

工业控制系统安全风险传播机理研究

王红敏¹, 魏强¹, 王兰敏²

(1. 信息工程大学, 河南 郑州 450001; 2. 天津工业大学, 天津 300000)

摘要: 随着工业化和信息化的深度融合, 工业控制系统在提升生产效率的同时也面临着日益复杂的安全威胁。深入研究工业控制系统安全风险的传播机理, 对保障其安全稳定运行具有重要意义。为此, 借鉴生物学中的SIRS (susceptible-infected-recovered-susceptible) 模型, 研究工业控制系统安全风险传播机理。首先, 基于SIRS模型绘制了系统状态转移图, 并建立对应的微分方程组。基于该模型, 以感染节点的变化率为核心指标分析风险传播速度, 识别并量化影响传播速度的关键因素。其次, 基于基本再生数 R_0 的阈值特性研究风险传播范围。当 $R_0 < 1$ 时, 通过构造Lyapunov函数证明系统在无毒平衡点 E_0 处具有全局稳定性, 表明风险将随时间逐渐衰减并最终在系统中完全消失; 当 $R_0 > 1$ 时, 通过求解雅可比矩阵的特征方程, 证明系统在有毒平衡点 E^* 处具有局部渐进稳定性, 揭示风险会在系统内持续稳定传播且不会自行消失的规律。最后, 应用最优控制理论研究风险传播的控制问题, 利用最优控制定理证明最优控制解的存在性, 并通过引入Hamilton函数求解最优控制策略。为验证理论模型的合理性, 通过数值模拟与实验分析, 分别验证无毒平衡点的全局稳定性与有毒平衡点的局部渐进稳定性, 为工业控制系统安全风险的量化评估与精准管控提供理论支撑。

关键词: 工业控制系统安全; SIRS模型; 风险传播速度; 风险传播范围; 风险传播控制

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025045

Research on the mechanism of industrial control system security risk propagation

WANG Hongmin¹, WEI Qiang¹, WANG Lanmin²

1. Information Engineering University, Zhengzhou 450001, China

2. Tianjin Polytechnic University, Tianjin 300000, China

Abstract: With the deep integration of industrialisation and informatisation, industrial control systems (ICS) were faced with increasingly complex security threats while productivity was being enhanced. An in-depth study of the propagation mechanism of industrial control system security risks was conducted to guarantee safe and stable operation. For this purpose, the susceptible - infected - recovered - susceptible (SIRS) infectious disease model from biology was drawn upon to analyse the mechanism of security risk propagation in industrial control systems. The system state transition diagram was constructed based on the SIRS model, and the corresponding system of differential

收稿日期: 2025-01-14; 修回日期: 2025-05-06

通信作者: 王红敏, 1542811931@qq.com

引用格式: 王红敏, 魏强, 王兰敏. 工业控制系统安全风险传播机理研究[J]. 网络与信息安全学报, 2025, 11(4): 107-116.

Citation Format: WANG H M, WEI Q, WANG L M. Research on the mechanism of industrial control system security risk propagation[J]. Chinese Journal of Network and Information Security, 2025, 11(4): 107-116.

equations was established. Based on this model, the rate of change of infected nodes was used as a core indicator to analyze the speed of risk propagation, and key factors influencing the propagation speed were identified and quantified. The range of risk propagation was studied based on the threshold properties of the basic reproduction number R_0 . When $R_0 < 1$, it was proven that the system exhibited global stability at the disease-free equilibrium point E_0 by constructing a Lyapunov function, indicating that the risk would gradually decay over time and eventually disappear entirely from the system. When $R_0 > 1$, by solving the characteristic equation of the Jacobian matrix, it was shown that the system achieved local asymptotic stability at the endemic equilibrium point E^* , revealing that the risk would propagate steadily within the system and would not disappear autonomously. Optimal control theory was applied to study the control of risk propagation. The existence of an optimal control solution was proven using optimal control theory, and the optimal control strategy was derived by introducing the Hamilton function. To verify the rationality of the theoretical model, the global stability of the disease-free equilibrium point and the local asymptotic stability of the endemic equilibrium point were validated through numerical simulation and experimental analysis, respectively. This study thus provides theoretical support for the quantitative assessment and precise control of safety risks in industrial control systems.

Keywords: industrial control system security, SIRS model, risk propagation speed, risk propagation scope, risk propagation control

0 引言

工业控制系统 (industrial control system, ICS) [1] 作为国家关键基础设施的核心组成部分, 被广泛应用于电力、水利、化工、能源等行业[2]。典型的 ICS 包含六大功能模块, 分别是人机界面、远程诊断与维护、控制器、执行器、传感器及物理过程模块, 其运行机制如图 1 所示[3]。在该架构中, 人机界面与控制器之间进行双向实时数据交互。一方面, 人机界面将控制器的过程状态信息及历史数据传输给工程师站或操作员站; 另一方面, 操作人员通过人机界面实时调整控制器的设置值、控制算法和参数约束过程数据。远程诊断与维护模块具备故障预防、识别和系统恢复功能。控制回路则通过传感器、执行器和控制器的协同运作实现对物理过程的调控, 而物理过程具有典型的系统动力学特征。

ICS 具有复杂的网络拓扑结构、高度互联的设备依赖关系及多样化的通信方式, 使得安全风险能够通过数据流和控制流在信息域与物理域之间传播。网络攻击可能导致物理过程发生变化, 这一现象直接印证了信息域风险向物理域传导的特性。通过深入研究风险传播的机理, 不仅可以精准定位风险传播的关键节点, 还能探究有效的风险控制方法, 进而部署针对性的风险缓解措施, 最终实现对风险传播链路的阻断。因此, 开

展 ICS 安全风险传播机理研究, 对保障系统安全稳定运行具有重大意义。

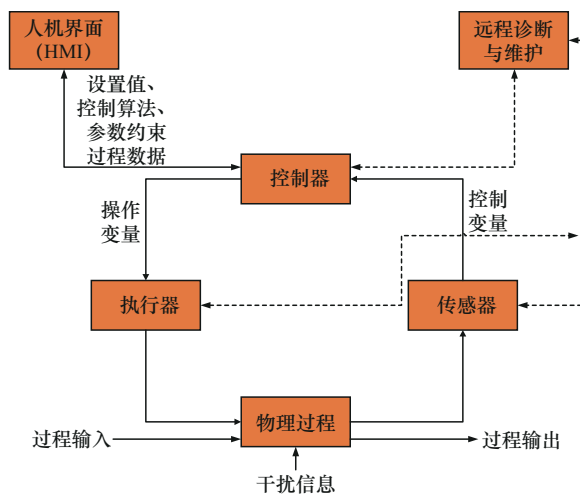


图 1 典型 ICS 的运行机制

Figure 1 Operation mechanism of typical ICS

目前, 针对 ICS 安全风险传播机理的研究仍相对有限, 但相关领域的安全风险评估研究成果[1-2,4-7]为该方向的研究工作提供了重要支撑。文献[1]构建了模糊概率贝叶斯网络模型, 用于分析和预测信息安全风险在系统中的传播机制。由于缺乏大量的历史数据, 研究人员基于专家知识构建了模糊条件概率表。该方法通过专家经验预测风险发生的概率, 为风险传播范围研究提供了新思路。文献[2]聚焦网络攻击对物理系统的

影响评估, 其研究方法包含3个关键步骤。首先, 构建包含脆弱性节点、权限提升节点和目标节点的贝叶斯网络架构; 其次, 基于通用漏洞评分系统 (common vulnerability scoring system, CVSS) 和逻辑门运算计算条件概率表; 最后, 应用贝叶斯理论计算给定攻击证据条件下目标节点的后验失效概率。考虑到网络攻击的离散特性与物理过程的连续性特征, 研究人员进一步采用随机混合系统 (stochastic hybrid system, SHS) 模型建立二者间的关联关系, 并设计鲁棒状态估计器来评估不同攻击模式下的物理过程状态。该方法通过量化网络攻击对物理域的影响, 直接印证了信息域风险向物理域传播的特性, 为风险传播范围研究提供了实证支撑。文献[4]指出攻击者的主要目标是破坏控制系统的功能, 并提出一种多层级贝叶斯网络模型用于预测信息安全风险。该模型整合了网络攻击特征、系统功能状态、危害事件类型及系统资产信息等维度的数据, 从而提升了风险传播机理研究对未知风险的覆盖度, 提高了研究的完备性。文献[5]基于SIR (susceptible-infected-recovered) 模型通过分析智能电网中感染节点的变化率来量化风险传播速度。由于电网系统是ICS的重要应用领域, 该方法为ICS风险传播动力学研究提供了可借鉴的思路。

由于病毒是引发ICS安全风险的主要因素之一, 因此除了借鉴安全风险评估的研究成果外, 还可以参考病毒传播领域的研究方法。已有学者运用数学模型对ICS中的病毒传播过程进行建模分析。文献[8]提出了SLBR (susceptible latent breaking recovered) 模型, 用于研究工业病毒在SCADA系统中的传播特性。该研究的创新点主要体现在3个方面: 首先, 模型考虑了工业病毒可能绕过潜伏期直接爆发的特殊情况; 其次, 针对工业病毒的特点设计了专用算法, 并采用真实的Facebook数据集验证算法的有效性; 最后, 通过对比实验证实了模型的有效性。由于病毒传播是风险传播的重要诱因, 这类研究对理解风险传播机制具有重要的参考价值。文献[9]详细分析了震网病毒在ICS中的传播过程。作为典型的

风险传播机理探索提供了新的研究视角。通过对风险评估和病毒传播等领域的现有研究成果进行系统分析, 本文将安全风险跨域传播机理归纳为风险传播速度、风险传播范围和风险传播控制3个关键问题。受SIRS (susceptible-infected-recovered-susceptible) 模型的启发, 本文采用微分动力学方法^[10-11]对这3个关键问题展开深入研究。

本文的主要贡献如下。

1) 风险传播速度方面: 基于SIRS模型框架, 风险传播速度可量化为系统感染节点的变化率。研究发现该变化率主要取决于3个关键参数, 分别是易感节点的感染概率、感染节点的恢复概率和设备被移除概率。考虑到设备因损坏等原因被移除的概率是系统固有属性, 与节点类型无关, 本文提出: 首先通过量化攻击方式和设备重要性计算易感节点感染的概率; 然后基于脆弱性的影响程度和优先级计算感染节点恢复概率; 最终结合SIRS模型建立感染节点变化率的动态方程。

2) 风险传播范围方面: 引入流行病学研究中的基本再生数 R_0 ^[11]作为评估感染节点传播能力的指标, 其数值大小直接决定了风险传播的范围。当 $R_0 < 1$ 时, 系统在无毒平衡点 E^* 处具有全局稳定性, 表明风险传播将呈现持续衰减并最终消失的趋势; 当 $R_0 > 1$ 时, 系统在有毒平衡点 E^* 处表现出局部渐进稳定性, 意味着风险将持续在系统中传播。这一发现为预测风险传播范围提供了量化依据。

3) 风险传播控制方面: 基于最优控制理论, 本文建立了风险传播的控制模型。首先, 运用最优控制理论的5条基本引理证明控制策略的存在性; 然后, 引入Hamilton函数求解最优控制方案。该方法为制定有效的风险控制措施提供了理论支撑, 有助于降低风险传播造成的危害。

1 模型构建

风险既可以在信息域、物理域内独立传播, 也可以在信息域与物理域之间跨域传播。在物理域中, 风险主要来源于设备故障、人员误操作等非故意性危害, 其发生概率相对较小。在正常状态下, 物理域可建模为线性时不变 (linear time-invariant, LTI) 系统^[12-13]; 当物理域风险发生变化时, 系统状态可由式(1)描述。

$$\begin{aligned} x_{k+1} &= Ax_k + B(u_k + d_k^u) + w_k \\ y_k &= Cx_k + d_k^y + v_k \end{aligned} \quad (1)$$

其中, x_k 表示系统状态, u_k 表示控制器状态, y_k 表示传感器读数, A 、 B 和 C 表示物理层的动力学矩阵, w_k 和 v_k 为零均值高斯噪声, d_k^u 和 d_k^y 分别表示传感器和执行器面临的风险^[2,12]。式(1)揭示了物理域设备间的依赖关系。信息域的风险则源于威胁对脆弱性的利用, 其发生概率通常较大。值得注意的是, 无论是物理域还是信息域, 风险都能通过系统拓扑结构在设备间形成级联传播效应。

在系统风险传播建模中, 设备节点可分为易感 (susceptible, S) 节点、感染 (infected, I) 节点、恢复 (recovered, R) 节点 3 种类型。由于感染节点经修复后可能因新的漏洞或攻击手段而重新变为易感节点, 因此本文采用 SIRS 模型来研究风险传播速度。该模型的状态转移关系如图 2 所示。其中, $S(t)$ 表示 t 时刻易感节点在系统中的比例, $I(t)$ 表示 t 时刻感染节点在系统中的比例, $R(t)$ 表示 t 时刻恢复节点在系统中的比例。 β 表示易感节点因自身脆弱性被攻击而转化为感染节点的概率; γ 表示感染节点通过修复等手段转化为恢复节点的概率; α 表示恢复节点因防护措施失效 (如版本未更新) 或攻击手段升级, 再次转化为易感节点的概率。同时, 该模型假设新设备以概率 δ 加入系统、旧设备以概率 μ 从系统中移除。基于上述模型与假设, 本文将从风险传播速度、风险传播范围、风险传播控制 3 个维度深入研究风险传播特性。

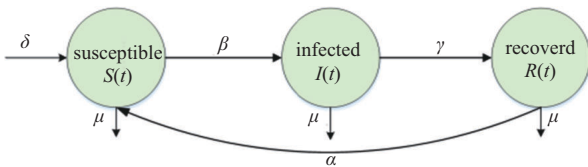


图 2 SIRS 模型的状态转移关系

Figure 2 State transition relationship of the SIRS model

1.1 风险传播速度

结合 SIRS 模型及文献[5]的证明结果, 风险传播速度可以表示为系统内感染节点的变化率, 即 $\frac{dI(t)}{dt}$ 。该模型的微分动力学方程如式(2)所示。

$$\begin{cases} \frac{dS}{dt} = \delta - \beta SI + \alpha R - \mu S \\ \frac{dI}{dt} = \beta SI - \gamma I - \mu I \\ \frac{dR}{dt} = \gamma I - \alpha R - \mu R \end{cases} \quad (2)$$

通过分析式(2)中第 2 个方程可以发现, $\frac{dI(t)}{dt}$ 与参数 β 、 γ 、 μ 相关, 但由于设备自身损坏等因素退出系统的概率 μ 为固定值, 因此仅需量化 β 和 γ 的值。基于此, 下文将对 β 和 γ 依次展开研究。

1.1.1 β 的计算

β 表示节点因自身脆弱性而被攻击的概率。通过分析 ICS 的 ATT&CK (adversarial tactics, techniques, and common knowledge) 模型^[14-15]可知, β 与设备脆弱程度、设备重要性密切相关。因此, 下文将分别对这两个因素进行量化。

(1) 设备脆弱程度量化

攻击者通常利用设备脆弱性发起攻击, 设备的脆弱程度与其被利用的可能性呈正相关。若某脆弱点更易被利用, 则其脆弱性更强。单个设备可能包含多个脆弱点, 设备 i 的第 j 个脆弱点被利用的可能性可通过通用漏洞评分系统 (common vulnerability scoring system, CVSS)^[16]基本矩阵中的攻击向量 (AV)、攻击复杂度 (AC)、特权要求 (PR)、用户交互 (UI) 这 4 个指标量化。设备 i 的第 j 个脆弱点程度 VE_{ij} 的计算公式如式(3)所示。

$$VE_{ij} = \frac{8.22 \times AV \times AC \times PR \times UI}{10} \quad (3)$$

其中, AV 表示攻击者使用的路径或者手段, AC 表示该脆弱点被利用的难易程度, PR 表示漏洞利用所需的权限等级, UI 表示攻击者对脆弱点的利用是否需要其他用户参与。这 4 个指标的具体量化方法可参考文献[17]中的表 2。

(2) 设备重要性量化

除设备脆弱程度外, 设备被攻击的可能性还与其重要程度相关。重要程度越高, 被攻击的可能性越大, 面临的风险也越高。因此, 衡量设备重要程度对分析风险传播速度同样具有重要的意义。设备重要程度通过其资产价值与

所在层设备总价值的比值计算, 计算公式如式(4)所示。

$$D_{\text{important}}^i = \frac{S_{\text{value}}^{ij}}{\sum_{i=1}^n S_{\text{value}}^{ij}} \quad (4)$$

其中, $D_{\text{important}}^i$ 表示系统中第 i 个设备的重要性, S_{value}^{ij} 表示系统第 j 层中第 i 个设备的价值, $\sum_{i=1}^n S_{\text{value}}^{ij}$ 表示系统第 j 层设备的总价值。

综合设备脆弱程度和设备重要性的量化结果, 设备 i 被攻击的概率 β_i 可通过式(5)计算。

$$\beta_i = \left(1 - \prod_{j=1}^n (1 - \text{VE}_{ij})\right) \cdot D_{\text{importance}}^i \quad (5)$$

1.1.2 γ 的计算

γ 表示感染节点的所有脆弱点被修复后转化为恢复节点的概率, γ 与脆弱点的影响程度 V_i 及优先级 L_i 密切相关。脆弱点的影响越大或优先级越高, 其被修复的可能性越高。脆弱点的影响通过其对信息系统安全3要素(可用性 A 、完整性 I 、机密性 C)的影响来衡量。根据文献[18], 这3个指标各采用 {none, low, high} 3种取值, 将 {none, low, high} 分别量化为0到1之间的数值为 {none = 0, low = 0.275, high = 0.660}。脆弱点 i 的影响程度 V_i 的计算公式如下。

$$V_i = \min(10, 10.14(1 - (1 - C)(1 - I)(1 - 1.51A))) \quad (6)$$

CVSS 中的脆弱点修复等级是确定脆弱点优先级 L_i 的关键指标。修复等级包含5种可能的状态取值, 分别为 {not defined; official fix; temporary fix; workaround; unavailable}。参照文献[19]的量化规则, 这些状态被映射为0到1之间的数值 {not defined = 1; official fix = 0.95; temporary fix = 0.96; workaround = 0.97; unavailable = 1}。

综合上述分析, 设备 i 的脆弱点 j 被修复的概率 γ_{ij} 可表示为 V_j 与 L_j 的乘积, 计算公式如下。

$$\gamma_{ij} = V_j \times L_j \quad (7)$$

考虑到设备 i 可能存在 n 个脆弱点, 设备 i 的恢复概率 γ_i 应取所有脆弱点修复概率中的最小值, 计算公式如下。

$$\gamma_i = \min\{\gamma_{i1}, \gamma_{i2}, \dots, \gamma_{in}\} \quad (8)$$

1.2 风险传播范围

基本再生数 R_0 是衡量风险在系统内传播范围的关键指标, 其定义为单个感染节点在整个易感群体中平均能够传播风险的节点数量。根据定义, R_0 的计算公式如下。

$$R_0 = \frac{\beta}{\gamma} \quad (9)$$

其中参数 β 的取值可由第 1.1.1 节的量化方法获得, 参数 γ 的取值可由第 1.1.2 节的量化方法获得。

为明确当 $R_0 < 1$ 时风险在系统内的传播规律, 下文将通过证明无毒平衡点的全局稳定性展开分析。

1.2.1 无毒平衡点及其全局稳定性

定理1 当 $R_0 < 1$ 时, 系统(2)[式(2), 下同]在无毒平衡点 E_0 处具有稳定性。

证明 根据无毒平衡点的全局性定义, 系统(2)存在唯一的无毒平衡点 $E_0\left(\frac{\delta}{\mu}, 0, 0\right)$ 。系统(2)在 E_0 处的雅可比矩阵如式(10)所示。

$$J(E_0) = \begin{bmatrix} -\mu & -\beta \frac{\delta}{\mu} & \alpha \\ 0 & \frac{\delta\beta}{\mu} - \gamma - \mu & 0 \\ 0 & \gamma & -\alpha - \mu \end{bmatrix} \quad (10)$$

式(10)对应的特征方程如式(11)所示。

$$|\lambda E - J(E_0)| = (\lambda + \mu) \left[\lambda - \left(\frac{\delta\beta}{\mu} - \gamma - \mu \right) \right] \cdot (\lambda + \alpha + \mu) \quad (11)$$

式(11)的特征值 λ_1 、 λ_2 和 λ_3 如式(12)所示。

$$\begin{cases} \lambda_1 = -\mu \\ \lambda_2 = \frac{\delta\beta}{\mu} - \gamma - \mu \\ \lambda_3 = -\alpha - \mu \end{cases} \quad (12)$$

显然, λ_1 和 λ_3 为负数。对于 $\lambda_2 = \frac{\delta\beta}{\mu} - \gamma - \mu$, 由于 $S + I + R = 1$ 且 $R_0 < 1$, 可以推导出 λ_2 为负数。通过上述推理, 结合 Hurwitz 定理, 可判定系统(2)在 E_0 处具有稳定性。

定理1表明, 当 $R_0 < 1$ 时, 随着时间的推移, 系统最终将仅存在易感节点, 感染节点及恢复节点的占比均会降至0, 风险在系统内不再传播。

定理 2 当 $R_0 < 1$ 时, 系统(2)在无毒平衡点 E_0 处具有全局稳定性。

证明 构造 Lyapunov 函数 $V(t) = I(t)$ 。那么

$$\begin{aligned}\frac{dV(t)}{dt} &= \frac{dI(t)}{dt} = \beta SI - \gamma I - \mu I \\ \frac{dV(t)}{dt} &= I(\beta S - \gamma - \mu) \\ \frac{1}{\gamma} \frac{dV(t)}{dt} &= I \left(\frac{\beta}{\gamma} S - 1 - \mu \right) \\ \frac{1}{\gamma} \frac{dV(t)}{dt} &= I(R_0 S - 1 - \mu)\end{aligned}\quad (13)$$

由于 $R_0 < 1$ 、 $S \leq 1$, 因此 $\frac{dV(t)}{dt} < 0$ 。且仅当 $I = 0$ 时, $\frac{dV(t)}{dt} = 0$ 。根据 LaSalle 不变原理, 可判定系统(2)在无毒平衡点 E_0 处具有全局稳定性。

定理 2 表明, 当 $R_0 < 1$ 时, 随着时间的推移, 易感节点和恢复节点的数量将趋于 0, 而感染节点数量呈持续递减趋势, 系统最终将稳定于无毒平衡点 E_0 。该结论表明系统风险将随时间持续衰减直至完全消除。

1.2.2 有毒平衡点及其稳定性

根据有毒平衡点的定义, 系统(2)存在唯一的有毒平衡点 $E^*(S^*, I^*, R^*) = \left(\frac{\gamma + \mu}{\beta}, \frac{(\alpha + \mu)(\beta - \gamma - \mu)}{\beta(\alpha + \gamma + \mu)}, \frac{\gamma(\beta - \gamma - \mu)}{\beta(\alpha + \gamma + \mu)} \right)$ 。

定理 3 当 $R_0 > 1$ 时, 系统(2)在有毒平衡点 $E^*(S^*, I^*, R^*)$ 处具有局部渐进稳定性。

证明 系统(2)在 E^* 处的雅可比矩阵如式(14)所示。

$$J(E^*) = \begin{bmatrix} \frac{-(\alpha + \mu)(\beta - \gamma - \mu)}{\alpha + \gamma + \mu} - \mu & -(\gamma + \mu) & \alpha \\ \frac{(\alpha + \mu)(\beta - \gamma - \mu)}{\alpha + \gamma + \mu} & 0 & 0 \\ 0 & \gamma & -\alpha - \mu \end{bmatrix}\quad (14)$$

式(14)的特征方程如式(15)所示。

$$|\lambda E - J(E^*)| = \lambda^3 + \alpha_2 \lambda^2 + \alpha_1 \lambda + \alpha_0 = 0 \quad (15)$$

其中,

$$\begin{aligned}\alpha_2 &= \alpha + 2\mu + \frac{(\alpha + \mu)(\beta + \gamma + \mu)}{\alpha + \gamma + \mu} > 0, \\ \alpha_1 &= \left\{ \left(\frac{(\alpha + \mu)(\beta - \gamma - \mu)}{\alpha + \gamma + \mu} + \mu \right) (\alpha + \mu) + \frac{(\alpha + \mu)(\beta - \gamma - \mu)}{\alpha + \gamma + \mu} (\gamma + \mu) \right\} = \\ &\quad \left\{ (I^* + \mu)(\alpha + \mu) + I^*(\gamma + \mu) \right\} > 0, \\ \alpha_0 &= \frac{(\alpha + \mu)(\beta - \gamma - \mu)}{\alpha + \gamma + \mu} (\gamma\mu + \alpha\mu + \mu^2) = \\ &\quad I^*(\gamma\mu + \alpha\mu + \mu^2) > 0\end{aligned}$$

通过上述分析可知, 特征方程的所有系数均为正数。根据 Hurwicz 定理, 系统(2)在有毒平衡点 E^* 处具有局部渐进稳定性。

该定理表明, 当 $R_0 > 1$ 时, 随着时间的推移, 感染节点的比率稳定为 $\frac{(\alpha + \mu)(\beta - \gamma - \mu)}{\beta(\alpha + \gamma + \mu)}$, 即风险将在系统内持续传播, 不会自行消失。

1.3 风险传播控制

本节运用最优控制理论^[20-23]研究风险在系统中传播速率的控制问题, 目的在于减少系统中感染节点的数量, 即实现风险传播速率的最优控制。由第 1.1.2 节可知, γ 表示脆弱点被修复的概率, 其取值与脆弱点影响、脆弱点优先级等因素相关, 因此可用控制变量函数 $\theta(t)$ 表示 γ 。其对应的微分动力学方程如式(16)所示。

$$\begin{cases} \frac{dS}{dt} = \delta - \beta SI + \alpha R - \mu S \\ \frac{dI}{dt} = \beta SI - \theta(t)I - \mu I \\ \frac{dR}{dt} = \theta(t)I - \alpha R - \mu R \end{cases} \quad (16)$$

式(16)中风险传播速率的目标泛函 $J(\theta)$ 如式(17)所示。

$$\begin{aligned}J(\theta) &= \int_0^T \left[F(\psi I(t) + \zeta \frac{\theta(t)^2}{2}) \right] dt \\ U &= \{ \theta, 0 \leq \theta(t) \leq 1, t \in [0, T] \}\end{aligned}\quad (17)$$

其中, ψ 表示感染节点变化率的权重系数, $\frac{\zeta \theta(t)^2}{2}$ 表示在系统中部署安全防护措施所需的成本。风险传播速率的最优控制问题为最小化目标泛函, 如式(18)所示。

$$\text{Minimize}_{\theta \in \Theta} J(\theta) = \int_0^T \left[\psi I(t) + \zeta \frac{\theta(t)^2}{2} \right] dt$$

$$U = \{\theta, 0 \leq \theta(t) \leq 1, t \in [0, T]\}$$
(18)

为求解该最优控制问题, 需要构建目标泛函 $J(\theta)$ 对应的拉格朗日函数, 如式(19)所示。

$$L(I, \theta) = \psi I(t) + \frac{\zeta \theta(t)^2}{2} \quad (19)$$

在此基础上, 下文将证明最优控制的存在性并推导最优控制的解决方案。

1.3.1 最优控制的存在性

若最优控制模型[式(16)]满足文献[22]中定理1的5个引理, 则可判定该模型存在最优控制。以下为各引理的证明过程。

引理1 容许控制集 U 是闭凸集。

证明 由于 U 包含其所有极限点 (根据闭集的定义), 因此 U 是闭集。令 $0 \leq \lambda \leq 1$, 对于 $\theta(t_1)$ 、 $\theta(t_2)$, $(1 - \lambda)\theta(t_1) + \lambda\theta(t_2) \in U$, 可得 U 是凸集。

引理2 存在 $\theta \in \Theta$, 使得微分动力系统[式(16)]有解。

证明 由于微分动力系统[式(16)]是连续可微且有界的, 因此微分动力系统[式(16)]有解。

引理3 $f(I, \theta)$ 是 θ 的线性函数。

证明 $f(I, \theta)$ 是 θ 的线性函数。

引理4 $L(I, \theta)$ 在 U 上是凸函数。

证明 由于 $L''(I, \theta) = \psi I''(t) + \frac{\zeta(\theta'(t)^2 + \theta(t)\theta'(t))}{2} > 0$, 因此可得 $L(I, \theta)$ 在 U 上是凸函数。

引理5 存在 $\sigma > 1$ 、 $k_1 > 0$ 和 $k_2 > 0$, 使得 $L(I, \theta) \geq k_1 + k_2|\theta|^\sigma$ 。

证明 由拉格朗日函数的定义[式(19)]可知, 其表达式包含状态变量与控制变量的二次项或线性项, 显然存在 $\sigma > 1$ 、 $k_1 > 0$ 和 $k_2 > 0$, 使得 $L(I, \theta) = \psi I(t) + \frac{\zeta \theta(t)^2}{2} \geq k_1 + k_2|\theta|^\sigma$ 。

1.3.2 最优控制的解决方案

为找到最优控制的解决方案, 引入该模型的 Hamilton 函数, 如式(20)所示。

$$H(t) = L(I, \theta) + \lambda_1[\delta - \beta SI + \alpha R - \mu S] + \lambda_2[\beta SI - \theta(t)I - \mu I] + \lambda_3[\theta(t)I - \alpha R - \mu R] \quad (20)$$

其中, $\lambda(t) = (\lambda_1(t), \lambda_2(t), \lambda_3(t))$ 为伴随向量。

定理4 $\theta^*(t)$ 为最优控制系统[式(16)]的最优控制, 存在 $\lambda(t) = (\lambda_1(t), \lambda_2(t), \lambda_3(t))$ 满足式(21)的条件。

$$\begin{cases} \frac{d\lambda_1}{dt} = \lambda_1\beta I + \lambda_1\mu - \lambda_2\beta I \\ \frac{d\lambda_2}{dt} = \lambda_1\beta S - \lambda_2\beta S + \theta(t) + \mu - \lambda_3\theta(t) \\ \frac{d\lambda_3}{dt} = -\lambda_1\alpha + \lambda_3\alpha + \lambda_3\mu \\ 0 \leq t \leq T \\ \lambda_1(T) = \lambda_2(T) = \lambda_3(T) = 0 \end{cases} \quad (21)$$

此外, 最优控制可表示为式(22)。

$$\theta^*(t) = \max \left\{ \min \left\{ \frac{\lambda_2 - \lambda_3}{\varpi}, 1 \right\}, 0 \right\} \quad (22)$$

证明 根据 Pontryagin 最小值原理^[23], 最优控制须满足 Hamilton 函数取最小值的条件, 即式(23)成立。

$$\begin{cases} \frac{d\lambda_1}{dt} = -\frac{\partial H}{\partial S}, 0 \leq t \leq T \\ \frac{d\lambda_2}{dt} = -\frac{\partial H}{\partial I}, 0 \leq t \leq T \\ \frac{d\lambda_3}{dt} = -\frac{\partial H}{\partial R}, 0 \leq t \leq T \end{cases} \quad (23)$$

因此满足式(21)的条件, 且满足 $\lambda_1(T) = \lambda_2(T) = \lambda_3(T) = 0$ 。此外, 通过求 H 对 θ 的偏导数, 可得式(24)所示的控制方程。

$$\frac{\partial H}{\partial \theta} = \varpi \theta^*(t) - \lambda_2 I^* + \lambda_3 I^* = 0 \quad (24)$$

2 数值模拟

本节通过数值模拟分别分析第1.2节已通过理论验证的无毒平衡点的稳定性及有毒平衡点的局部渐进稳定性。

2.1 无毒平衡点的稳定性

假设给定参数 $\beta=0.0003$ 、 $\gamma=0.007$, 根据式(9)可得 $R_0 = 0.043 < 1$ 。根据定理1和2可知, 系统在无毒平衡点 E_0 处具有全局稳定性。当初始条件 $((S(0), I(0), R(0))=(0.8, 0.1, 0.1))$ 时, 借鉴文献[8]的实验分析结果, 对系统进行数值模拟, 得到 S 、 I 、 R 节点随时间变化的比率曲线如图3所示。从图3可以看出, 随着时间的推移, S 节点的比率最终

稳定为1, I 节点和 R 节点的比率均稳定为0。进一步分析表明, 无论初始状态取何值, 系统的最终稳定状态均一致, 即收敛至 $((S(0), I(0), R(0))=(1, 0, 0))$ 。上述数值模拟结果与定理1和2的理论结论完全吻合, 验证了理论分析的正确性。

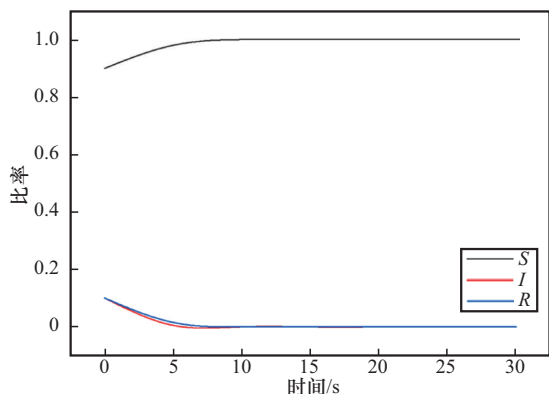


图3 S, I, R 节点随时间变化的比率曲线
Figure 3 Ratio curves of S, I , and R nodes over time

2.2 有毒平衡点的局部渐进稳定性

假设给定参数 $\alpha=0.3$ 、 $\beta=0.6$ 、 $\gamma=0.5$ 、 $\mu=0.2$, 根据式(9)可得 $R_0 = 1.2 > 1$ 。当初始条件 $((S(0), I(0), R(0))=(0.6, 0.2, 0.2))$ 时, 对系统进行数值模拟, 得到 S, I, R 节点随时间变化的比率曲线如图4所示。从图4可以看出, 随着时间的推移, S 节点的比率最终稳定为0.85, I 节点的比率稳定为0.057, R 节点的比率稳定为0.093。上述数值模拟结果与定理3的理论结论完全吻合, 验证了理论分析的正确性。

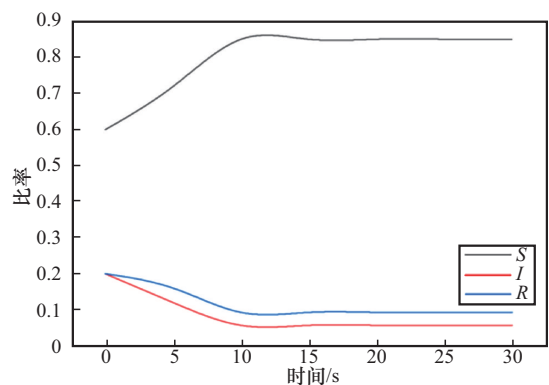


图4 S, I, R 节点随时间变化的比率曲线
Figure 4 Ratio curves of S, I , and R nodes over time

3 实验分析

为验证本文所提模型的有效性, 本节以

GRFICS^[24]作为测试环境开展验证实验。GRFICS的体系结构如图5所示, 包含SCADA BR、工作站、防火墙、可编程逻辑控制器(programmable logic controller, PLC)及物理过程5个部分^[12], 且所有部分均通过虚拟机仿真实现。其中, SCADA BR、工作站与PLC之间虽设有防火墙, 但二者均可穿透防火墙与PLC通信; PLC则通过阀门、传感器对反应器进行控制。图5中, PT为压力传感器, AT为反应器内气体A含量传感器, LT为液体传感器, FT为流量传感器。

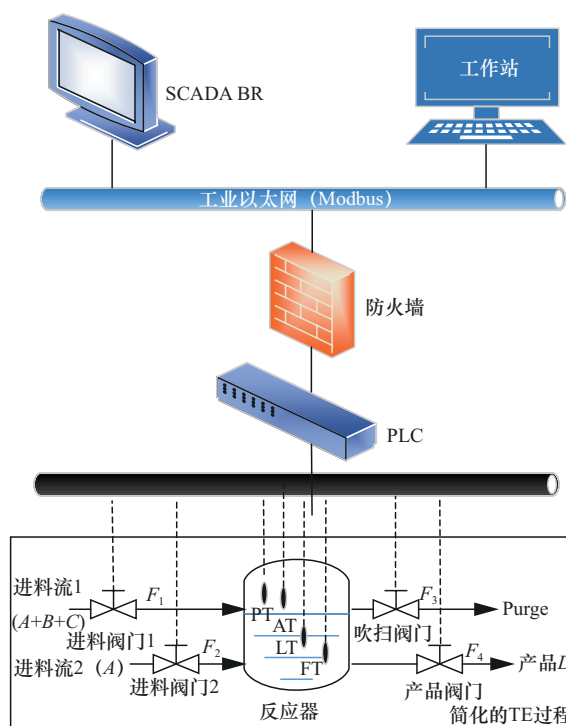


图5 GRFICS的体系结构
Figure 5 GRFICS architecture

通过查阅CVSS数据库, 获取了各设备的脆弱性信息, 具体如表1所示。由表1可知, 任一设备均存在一个或多个脆弱性。

3.1 无毒平衡点的全局稳定性

为进一步验证无毒平衡点的全局稳定性, 本节采用与第2.1节相同的参数设置: $\beta=0.0003$ 、 $\gamma=0.007$ 。由于测试系统包含5个节点, 当初始条件 $((S(0), I(0), R(0))=(0.6, 0.2, 0.2))$ 时, 对应的节点数量为易感节点3个、感染节点1个、恢复节点1个。考虑到感染节点在系统中所处位置的差异可能对传播过程产生影响, 本文设计了5种不同的初始

表1 设备脆弱性信息
Table 1 Information on equipment vulnerability

编号	设备	脆弱性	脆弱性描述	被利用概率
①	SCADA BR	CVE-2020-1938	Apache Tomcat 文件	3.9
		CVE-2021-26828	任意文件上传	2.8
②	工作站	CVE-2022-31685	身份认证绕过	3.9
③	PLC	CVE-2021-22779	身份认证绕过	3.9
		CVE-2020-7559	远程代码执行	3.9
		CVE-2023-6448	身份认证验证	3.9
		CVE-2019-10910	SQL 注入	3.9
④	pfSense	CVE-2021-41282	远程代码执行	2.8
⑤	HMI	CVE-2020-10920	SQL 注入漏洞	3.9
⑥	HMI, PLC	MAC 与 IP 非静态映射	ARP 脆弱性	3.9
		CVE-2021-4161	Modbus 协议脆弱性	

感染场景，具体如表2所示。

参照文献[25]的算法设置，在仿真过程中，易感节点以0.000 3的概率转化为感染节点，感染节点以0.007的概率转化为恢复节点。由于恢复概率 γ (0.007) 大于感染概率 β (0.000 3)，结合第1.2.1节中关于 $R_0 < 1$ 的结论可知，无论初始感染节点位于系统的哪个位置，风险最终都会逐渐衰减并消失。

3.2 有毒平衡点的局部渐进稳定性

为进一步验证有毒平衡点的局部渐进稳定性，本节采用与第2.2节相同的参数设置： $\alpha=0.3$ 、 $\beta=0.6$ 、 $\gamma=0.5$ 、 $\mu=0.2$ 。当初始条件 $((S(0), I(0), R(0))=(0.6, 0.2, 0.2))$ 时，节点分类情况与表2保持一致。在仿真过程中，易感节点以0.6的概率转化为感染节点，感染节点以0.5的概率转化为恢复节点，各节点以0.2的概率从系统中移除，恢复节点以0.3的概率转化为易感节点。由于此时感染概率 β 大于恢复概率 γ ，结合第1.2.1节中关于 $R_0 > 1$ 的结论可知，风险在系统内不会消失，而是会达到稳定的传播状态。

表2 节点分类情况
Table 2 Node classification situation

易感节点	感染节点	恢复节点
SCADA BR、PLC、pfSense	工作站	HMI
工作站、PLC、pfSense	SCADA BR	HMI
工作站、pfSense、HMI	PLC	SCADA BR
SCADA BR、PLC、HMI	pfSense	工作站
工作站、SCADA BR、PLC	HMI	pfSense

4 结束语

本文围绕ICS的安全风险传播机制展开研究。风险传播机制对于保障ICS的安全稳定运行具有重要的意义，因此本文聚焦于风险传播速度、风险传播范围及风险传播控制3个方面发展研究，具体研究内容如下。首先通过量化攻击方法、设备重要性及防御措施，并分析三者之间的攻防态关系，构建了风险传播速度的量化模型。其次，证明了风险传播的边界特征：当 $R_0 < 1$ 时，系统无毒平衡点 E_0 处具有全局稳定性，这意味着风险会随时间逐渐衰减并最终在系统内完全消失；当 $R_0 > 1$ 时，系统在有毒平衡点 E^* 处呈现局部渐进稳定性，表明风险会在系统内稳定存在并持续传播，不会自行消失。最后，基于最优控制理论，证明了最优控制的存在性，并通过Pontryagin最小值原理推导了最优控制的求解方法。为验证研究结论的可靠性，本文通过数值模拟与实验验证相结合的方式，验证了理论模型的有效性。

参考文献：

- [1] 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.
- [2] 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.
- [3] National institute of standards and technology guide to industrial control system (ICS) security: NIST SP800-82[S]. Gaithersburg: National Institute of Standards and Technology (NIST). 2011.

- [4] ZHANG Q, ZHOU C, XIONG N, et al. Multimodel based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems[J]. IEEE Transactions on Systems, 2016, 46(10): 1429-1444.
- [5] DENG S, ZHANG J T, WU D, et al. A quantitative risk assessment model for distribution cyber-physical system under cyberattack[J]. IEEE Transactions on Industrial Informatics, 2022, 19(3): 2899-2908.
- [6] CÁRDENAS A A, AMIN S, LIN Z S, et al. Attacks against process control systems: risk assessment, detection, and response[C]//Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2011: 355-366.
- [7] CUI Y, QUDDUS N, MASHUGA C V. Bayesian network and game theory risk assessment model for third-party damage to oil and gas pipelines[J]. Process Safety and Environmental Protection, 2020, 134: 178-188.
- [8] ZHU Q Y, ZHANG G, LUO X H, et al. An industrial virus propagation model based on SCADA system[J]. Information Sciences, 2023, 630: 546-566.
- [9] MASOOD Z, SAMAR R, RAJA M A Z. Design of a mathematical model for the Stuxnet virus in a network of critical control infrastructure[J]. Computers & Security, 2019, 87: 101565.
- [10] 散学峰. 斑块环境下传染病模型的传播动力学[D]. 兰州: 兰州大学, 2022.
SAN X F. Propagation dynamics of epidemic models in patchy environments[D]. Lanzhou: Lanzhou university, 2022.
- [11] 周勇. 基本再生数新方法和传染病模型动力学分析[D]. 武汉: 武汉科技大学, 2023.
ZHOU Y. New method for basic reproduction number and dynamics analysis of infectious disease models[D]. Wuhan: Wuhan University of Science and Technology, 2023.
- [12] 王红敏, 韩少云, 魏强, 等. 工业控制系统安全一体化风险评估方法[J]. 物联网学报, 2025, 9(2): 139-151.
WANG H M, HAN S Y, WEI Q, et al. A integrated risk assessment method for industrial control system security[J]. Chinese Journal on Internet of Things, 2025, 9(2): 139-151.
- [13] 刘炆, 田决, 王稼舟, 等. 信息物理融合系统综合安全威胁与防御研究[J]. 自动化学报, 2019, 45(1): 5-24.
LIU T, TIAN J, WANG J Z, et al. Integrated security threats and defense of cyber-physical systems[J]. Acta Automatica Sinica, 2019, 45(1): 5-24.
- [14] AMRO A, GKIOULOS V, KATSIKAS S. Assessing cyber risk in cyber-physical systems using the ATT&CK framework[J]. ACM Transactions on Privacy and Security, 2023, 26(2): 1-33.
- [15] WANG Y M, WANG W H, BAI X X, et al. RRDD: an ATT&CK-based ICS network security risk assessment method[C]//Proceedings of the 2023 2nd International Conference on Networks, Communications and Information Technology. New York: ACM, 2023: 186-192.
- [16] FIRST. Common vulnerability scoring system version 3.1: specification document[R]. 2019.
- [17] ZHOU B X, SUN B J, ZANG T L, et al. Security risk assessment approach for distribution network cyber physical systems considering cyber attack vulnerabilities[J]. Entropy, 2023, 25(1): 47.
- [18] LIU K X, XIE Y F, XIE S W, et al. SEAG: a novel dynamic security risk assessment method for industrial control systems with consideration of social engineering[J]. Journal of Process Control, 2023, 132: 103131.
- [19] WANG Y H, YU B, YU H Y, et al. Automotive cybersecurity vulnerability assessment using the common vulnerability scoring system and Bayesian network model[J]. IEEE Systems Journal, 2022, 17(2): 2880-2891.
- [20] KUMARI S, UPADHYAY R K. Exploring the behavior of malware propagation on mobile wireless sensor networks: stability and control analysis[J]. Mathematics and Computers in Simulation, 2021, 190: 246-269.
- [21] RAJA M A Z, MEHMOOD A, ASHRAF S, et al. Design of evolutionary finite difference solver for numerical treatment of computer virus propagation with countermeasures model[J]. Mathematics and Computers in Simulation, 2022, 193: 409-430.
- [22] BI J C, YANG X F, WU Y B, et al. On the optimal dynamic control strategy of disruptive computer virus[J]. Discrete Dynamics in Nature and Society, 2017: 8390784.
- [23] ATHANS M, FALB P L. Optimal control: an introduction to the theory and its applications[M]. New York: Dover Books on Engineering, 2015.
- [24] FORMBY D, RAD M, BEYAH R A. Lowering the barriers to industrial control system security with GRFICS[C]//Proceedings of the 2018 USENIX Workshop on Advances in Security Education (ASE 2018). Berkeley: USENIX Association, 2018.
- [25] SHAH D, ZAMAN T. Detecting sources of computer viruses in networks[J]. ACM SIGMETRICS Performance Evaluation Review, 2010, 38(1): 203-214.

[作者简介]



王红敏 (1989-), 女, 河南濮阳人, 信息工程大学博士生, 信息工程大学讲师, 主要研究方向为工业控制系统安全入侵检测、风险评估。



魏强 (1979-), 男, 江西南昌人, 信息工程大学教授、博士生导师, 主要研究方向为网络与信息系统安全、软件脆弱性分析、云计算安全、工控系统安全、智能终端安全、软件定义网络等。



王兰敏 (1992-), 女, 河南濮阳人, 天津工业大学博士生, 主要研究方向为智能可穿戴传感器、智能可穿戴服装。