系统800xA网络安全
最大化过程自动化中的网络安全

如果它对你有价值，那么它可能对其他人也有价值

在关键的基础设施中，保护范围不仅限于知识产权，还包括在攻击下可能减少的资产的可用性。事实上，公司未来的样子和规模将取决于您的专业知识、想法和运营 - 以及您保护它们的能力。

在面对这么多风险时，其最大的问题便是：您将如何保护您的公司免受网络风险，如病毒、黑客和人为错误的攻击？

ABB致力于对网络安全的承诺

网络安全对每个公司来十分重要。如果没有它，您的公司将面临生产中断、知识产权损失和无法重新创建数据的风险。

如ABB的任何解决方案一样，我们希望您对我们为您提供的安全解决方案感到满意。

我们充分理解网络安全的重要性及其促进控制系统安全的责任。您可以依赖我们提供的可靠性和安全性具有最高优先级的系统解决方案。

ABB帮助您确保公司的未来

面对新技术、机遇和挑战，过程自动化世界正在发生变化。ABB始终致力于帮助客户利用最先进的技术，同时最大限度地减少网络风险。

ABB是面向所有行业的控制系统领先供应商，我们可以结合我们的技术优势和领域内专业知识，提供以客户为中心的解决方案，同时提高资产生产率和效率。

我们的目标是建立必要的网络安全级别，并在保持系统可用性和功能互操作性的同时保持该级别。

为什么控制系统所有者必须关注网络安全

由于技术的进步，工业自动化和控制系统在过去十年中不断发展。这些进步的核心是专门的IT系统。为了向最终用户提供全面的实时信息，并允许更高级别的可靠性和控制，这些系统已经变得越来越相互关联。

新一代自动化系统采用开放标准，如OPC、 PROFINET、FOUNDATION Fieldbus、IEC 61850和商业技术，特别是基于以太网和TCP/IP的通信协议。它们还可以链接到外部网络，如办公室内部网和Internet。这些技术变化从运营角度带来了巨大的好处，但它们也带来了网络安全问题。以前只有在办公室或企业IT系统中才指导。

网络风险是通过采用开放式IT标准继承的。但幸运的是，在企业环境中开发的网络安全机制也解决了这些风险。依靠成熟的技术，这些机制可以支持开发专为工业自动化和控制系统量身定制的网络安全解决方案。

ABB完全理解网络安全的重要性，以及它在促进控制系统安全方面的作用。ABB客户可以依赖可靠性和安全性最高的系统解决方案。

ABB的系统方法确保网络安全

在过去几年中，全球工业稳步增加了对工业自动化和控制系统网络安全的关注。因此，出现了许多不同的驱动因素以及趋势。

在ABB，我们始终将网络安全视为一项关键要求，并致力于提供明确解决这一关键问题的产品、系统和服务。 ABB通过其在全球范围内的运营，对网络安全采取系统的方法。例如，ABB建立了一个组织，并在公司和部门层面设有安全理事会，以跟踪全球网络安全需求和要求。

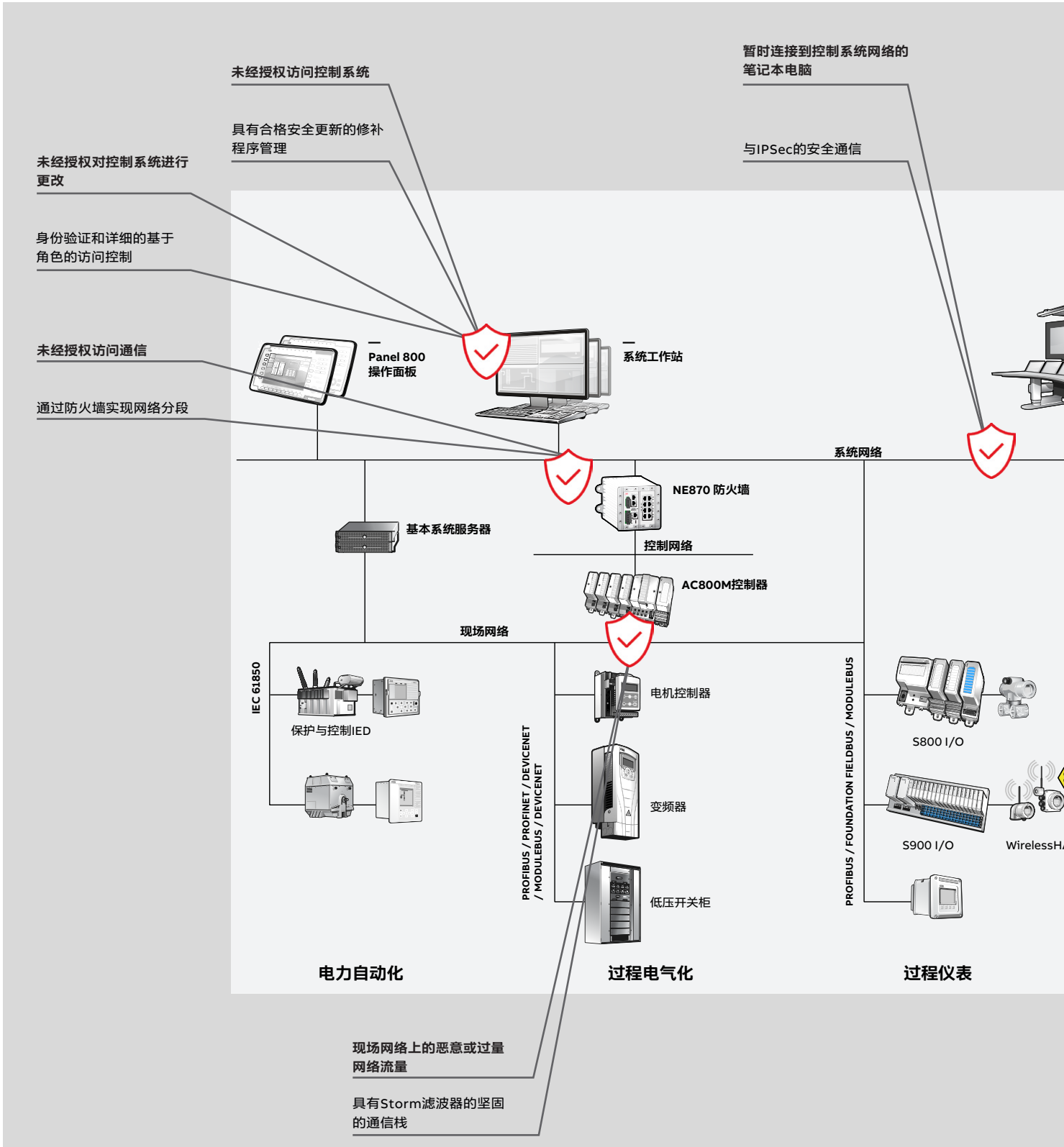
最佳的合规性

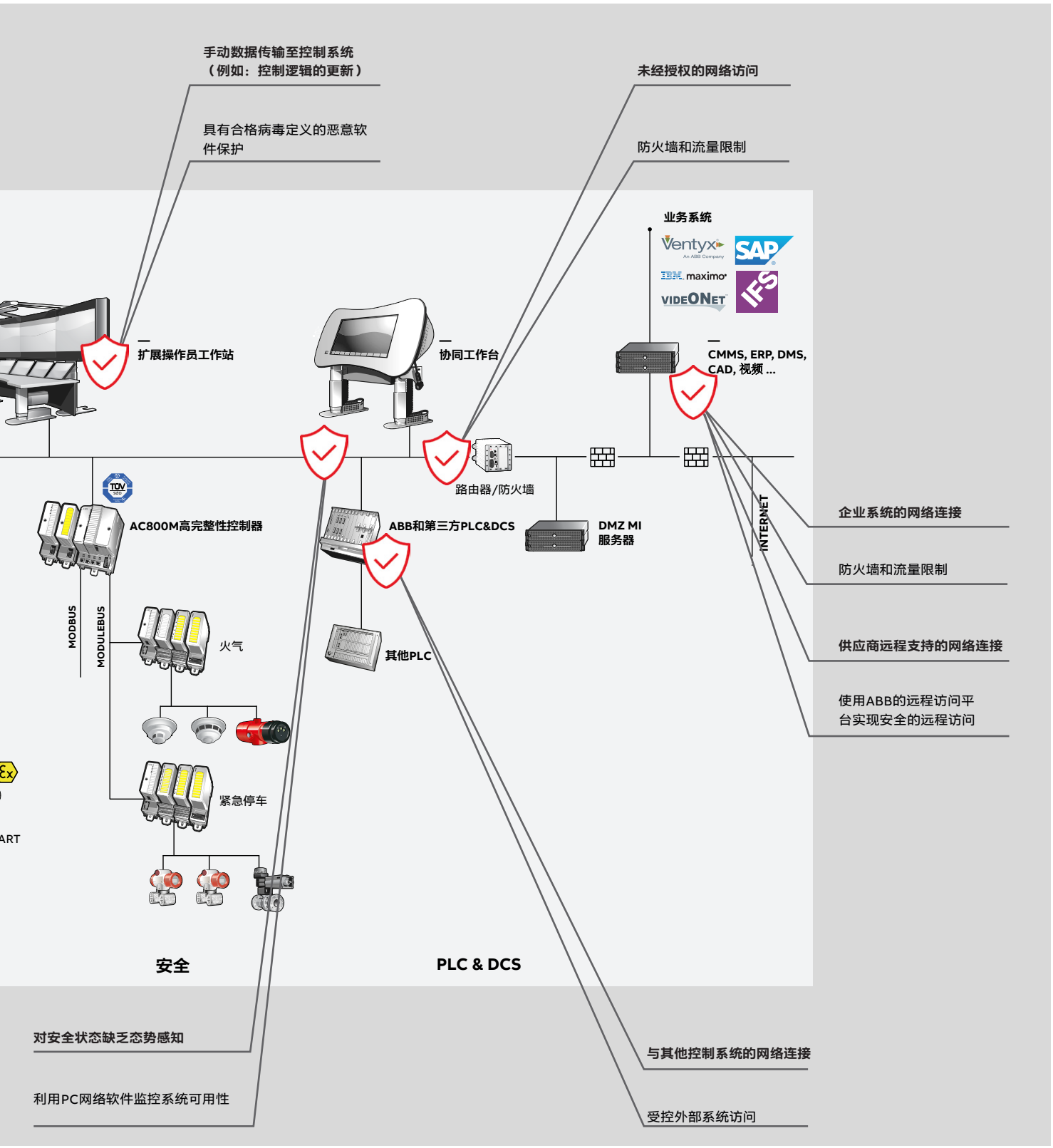
在网络安全标准方面，我们也尽了自己的一份力量。ABB 是行业倡议的积极成员和推动者，包括在ISA、IEEE、网络安全标准委员会和IEC中。

我们的参与还使安全理事会能够确保ABB的产品和系统符合并支持与网络安全相关的行业标准和法规。我们不断开发和改进符合最新网络安全标准的产品。

系统800xA的设计考虑到了网络安全，并提供了最先进的功能。这使您能够轻松满足NERC CIP要求，并根据这些标准和其他标准保持合规性。

所有控制系统都面临着威胁
系统800xA有适当的保护机制




手动数据传输至控制系统
（例如：控制逻辑的更新）
具有合格病毒定义的恶意软件保护
未经授权的网络访问
防火墙和流量限制
业务系统
Ventyx
SAP
IBM maximo
IFS
VIDEONET
扩展操作员工作站
协同工作台
CMMS, ERP, DMS, CAD, 视频 ...
路由器/防火墙
AC800M高完整性控制器
ABB和第三方PLC&DCS
DMZ MI 服务器
INTERNET
企业系统的网络连接
防火墙和流量限制
供应商远程支持的网络连接
使用ABB的远程访问平台实现安全的远程访问
MODBUS
MODULEBUS
火气
其他PLC
紧急停车
安全
PLC & DCS
对安全状态缺乏态势感知
利用PC网络软件监控系统可用性
与其他控制系统的网络连接
受控外部系统访问

嵌入到系统800xA的网络安全

网络安全嵌入在ABB系统生命周期的所有阶段（产品、项目和工厂生命周期），它是系统800xA的一个组成部分。这意味着网络安全在系统生命周期的每个阶段都得到了解决，从设计和开发到维护。威胁模型和安全设计审查、软件开发人员的安全培训以及内部和外部安全测试都是ABB为确保可靠和安全的解决方案而采取的行动的例子。系统交付遵循我们关于处理网络安全的严格指导原则。

系统800xA的安全性遵循SD3+C安全框架（由Microsoft创建），以确保和提高系统组件的安全性。

通过设计确保安全
这里的目标是确保新软件中不存在安全缺陷或漏洞。要做到这一点，网络安全必须从产品设计的一开始就成为一个因素。从创建规范到编写代码，再到测试产品的所有阶段。

安全的设计理念表现为安全培训、代码审查和演练、威胁分析以及产品的坚固测试。安全性集成在ABB的质量管理系统中。正式威胁分析和威胁建模为系统的安全要求和设计原则提供了基础。项目大门处的安全检查点确保满足安全目标。

这一过程的一个关键要素是我们独立的坚固测试实验室，即ABB设备安全保证中心，我们的产品在这里进行测试。该实验室由不属于任何产品开发团队的专业人员管理。他们使用几种专门的安全测试工具，例如Wurldtech的Achilles Satellite和Mu Dynamics Mu8000。除了我们会采用SD3+C安全框架和ABB设备安全保证中心（DSAC）执行的广泛内部测试外，ABB还采用了ISA安全认证研究所（ISCI）针对选定型号的AC800M控制器的IEC62443标准的第三方安全认证。

系统800xA安全功能旨在满足监管要求，如FDA的要求。用户账户管理和身份验证基于Windows Active Directory，或适用于小型系统的Windows工作组。

默认安全
此阶段的目标是通过减少攻击面（黑客可以尝试利用的点数），创建更抗攻击的默认产品安装和配置。

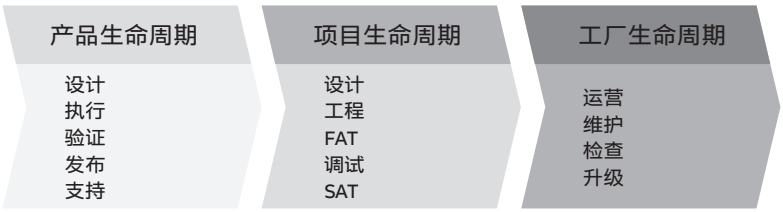
为了实现这一目标，软件必须安装在最安全的配置中，并且必须一直保持这种状态，直到客户采取知情的步骤将其松开。

使用系统安装程序时，系统800xA以预定义的方式安装，这使得过程简单可靠，确保以一致和可重复的方式进行设置。禁用或未安装不需要的功能和特性，并自动配置Windows防火墙。系统800xA为控制工程师提供了管理每个用户访问权限的独特机会。可以根据参数授予访问权限，例如用户是谁在哪里、用户想做什么以及对象的哪个方面。

通过部署确保安全
这里的目标是确保产品能够以安全的方式安装、配置、操作和维护。

用户文档描述了如何在最高安全级别下安装和操作系统800xA。文档包括关于如何使用安全区域和纵深防御构建安全系统体系结构的建议。安全合规项目检查表确保在项目执行期间采取所有重要步骤，以确保安全部署。

—
网络安全是系统生命周期所有阶段的重要因素



系统800xA让您的生产更加安心

当您不再担心风险的时候，您的内心就会平静下来。而事实上，当您操作系统800xA时，我们可以帮助您消除对风险的担心。我们会尽一切努力来保护您公司的专有技术、想法和运营，这将让您感到放心。

系统800xA中嵌入的安全功能概述：

- 详细的系统监控和诊断
- 使用IPSec进行网络保护
- 服务器和工作站的主机防火墙
- 服务器和工作站中的网络环路保护
- 经过可靠性测试的产品
  (AC 800M 已获得Achilles通信认证)
- 控制器和通信模块的网络保护过滤器和Storm保护
- 详细的基于角色的访问控制
- 快速操作员登录
- 基于硬件的安全系统访问控制
- 数据完整性和历史数据的受保护档案
- 用于灾难恢复的备份和恢复

其他安全功能概述：

- **数字签名**
  使对属性对象进行数字签名成为可能，以确保数据在批准后保持不变
- **高级访问控制**
  重新验证和双重重新验证，用于安全交互和非活动注销
- **审计追踪**
  记录系统中所有用户启动的操作，如操作员交互、配置更改和下载到控制器、批量配方编辑和执行、服务器启动/停止等

通过我们的合作伙伴概述可选的安全功能：

- **恶意软件保护：防病毒**
  ABB建议在所有系统800xA服务器和工作站使用病毒扫描器
  - McAfee VirusScan® Enterprise 和 McAfee Endpoint Security已经经过测试，并通过了鉴定，以确保系统800xA的操作和性能达到最佳性能

- **恶意软件保护：白名单**
  - McAfee Application Control 也是针对系统800xA的预调试/验证的白名单解决方案

- 应用程序白名单
  - 旨在防止未经授权和恶意程序的执行

系统800xA的网络安全服务产品

ABB提供的服务包括：

基础

- **评估**，了解您的系统的网络安全态势
- **安全控制**，通过实施网络安全控制抵御基本威胁
- **培训**，通过为您的团队配备网络安全洞察力来减少事故

服务

- **维护**，确保使用我们熟练的工业网络安全工程师持续保护您的自动化系统
- **咨询**，执行系统强化或实施您的网络安全项目，利用我们的全球工业网络安全专家网络

运营

- **协作运营**，通过ABB协作运营中心利用我们的全球专家网络进行全天候连续监控和支持

有关更多信息，请访问我们的
ABB Ability网络安全服务网站

如果最坏的事情发生，什么都不会失去

系统总是在最新状态
自动化哨兵（Automation Sentinel）使ABB基于订阅的控制系统生命周期支持计划，允许系统的所有者积极监控其控制系统版本和软件生命周期成本。

对于自动化哨兵的订阅者来说，使用最新的安全更新和病毒特征文件使系统保持最新状态时非常容易的。

ABB评估系统800xA的所有第三方软件安全更新，并测试所有相关更新的兼容性。自动化哨兵的订阅者可以从ABB门户网站下载“ABB System 800xA Qualified Security Updates”。

此外，我们还测试了支持的病毒扫描程序（包括病毒定义文件）的更新与系统800xA的兼容性，以确保合法代码不会被错误地归类为恶意软件。

ABB每周每天测试McAfee Vi-rusScan® Enterprise, McAfee Endpoint Security和Symantec Endpoint Protection的病毒定义文件。

最大化安全性的服务
ABB开发了非侵入性工具来诊断潜在的网络安全问题，提供最大化安全性的解决方案，并为未来提供支持。

网络安全Fingerprint
服务、诊断潜在的安全风险并提供解决方案。它包括减少脆弱性的详细建议，并有助于为控制系统制定可持续的安全战略。该服务由ABB现场工程师提供。

现在就开始为您的系统投资网络安全

投资网络安全使投资公司未来的最佳方式之一。而这绝不应该是一个等着看事情是否会发生的问题，因为没有人愿意去承担这种风险。

最后，也许是最重要的，网络安全不是一次性事件，而是一个持续的过程。在ABB，我们很高兴在整个过程中为您提供帮助。

solutions.abb/800xA
abb.com/controlsystems

3BSE074956 en F