工业自动化

ABB 网络安全集成方案

随着数字化服务相关优势的不断扩大，网络攻击风险也随之增加。事实上，此类攻击的威胁已变得无处不在，现已成为高管层和董事会级别经常讨论的话题，无关乎垂直业务。然而，网络风险是可控的，相关控制是所有数字化转型的关键一环。本文重点介绍了 ABB 网络安全方案的核心理念，其目标是保持客户运营完整性和数据安全性。

Ragnar Schierholz
工业自动化事业部
网络安全委员会
德国明登

ragnar.schierholz@
de.abb.com

Robert Putman
产品与服务部网络安全委员会
瑞士苏黎世
Zurich, Switzerland

robert.putman@
ch.abb.com

人、过程和技术是 ABB 理念的核心所在。长期以来，ABB 一直是工业自动化和控制技术领域值得信赖的合作伙伴，对所服务的行业及其面临的挑战有着深入了解。在全球范围内，公司已交付了 7,000 多万台连接设备、70,000 套数字控制系统，以及 6,000 套企业软件解决方案。作为工业领域的领导者，ABB 拥有 40 年经验，致力于为所有行业客户提供安全的数字化解决方案。

多年来，网络安全已成为 ABB 产品组合中不可或缺的组成部分，就如同每辆车都必须配备安全带和安全气囊一样。如今，从设计和开发到产品维护和支持，网络安全在每个阶段都被放在最突出的位置。此外，这不仅适用于新安装的产品，也适用于遗留设施。事实上，许多行业都面临着如何改造或升级遗留环境的挑战，

两类威胁

威胁主要分为两大类 - 针对性攻击和所谓的白噪声攻击。大约发生在 10 年前的 Stuxnet 病毒就是针对性攻击的一个例子。

白噪声攻击

另一方面，白噪声攻击在过去十年间急剧增加，对许多组织构成真正威胁。其中的多次攻击（也被称为勒索软件）本质上是犯罪组织进行的勒索。他们所构成的危险与其说是因为其复杂性，不如说是因为他们所能攻击的目标数量众多，以及受害者防御能力薄弱。WannaCry 勒索软件就是其中一个例子，它在 2017 年感染了数千台电脑，给受害者造成了数亿美元的损失。

在工业自动化系统中，白噪声攻击通常可达到 HMI 级别，这是因为它们一般会针对 Windows 或 Linux 等操作系统，而针对性攻击大多基于对某一特定企业的深入了解而构成的民族国家攻击。例如，它们会被设计成可一路渗透到分布式控制系统（DCS）的较低层中，或导致传感器、执行器、闭环控制甚至安全系统产生不准确的信息，或使其完全失效。因此，针对性攻击和白噪声攻击带来的后果有所不同。就工业领域而言，其风险在于物理过程会受到影响，从而可能对人员、环境和基础设施造成危险。另一方面，对于涉及企业 IT 系统的攻击，攻击者通常会窃取个人信息或可获利信息。

01

这些环境是在防范针对性攻击和所谓的白噪声攻击成为网络安全优先事项之前设计和安装的（见文本框→01）。ABB 可针对此类情况提供指引、产品和服务，以解决绿地和棕地应用中的问题→02。

安全参考架构

作为公司工业自动化网络安全产品的一部分，ABB制定了安全参考架构和标准。这是适用于整个 ABB 控制套件的模板，以公司提供有效技术和解决方案的能力为基础。

ABB 拥有 40 年经验，致力于为所有行业客户提供安全的数字化解决方案。

ABB 的安全参考架构涵盖从访问控制定义到数据流的所有内容，基于多年部署和维护此类系统的专业知识。其可定义如何安全配置和管理技术，得益于其架构级别查看功能，用户可在设计中添加安全层和功能层（如远程访问）。

工业伙伴关系与协作

控制环境可包含多种第三方工具和解决方案，这些工具和解决方案可集成进 ABB 的安全参考架构设计中并进行验证。借助公司的领域知识和技术专长，可以实现经过验证的设计。作为其设计策略的一部分，公司还可帮助客户选择第三方供应商，以优化其集成和验证，并寻找和选择最佳解决方案，同时随着市场或技术条件的发展应用同等或更好的技术。此外，ABB 会与关键技术合作伙伴保持紧密合作，以提供集成技术包。从业务和技术角度来看，此类合作伙伴关系对于实现公司愿景是至关重要的。

超越标准

有效的网络安全不仅仅只是遵守标准和法规。ABB 了解 IEC 62443、NIST 800-82 和 ISO 27002 等法规在确保网络安全合规性方面所起的重要作用，同时与客户保持紧密合作，确保

02

01 针对性攻击和白噪声攻击概述。

02 ABB 可提供指引、产品和服务，以解决绿地和棕地应用中的问题。

其设计和配置完全满足客户基于其所选标准的合规需求。

ABB 意识到，客户关心防范网络安全事件风险，并将其降至最低。虽然资产所有者对所有事件响应程序负有主要责任，但 ABB 会积极监视任何可能对 ABB 控制系统造成潜在影响的网络安全威胁。另外，ABB 会在发生危急情况时主动与客户沟通，并维持良好机制，

ABB 拥有提供安全纵深防御的领域知识和经验。

使客户能够通过双向沟通向 ABB 产品安全小组传达任何潜在的担忧或威胁。总而言之，ABB 的定位是一家系统集成商，这是公司在工业控制领域的网络安全战略的基础考虑因素。主要涵括两个方面：首先，让客户相信，在 ABB 参考架构中实施第三方解决方案将会产生最佳价值；其次，让客户放心，如果在实施中出现故障或问题，对资产可用性或安全性产生影响的可能性极低，而且资产恢复更容易。

尽享数字化优势

网络安全涉及人、过程和技术。ABB 拥有提供安全纵深防御的领域知识和经验，这是现代公司选择 ABB 的先决条件。随着数字化时代趋于成熟，网络安全的意义远远不止于防范网络犯罪；联网一定要安全，而相关数据的价值也应得到保护。ABB 认为，客户不应该为了实现数字化的优势而牺牲安全、价值或控制。有鉴于此，ABB 采用创新型多层安全方法来封闭这些需求间的循环。•