工业制造业热门话题

如何保护运营技术免受网络攻击

pwc 普华永道

工业制造企业正在经历第四次工业革命，数字化程度的提升使企业效率显著提高。然而，数字化转型也加剧了企业受到网络攻击的可能性，尤其是那些使用过时运营技术（以下简称为OT）的企业。

OT被称为网络与物理世界相遇的技术。在当下工业4.0以及新基建浪潮下，许多工业制造企业却仍在使用20年前建立的遗留系统。这些工业控制系统(ICS)例如逻辑可编程控制器（PLC）、远程控制终端（RTU）以及数据采集与监视控制系统（SCADA）等等，缺乏安全的网络设计，容易成为网络攻击目标。7月23日，美国国家安全局（NSA） 联合国土安全部下属的网络安全和基础设施安全局（CISA）共同发出预警，指出攻击者在持续利用可通过互联网访问的OT资产对关键基础设施开展恶意攻击。预警建议美国的工业企业立刻减少OT控制系统对外暴露的访问路径，从而减少各类攻击的可能。对于中国工业制造企业而言，也要对网络威胁这个关键风险因素提高警惕并加速部署应对方案。本文将探讨工业制造企业OT的网络安全风险和应对措施。

IT/OT的深度融合凸显网络安全问题

工业制造企业在发展过程中往往会引入IT技术，尤其是数据分析、处理与实时监控方面，使企业能够更智能、更准确地捕捉市场需求，从而获得更高的利润。工业4.0以及新基建浪潮将更加深入地推动工业互联网发展，也将为整个行业带来更广阔的发展空间。

随着制造业IT和OT领域深度融合，网络安全的范畴也从IT领域扩大到OT环境。但OT下的网络安全与传统IT安全仍存在较大差异。例如：OT安全更注重工业自动化控制设备的高可用性，而传统IT环境更注重数据的机密性。由于性能和属性不同，OT安全的影响范围也从系统和数据延伸到人员安全、环境安全以及财产安全，甚至国家安全。

OT环境下网络安全风险案例

随着工业企业不断增加远程操作、远程监控、以及为了工作效率而不断扩大的关键技能领域（如仪器和控制、OT资产管理/维护）的外包规模，可通过互联网访问的OT资产变得越来越多。最近几年，普华永道观察到越来越多针对工业制造业OT环境的网络攻击事件。2017年，一家中东地区的石油企业遭受到TRITON恶意软件攻击，攻击目标是某全球主流工控系统厂商的安全仪表系统（SIS），此次攻击导致一些SIS控制器的正常安全状态被破坏转而切换到失败的安全状态，甚至自动关闭了工业流程。通过分析得知，该恶意软件从IT渗入到OT核心组件已经有一段时间，但攻击者并不急于兑现攻击效果，而是策划长时间潜伏在网络中等待关键时刻发起攻击，进而影响石油供应和期货价格，给受害者造成重大损失。

另一个案例是在2018年3月，某全球领先的半导体台商工厂内，一位工程师的上位机遭勒索病毒入侵，造成该企业台湾新竹厂区、台中厂区及台南厂区这三大生产基地产全线停产。其后分析得知，上位机感染的勒索病毒为Wannacry。起因是第三方装配人员在配置过程中使用U盘拷贝文件，且结束操作后未进行恶意软件查杀操作，从而引致勒索病毒大范围传播。

无独有偶，2019年3月挪威铝业巨头也遭受到勒索病毒LockerGoga攻击，导致该企业多个区域工厂生产环境停摆并需要数月才能完全恢复，损失金额高达数亿人民币甚至更多。

OT网络安全风险应对六大措施

由于工业制造业所面对的网络安全风险不断增加，一旦资产受到破坏不但可能给企业带来损失，也会对社会和公众带来负面影响，由此国家监管机构的合规要求也随之增加和强化。例如《网络安全法》中对关键信息基础设施的规定、等级保护2.0基本要求中对工业控制系统的扩展要求、工信部发布的工业控制系统多项规定（如《工业控制系统信息安全防护指南》、《工业控制系统信息安全事件应急管理工作指南》、《工业数据分类分级指南（试行）》等），以及与之相对应的合规检查工作也已经由相关部门组织逐步开展。

针对于此，普华永道网络安全专家团队认为，工业制造业可采取以下措施减轻风险。

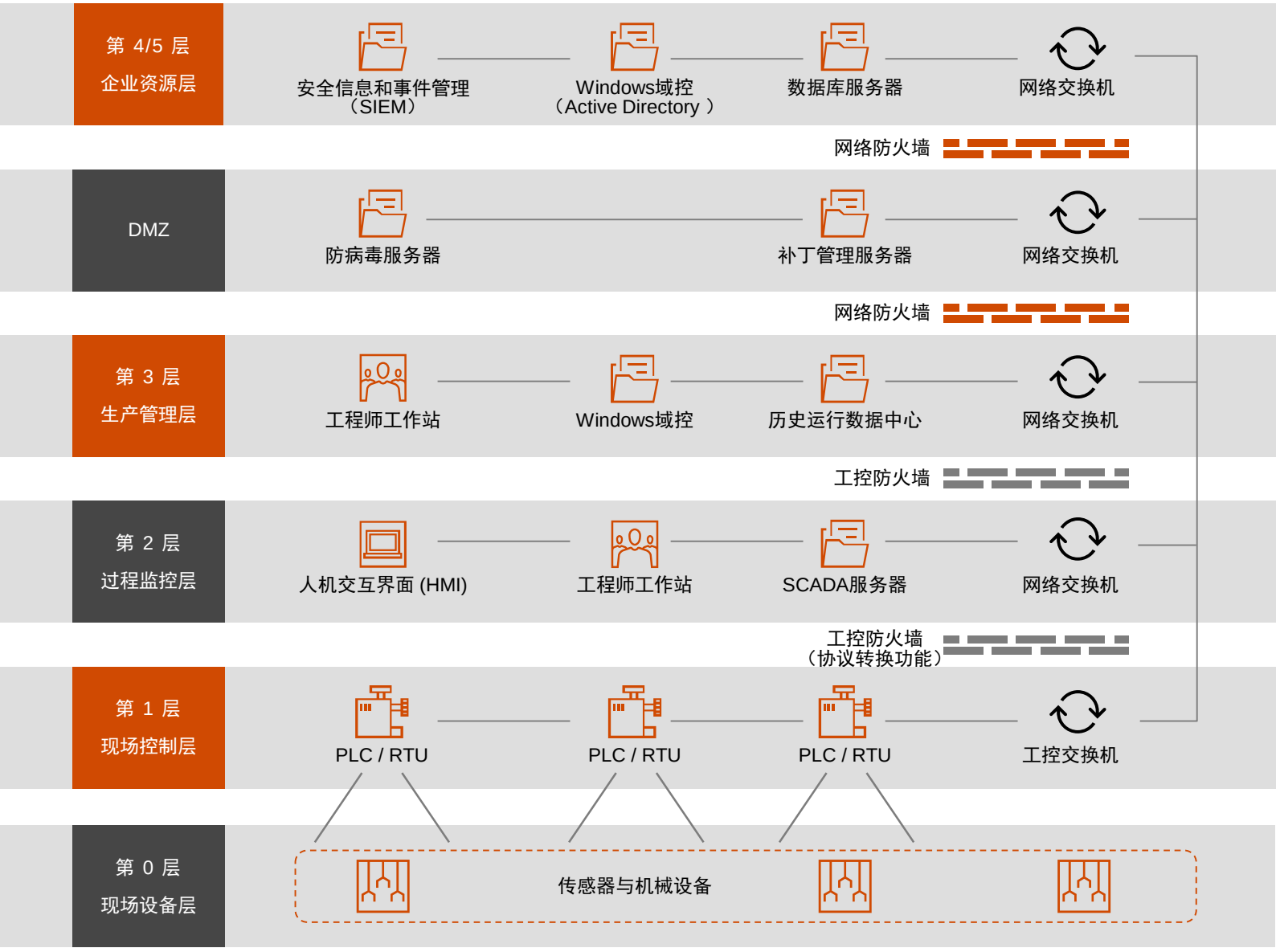
1) 识别和保护关键资产

工业制造企业在OT安全建设过程中，最重要的步骤之一是梳理现有资产，识别资产重要性进而准备可行的措施保护它们免受网络攻击。通过工具（或专业的商业方案）自动识别创建准确的资产清单，为持续降低网络风险提供基础。

2) 评估和设计OT网络隔离及安全架构

由于OT环境一般由专门的工程团队维护管理，因此往往缺少专业安全团队定期实施的专项OT安全评估。此类评估能更准确了解企业OT环境与业界最佳实践、合规要求的差距，发现问题后可及时采取修复措施。还应利用专业团队为企业设计规划OT网络安全架构（可参考业界常用的Purdue model架构），包括网络分级隔离，制定不同安全区域，访问控制等内容。针对必要的远程访问，需要进行强身份验证并部署实时日志监控措施以保证相关访问操作都是授权及必要的。企业还应该对标行业最佳实践，如NIST 800-82标准或IEC-62443系列标准帮助识别风险点，增强OT环境的安全防御能力。

OT环境安全架构示例图



3) 定期检测漏洞及配置管理

完成上述资产梳理与网络隔离后，定期检测以预防OT资产遗留重大漏洞也是重中之重。 与传统IT资产不同，OT资产无法经常打补丁、更新系统；但针对一定程度的重大漏洞，仍需要考虑采取一定的风险缓解措施，防止其被恶意利用。同时需要有完善的变更管理流程，确保系统、网络的配置变更是记录并授权的。

4)部署终端防护

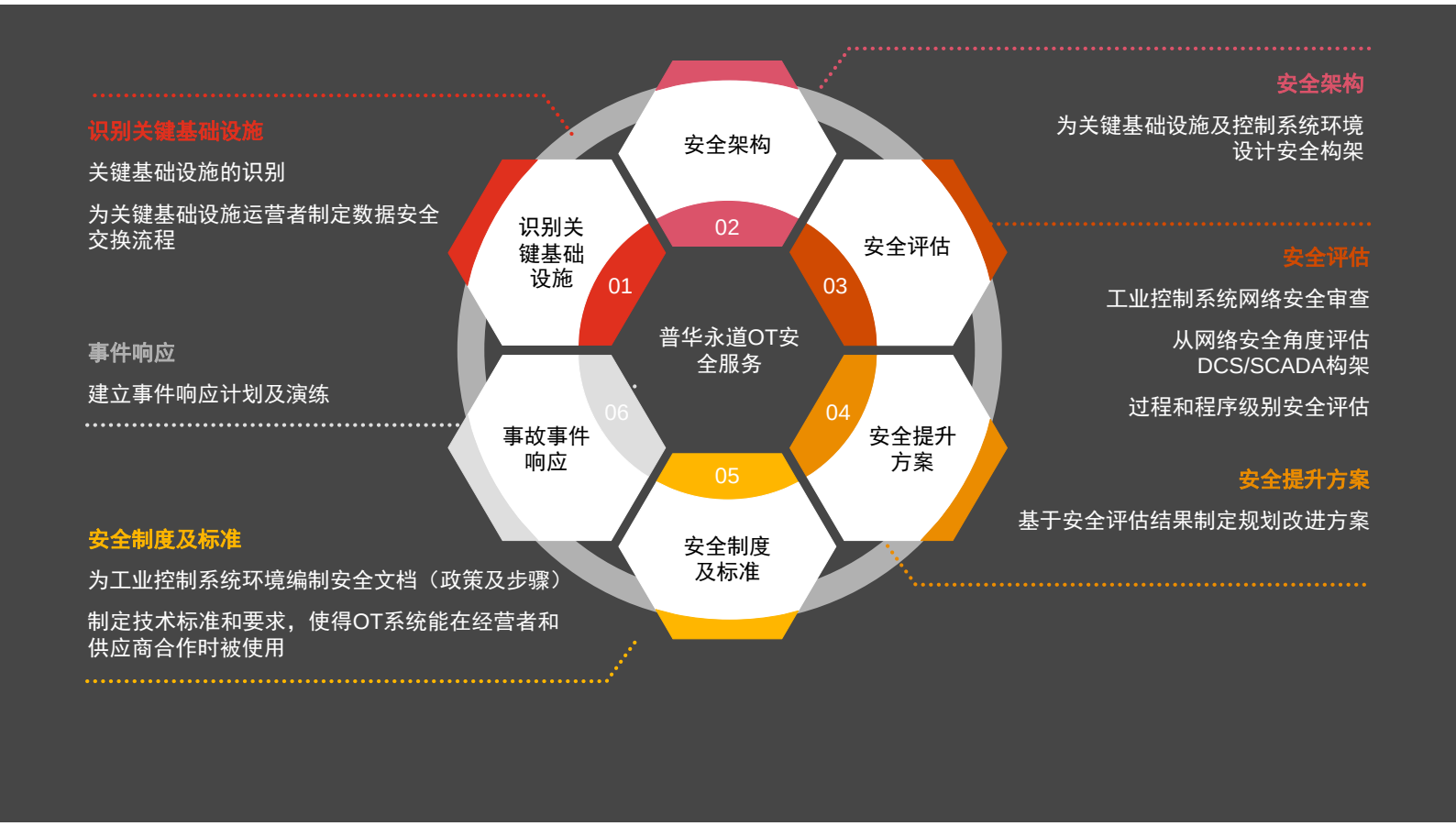
终端防护也是工业企业需关注的一个重要领域。在OT终端会使用与传统IT终端不同架构、不同操作系统的终端类型，也会使用基于特殊版本或老旧版本Windows或Linux操作系统的终端来支持各类工业应用。如此混杂环境给企业的终端管理带来了挑战，也会给病毒传播留下机会。这需要企业按照规模和实际预算部署杀毒软件、采用主机入侵防御系统（HIDS, Host Intrusion Detection System）、终端检测与响应（EDR, Endpoint Detection & Response）、白名单应用控制等解决方案降低来自终端的网络风险。

5) 建立安全事件应急响应机制

企业必须采取措施保持网络复原能力。良好的备份措施以及事件响应计划是保持OT环境及时恢复的基础。通过分析过去的违规行为，企业可以避免重复犯错。管理层还须定期与应急管理团队一起开展网络安全事件演练，当网络安全事件发生后，能迅速应对并恢复运营能力。

6) 组织培养网络安全人才

在IT/OT安全建设中，拥有经验的专业安全人才对监控及运营工业控制系统起着至关重要的作用。人员是所有网络安全问题的基础，企业必须实施培训计划，使员工在发生内部或外部攻击时知道如何采取行动。同时，企业还必须增强安全意识教育，发展企业内的安全文化。



总而言之，一个健全的OT安全防御系统对保护企业工业控制环境免受网络攻击至关重要。在OT运营和企业生产过程中，企业和董事会应重视OT安全建设并投入足够的资金、时间和精力，在业务发展的关键时刻需要咨询专业安全团队共同打造适合企业的安全防御体系。

联系我们

冯昊
普华永道中国能源与基建行业管理咨询合伙人
stanley.h.feng@cn.pwc.com
+86 (21) 2323 2818

李扬
普华永道中国网络安全管理咨询合伙人
Dennis.y.li@cn.pwc.com
+86 (10) 6533 7800

祁英
普华永道中国能源与基建行业管理咨询总监
ying.qi@cn.pwc.com
+86 (10) 6533 7588

潘晓鸥
普华永道中国网络安全管理咨询总监
sean.pan@cn.pwc.com
+86 21 2323 2693