控制与决策
Control and Decision

面向工业控制系统全生命周期的脆弱性多维协同分析

李欣格, 胡晓娅, 周纯杰, 尹泉

引用本文:
李欣格,胡晓娅,周纯杰,尹泉. 面向工业控制系统全生命周期的脆弱性多维协同分析[J]. 控制与决策, 2022, 37(11): 2827–2838.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2021.0618

面向工业控制系统全生命周期的脆弱性多维协同分析

李欣格[1,2], 胡晓娅[1,2†], 周纯杰[1,2], 尹 泉[1]

(1. 华中科技大学 人工智能与自动化学院，武汉 430070；2. 华中科技大学 网络空间安全学院，武汉 430070)

摘 要: 工业互联网背景下,工业控制系统面临攻击防不住、脆弱性易暴露的安全挑战,要保障系统安全稳定运行,首先需要深入探究引发工业控制系统故障的原因,明确系统脆弱性机理. 针对当前单点或局部脆弱性分析的局限性,面向工业控制系统全生命周期安全需求及特征,提出脆弱性多维协同分析框架,通过模型驱动的系统静态、动态脆弱性分析以及多域融合评估,剖析和挖掘系统脆弱点及其关联渗透过程,生成系统脆弱性知识. 所提出框架首次明确脆弱性含义,同时全生命周期需求覆盖以及一体化架构特性有助于实现系统全局脆弱性机理揭示.

关键词: 工业控制系统；脆弱性；多维协同分析；全生命周期

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2021.0618

引用格式: 李欣格, 胡晓娅, 周纯杰, 等. 面向工业控制系统全生命周期的脆弱性多维协同分析 [J]. 控制与决策, 2022, 37(11): 2827-2838.

Multi-dimensional collaborative analysis of vulnerability for full-lifecycle of industrial control systems

LI Xin-ge[1,2], *HU Xiao-ya*[1,2†], *ZHOU Chun-jie*[1,2], *YIN Quan*[1]

(1. School of Artificial Intelligence and Automation，Huazhong University of Sicience and Technology，Wuhan 430070，China；2. School of Cyber Science and Engineering，Huazhong University of Sicience and Technology，Wuhan 430070，China)

Abstract: In the context of industrial internet, industrial control systems are faced with the challenges of attack intrusion and vulnerability exposure. In order to ensure the safe and stable operation of industrial control systems, it is neccessary to explore the cause of system failures and clarify potential vulnerabilities. In this paper, based on the full-lifecycle security requirements and characteristics of industrial control systems, a multi-dimensional collaborative vulnerability analysis framework is proposed. With model-driven system static and dynamic vulnerability analysis, the system vulnerability knowledge is then generated. Meanwhile, the proposed framework firstly clarifies the meaning of vulnerability in industrial control systems, and the full-lifecycle coverage and integrated architectural features are benificial to realize the global vulnerability disclosure of industrial control systems.

Keywords: industrial control systems；vulnerability；multi-dimensional collaborative analysis；full-lifecycle

0 引 言

工业控制系统(industrial control system, ICS)作为国家关键基础设施的重要基石,广泛应用于石化、电力等核心领域. 随着工业互联网、工业4.0、智能制造等功能需求迅速提升,时间敏感网络(time sensitive networking, TSN)、5G等新一代信息通信技术推进,工业控制系统信息域与物理域深度耦合交互,信息化程度越来越高,使得其开放性和互联性达到了前所未有的高度. 工业控制系统作为关键领域的重要支撑,一旦出现问题将造成不可预估的损害. 然而,日渐开放的工业控制系统使得原有较为封闭的脆弱性逐渐被暴露在外部网络攻击之下,从而不仅扩大了攻击面,也降低了外部攻击入侵门槛[1-4]. 因此,工业控制系统的信息安全问题不容忽视.

然而,网络安全攻击日益智能化、复杂多样化,如APT (advanced persistent threat)攻击,使得攻击具备避

收稿日期: 2020-04-12；**录用日期:** 2021-07-29.
基金项目: 国家重点研发计划项目(2020YFB1708601)；国家自然科学基金项目(61873103, 61433006).
责任编委: 林崇.
†通讯作者. E-mail: huxy@hust.edu.cn.

开系统入侵检测的能力. 另外,现有安全防护措施往往仅聚焦系统单点或局部区域,缺乏全面系统的安全防御. 因此,目前安全防护下的系统整体安全性难以得到保证,提升系统或网络弹性,增强攻击抵御能力的安全思想逐渐显现. 2018年,美国防部发布《国防部网络战略》并强调部署和提高可扩展、适应性强的多样化网络能力. 同年,美国《国家网络战略》提出增强网络稳定性,对网络空间不可接受行为进行归因和威慑的发展目标. 不仅如此,我国互联网信息办公室及相关部门就《加强工业互联网安全工作的指导意见》政策解读时指出“安全的本质是没有不可接受的风险”. 这些战略方针和专家意见都表明无论是系统或者网络,攻击威胁是防不住的,网络自身防御能力应得到增强. 工业控制系统脆弱性作为外来攻击的切入点,是系统全生命周期安全运行的关键因素. 面对无法避免的攻击,分析系统脆弱性和提高攻击抵御能力才是更切实的选择. 因此,为了应对攻击防不住、脆弱性易暴露等严峻安全挑战,开展系统脆弱性机理揭示以增强系统安全韧性的研究刻不容缓. 工业控制系统必须梳理系统潜在安全隐患,明确系统可能遭受危害的原因,评估系统攻击抵御能力.

当前工业控制系统中针对脆弱性机理的研究较为分散,且现有工作更多关注静态或动态的局部安全问题,缺乏对全局脆弱性的考虑,因此需要采取整体性的方法综合考量系统不同阶段安全需求以及安全问题,挖掘和剖析全局脆弱性特征. 本文以多维度揭示系统脆弱性机理为目标,针对工业控制系统攻击多样性和不可预见性特征,提出面向工业控制全生命周期的脆弱性多维协同分析框架. 首先,总结现有脆弱性分析研究和理论方法,依据全生命周期不同阶段的安全需求与特征,设计全局系统脆弱性分析基本框架;然后,针对性提出系统全生命周期各阶段脆弱性分析思路、关键技术的实现方案以及主要模型设计,并结合具体案例阐述方案执行过程;最后,进一步指明了脆弱性多维协同分析框架的前景应用.

1 工业控制系统脆弱性机理研究进展

1.1 工业控制系统脆弱性含义

工业控制系统的外来攻击威胁和内部潜在安全隐患不仅关系着系统脆弱性程度,同时也影响系统面临的信息安全风险. 风险作为系统面临安全威胁或损失伤害可能性的描述,重视安全事件不确定性和后果严重性. 目前,工业控制系统信息安全风险评估分为定性和定量评估两大类. 定性评估利用安全知识、经验对系统的风险状况进行整体性评估,这种方法最终大多定性分析风险等级且实现系统风险的粗略描述,适用于对风险评估精度较低的场景. 定量评估主要使用概率分析等数学方法量化风险值,其精确结果有助于专家制定合理的防护策略[5-6].

脆弱性注重系统潜在安全缺陷表征,反映抵御攻击的能力. 目前脆弱性分析研究集中在协议和系统对象两方面,其中工业控制系统协议脆弱性研究工作分为静态和动态分析两种[7-8],重点在于挖掘协议实现过程中的安全漏洞. 然而,工业控制系统脆弱性不仅包括固有安全漏洞,还涵盖系统动态运行的薄弱环节. 目前,面向系统对象脆弱性研究可以分为定性和定量分析两大类,主要针对攻击对象的局部或全局损失进行研究.

综上,工业控制系统风险评估和脆弱性分析虽然都遵循“识别-攻击-评估”流程体系,但关注角度有所差异. 风险评估更多从攻击威胁角度考虑攻击可行性及危害程度,关注系统可能的危害结果. 脆弱性从全生命周期角度考虑攻击对系统内部运行或组件产生的损害影响,注重系统安全状态. 因此,工业控制系统的脆弱性是引发系统信息安全风险的诱因,开展工业控制系统脆弱性分析是识别安全风险危害程度的必由之路. 目前,工业控制系统脆弱性的描述多视为对静态脆弱点或风险评估中攻击收益的衡量. 除了攻击属性外,系统脆弱性还与网络拓扑、通信协议以及其他特性相关. 所以,工业控制系统的脆弱性是引起某一威胁事件发生的诱因危害性描述,是系统静态脆弱点(漏洞)和动态薄弱运行环节的组合. 而脆弱性分析是为了确定这一诱因影响程度以及系统对象损失程度的推测.

总而言之,仅考虑风险评估下攻击收益来反映系统脆弱性程度具有片面性,难以覆盖系统全局的脆弱性特征. 针对工业控制系统的脆弱性分析必须聚焦系统全生命周期安全状态,重点关注攻击对系统运行的危害影响和全局综合评估,通过建立一个系统性的分析体系架构来揭示系统全局脆弱性.

1.2 研究现状

1.2.1 定性分析

系统脆弱性定性分析利用安全知识、专家经验等分析概述系统可能存在的脆弱性. 在相关标准指南方面,有专家针对工业控制系统潜在脆弱性进行了总结. 例如,《工业控制系统安全控制应用指南》从策略和规程、网络、系统平台3个方面概述系统脆弱性;

《工业控制系统信息安全防护能力评估方法》将系统脆弱性定义为系统存在的固有的、静态安全漏洞,并指明可通过脆弱性扫描工具定性判别. 然而,这些标准指南更侧重对系统静态潜在安全漏洞的定性考察,缺乏通过科学理论方法明确系统内部脆弱环节以及关联危害程度.

与此同时，相关理论研究虽然阐述了系统潜在脆弱性,但系统内部运行交互特征使得脆弱点或环节之间具有较强的关联性,极易被攻击者利用或控制[9]. 如攻击者可以利用系统平台无认证特性进行非授权访问,从而修改相关配置信息并引发安全事件发生. 因此,必须从整体、关联的角度分析工业控制系统动态运行下的脆弱性程度.

1.2.2　定量分析

定量分析聚焦关联脆弱性研究,通过理论方法精确量化系统脆弱程度. 具体归纳为以下两方面:

1) 模型驱动分析.

模型驱动分析主要包括树结构模型、图模型和系统模型3类. 基于树结构的分析方法以攻击树和故障树为主[10-11]. 两种方法虽然分别从攻击结果和攻击过程表征攻击,但是其局限于单次攻击识别,缺乏并发攻击的建模表达能力.

攻击图是图模型分析主流方法,相关工作利用这种方法评估系统恶意攻击下的生存能力[12-13]. 该方法充分考虑了系统拓扑信息,将利用脆弱性过程表征为多个攻击序列集合,较好地覆盖了所有攻击可能性. 另外,级联故障图多应用于电力信息物理系统脆弱性评估,通过紧密结合拓扑状态及复杂网络理论,以链路失效为攻击目标评估系统物理运行特性变化,但缺乏对攻击生成过程的描述[14].

面向系统模型的脆弱性分析重点针对系统拓扑、资产需求等搭建系统环境模型,开展攻击安全研究. Petri网是系统建模主流的方法,文献[15]结合资产知识构建基于Petri网的系统资产模型,并通过攻击建模分析资产损失程度,量化危害后果;文献[16]构建基于随机Petri网的系统模型,并建立攻击模型评估信息物理系统攻防作用下的生存能力.

与模型驱动相比,数据驱动方法依据海量时空运行数据分布特性,通过不断反馈优化满足目标需求. 该方法的特征是数据必须满足总量庞大、类别全面、内容细化等需求. 然而,工业控制系统中安全事件数据相较于正常运行数据非常稀缺,这种非均衡特征的数据驱动难以保证系统内部的客观表达. 总体而言,模型驱动方法聚焦目标具体功能而并不关心其工作机理,这种高层次抽象表达特征能有效反映系统各节点间的交互耦合特征,有助于分析工业控制系统非运行状态下的固有脆弱点.

2) 指标评价分析.

脆弱性指标是攻击威胁作用下系统可生存能力的重要度量,其指标量化可以分为物理安全损失与信息安全脆弱性评估两大类.

物理安全损失评估基于系统环境信息、攻击属性知识,利用数学理论方法评估系统韧性能力. Wei等[14]基于系统和攻击模型,以复杂网络统计特性指标作为系统脆弱性评价依据分析系统运行或物理损失;类似地,文献[17-18]基于电网拓扑,通过复杂网络无标度特性或相关指标讨论系统物理运行层面的脆弱程度.

信息安全脆弱性评估主要针对系统信息域风险,统计学习漏洞库的漏洞属性实现综合评价. 例如,Anikin[19]针对CVSS中漏洞属性采用智能算法进行分类计算,综合评估系统脆弱性. 不过,面向工业控制系统信息域和物理域高度交互耦合特性,局部信息域脆弱性指标难以反映系统整体状况.

总而言之,当前针对工业控制系统的脆弱性分析主要采用定量分析方法,具体包括两种典型思路:一是利用攻击树、攻击图、Petri网等方法或相关建模语言构建系统对象或攻击者模型,分析系统遭受攻击的损失程度,这类方法也是主流研究方向;二是基于系统信息层面,利用公开漏洞库的漏洞知识和属性量化描述,采用层次分析、模糊理论等方法处理脆弱性指标,实现系统脆弱性的统一量化. 第1种思路注重系统对象和攻击过程的描述,清晰表征系统脆弱性渗透;第2种侧重对攻击结果评价,缺乏安全事件发生的潜在原因研究. 由于工业控制系统中结构愈加开放,外来攻击可能渗透作用于系统信息、物理空间对象,极易造成信息或功能安全事故. 因此,工业控制系统脆弱性分析需要充分总结上述两种思路优势实现全局角度的系统脆弱性机理揭示.

综上所述,现有研究缺乏从系统工程角度充分挖掘工业控制系统内部特性与外部攻击属性对系统脆弱程度的影响,急需建立一个系统级脆弱性理论分析框架,以多维度、多层次支持系统安全性分析为目标,以模型驱动、多域指标评价为核心研究方法有效揭示全局脆弱性机理,评估系统可生存能力.

2 工业控制系统脆弱性多维协同分析框架

2.1 设计思路

工业控制系统全生命周期不同阶段的安全隐患及脆弱环节是安全威胁的攻击目标及对象. 同时,外来攻击的渗透传播是破坏系统安全运行的诱因. 另外,系统脆弱性指标的精准量化评估是其自身韧性表现的重要支撑. 因此,为了揭示系统脆弱性机理特征,所提出框架将针对工业控制系统对,通过基于模型驱动的安全分析方法和指标评价方法进行系统多域脆弱性融合评估.

明确基于全生命周期的系统对象是需求. 工业控制系统中丰富的设备及复杂的通信控制机制存在固有的安全缺陷,这些要素间强关联作用极易引发系统多环节的安全隐患联动. 因此,系统脆弱性分析需要基于全生命周期开展设计阶段的固有漏洞挖掘、运行阶段的脆弱点关联渗透分析、维护阶段的安全管理优化完善,实现系统全局脆弱性机理揭示.

研究攻击威胁传播是手段. 为了更客观地开展系统脆弱性机理研究,首先需要识别能够利用系统脆弱性的攻击类型,依据系统的漏洞、拓扑结构以及权限控制等信息,还原攻击入侵场景,理清攻击传播过程并反向识别工业控制系统关键薄弱环节. 因此,攻击视角下的脆弱性分析将从“点-线-面”维度依次讨论原子攻击、攻击路径和攻击面关键属性.

评估系统层面脆弱性程度是目标. 工业控制系统的脆弱性是系统信息、物理域的不同安全状态的综合表征. 因此,需要针对全生命周期系统不同阶段特性多维评估面向攻击作用后的系统安全状态,明确系统安全韧性. 这里,脆弱性分析评估将从静态、动态和多域融合3个维度确定不同阶段的安全属性量化指标,综合度量系统脆弱性程度.

2.2 框架介绍

工业控制系统的脆弱性分析框架从系统对象解析、攻击传播分析和脆弱性指标评估3个视角构建,具体如图1所示. 其中,系统对象解析视角涵盖了系统全生命周期中设计、运行和维护3个关键阶段,根据阶段特性及分析目标,依次讨论系统不同阶段的脆弱性程度;攻击传播分析视角包括原子攻击识别与筛选、面向传播路径行为的有效攻击建模和基于攻击属性计算的攻击面分析3大环节,还原不同攻击入侵场景;脆弱性指标评估视角将围绕全生命周期不同阶段安全的需求,充分考虑静态结构、动态运行和多域融合关联过程的脆弱性指标性能.

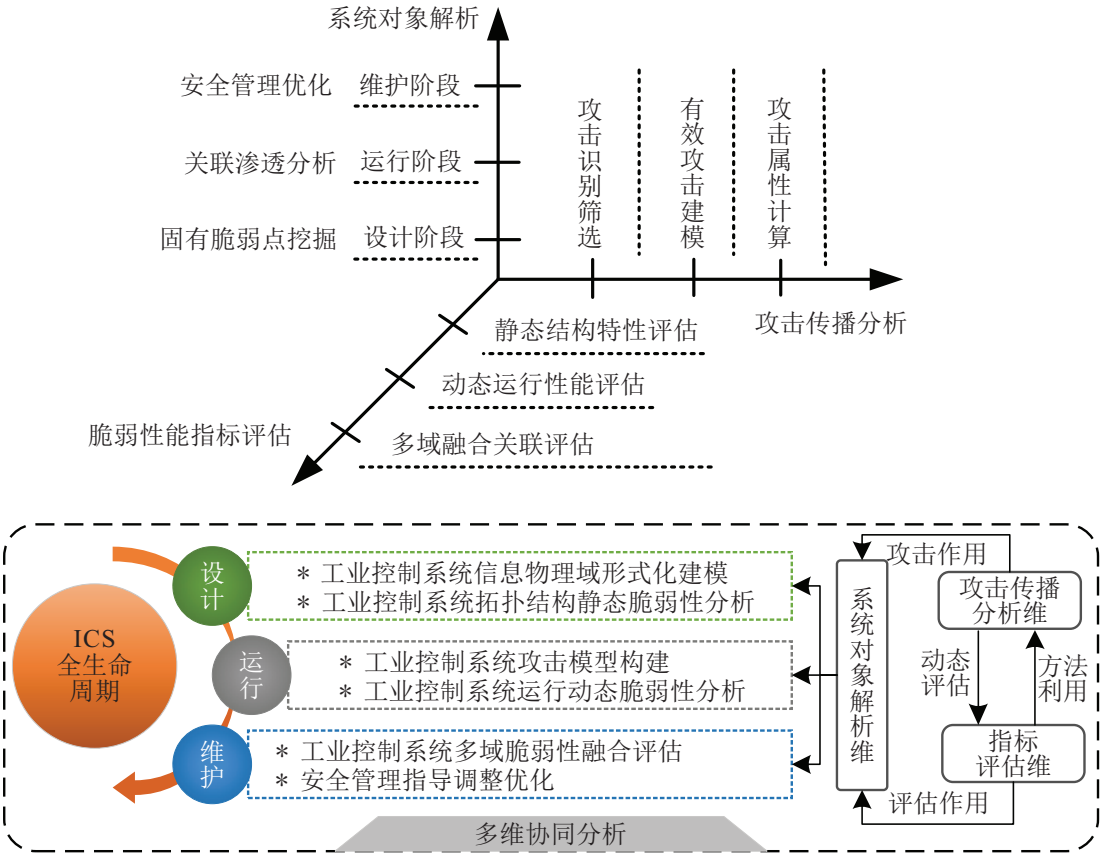

图1 工业控制系统脆弱性多维协同分析基本框架

在此基础上, 以系统对象解析维为核心, 攻击传播和指标评估维协同辅助, 形成多维分析研究体系. 其中, 系统对象分别是攻击传播分析和脆弱性指标评估的攻击对象及评估对象, 且攻击传播和指标评估维度理论方法与技术路线辅助实现对象解析维度三阶段目标. 进一步地, 针对系统设计阶段静态特征, 基于系统模型利用指标评估维的静态结构特性评估方法实现固有脆弱点挖掘目标, 为运行和维护阶段提供理论模型和静态脆弱性知识; 针对运行阶段动态特征, 通过攻击传播分析维的内容方法辅助实现指标评估为的动态脆弱性评估, 达到关联渗透分析的目的, 为维护阶段提供动态脆弱性知识; 依据维护阶段系统综合脆弱性考量, 结合固有安全漏洞和攻击传播结果, 采用多域关联评估方法探究系统全局脆弱性, 为安全管理优化提供指导.

3　脆弱性多维协同分析实现方案

基于上述工业控制系统脆弱性多维协同分析框架, 结合已有研究工作和不同理论方法特性, 针对系统不同阶段对象明确脆弱性分析的具体方法, 最终形成综合的脆弱性分析实现方案, 具体如图 2 所示.

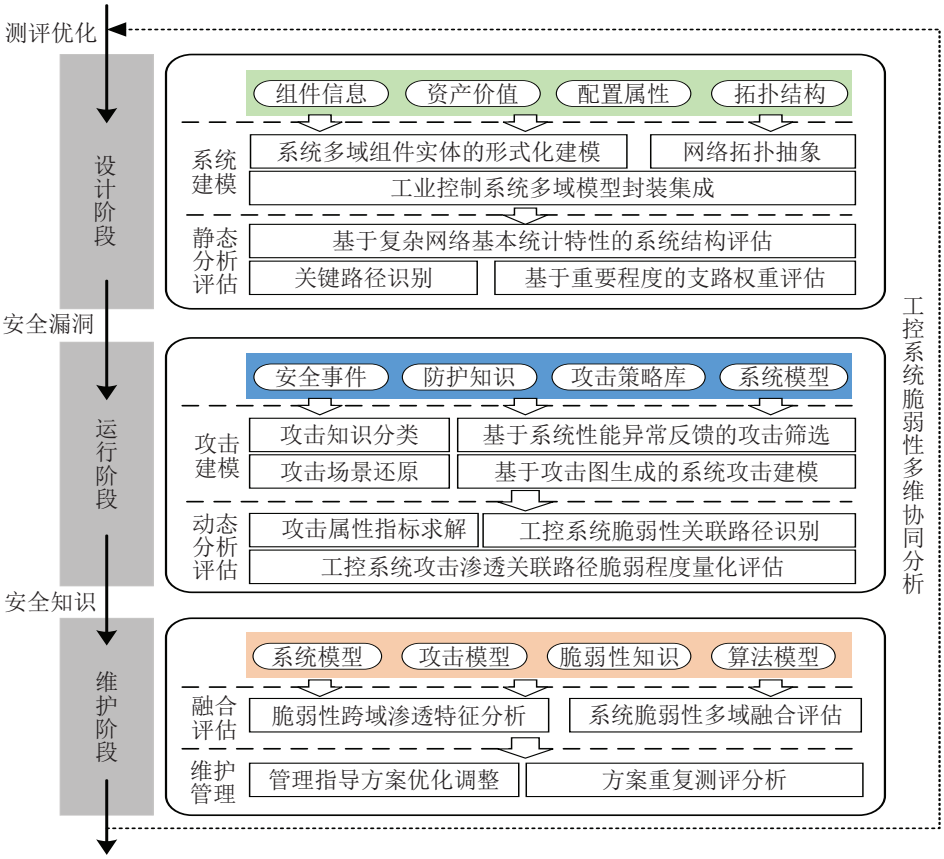

图 2　具体实现方案

3.1　方案介绍

1) 设计阶段.

该阶段需要针对系统功能、运行等安全需求, 分析系统非运行状态的固有脆弱性特征. 因此, 该阶段脆弱性分析首先需进行系统形式化模型构建, 实现工业场景的真实映射. 由于拓扑结构是开展系统脆弱性研究的先决条件[20], 在构建模型的基础上针对系统组件和结构特征等开展静态脆弱性分析, 挖掘固有脆弱点.

面向系统的模型构建需针对信息域计算过程、物理域运行事件和网络通信进行信息获取和分析, 包括拓扑结构、资产知识和配置属性等, 进而采用 Petri 网形式化描述系统运行过程. 这里, 通过提取物理域和信息域的系统属性, 模拟计算和行为操作, 定义信息物理状态和动作, 建立系统多域组件实体模型. 与此同时, 利用图论知识抽象系统拓扑结构, 并进一步关联系统组件实体模型.

通过系统模型形式化表达能够清晰反映攻击入侵前后系统行为演化和状态变化, 包括错误控制指令扰乱控制器正常运行等功能失效状态和信息系统非法入侵等信息安全状态. 然而, 工业控制系统固有脆弱点, 如组件漏洞、拓扑薄弱特征是系统脆弱性的关键点, 使攻击者有了可趁之机. 因此, 设计阶段需要开展系统静态脆弱性分析与评估. 系统静态安全属

性特征不仅由ICS组件漏洞反映,更多体现在通信拓扑结构方面. 本框架重点探究工业控制系统拓扑结构的静态脆弱性. 在系统模型基础上抽象拓扑,利用复杂网络知识开展静态脆弱性分析. 例如统计工业控制系统安全网关的度分布,分析其在系统的关键程度;统计现场控制层物理节点的聚类系数,评估节点紧密耦合程度等. 通过拓扑脆弱性分析方法,可明确攻击利用某一脆弱点进行传播的可能性及影响,从而筛选和识别系统关键传输路径.

2) 运行阶段.

由于系统复杂化和攻击多样化特点,静态脆弱性分析难以反映系统脆弱点间可能的动态关联关系. 而攻击者利用脆弱性关联特征形成的攻击序列将加速危害系统安全运行. 因此,需要在攻击传播基础上识别系统脆弱性联动关系. 运行阶段的脆弱性分析重点探究攻击状态下系统动态脆弱性渗透关联过程,探究薄弱运行环节,主要包括攻击建模和动态分析评估两方面.

攻击建模环节针对攻击未知性和不可预见性,首先判别未知攻击的有效性,明确具体建模对象. 这里,结合历史安全事件和信息安全防护指南等对攻击类型分类识别,包括攻击者远程劫持、非法登录监控系统的信息攻击,试图引发控制器等内部功能模块失效的物理攻击. 接着还原攻击入侵场景,实现攻击模拟注入. 在此基础上,根据系统运行性能是否异常的反馈结果筛选有效攻击,例如判断现场系统生产速率是否偏离期望值、监控系统是否被非法用户入侵等. 若系统运行在安全范围内,则表明系统可以抵抗该攻击,攻击无效. 若运行异常,则表明该攻击为有效攻击. 确定有效攻击后,根据系统异常反馈和入侵证据确定攻击起点和目标,结合系统拓扑、攻击策略库知识以及攻击图生成技术搜索满足所有条件的攻击路径,自动化生成攻击图模型,为分析系统内部脆弱性联系、明确攻击策略提供模型支持.

动态分析评估负责通过攻击模拟求解攻击属性指标,包括攻击成功概率、攻击路径、攻击成本和攻击收益等. 其中,攻击成功概率将基于贝叶斯网络框架和CVSS提供的相关指标进行推理估计;攻击路径通过生成的攻击图可视化得到;攻击成本和攻击收益则需要考虑系统资产价值知识、系统性能牺牲程度以及危害程度计算得到.

3) 维护阶段.

工业控制系统设计和运行阶段暴露出的潜在安全隐患,不仅需要相应的安全策略防御,还需要定期维护检查. 另外,由于长期攻击作用累积的安全缺陷,系统也应及时调整优化. 因此,维护阶段需要针对系统局部脆弱性进行多域融合分析与评估,根据评估结果拟定安全管理指导方案,针对性完善系统安全管理与维护.

目前,工业控制系统信息域(Cyber, C)和物理域(Physical, P)攻击相互渗透影响引发的安全问题尚不明确,且攻击作用下的信息物理域间脆弱性渗透关联影响存在差异(C2P和P2C). 其中C2P攻击通过网络渗透、攻击者权限提升、破坏系统功能、引发危险事件、造成物理损害的攻击步骤实现信息域到物理域的攻击传播;P2C攻击通过破坏现场物理组件功能上传有偏差的状态信息,误导信息系统做出正确指令. 因此,需要针对不同攻击下的局部脆弱性特征,探究系统多域脆弱性融合评估. 多域融合的前提是明确系统信息域和物理域间关联关系. 框架首先充分考虑系统拓扑关系,利用相关方法探究系统多域脆弱性间渗透传播过程以明确脆弱性跨域渗透特点;在此基础上结合安全防护知识,利用模糊理论消除不同脆弱性指标间的差异性并进行指标分类;最后,根据多域渗透特征以及脆弱性指标,利用层次分析法对信息物理域的脆弱性进行融合评估,从而调整ICS安全管理指导方案使系统达到最佳运行状态.

3.2 脆弱性分析的主要模型

脆弱性分析实现方案不仅要明确系统对象拓扑结构、安全约束、行为机制和多域间通信交互作用等,还需分析攻击切入手段和系统受损程度. 因此,脆弱性分析实现方案需要系统模型、攻击模型和脆弱性评估模型的共同支持以形成系统脆弱性综合分析模型. 工业信息物理融合系统是传统工业控制系统的升级,也是系统主流研究对象. 本节首先结合脆弱性分析支撑技术,依次阐述基于Petri网的系统形式化模型和基于攻击图生成的攻击模型构建方法,进而针对信息域和物理域耦合性挑战,提出多域脆弱性融合评估模型.

3.2.1 工业控制系统形式化模型

系统形式化建模通过描述系统传感器、控制器和执行器等组件的功能和交互行为,表征系统动态运行过程. 框架提出基于面向对象Petri网的系统形式化定义,攻破系统多域复杂关联难以表达的难题.

定义1 (系统SOPN) 形式化描述组件实体、网

络实体等基本行为特性,并定义系统三元组

$$\text{SOPN} = \{\text{Object}, \text{Network}, \Sigma\}. \tag{1}$$

其中: $\text{Object} = (\text{Ob}_1, \text{Ob}_2, \ldots, \text{Ob}_i)$ 为系统组件实体,包括生产过程单元、执行单元和控制中心单元; $\text{Network} = (\text{channel}_{12}, \ldots, \text{channel}_{ij})$ 表示系统网络实体,描述不同组件间的通信链路; Σ 为颜色集,用于定义系统数据类型、变量和函数.

定义 2 (组件实体 Object)　表征系统生产、执行和控制中心的行为演化过程,任一实体 Ob_i 用八元组表示为

$$\text{Ob}_i = (\text{SP}, \text{IP}, \text{OP}, T, I, O, C, \text{CM}), \quad i \in [1, 2, \ldots, n]. \tag{2}$$

其中: Ob_i 为系统第 i 个对象; $\text{SP} = (\text{sp}_1, \ldots, \text{sp}_{N(\text{SP})})$ 为对象实体的状态库所有限集合; $\text{IP} = (\text{ip}_1, \text{ip}_2, \ldots, \text{ip}_{N(\text{IP})})$ 为输入信息库所有限集合; $\text{OP} = (\text{op}_1, \text{op}_2, \ldots, \text{op}_{N(\text{OP})})$ 为输出信息库所有限集合; $T = (t_1, t_2, \ldots, t_{N(T)})$ 为动作变迁的有限集合; $I(P,T)$ 为从状态或信息库所到变迁 T 的输入映射,对应 P 到 T 的有向弧; $O(P,T)$ 为从变迁 T 到库所 P 的输出映射,对应 T 到 P 的有向弧; $I(P,T)$ 和 $O(T,P)$ 均为矩阵,且 $P = \text{SP} \bigcup \text{IP} \bigcup \text{OP}$; C 为库所和变迁的颜色集合; $\text{CM} = (\text{cm}_1, \text{cm}_2, \ldots, \text{cm}_{N(T)})$ 为行为变迁 t_i 触发约束条件的有限集合, cm_i 由输入映射 $I(P,t_i)$ 的触发约束函数组成,且 $\text{cm}_i = [\text{consf}(p_1,t_i), \ldots, \text{consf}(p_k,t_i)]^{\text{T}}_{1\times k}$ (k 为变迁 t 的关联输入库所总数目), $\text{consf}(p,t)$ 定义为

$$\forall (p_m, t_i) \in I(P, t_i),$$
$$\text{consf}(p_m, t_i) = \begin{cases} 1, \ \text{transitionenable}; \\ 0, \ \text{otherwise}. \end{cases} \tag{3}$$

当该变迁的所有触发条件均满足才能激活变迁,即当且仅当 $\text{Rank}(\text{CM}) = k$; 另外, $N(\text{SP})$、$N(\text{IP})$、$N(\text{OP})$ 和 $N(T)$ 依次表示状态库所、输入信息库所、输出信息库所以及动作变迁的总数目.

定义 3 (通信关系网 Network)　表示系统信息域与物理域的交互关系,由 n 个通信信道组成,有

$$\text{Network} = (\text{channel}_{12}, \ldots, \text{channel}_{ij}), \quad i, j \in [1, 2, \ldots, n]. \tag{4}$$

其中: channel_{ij} 为系统组件 i 到 j 的通信信道, n 为系统实体的总数目. channel_{ij} 用四元组具体表示为

$$\text{channel}_{ij} = (I, O, T, \text{TA}). \tag{5}$$

其中: I 和 O 分别为发送端和接收端实体组件; T 为二者间的通信变迁过程: $\text{TA} = (C_{\text{prob}}, C_{\text{delay}})$ 为通信变迁属性, C_{prob} 为通信可靠性, C_{delay} 为通信时延. 特别地,通信可靠性不仅反映了多域耦合程度,也是跨域脆弱性渗透的重要表征.

3.2.2　攻击者模型

传统攻击图是一种由顶点与有向边组成的有向图. 根据不同目标需求,顶点可以表示为安全服务、攻击行为、可利用漏洞以及实体对象等安全要素,而节点间的边关系实现攻击路径可视化. 基于攻击图的方法虽然能够直观展示系统具体的攻击行为,但是其更多聚焦单一攻击在系统中的局部作用,缺乏系统全局所有攻击特征的描述. 本文框架提出攻击子图和攻击全图的概念并定义如下.

定义 4 (攻击子图 Sub_G)　将系统拓扑中组件和通信关系分别抽象为节点和边的形式,还原攻击行为过程,有

$$\text{Sub\_}G = (\text{Node}, \text{Edge}, \text{Condition}, \text{Aprob}). \tag{6}$$

其中: $\text{Node} = N_{\text{vul}} \bigcup N_{\text{att}}$ 为攻击子图节点集合, N_{vul} 为被攻击节点, N_{att} 为攻击节点; Edge 为通信链路集合; Condistion 为攻击行为条件; Aprob 为攻击概率集合.

定义 5 (攻击全图 Global_G)　将不同攻击场景的攻击子图集合为攻击全图,描述系统不同节点间的关联程度以及关键节点的重要程度,有

$$\text{Global\_}G = (\text{GNode}, \text{GEdge}, N_w, E_w). \tag{7}$$

其中: GNode 和 GEdeg 分别为攻击全图的边和节点; N_w 反映了攻击图中某一节点遭受多种攻击的难度,通过该参数以表征节点的脆弱程度; E_w 为节点间攻击关联强度,但未考虑信息物理域攻击有向性.

攻击全图的生成将利用强化学习算法,通过自主学习更新节点间的关联程度和节点自身的关键程度两个量化指标. 这里将攻击子图生成的不同攻击行为序列 $\text{Seq}_{\text{att}} = (E_1, E_2, \ldots, E_m)$ 转化为搜索约束输入,以攻击收益为奖赏函数 Reward,将强化学习算法参数 Q 矩阵和 R 矩阵分别视为 E_w 和 N_w 的量化,攻击全图生成的简要过程如图 3 所示. 对于节点 j 而言, $N_w(j) = \sum_{i \in N(j)} \alpha_i \times R[i,j]$ 表示可利用节点 j 脆弱性的所有攻击对节点 j 的攻击难度累积,且 α_i 为节点 i 作用节点 j 的攻击权重, $N(j)$ 表示节点 j 的邻居节点范围. 同时,节点 i 与 j 间的攻击关联强度定义为 $E_w(i,j) = Q(i,j)$.

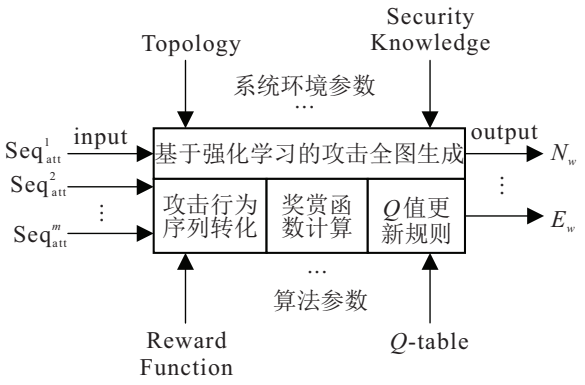

图 3 攻击全图生成体系

3.2.3 多域脆弱性融合评估模型

基于系统模型和攻击模型安全性分析,能够得出静态、动态脆弱性知识. 多域脆弱性融合分析是系统自身脆弱点和攻击切入作用下进一步脆弱性渗透程度的度量,最终得出工业控制系统整体的脆弱性态势. 针对目前工业控制系统脆弱性分析缺乏对信息域和物理域中不同攻击相互渗透影响因素考虑的问题,本文框架将在系统形式化模型和攻击全图模型基础上,提出基于贝叶斯网络和细胞自动机理论的多域脆弱性渗透分析模型,并对分析结果进行层次分析下的脆弱性融合评估. 这里,基于贝叶斯网络的多域细胞自动机模型将深入探究同一空间域和跨域过程的脆弱性传播,也是融合评估模型的核心. 结合文献[21]对基于细胞自动机理论的安全风险传播机制研究,本框架中多域细胞自动机模型的细胞状态、空间、邻居、以及演化规则定义如下.

定义6(细胞状态) 针对系统多域空间特点,将系统组件分为信息域细胞和物理域细胞两类. 这里将系统多域组件性能受损(脆弱特性)表示为细胞状态. 其中0表示组件脆弱特性未利用,1表示被利用.

定义7(细胞空间) 信息域细胞的细胞空间由信息域m个组件节点组成,物理域细胞空间包括物理域k个组件节点.

定义8(细胞邻居) 用邻接矩阵H表示系统多域细胞空间各个细胞之间的关系,有

$$H=\begin{bmatrix}A_{m\times m} & B_{m\times k}\\ C_{k\times m} & D_{k\times k}\end{bmatrix}. \tag{8}$$

其中:$A=(a_{ij})_{m\times m}$为信息域细胞的邻接矩阵,a_{ij}为信息域中攻击者从节点i利用节点j脆弱特性的概率. 这里,结合攻击全图中节点间脆弱关联度E_w和节点脆弱程度N_w,定义脆弱性利用概率a_{ij}计算公式如下:

$$a_{ij}=E_w(i,j)\times N_w(j)\Big/\sum_{l\in N(i)}N_w(l). \tag{9}$$

同理,$D=(d_{i,j})_{k\times k}$为物理域细胞的邻接矩阵,$d_{i,j}$为物理域攻击者从节点i利用节点j脆弱特性的概率,具体公式定义与式(9)类似. $B=(b_{i,j})_{m\times k}$与$C=(c_{i,j})_{k\times m}$分别为信息域至物理域(C2P)、物理域至信息域(P2C)的脆弱性跨域渗透传播过程,$b_{i,j}$、$c_{i,j}$为对应跨域渗透传播的可能性. 在攻击全图中,E_w参数反映了节点间的关联性,包括跨域节点间关系. 以$b_{i,j}$计算公式为例,有

$$b_{i,j}\begin{cases}\neq 0,\ i \text{ in cyber area and } j \text{ in physical area;}\\ =0,\ i \text{ and } j \text{ in the same area.}\end{cases} \tag{10}$$

考虑到C2P和P2C的脆弱性渗透可能性及程度不同,且与安全防御措施、脆弱点自身特性和组件资产等因素有关,基于历史安全事件,结合攻击全图中节点间关联程度E_w、节点关键程度N_w和攻击方向向量$\overrightarrow{V_{\text{att}}}$,采用贝叶斯网络方法推理计算跨域渗透传播概率.

定义9(演化规则) 演化规则是细胞状态变化机制的核心. 对于同一空间域的细胞状态演化将遵循规则$R_1:S_i(t)\to S_j(t+1)$,同一域中t时刻节点i脆弱性根据规则R_1在$t+1$时刻关联至节点j的某一脆弱特征. 类似地,跨域细胞状态演化将遵循规则$R_2:S_i(t)\to S_j(t+1)$.

通过深入分析多域关联特征,能够有效分析系统脆弱性的渗透传播过程,综合反映工业控制系统脆弱性程度. 进一步地,划分系统不同域的脆弱性指标,设置多域脆弱性层次评价体系,将多域细胞自动机模型中细胞间的状态转移概率作为层次权重参数实现系统整体评估. 多域脆弱性融合评估模型基本结构如图4所示.

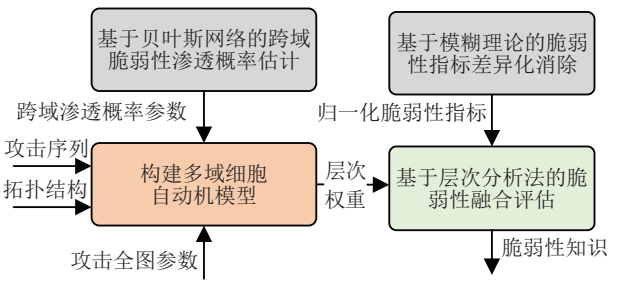

图 4 多域脆弱性融合评估模型基本结构

3.3 方案执行

实现方案的执行主要基于脆弱性多维协同分析框架,围绕具体系统对象描述如何分阶段揭示系统脆弱性机理,从而指导实际系统安全运行. 一般而言,具体执行过程将结合实际工业控制系统对象,以系统环境参数为核心输入,以安全知识和算法模型为辅助输入,基于脆弱性分析框架生成系统模型、攻击模型以

及脆弱性知识等输出结果. 图5给出了多维协同分析的执行过程. 其中,信息层负责提供系统对象环境参数变量,包括系统拓扑结构、设备组件类型、系统行为规则、安全状态约束条件以及基本功能需求;知识层主要涵盖开展系统脆弱性分析所需要的辅助知识及支撑技术,如系统攻击建模算法模型、支持攻击识别的攻击策略等.

本节以沸水反应炉系统(boiling water power plant, BWPP)为例[22],为上述脆弱性多维协同分析执行过程提供简要示例. BWPP系统基本架构如图6所示,主要由控制网络、物理网络以及二者之间的通信网络等组成. 其中,控制网络包括控制服务器和HMI两部分;物理网络由物理设备、传感器(压力传感S_1、电量传感S_2、水位传感S_3)和执行器(蒸汽阀V_1、燃气阀V_2、给水阀V_3)组成;通信网络负责系统多域间的数据信息交互传输,并由网关和防火墙支持. BWPP系统的行为规则包括: 1) 传感器读数通过通信网送至HMI; 2) 炉内压力控制遵循线性时变机理等一系列操作,且系统安全约束是:①保证炉内压力不超过Up_lim;②阀门开度在规定范围内等. 此外,BWPP系统的主要功能需求通过测量感知炉内蒸汽压力、水位以及电量状态等信息,结合;过程控制理论动态调整相应阀门装置开合度,保证反应炉内压力维持在安全运行约束范围内.

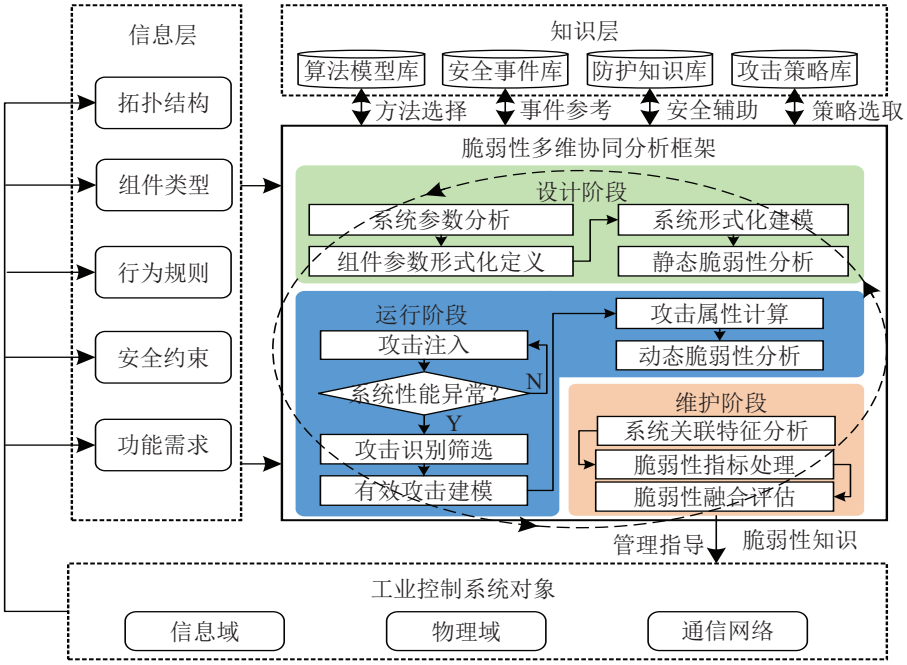

图 5　脆弱性多维协同分析执行过程

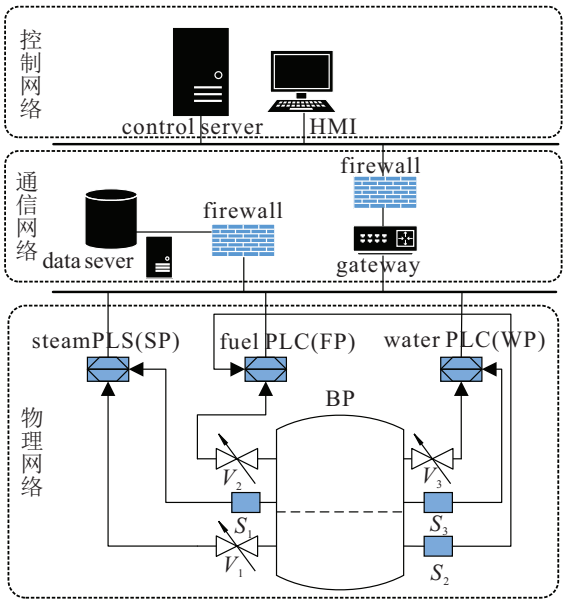

图 6　BWPP系统基本结构

在面向BWPP系统脆弱性分析实践中,设计阶段首先处理信息层先验知识,形式化定义系统控制器、执行器和传感器等组件及业务类型,如以元组形式描述组件编号、行为属性、安全约束、工作状态等. 在此基础上结合系统运行规则、功能需求及组件结构关系构建并关联为统一系统模型. 系统静态分析将通过理论方法评估节点间关联关系及节点重要程度,如复杂网络耦合系数、节点中心性等指标,最终得出BWPP系统结构特点,为攻击识别提供可利用的静态脆弱点.

接着,运行阶段根据漏洞知识以及设计阶段输出的静态脆弱点信息,结合匹配规则算法从攻击策略库中搜索可能的攻击方式,如BWPP系统物理扰动、通信报文丢失、控制时序故障等具体攻击手段. 基于系统形式化模型还原攻击场景. 考虑到BWPP系统

存在炉内压力是否逼近或超过安全上限Up_lim的安全约束,通过攻击模拟监测系统炉内蒸汽压力变化,直观地识别和筛选所有可能攻击的有效性和可行性. 在此基础上利用攻击图生成技术对有效攻击进行局部细化建模,以可利用漏洞、攻击方式、系统拓扑结构、安全配置为输入,以攻击路径及目标为输出,通过路径搜索算法、概率统计等方法,明确攻击路径、目标节点以及攻击效果等属性,为系统动态脆弱性分析提供更精确的结果.

BWPP系统静态和动态脆弱性分析更多关注BWPP系统结构、反应炉内压力控制、HMI控制信令生成等局部过程的脆弱程度. 维护阶段首先进行BWPP系统多域关联特征分析. 这里,采用贝叶斯网络等方法统计学习历史安全事件,以BWPP系统安全事件作为输入训练样本,将系统控制中心与物理组件间关联特征作为多域间脆弱性渗透传播可能性表征. 在此基础上,构建基于细胞自动机的脆弱性渗透分析模型,为脆弱性融合评估提供重要参数. 其次,统一处理动静态脆弱性评估指标,如控制信令实时性、压力稳定性等,消除量化指标间差异特征. 接着,基于信息物理域指标分区,依据渗透分析模型中多域关联属性参数,利用层次分析算法实现系统多域脆弱性的融合评估,优化指导现场执行与维护管理. 面向BWPP系统的脆弱性分析流程如图7所示.

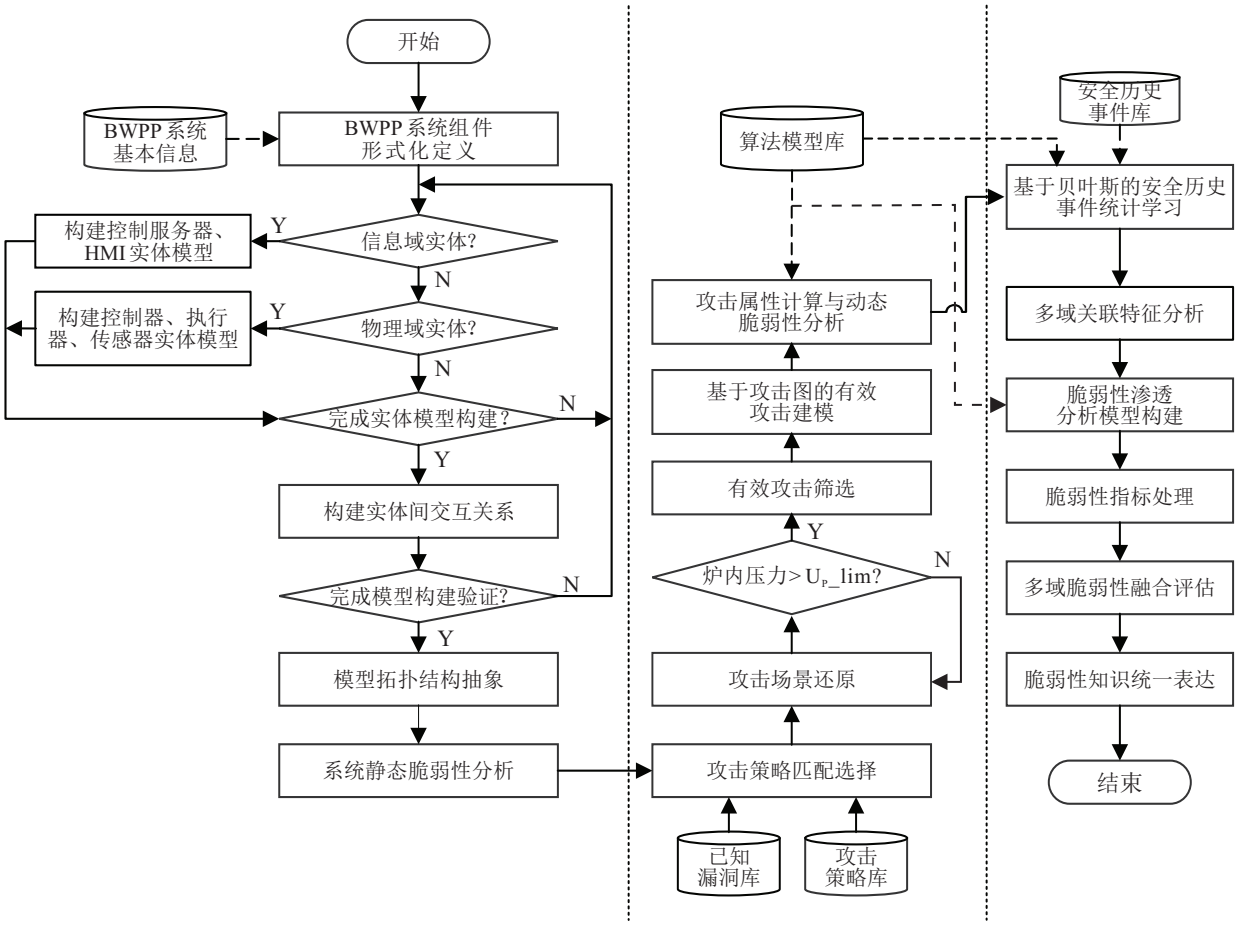

图7 BWPP系统脆弱性分析流程

4 脆弱性多维协同分析框架应用

工业控制系统脆弱性多维协同分析框架的设计是传统单点或局部安全性分析的重要突破. 分析框架如何覆盖并保障系统全生命周期安全运行是框架设计的核心问题. 开展面向工业控制系统的静态脆弱点挖掘、动态关联渗透分析、融合评估与优化指导等研究,将有助于从全局角度剖析系统全生命周期各阶段的安全需求,明确不同环节的脆弱性特征,最终有效指导、优化系统安全防护及安全管理. 脆弱性多维协同分析框架面向工业控制系统安全需求及特征属性,从多个维度提出脆弱性分析的技术路线和具体实现方案,主要具有以下优势:

1) 工业控制系统脆弱性含义确定. 结合国家标准、指南政策,深入比较风险评估及脆弱性分析研究现状、需求特征,明确工业控制系统脆弱性基本含义.

2) 全生命周期需求覆盖. 分阶段、分方法提出工业控制系统脆弱性分析思路与支撑技术,充分挖掘系统全生命周期脆弱属性.

3) 一体化架构设计. 框架不同阶段之间的动态联动不仅层层递进剖析系统安全问题,同时闭环反馈模式可进一步验证优化指导结果的有效性.

4) 全生命周期脆弱性机理揭示. 框架提出多域脆弱性融合评估方法攻克系统信息物理域脆弱性渗透关联难题,突破了系统局部脆弱性评估的有限性.

4.1　工业控制系统长效安全防护

面向工业控制系统的安全防护体系是实际系统长期稳定运行的主要支撑. 安全策略决策作为系统安全防护中极为重要的环节,其决策精度是系统安全防护有效性和及时性的关键. 然而,决策精度的保证不仅需要高质量的策略生成算法,更需要真实详细的先验知识辅助.

在传统系统安全防护中,主要通过入侵检测发现异常攻击并评估当前安全态势,采用合适的策略决策机制抵御及缓解攻击影响,最终达到保障系统安全运行的目的. 基于入侵反应的安全防护框架虽然能有效防止或降低攻击作用,但整个体系聚焦系统异常状态以及攻击证据来注重保护系统当前状态安全,缺乏长期安全防护的实现目标.

然而,脆弱性多维协同分析框架充分考虑系统运行特点、环境参数等信息,通过揭示全生命周期脆弱性机理明确系统脆弱特征. 结合脆弱性分析方法,系统安全防护的策略决策环节不仅从攻击者角度考虑如何抵御攻击引入的安全风险,而且从防护角度结合系统脆弱性特征明确哪些环节或区域需加强安全部署,为策略执行提供更加优化的策略防护方案. 二者结合应用架构如图 8 所示,生成的安全策略在抵御入侵的同时也加强了脆弱环节的防护,防止二次攻击再次危害,提高系统自身韧性能力并有望实现长效安全防护的目标.

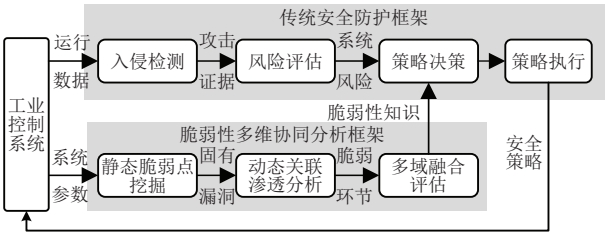

图 8　脆弱性多维协同分析框架在安全防护中的应用架构

4.2　未来工业安全研究支持

新一代工业控制系统或智能化工业生产过程将面临更多未知、开放性的脆弱性及安全问题. 因此,脆弱性分析在未来工业安全研究中更应受到关注与支持. 工业互联网作为新一代信息通信技术与工业经济深度融合的新型应用模式,是未来工业发展的中坚力量. 然而,在工业互联网发展的同时,安全保障将成为愈加重要的问题. 虽然面向工业互联网安全问题已出台相关保障机制,但是其安全分析与防护不应局限于某一区域和针对性的安全部署,更需从系统工程角度出发建立一个全局整体的安全分析与防护框架. 脆弱性多维协同分析框架在工业互联网安全研究中,能够深入揭示工业互联网网络和平台层静态部署、动态运行脆弱点,并在工业互联网安全层进行评估,从而提出安全防护与指导方案.

5　结　论

本文提出了一套面向全生命周期工业控制系统的脆弱性多维协同分析框架,从系统对象、攻击传播和指标评估 3 个层次探讨脆弱性分析的关键思路. 在此基础上充分结合工业控制系统全生命周期安全需求,依次明确设计阶段、运行阶段和维护阶段脆弱性分析具体方案. 同时,简要阐述了脆弱性多维协同分析框架的主要模型支撑技术,并结合具体对象细化描述方案执行过程. 最后总结框架优势特性,指明脆弱性协同分析框架的未来应用.

面临外来攻击无法避免的严峻形势,脆弱性多维协同分析框架有望在系统全生命周期明确脆弱程度,识别引发威胁事件发生的原因. 同时,一体化框架结构以及多维度协同作用有助于实现系统脆弱性机理的全局揭示.

参考文献(References)

[1] Zhou C J, Hu B W, Shi Y, et al. A unified architectural approach for cyberattack-resilient industrial control systems[J]. Proceedings of the IEEE, 2021, 109(4): 517-541.

[2] Humayed A, Lin J Q, Li F J, et al. Cyber-physical systems security — A survey[J]. IEEE Internet of Things Journal, 2017, 4(6): 1802-1831.

[3] Lu Y. Industry 4.0: A survey on technologies, applications and open research issues[J]. Journal of Industrial Information Integration, 2017, 6: 1-10.

[4] Messenger J L. Time-sensitive networking: An introduction[J]. IEEE Communications Standards Magazine, 2018, 2(2): 29-33.

[5] Zhang Q, Zhou C J, Tian Y C, et al. A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems[J]. IEEE Transactions on Industrial Informatics, 2018, 14(6): 2497-2506.

[6] Huang K X, Zhou C J, Tian Y C, et al.

Assessing the physical impact of cyberattacks on industrial cyber-physical systems[J]. IEEE Transactions on Industrial Electronics, 2018, 65(10): 8153-8162.

[7] Xu Y, Yang Y, Li T, et al. Review on cyber vulnerabilities of communication protocols in industrial control systems[C]. Proceedings of the Energy Internet and Energy System Integration Conference. Beijing, 2017: 1-6.

[8] Yi M B, Fu J Q. Improved modbus/TCP multi-dimensional fuzzing test method[C]. Chinese Control and Decision Conference. Nanchang, 2019: 3233-3237.

[9] Zolanvari M, Teixeira M A, Gupta L, et al. Machine learning-based network vulnerability analysis of industrial internet of things[J]. IEEE Internet of Things Journal, 2019, 6(4): 6822-6834.

[10] Ten C W, Liu C C, Govindarasu M. Vulnerability assessment of cybersecurity for SCADA Systems using attack trees[C]. Proceedings of the Power Engineering Society General Meeting Conference.Tampa, 2007: 1-8.

[11] Ruijters E, Stoelinga M. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools[J]. Computer Science Review, 2015,15/16(3): 29-62.

[12] Wang H, Chen Z, Zhao J, et al. A vulnerability assessment methodin industrialInternet of things based on attack graph and maximum flow[J]. IEEE Access, 2018, 6: 8599-8609.

[13] Jajodia S, Noel S. Topological vulnerability analysis: A powerful new approach for network attack prevention, detection, and response[C]. Algorithms, Architectures and Information Systems Security. World Scientific, 2008: 285-305.

[14] Wei X G, Gao S B, Huang T, et al. Complex network-based cascading faults graph for the analysis of transmission network vulnerability[J]. IEEE Transactions on Industrial Informatics, 2019, 15(3): 1265-1276.

[15] Li X, Zhou C J, Tian Y C, et al. Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems[J]. IEEE Transactions on Industrial Informatics, 2018, 14(2): 608-618.

[16] Mitchell R, Chen I. Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems[J]. IEEE Transactions on Reliability, 2016, 65(1): 350-358.

[17] Wei X G, Gao S B, Huang T, et al. Electrical network operational vulnerability evaluation based on small-world and scale-free properties[J]. IEEE Access, 2019, 7: 181072-181082.

[18] Panigrahi P, Maity S. Vulnerability analysis of weighted indian power grid network based on complex network theory[C]. Proceedings of the India Council International Conference. Roorkee, 2017: 1-6.

[19] Anikin I V. Using fuzzy logic for vulnerability assessment in telecommunication network[C]. International Conference on Industrial Engineering, Applications and Manufacturing. Petersburg, 2017: 1-4.

[20] Huang K K, Xiang Z L, Deng W F, et al. Reweighted compressed sensing-based smart grids topology reconstruction with application to identification of power line outage[J]. IEEE Systems Journal, 2020, 14(3): 4329-4339.

[21] 叶夏明, 文福拴, 尚金成, 等. 电力系统中信息物理安全风险传播机制[J]. 电网技术, 2015, 39(11): 3072-3079.
(Ye X M, Wen F S, Shang J C, et al. Propagation mechanism of cyber physical security risks in power systems[J]. Power System Technology, 2015, 39(11): 3072-3079.)

[22] Orojloo H, Azgomi M A. Evaluating the complexity and impacts of attacks on cyber-physical systems[C]. CSI Symposium on Real-Time and Embedded Systems and Technologies. Tehran, 2015: 1-8.

作者简介

李欣格(1996−), 女, 博士生, 从事信息安全的研究, E-mail: xingeli@hust.edu.cn;

胡晓娅(1974−), 女, 教授, 博士生导师, 从事网络及系统安全等研究, E-mail: huxy@hust.edu.cn;

周纯杰(1965−), 男, 教授, 博士生导师, 从事工业互联网及工业控制系统安全等研究, E-mail: cjiezhou@hust.edu.cn;

尹泉(1968−), 男, 教授, 博士生导师, 从事伺服控制与数字化控制等研究, E-mail: yinquan@mail.hust.edu.cn.

(责任编辑：郑晓蕾)