白皮书

保护网络设备安全：
IEC 62443-4-2标准介绍

陈文翰
产品经理

MOXA®

行业背景

随着工业互联网的发展，越来越多的工业设备连接入网。企业内部的封闭IT网络正逐渐与公众互联网连通。一方面，工业互联网大大推动了生产效率的提升；另一方面，由此产生的网络安全威胁也日益引起终端用户的重视。这种对网络安全的担忧并非杞人忧天。根据美国工业控制系统网络应急响应小组(ICS-CERT)近期发布的一项报告，2015年，调查人员在美国共处理了295起针对基础设施的网络攻击事件，其中有33%发生在关键制造行业；而在2014年，这两个数字分别为245和27%。由此可见，终端用户越来越需要网络安全解决方案来为工业应用建立安全保障系统。

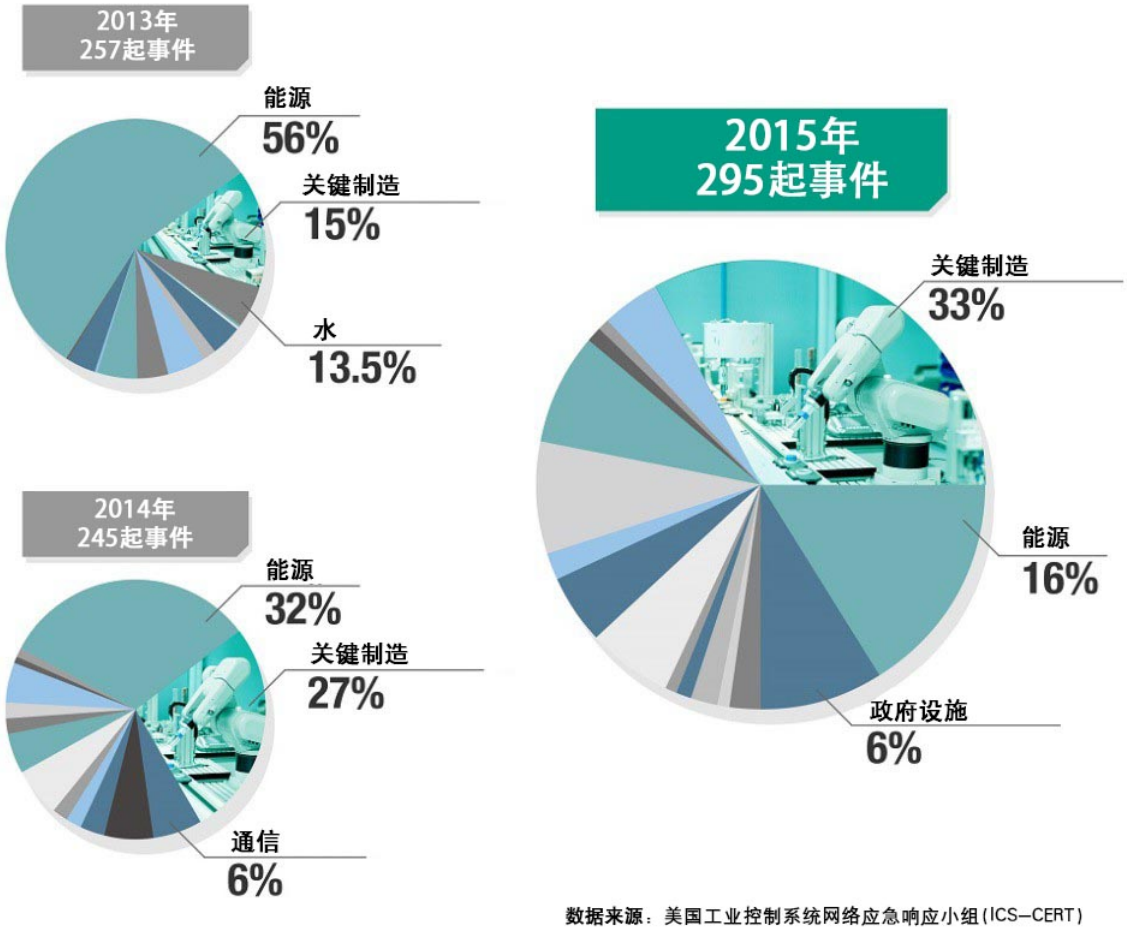

图1：关键制造行业网络攻击事件概况

2017年2月6日发布

Moxa是工业自动化的领导厂商，提供完整的工业接口设备连网、工业计算机及工业网络解决方案，致力于工业互联网的共同推动与实践。Moxa以逾30年的产业经验、连结全球逾4,000 万台的工业设备，跨越70余国，提供全球完善的经销和服务网络；Moxa以「可靠连网，真诚服务」的品牌承诺，协助客户打造工业通讯基础建置，提升工业自动化与通讯应用，创造长远的竞争优势及商业价值。如需获取Moxa解决方案的更多信息，请访问www.moxa.com.cn。

联系方式
电话：+86 21 5258 9955
传真：+86 21 5258 0055

MOXA
Reliable Networks ▲ Sincere Service

网络安全标准的发展

2002年，国际自动化学会(ISA)制定了ISA-99标准，为工业自动化领域的企业防范网络安全威胁提供建议。当时，网络安全问题尚未成为热点话题。ISA标准发布后，网络安全开始受到越来越多的关注。为与使用频率更高的国际电工委员会(IEC)相关标准命名统一，ISA-99更名为ISA 6244，即IEC 62443。IEC 62443标准体系包含一系列标准、报告和指导文件，提供了保障工业自动化控制系统(IACS)信息安全的规范做法。遵循IEC 62443标准可以有效减少网络安全危机的发生。

IEC 62443标准简介

IEC 62443标准涉及到了网络上的各个节点，为不同职责的参与方提供了操作规范。过去，终端用户依靠Siemens、Honeywell和ABB等系统集成商提供网络安全解决方案。但是现在，很多系统集成商会要求组件供应商提供符合IEC 62443相关标准的设备。下图展示了IEC 62443标准体系的结构以及每个部分对网络安全保障的作用。

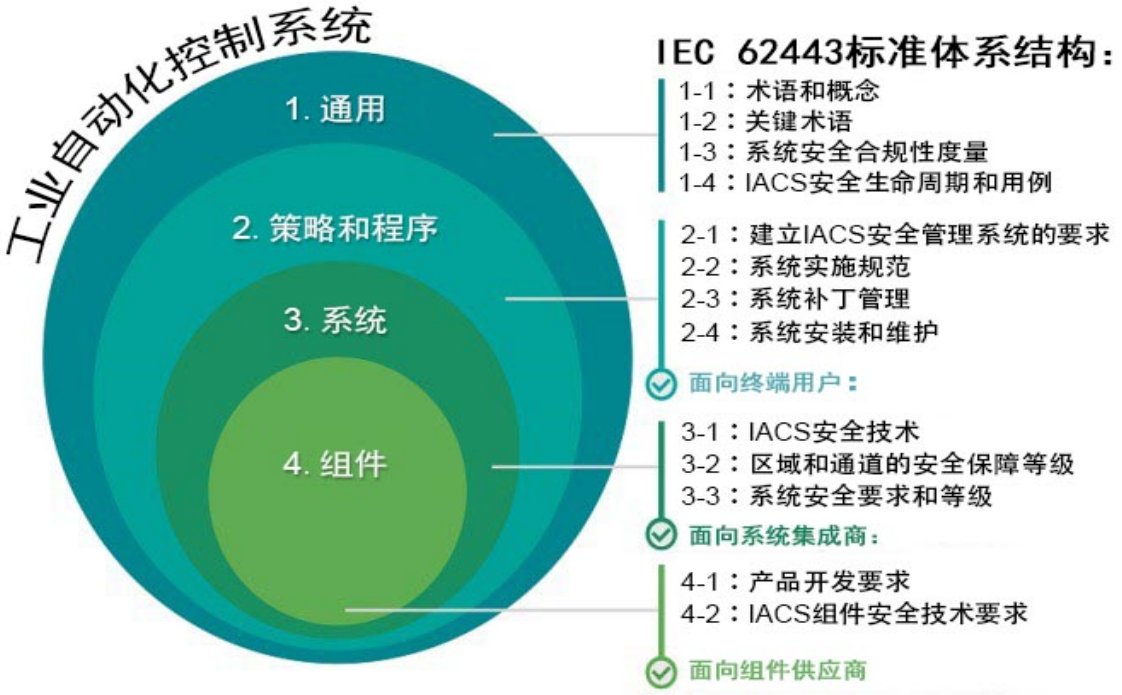

图2：工业自动化控制系统(IACS)概览

IEC 62443标准定义了四个安全保护等级。Level 2安全等级是适用于自动化行业的基本要求，主要针对工业网络系统集成商最常遇见的网络攻击威胁。Level 1针对偶发的未经授权访问，Level 3和4则针对使用了特殊工具及技术的恶意攻击。

IEC 62443-4-2 Level 2：自动化行业的基本要求

IEC 62443标准包含为不同对象制定的各项细则。由于系统集成商不断要求组件供应商遵守IEC 62443-4-2细则提供的相关指导，这部分内容变得愈发重要。对组件的要求源自最基本的行业要求，包括识别和验证控制、使用权限控制、数据完整性与保密性、确保资源可用性的备份功能等。鉴于组件供应商在工业互联网中扮演着日益关键的角色，本文接下来将重点介绍组件供应商在设计工业互联网设备时必须满足的几点安全要求。

基础设施

若某个网络组件允许用户访问设备或应用，该组件必须能够识别和验证包括人、程序和设备在内的所有用户，进而实现责任分离。用户只需获得完成其特定职责所需信息和设备的最小权限访问。应避免给予用户过多的访问权限，以免造成不必要的安全风险。而摒除此种风险，将能防止不怀好意的用户给网络带来损失。遵守这一原则有助于确保网络基础设施安全，为网络的发展打下坚实基础，以便更好地应对当前及日后的安全挑战。

账号管理

网络必须支持包括设立、激活、更改、停用、注销账号在内的账号管理能力。如此一来，未经授权者便无法创建、更改或删除账号；也避免了内置设备在未经授权的情况下相互连接。账号管理涉及多种可能的情形，如处置不当可能会给终端用户带来诸多麻烦。例如，某位员工升职后需要访问更多设备和应用，其权限也应相应调整。另一种常见的情形发生在员工离职后：员工离职后必须立即注销其登录账号，并撤销其权限。不难想象，一个刚被辞退的员工如心怀不满，很可能会恶意破坏公司的网络。

标识符管理

任何带有直接用户界面的网络组件都应集成识别系统，通过用户身份、组别、职责和/或系统界面识别用户，从而防止未授权用户访问联网设备。职责不同的用户所拥有的权限也不同。例如：使用网络管理员账号可管理网络中的设备配置，但一般访客只能浏览设备内容，无权更改设备配置。此外，还应制定安全程序，如对闲置超过特定时限的账号予以撤销。标识符管理能控制网络中的用户账号，确保用户严格遵循管理员分配的角色，防止用户无意进入或故意闯入访问权限以外的区域。

验证器管理

所有联网设备都必须能够验证系统或固件升级请求的真实性，并确保升级来源不包含病毒或恶意软件。可供选择的验证方式包括使用令牌、密钥、证书或密码。若未启用验证器管理，任何想要入侵网络的人都能随意上传恶意软件，继而更改设置或控制整个网络。

密码验证

使用密码进行验证的网络组件应采用执行以下规定的密码策略：

A) 在用户设立密码前，必须明确说明构成有效密码的字符类型和数量

B) 规定用户更换密码的频率

使用密码的好处是，能在不增加系统工程师工作量的同时，方便网络管理员保护网络安全。有效的密码策略能阻止大部分黑客通过暴力解码获得访问权限。对不支持密码策略或允许用户使用弱密码的网络而言，遭到黑客入侵的几率会大大增加。

公共密钥认证

公共密钥认证的使用，是为了在服务器与设备、设备与设备之间建立安全连接。为实现这一功能，每个网络组件都必须能够确认签名真伪以及证书的吊销状态，从而验证证书的有效性。此外，每个网络组件都应建立一个认证通道，与公认的认证中心相连接。如果是自签名证书，则应将证书部署于与证书发布主体通信的所有主机设备。公共密钥认证至关重要，不仅因为它可以防止将信息传送到错误的地方，还可以防止本应在网络内部保存的机密信息被转移至无法验证来源的外部网络。

使用权限控制

网络中部署的所有设备都必须支持登录验证。为防止不相关的用户访问设备或网络，应用或设备必须限制用户输错密码的次数，超出次数则锁定账号。鉴于对工业网络的大多数攻击都是由黑客使用暴力解密完成，因此登录验证是防止黑客获得访问网络权限的最有效途径。此外，系统或设备必须能够告知用户登录尝试是否成功。当用户知道已成功登录到网络，他们就可以确认自己当前的状态，并知晓他们对网络设置或设备的更改已获得认证。

数据完整性

数据完整性在工业互联网中发挥着十分重要的作用。它可以确保数据准确无误，并且能保证可靠地处理和恢复这些数据。保护数据的安全措施多种多样，包括能对网站浏览器和服务器之间的传输进行加密的SSL协议。由于数据在网络中不停移动，网络运营商需确保数据以安全、可靠、有效的方式传输。如果数据传送至不相关的接收者，网络运营商不仅无法控制这些数据，而且会使他们的网络更易遭到黑客攻击。

确保资源可用性的备份功能

网络中的所有应用或设备都应能够在不影响网络运行的情况下进行数据备份。定期备份数据的最大好处在于可以确保数据完整无缺，且如果网络运行出现故障，可以利用已备份的数据让网络恢复正常。此外，在数据备份过程中，必须保证网络上的私人信息按照数据保护策略妥善储存，任何不应获取这些信息的人都无法访问这些信息。在某些情况下，这意味着数据不能保存在网络之外。包含用户个人信息的任何数据外泄，都会对网络运营商和信息遭泄露的用户造成严重损害。

总结

随着联网设备日益增多，这些设备的安全成为终端用户关注的首要问题。业内一致认为，采用最佳安全保障措施能帮助用户保护他们的网络不受恶意攻击。为了增强组件级别的网络安全，Moxa最新推出一款交换机固件——Turbo Pack 3，它不仅符合IEC 62443-4-2 Level 2标准，同时还支持增强型MAC地址和RADIUS身份认证等其他安全功能，能确保数据完整，防止网络受到已知安全漏洞和未知攻击的影响。

了解更多有关Moxa工业以太网交换机的信息，请访问：

http://www.moxa.com.cn/product/Industrial_Ethernet_Switches.htm

免责声明

本文仅供参考，内容如有更改，不做另行通知。本文不保证无错误，任何口头明示或法律默示的担保或条款，包括任何适销性或特定用途的担保或条款，对本文不具有约束力。我们特此声明，不承担与本文有关的任何责任，本文不直接或间接构成任何合同义务。