protiviti®
Global Business Consulting
甫瀚

OT 安全：日益增长的威胁与应对方式

敏于知

什么是 OT 安全

OT（Operational Technology），或称运营技术，通常指工业生产环境中检测和控制的物理设备，以及工艺流程中涉及的各种硬件和软件，其核心组件包括数据采集与监控系统（SCADA）、集散控制系统（DCS）、可编程逻辑控制器（PLC）等。

随着信息化的发展，越来越多的攻击或瞄准了 OT 环境中特有的漏洞，或针对了现代化的生产环境中 OT 环境与外界的交互，或利用了 OT 环境较陈旧的安全设备（通常出于稳定性的考虑带来的后果）。如何确保 OT 环境中系统的安全性、数据的可用性及保密性、环境的稳定性等等，是 OT 安全急需考虑的。

企业的 OT 安全趋势

2017 年，美国 FDA（美国食品药物管理局）承认并确认，圣犹达医疗公司（St. Jude Medical）的植入式心脏设备（心脏起搏器和除颤器）是可以被入侵的[1]，FDA 表示，负责读取与医生共享设备数据的设备发射器是受到攻击的一个薄弱点。2016 年，出现一种名为 Mirai 的恶意软件，其旨在攻击连接到网络的基于 Linux 的设备，并将其变成远程控制的机器人，以攻击众多物联网设备[2]。

从以上案例可以看出，近年来，相较于传统的 IT 安全，OT 安全在各大企业中越来越受到重视，尤其是在后疫情时代，日趋复杂的网络环境和攻击手段，使得越来越多的企业将目光聚焦于生产与运营安全之上。

对相当大一部分企业，包括制造业、制药、能源、食品等，OT 网络是其日常运作的关键部分。但并非所有 OT 技术都与 IT 相关，也并非所有 OT 相关的安全问题都能被 IT 安全方案解决，所以正确认识到 OT 安全的重要性和独特性，是确保 OT 安全的必要前提。

OT 安全包括范围

顾名思义，OT 描述了支持和实现工业运营的技术组合。其涵盖了从运输（铁路、海运等）到物流（港口、仓库等）等众多行业的各种系统。OT 还包括所谓的“网络物理系统”，即负责监测和控制现实中生产流程的一组技术，常见的系统包括有：

ICS（工业控制系统）	ICS 包括一系列有时被称为“工厂自动化”或“分布式控制系统”的系统，有时包括下述 DCS、SCADA 和 IIoT。通常，工业控制系统是作为制造、过程管理、铁路或海上运输控制以及其他类似功能的接口。

[1] Abbott (formally known as “St. Jude Medical”) Recalls Assurity™ and Endurity™ Pacemakers for Potential Moisture Ingress Causing Electrical Short and Reduced Battery Life
[2] NJCCIC Threat Profile Mirai

DCS（分布式控制系统）	作为 ICS 的一个子集，DCS 描述了离散或连续制造环境中的复杂系统，帮助控制和管理生产设施。发电、制造和炼油等功能通常在一个单一的地理地点拥有大量的 OT 资产。
SCADA（监督控制和数据采集系统）	SCADA 系统作为一个总体的数据网络运作，捕捉工业过程的输入和输出，并促进系统的监测、分析和控制。SCADA 系统从广泛分布的 I/O 设备中收集数据，这些设备分布在很大的地理范围内，诸如电力传输、管道和铁路等过程通常都部署了 SCADA 技术。
建筑物和物理访问控制	OT 还包括控制物理设施的系统，如电梯、HVAC 系统、照明和其他物理元素。建筑和访问控制还包括安全摄像机、刷卡、电子门锁和类似系统。这种建筑控制使用专有协议，并采用与上述工业控制系统非常不同的方法。
IIoT（工业物联网）	IIoT 有时被认为是 ICS 或 SCADA 的一个子集，但实际上它属于一个单独的子类别，因为 IIoT 设备通常不连接到控制网络，而是通过公共或私人无线网络运行，这种区别引起了独特的安全挑战。

与传统的 IT 环境不同的是，OT 会涉及到更多类型的设备。如服务器、工作站、防火墙、二极管、远程终端设备（RTU）、继电器、I/O 设备、IIoT 传感器、摄像头和备用电源等，只是构成现代 OT 环境的数千种设备类型中的一小部分。我们通常将这些设备分为四个主要的类型：

服务器、工作站、HMI 等	此类设备通常运行传统的操作系统，如 Windows 或 Linux，用于各种控制和报告任务，从领域控制到操作关键的过程应用软件。它们也可以充当数据服务器，来收集和转发数据。
网络设备	除了传统的 IT 风格的交换机和防火墙外，OT 系统还包括专门的网络设备，如使用工业协议控制流量的工业防火墙。这些特制的设备通常是使用制造商的专有嵌入式操作系统。
嵌入式控制设备	此类设备包括 PLC（可编程逻辑控制器）、分布式控制系统控制器、远程终端设备、保护性继电器、制造设备的机器控制、物理访问控制等。如在医疗领域，这些设备控制输入和输出的药物剂量或生物调控信号。这些设备在由制造商开发的专有的嵌入式操作系统中运行，而该系统则通常建立在带有定制元素的商品组件上。
输入 / 输出（I/O）设备	I/O 设备有时与控制集成在一起，但在这里我们将纯 I/O 设备分开，它们为过程提供输入或输出。这些设备可以是 PLC 机架上的集成控制卡、摄像机、压力或温度传感器，以及成千上万的其他类型。与嵌入式控制设备一样，这些设备也运行在专有的制造商操作系统上，这些系统通常建立在带有定制元素的商品组件上。

常见 OT 安全威胁状况

对 OT 系统日益增长的威胁主要由以下几个因素驱动：

- **OT 和 IT 之间的连接性**

历史上，许多 OT 系统与企业 IT 系统的连接有限。大多数 OT 系统是在 OT 协议上运行，不依赖于企业应用程序，其通常利用专有的操作系统和设备，并保持与企业网络的隔离。在过去的二十年里，IT 和 OT 之间的这种分离已经消失了。甚至在现代推动 IIoT 或“工业 4.0”之前，提供控制系统的工业组织和 OEM 就已经对系统进行了“现代化”，导致与传统 IT 网络和设备的连接增加。现代 OT 环境也采用了传统的硬件和软件，如 Windows 操作系统、虚拟环境和 IT 网络设备。随着 IIoT 计划的增加，这种连接正在扩大，因为分析和生产力需要与企业云和数据中心应用直接连接。

- **对 OT 漏洞的研究和关注**

多年来，OT 受益于所谓“隐蔽的安全”。虽然众所周知且广泛分布的 IT 系统对攻击者来说是很有吸引力的目标，但 OT 安全中不太为人所知的定制产品却大多不被黑客所关注。随着商品化 IT 设备在 OT 中的使用增加，以及利用传统 IT 嵌入式组件来构建 OT 固件和应用程序的普遍做法，这种情况已经改变。

- **有针对性的攻击增加**

在过去 20 年的大部分时间里，犯罪分子专注于窃取高价值数据，如信用卡或私人医疗信息。随着攻击者在工业目标中发现新的获利方式，这种情况正在改变。工业组织已经表现出愿意向勒索软件行为者支付数百万美元，以避免昂贵的停工。同时，正如近年来一些报告所指出的那样，一些对关键基础设施的威胁也日益增加。

常见 OT 安全框架

NIST CSF [3]	NIST 有非常详细的网络安全控制建议，包括一些专门针对工业控制系统的建议，以及针对物联网环境的新兴指南。NIST 的五个功能涵盖了技术和程序控制，为网络安全评估提供了一个基础。在其每个功能领域，NIST CSF 描述了具有详细指南的子控制，以达到特定的成熟度水平。
CIS 控制清单 [4]	CIS 是一个非营利性的非政府组织，旨在全面提高个人、企业和政府的网络安全。大约十年前，DHS/CISA、SANS 和一些国际网络安全机构走到一起，建立了一套共同的控制措施，目的是提高任何组织的安全成熟度。该框架最初被称为 CSC 20，在 2021 年 5 月被缩减为 18 个高级控制的简化列表。更新后的顶级控制清单有 153 个子控制或“保障措施”，比 NIST CSF 提供更多的规范性指导。CIS 在设计其框架时考虑到了 IT，但许多 CIS 的控制措施并没有转化为 OT 中的敏感和嵌入式设备。好消息是，CIS 已经开发了一个 “OT” 版本，试图解决这些限制。
NIST 800-53 [5]	大多数组织将使用 800-53 作为其基于 CSF 的计划的改进，而不是试图实现对 800-53 标准中所有元素的全面控制。NIST 800-53 有 200 多页，涵盖了从传统的 IT 类控制到 ICS 安全的具体细节。
ISO 27000 [6]	ISO 27000 是一个通用的 IT 安全标准。虽然它不是专门针对 OT 或 ICS 系统设计，然而，与 NIST CSF 和 CIS 类似，ISO 27000 标准的许多组件与 OT 环境高度相关。ISO 27000 系列是程序性的,通常与技术性更强的 NIST CSF 或 IEC 62443 一起使用。
IEC 62443/ ISA 99 [7]	IEC 62443/ISA 99 是一个针对 OT 的标准。该框架由国际标准化组织和国际自动化学会联合开发,详细说明了四个级别,旨在为不同类型或成熟度的攻击提供安全保障。企业可以根据自己独特的合规性或供应链要求来决定哪一个安全级别是最合适的。整体性的 IEC 62443/ISA 99 可以作为一个 NIST CSF 外的框架，帮助指导基于 NIST 的项目中的特定 OT 实施。

[3] Cybersecurity Framework | NIST
[4] The 18 CIS Critical Security Controls (cisecurity.org)
[5] SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
[6] The ISO 27000 family of standards (isms.online)
[7] ISA99, Industrial Automation and Control Systems Security (isa.org)

加强 OT 系统管理的必要性

在未来五到十年内，OT 需要采用 IT 系统和安全管理的核心要素。迄今为止，大多数工业组织都依赖于对其 OT 系统的网络保护，即防火墙或网闸、空气隔离、网络异常检测或 IDS/IPS 等。这些举措在深度防御模式中固然有价值，但其效果会在未来五年变得越来越小，需要实施更全面的 OT 安全管理计划。以下几个趋势和事件将会推动这种变化：

- IIoT/ 工业 4.0 在工业运营和互联网之间的连接性越来越高
- OT 设备的公共漏洞越来越多
- OT 安全方面的监管压力越来越大
- 来自 CISO/ 董事会的压力越来越大

企业的应对之道 — OT 网络安全计划

要在 OT 安全方面获得成功，企业需要以系统性的方法来不断提高 OT 环境中的网络安全成熟度和有效性。有效评估和优先排序的步骤包括：

- **了解自身情况**

这包括了深入到资产本身，收集必要的数据，对风险和解决这些风险的潜在成熟度影响进行优先排序。涉及到逐个资产的风险评估，收集细节，如已知的漏洞、用户和账户风险、访问风险、配置风险，以及网络设计和实施。

- **制定路线图**

将风险转化为一个计划性的路线图，以弥补已知的差距。路线图通常包括规定行动的不同时间范围。

- **开始修复计划**

在几乎所有的 OT 安全评估中，开始时都会涉及到不安全架构、漏洞软件和管理不当的用户账户等问题。以我们的经验，通常需要大量的项目资源来解决诸如网络分段、安全远程访问、备份以及系统补丁和升级等项目。

- **监测和维护**

这是区分成熟和不成熟的关键时期。项目计划和路线图应该包括预算、资源和流程，来确保对工作进行监测和维护。这涵盖了对配置、威胁、漏洞、补丁、访问管理等的监控，以及应具备报告所有这些指标的能力。而且最为重要的是，这项工作还需要高级管理层的持续支持。

达于行

甫瀚咨询可提供的服务

甫瀚咨询为企业提供 OT 安全评估，从治理、合规及技术角度，全面协助企业提升 OT 安全防护水平，达成 OT 安全防护从无到有、从弱到强的转变，为优化企业综合安全治理水平奠定基础。我们可提供的 OT 安全相关服务包括：

OT 安全评估

通过包括从 OT 安全管理到具体实施措施的全方面评估及修复提升计划，为企业提供一站式的 OT 安全解决方案。

物理安全评估

涵盖物理控制、访问控制、HVAC 等各方面，确保在企业信息安全和 OT 安全的基础上，提供最高级的物理安全保证。

数据安全评估

保护客户最珍贵的数据资产，在企业数据安全管理和运营的基础上，为数据的全生命周期进行定制化的安全评估。

安全意识与能力培训

针对行业 / 企业 / 部门 / 角色等高度定制化的安全意识与能力培训，提供最大化的效率和安全意识，确保人员管理不再是企业安全的短板。

安全体系建设

从 OT 安全出发，帮助客户从更全面的商业和技术角度看待风险状况，运用行业通用的信息安全框架来实现整体安全能力和安全价值提升。

关于甫瀚咨询

甫瀚咨询是一家全球性的咨询机构，为企业带来领先的专业知识、客观的见解、量身定制的方案和卓越的合作体验，协助企业领导者们充满信心地面对未来。透过甫瀚咨询网络和遍布全球超过25个国家的逾85家分支机构和成员公司，我们为客户提供财务、信息技术、运营、数据、数字化、环境、社会及管治、治理、风险管理以及内部审计领域的咨询解决方案。

甫瀚咨询荣膺2022年《财富》杂志年度最佳雇主百强，我们为超过80%的财富100强及近80%的财富500强企业提供咨询服务，亦与政府机构和成长型中小企业开展合作，其中包括计划上市的企业。甫瀚咨询是Robert Half International Inc.（纽约证券交易所代码：RHI）的全资子公司。RHI于1948年成立，为标准普尔500指数的成员公司。

联络方式

北京
朝阳区建国门外大街 1 号
国贸写字楼 1 座 718 室
电话：(86.10) 8515 1233

上海
徐汇区陕西南路 288 号
环贸广场二期 1915-16 室
电话：(86.21) 5153 6900

深圳
福田区中心四路 1 号
嘉里建设广场 1 座 1404 室
电话：(86.755) 2598 2086

香港
中环 干诺道中 41 号
盈置大厦 9 楼
电话：(852) 2238 0499

protiviti 甫瀚