数字化进程中OT-IT融合面临的安全挑战探讨

王进华

（胜科（中国）投资有限公司，江苏 南京 210000）

摘 要 在各行各业的数字化转型发展中，通过手机、PAD等IT终端远程访问和控制OT生产设备、实时了解生产信息非常普遍和高效。数字化的高效应用迫切需要OT-IT的技术融合，但同时也将生产安全、设备安全暴露在网络之上，如何保证生产安全，保护设备免遭网络的恶意攻击和勒索尤为重要。然而，OT-IT二者存在差异，将两者融合在一起共同保证系统和网络的安全，必然会带来更多的挑战。基于此，文章分析了这些挑战存在的客观原因，并提供了解决这些挑战的基本原则和思路，以期为相关人员提供参考。

关键词 运营技术；信息技术；工业控制系统；工业网络安全；漏洞管理

中图分类号：TN91 **文献标志码**：A **文章编号**：2097-3365(2024)10-0022-03

运营技术（OT）和信息技术（IT）两者源自两个完全不同的专业和方向。在互联网出现之前，OT和IT之间的界限是明确的、可见的。随着技术发展，为工厂车间和现场的几乎所有设备带来互相连接，界限已经模糊。这种连接正在以新的方式诠释OT和IT。它们需要融合到一起，然而，两个群体在这个话题上有不同的方法论和观念，势必带来了两者融合的矛盾，甚至是明显的冲突[1]。如何解决矛盾冲突，达成共识，共同提高系统的安全性和抗风险能力至关重要。

1 OT-IT的差异说明

如何能够让OT-IT经济、安全、有效地融合在一起，充分发挥数字化转型带来的业务发展，首先我们需要清楚地认识到它们之间的差异，才能很好地求同存异，才能全面、系统、有效地分析出安全风险，设计并实施有效的安全管理策略，为企业的数字化转型保驾护航。

1.1 安全职责不同

从根本上说，IT保护数据首要任务是保护知识产权、公司财务、业务、员工或客户私人信息等数据。有意或无意的网络威胁可能导致知识产权、公司财务、业务以及员工或客户信息的泄露损失，连锁反应可能会带来高昂的代价。

相比之下，OT使用工业控制系统（ICS）逻辑来执行控制过程，操控设备如阀门、电机、泵等，这会产生现实世界中物理、化学、生物等方面的影响[2]。网络威胁、错误指令等不安全行为可能对设备设施安全、服务、人员生命以及周边环境造成毁灭性的后果，正如许多事故发生所表明的那样。

1.2 安全性、完整性、可用性（CIA）优先级不同

关于信息系统我们通常会用安全性、完整性和可用性三个指标去衡量。IT和OT的不同优先级是理解为什么两个群体之间如此容易发生冲突的关键。IT的首要任务是保护数据，所以安全性是绝对优先，完整性其次，可用性最后，所以有时候为了保证数据的安全，IT可以随时终止相关的系统服务，牺牲可用性去保证数据安全。然而，OT的首要任务是保护生产流程的可用性和完整性，安全性排在最后[3]。因为OT的可用性一旦丧失，会引发物理世界的设备、流程状态失去监视和控制，可能导致设备财产、人员、环境等重大事故。

国内外相关权威标准同样能够证实这一观点，如OT领域全球知名和公认的网络安全标准ISA/IEC 62443系列，以及中国国家标准GB/T 40211/33007/35673等。其优先级不同，决定了IT和OT的解决方案的着重点不同。

1.3 网络结构和层次划分不同

典型的IT系统的网络结构大都以星型结构进行连接，再根据业务性质和规模确定是否需要层次划分。IT系统的网络结构灵活多变，力求互联互通，能够适应小至家庭、大至万人的企业需求。

OT系统的网络结构由于早期受制于不同制造厂商的限制，以及工厂控制系统规模的影响，所以结构形式复杂多样，无统一标准。20世纪90年代普渡模型（Purdue Model）概念被提出，并被ISA-99标准（现在的ISA/IEC 62443）及其他工业安全标准所采纳，同时也被中国国家标准采纳，作为工业控制系统网络分段的关键概念。其将工业控制网络由下至上分为0～5层：0现场设备层、1控制层、2区域监控、3企业监控、4、企

业管理层、5、信息化层[4]。部分规模较小的系统可能2～3层为同一层。同时，为了保证系统的及时性，减小网络负载，层与层之间的连接保持尽用、最少原则，减少一切非必要的连接。网络结构的不同使得集中化、商业化的IT安全解决方案不能适应OT的环境。

1.4 连接对象和通信协议不同

典型的IT系统的连接对象主要为计算机、服务器及相关的网络和安全设备，其适用的协议主要为TCP/IP、HTTP、FTP等公开、常用标准协议。

而OT系统的连接对象除了常规的工控机、服务器以外，其它还包括现场各种各样的设备、仪表等，如风机、电机、水泵、阀门、流量计、分析仪等，以及不同品牌厂家的控制器、HMI等。其所使用的通信协议也是基于不同厂家多种多样，如Modbus、OPC、Profibus、Profinet、CANopen、Modbus RTU、Modbus TCP、西门子PPI、S7、欧姆龙通信协议、OPT等。其多样性和私有性，也给网络设备兼容、协议的安全解析带来了很大的困难，常规的适用于IT环境的防火墙、威胁检测等设备可能无法很好地适用于OT环境。

1.5 漏洞管理的原则不同

在常规的IT系统中，我们的硬件设备可能3～5年就进行一次淘汰或升级，Windows及相关的应用软件的漏洞和补丁不停被发现和修复。作为IT安全的重要措施之一就是及时地为这些系统和软件安装上相应的补丁，避免因此遭受的威胁和风险。

但是OT工业控制系统决定着企业的生产制造，其设计生命周期往往是10～15年，乃至更长。频繁的软硬件的更新不仅会造成生产制造业务的中断，同时还需要巨额的资金投入[5]。另外，因为OT系统的私有性和兼容性，决定着控制系统软硬件的原始制造商的研发速度、更新速度会远远落后于IT的硬件升级和软件系统的漏洞更新。例如新的Windows系统的版本或漏洞补丁的发布，需要厂商在新的控制系统上进行大量的、长期的测试和验证，才能保证新版本或补丁对工控软硬件的可用性不产生任何影响。任何一点影响都有可能会带来巨大的损失，甚至灾难性的后果。所以，OT的生产运营和安全负责部门往往不支持漏洞的及时修复，甚至是不修复，因为他们存在不确定的后果。未经评估和验证的升级和修复带来的风险和损失可能大于漏洞本身的风险。

2 解决矛盾的管理措施

因为OT-IT之间存在诸多的不同，所以在企业设备管理运营团队和网络管理团队之间面临着各种分歧意见。ICS设备安全和网络安全的所有权通常存在混淆，但事实是IT团队并不监督或负责ICS的日常运营。生产安全和操作过程完整性通常不属于IT的职能或责任。在工业环境范围内操作时，IT部门虽然遵守了安全措施、政策和程序，但是他们无法确定生产运行、生产设备的策略或程序。期望IT部门负责OT或ICS的运行或通信协议是否安全是不合理的。他们没有相应的技能、措施、经验以及确保生产安全的能力。所以，消除这样的矛盾不仅需要从技术上，更需要从管理体系上求同存异，寻求安全目标的统一。

2.1 在最高级别获得战略一致性

目前，大多数企业负责OT和IT仍然是两个高度独立的部门，分别是运营部门和IT。他们有不同的人员、目标、政策和项目。建议从重组IT和OT部门开始，使其在战略上保持一致和统一。至少首席信息官（CIO）/首席信息安全官（CISO）和首席运营官（COO）应该有部分共同和重叠的安全目标和指标，这将迫使他们合作。CIO/CISO还必须对ICS的网络安全以及网络事件直接或间接造成的任何安全事件、可靠性事件或设备损坏承担全部责任。

2.2 成立联合工作组

参考NIST SP800-82r2建议创建一个联合工作组作为跨职能网络安全团队，以共享各种领域知识和经验，以评估和降低ICS的风险。NIST甚至特别指出了应该成为该网络安全工作组成员的要求，其中应包括：IT人员、控制工程师、控制系统操作员、网络和系统安全专家、一名管理人员、物理安全部门的成员。

联合工作组还应咨询：现场管理/设施主管、控制系统供应商、系统集成商以及企业CIO和COO。

2.3 制定统一目标和治理结构

联合工作组需要编制一份完整、有效的ICS关键资产清单，并开始风险评估，风险评估需要结合实际的资产价值、威胁、漏洞，并给出合理的风险处理意见，确定需要做什么。众所周知，风险无法100%消除，联合团队成员不能仅仅考虑自己团队的业绩或目标，不顾经济成本、盲目追求“零”风险，高安全都是不可接受的评估结论。

联合网络安全团队应该有“共同治理”的责任和意识，并促进公司跨部门协作、跨学科技能的发展。

3 解决矛盾的建议实践

在管理目标实现一致的基础上，如何实施网络安全的最佳实践，如何面对越来越多的网络威胁，相关标准在塑造这些实践方面提供了重要的结构化指导和框架。相关OT网络安全的通用标准包括IEC 62443、NIST SP 800-82。参考既定标准和指南，结合现场的

实际应用得出的一些最佳实践如下。

3.1 制定风险管理和安全政策

整理和收集所有OT设备和软件的资产清单，根据资产的重要性及其入侵对组织的潜在影响对资产进行分类。然后执行定期风险评估，识别出其中的漏洞、风险，并根据它们潜在的风险级别确定其优先级。最后，建立和维护特定于OT环境需求的安全策略，明确划分人员之间的安全责任。

3.2 有效的物理防护

在系统安全防护方面，我们会着重强调网络安全的风险，往往忽视了物理安全的风险存在。因为OT设备主要服务于生产，它的分布范围比较广，遍布全厂，不像IT的设备和服务器主要集中于机房，所以难以用集中管理的方式进行保护。而且OT设备面对的用户除了专业的控制工程师，还有电气、仪表、机械工程师、维修工人，以及生产操作人员。所以设计时需要充分考虑到OT设备用户对象、工作权限，采取有效的物理防护，减少非必要人员的直接接触，可以大大降低可能带来的安全风险。著名的伊朗铀浓缩设施遭受“震网”蠕虫病毒的攻击，其病毒就是通过工作人员的U盘介质，在不同的电脑设备间传递、摆渡到核设施的OT系统中，造成了核电站离心机损坏，导致了核电站推迟发电达两年之久。

3.3 具有持续的网络安全监控

将OT网络与IT网络逻辑上隔离开来，并使用防火墙和非军事区（DMZ）来控制不同网段之间的流量，实施持续监控策略，以实时检测异常活动或未经授权的访问尝试。这可能涉及为OT环境量身定制的入侵检测系统（IDS）。

3.4 进行访问控制和管理

标准化访问控制、身份验证和授权（通常称为3A策略），以确保关键系统仅供授权用户访问。强制执行最小权限原则，确保用户仅具有执行其工作职能所需的访问权限。不仅在本地进行访问时需要进行必要有效的控制和管理，必要时在远程访问OT系统时，也需要利用多因素身份验证（MFA），在传统用户名和密码之外增加额外的安全层。

3.5 维护系统和数据的完整性

建立应用补丁、改造升级的系统方法，同时考虑OT环境的操作限制。在实施各种改造、升级、补丁修复之前做好充分的风险评估和应急措施，积极寻求相关专家和原始制造商OEM的意见和支持，不能仅仅为了完成某些安全指标而进行非必要的升级改造或补丁修复。当然，如果升级、修补不可行，需要实施其他补偿措施来防范或缓解可能带来的风险。另外，通过实施备份过程并在适当的情况下使用加密措施来保护传输中和静态的敏感数据，从而确保数据完整性。

3.6 制定事件响应和恢复

制定事件响应计划，其中包括针对OT环境的特定程序，同时考虑网络事件的潜在物理影响。制定灾难恢复计划，以便在发生网络安全事件时以最短的停机时间恢复运营。

3.7 持续开展教育培训

定期对所有OT人员进行网络安全意识培训，重点关注OT网络安全的独特方面。为IT和OT安全团队提供技术培训，涵盖OT环境中使用的特定技术和流程。

4 结论

缓解或解决IT和OT融合中固有的矛盾冲突并提高ICS安全性并非一蹴而就。管理者需要学会共享目标，共同评估和承担业务风险和后果。这意味着IT和OT专业人员必须找到共同点，使两者之间没有明显的分界线。IT专业人员需要了解OT和设备，例如PLC、HMI、VFD以及监控和数据采集（SCADA）软件。OT专业人员需要了解网络、安全性，并能够配置使用防火墙和路由器等网络安全设备。这两个协作部门需要扩展他们各自的技能，以调整IT安全项目模型，以便在OT中适用，同时考虑到其安全优先级和风险偏好及固有的差异，对团队进行技能培训，最终将引导他们正确地制定OT安全流程、策略和人员计划以及更好地使用OT/ICS相关的专业安全产品。

虽然将IT和OT融合在一起会带来许多技术、文化和结构性挑战，但长期来看，数字化发展的利益远远超过开始时可能出现的任何困难。

参考文献：

[1] 张翔宇，路来顺．工业控制系统网络安全分析与研究[J]．网络空间安全，2019,10(05):114-120.

[2] 王红岗．工业控制系统网络安全分析与管理策略探究[J]．化工管理，2020(11):93-94.

[3] The International Society of Automation.Security for industrial automation and control systems, Part 2-3: Patch management in the IACS environment(ISA TR62443-2-3)[S]. 2015-07-01.

[4] 国家质量监督检验检疫总局，国家标准化管理委员会．工业自动化和控制系统网络安全 集散控制系统(DCS) 第1部分(GB/T 33009.1-2016)[S].2016-10-13.

[5] National Institute Of Standards And Technology.Guide to Operational Technology (OT) Security: NIST Requests Comments on Draft SP 800-82r3[S].2022-04-26.