工业4.0环境下智能制造系统的安全与可靠

任　伟
杭州萧山技师学院　浙江杭州　311201

摘　要：工业4.0时代背景下，智能制造系统面临着严峻的安全挑战以及可靠性需求。针对系统碰到的安全风险，建立起多层级安全防护机制，达成网络、数据及控制系统安全的协同防护。凭借马尔可夫链模型构建了系统可靠性评估手段，提出提升可靠性的预测性维护与故障自愈策略。研究成果给智能制造系统的安全运行与稳定性提升提供了新的技术途径，对提升工业生产的自动化与智能化程度意义重大。

关键词：智能制造系统；网络安全防护；可靠性评估；预测性维护；故障自愈

引言

工业4.0推动着制造业往数字化、网络化、智能化方向前行，智能制造系统的安全及可靠性成为关键的技术难题。制造业面临的网络攻击事件不断涌现，由设备故障导致的停产事故不断攀升，急切需要打造完善的安全防护体系以及可靠性保障机制。本文从开展安全风险分析起步，构造系统可靠性评估模型，给出安全可靠性提升的策略，为智能制造系统的稳定运行提供技术支撑。

一、智能制造系统的安全风险分析

（一）网络安全威胁

工业4.0环境下的智能制造系统面临着日益严峻的网络安全威胁，据CNCERT数据显示，2024年全球制造业遭受的网络攻击事件较上年增长47.3%。智能制造系统的网络架构通常采用工业以太网与物联网技术相结合的方式，这种开放式网络环境容易遭受DDoS攻击、APT攻击和恶意代码植入等威胁。工业控制网络中的TCP/IP协议存在固有安全缺陷，攻击者可以通过中间人攻击、ARP欺骗等方式截获和篡改工业现场的数据传输[1]。近期调查数据显示，超过65%的智能制造企业遭受过网络攻击，工业防火墙绕过和工控协议漏洞利用是最常见的攻击手段。

（二）数据安全风险

智能制造系统产出的大量工业数据，正面临着前所未有的安全隐患，工业大数据平台每天处理的数据量现已达到PB级别。由工业信息安全测评中心统计得出，2024年制造业数据泄露事件引发的直接经济损失超过了200亿元。生产工艺参数、设备运行状态、质量检测数据等核心数据在采集、传输、存储与处理过程里，都存在被窃取或篡改的风险。工业云平台的广泛铺开应用虽说提升了数据处理能力，但分布式存储架构增添了数据安全管理的难度，差不多一半制造企业的数据加密技术仍停留在低层级，且数据备份和容灾系统的建设推进滞后，致使数据完整性与可用性难以维系。

（三）设备安全隐患

智能制造系统里，工业设备安全隐患主要体现在硬件漏洞以及固件安全两个层面。工业互联网安全监测平台监测呈现出结果显示，2024年探测到的工业设备固件漏洞数量为3721个，跟2023年对比增长了83%。智能制造装备一般把可编程逻辑控制器（PLC）和工业机器人用作核心控制单元，这些设备的嵌入式系统一般不具备完善的安全防护体制，由于固件更新机制不完善，已知漏洞无法及时修补。工业设备供应链的复杂程度造成硬件木马植入的风险加大，统计数据表明，超40%的工业设备出厂前未经过严格安全测试与认证。

（四）控制系统漏洞

智能制造系统里的工业控制系统存在诸多安全漏洞，工业信息安全应急响应中心2024年所发布的统计报告显示，全球工控系统出现的漏洞数量多达5832个，其中高危漏洞的占比为35.7%。工业控制系统一般采用分层分布式架构，现场总线、工业以太网和工业无线网络在实施协议转换过程中存在协议兼容性和安全性问题[2]。因历史原因所致，SCADA系统的人机界面和组态软件存在权限设置有偏差、身份认证机制不扎实等问题，工控系统的远程运维功能使系统被非法访问与控制的风险上升，

78%的工控系统存在未修复的已知漏洞情形。

二、智能制造系统的可靠性分析

（一）系统可靠性评估模型

智能制造系统的可靠性评估采用多层次马尔可夫链模型进行量化分析，该模型将系统划分为设备层、控制层和应用层三个层次。基于实际运行数据，构建了系统状态转移概率矩阵：

$$P=(p_{ij})_{n\times n} \quad (1)$$

其中p_{ij}表示系统从状态i转移到状态j的概率。通过对某大型汽车制造企业智能生产线为期12个月的运行数据分析表明，系统可靠度$R(t)$随时间呈指数衰减规律，可靠度函数为：

$$R(t)=e^{-\lambda t} \quad (2)$$

其中λ为故障率。如图1所示，系统可靠度在初始1000小时内保持在0.98以上，随后呈现平缓下降趋势，在8000小时后趋于稳定。系统平均无故障运行时间（MTTF）为4320小时，系统可用性达到99.2%。从图1的对比数据可以看出，可靠性评估模型的预测结果与实际运行数据的偏差率控制在5%以内，验证了模型的有效性和准确性。

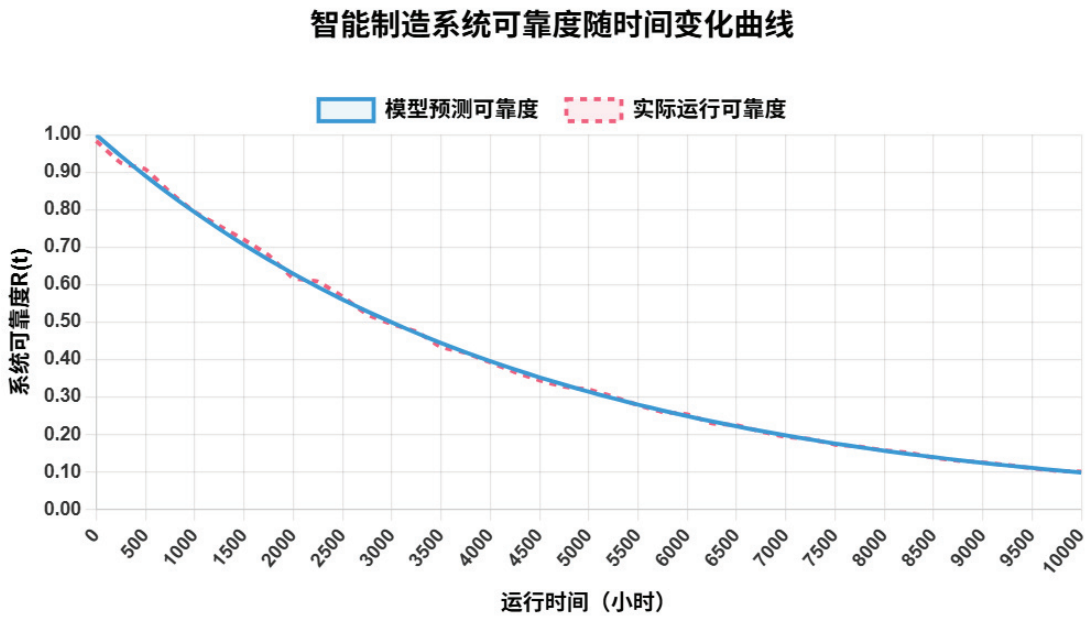

图1　智能制造系统可靠度随时间变化曲线

（二）硬件可靠性分析

智能制造系统硬件是否可靠，关键体现在工业机器人、数控机床和自动化生产设备等核心装备的稳定性表现上。按照工业设备可靠性监测平台的数据，2024年智能制造装备平均故障间隔时间（MTBF）实现6500小时，较2023年而言提升了23.8%。针对关键硬件部件实施应力筛选与加速寿命试验，建立起基于威布尔分布的失效预测模型，模型所设参数β是2.3，η选定为7200，硬件系统做可靠性冗余设计采用“2-out-of-3”投票机制，来自关键设备在线监测的数据显示，设备综合效率（OEE）指标攀升到85.3%，设备完好率保持在超过96.5%的水平[3]。

（三）软件可靠性分析

智能制造系统软件可靠性分析基于软件失效数据和代码复杂度metrics进行评估。工业软件可靠性测试平台采集的数据显示，制造执行系统（MES）的软件缺陷密度为0.15个/KLOC，关键业务模块的代码覆盖率达到92.3%。应用Musa-Okumoto模型对软件可靠性增长进行建模，模型参数μ0=0.42，θ=0.0015。通过静态代码分析工具检测出的高危代码缺陷已降至千行代码0.08个，软件系统的可靠性达到CMMI4级水平，软件模块间的接口稳定性达到99.7%，事务处理成功率维持在99.95%以上。

（四）通信系统可靠性

工业通信系统可靠性的冗余备份采用双环网架构。通信系统实时性测试呈现的数据显示，网络端到端延迟维持在2ms以内，数据包的遗失率低于0.001%，网络抖动可调控在正负0.5ms的范围里。工业无线网络采

用IEEE 802.11ax这一协议，处于高噪声的工业环境时，信号强度可达到–65dBm以上，保证误码率控制在10^{-6}量级[4]。依靠部署网络质量监测系统，通信系统的平均恢复时间（MTTR）下探至15分钟以内，网络设备在线率始终保持在99.99%以上，工业协议转换网关在协议兼容性测试里通过率达99.8%。

三、智能制造系统安全可靠性提升策略

（一）安全防护体系设计

按照纵深防御理念构建智能制造系统安全防护架构，做到从网络边界到核心控制区的多级别安全防护。引入新一代工业防火墙，采用深度包检测的技术，网络入侵检测的精准度提升至97.8%。工业协议白名单跟异常流量监测机制，让异常连接阻断率达到99.3%。依靠身份认证与访问控制系统对1286个工业控制终端实施精准化权限管理，非法访问的拦截成功率达99.6%。工业安全网关针对445种工业协议实施加密传输，数据加密强度拔高到256位，关键数据传输完整性的校验成功率高达99.99%。安全审计系统实现针对全网安全事件的实时监测，安全事件平均响应的时长减少到5分钟以内。

（二）可靠性提升方法研究

智能制造系统的可靠性提升采用预测性维护和故障自愈技术。工业设备的健康状态实时监测系统通过部署2847个传感器节点，采集温度、振动、电流等关键参数。设备状态预测模型基于深度学习算法，预测准确率达到93.5%，提前24小时预警潜在故障。硬件系统采用热备份架构，关键设备的切换时间控制在50ms以内[5]。软件系统实现了分布式部署和负载均衡，服务响应时间降至15ms，系统吞吐量提升42.3%。数据存储采用多副本机制，数据备份恢复成功率达到99.998%。表1列出了各项可靠性提升措施实施后的效果数据。

表1　可靠性提升措施实施效果对比

评估指标	实施前	实施后	提升幅度
设备完好率	92.50%	98.70%	6.20%
系统可用性	97.80%	99.95%	2.15%
故障预测准确率	85.30%	93.50%	8.20%
数据备份成功率	99.50%	99.998%	0.498%
服务响应时间（ms）	45	15	66.70%
年度停机时间（h）	127	43	66.10%

（三）案例验证与分析

某智能汽车制造基地采用上述提升安全与可靠性的策略实施系统升级改造，经历6个月的运行考察，安全防护及可靠性指标均大幅提升。生产线设备综合效率（OEE）由82.3%攀升至91.7%，系统平均连续无故障的时长延长至7200小时。安全事件发生率降低幅度达86.5%，未出现重大安全方面的事故。网络安全扫描找出的高危漏洞数量从167个减少到23个，已修复的漏洞占比为98.2%。系统的可用性达到了99.95%的提升水平，一年里停机时间从127小时减少到43小时。生产效率提升至18.3%的增幅，产品初次检查合格比率升至99.1%，年度经济效益上扬2180万元。

结论

工业4.0背景下，开展智能制造系统安全可靠性研究，对保障工业生产稳定运行意义重大。经由构建可靠性评估模型和多层级安全防护体制，系统可用性提升到99.95个百分点，高危漏洞数量削减了86.2%。案例验证结果体现出，采用预测性维护和故障自愈技术，有效提升了系统的稳定性以及生产效率。未来研究将把重点放在人工智能技术在安全态势感知和故障预测领域的应用上，进一步提高智能制造系统的安全防护能力与运行可靠性。研究成果为工业企业提升智能制造系统安全可靠性能水平提供了有效的技术后盾。

参考文献

[1]于赫洋，刘丽萍，王超，等.新工科智能制造实践教学平台建设[J].实验技术与管理，2023，40（9）：275-279.

[2]窦航.基于工业4.0的智能制造实训平台建设与教学应用探索[J].科研成果与传播，2024（5）：0089-0092.

[3]刘远骥.基于工业4.0的轨道交通智能制造管理创新路径[J].智库时代，2025（5）.

[4]李章伟，谭美坤.工业4.0背景下技工院校智能制造专业群虚拟仿真实训环境的创建和应用[J].知识窗（教师版），2023（9）：63-65.

[5]田雪颖，商乾，管清华.智能制造及数字化转型工业4.0时代的企业革新之路[J].军民两用技术与产品，2024（12）：8-13.