工业控制系统功能安全和信息安全融合研究综述

刘圃卓[1,2], 马叶桐[1,2], 吕世超[1,2], 方栋梁[1,2], 朱红松[1,2], 孙利民[1,2]

[1] 中国科学院大学网络空间安全学院 北京 中国 100049
[2] 中国科学院信息工程研究所 物联网信息安全技术北京市重点实验室 北京 中国 100093

摘要 随着工业互联网的快速发展, 工业控制系统(ICS)中功能安全和信息安全分离的传统防御方案已经无法应对当前的网络威胁。例如, Stuxnet 病毒利用信息领域的安全漏洞修改离心机业务运行的相关参数, 使其运行于不稳定状态, 最终导致系统瘫痪。为了应对日益复杂的高级威胁, 针对功能安全和信息安全的融合技术逐渐成为研究热点。该融合技术产生一体化的安全需求, 使风险分析和缓解更加全面和有效, 同时减少系统性能开销和开发运行成本。然而, 需要注意的是, 功能安全和信息安全具有不同的目标和要求。功能安全旨在避免系统功能故障造成的不可接受风险, 而信息安全旨在保护计算机硬件、软件和数据免受意外和恶意的损害、更改和泄露。此外, 工业控制系统的计算、通信和存储资源受限, 具有时效性、行业复杂性和设备多样性等特点。因此, 融合安全研究面临重大挑战。本文首先从概念术语、安全生命周期、安全级别评估和缓解措施等 4 个方面分析了功能安全和信息安全领域融合安全研究的可能性和必要性。其次, 根据保密性、完整性、可用性和可靠性 4 个安全目标, 总结和分析了学术界和工业界现有的融合安全方法和技术进展, 以及现有的功能安全和信息安全融合标准和计划。最后, 从不同的角度分析和总结了功能安全和信息安全融合研究中的挑战和机遇, 以促进不同学科之间的跨学科研究。

关键词 功能安全和信息安全融合; 工业控制系统; 信息物理融合系统
中图法分类号 TP29 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2026.01.19

Survey on the Integration of Safety and Security in Industrial Control Systems

LIU Puzhuo[1,2], MA Yetong[1,2], LV Shichao[1,2], FANG Dongliang[1,2], ZHU Hongsong[1,2], SUN Limin[1,2]

[1]School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
[2] Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract With the rapid development of the industrial Internet, the traditional defense scheme that separates functional safety and information security in industrial control systems (ICS) can no longer cope with current Internet threats. For example, the Stuxnet virus uses the security vulnerabilities in the information domain to modify relevant parameters of centrifuge business operations to make it run in an unstable state, ultimately leading to system destruction. In order to deal with increasingly complex advanced threats, the fusion technology for functional safety and information security has gradually become a research hotspot. This fusion technology generates integrated requirements, enabling comprehensive and effective risk analysis and mitigation, while reducing system performance overhead and development and operation costs. However, it is important to note that functional safety and information security have different goals and requirements. Functional safety aims to avoid unacceptable risks caused by system functional failures, while information security is designed to protect computer hardware, software, and data from accidental and malicious damage, changes, and leaks. Additionally, industrial control systems have limited computing, communication, and storage resources, and are characterized by time sensitivity, complexity in industry, and diverse equipment. Moreover, due to the limited computing, communication, and storage resources of industrial control systems, as well as their characteristics of time sensitivity, complex industry, and diverse equipment, fusion research is faced with significant challenges. This paper first analyzes the possibility and necessity of converged security research from the four aspects of conceptual terminology, security life cycle, security level assessment and mitigation measures in the field of functional safety and information security. Then, according to the four security objectives of confidentiality, integrity, availability and reliability, the existing fusion security methods and technical progress in academia and industry are summarized and analyzed, and the existing functional security and information security fusion standards and plans. Finally, the challenges and opportunities in the fusion research of functional safety and information security are analyzed and summarized from different perspectives, so as to promote interdisciplinary research between different disciplines.

通讯作者: 吕世超, 博士, 高级工程师, Email: lvshichao@iie.ac.cn。
本课题得到国家重点研发计划(No. 2020YFB2010902), 国家自然科学重点基金(No. U1766215)资助。
收稿日期: 2020-12-11; 修改日期: 2021-03-08; 定稿日期: 2023-02-16

Key words safety and security integration; industrial control system; cyber-physical system

1 引言

工业控制系统 (Industrial control system, ICS) 在国家基础设施建设过程中被广泛应用, 扮演着能源、交通和其他自动化工业过程中的重要角色, 因此, 系统安全性保护一直是研究的重点。随着工业需求的不断发展, 为了降低工业控制设备在部署、维护和操作等方面的成本, 同时提高生产效率, 信息技术和通信设备逐步集成到系统架构中, 从而提高设备之间和系统之间的互联互通性。随工业互联网、工业物联网、智能制造等概念相继被提出[1]。根据 IEC-62443 标准工业控制系统可划分为 5 个层次, 如图 1 所示[2]。其中, 企业系统层属于传统互联网技术(Internet technology, IT), 组织和管理工业生产所需业务的相关活动, 其促进了业务功能之间的信息流动, 并管理与外部利益相关者的联系; 运行管理层负责生产调度、生产统计、资源管理及可靠性保障等; 监测控制层主要负责监测和控制生产过程, 包括人机接口、数据采集、监测控制等, 通过使用标准协议与远程终端单元(Remote terminal unit, RTU)通信, 完成地理上分散的系统收集信息; 基本管理层通过可编程逻辑控制器(Programmable logic controller, PLC)、可编程自动化控制器(Programmable automation controller, PAC)等设备提供逻辑控制功能, 完成对过程层设备的周期性信号采集和执行器控制的任务, 并且提供功能安全和相关的保护措施; 过程层包括各种类型的传感器和执行器, 例如: 温度传感器、伺服电机等, 它们负责对物理空间的各类信号进行感知和采集, 并完成生产和控制任务。

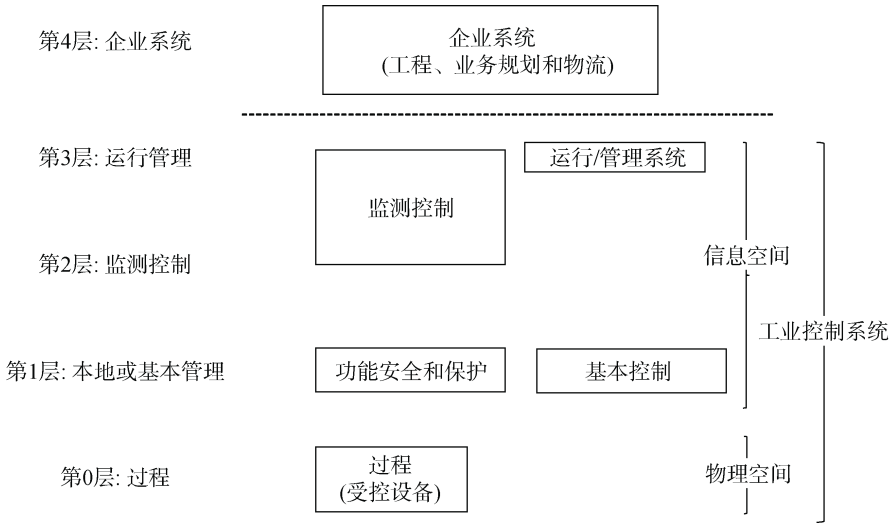

图 1 工业控制系统

Figure 1 industrial control systems

在工业控制系统未接入互联网之前, 工厂内部利用总线协议进行通信, 工厂和外界是物理隔离的状态。因此一直将安全防护的重点置于功能安全(Safety)之上, 功能安全主要应对系统故障和随机失效带来的可能对环境、系统、人员造成损伤的风险, 并对误操作、重复操作或多路控制等方面提供安全处理机制, 保障系统的稳定运行。控制系统从未考虑外界对系统的风险, 系统中存在通信明文传输、无认证等情况。因此在工业企业升级换代的大环境中, 信息安全(Security)领域的风险对设备的威胁日益突出, 恶意人员主动利用系统中的脆弱性, 破坏或降低系统的机密性、完整性和可用性。工业控制系统不再是过去隔离即安全的时代。经过不断的升级, 其从单体安全晋升到纵深防御保护体系, 通过划分网络区域并增加安全网关、防火墙和入侵检测设备等外围安全设备来构建防御体系。近年来针对工业控制系统的入侵和攻击呈现快速增长趋势。如图 2 所示, 2010~2019 针对工业控制系统攻击的报告以及漏洞数量的趋势可以反映攻击态势[3-4]。同时越来越多的攻击工具例如 AutoSploit[5]、ICSSPLOIT[6]等都提供针对 ICS 的漏洞利用模块, 根据火眼最新发布的工控系统安全报告, 工控系统攻击工具的大量涌现使得普通黑客也能实施过去需要特殊知识和高级黑客技术的工控系统攻击[7], 并且黑客大会上也出现针

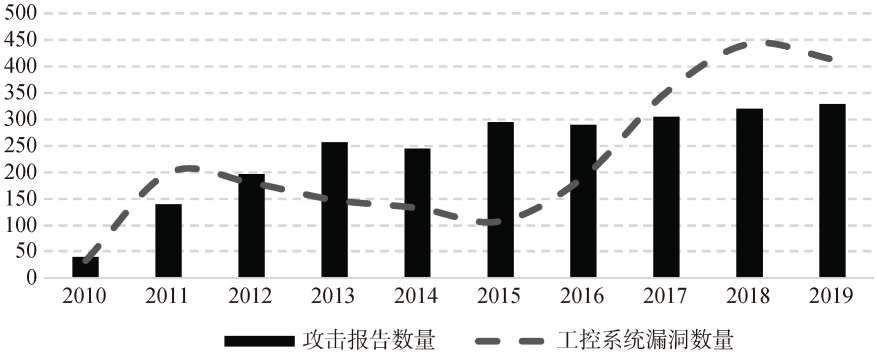

图 2　工业控制系统威胁趋势

Figure 2　Industrial control systems threat trends

对工业控制设备的研究, 例如针对西门子 PLC 后门的发现[8-9], 未来工控系统安全形势变得极为严峻。

2019 年, 发生了 30 多起重大影响工控安全的事件, 其中包括委内瑞拉水电站遭到网络攻击、乌克兰某核电厂发生严重网络攻击事故等[10]。回顾 Stuxnet 病毒可以发现, 虽然工控系统内部具备风险检测和缓解措施, 但是攻击者会构造看上去合法的操作去控制设备, 利用信息层的漏洞来破坏物理层的设备, 进而对系统造成损伤。因此, 功能安全和信息安全的独立发展已经无法适应当前的威胁环境[11]。工业控制系统是一个复杂系统, 信息安全领域风险可以进一步威胁功能安全领域, 风险进而由信息域传递到物理域。近年来, 国内外的研究人员提出了工业控制系统内生安全和本体安全的概念, 其本质是功能安全与信息安全的融合, 也是从被动防御升级为主动防御。因此, 本文介绍了学术界和工业界在功能安全和信息安全融合研究工作方面的进展。

本文的组织结构如下: 第 2 节首先介绍了功能安全和信息安全的定义及各自的安全目标, 并从不同角度分析了它们之间的关系, 同时对在融合过程中可能出现的矛盾进行了分析; 第 3 节归纳总结了已有的融合安全方法和技术; 第 4 节从安全标准和实施方案的角度总结了功能安全和信息安全融合的进展; 第 5 节对融合安全研究存在的难点进行了归纳总结, 并展望了未来的发展趋势; 第 6 节对全文进行了总结。

2　功能安全和信息安全的关系分析

由于工业控制系统具有行业复杂性、设备多样性和跨学科性等特点, 且功能安全和信息安全长期处于独立发展状态, 因此在融合安全研究过程中可能存在多个方面冲突, 如概念术语、评估模型和缓解措施。本节将分别对功能安全和信息安全相关的概念、定义、安全等级评估、风险缓解措施等方面进行总结和介绍, 并对二者在融合过程中各个方面的可能关系进行分析。

2.1　功能安全

在IEC-61508标准中, 工业控制系统的功能安全被定义为“功能安全是受控设备或受控设备系统总体安全中的一部分, 其安全性是依赖于电气/电子/可编程电子安全相关系统、其他技术的安全相关系统或外部风险降低措施的正确机能”[12]。功能安全的目标是保护环境、人员、系统不因随机失效或系统性失效造成损伤。其中随机失效包括硬件磨损和人员误操作等可能带来的风险; 系统性失效包括硬件设计和软件实现中存在的风险。

功能安全的实施过程可以用安全生命周期来描述, 该过程覆盖系统功能安全从需求分析到停止使用的整个生命周期。具体而言, 功能安全生命周期内容主要包括以下步骤: 确定保护目标和资产范围, 编制相应的安全需求, 利用故障树、马尔可夫模型等风险评估方法识别风险并评估风险的严重程度, 最终确定目标安全等级; 然后根据安全需求分配对应的安全要求并制定安全要求规范; 再进行安全系统和安全软件的实现, 系统实现之后重新进行风险分析和评估以确保安全功能满足目标要求, 如不满足需要重新进行风险分析和安全设计, 直至满足要求后进行安装调试和使用[13]。

为了能够衡量产品抵御风险的能力, 同时方便根据产品的应用场景进行成本与能力的平衡。DEFSTAN 在 1991 年引入安全完整性等级(Safety integrity level, SIL)的概念[14], IEC-61508、IEC-61511 等大部分与功能安全相关的标准都采用这一概念。安全完整性等级的定义是由安全机能所降低风险的相对水准。通过度量安全完整性量值的范围, 通常将其分为 SIL 1(最低)至 SIL 4(最高)4 个不同级别。在

SIL 等级中可以使用 ALARP 原则、风险图法、保护层分析法、危害事件严重程度矩阵等方法确定安全等级。安全完整性包括硬件安全完整性、系统安全完整性和软件安全完整性。硬件安全完整性等级受限于硬件故障裕度(Hardware fault tolerance, HFT)和安全失效分数(Safe failure fraction, SFF)的约束, 它们分别反映系统的硬件容错能力和在线诊断能力。同时还需要估算由随机硬件失效引起的风险概率, 该概率应该低于安全目标等级的失效量。在估算过程中需要结合系统结构、工作模式等分析失效因子并估算失效率。系统安全完整性包括避免失效要求: 通过对使用技术和措施的细化要求避免在安全相关系统的设计和开发期内引入故障; 控制系统故障要求: 在设计安全相关系统过程中需要考虑到对残余风险的容忍度以及系统的可维护性和可测试性; 故障检测时对系统行为要求: 在检测出的危险故障应保证系统维持或进入安全状态, 同时计算平均修复时间等指标。软件安全完整性除传统计算机使用的系统和软件外, 还包含对可编程电子器件中使用的配置文件的相关要求。不同的软件安全等级对软件开发过程中使用的设计方法、架构和语言、测试方法等进行了详尽的描述。

功能安全领域所应对的风险可以分为两类:系统失效和硬件失效, 二者的机制不同, 因此对应的缓解措施也不同。针对系统失效, 主要通过改变设计和操作模式、操作指令或其他影响因子来避免失效, 例如使用防御性编程技术; 而针对硬件失效, 主要是通过并联冗余来避免, 使用冗余的硬件来执行相同的功能来实现系统防护。功能安全提供由内向外的安全保护机制, 其第一道防线是系统功能本身的安全措施, 因为功能安全的风险来源是系统内部。此外, 功能安全还会需要预防因操作失误而带来的风险, 例如操作员非故意造成的与工作流程不符或可能对设备和人员造成损害的操作。为此, 通常会通过监测设备状态、监测异常行为、划分人员权限和危险操作双重确认等机制来避免这些风险的发生。

2.2 信息安全

在工业控制系统中, IEC-62443 标准给出了信息安全的定义, 包括以下 5 个方面: 1) 保护系统所采取的措施; 2) 由建立和维护的保护系统措施所得到的系统状态; 3) 能够免于对系统资源非授权访问和意外的变更、破坏或损失; 4) 基于计算机系统的能力, 能够保证非授权人员和系统既无法修改软件及其数据, 也无法访问系统功能, 却保证授权人员和系统不被阻止; 5) 防止对工控系统的非法和有害入侵, 或干扰系统正确和计划的操作[2]。信息安全目前在 IT 领域和传统计算机方面已经发展相对成熟, 但在工业控制系统中起步较晚, 且限制条件苛刻。因此, NIST SP 800-82 标准对工业控制系统和计算机系统在信息安全方面进行了详细的比较和分析, 并提供了适用于工业控制系统的安全建议[15]。

信息安全的生命周期可以分为 3 个阶段: 评估阶段、开发和实施阶段、维护阶段。在评估阶段, 通常采用基于风险的方法进行需求分析。通过使用攻击树或错误用例等方法, 识别可能对系统造成威胁的脆弱点。然后结合法律、网络功能等方面创建安全需求, 目的是降低攻击成功的概率或减轻攻击造成的影响。在开发阶段, 选择合适的开发语言进行功能开发并测试, 以满足系统安全和性能需求。同时进行脆弱性和攻击面的分析, 使评估与开发工作进入循环状态, 直至满足目标安全需求。维护阶段包括补丁管理、发布新版本等工作。

ISA 99 引入了安全等级(Security level, SL)的概念, 该概念在提出时是模仿功能安全中安全完整性等级概念用于信息安全的等级评估[16]。该方法定义 7 个基本要求: 身份和授权控制、使用控制、数据完整性、数据保密性、受限数据流、事件实时响应、资源可用性, 根据设定的目标安全等级给予针对这 7 个方面的安全建议。在实施过程中安全等级分为目标安全等级、已达成安全等级和能力安全等级。目标安全等级是开发人员希望赋予系统的安全能力, 根据具体的系统级和组件级的安全要求进行实施, 例如安全等级 1 要求系统必须对人类用户进行身份验证和授权, 安全等级 2 中则增加对软件和设备的身份认证和授权; 在设计和实现之后, 对系统进行测量判断已达成的安全等级, 不符合要求则重新设计; 在最终部署之后, 可能会受到其他因素的干扰, 因此其实际提供的安全功能是能力安全等级。

在信息安全领域, 应对风险的方式是通过划分网络区域, 并在管道处采用串联异构来建立保护边界来实施的, 例如, 在通信链路中增加防火墙设备、入侵检测设备、加密设备等可以增加多层的保护措施, 以保护外界接入设备或设备传递信息的过程。然而, 加解密、认证等一系列安全措施会增加数据的处理时间, 因此, 应根据资产的重要程度划分网络区域并构建不同级别的保护方法, 这样不仅可以减少不必要的系统性能开销, 也可以减少开发成本。信息安全提供由外向内的保护技术, 其第一道防线是最外层的防火墙, 因为信息安全需要应对来源于外部的风险, 所以保护外部网络是非常重要的。在这种保

护模式下, 外部网络的风险可以通过防火墙和其他保护措施来隔离和降低, 从而确保内部网络的安全。

2.3 关系分析

本节旨在总结和概述功能安全和信息安全领域中涉及的概念术语、安全生命周期、安全等级评估和缓解措施等 4 个方面的融合研究。我们将从不同的角度分析这两者之间的关系, 并讨论融合的可能性和必要性。

2.3.1 概念术语

随着功能安全和信息安全融合的趋势不断增强, 研究人员从概念和术语层面进行了二者融合的可能性分析。然而, 由于不同的安全观念导致不同的术语被用于相似的概念, 甚至相同的术语被用于略有不同的含义, 同时由于各国语言的差异也增加了术语误用的概率, 因此对概念术语的分析是解决明显冲突或趋于融合的第一步。

研究人员 Line 等通过对两个领域使用的术语进行共性和差异性分析, 认为存在互补的关系, 未来存在融合的可能性[17]; Burns 等从威胁事件的角度出发, 分析安全需求的区别和联系, 认为二者存在很多共性[18]; Piètre-Cambacédès 等使用布尔逻辑驱动马尔可夫过程模型分析风险识别和评估在功能安全和信息安全中的相似性, 认为两个领域存在依赖性[19]。他们还从语言陷阱、文献调研、行业标准中对功能安全和信息安全进行了全面的调研, 认为二者存在很大的相似性[20]。研究人员主要通过辨析描述“风险”和“事件”的相关术语对功能安全和信息安全从概念上进行关系分析, 本节对这两个术语相关内容进行总结。

1) 风险

在功能安全和信息安全领域, 关于“风险”一词存在不同的定义。为了避免在融合过程中产生冲突, 并提高风险分析的准确性, 对“风险”的概念进行明确定义是非常重要的。根据文献[17-18]中提到的相关术语解释总结如下:

风险(risk): 是指事件发生的概率以及事件后果的严重性组合, 对目标产生影响的可能性。风险包括危险事件和威胁事件。

危险(hazard): 是可能对健康、生命或环境造成不良影响的事件, 是造成伤害的根源。

威胁(threats): 是指由故意行为引起的可能造成信息丢失或功能失效等情况发生的事件。

可见, 关于“风险”的不同术语在其影响目标和衡量影响方面存在区别。风险是一个总体描述词, 其衡量与其发生概率和影响程度存在关联。功能安全风险评估是对非人为引起的具有风险的事件, 而信息安全则是对外部威胁进行评估。信息安全和功能安全划分为两个领域最主要的原因是风险的本质不同, 如表 1 所示[21-22]。它们在风险来源、风险影响、风险概率以及风险成因方面都存在很大区别。但是在风险的分析方法和模型方面两个领域存在很多相似性, 例如, 目的都是提出针对风险的安全需求或约束, 这些约束可能与功能和其他与性能相关的需求产生冲突, 因此, 一般会形成循环过程来解决不断产生的矛盾[23]; 在分析流程方面, 两个领域都需要对目标系统进行功能或资产分析, 结合定量或定性的方法对影响进行评估, 并提出缓解措施[24]。风险分析的方法不仅存在很多共性, 而且存在互补性。目前, 存在很多融合研究工作, 将在 2.1 节中进行详细分析。

表 1 功能安全与信息安全面临风险区别

Table 1 Risk difference between safety and security

	功能安全	信息安全
风险来源	系统内部	系统外部
风险影响	对环境、人员、系统造成损伤	信息资产损失 系统功能受损
风险概率	可知, 可预测	未知, 不可预测
风险成因	人员操作失误 随机硬件失效	外部攻击 安全策略配置错误

2) 事件

从安全的角度来看, 采取措施是为了防止系统、环境、人员、信息受到或造成损失和损害。这些安全措施通常是通过技术手段、设计性能和管理程序来实施的, 缓解目标“事件”的发生概率或减小影响程度。由于在功能安全和信息安全领域中衡量“事件”的影响角度和诱因等方面存在差异, 因此存在不同的术语, 具体如下[12,25]:

事态(event): 信息安全中系统、服务或网络状态出现可能违反安全政策、策略或法律的事件, 但没有造成实际损失且没有办法阻止的情况。

事件(incident): 在信息安全领域, 其是指单个或一系列的非预期信息安全事态, 造成或可能造成系统提供服务质量的中断或降低。而在功能安全中是指因系统故障或失效导致不希望的后果发生, 但没有造成生命或环境的永久损害, 且在法律允许的范围内的情况。

事故(accident): 功能安全中系统故障造成生命或环境的损害, 且超出法律允许的范围内的情况。

从上述可以看出, “事件”这一描述词在影响后果方面存在差异。由于信息安全关注的主体是信息本

身, 所以在定义上并没有考虑到对生命或环境的损害, 因此没有事故的定义。然而, 在针对工业控制系统的网络攻击事件中, 即使在不违背功能安全的情况下, 也可能造成生产环境的永久损害。因此, 功能安全和信息安全的融合发展具有必要性。这样可以充分考虑到事件和事故之间的递进关系, 并对不同情况进行合理的描述, 从而使得缓解措施更加合理。

在功能安全和信息安全的概念和术语层面上, 它们之间存在的差异主要是基于对风险性质、保护对象和衡量风险影响角度的不同考虑。然而, 随着 IT 和操作技术(Operational technology, OT)的深度融合, 二者的关系越来越密切。信息安全的威胁逐渐突破自身边界, 可能会对功能安全领域产生威胁, 进而对人、环境、系统造成危害, 反之亦然。因此, 从概念层面上, 功能安全和信息安全逐渐呈现出互补的趋势。通过概念的统一和术语的完善, 可以更加准确和完整地描述风险事件, 从而增强两个领域之间的内在联动性, 并促进安全一体化的发展。

2.3.2 安全生命周期

安全生命周期对于系统或软件的安全防护至关重要, 在设备或软件的设计、评估、实施、使用、维护各个阶段都起到指导作用。在安全生命周期中, 两个领域都采用循环的思想, 整体流程和每个阶段的设计目标具有很大的相似性, 但在不同阶段使用的方法和考虑问题的角度存在差异性。例如, 在设计阶段功能安全会结合考虑设备的工作场景和业务流程, 根据设备业务的特征和风险设定安全需求。而信息安全则结合机密性、完整性等目标考虑信息的重要程度, 并没有结合业务特征。总体来说二者的差异在安全生命周期的设计上并不突出, 因此目前融合工作也取得较大进展。

针对一些特定的使用场景, 例如楼宇控制系统、智能制造等提出融合安全的生命循环周期[26-27], 同时文献[28]将 IEC-61511 标准和 IEC-62443 标准中提出的安全生命周期进行融合, 在需求和实现阶段加入了矛盾和解的步骤, 适用于整个工业控制系统领域。在 2019 年发布的 IEC-63069 标准中提出功能安全和信息安全交互框架[29], 根据安全目标的不同进行需求冲突缓解, 为生命周期融合起到指导作用。2020 年发布 IEC-63325 标准对工业自动化控制系统的功能安全和信息安全提出一体化生命周期要求, 通过引入整体安全指标来权衡功能安全和信息安全的实施, 进行全面的危害与威胁分析[30]。安全生命周期融合对于功能安全和信息安全两个领域而言是一种互利关系, 不仅能够使生命周期更加完善, 而且会在一定程度上节约开发成本, 缩短设计和开发周期。

2.3.3 安全等级评估

在安全等级评估中, 信息安全的思想借鉴于功能安全, 因此存在很多共性。其中最大的区别体现在评估方法方面, 功能安全由于其风险可量化可预测的特点, 在安全等级评估过程中大多采用量化方法, 利用数学公式辅助进行评估, 通过计算故障冗余度、失效概率等确定安全等级。相比之下, 信息安全在发展初期由于缺乏威胁数据的收集, 并且攻击的不可预测性, 因此采用更多的定性方法进行等级评估, 通过提出不同层次的安全要求来执行。但是随着信息安全的发展, 态势感知、入侵诱捕等信息收集系统的部署, 收集的可用数据越来越多, 逐渐可以使用数学方法辅助进行威胁的评估, 对系统在信息安全方面的能力进行评估和验证[31]。文献[32-33]从 SIL 角度出发考虑是否可以对信息安全等级进行评估, 并解释了融合后可能存在的问题, 并提出了融合安全等级评估模型。在安全等级评估方面, 两个领域目前缺乏一体化的评估方法, 但随着可用数据的增加和融合安全的推进, 通过分析安全等级评估方法之间的关联性, 建立融合安全等级评估方法会增加工业控制系统安全性衡量的全面性和可靠性。

2.3.4 缓解措施

在缓解措施方面, 由于功能安全与信息安全所面临的风险性质和防护目标不同, 例如功能安全重点是对生产过程和受控设备进行风险评估和缓解; 而信息安全则关注于生产过程的区域和管道, 重点保护其中的信息资源。因此, 二者应对风险的理念也存在差异, 并体现在防御思想中。这些差异既是融合的动力也是阻碍融合的难点。例如, 功能安全中通过并联冗余的方式缓解硬件随机失效所带来的风险, 而从信息安全角度来看, 这无疑增加了攻击路径, 使系统中存在后门、漏洞等脆弱点的可能性增加。但是通过并联不同的软件或设备执行相同的功能, 在提高系统可用性的同时, 也提高了系统的复杂度, 因此攻击者需要付出更多的代价去了解系统, 进而起到防御的作用。

如何平衡功能安全和信息安全缓解措施在融合过程中产生的问题是研究的重点, 不同缓解措施之间存在不同的关系, 甚至具有多种关系, 文献[28]将它们的关系分为: 互利、无关、包含和冲突, 在融合过程中考虑安全功能彼此产生的影响; 通过分析缓解措施之间的影响和关系, 解决可能存在的矛盾是一体化安全协调方案中重要的一步[34]; 同时需要结

合性能和需求去考虑安全功能的设计与部署, 因为安全功能的实施无疑会增加性能的开销, 所以需要确定缓解措施是否有必要在单体设备中实施, 或是确定在系统架构下的哪些关键位置实施。在缓解措施的融合中, 不同的方法存在互斥互利的关系, 通过对共性安全技术进行融合和个性安全技术进行改进, 必定会对工业控制系统的成本、性能及安全性等方面带来益处, 详细的融合安全方法和技术将在第 3 节中进行对比介绍。

3 融合安全方法与技术

在功能安全和信息安全融合的过程中, 最终的研究目标是找到一种可融合的安全方法或技术, 能够在不影响正常业务的情况下有效抵御风险。然而, 由于工业控制系统自身的特点对融合安全研究造成了挑战。例如, 信息物理融合的特点意味着不能仅考虑信息层的风险传播和影响, 还需要结合物理层进行全方位的考虑; 流程作业的特点导致设备之间存在依赖关系, 因此模型的复杂度相对较高; 同时, 工业控制系统对时间和可用性的敏感程度高于传统 IT 系统, 且嵌入式设备的大量使用带来了运算和存储能力方面的限制[35], 这使得风险缓解措施的设计面临更高的要求。此外, 功能安全和信息安全在防护目标和风险性质等方面存在差异, 可能导致缓解措施存在冲突的可能性。因此, 目前学术界和工业界尚未形成一套完善的融合防御体系, 但存在一些值得参考借鉴的融合思想。本节将安全方法和技术分为两类: 风险评估方法和风险缓解技术。在风险缓解技术中, 根据安全目标将其分为完整性、机密性、可用性和可靠性进行分类和总结。

3.1 风险评估方法

功能安全和信息安全都利用风险评估方法来帮助确定系统的安全需求。风险评估在整个安全防护体系中是基础环节, 评估模型能否全面地识别系统面临的风险输入, 对风险传播过程的假设和模拟是否合理和有效, 以及对风险影响的评估是否正确, 将直接影响到后期缓解措施的有效性和合理性。同时, 风险评估方法的选择还会对开发时间、人力成本、系统性能和安全等级产生影响。在 2.3.1 节中已经对风险的概念进行了分析, 本节将介绍功能安全和信息安全领域中关于风险评估模型和方法融合工作的进展与思路。

在设计一个新系统或检查一个现有系统时, 都需要进行风险分析, 功能安全和信息安全领域从不同角度考虑风险, 功能安全从系统内部出发考虑系统功能和设备本身失效或操作失误对环境、资产和人员带来的风险, 而信息安全则考虑由于系统存在的脆弱性, 被外部人员恶意利用带来的风险。但它们的分析过程存在相似性。例如, 对可能造成危害或存在的脆弱性进行分析, 对潜在后果和产生的影响进行评估等。功能安全领域的评估模型在属性、可靠性和可用性方面使用了更多的定量评估方法, 同时会结合场景中控制关系、信息传递关系等进行评估。具有代表性的分析评估方法有: 功能危害评估技术、危害和可操作性研究(Hazard and operability, HAZOP)、故障模式影响分析、故障树、失效模式与影响分析 (failure mode and effect analysis, FMEA)方法等[21]。在信息安全领域, 风险评估是对系统及其传输和存储信息的保密性、完整性和可用性等安全属性进行评价的过程, 识别网络系统中存在的脆弱性, 结合资产价值、被利用的可能性和被利用后带来的后果进行有效评估, 提出合理的安全策略和防护措施[36]。目前信息安全风险评估方法中, 使用基于模型的评估方法和基于脆弱性分析的评估方法最为广泛, 其中基于模型的评估方法, 具体可以分为定性评估方法, 例如攻击链模型、攻击面模型、自动机模型和定量评估方法, 例如攻击树模型、马尔可夫模型、贝叶斯网络模型[37-38]。

表 2 功能安全和信息安全现有风险评估模型交叉使用示例

Table 2 Examples of cross-use of existing risk assessment model for safety and security

方法	参考
功能安全应用到信息安全领域的方法	
故障树→攻击树	[28,39-40]
通用误差模型→信息通用误差模型	[41]
HAZOP→HAZOPs	[42-44]
BDMP→用于攻击建模的 BDMP	[45-46]
域分析→信息安全域分析	[44]
信息安全应用到功能安全领域的方法	
错误用例模型→失败用例模型	[47-48]

在评估模型方面功能安全和信息安全风险分析融合通常采用两种观点中的一种: 要么源于信息安全或功能安全领域将现有的方法进行对两个领域的风险进行分析, 要么研究多种风险评估方法的相似之处[49]。由于两个领域过去的独立发展, 它们没有考虑到其他领域风险对自身评估有效性和准确性的影响, 所以模型的设计存在欠缺。不同的分析模型拥有不同的特点, 因此模型的融合或跨领域的使用在实践过程中得到了不错的成果, 如表 2 对功能安全和

信息安全跨域使用方法的总结。在方法融合方面, 文献[28,50]通过融合故障树和攻击树, 或利用蝴蝶结分析方法统一故障树等树形结构的分析方法对工业控制系统进行全面的风险分析, 使功能安全领域和信息安全领域所面临的风险可以进行综合分析。文献[51-52]提出针对工业控制系统的融合安全风险分析方法, 可以有效评估信息安全风险和功能安全风险之间的影响, 进而有助于提出更有效的缓解策略。风险评估方法的融合会造成模型的复杂程度增加, 方法的易用性降低, 但是通过利用跨域或融合分析方法可以增加风险评估的全面性和有效性。

在基于脆弱性分析的评估方法方面, 由于信息安全领域中风险产生的根本原因是代码、配置文件等存在脆弱性, 使攻击者有机可乘。与功能安全面临的风险不同的是脆弱性的存在无法预测, 其只有在人为故意触发的情况下才能发现。为了尽可能减少脆弱性的存在, 一般会使用模糊测试、污点传播、符号执行等方法进行分析。其中模糊测试技术的使用与 IT 领域相差较大, 因为工业控制系统存在设备依赖和流程作业的特点, 同时控制设备与工业软件中的程序执行存在更强的状态约束, 因此对代码覆盖率和状态检测都造成新的挑战。进行协议模糊测试是工业控制系统中最常用且最有效的方法, 因为设备与设备、软件与设备、软件与软件之间都是通过协议进行通信, 且远程攻击者往往也是通过协议通讯端口作为攻击入口。但工业控制系统中存在很多专有协议, 目前主要通过协议逆向分析技术或使用状态反馈辅助模糊测试, 同时利用概率统计方法结合机器学习捕捉协议特征提高代码覆盖率[53-56]; 针对工业控制系统的状态约束的特点, 通过引入状态机、更改变异策略等方法来达到深层模糊测试的目的, 提高模糊测试效率[57-59]。在监测方面由于设备的定制化和私有化, 传统基于日志收集或内存插桩监测等手段方法不再适用, 文献[60]提出使用心跳报文或构造有效的探测报文来实现嵌入式设备的状态监测; 文献[61]使用数字示波器监测 PLC 的输出模块, 从信号的角度判断设备状态。

3.2 风险缓解技术

在系统面临未知概率或可能发生的风险情况下, 通过使用缓解技术来降低风险发生的概率和减少风险发生后造成的影响是一种有效的防御手段。提高风险发生的代价是网络安全中最常用且最有效的手段。在信息安全领域中一般以机密性、完整性和可用性作为衡量指标, 而在功能安全中则以可靠性和可用性作为主要衡量指标。由于衡量指标的不同, 再结合工业控制系统本身的特点, 造成风险缓解技术融合的困难, 甚至存在冲突。上述 4 个安全目标在一定程度上是相互影响和相互制约的, 本节将分别根据缓解措施的实施目的即机密性、完整性、可用性和可靠性, 对融合安全的风险缓解技术进行总结。

3.2.1 机密性保护技术

机密性是确保非授权人员或设备无法访问敏感信息, 同时确保授权人员或设备可以正确的访问这些信息。在工业控制系统信息安全领域, 机密性是重要的一项安全目标。然而, 在功能安全领域机密性的重要程度相对较低, 因为相关保护措施对功能安全所应对的风险产生较小的缓解作用, 而且保护措施会对系统性能产生影响。因此系统中很少使用加密算法进行数据保护或者会使用一些简单的编码技术[62]。信息安全通常使用复杂加密算法对通信内容或存储数据进行加密保护, 采取密钥交换、挑战应答、口令验证等身份认证方式来防止非授权人员的接入, 同时利用权限划分等访问控制技术, 针对不同级别的用户划分其所能接触的数据范围, 来实现数据机密性的保护, 降低非授权人员盗取、窃听等风险情况发生的概率, 提高恶意人员攻击的代价[63]。

在加密性算法方面, 功能安全和信息安全融合的难点是在存储资源、计算资源有限的条件下, 完成兼顾系统性能和保护算法有效性的方法实施。因此存在大量的研究工作针对传统加密算法 AES[64-65]、RSA[66]等进行改进, 并针对工业控制系统中使用的系统或设备例如数据采集与监视控制系统(Supervisory control and data acquisition, SCADA)[67]、RTU[68]等根据系统工作中的特性提出针对性的加密方案, 通过利用工业控制系统本身的机制来辅助进行密钥传输, 进而减少资源的消耗。同时为了衡量工业控制系统中加密算法的有效性和可行性, 研究人员对实施加密算法的工控系统进行实时性和准确性的评估[69], 或对已实施加密算法的嵌入式设备进行缺陷检查[70]。

在身份认证和访问控制方面, 功能安全领域中实施相关措施并不是为了保护数据的机密性, 而是为了缓解人员因操作失误而带来的风险, 因此会采用简单的身份认证方式例如口令, 来限制无关人员的操作或者在进行可能会对物理世界产生影响的操作时进行二次确认, 一般会在 HMI、SCADA、编程配置软件等人机交互且具有控制功能的组件中实施。在信息安全中实施认证等相关措施是为了保护目标中存储数据或传输数据的机密性, 而且从简单的拒绝服务到复杂的远程代码执行, 其本质原因都是没有做好访问控制, 导致攻击者有机会与设备建

立通信。所以有效的身份认证和访问控制措施不仅仅可以对机密性进行保护, 还对可用性和完整性也起到保护作用。融合工作需要在原本具备认证和访问控制功能的组件中提高方法的复杂性, 在不具备保护措施的被控设备上进行严格的认证和访问控制, 尤其是具备远程通信功能的设备。因此对系统运行和通信性能产生可允许影响的轻量级认证方法被广泛研究, 文献[71-74]通过对已有工控协议进行改进, 增加认证字段或利用逻辑运算等方法提供工控系统可接受的设备间的认证技术。同时随着区块链和可信计算等技术的成熟, 文献[75]提出一个基于区块链的安全互认证系统 BSeIn, 以实施细粒度的访问控制策略。该系统集成了属性签名、多接收方加密和消息认证码, 能够提供匿名认证、可审计性和保密性等隐私和安全保障。文献[76]针对工业控制系统接入安全威胁提出基于可信计算 PLC 身份认证方法, 针对工业控制系统启动安全威胁, 提出基于信任链传递的终端度量技术解决方案, 从不同层面保证工业控制系统安全运行。

3.2.2 完整性保护技术

为了确保数据在其生命周期中保持可靠性和准确性, 数据完整性是一个重要的考虑因素, 尤其在信息安全领域。在功能安全领域, 设备和数据的可用性和可靠性要求非常高, 因此也会间接依赖于数据完整性保护技术。除了在 3.2.1 节中提到的访问控制技术可以起到完整性保护的作用, 消息认证码、消息校验码、数字签名等技术也是重要的保护手段。在功能安全中常采用简单且具备一定自纠正能力的完整性算法, 对于微小的误差进行自动纠正[77], 例如对传感器或控制器的数据计算校验和并将结果与存储在非易失性介质中的预定值进行比较, 这样的检查是定期执行的, 根据校验和的确定方式, 任何偏差都将会引起设备的隔离或数据的纠正。在信息安全中, 攻击者会通过伪造报文、篡改设备固件、修改配置信息文件等方式给设备埋入后门或对设备的功能进行破坏, 为了提高攻击成功的概率, 攻击者通常需要对完整性算法进行破解, 使被修改后的数据可以通过校验检查。因此, 系统需要采用复杂的完整性算法或方案来提高安全性。但复杂算法意味着对系统性能的消耗, 因此传统方法很难直接应用到工业控制系统中。此外 IT 系统对校验不通过的报文通常采取丢弃处理的方式, 由于网络服务质量等很可能会严重影响工业控制系统的可用性, 因此, 在 IT/OT 融合的系统中, 丢弃的处理方法并不适用, 这对融合工作带来了挑战。

针对完整性的保护, 提高完整性算法的校验效率是当前研究的重点, 即在系统资源受限的条件下, 使保护方法能满足信息安全的需求且不影响设备的可靠性和可用性指标。本文根据完整性保护的使用位置分为数据传输和数据存储, 如表 3 所示。在数据传输中一类是对消息认证、校验等算法进行优化来保证完整性; 另一类则是通过设计新的网络结构或对 Modbus 等控制协议字段进行改进, 从控制器端和工厂端来提升数据传输的完整。在数据存储中, 由于一方面嵌入式设备在控制领域的广泛使用, 攻击者往往会利用替换或修改固件的方式进行攻击, 因此研究人员通过提出适用于固件层次的完整性校验算法来保证设备的安全性; 另一方面则与传统计算机存储数据保护类似, 为数据的存储和执行提供安全环境。我们认为未来完整性算法还需要融合自纠正的能力, 以适应控制环境中对于可用性的高要求, 这会进一步提升安全一体化的水平。

表 3 完整性保护方法在工业控制系统中的改进应用

Table 3 The improved integrity protection technology is applied to the industrial control system

方法	参考
数据传输	
对消息认证码等传统方法改进, 降低性能消耗且提供完整性监控	[78-80]
提出新的适用于工业控制系统完整性校验的方案或方法	[81-83]
数据存储	
针对嵌入式设备例如 PLC 等, 提出固件的完整性校验方法	[84-87]
利用可信技术提出系统层面的可信域, 为数据提供安全执行环境	[88-89]

3.2.3 可用性保护技术

可用性是保证授权人员可以可靠和持续访问数据或设备, 并及时得到响应的能力, 一般指系统在执行任务的任意时刻能够正常工作的概率来衡量。在工业控制系统中, 可用性是功能安全的重要保障指标。上述的完整性保护方法和机密性保护方法都可以对可用性起到一定的保护作用, 但对于部分风险仍需要其他缓解措施应对。在功能安全中一般通

过提高通信吞吐量、设计冗余链路、设备和采取故障转移等方法避免破坏可用性问题的出现。同时建立快速、适应性强的灾难隔离和恢复计划应对最坏情况的发生。在功能安全中还常使用故障容忍方法来提高可用性, 例如允许数据在可允许阈值内进行波动, 不采取中断作业等手段进行干预[90-91]。在信息安全中, 保护可用性的主要目的是防止外界故意对数据和设备的破坏, 防止因拒绝服务攻击或网络入侵等恶意攻击而导致的停机事件。除了正确维护所有必要的硬件和软件外, 及时进行系统和软件的升级, 并使用额外的安全防护软件和设备是必不可少的, 例如入侵检测、恶意代码检测等技术。在 IT/OT 系统融合之后, 由于工控系统并不适合停止作业来进行升级或打补丁, 同时为了保证软件的兼容性往往使用较低版本的系统, 这给工业控制系统带来了较大的威胁。此外, 由于控制设备之间和控制设备与传感执行设备之间协调配合的工作方式, 使通过构造满足约束的通信数据包情况下, 可以对工业控制系统采用基于时间序列的攻击方式, 进而造成设备间的协调错误并对物理世界产生影响, 因此, 传统的基于单点检测的方法无法有效应对此类威胁。

在可用性保护工作的融合方面, 为了适应工业控制系统安全的需求, 信息安全借鉴功能安全的故障容忍的思想提出入侵容忍技术[92], 通过调整系统结构和冗余资源来保证系统的可用性, 可见动态再配置的思想在两个领域得到了共识。文献[93]通过对生产数据进行深度学习建立正常工作模型, 以预测故障和异常的发生, 入侵监测和恶意代码检测也可以结合生产数据和安全数据建立一体化的安全监测模型, 来适应控制环境。目前的研究工作集中于针对序列攻击的检测并积极探索在资源有限和时间敏感的条件下实施检测。文献[94-97]通过引入时间和设备状态特征利用机器学习、主成分分析方法等进行数据分析, 构建更准确的入侵检测模型来抵序列攻击; 文献[98]通过利用控制系统的控制逻辑结合图论方法来实现逻辑层次的入侵监测; 文献[99]则通过聚合物理世界传感器和执行器产生的数据进行入侵监测。为了构建真正的安全融合系统, 数据的融合是关键, 因此未来对生产数据和安全数据、信息域数据和物理域数据的融合分析是必然的趋势, 通过充分学习和挖掘数据的特征, 可以使系统具备自主、自成长、自学习的能力, 构建主动防御体系。

3.2.4 可靠性保护技术

可靠性是指在规定的条件下, 在规定时间内完成规定功能的能力, 主要是保证功能和数据的正确性。一般用系统平均无故障运行时间进行衡量。可靠性与可用性是互斥互利的关系。在功能安全中为了保证可靠性, 在调用某项功能时, 会调用两个相同的服务计算并比较结果决定是否执行, 以防止错误响应的发生。但是, 任何一项服务的失效都将影响系统的可用性, 为了缓解这样的情况发生设备投票表决的方式被广泛采用。对于冗余配置、双重保护、完整性检验等保护措施来说, 它们对可靠性和可用性都具有保护作用。此外在功能安全领域会采用信号滤波、设备接地、增加抗干扰设备等措施来保证可靠性。在信息安全中, 由于攻击的不确定性和故意性, 很难衡量信息安全措施的可靠程度。目前通过利用攻击库、漏洞库和恶意代码库等资源进行功能可靠性和有效性的测试。同时也会采用红蓝对抗的方式来发现问题以提高系统的可靠性。

在融合工作中, 功能安全领域为了减少复杂系统因不确定性而造成的故障, 文献[100-101]提出采用模糊理论思想对工业控制系统的可靠性进行度量, 以进一步优化系统。这与信息安全中采用模糊理论发现系统的脆弱性相似, 未来可能会有融合工作的出现。在保护数据的可靠性方面与上述保护完整性和可用性等使用的措施不尽相同, 不再赘述。

4 融合安全标准与方案

在功能安全和信息安全的融合过程中, 安全标准的制定和安全方案的研究扮演着推进和指导的重要角色。这些标准通过统一概念、规范流程, 减少了行业内的不必要冲突。同时, 安全方案的推广也为整个行业提供了成熟的思路和方向。本章对安全标准和安全方案融合工作的进展进行了总结。

4.1 安全标准

工业控制系统在功能安全领域根据应用场景的不同存在相应的安全标准或规范, 其中 IEC-61508 标准[12]作为整个控制领域的基础功能安全标准, 工业控制系统、医疗、汽车、航空等行业会参考这一标准制定自己行业的功能安全标准。在工业控制系统中根据作业特点分为离散系统和流程系统分别对应 IEC-62061 和 IEC-61511 功能安全标准。国内在 2006 年对 IEC-61508 标准进行了翻译和整理形成对应的国标 GB/T-20438[102]。在信息安全领域 IEC-62443[2] 是工业通信网络和系统的安全标准, 其涵盖行业所有的利益相关方, 利用 4 个部分共计 12 个文档对工业控制系统中涉及的概念术语、生命周期、策略要求等进行规范。国内还没有对完整的 IEC-62443 系列

标准进行翻译和整理, 目前 GB/T-33007[103]主要覆盖 IEC-62443-2-1 标准内容, 提供了工业自动化控制系统在建立网络安全管理系统时需要的元素指南; GB/T-30976[104]对应 IEC62443-3-3 标准, 主要对工业控制系统的信息安全的评估和验收环节进行规范。

在标准融合方面, 国际上具备影响力的标准化委员会已经开始功能安全和信息安全融合标准的制定工作, 国际电工委员会(International electrotechnical commission, IEC)成立 TC 65-WG 20 工作小组, 其任务是负责搭建工业过程测量、控制和自动化功能安全和信息安全的桥梁。2019 年 5 月该小组通过对 IEC-61508 和 IEC-62443 进行整合形成 IEC-63069 标准, 该标准提出功能安全和信息安全框架, 协调功能安全和信息安全在工业控制系统中的应用, 其中除对可能产生歧义的概念进行统一定义和解释以外, 还提出功能安全和信息安全交互框架, 如图 3 所示。交互框架为二者融合过程中可能出现的冲突提供了解决方案, 该标准认为信息安全是为系统功能和功能安全提供一个安全执行环境[29]。国际自动化协会在 2009 年成立联合工作组 ISA99-WG7, 负责调查功能安全和信息安全之间的衔接以及常见问题, 目的是提高人们对网络安全问题在工业过程运行中的影响和认识。ISA99-WG7 在 2017 年发布融合安全生命周期框架, 旨在整合工业自动化控制系统中信息安全生命周期和功能安全生命周期, 为常见风险和安全需求提供指导[105]。IEC 组织也在 2020 年 12 月发布工业自动化控制系统的功能安全和信息安全的生命周期要求 IEC-63325 标准, 建立了通用的一体化风险评估流程[30]。此外 IEC-63074 技术报告分析了信息安全对功能安全关键系统的影响, 通过对二者关系进行刻画分析认为信息安全的脆弱性最终可能会一步威胁功能安全[106]。国内目前也积极推进融合安全标准的制订工作, 工业信息安全产业联盟采用国际先进的功能安全和信息安全理念, 参考国际前沿技术, 结合国内实践经验, 提出《智能工厂安全一体化》《智能制造安全一体化》等标准的制订草案[107], 在正式公布之后也能对融合安全的发展起到推动作用。

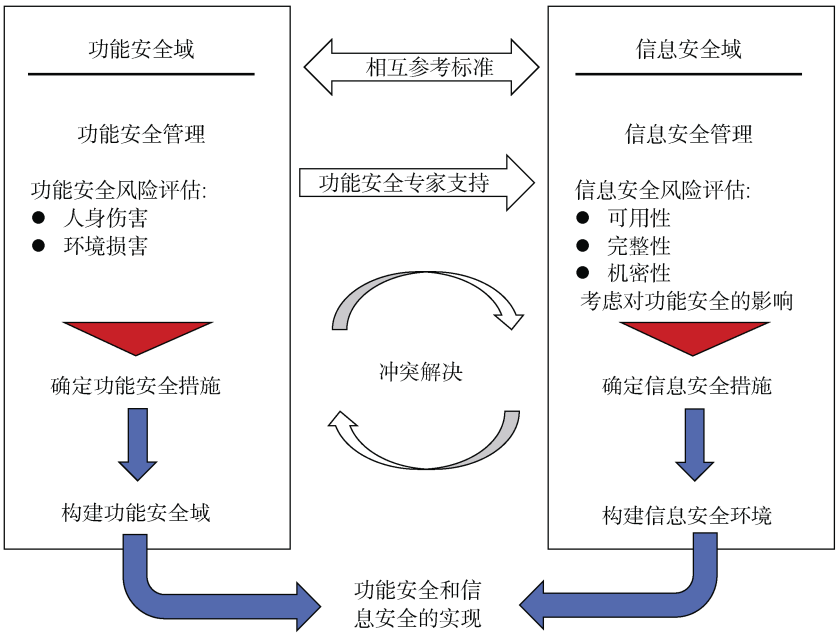

图 3 功能安全和信息安全交互框架

Figure 3 Safety and security interaction

4.2 安全方案

工业控制系统具有系统资源有限、对时效性敏感和可用性要求高等特点, 而且在真实环境部署后, 还可能存在系统难以定期更新打补丁、系统是否存在后门不确定等情况。这些问题是实现融合安全在真实环境中的难点。为了应对这些挑战, 学术界和工业界提出了许多具有实施性的有效防御方案。其中, 拟态防御和伴生安全是目前已经取得不错效果的方案。

拟态防御是由邬江兴院士提出[108],该方案在保证目标对象给定服务功能和性能不变的前提下, 通过对内部架构、冗余资源、运行机制、核心算法、异常表现等环境因素做出策略性地时空变化, 使附着在其上的未知漏洞、后门、木马或病毒等都发生

变化, 从而使攻击场景变化并扰乱攻击链的构造, 进而提高攻击者代价, 增加防守方的应对时间。拟态防御技术可以通过伪装真实系统的特征, 混淆攻击者的视线, 从而减小攻击面和提高安全性。拟态技术可以针对不同的组件进行实施, 如拟态 PLC、拟态网络等。拟态防御的优点是可以快速实施和适应各种环境, 但缺点是需要大量的资源, 有时可能会影响系统的性能。

伴生安全是指通过引入附加安全功能, 实现对系统的动态防御。伴生安全技术可以通过在系统中加入另一个系统或功能模块, 来监控、检测和响应安全事件。伴生防御方案是基于针对工业控制系统的攻击需要产生实际的破坏效果就需要对生产系统造成影响才能达到目的的假设。攻击者一般通过非法操控设备或篡改传感器数据造成对业务流程和物理世界造成影响, 而产生的影响一般也会直接体现在生产过程中, 因此工业界提出伴生安全防御方案[109]。其通过建立一套与工业控制系统并行伴生的安全系统, 将安全控制与工控系统进行镜像运行, 潜在风险的影响将会在镜像系统中得到体现, 所以可以提前终止其在真实系统中的工作。在不影响工控系统运行效率的前提下, 通过与系统控制过程监测的结合, 在发现安全隐患之后, 对工业生产过程进行及时有效的监督诊断和干预恢复, 实现工业生产过程的安全管控。伴生安全技术可以帮助工业控制系统在运行时进行安全检测和攻击响应, 从而提高系统的安全性。但是伴生安全技术可能会增加系统复杂度, 降低系统的可靠性和性能。

5 挑战与展望

在工业控制系统中, 单独考虑功能安全或者信息安全可以减小风险发生的概率和影响, 这在一定程度上可以提高攻击代价或降低故障危害。然而, 由于不存在绝对的安全, 因此综合考虑信息安全和功能安全的风险管理和应对策略可以提高安全防御的全面性和有效性。为了实现功能安全和信息安全的融合共存, 需要克服二者融合发展过程中可能遇到的挑战。本节将总结可能存在的挑战, 并展望发展趋势。

1) 从信息物理融合的角度考虑, 融合安全面临着许多挑战。信息物理融合系统(Cyber-physical system, CPS)可以理解为基于嵌入式设备的高效网络化信息系统, 其通过多维异构的计算单元和物理对象在网络环境中进行高度集成和交互来完成工作任务。这种系统在信息处理、数据通信、控制等方面具有实时、自主协调、高性能、高可用性等特点[110]。工业控制系统是一种典型的信息物理融合系统, 其中信息域和物理域的深度耦合为融合安全带来挑战[111]。

从信息物理融合系统的本质出发, 在风险评估、传播和缓解等各个阶段, 融合计算、通信和控制等领域的知识都需要被考虑进来, 才能构建一体化安全防御机制和评估标准。这也是研究融合安全的最终目标, 但同时也是研究过程中的主要难点。在工业控制系统中, 信息和物理之间的紧密关联意味着信息安全和功能安全之间的相互影响。信息物理融合系统的安全性评估需要同时考虑信息安全和物理安全的风险, 以及二者之间的相互作用。因此, 在评估安全风险时, 需要综合考虑多个方面, 如网络安全、物理安全、控制安全和安全管理等。此外, 信息物理融合系统的开发和部署过程中, 需要考虑多种约束因素, 如能耗、存储、带宽和时延等。这些因素会对安全方案的设计和实现带来挑战, 因为安全方案需要在满足性能要求的同时, 保证系统的安全性。总之, 信息物理融合系统的安全性评估和安全方案的设计与实现都需要考虑多个因素, 如信息安全、物理安全、控制安全、约束因素等。因此, 为了实现融合安全的目标, 需要综合考虑这些因素, 并开展更加深入的研究。

2) 从 IT/OT 融合系统角度去考虑融合安全面临的挑战。在 IT/OT 融合系统中, 企业和工业运营可以通过集成用于数据中心计算的 IT 系统和用于监视事件、过程和设备的 OT 系统来实现更好的决策和控制。然而, 这种融合系统也带来了一些安全挑战, 需要在 IT 和 OT 领域之间搭建安全防护措施来缓解安全风险。其中一个主要的挑战是在安全方面存在知识领域之间的鸿沟, 需要将 IT 和 OT 领域的安全防护措施进行整合。

传统的 IT 安全方法可能无法直接适用于 OT 系统, 因为 OT 系统具有特定的特性, 如不定期升级修补漏洞和内部存在控制依赖关系[112-113]。因此, 需要建立一种针对 IT/OT 融合系统的综合安全策略, 以确保该系统的安全性。此外, 由于 IT 和 OT 系统通常由不同的部门或公司管理, 因此协调和整合这些系统的安全策略也是一项挑战。此外, OT 系统中使用的传感器和执行器可能存在与 IT 系统不同的通信协议和安全标准, 这也需要加以考虑。为了应对这些挑战, 需要制定一种综合的 IT/OT 安全策略。该策略应该考虑到 IT 和 OT 系统之间的差异, 并结合特定的应用背景和领域特性来制定。在实施安全策略时,

需要注意 IT 和 OT 系统之间的集成和协调, 并确保传感器和执行器等设备与系统的安全标准和协议的兼容性。在 IT/OT 融合系统的安全方面, 还需要采用一些具体的措施, 例如建立网络隔离、实施访问控制、加密数据传输、实施漏洞管理等。此外, 还需要对系统进行定期的安全审计和风险评估, 以确保系统的安全性。总之, IT/OT 融合系统的安全是一个复杂的问题, 需要针对该系统的特殊需求和挑战制定综合的安全策略。通过搭建 IT 和 OT 领域之间的安全防护措施, 并加强协调和整合, 可以提高融合系统的安全性和稳定性。

3) 从复杂系统的角度考虑, 实施融合安全方法是具有挑战性的。复杂系统是通过实体之间的交互、关系或依赖形成的整体。随着自动化和智能化的提升, 工业控制系统的复杂性不断增加, 这导致系统不确定性增加, 因为复杂性和非线性特性使系统更加难以预测和分析。为了应对这些挑战, 我们需要建立有效的复杂网络模型, 以便根据系统特征进行分析。这样做有助于减少噪声等扰动, 确保结果准确。此外, 我们需要考虑设备和信息的依赖性, 这有助于分析风险在系统内的传播以及风险发生后设备之间的相互影响。这些因素可以为工业控制系统的安全决策提供有力支持。然而, 建立有效的分析模型仍然是工业控制系统融合安全研究中的一个难点[114]。这需要在建模过程中充分考虑系统的复杂性和不确定性, 并使用合适的工具和技术进行分析和评估。因此, 我们需要开发新的方法和工具来帮助我们更好地理解和应对工业控制系统的安全挑战, 以确保这些系统的安全性和可靠性。

4) 从安全外延和安全内延的角度去考虑融合安全方法实施的挑战。安全内延是指针对工业控制系统中使用的组件, 例如 SCADA、PLC 等生产运行设备, 重点研究单个设备的操作系统、服务、协议等安全性并实施安全保护技术。安全外延是指在工业控制系统行业或一个完整的生产架构下去考虑安全防护, 重点分析设备依赖关系、风险传播路径等, 研究整个架构下的宏观安全保护[15]。

在研究融合安全的过程中需要结合宏观和微观去考虑安全措施的实施位置, 平衡单体设备面临计算存储资源的限制和整体安全布局下防御有效性的问题。此外, 我们还需要考虑安全功能和业务功能以及安全功能之间的关系依赖, 以确保安全措施的综合效果。从安全内延的角度来看, 融合安全方法的实施需要解决单个设备的安全问题。这需要实施各种技术, 例如访问控制、身份验证、数据加密等, 以确保单个设备的安全性。从安全外延的角度来看, 需要考虑设备之间的依赖关系和风险传播路径, 以便在整个生产架构下进行宏观安全保护。这需要实施各种措施, 例如安全漏洞扫描、漏洞管理、网络流量分析等, 以确保整体安全性。综上所述, 无论是从安全内延还是安全外延的角度来看, 融合安全研究都需要结合宏观和微观的角度来考虑安全措施的实施位置。这需要平衡单体设备和整体安全布局下的防御有效性, 并考虑安全功能和业务功能之间的关系依赖。因此, 融合安全研究的重点在于从宏观和微观的角度来分析和解决工业控制系统的安全挑战。

6 结论

随着工业互联网的快速发展, 功能安全和信息安全已经不能独立发展来应对当下的风险环境。因此, 越来越多的研究表明二者的融合是可能和必要的。融合安全可以产生一体化的安全需求, 使风险分析和缓解更加全面和有效, 同时还可以减少系统性能的开销和开发运行的成本。目前, 学术界和工业界已经展开了对安全融合的研究。在安全方法的相似性分析、融合安全技术研究、融合安全标准制定等方面都已经取得了进展。安全融合的发展可以带来诸多好处, 例如提高安全性能、降低系统运行成本、增强信息安全和功能安全的协同作用。然而, 由于工业控制系统资源受限、对时效性和可用性要求高、信息物理融合等特点, 使得融合安全的研究仍然存在着很多挑战和难点需要解决。其中, 一些主要挑战包括如何平衡信息安全和功能安全的权衡、如何开发出适用于特定应用场景的融合安全技术、如何将融合安全标准与现有标准对接等。因此, 需要进一步加强对融合安全的研究和开发, 以满足工业控制系统的安全需求。

参考文献

[1] Knowles W, Prince D, Hutchison D, et al. A Survey of Cyber Security Management in Industrial Control Systems[J]. *International Journal of Critical Infrastructure Protection*, 2015, 9: 52-80.

[2] International Electrotechnical Commission. Security for industrial automation and control systems (IEC-62443). Jul.2009.

[3] White Paper on industry Information Security Situation, NISIA[Z]. http://www.cics-cert.org.cn/etiri-edit/kindeditor/attached/file/20180105/20180105165446_94401.pdf. Dec, 2017.

[4] White Paper on Cyber Security Situation of Industrial Control in 2019[Z]. Northeastern University. http://www.ditecting.com/. 2019.

[5] AutoSploit[Z]. https://github.com/NullArray/AutoSploit. Oct.2019.

[6] Industrial Exploitation Framework[Z]. https://github.com/dark-lbp/

isf, Jun.2017.

[7] Monitoring ICS Cyber Operation Tools and Software Exploit Modules[Z]. FIREEYE. https://www.fireeye.com/blog/threat-research/2020/03/monitoring-ics-cyber-operation-tools-and-software-exploit-modules.html. Mar, 2020.

[8] The spear to break the security wall of S7CommPlus. Cheng, L., Donghong, L. and Liang, M. https://media.defcon.org/DEF CON 25/DEF CON 25 presentations/Cheng Lei/DEFCON-25-Cheng-Lei-The-Spear-to-Break-the-SecurityWall-of-S7CommPlus-WP.pdf. Jul.2018.

[9] Doors of Durin: The Veiled Gate to Siemens S7 Silicon. Ali Abbasi, Tobias Scharnowski and Thorsten Holz[Z]. https://www.blackhat.com/eu-19/briefings/schedule/#doors-of-durin-the-veiled-gate-to-siemens-s-silicon-18023. Dec.2019.

[10] Global Industrial Safety Memorabilia[Z]. https://www.ics-cert.org.cn/portal/page/132/c8b128a51350471d9e99e0bfa59b92b3.html. Jan, 2020.

[11] Stuxnet Under the Microscope ESET[Z]. https://web.archive.org/web/20101003183945/http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf. 2012.

[12] International Electrotechnical Commission. Functiona-l safety of electrical/electronic/programmable electronic safety-related systems(IEC 61508 Edition 2.0). 2010.

[13] Kriaa S, Pietre-Cambacedes L, Bouissou M, et al. A survey of approaches combining safety and security for industrial control systems[J]. *Reliability Engineering & System Safety*, 2015, 139: 156-178.

[14] DEFSTAN 05-91/1(1991). UK Ministry of Defence Standards.[Z] https://infostore.saiglobal.com/en-us/Standards/DEFSTAN-05-91-1-1991-1991-365497_SAIG_DEFSTAN_DEFSTAN_833728/. 1991.

[15] USA: National Institute of Standards and Technology (NIST). Guide to Industrial Control Security (NIST SP800-82). 2011.

[16] Research Triangle Park. ANSI/ISA-99-00-01-2007. Security for Industrial Automation and Control Systems. The Instrumentation, Systems, and Automation Society. 2007.

[17] Line, M B, Nordland O, Røstad L, et al. Safety *vs.* Security[C]. *In Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management*. 2006.

[18] Burns A, McDermid J, Dobson J. On the meaning of safety and security[J]. *The Computer Journal*, 1992, 35(1): 3-15.

[19] Piètre-Cambacédès L, Bouissou M. Modeling Safety and Security Interdependencies with BDMP (Boolean Logic Driven Markov Processes)[C]. *2010 IEEE International Conference on Systems, Man and Cybernetics*, 2010: 2852-2861.

[20] Piètre-Cambacédès L, Chaudet C. The SEMA Referential Framework: Avoiding Ambiguities in the Terms “Security” and “Safety”[J]. *International Journal of Critical Infrastructure Protection*, 2010, 3(2): 55-66.

[21] Donald Firesmith. Common Concepts Underlying Safety, Security, and Survivability Engineering. Software Engineering Institute, Pittsburgh, Pennsylvania, 2003.

[22] Nancy G. Leveson. Safeware, System Safety and Computers. Addison-Wesley Publishing Company Inc, 1996.

[23] Eames D P, Moffett J. The Integration of Safety and Security Requirements[M]. Computer Safety, Reliability and Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999: 468-480.

[24] International Electrotechnical Commission. IEC 17799 - Information Technology - Security Techniques - Code of practice for information security management, 2005.

[25] Novak T, Treytl A. Functional Safety and System Security in Automation Systems - a Life Cycle Model[C]. *2008 IEEE International Conference on Emerging Technologies and Factory Automation*, 2008: 311-318.

[26] Riel A, Kreiner C, Macher G, et al. Integrated design for tackling safety and security challenges of smart products and digital manufacturing[J]. *CIRP Annals*, 2017, 66(1): 177-180.

[27] Sabaliauskaite G, Mathur A P. Aligning Cyber-Physical System Safety and Security[C]. *Complex Systems Design & Management Asia*. Cham: Springer, 2015: 41-53.

[28] International Electrotechnical Commission. Industrial-process measurement, control and automation - Framework for functional safety and security (IEC-TR-63069), 2019.

[29] International Electrotechnical Commission. Lifecycle requirements for functional safety and security for IACS(IEC-PAS-63325). 2020.

[30] Piggin R S H. Development of Industrial Cyber Security Standards: IEC 62443 for SCADA and Industrial Control System Security[C]. *IET Conference on Control and Automation 2013*: *Uniting Problems and Solutions*, 2013: 1-6.

[31] Security Assurance Levels: A SIL Approach to Security. Dr. Nate Kube, Bryan Singer[Z]. https://www.controlglobal.com/assets/Media/MediaManager/wp_080401_Wurldtech_SALSIL.pdf. Jan.2008.

[32] M.Sliwinski, E.Piesik, J.Piesik. Integrated functional safety and cyber security analysis[C]. *Symposium on Fault Detection, Supervision and Safety for Technical Processes SAFEPROCESS,* 2018:126-1270.

[33] Jin J H, Zhao Z C, Wang Y T. Coordination Method of Functional Safety and Cyber Security for Industrial Control Systems[C]. *2021 China Automation Congress*, 2022: 122-127.

[34] Galloway B, Hancke G P. Introduction to industrial control networks[J]. *IEEE Communications Surveys & Tutorials*, 2013, 15(2): 860-880.

[35] Wang S, Liu C X, Yu D J, et al. Overview of Network Security Risk Assessment Model. Radio Communications Technology. https://kns.cnki.net/kcms/detail/13.1099.TN.20200525.1555.002.html, May,2020

[36] Raspotnig C, Opdahl A. Comparing risk identification techniques for safety and security requirements[J]. *Journal of Systems and Software*, 2013, 86(4): 1124-1151.

[37] Liu J. Network Security Risk Assessment Based on the Vulnerability Scanning[D]. Hefei: Anhui University, 2013.
(刘杰. 基于漏洞扫描的网络安全风险评估[D]. 合肥: 安徽大学, 2013.)

[38] Piètre-Cambacédès L, Bouissou M. Cross-fertilization between safety and security engineering[J]. *Reliability Engineering & System Safety*, 2013, 110: 110-126.

[39] Weiss JD. A system security engineering process[C]. *In Proceedings of the 14th National computer security conference*,

1991:572-581.

[40] Schneier B. Attack trees: Modeling security threats[J]. *Dobb's Journal,* 1999,12(24):21-29.

[41] Brostoff S, Sasse M A. Safe and Sound: A Safety-Critical Approach to Security[C]. *The 2001 Workshop on New Security Paradigms*, 2001: 41-50.

[42] Winther R, Johnsen O A, Gran B A. Security Assessments of Safety Critical Systems Using HAZOPs[C]. *The 20th International Conference on Computer Safety*, *Reliability and Security*, 2001: 14-24.

[43] Foster N, Jacob J. Hazard Analysis for Security Protocol Requirements[M]. IFIP Advances in Information and Communication Technology. Boston, MA: Springer US, 2002: 75-92.

[44] Srivatanakul T. Security Analysis with Deviational Techniques[D]. Heslington: University of York, 2005.

[45] Pietre-Cambacedes L, Bouissou M. Attack and defense dynamic modeling with BDMP[C]. *In Proceedings of the 5th International Conference on Mathematical Methods Models and Architectures for Computer Networks Security*, 2010:86-101.

[46] Pièrre-Cambacédès L, Bouissou M. Beyond Attack Trees: Dynamic Security Modeling with Boolean Logic Driven Markov Processes (BDMP)[C]. *2010 European Dependable Computing Conference*, 2010: 199-208.

[47] Raspotnig C, Opdahl A L. Improving security and safety modelling with failure sequence diagrams[J]. *International Journal of Secure Software Engineering*, 2012, 3(1): 20-36.

[48] Stålhane T, Sindre G. A Comparison of Two Approaches to Safety Analysis Based on Use Cases[C]. *The 26th international conference on Conceptual modeling*, 2007: 423-437.

[49] Kitchenham B A. Procedures for performing systematic reviews[J]. *Computer Science*, 2004, 33(4): 1-26.

[50] Abdo H, Kaouk M, Flaus J M, et al. A safety/security risk analysis approach of industrial control systems: A cyber bowtie - combining new version of attack tree with bowtie analysis[J]. *Computers & Security*, 2018, 72: 175-195.

[51] Friedberg I, McLaughlin K, Smith P, et al. STPA-SafeSec: Safety and security analysis for cyber-physical systems[J]. *Journal of Information Security and Applications*, 2017, 34: 183-196.

[52] Kriaa S, Bouissou M, Laarouchi Y. A new safety and security risk analysis framework for industrial control systems[J]. *Proceedings of the Institution of Mechanical Engineers*, *Part O*: *Journal of Risk and Reliability*, 2019, 233(2): 151-174.

[53] Niedermaier M, Fischer F, von Bodisco A. PropFuzz—An IT-Security Fuzzing Framework for Proprietary ICS Protocols[C]. *2017 International Conference on Applied Electronics*, 2017: 1-4.

[54] Zhang W Y, Zhang L, Mao J L, et al. An automated method of unknown protocol fuzzing test[J]. *Chinese Journal of Computers*. 2020, 43(4): 653-667.

[55] Zhao H, Li Z H, Wei H S, et al. SeqFuzzer: An Industrial Protocol Fuzzing Framework from a Deep Learning Perspective[C]. *2019 12th IEEE Conference on Software Testing*, *Validation and Verification*, 2019: 59-67.

[56] Luo Z X, Zuo F L, Jiang Y, et al. Polar: Function code aware fuzz testing of ICS protocol[J]. *ACM Transactions on Embedded Computing Systems*, 2019, 18(5s): 1-22.

[57] Zhang Y, Hong L, Wu L, et al. Protocol state based fuzzing method for industrial control protocols[J]. *Computer Science*. 2017, 44(1): 132-140.

[58] Voyiatzis A G, Katsigiannis K, Koubias S. A Modbus/TCP Fuzzer for Testing Internetworked Industrial Systems[C]. *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation*, 2015: 1-6.

[59] Pfrang S, Meier D, Friedrich M, et al. Advancing Protocol Fuzzing for Industrial Automation and Control Systems[C]. *The 4th International Conference on Information Systems Security and Privacy*, 2018: 570-580J.

[60] Chen J Y, Diao W R, Zhao Q C, et al. IoTFuzzer: Discovering Memory Corruptions in IoT through App-Based Fuzzing[C]. *Proceedings 2018 Network and Distributed System Security Symposium*, 2018.

[61] Liu P Z, Zheng Y W, Song Z W, et al. Fuzzing proprietary protocols of programmable controllers to find vulnerabilities that affect physical control[J]. *Journal of Systems Architecture*, 2022, 127: 102483.

[62] Fauri D, de Wijs B, den Hartog J, et al. Encryption in ICS Networks: A Blessing or a Curse? [C]. *2017 IEEE International Conference on Smart Grid Communications*, 2018: 289-294.

[63] Sadeghi A R, Wachsmann C, Waidner M. Security and Privacy Challenges in Industrial Internet of Things[C]. *The 52nd Annual Design Automation Conference*, 2015: 1-6.

[64] Yu Y F, Su Q J, Yang G. An encryption transmission scheme for industrial control system[J]. *Journal of Electronics & Information Technology*, 2020, 42(2): 348-354.

[65] Gao M Z. Research on Selective and Stochastic E Ncryption Strategies for the Resource-Constrained Control Systems Security[D]. Hangzhou: Zhejiang University, 2017.
(高梦州. 面向资源受限控制系统安全的选择性及随机性加密策略研究[D]. 杭州: 浙江大学, 2017.)

[66] Hussain I, Negi M C, Pandey N. A Secure IoT-Based Power Plant Control Using RSA and DES Encryption Techniques in Data Link Layer[C]. *2017 International Conference on Infocom Technologies and Unmanned Systems* (*Trends and Future Directions*), 2018: 464-470.

[67] Kang D J, Lee J J, Kim B H, et al. Proposal strategies of key management for data encryption in SCADA network of electric power systems[J]. *International Journal of Electrical Power & Energy Systems*, 2011, 33(9): 1521-1526.

[68] Ádámkó É, Jakabóczki G, Szemes P. Proposal of a secure modbus RTU communication with adi shamir's secret sharing method[J]. *International Journal of Electronics and Telecommunications*, 2018, 64: 107-114.

[69] Liang Y, Feng D Q, Xu S S, et al. Feasibility analysis of encrypted transm ission on security of industrial control systems[J]. *Acta Automatica Sinica*, 2018,44(3):434-442.

[70] Liu J F. Firmware Cryptographic Algorithm Identification and Defects Detection and Their Application[D]. Jinan: Shandong University, 2018.
(刘剑飞. 固件的密码算法识别和缺陷检测及其应用[D]. 济南:

山东大学, 2018.)

[71] Esfahani A, Mantas G, Matischek R, et al. A lightweight authentication mechanism for M2M communications in industrial IoT environment[J]. *IEEE Internet of Things Journal*, 2019, 6(1): 288-296.

[72] Zhang Y G. Research on Security Technology of Network Control System Based on Cyber-Physical Concept[D]. Harbin: Harbin Institute of Technology, 2015.
(张云贵. 信息物理融合的网络控制系统安全技术研究[D]. 哈尔滨: 哈尔滨工业大学, 2015.)

[73] Shang W L, Yang L Y, Chen C Y, et al. Lightweight group authentication mechanism for industrial control system terminals[J]. *Information and Control,* 2019,48(3):344-353.

[74] Abbasinezhad-Mood D, Nikooghadam M. Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications[J]. *Future Generation Computer Systems*, 2018, 84: 47-57.

[75] Lin C, He D B, Huang X Y, et al. BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0[J]. *Journal of Network and Computer Applications*, 2018, 116: 42-52.

[76] Wang Y. Research on the Authentication and Terminal Measurement Technology of PLC Based on Trusted Computing[D]. Shenyang: Shenyang Ligong University, 2018.
(王勇. 基于可信计算 PLC 的身份认证与终端度量技术的研究[D]. 沈阳: 沈阳理工大学, 2018.)

[77] Zumalde A A J, Secall J M, Junior J B C. Comparative Analysis on the Impact of Defensive Programming Techniques for Safety-Critical Systems[C]. *2009 Fourth Latin-American Symposium on Dependable Computing*, 2009: 95-102.

[78] Mahmood K, Ashraf Chaudhry S, Naqvi H, et al. A lightweight message authentication scheme for smart grid communications in power sector[J]. *Computers & Electrical Engineering*, 2016, 52: 114-124.

[79] Fischer, K. Control System Data Authentication and Verification Using Elliptic Curve Digital Signature Algorithm[D]. *Presented at ASNE Intelligent Ships Symposium*, 2013: 22-23.

[80] Song Y, Wang T R, Xu A D, et al. Communication Security Problem and Solution in Safety-Related System[C]. *2012 International Conference on Systems and Informatics*, 2012: 524-528.

[81] Keoh S L, Au K W K, Tang Z. Securing Industrial Control System: An End-to-End Integrity Verification Approach[D]. *Proc. Industrial Control System Security Workshop*, Dec. 2015.

[82] Pang Z H, Liu G P. Design and Implementation of Secure Networked Predictive Control Systems under Deception Attacks[J]. *IEEE Transactions on Control Systems Technology*, 2012, 20(5): 1334-1342.

[83] Xu R M. Research and Implementation of Key Technology for Modbus TCP/IP Protocol Security Enhancement[D]. Xi'an: Xidian University, 2017.
(徐荣茂. Modbus TCP/IP 协议安全加固关键技术研究与实现[D]. 西安: 西安电子科技大学, 2017.)

[84] Li B. Integrity of the PLC Firmware Enhancement Method Based on MD5[D]. Guangzhou: South China University of Technology, 2013.
(李彬. 基于 MD5 算法的 PLC 固件完整性增强方法研究[D]. 广州: 华南理工大学, 2013.)

[85] Huang X B, Liu G X. PLC firmware integrity verification method of SCADA system based on SHA1[J]. *China Measurement & Test*, 2017, 43(6): 114-117.

[86] Wang X Y, Konstantinou C, Maniatakos M, et al. ConFirm: Detecting Firmware Modifications in Embedded Systems Using Hardware Performance Counters[C]. *2015 IEEE/ACM International Conference on Computer-Aided Design*, 2016: 544-551.

[87] McMinn L, Butts J. A Firmware Verification Tool for Programmable Logic Controllers[C]. *International Conference on Critical Infrastructure Protection*. Berlin, Heidelberg: Springer, 2012: 59-69.

[88] Fitzek A, Achleitner F, Winter J, et al. The ANDIX Research OS—ARM TrustZone Meets Industrial Control Systems Security[C]. *2015 IEEE 13th International Conference on Industrial Informatics*, 2015: 88-93.

[89] Maene P, Götzfried J, de Clercq R, et al. Hardware-based trusted computing architectures for isolation and attestation[J]. *IEEE Transactions on Computers*, 2018, 67(3): 361-374.

[90] Dobson J E, Randell B. Building Reliable Secure Computing Systems out of Unreliable Insecure Components[C]. *1986 IEEE Symposium on Security and Privacy*, 2014: 187.

[91] Campelo J C, Rodríguez F, Rubio A, et al. Distributed industrial control systems: A fault-tolerant architecture[J]. *Microprocessors and Microsystems*, 1999, 23(2): 103-112.

[92] Huang S, Zhou C J, Yang S H, et al. Cyber-physical system security for networked industrial processes[J]. *International Journal of Automation and Computing*, 2015, 12(6): 567-578.

[93] Alzghoul A, Löfstrand M. Increasing availability of industrial systems through data stream mining[J]. *Computers & Industrial Engineering*, 2011, 60(2): 195-205.

[94] Caselli M, Zambon E, Kargl F. Sequence-Aware Intrusion Detection in Industrial Control Systems[C]. *The 1st ACM Workshop on Cyber-Physical System Security*, 2015: 13-24.

[95] Gharaibeh A, Salahuddin M A, Hussini S J, et al. Smart cities: A survey on data management, security, and enabling technologies[J]. *IEEE Communications Surveys & Tutorials*, 2017, 19(4): 2456-2501.

[96] Zeng P, Zhou P. Intrusion Detection in SCADA System: A Survey[M]. Intelligent Computing and Internet of Things. Singapore: Springer Singapore, 2018: 342-351.

[97] Jia X T. Research on Sequence Perceptible Industry Control System Intrusion Detection Technology Based on Machine Learning[D]. Beijing: Institute of Computing Technology, Chinese Academy of Sciences, 2019.
(贾新桐. 基于机器学习的可感知序列型工控入侵检测技术研究[D]. 北京: 中国科学院大学(中国科学院沈阳计算技术研究所), 2019.)

[98] Hailesellasie M, Hasan S R. Intrusion detection in PLC-based industrial control systems using formal verification approach in conjunction with graphs[J]. *Journal of Hardware and Systems Security*, 2018, 2(1): 1-14.

[99] Ghaeini H R, Tippenhauer N O. HAMIDS: Hierarchical Monitor-

ing Intrusion Detection System for Industrial Control Systems[C]. *The 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, 2016: 103-111.

[100] Garg H, Rani M. An approach for reliability analysis of industrial systems using PSO and IFS Technique[J]. *ISA Transactions*, 2013, 52(6): 701-710.

[101] Garg H. A Hybrid GA-GSA Algorithm for Optimizing the Performance of an Industrial System by Utilizing Uncertain Data[M]. Handbook of Research on Artificial Intelligence Techniques and Algorithms, 2015: 620-654.

[102] Functional safety of electrical/electronic/programmable electronic safety-related systems (GB/T 20438). 2017
(电气/电子/可编程电子安全相关系统的功能安全(GB/T 20438). 2017.)

[103] Industrial communication networks—Network and system security—Establishing an industrial automation and control system security program (GB/T 3307—2016). 2016
(工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序(GB/T 33007-2016). 2016.)

[104] Industrial control system security (GB/T 30976-2014). 2014
(工业控制系统信息安全(GB/T 30976—2014). 2014.)

[105] International Society of Automation. ISA99 Plans Working Group on Cyber Security and Safety in Industrial Processes. May, 2009.

[106] Safety of machinery - Security aspects related to functional safety of safety-related control systems (IEC TR 63074:2019), https://webstore.iec.ch/publication/31572.

[107] Functional Safety Standards Group 2019 work plan, NISIA, http://www.nisia.org.cn/newsitem/278359579, 2019.

[108] Wu J X. Research on cyber mimic defense[J]. *Journal of Cyber Security*, 2016, 1(4): 1-10.
(邬江兴. 网络空间拟态防御研究[J]. *信息安全学报*, 2016, 1(4): 1-10.)

[109] WANG B, XU X G . Study on the intrinsic safetyof industrial control system[J]. *Automation Panorama*, 2019, 36(s2): 46-49.

[110] Lee E. Computing Foundations and Practice for CyberPhysical Systems: A Preliminary Report.Technical Report UCB/EECS-2007-72, University of California, USA, 2007.

[111] Assuring industrial control system (ICS) cyber security[Z]. http://csis.org/files/media/csis/pubs/080825_cyber.pdf. Aug, 2008.

[112] Protecting industrial control systems—Recommendations for Europe and memberstates. European Network and Information Security Agency (ENISA), https://www.enisa.europa.eu/. 2011.

[113] Cyber securityassessments of industrial control systems. Center for the Protection of National Infrast A lightweight message authentication scheme for Smart Grid communications in power sectorructure (CPNI), https://icscert.uscert.gov/sites/default/files/documents/Cyber_Security_Assessments_of_Industrial_Control_Systems.pdf. 2010.

[114] Peng Y, Jiang C Q, Xie F, et al. Industrial control system cybersecurity research[J]. *J Tsinghua* (*Sci &Tech*), 2012, 52(10): 1396-4408.

刘圃卓 于 2018 年在吉林大学通信工程专业获得学士学位。现在中国科学院大学网络空间安全专业攻读博士学位。研究领域为物联网安全、嵌入式设备安全。研究兴趣包括模糊测试、脆弱性分析、风险评估。Email: liupuzhuo@iie.ac.cn

马叶桐 于 2019 年在华北电力大学信息安全专业获得学士学位。现在中国科学院大学网络空间安全专业攻读博士学位。研究领域为物联网安全、工业控制系统安全。研究兴趣包括风险评估。Email: mayetong@iie.ac.cn

吕世超 于 2018 年在中国科学院大学信息安全专业获得工学博士学位。现任中国科学院信息工程研究所第四研究室高级工程师。研究领域为物联网安全、工业控制系统安全。研究兴趣包括工控入侵诱捕、工控态势感知。Email: lvshichao@iie.ac.cn

方栋梁 于 2017 年在武汉大学软件工程专业获得学士学位。现在中国科学院大学网络空间安全专业攻读博士学位。研究领域为工业控制系统安全、嵌入式设备安全。研究兴趣包括二进制程序分析、漏洞分析与利用。Email: fangdongliang@iie.ac.cn

朱红松 于 2009 年在中国科学院计算技术研究所计算机体系结构专业获得博士学位。现任中国科学院信息工程研究所研究员。研究领域为网络空间安全。研究兴趣包括物联网安全、网络对抗、智能攻防、网络空间安全测量和威胁态势感知等。Email: zhuhongsong@iie.ac.cn

孙利民 于 1998 年在国防科学技术大学计算机体系结构专业获得工学博士学位。现中国科学院信息工程研究所第四研究室研究员。物联网安全、工业控制系统安全。研究兴趣包括工控入侵诱捕、工控态势感知。Email: sunlimin@iie.ac.cn