工业控制系统信息安全风险评估体系研究

张达超*
中航西安飞机工业集团股份有限公司 陕西 西安 710089

摘 要：与传统的信息系统不同，工业控制系统是网络空间和物理空间的重要纽带，一旦发生网络安全事件，不仅造成信息损坏和丢失，还可能造成人员生命健康损害、环境破坏等物理的实际损害，因此会造成更严重的经济损失和社会影响。

关键词：工业控制系统；信息安全；风险评估
DOI：https://doi.org/10.37155/2717-5170-0306-9

前言

工业控制系统（ICS）是指用于操作、控制、辅助自动化工业生产过程的设备、系统、网络以及控制器的集合，包括数据监控与采集系统（SCADA）、分布式控制系统（DCS）、可编程逻辑控制器（PLC）、智能终端、人机交互接口（HMI）等系统。工业控制系统关系着工厂生产、电网、能源、水处理等国家关键基础设施的运行，在国民经济中具有作用。近年来，在工业企业转型升级、工业4.0、工业互联网等技术浪潮的推动下，工业控制系统的对外连接性日益增加，在提高效率、促进创新的同时，也显著增加了工业控制系统所面临的网络安全威胁。

1 风险分析

（1）企业工控系统网络为开放式设计，可以与任意第三方智能化设备和上级调度管理网络对接，该系统网络与其它系统网络之间存在大量的接口，但不同的系统网络之间缺少完善的数据及网络隔离措施，从而导致一旦有某种威胁进入某系统网络，将会在整个工控系统网络内快速扩散。

（2）出于对使用习惯和应用程序开发的便利性以及程序运行的稳定性和兼容性等各方面因素的考虑，工控系统工作站的人机交互软件通常采用微软的windows系列操作系统（其中含大量老旧操作系统）。为保持系统的稳定运行，现场工程师在工控系统软件平台运行后不会对操作系统安装任何补丁，导致工控系统终端设备的操作系统存在大量漏洞且难以及时处理，进而导致工控系统网络存在巨大的安全风险[1]。

（3）目前很多工控协议已经演化或扩展为在通用计算机和通用操作系统上实现，并在以太网甚至互联网上运行，以满足发展需要，这就将一些有漏洞的协议暴露给攻击者。其中，工控系统网络使用的TCP／IP（传输控制协议／因特网互联协议）诞生本身就不是立足于安全，而是主要解决网络间的通信问题。随着TCP／IP的发展，很多方面被一些不法分子利用，也暴露出TCP／IP自身大量安全问题。TCP／IP存在的不足导致基于TCP／IP的工控协议存在较大风险，一类是由于主机依赖IP源地址来寻求认证，另一类则是利用了网络中的某些控制协议，尤其是路由协议。所以TCP／IP自身的安全问题不可避免地会影响到运行于其上的工控协议，因此需要实施动态安全防护。

（4）工控系统操作人员的技术水平和安全意识差别较大，容易发生越权访问和违规操作，给工控系统网络埋下极大的安全隐患。事实上，国内工控系统网络相对封闭的环境也使得来自工控系统内部人员在应用系统层面的误操作和越权操作成为其所面临的主要安全风险。由于当前工控系统网络中管理终端缺乏技术措施，对U盘和光盘的使用不能进行有效管理，导致外设的无序使用，进而引发的安全事件时有发生。例如，一个没有到达一定安全基线的笔记本电脑接入工控系统网络，就会对其造成很大的安全威胁。

（5）由于工控系统网络不像互联网或与传统企业IT网络那样备受黑客的关注，在2010年“震网”事件发生之前很少有黑客攻击工控系统网络的事件发生，工控系统网络在设计时也多考虑系统的可用性，因此对安全性问题的考虑普遍不足，更没有制订完善的工控系统网络安全政策，造成操作人员安全意识淡薄。随着工控系统网络在国计民生中重

*通讯作者：张达超，1989.05，汉，男，陕西宝鸡，中航西安飞机工业集团股份有限公司，技术员，工程师，本科，研究方向：信息安全。

要性的日益增长以及IT通用协议和系统在工控系统网络的普遍应用，操作人员淡薄的安全意识将成为其安全风险的一个重要因素[2]。

（6）APT（高级可持续性威胁）的攻击目标更为明确，攻击时会利用最新的0—day漏洞，强调攻击技术的精心组合与攻击者之间的协同，而且是不达目的不罢休的持久性攻击。针对这种APT攻击，现有的安全防护手段均显得无力，故需要整合各种安全技术，将防御手段进行组织化和体系化，形成完善的安全防御体系，才能在面临APT攻击时将损失降到最低。

（7）工控系统最早和企业管理系统是隔离的，但近年来为了实现实时的数据采集和生产控制，满足“两化融合”的需求和管理的方便，才使得工控系统和企业管理系统可以直接进行通信。企业管理系统一般直接连接Internet，因此工控系统网络接入的范围不仅扩展到了企业网，而且面临着来自Internet的安全威胁。

2 工业控制系统风险评估框架

2.1 摸清当前安全状态

ISO27001：该标准在风险评估方法下提供了指导方针，以清楚地定义IT系统的当前状态，确定安全管理体系相关方，资产所有者的角色、责任的定义。IEC62443：该标准增强了当前的状态定义。使用“区域”和“管道”的概念，分割和隔离控制系统中各种子系统的方法。区域是指基于关键性和后果等因素共享共同安全需求的一组逻辑或物理资产。“管道”是应用于特定通信过程的特定区域，提供使两个区域能够安全通信的安全功能，不同区域之间的所有通信必须通过管道进行。NIST：该研究所提供了定义ICS系统当前状态的相关工具。ENISA：为当前状态定义提供了“外部和内部环境定义”的附加方法[3]。

2.2 设定安全期望目标

ISO27001：与定义当前状态步骤相同，ISO状态定义方法可用于定义要实现的安全目标状态。IEC62443：标准引入“基本要求”和“安全级别”，从ICS的角度对网络安全定义提供了增强。NIST：该研究所提供了“网络安全核心模型”，这是一个指导方针，以解决ICS系统上的所有网络安全目标。

2.3 安全差距分析

IEC62443：在GAP分析中使用了4个保护层级的安全级别定义方法。NIST：通过漏洞识别实践来解决差距，该方法（SP800-30）由研究机构提供，可作为额外用于一致性目标差距分类的方法。

2.4 安全威胁情景收集

通过完整的威胁情景描述，为各组织提供明确的威胁说明。当前和目标状态模型提供了一种简化的方法来识别和解决它们之间的差距。把这两种模式细分为更简单的实体，并可进行比较，获得它们的细分差距，便于实施主动的事件管理方案，方案侧重于风险的威胁部分。非简单的将这些威胁视为单一事件，当其与其它不同威胁结合起来后会大大提高穿透IACS（工业自动化控制系统)的攻击成功率。创建威胁场景脚本就是研究可能影响IACS的威胁场景的过程，需要对各种威胁场景脚本进行详细的汇总收集，作为工业网络风险评估的主要精力投入。NIST：NIST为识别威胁提供了大量信息，列出了美国的历史上曾经面临的网络安全威胁。ENISA：ENISA威胁视图（ETL）概述了威胁，以及当前威胁的新趋势。

2.5 安全风险分析

（1）风险映射表。一是识别每个风险；二是简要定义每个风险；三是指出受风险影响的工业自动化控制区域；四是显示风险的影响程度。这可以用健康和安全来表达，也可以用经济的方式来表达影响。五是显示风险的可能性。在与IACS所有者协商一致的情况下，必须估计每种风险发生的概率；六是确定风险利益相关者。

（2）风险影响。风险影响的定义可以用两种不同的方式来处理，采用定量的方法客观的确定风险优先级和确定补救顺序。定量方法的问题是，将风险的影响准确地转化为数值表达式并不容易，有时可能会导致网络安全问题不仅得不到处理，还会变得模糊。为了避免上面问题，可以使用定性的方法。定性方法意味着要与管理层和资产所有者达成共识，并将不断持续改进影响风险水平定义的过程。即便达到可接受的风险水平，过程也不会停止，仍需要对当前风险和新风险进行持续监控。为达到最佳实践水平，可混合使用定量法来确定风险的处理顺序，定性法来处理所需的控制。

（3）风险可能性。风险可能性通常使用定量方法，因为不可能对未来事件建立准确的定性预测。使用定量的方法

可以利用历史数据来帮助促进未来的概率预测。

（4）风险优先级。一是需要尽快处理的风险（红色）；二是可加入中期处理计划的风险（橙色）；三是可纳入长期处理计划残余风险组（绿色）。ISO27001：该标准提供了普世性的IT系统中执行风险分析的方法。IEC62443：该标准将ISO27001提供的方法推向ICS应用。

2.6 安全风险缓解

IEC62443按照威胁的类别将补救分成了“人-流程-技术”三角要素组。人员：包括开发、跟踪、实施、执行和管理ICS网络安全计划所有管理人员、工作人员、承包商和其他人员。流程：包括与ICS安全管理系统相关的策略、程序、表单、业务流程和其他文档。技术：包括所有现有的技术安全控制，以维护系统的可用性、完整性和保密性。

2.7 安全持续评估

风险评估工作不是特定时间的项目，而是一个持续的过程。伴随着新技术的发展与应用会出现新的脆弱性和威胁，例如随着系统配置的不断变更，也会因误配引入威胁。我们需要一种新的方法来维持安全收益，将风险控制在可接受的水平。框架源于ISO27001和IEC62443，包括重新评估风险的规定并采取纠正措施，减少安全能力随时间下降的趋势，持续保持安全态势。

3 结束语

本文所探索的网络安全框架被定义为一种能够处理不同系统类型（IT、OT）的评估，并具有潜在的风险偏好定制能力。使用来自NIST、ENISA等组织的信息源来维护和更新这种不断演变的威胁和对策模型意味着企业可以保护他们的IT和OT网络免受实际的网络安全威胁。

参考文献：

[1]安高峰,朱长明,雷晓锋,等.我国工业控制系统信息安全政策和标准体系架构研究[J].信息安全研究,2018(10):33-34.

[2]安高峰,朱长明,雷晓锋,等我国工业控制系统信息安全政策和标准体系架构研究[J].信息安全研究2018(1):33-34.

[3]范科峰,周睿康,李琳.工业控制系统信息安全标准体系研究[J].信息技术与标准化,2016(06):17-21.