中国科技期刊卓越行动计划项目入选期刊

控制与决策

CONTROL AND DECISION

基于多目标的无人值守工业控制系统安全策略协同决策

郭伟杰, 刘璐, 杜鑫, 周纯杰

引用本文:
郭伟杰,刘璐,杜鑫,周纯杰. 基于多目标的无人值守工业控制系统安全策略协同决策[J]. 控制与决策, 2024, 39(11): 3617–3627.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2023.1053

基于多目标的无人值守工业控制系统安全策略协同决策

郭伟杰[1], 刘 璐[1], 杜 鑫[1], 周纯杰[1,2†]

(1. 华中科技大学 人工智能与自动化学院，武汉 430074；2. 华中科技大学 网络空间安全学院，武汉 430074)

摘 要: 工业互联网的发展实现了工业生产的“少人化”“无人化”的同时也使得工业控制系统面临着更多的信息安全威胁. 针对信息安全防护需求实现过程中信息安全策略与功能安全策略存在冲突以及无人值守工业控制系统现场端与监控端的安全策略决策目标存在冲突的问题,提出一种基于多目标的安全策略协同决策方法. 通过设置安全策略协同规则实现信息安全策略与功能安全策略的协同,构建风险收益量化模型和冲突风险量化模型对安全策略的风险收益属性以及实施所增加的冲突风险进行量化,结合各现场端的可接受风险阈值,利用多目标优化算法实现无人值守工业控制系统现场端与监控端的协同决策. 最后,以煤矿行业无人值守压风机控制系统为对象,通过仿真验证所提出方法的有效性.

关键词: 无人值守工业控制系统；信息安全；功能安全；协同决策；多目标；风险控制

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2023.1053

引用格式: 郭伟杰,刘璐,杜鑫,等. 基于多目标的无人值守工业控制系统安全策略协同决策[J]. 控制与决策, 2024, 39(11): 3617-3627.

Multi-objective cooperative decision-making of security and safety strategies for unattended industrial control system

GUO Wei-jie[1], *LIU Lu*[1], *DU Xin*[1], *ZHOU Chun-jie*[1,2†]

(1. School of Artificial Intelligence and Automation，Huazhong University of Sicience and Technology，Wuhan 430074，China；2. School of Cyber Science and Engineering, Huazhong University of Sicience and Technology，Wuhan 430074，China)

Abstract: The development of industrial Internet has realized the “reduced manpower” and “unmanned” industrial production. At the same time, industrial control systems are also facing more information security threats. Aiming at the conflict between information security strategies and functional safety strategies and the conflict between the security and safety strategies decision objectives of the field end and the monitoring end of the unattended industrial control system in the implementation process of information security protection requirements, this paper proposes a multiple-objective collaborative decision method of security and safety strategies. The collaboration of information security strategies and functional safety strategies is realized by setting security and safety strategies collaboration rules. A risk return quantification model is constructed to quantify the risk return attributes of security and safety strategies and a conflict risk quantification model is constructed to quantify the increased conflict risk associated with implementing security and safety strategies. Combining the acceptable risk thresholds of each field end, a multi-objective optimization algorithm is used to achieve collaborative decision-making between the field end and the monitoring end of the unattended industrial control system. Finally, the effectiveness of the proposed method is verified through simulation using the unattended pressure fan control system in the coal mining industry.

Keywords: unattended industrial control system；information security；functional safety；collaborative decision-making；multi-objective；risk control

0 引 言

物联网、大数据以及云计算等技术的发展使得无人值守工业控制系统(unmanned industrial control system, UICS)在煤矿、电力以及石油化工等行业得到了广泛应用[1-3]. 相比于需要工作人员亲临生产现场记录数据或操作设备的工业控制系统,UICS的优点在于可以实现生产过程的自动化和无人化,提高生产效率和生产质量,同时减少了人为操作的错误和安

收稿日期: 2023-07-27；**录用日期:** 2023-12-03.

基金项目: 国家自然科学基金项目(62127808, 62320106005).

†通讯作者. E-mail: cjiezhou@hust.edu.cn.

全风险. 另外, UICS 还具有远程监控和控制能力, 可以通过互联网实现对生产过程的远程监控和管理, 提高生产过程的灵活性和适应性. 然而, 互联网技术的引入也使得 UICS 面临更多的信息安全威胁[4-5]. 攻击者会通过扫描 UICS 监控端和现场端网络设备漏洞并获取权限, 进而篡改控制设备系统参数, 引起生产事故发生, 最终导致人员伤亡、环境污染以及巨大的财产损失. 因此, 研究针对 UICS 的信息安全防护方法对于保障 UICS 的安全平稳运行、避免重大安全事故的发生具有重要意义.

安全策略决策作为信息安全防护体系中的重要环节, 其目标是根据检测到的系统入侵证据同时结合系统安全态势, 生成合适的信息安全策略并实施, 最终使系统风险降低至可接受的范围内[6]. Zhai 等[7] 针对工业生产过程中系统状态具有不确定特征的问题, 提出了一种具有自适应性和可解释性的基于数据驱动的连续决策模型. Chung 等[8] 提出了基于博弈论的安全策略决策方法, 结合 Q-Learning 算法构建了攻防博弈模型. Pan 等[9] 利用 Petri 网对攻击者和防御者的行为进行建模, 根据攻防博弈结果选择合适的安全策略. 作为典型的分层控制系统, UICS 通过监控端对各现场端进行协调控制, 确保系统整体安全稳定运行. 因此, UICS 监控端与现场端的安全策略决策目标具有一定的差异性, 现有的安全策略决策方法大都是将监控端与现场端的安全策略基于相同目标进行决策, 无法直接应用于 UICS.

信息安全是防止系统硬件、软件以及数据等遭受外部未经授权的篡改、泄露导致系统损失; 功能安全是防止系统功能失效并引发安全事故, 进而导致人员伤亡、环境污染等事件的发生. UICS 作为典型的信息域与物理域紧密耦合的系统, 信息攻击的渗透可能会引发功能安全问题. 因此, 研究 UICS 信息安全与功能安全一体化方法是保障 UICS 安全运行的必然趋势[10]. 现阶段针对信息安全与功能安全一体化研究主要集中于分析信息安全失效与功能安全失效之间的因果关系[11-14], 例如, Kaloudi 等[11] 提出了一体化安全自适应压力测试方法, 利用强化学习技术识别系统在正常或者失效状态下的信息攻击路径. Ji 等[12] 构建了信息攻击路径模型, 提出一体化蝴蝶结法生成防御路径, 根据系统关键变量值的范围确定功能安全与信息安全一体化风险等级. 然而, 由于信息安全防护目标与功能安全防护目标不同, 两类安全策略之间存在一定的冲突, 不加协调地实施两类安全策略可能不仅无法提高系统的安全防护能力, 甚至使系统崩溃. 针对此问题, Novak 等[15] 构建了一种信息安全与功能安全一体化生命周期模型, 从需求层和功能层对两类安全策略进行协同. 靳江红等[16] 应用故障模式与脆弱性影响分析技术评估信息安全与功能安全的兼容性, 利用事件树给出信息安全策略与功能安全策略协同解决方案. 目前, 针对信息安全策略与功能安全策略的协同研究主要聚焦于平衡两类安全需求或者通过定性的方法实现两类安全策略的协同, 很少考虑如何在系统运行阶段通过定量的方法协同两类安全策略.

针对上述问题, 本文提出一种基于多目标的 UICS 安全策略协同决策方法框架. 首先基于安全策略协同规则实现监控端与现场端的信息安全策略与功能安全策略协同; 然后构建安全策略风险收益量化模型以及冲突风险量化模型, 对现场端和监控端的安全策略实施能够缓解的信息安全风险以及增加的冲突风险进行量化; 最后利用多目标优化算法生成各现场端的最优安全策略, 通过对监控端的协同风险进行量化; 生成监控端最优安全策略.

1 基于多目标的 UICS 安全策略协同决策框架

1.1 UICS 架构

UICS 是一种基于计算机技术、自动化技术和通信技术的工业控制系统, 能够对设备 (空压机、变电站、自动化生产线等) 的过程参数和生产信息集中监控, 并将它们通过交换机上传至服务器, 实现现场信息实时监控功能. UICS 主要包括现场端和监控端两部分, 典型系统架构如图 1 所示.

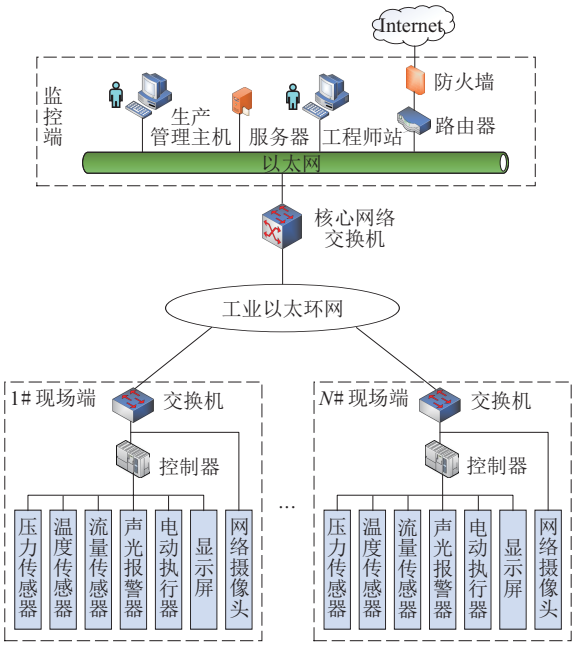

图 1 UICS 架构

现场端主要包括交换机、PLC、各类传感器/执行器以及网络摄像头等设备. 传感器负责实时获取现场端的压力、温度以及流量等关键数据, PLC 和电动执行器主要负责完成信号处理与传输、接收各类操作指令进行设备控制以及联锁保护等重要功能[17]. PLC 和网络摄像头通过交换机接入到工业以太环网, 实现了现场端与监控端的远程数据传输. 监控端主要包括生产管理主机、核心网络交换机、服务器以及工程师站等设备. 生产管理主机负责现场端的生产调度, 核心网络交换机负责给监控端提供现场端的实时数据, 服务器负责完成数据的存储和处理功能, 并交由工程师站调用, 工程师站对数据进一步处理和显示.

一方面, 信息安全策略的防护目标与功能安全策略的防护目标存在一定冲突; 另一方面, 监控端安全策略决策的目标是确保系统全局能够将安全风险控制在可接受范围内, 而现场端的安全策略决策目标为将本地安全风险控制在可接受的范围内, UICS 监控端与现场端安全策略决策目标同样存在冲突. 因此, 实现信息安全策略与功能安全策略协同以及 UICS 现场端与监控端的协同是研究 UICS 安全策略决策方法的两大挑战.

1.2　安全策略协同决策方法框架

结合 UICS 的结构特征和应用场景, 本文提出一种 UICS 安全策略协同决策方法, 总体框架如图 2 所示. 利用安全策略协同规则实现信息安全策略与功能安全策略协同, 构建风险收益量化模型和冲突风险量化模型, 实现安全策略的风险收益属性和实施所增加的功能安全风险量化. 考虑现场端安全策略的风险收益、实施所增加的冲突风险以及实施成本, 结合多目标优化算法实现 UICS 各现场端的安全策略决策. 根据各现场端的安全策略决策结果, 考虑监控端安全策略的风险收益与实施所增加的冲突风险, 结合多目标优化算法实现 UICS 现场端的安全策略决策.

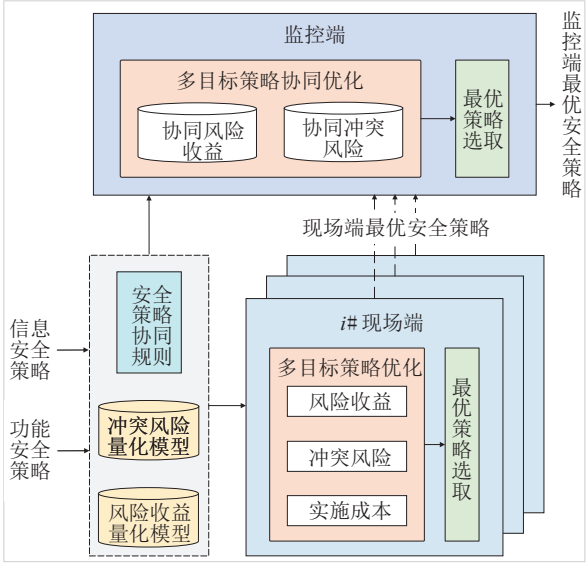

图 2　UICS 安全策略协同决策框架

2　基于多目标的 UICS 安全策略协同决策方法

2.1　信息安全策略与功能安全策略协同

2.1.1　安全策略冲突定义与形式化建模

安全策略冲突是指两类安全策略针对同一对象实施的动作互相矛盾或者占用系统资源存在冲突的情况. 例如当系统遭受信息攻击导致通信数据异常时, 信息安全策略通常选择对数据进行加密或关闭通信链路, 优先保障系统的机密性; 而功能安全策略通常选择对通信链路进行冗余重构, 优先保障系统的实时性, 两类安全策略的防护目标无法同时实现. 因此根据策略的作用对象确定存在冲突的安全策略, 结合安全策略的功能属性设置策略实施优先级规则, 进而实现信息安全策略和功能安全策略的协同. 对信息安全策略和功能安全策略进行形式化建模如下:

$$M = (\text{objectID}, \text{function}, \text{category}, \text{sl}). \tag{1}$$

其中: objectID 为安全策略实施的作用对象; function 为安全策略的功能属性, function $=0$ 表示防御策略(预防、检测故障或攻击的发生), function $=1$ 表示恢复策略(对故障或攻击作出响应, 使系统恢复至正常或安全状态); category 表示安全策略的安全属性, category $=0$ 为信息安全策略, category $=1$ 为功能安全策略; sl 表示安全策略的信息安全防护等级.

2.1.2　安全策略协同规则

本文根据冲突策略的功能属性, 即恢复策略冲突和防御策略冲突, 设置相应的协同规则.

协同规则 1　当信息安全恢复策略与功能安全恢复策略发生冲突, 即

$$M_i.\text{objectID} = M_j.\text{objectID}, \tag{2}$$

$$M_i.\text{function} = M_j.\text{function} = 1, \tag{3}$$

$$M_i.\text{category} \neq M_j.\text{category} \tag{4}$$

时, 以保障功能安全为主, 优先选择功能安全策略. 例如, 为了恢复因信息攻击导致失效的 PLC 控制功能, 信息安全防护通常采用重启 PLC, 而功能安全防护通常采用对 PLC 进行冗余切换, 选择功能安全策略确保系统在运行过程中的实时性、可靠性和安全性.

协同规则 2　当信息安全防御策略与功能安全防御策略发生冲突, 即

$$M_i.\text{objectID} = M_j.\text{objectID}, \tag{5}$$

$$M_i.\text{function} = M_j.\text{function} = 0, \tag{6}$$

$$M_i.\text{category} \neq M_j.\text{category} \tag{7}$$

时,优先选择sl较大的安全策略. 如果sl相同,则优先选择功能安全策略. 例如,为了确保通信数据的完整性,信息安全防护通常采用消息验证码(message authentication code, MAC)校验,而功能安全防护通常采用循环冗余(cyclic redundancy check, CRC)校验,因为MAC校验在缺乏秘钥的条件下能够检测随机失效,所以选择sl更高的信息安全策略.

2.1.3 安全策略协同算法

安全策略的协同过程可形式化如算法1所示. 在UICS运行过程中,信息安全防护机制与功能安全防护机制当已知攻击在系统中的作用位置并评估到系统当前风险值超过了可接受的风险阈值后,分别生成信息安全策略集M_{se}和功能安全策略集M_{sa},通过在M_{se}中随机选取一个策略,遍历M_{sa}中具有相同功能属性的策略,然后依据2.1.2节制定的协同规则删除冲突策略,最终得到协同安全策略集$M_{\text{s\&s}}$.

算法1 安全策略协同算法.

输入: 信息安全策略集M_{se},功能安全策略集M_{sa};

输出: 协同安全策略集$M_{\text{s\&s}}$.

初始化: $M_{\text{con}} \leftarrow \varnothing$; $M_{\text{s\&s}} \leftarrow \varnothing$; $M \leftarrow M_{\text{se}} \bigcup M_{\text{sa}}$.

step 1: while M_{se}不为空集

step 2: $\gamma \leftarrow$ 从策略集M_{se}中任选一个策略

step 3: $M_{\text{Temp}} \leftarrow M$ find object and function (M_{sa}, γ)./*在M_{sa}中寻找与γ具有相同对象和功能的策略*/

step 4: if Sizeof ($M_{\text{Temp}} > 1$)

step 5: if γ. function $= 1$

step 6: $M_{\text{con}} \leftarrow M_{\text{con}} \bigcup \{\gamma\}$

step 7: else

step 9: if γ. sl $\leqslant M_{\text{Temp}}$.sl

step 10: $M_{\text{con}} \leftarrow M_{\text{con}} \bigcup \{\gamma\}$

step 11: else

step 12: $M_{\text{con}} \leftarrow M_{\text{con}} \bigcup \{M_{\text{Temp}}\}$

step 13: end if

step 14: end if

step 15: end if

step 16: $M_{\text{se}} \leftarrow M_{\text{se}} - \{\gamma\}$

step 17: end while

step 18: $M_{\text{s\&s}} \leftarrow M - M_{\text{con}}$

step 19: return $M_{\text{s\&s}}$

2.2 风险收益量化模型与冲突风险量化模型

实施安全策略的目的是将系统的风险降低至可接受的范围内,因此对安全策略进行决策需要对各安全策略的风险收益进行量化. 构建安全策略风险收益量化模型,如图3所示,包括由攻击节点a_i组成的攻击层、失效功能节点f_i组成的功能层、安全事故节点e_i组成的事故层以及损失资产z_i组成的资产层. 在安全策略风险收益量化模型中,有向边指向的节点称为子节点,有向边被指向的节点称为父节点,不存在父节点的节点称为根节点,不存在子节点的节点称为目标节点.

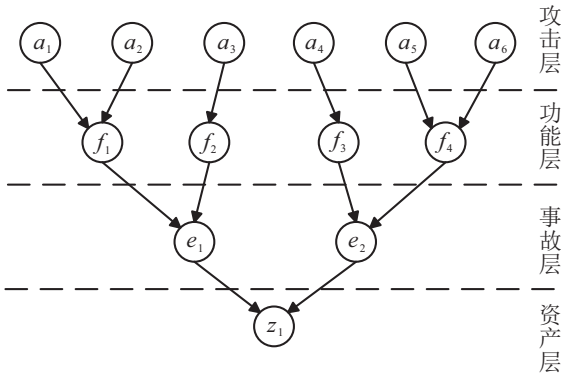

图3 安全策略风险收益量化模型

根据父节点事件的发生概率确定子节点事件的发生概率,计算如下:

$$P(i) = 1 - \prod_{j=1}^{n}(1 - P(j)). \tag{8}$$

其中: $P(i)$为子节点事件的发生概率, $P(j)$为父节点事件的发生概率.

根据式(8)计算资产损失概率$P(z_i)$,结合资产实际价值$q(z_i)$得到初始风险值R_0,计算公式如下:

$$R_0 = \sum_{i=1}^{n} P(z_i)q(z_i). \tag{9}$$

分析安全策略M_i能够防御的信息攻击a_i或者恢复的失效功能f_i,将对应的a_i或f_i节点概率置零,根据式(9)计算重置后的风险值R',则安全策略M_i的风险收益量化值计算如下:

$$\text{RR}(M_i) = R_0 - R'. \tag{10}$$

实施安全策略可能会导致UICS功能失效事件的发生,从而增加UICS功能安全风险. 实施安全策略增加的功能安全风险(冲突风险)取决于该策略所导致的失效功能对于系统总目标的重要程度. 由于UICS功能结构相对固定,可抽象为具有层次特征的功能树模型[18],即安全策略冲突风险量化模型. 图4为安全策略冲突风险量化模型示意图. 其中: f^*为系统最终要实现的目标功能; $f_1, \ldots, f_k$为中间

功能, $f_{11},\ldots,f_{1c},f_{k1},\ldots,f_{kc}$ 为基本功能; $\omega_i,\ldots,\omega_k$ 为中间功能 $f_1,\ldots,f_k$ 在完成目标功能方面 f^* 的重要程度权重; $\omega_{11},\ldots,\omega_{1c},\omega_{k1},\ldots,\omega_{kc}$ 同理.

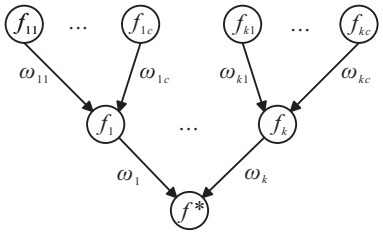

图 4　安全策略冲突风险量化模型

本文利用层次分析法(AHP)对系统功能重要度进行量化, 该方法是一种层次化权重计算方法, 因其只需较少的计算数据, 且计算过程相对简易, 被广泛用于工业控制系统的风险评估[19], 计算步骤如下.

step 1: 确定评价元素 $U=(f_e,\ldots,f_f,\ldots,f_g)$, U 为实施安全策略导致的同一层次的失效功能集合.

step 2: 构建模糊判断矩阵 $J=(j_{xy})_{n\times n}$ 如表 1 所示. 其中: $j_{xy}\times j_{yx}=1; x,y=1,2,\ldots,n$; j_{xy} 表示 f_x 相对 f_y 的重要程度, 评价元素的重要程度判断标准如表 2 所示.

表 1　模糊判断矩阵

J	f_1	f_2	$\cdots$	f_n
f_1	j_{11}	j_{12}	$\cdots$	j_{1n}
f_2	j_{21}	j_{22}	$\cdots$	j_{2n}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
f_n	j_{n1}	j_{n2}	$\cdots$	j_{nn}

表 2　判断矩阵元素标度表

标度	含义
1	f_x 和 f_y 同等重要
3	f_x 比 f_y 稍微重要
5	f_x 比 f_y 明显重要
7	f_x 比 f_y 强烈重要
9	f_x 比 f_y 极端重要
2, 4, 6, 8	上述两相邻判断的中值

step 3: 完成构建判断矩阵 J 后对其进行一致性验证, 验证指标为

$$\mathrm{CI}=\frac{\lambda-n}{n-1},\tag{11}$$

其中 λ 为判断矩阵 J 的最大特征根. 获取一致性比率 $\mathrm{CR}=\mathrm{CI}/\mathrm{RI}$, RI 为平均一致性指数. 指数值范围如表 3 所示. 若 $\mathrm{CR}<0.1$, 则判定矩阵 J 的一致性在允许范围内, 通过一致性校验. 若 $\mathrm{CR}\geqslant 0.1$, 则判定 J 的一致性不在允许范围内, 需要重新调整矩阵元素, 直至通过一致性校验.

表 3　平均一致性指数值列表

n	1	2	3	4	5	6	7	8	9
RI	0	0	0.52	0.89	1.12	1.24	1.32	1.41	1.45

step 4: 通过一致性校验后, 计算判断矩阵 J 的特征根, 采用最大特征值法获取失效功能 $f_e,\ldots,f_f,\ldots,f_g$ 的重要度权重 $\omega_e,\ldots,\omega_f,\ldots,\omega_g$.

安全策略 M_i 的冲突风险量化值计算如下:

$$\mathrm{RC}(M_i)=\sum_{n=1}^{k}\omega_n\sum_{j=1}^{l}\omega_{nj}.\tag{12}$$

其中: ω_{nj} 为实施安全策略 M_i 导致的失效功能 f_{nj} 的权重, ω_n 为基本功能 f_{nj} 对应的中间功能 f_n 的权重.

2.3　基于多目标的现场端与监控端安全策略协同决策方法

2.3.1　现场端安全策略决策形式化描述

考虑 UICS 现场端实时性以及资源有限性特征, 将安全策略的实施成本作为决策目标之一. 安全策略实施成本通过时间资源消耗、计算资源消耗和存储资源消耗两个属性进行描述, 计算公式如下:

$$\mathrm{CT}(M_i)=\omega_t\times\mathrm{time}+\omega_c\times\mathrm{comp}+\omega_s\times\mathrm{stor}.\tag{13}$$

其中: ω_t、ω_c、ω_s 表示各成本属性的权重, $\omega_t+\omega_c+\omega_s=1$, time、comp、stor 表示各成本属性量化等级. 成本属性等级评分如表 4 所示.

表 4　成本属性等级评分标准

时间/计算/存储资源消耗	等级
很多	5
多	4
中等	3
少	2
很少	1

对于 $i\#$ 现场端, 定义二进制决策变量 $X_i=\{x_{i1},x_{i2},\ldots,x_{in}\}_{1\times n}$, x_{ij} 表示 $i\#$ 现场端检测到异常(攻击或失效)后生成的安全策略, x_{ij} 取值如下:

$$x_{ij}=\begin{cases}1,\ \text{执行该安全策略;}\\ 0,\ \text{otherwise.}\end{cases}\tag{14}$$

则 $i\#$ 现场端安全策略决策问题可形式化为一个多目标优化问题, 其中优化目标包括风险收益、冲突风险、实施成本. 该问题的形式化描述如下:

$$\begin{aligned}&\max\langle\mathrm{RR}(X_i)\rangle,\min\langle\mathrm{RC}(X_i)\rangle,\mathrm{CT}(X_i);\\ &\text{s.t. }\ \mathrm{RR}(X_i)\geqslant\mathrm{RR}_{Thi\#},\\ &\qquad\mathrm{RC}(X_i)\leqslant\mathrm{RC}_{Thi},\\ &\qquad\mathrm{CT}(X_i)\leqslant\mathrm{CT}_{Thi}.\end{aligned}\tag{15}$$

其中: $\mathrm{RR}(X_i)$、$\mathrm{RC}(X_i)$、$\mathrm{CT}(X_i)$ 分别为安全策略 X_i 下 $i\#$ 现场端的风险收益、冲突风险和安全策略实施

成本,$\mathrm{RR}_{Thi\#}$、RC_{Thi}、CT_{Thi}分别为$i\#$现场端可接受的风险收益阈值、冲突风险阈值和安全策略实施成本阈值.

2.3.2 监控端安全策略决策形式化描述

为了确保UICS各现场端能够平稳运行,实施监控端安全策略和现场端安全策略,需要确保信息安全风险降低至可接受范围内以及控制实施安全策略增加的冲突风险在可接受的范围内. UICS各现场端具有一定的自主性,因此监控端安全策略决策需要根据各现场端安全策略决策结果,确定监控端需要协同降低的信息安全风险以及协同控制的冲突风险.

定义二进制决策变量$Y=\{y_1,y_2,\dots,y_m\}$,y_i表示监控端在检测到异常(攻击或失效)后生成的安全策略,取值如下:

$$y_i=\begin{cases}1,\ \text{执行该安全策略};\\ 0,\ \text{otherwise}.\end{cases}\tag{16}$$

则监控端安全策略决策问题可形式化为一个多目标优化问题,其中优化目标包括风险收益、冲突风险. 该问题的形式化描述如下所示:

$$\begin{aligned}&\max\langle \mathrm{RR}(Y)\rangle,\min\langle \mathrm{RC}(Y)\rangle;\\ &\text{s.t. }\ \mathrm{RR}(Y)\geqslant\max(R_{0i}-\mathrm{RR}_{Thi}-\mathrm{RR}(X_i)),\\ &\qquad \mathrm{RC}(Y)\leqslant\min(\mathrm{RC}_{Thi}-\mathrm{RC}(X_i)).\end{aligned}\tag{17}$$

其中:$\mathrm{RR}(Y)$、$\mathrm{RC}(Y)$分别表示在安全策略Y下,监控端的风险收益、冲突风险;RR_{Thi},R_{0i}分别表示$i\#$现场端可接受的信息安全风险阈值以及初始信息安全风险值.

2.3.3 基于NSGA-II的现场端与监控端安全策略协同决策

当生成的安全策略较少时,可通过“遍历”的方法评价各安全策略相对于目标的优劣情况,最终得到Pareto最优解. 当生成的安全策略较多时,“遍历”方法耗时较长,可采用多目标优化算法,如模拟退火算法、多目标粒子群算法、蚁群算法、NSGA-II算法等. 其中NSGA-II具有很好的收敛性,其解的Pareto前端具有相对均匀的密度,采用精英机制能够较快地获取Pareto最优解[20]. 本文利用NSGA-II算法对UICS现场端和监控端进行安全策略决策,NSGA-II算法流程如算法2所示.

算法2 NSGA-II算法总体流程.

初始化: $k\leftarrow 0$,迭代次数上限$K_{\max}$,种群规模P_{size},初始种群P_0.

step 1: 评价P_0中个体的各目标值.

step 2: 计算种群P_0中个体的支配等级i_{rank}和拥挤度i_{distance}.

step 3: while $K\leqslant K_{\max}$ do.

step 4: 从种群P_k中选取一定数量的个体.

step 5: 通过单点交叉和位变异的操作生成子代种群Q_k.

step 6: 评价子代种群Q_k中个体的各目标值.

step 7: 将P_k和Q_k进行合并,得到种群R_k.

step 9: 计算种群R_k中各个体的支配等级i_{rank}和拥挤度i_{distance}.

step 10: 从种群R_k中挑选P_{size}个体作为新一代种群R_{k+1}.

step 11: $k\leftarrow k+1$.

step 12: end while.

对现场端和监控端生成的Pareto解集进行优先级评价,定义$i\#$现场端和监控端的Pareto理想前端,即

$$\langle \max_{\forall X_i\in\text{Pareto}}\mathrm{RR}_i,\min_{\forall X_i\in\text{Pareto}}\mathrm{RC}_i,\max_{\forall X_i\in\text{Pareto}}\mathrm{CT}_i\rangle,\tag{18}$$

$$\langle \max_{\forall Y\in\text{Pareto}}\mathrm{RR}_i,\min_{\forall Y\in\text{Pareto}}\mathrm{RC}_i\rangle.\tag{19}$$

则基于L_2范数的$i\#$现场端和监控端的Pareto解X_{ij},Y_m与理想前端的距离分别为

$$\|\mathrm{Dis}(X_{ij})\|=\sqrt{(\mathrm{RR}^{\text{dis}}_{X_{ij}})^2+(\mathrm{RC}^{\text{dis}}_{X_{ij}})^2+(\mathrm{CT}^{\text{dis}}_{X_{ij}})^2},\tag{20}$$

$$\|\mathrm{Dis}(Y_m)\|=\sqrt{\mathrm{RR}^{\text{dis}\ 2}_{Y_m}+\mathrm{RC}^{\text{dis}\ 2}_{Y_m}}.\tag{21}$$

其中

$$\mathrm{RR}^{\text{dis}}_{X_{ij}}=\frac{\max\limits_{\forall X_i\in\text{Pareto}}\mathrm{RR}_i-\mathrm{RR}_i(X_{ij})}{\max\limits_{\forall X_i\in\text{Pareto}}\mathrm{RR}_i-\min\limits_{\forall X_i\in\text{Pareto}}\mathrm{RR}_i},\tag{22}$$

$$\mathrm{RC}^{\text{dis}}_{X_{ij}}=\frac{\mathrm{RC}(X_{ij})-\min\limits_{\forall X_i\in\text{Pareto}}\mathrm{RC}_i}{\max\limits_{\forall X_i\in\text{Pareto}}\mathrm{RC}_i-\min\limits_{\forall X_i\in\text{Pareto}}\mathrm{RC}_i},\tag{23}$$

$$\mathrm{CT}^{\text{dis}}_{X_{ij}}=\frac{\mathrm{CT}(X_{ij})-\min\limits_{\forall X_i\in\text{Pareto}}\mathrm{CT}_i}{\max\limits_{\forall X_i\in\text{Pareto}}\mathrm{CT}_i-\min\limits_{\forall X_i\in\text{Pareto}}\mathrm{CT}_i},\tag{24}$$

$$\mathrm{RR}^{\text{dis}}_{Y_m}=\frac{\max\limits_{\forall Y\in\text{Pareto}}\mathrm{RR}_i-\mathrm{RR}(Y_m)}{\max\limits_{\forall Y\in\text{Pareto}}\mathrm{RR}_i-\min\limits_{\forall Y\in\text{Pareto}}\mathrm{RR}_i},\tag{25}$$

$$\mathrm{RC}^{\text{dis}}_{Y_m}=\frac{\mathrm{RC}(Y_m)-\min\limits_{\forall Y\in\text{Pareto}}\mathrm{RC}_i}{\max\limits_{\forall Y\in\text{Pareto}}\mathrm{RC}_i-\min\limits_{\forall Y\in\text{Pareto}}\mathrm{RC}_i}.\tag{26}$$

根据计算得到的$\|\mathrm{Dis}(X_{ij})\|$、$\|\mathrm{Dis}(Y_m)\|$确定现场端和监控端各安全策略Pareto解的优先级. $\|\mathrm{Dis}(X_{ij})\|$、$\|\mathrm{Dis}(Y_m)\|$越小,对应的安全策略解集优先级越高,本文选取现场端和监控端优先级最高的

Pareto解作为多目标优化问题的最终解.

3　仿真研究与分析

为验证所提出方法的有效性,采用如图5所示的煤矿行业无人值守压风机控制系统为仿真对象. 该系统通过控制风机压缩空气,为煤矿井下设备提供动力源并且将新鲜空气送入矿井下,为煤矿生产提供安全保障. 图中系统包括2个现场端和监控端,每个现场端包括交换机、控制器(压风机压力控制器JC、风包压力控制器TC、风包温度控制器FC)以及物理设备. 物理设备包括传感器(压风机压力传感器JP、风包压力传感器FP、风包温度传感器FT)、执行器(进风阀、出风阀以及排污阀). 监控端包括生产管理主机1和主机2、Web服务器、控制服务器、工程师站等. 现场端通过交换机将现场实时数据上传到监控端,监控端通过核心网络交换机向各现场端发送控制命令. 为了模拟信息攻击渗透影响过程,对系统设置信息安全漏洞,例如生产管理主机漏洞(CVE-2015-0728,跨站脚本攻击(CSS)漏洞)、交换机漏洞(CVE-2021-33514,允许执行任意SQL命令)、控制器漏洞(CVE-2013-0659,任意代码执行漏洞)等.

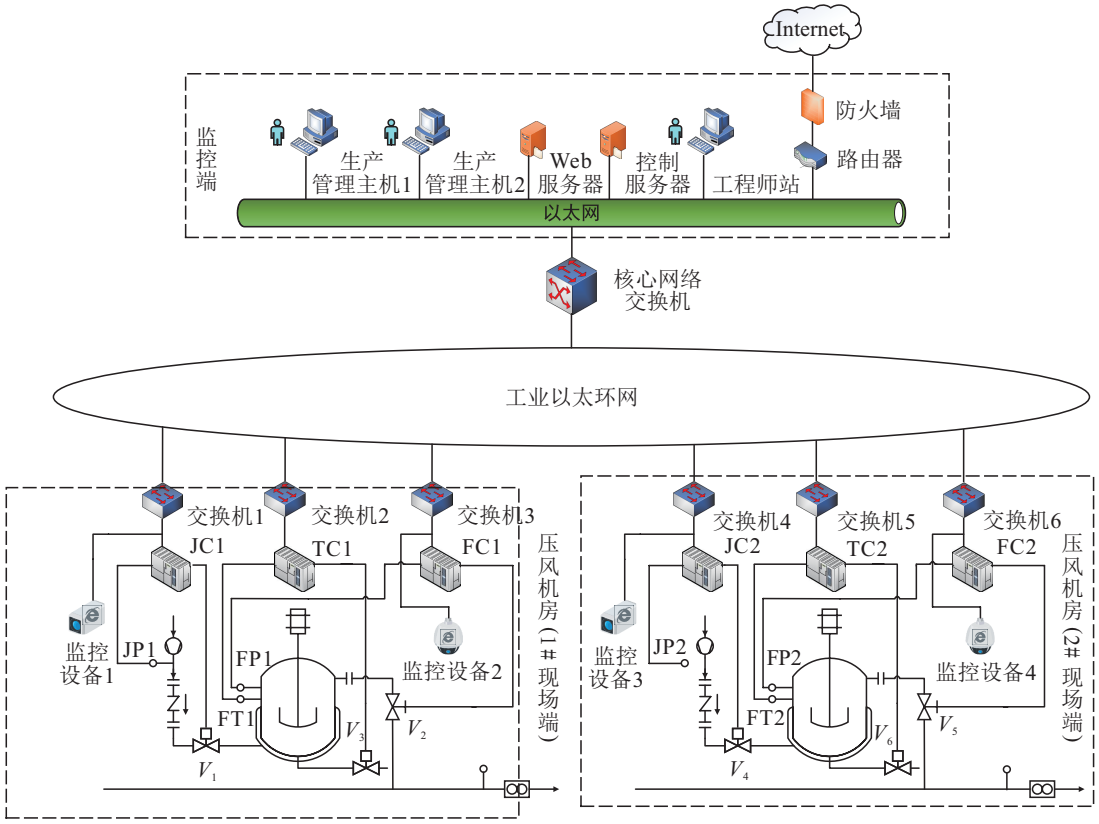

图 5　煤矿行业无人值守压风机控制系统简图

3.1　信息安全策略与功能安全策略协同结果分析

本文设置如下攻击场景: 1#现场端受到信息攻击,1#现场端和监控端检测到信息攻击导致的异常,为了降低信息安全风险,入侵响应机制和功能安全防护机制生成相应的信息安全策略和功能安全策略,具体如表5所示.

根据2.1.2节设置的信息安全策略与功能安全策略协同规则,对现场端与监控端的信息安全策略和功能安全策略进行协同,最终得到协同安全策略集如表6所示.

3.2　风险收益量化模型和冲突风险量化模型构建

根据信息攻击的渗透影响过程,即信息攻击导致功能失效,进一步引起安全事故,最终导致资产损失,

表 5　未协同信息安全策略与功能安全策略集

	信息安全	功能安全
监控端	T_{se1}: 关闭工程师站	T_{sa1}: CRC校验
	T_{se2}: 关闭生产管理主机	T_{sa2}: 通信数据添加时间戳
	T_{se3}: 关闭核心网络交换机	T_{sa3}: 通信数据添加序列号
	T_{se4}: 关闭控制服务器	
	T_{se5}: 通信数据加密	
	T_{se6} :MAC校验	
现场端	N_{se1}: 重启控制器FC1	N_{sa1}: 传感器JP1冗余切换
	N_{se2}: MAC校验	N_{sa2}: CRC校验
	N_{se3}: 上位机通信数据加密	N_{sa3}: 总线数据添加时间戳
		N_{sa4}: 总线数据添加序列号
		N_{sa5}: 模拟量输入终止,控制器FC1输出故障安全状态

表 6 协同安全策略集

监控端	现场端
T_1: 关闭工程师站	N_1: 传感器 JP1 冗余切换
T_2: 关闭生产管理主机	N_2: MAC 校验
T_3: 关闭核心网络交换机	N_3: 上位机通信数据加密
T_4: 关闭控制服务器	N_4: 总线数据添加时间戳
T_5: 通信数据加密	N_5: 总线数据添加序列号
T_6: MAC 校验	N_6: 模拟量输入终止, 控制器 FC1 输出故障安全状态

以及无人值守压风机控制系统存在的信息安全漏洞, 分析面临的信息安全威胁, 构建无人值守压风机控制系统安全策略风险收益量化模型如图 6 所示, 各节点含义如表 7 所示.

根据无人值守压风机控制系统功能之间的关联关系, 构建安全策略冲突风险量化模型如图 7 所示, 各节点含义如表 8 所示.

3.3 UICS 安全策略协同决策结果分析

设置对 UICS 监控端进行以太网扫描事件概率 $P(a) = 0.001$, 资产价值 $z_1 = 90\,000$, $z_2 = 20\,000$, $z_3 = 40\,000$, 根据 2.2 节的安全策略风险收益量化公式以及 3.2 节构建的风险收益量化模型, 计算各安全策略的风险收益如图 8 所示. 根据 2.2 节的安全策略冲突风险量化公式以及 3.2 节构建的冲突风险量化模型, 计算各安全策略的冲突风险如图 9 所示. 根据 2.3.1 节现场端安全策略实施成本量化公式计算现场端各安全策略的实施成本如图 10 所示.

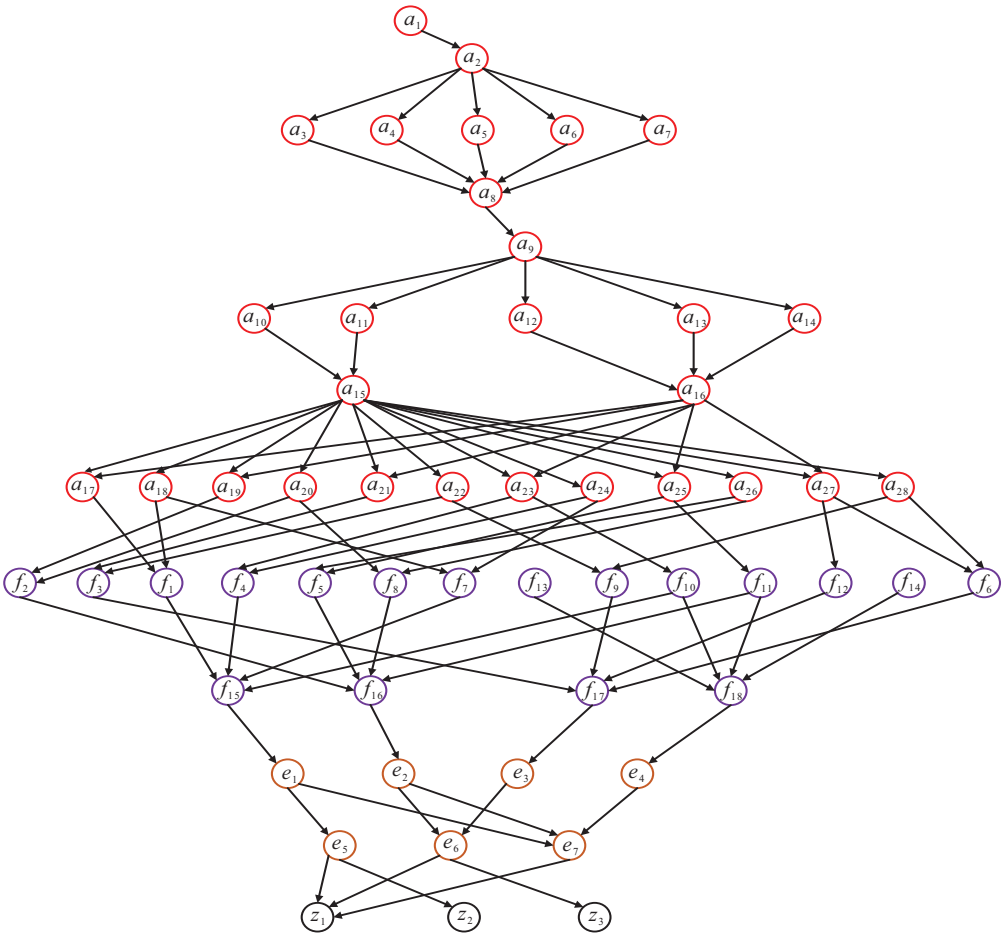

图 6 安全策略风险收益量化模型

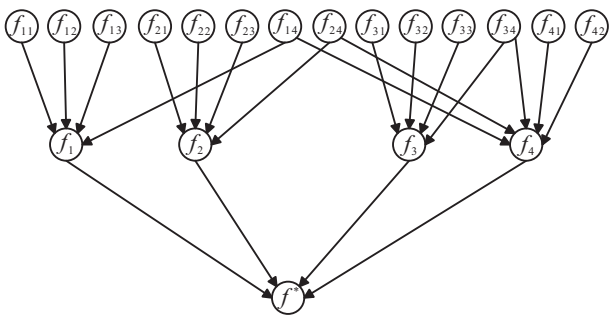

图 7 安全策略冲突风险量化模型

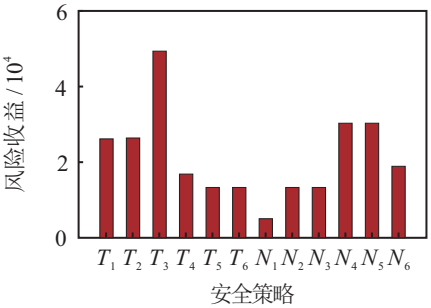

图 8 安全策略风险收益

表 7　安全策略风险收益量化模型节点含义

符号	含　义	符号	含　义	符号	含　义
a_1	对监控端以太网进行网络扫描	a_{20}	对FP1进行完整性(MAX/MIN)攻击	f_{11}	风包压力控制器配置和监控功能
a_2	风包压力采集功能	a_{21}	对FT1进行DoS攻击	f_{12}	风包温度控制器配置和监控功能
a_3	对Web服务器进行CSS攻击	a_{22}	对FT1进行完整性(MAX/MIN)攻击	f_{13}	管理主机1生产调度功能
a_4	对Web服务器进行认证旁路攻击	a_{23}	对JC1进行DoS攻击	f_{14}	管理主机2生产调度功能
a_5	对管理主机1进行缓冲区溢出攻击	a_{24}	对JC1进行完整性(MAX/MIN)攻击	f_{15}	压风机压力控制功能
a_6	对管理主机2进行远程代码攻击	a_{25}	对FC1进行DoS攻击	f_{16}	风包压力控制功能
a_7	对管理主机2进行缓冲区溢出攻击	a_{26}	对FC1进行完整性(MAX/MIN)攻击	f_{17}	风包温度控制功能
a_8	对工业以太网进行网络扫描	a_{27}	对TC1进行DoS攻击	f_{18}	生产调度功能
a_9	对工业以太网挂载设备进行设备扫描	a_{28}	对TC1进行完整性(MAX/MIN)攻击	e_1	压风机压力过大
a_{10}	对工程师站进行缓冲区溢出攻击	f_1	机头压风机采集功能	e_2	风包压力过大
a_{11}	对工程师站进行暴力破解攻击	f_2	风包压力采集功能	e_3	风包温度过高
a_{12}	对控制服务器进行SQL注入攻击	f_3	风包温度采集功能	e_4	生产调度错误
a_{13}	对控制服务器进行暴力破解攻击	f_4	进风阀V_1的压力控制功能	e_5	压风机爆炸
a_{14}	对控制服务器进行远程代码执行攻击	f_5	出风阀V_2的压力控制功能	e_6	风包爆炸
a_{15}	获取工程师站管理员权限	f_6	排污阀V_3的温度控制功能	e_7	供风量异常
a_{16}	获取控制服务器管理员权限	f_7	进风阀V_1控制指令计算功能	z_1	供风
a_{17}	对JP1进行DoS攻击	f_8	出风阀V_2控制指令计算功能	z_2	压风机
a_{18}	对JP1进行完整性(MAX/MIN)攻击	f_9	排污阀V_3控制指令计算功能	z_3	风包
a_{19}	对FP1进行DoS攻击	f_{10}	压风机压力控制器配置和监控功能		

表 8　安全策略冲突风险量化模型节点含义

符号	含　义
$f*$	井下供风功能
f_1	压风机压力控制功能
f_2	风包压力控制功能
f_3	风包温度控制功能
f_4	生产调度功能
f_{11}	机头压力采集功能
f_{12}	进风阀V_1的压力控制功能
f_{13}	进风阀V_2控制指令计算功能
f_{14}	压风机压力控制器配置和监控功能
f_{21}	风包压力采集功能
f_{22}	出风阀V_2的压力控制功能
f_{23}	出风阀V_2控制指令计算功能
f_{24}	风包压力控制器配置和监控功能
f_{31}	风包温度采集功能
f_{32}	排污阀V_3的温度控制功能
f_{33}	排污阀V_4控制指令计算功能
f_{34}	风包温度控制器配置和监控功能
f_{41}	管理主机1生产调度功能

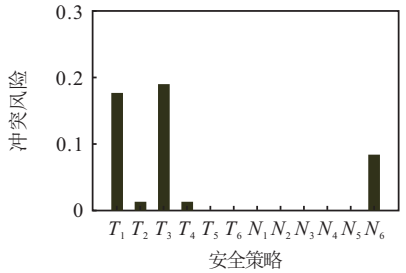

图 9　安全策略冲突风险

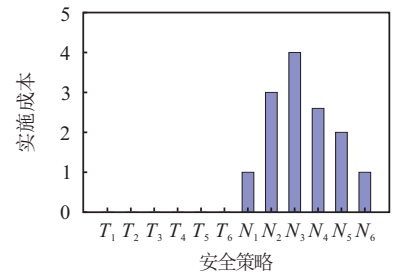

图 10　安全策略实施成本

表9给出了约束条件下最终得到的现场端安全策略解集参数、对应的评价指标和距离. 由表9可知, 理想Pareto前端为$\langle 84\,560, 0, 3\rangle$. 从安全距离可以看出安全策略集$X_{ij} = \{100110\}$距离理想点最近, 因此, 实施安全策略$N_1, N_4, N_5$具有最高的优先级.

表 9　现场端安全策略解集评价表

X_{ij}	RR_i	RC_i	CT_i	$\|\mathrm{Dis}(X_{ij})\|$
100111	84 560	0.084	6.6	1.414
000111	79 510	0.084	5.6	1.24
100011	54 260	0.084	4	1.2
000011	49 210	0.084	3	1.414
100110	65 650	0	5.6	0.66
000110	60 600	0	4.6	0.81

表10给出了约束条件下最终得到的监控端安全策略解集参数、对应的评价指标和距离. 由表10可知, 理想Pareto前端为$\langle 119\,200, 0.013\,2\rangle$. 从安全距离可以看出安全策略集$X_{ij} = \{010111\}$距离理想点最近, 实施安全策略$\{T_2, T_4, T_5, T_6\}$具有最高的优先级.

表 10　监控端安全策略解集评价表

Y_m	RR	RC	$\|\mathrm{Dis}(Y_m)\|$
011100	119 200	0.216 4	1
001011	79 180	0.19	1.04
010111	69 870	0.026 4	0.75
010011	53 020	0.013 2	1

3.4　后续分析

本节进一步分析安全策略的不同风险收益量化值以及冲突风险量化值对现场端与监控端策略决策结果的影响. 通过赋予风险收益量化模型中不同的资产价值以及冲突风险量化模型中功能节点不同的重要度权重, 得到新的安全策略风险收益量化值和安全策略冲突风险量化值如图11和图12所示. 基于提

出的安全策略协同决策方法得到相应的现场端与监控端的策略决策结果如表11和表12所示.

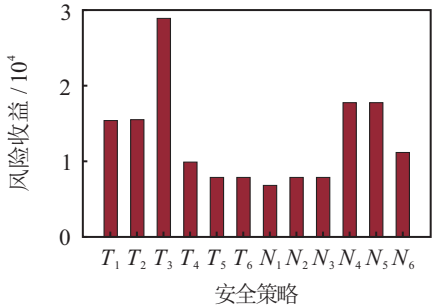

图 11 新安全策略风险收益

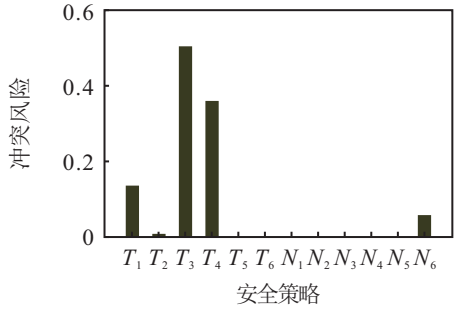

图 12 新安全策略冲突风险

表 11 新现场端安全策略解集评价表

X_{ij}	RR_i	RC_i	CT_i	$\|\mathrm{Dis}(X_{ij})\|$
100111	53 494.1	0.058	6.6	1.414
000111	46 680	0.058	5.6	1.26
100011	35 738.1	0.058	4	1.31
000011	28 924	0.058	3	1.414
100110	42 326.1	0	5.6	0.85
000110	35 512	0	4.6	0.86

表 12 新监控端安全策略解集评价表

Y_m	RR	RC	$\|\mathrm{Dis}(Y_m)\|$
110 011	46 638.7	0.144 4	0.54
110 111	56 535.7	0.504 4	0.99
010 111	31 246.6	0.008 4	1
010 011	60 146.6	0.512 8	1

由表11可见,实施安全策略N_1, N_4, N_5具有最高的优先级. 由于实施现场端安全策略产生的冲突风险较小,安全策略的冲突风险量化值的变化对现场端安全策略决策结果无影响,而安全策略的风险收益量化值由式(10)计算风险更新前后的差异值得到,资产价值的不同取值未改变安全策略风险收益量化值之间的相对大小,因此安全策略的风险收益量化值的变化对现场端安全策略决策结果无影响.

由表12可见,实施安全策略$\{T_1, T_2, T_5, T_6\}$具有最高的优先级. 由于层次分析法是通过构建重要度判断矩阵确定失效功能的相对权重,存在一定的主观性,反映了策略决策者之间的不同防护偏好,构建不同重要度判断矩阵最终得到的功能重要度权重也不同,从而导致监控端策略决策结果存在差异性.

3.5 方法对比与分析

现有策略决策方法主要针对特定的研究问题所提出,表13将所提出方法与现有相关工作从考虑问题的维度进行了定性比较,可以发现所提出基于多目标的策略决策方法充分考虑了UICS的分层控制特征,而现有策略决策方法很少考虑系统层级之间差异性问题. 此外,现有相关工作也很少考虑信息安全策略与功能安全策略之间的冲突问题. 本文根据安全策略的功能属性提出了相应的协同规则,并依据信息安全防护要求与功能安全防护准则,即从风险控制的角度通过定量的方法实现信息安全策略与功能安全策略的协同决策,相比于文献[16, 21]提出的基于定性的安全策略协同方法,前者兼具科学性和准确性.

表 13 所提出方法与现有相关工作的对比

方法	文献						
	本文	[6]	[21]	[22]	[23]	[24]	[25]
信息层决策	✓	✓	×	✓	✓	✓	×
物理层决策	✓	✓	✓	✓	✓	×	✓
策略冲突	✓	×	✓	×	×	×	×
系统层级特征	✓	×	×	✓	×	×	×
考虑安全风险	✓	✓	✓	×	×	✓	✓

4 结 论

本文提出了一种基于多目标的UICS安全策略协同决策方法,通过设置安全策略协同规则实现了UICS信息安全策略与功能安全策略的协同,构建了安全策略风险收益量化模型和冲突风险量化模型,并结合多目标优化算法实现了UICS现场端和监控端的安全策略协同决策. 所研究的安全策略为UICS在运行阶段通过入侵响应机制生成的信息安全策略和故障容忍机制生成的功能安全策略,后续将研究信息安全策略与功能安全策略一体化生成方法,进一步提高安全策略协同决策方法的准确性.

参考文献(References)

[1] 贾保峰. 煤化工行业地磅无人值守系统的应用研究[J]. 中国仪器仪表, 2022(11): 44-48.
(Jia B F. The application research of unattended weighometer system in coal chemical industry[J]. China Instrumentation, 2022(11): 44-48.)

[2] 鲜帅, 李正阳, 穆继亮. 基于无人值守的电网环境智能监测系统设计[J]. 自动化与仪器仪表, 2023(3): 204-208.
(Xian S, Li Z Y, Mu J L. Design of intelligent monitoring systemfor power grid environment based on unattended[J]. Automation & Instrumentation, 2023(3): 204-208.)

[3] 李秉军, 刘玉芳, 刘贵强, 等. 油田站场无人值守模式

的推广应用[J]. 石油石化节能, 2023, 13(1): 54-58.
(Li B J, Liu Y F, Liu G Q, et al. Promotion and application of unattended mode in oilfield stations[J]. Energy Conservation in Petroleum & Petrochemical Industry, 2023, 13(1): 54-58.)

[4] 孟庆勇, 顾闯. 煤矿工业互联网信息安全风险评估[J]. 工矿自动化, 2019, 45(8): 43-47.
(Meng Q Y, Gu C. Information security risk assessment of industrial internet of coal mine[J]. Industry and Mine Automation, 2019, 45(8): 43-47.)

[5] 戴洋. 浅析智能变电站监控系统网络安全渗透技术[J]. 网络安全技术与应用, 2023(1): 91-93.
(Dai Y. Analysis of network security penetration technology in intelligent substation monitoring system[J]. Network Security Technology & Application, 2023(1): 91-93.)

[6] Qin Y Q, Zhang Q, Zhou C J, et al. A risk-based dynamic decision-making approach for cybersecurity protection in industrial control systems[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2020, 50(10): 3863-3870.

[7] Zhai Y W, Lv Z, Zhao J, et al. Associative reasoning-based interpretable continuous decision making in industrial production process[J]. Expert Systems with Applications, 2022, 204: 117585.

[8] Chung K, Kamhoua C A, Kwiat K A, et al. Game theory with learning for cyber security monitoring[C]. IEEE 17th International Symposium on High Assurance Systems Engineering. Orlando, 2016: 7-15.

[9] Pan W, Wang M Z, Fu Y Y, et al. Cybersecurity decision making mechanism for defense strategies in vehicle networks[C]. Information Technology and Intelligent Transportation Systems. Cham: Springer, 2017: 611-621.

[10] Zhou C J, Li X, Yang S H, et al. Risk-based scheduling of security tasks in industrial control systems with consideration of safety[J]. IEEE Transactions on Industrial Informatics, 2020, 16(5): 3112-3123.

[11] Kaloudi N, Li J Y. AST-SafeSec: Adaptive stress testing for safety and security Co-analysis of cyber-physical systems[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 5567-5579.

[12] ji Z Z, Yang S H, Cao Y, et al. Harmonizing safety and security risk analysis and prevention in cyber-physical systems[J]. Process Safety and Environmental Protection, 2021, 148: 1279-1291.

[13] Carreras Guzman N H, Kozine I, Lundteigen M A. An integrated safety and security analysis for cyber-physical harm scenarios[J]. Safety Science, 2021, 144: 105458.

[14] Song G Z, Khan F, Yang M. Probabilistic assessment of integrated safety and security related abnormal events: A case of chemical plants[J]. Safety Science, 2019, 113: 115-125.

[15] Novak T, Gerstinger A. Safety- and security-critical services in building automation and control systems[J]. IEEE Transactions on Industrial Electronics, 2010, 57(11): 3614-3621.

[16] 靳江红, 夏侨丽, 莫昌瑜. 核安全级DCS功能安全与信息安全权衡技术[J]. 核动力工程, 2021, 42(1): 100-106.
(Jin J H, Xia Q L, Mo C Y. Integration technology of functional safety and cyber security for nuclear safety class DCS[J]. Nuclear Power Engineering, 2021, 42(1): 100-106.)

[17] Yuan X. Design of an EMS Unmanned Control System Based on PLC[C]. Proceedings of the 2014National Metallurgical Automation Information Network Annual Conference. Beijing: Metallurgical Automation Magazine, 2014: 312-316.

[18] Modarres M, Cheon S W. Function-centered modeling of engineering systems using the goal tree-success tree technique and functional primitives[J]. Reliability Engineering & System Safety, 1999, 64(2): 181-200.

[19] Chen J, Zhu H J, Chen Z X, et al. A security evaluation model based on fuzzy hierarchy analysis for industrial cyber-physical control systems[C]. IEEE International Conference on Industrial Internet. Orlando, 2019: 62-65.

[20] Qiu J H, Sun J, Zhong Z M. A multi-objective green vehicle routing optimization algorithm based on delivery benefit balance[J]. Control and Decision, 2023, 38(2): 365-371.

[21] Zhu M P, Yang J H, Li X G, et al. A security decision-making approach for field layer of cloud-integrated industrial cyber-physical systems[J]. Control and Decision, 2024, 39(1): 281-290.

[22] Huang K X, Zhou C J, Qin Y Q, et al. A game-theoretic approach to cross-layer security decision-making in industrial cyber-physical systems[J]. IEEE Transactions on Industrial Electronics, 2020, 67(3): 2371-2379.

[23] Ganjkhani M, Hosseini M M, Parvania M. Optimal defensive strategy for power distribution systems against relay setting attacks[J]. IEEE Transactions on Power Delivery, 2023, 38(3): 1499-1509.

[24] Hu H, Liu Y L, Chen C, et al. Optimal decision making approach for cyber security defense using evolutionary game[J]. IEEE Transactions on Network and Service Management, 2020, 17(3): 1683-1700.

[25] Zhang H F, Yue D, Dou C X, et al. Two-stage optimal operation strategy of isolated microgrid with TSK fuzzy identification of supply security[J]. IEEE Transactions on Industrial Informatics, 2020, 16(6): 3731-3743.

作者简介

郭伟杰(1995−), 男, 博士生, 从事工业控制系统安全防护技术的研究, E-mail: 13775135919@163.com;

刘璐(1997−), 女, 博士生, 从事无人驾驶安全技术的研究, E-mail: liuluddex@hust.edu.cn;

杜鑫(1996−), 男, 博士生, 从事过程控制系统信息安全技术的研究, E-mail: xdhust@hust.edu.cn;

周纯杰(1965−), 男, 教授, 博士, 博士生导师, 从事工业互联网安全的研究, E-mail: cjiezhou@hust.edu.cn.