期更新升级，这对于流程企业也并

本文作者系 PROCESS 德文版编辑。



除了发行新版本软件和安全补丁外，B&R 公司每个月都提供操作系统的软件更新

非一件易事。

定期更新以修复薄弱环节

B&R 公司认为在流程设备规划设计阶段，在网络安全战略制定中设置生命周期管理至关重要。定期的安装补丁程序、固件更新、BIOS 更新和安全认证可以很快地修复安全漏洞。

除了通常发行的主版本软件和补丁软件之外，B&R 公司

每个月还提供操作系统的软件更新，这使得用户的控制系统能够满足许多网络的安全保护战略要求。

B&R 公司发布 Apröl 软件已经 4 年时间，一旦新版软件开发成功，先前版本软件的状态立即从“活动状态”转换为“经典状态”。在软件更新后，B&R 公司都会提供 Linux 操作系统的安全更新。B&R 公司每年都会为当前版本的

PROCESS-Tip

* 更多信息请扫描二维码：



chem.vogel.com.cn

* 反馈编码：A200135

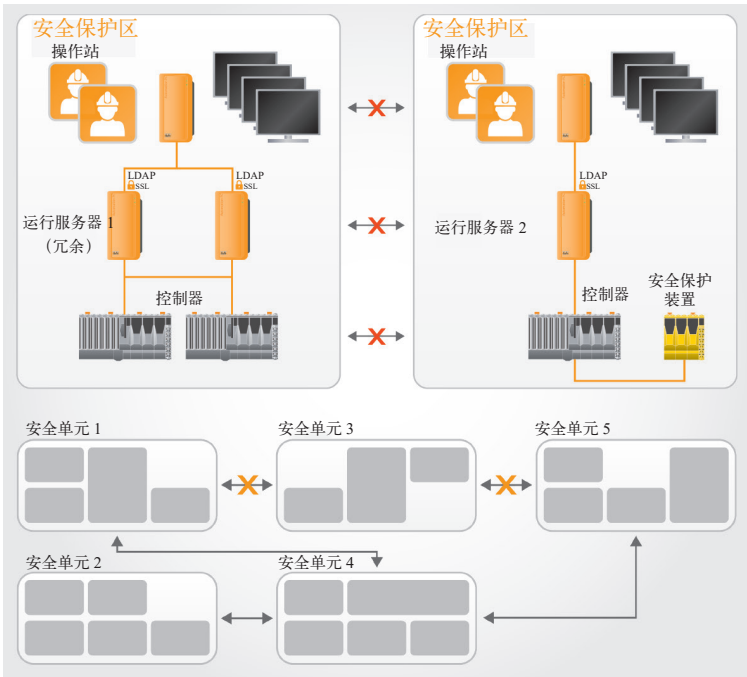
软件提供一些新功能，在随后的软件使用受限阶段中，B&R 公司也将不再进行更新。

此外，企业需要安装补丁程序来维护现有的系统软件。当前的最新补丁程序都是针对特定版本编写的，其中包括了所有可用的错误修复程序。而发布补丁程序的时间间隔取决于需要被修复的错误的严重程度。

始终保证安全

B&R 公司每个月都为 Linux 操作系统提供底层的软件更新。在发布 Suse Linux Enterprise Server 多模式操作系统的更新软件之前，B&R 公司对这些更新内容进行了大量测试。对于每年发布一次的 Build 版本，每个月都要进行 14 次更新，然后每 6 个月更新 4 次。这些都可以在 AutoYaST-DVD 的帮助下完成，以 ISO 映像文件的格式下载下来。

这样做带给用户的好处是，用户始终可以收到最新版本的软件，同时也可以确保操作系统的安全，定期地补充一些新功能非常重要。



在规划设计安全保护区时，首先将设备划分为若干自动化单元，然后通过安全保护措施将其整合成安全保护区

分布式可以抵御网络威胁

另外，B&R 公司还进一步开发了用户管理软件 Aprot。现在，每一个多进程服务器上都有自己符合 LDAP 轻量目录访问协议的 389 个目录服务。这样就可以轻松建立自给自足的、带有安全保护单元的分布式操作系统，并能保障整个系统的连续性。

为了保护大型流程设备免受网络风险的影响，通常都会将这些大型流程设备划分在若干“安全保护区”中。如果这种基础结构中的某个区域受到了网络攻击，则其他区域内的设备仍可以安全运行。一个安全保护区由一个或者多个自动化单元组成，只有经授权许可的人员才能访问这些区

从实验室到大型流程设备的应用

Aprot 控制技术的应用范围涵盖了从小型实验室系统，到大型流程设备的自动化控制系统。B&R 公司的 Aprot 4.2 系统以其灵活的可扩展性能覆盖了整个应用领域，它从流程设备生命周期的规划设计、建立数据库、设备配置和设备调试开始，直至流程设备的系统运行，都为系统集成商和流程设备运营商带来许多益处。无缝的链接和直观的操作减少了软件系统的设置时间，除保障设备高生产效率外，还可以灵活实现产品转换。

在 Aprot 软件系统中，用户可以连续监测工艺装备，从而减少维护保养成本和设备停机时间。用户也可以通过振动监测及时发现机床设备和系统的损坏和污染情况。振动测量的结果可以被制成交互式 3D 图像，并在流程设备操作者或者设备维修人员优化设备时提供帮助。操作总线、过程控制总线以及运行服务器和监控器等都可以冗余配置，根据每个控制回路的标准数据，CPM 监控模块能够自动计算用于调节产品质量的关键指标。

域。进入这些区域的人员和仪器设备都必须经过身份验证和授权，这就限制了可能发生的安全威胁，减少了危险带来损失的同时，也提高了流程设备的可用性。在规划设计安全保护区时，首先将设备划分为若干自动化单元，即过程单元，然后通过安全保护措施将其整合成安全保护区，即安全单元。

自动化单元包括了与生产相关的区域、分区、子区域或者子系统，有着自主运行功能，并且可以在一定时间段内无需与系统其它部分连接而自动运行的设备。在这些区域中，网络通信都是在本区域内进行的。

灵活的结构

Aprol 多进程服务器体系支

持分布式的控制方式。一个这样的服务器系统包含了自主操作所需的所有软件系统，例如可视化、编排、趋势、报警和报告系统。

数据的分类

归档也可以在每一个区域中完成，这就意味着可以长期将整个系统中的某一个单元隔离出去。Aprol 多进程服务器系统灵活的客户端 / 服务器架构最多可以支持 64 个安全保护单元。

为保证网络安全，这一解决方案为每一个运行服务器都配备了符合 LDAP 轻量目录访问协议的专用服务。操作员的身份验证可在专用的 389 目录服务器中进

行设置，并复制到运行服务器的

本地服务器中。这样就可以在断开连接后，也可以由操作员在某一个安全保护区中进行操作。

用户得到一个自主运行的安全保护单元的同时，也保证了工程设计工作的一致性。

此外，Aprol 系统还可以在计算机上完成任意数量控制器的模拟。这也就意味着，用户可以在每一种控制器配置迁移到实际应用的硬件之前，就在安全保护区内进行广泛的安全测试了。

“为了能够对抗网络攻击，我建议使用单独的安全保护区解决方案。”

——Martin Reichinger 先生，
B&R 公司

专访 B&R 公司软件和过程自动化负责人 Martin Reichinger 先生

PROCESS: 流程工业企业遭受网络攻击的实际风险到底有多大？

Martin Reichinger: 我们不知道准确的数字，但从发展趋势来看，只要您的系统与外部世界联网，遭受网络攻击的风险就会非常高，网络中可以得到的所有东西都能给网络攻击可乘之机。

PROCESS: 流程工业企业的状况如何？

Martin Reichinger: 如今，杀毒软件、防火墙和密码等已经是大多数流程企业 IT 系统标准的安全保护技术措施。但在 OT 领域中，许多企业还很难 1:1 地贯彻落实安全保护标准。例如与实时数据相比较，数据库可以更容易地交换数据。

PROCESS: 用户集成会犯的错误是什么？

Martin Reichinger: 许多流程设备运营商低估了网络攻击的风险。密码不安全，系统维护不足以及不及时更新升级等都是用户经常犯的错误。安全保护必须是软件系统整个寿命周期内关注的重点。

PROCESS: 哪些安全保护措施是流程设备用户应该而且能够采取的重要措施？

Martin Reichinger: 当前的杀毒软件、加密通信和定期的安全备份等在控制网络攻击及其影响方面都起到了重要的作用。但网络攻击的威胁每天都在增加，确保安全补丁是最新版本的非常重要。为了能够对抗网络攻击，我建议使用单独的安全保护区解决方案。这样，受到网络攻击的影响就仅限于很小的子区域中，不会对整个系统带来致命的影响。

