DOI: 10.19650/j.cnki.cjsi.J2209592

基于动态因果图的智能仪表一体化失效分析*

刘 璐,杜 鑫,周纯杰
(华中科技大学人工智能与自动化学院 武汉 430074)

摘 要:工业互联网在推动制造业升级换代的同时,也引入了信息安全问题,智能仪表等现场设备面临信息安全风险。为明确和分析在功能安全危险和信息安全威胁下智能仪表的失效原因和危害,本文提出了一体化因果失效分析方法框架,通过对功能安全和信息安全的融合失效分析,实现一体化因果失效路径推理。此外,对失效路径重要度通过结构、概率以及关键程度等属性量化评估,重要度表征失效路径发生的可能性大小,由此实现仪表安全失效场景精确分析。最后,通过智能变送器实践验证所提方法的有效性和可行性。本文通过动态因果图失效路径推理方法,首次揭示了智能仪表内部功能模块间安全失效渗透影响机理,实现仪表功能安全与信息安全一体化失效分析。

关键词: 智能仪表;功能安全;信息安全;动态因果图;失效分析
中图分类号: TH86 **文献标识码**: A **国家标准学科分类代码**: 460.40

Integrated failure analysis for intelligent instruments with dynamic causal diagrams

Liu Lu, Du Xin, Zhou Chunjie
(*School of Artificial Intelligence and Automation*, *Huazhong University of Science and Technology*, *Wuhan 430074*, *China*)

Abstract: While promoting the upgrading of traditional manufacturing, the industrial internet has introduced cyber security issues which makes industrial devices such as intelligent instruments face more severe cyber security risks. To effectively clarify and analyze the failure causes and hazards of intelligent instruments under functional safety and cyber security threats, this article proposes a method framework that enables reasoning and evaluation of integrated casual failure paths. Based on the framework, this article realizes the integrated failure analysis of functional safety and cyber security, and realizes the integrated causal failure path reasoning. Meanwhile, the importance of the failure path which represents the possibility of the path is quantitatively evaluated by attributes such as structure, probability and essence. Therefore, it realizes accurate analysis of instruments failure scenarios. Finally, the effectiveness and feasibility of the proposed method are evaluated by the intelligent transmitter. Through the failure path reasoning method based on dynamic causal diagram, it is the first time to reveal the influence principle of cyber security failure penetration between the internal functional modules of intelligent instruments, and realize the integrated failure analysis process of functional safety and cyber security.

Keywords: intelligent instrument; functional safety; cyber security; dynamic causal diagrams; failure analysis

0 引 言

随着工业互联网的快速推进,工业仪表进入智能化发展阶段[1]。智能仪表作为工业控制现场关键设备,具备精准测量、自诊断与运算、通信功能等特点[2],具体包括收集并处理多类物理设备数据以及同远程控制中心信息交互。为了保障仪表的安全稳定运行,传统工业仪表主要考虑功能性故障引起的不安全行为。针对此类功能安全问题,现有安全防护措施能够有效抵御此类安全风险[3]。然而,随着仪表的信息化与智能化升级,多样的网络攻击渗透影响使得仪表面临更复杂的失效形势[4]。考虑传统安全防护措施往往致力于功能安全保护,难以保障信息安全威胁下仪表正常运行的难题,因此,信息安全

收稿日期:2022-04-11 Received Date: 2022-04-11
*基金项目:国家重点研发计划(2019YFB2006301)、国家自然科学基金项目(62127808)项目资助

问题必须纳入考虑范围,以避免仪表硬件、软件和数据等遭到恶意破坏、更改和泄露[5]。与此同时,在智能仪表内部结构日益复杂且资源受限情况下,仪表面临功能安全危险和信息安全威胁共存情况,如何对其两类安全融合分析是目前研究重点[6]。功能安全与信息安全融合分析,能够明确安全失效过程,挖掘失效环节,对后续安全防护措施加固具有重要研究意义。

为了实现智能仪表功能安全与信息安全融合分析,需要通过失效一体化研究明确信息攻击对智能仪表功能安全的渗透影响[7]。目前,面向智能仪表的功能安全与信息安全一体化失效分析研究较少,主要聚焦于工业控制系统。Piètre 等[8]从理论上分析了功能安全与信息安全融合的可行方案,然而并未对具体实现方案详细说明。类似地,针对典型工业控制系统结构的失效模式和防护措施,靳江红等[9]以工业控制系统为目标,提出了一种基于事件树和风险的两安协同解决方案,但是缺乏对仪表内在两安失效演化过程的分析。与此同时,Nagaraju 等[10]针对信息物理系统中由网络攻击导致的物理设备安全失效问题,提出基于故障攻击树建模理论的物理系统潜在信息安全风险描述方法,直观描述攻击事件对物理设备功能安全的影响。然而,随着智能仪表安全状态演变复杂化,该方法可能面临复杂状态转换的难题。上述工作均通过定性分析对两安一体化失效分析提供可参考方案,可是缺乏对其内在耦合情况展开精准描述。因此,为了更精确分析两类安全交互关系,有学者展开了定量评估相关研究工作。Khan 等[11]针对动态可修复物理系统失效分析需求,提出了基于布尔逻辑驱动的马尔可夫过程分析(boolen logic driven Markov process, BDMP)方法。该方法通过动态定量构建两类安全一体化安全失效模型,为二者融合分析提供了有效方案。然而,此方法不可预测未知威胁及潜在状态空间爆炸问题,极有可能阻碍对资源受限的嵌入式仪表设备的实时分析。Wang 等[12]结合专家经验知识,提出基于贝叶斯网络的系统可靠性失效分析方法。该方法将故障树转为贝叶斯网络,并通过统计数据生成的失效概率来分析系统的安全问题。虽然贝叶斯网络的自顶向下建模路线有效表达了工业控制系统失效路径,但面向内部双向联通的智能仪表,该方法可能无法实现仪表内部的因果失效回路识别。综合以上分析可知,针对内部结构复杂且资源受限的智能仪表,如何开展仪表功能安全和信息安全一体化失效分析是目前亟待解决的难题。

为克服智能仪表面临的一体化安全失效分析难题,针对智能仪表内部复杂结构及其特性,本文提出一种基于动态因果图(dynamic causality diagrams, DCD)的安全一体化失效分析方法,包括一体化失效路径推理和路径评估两部分。首先针对智能面临的功能安全与信息安全双重失效因素,提出基于动态因果图的失效路径推理,得到一体化因果失效路径。接着,通过融合分析失效路径的多维安全属性,计算失效路径的重要度,评估信息攻击对智能仪表安全功能的影响。最后,以智能变送器为研究对象,验证本文所提方法的有效性。本方法对智能仪表功能安全与信息安全失效进行融合分析,有助于提高智能仪表自诊断效率,保证智能仪表安全稳定运行,对后续安全一体化智能仪表研制具有重要研究意义。

1 智能仪表功能安全与信息安全一体化分析框架

1.1 智能仪表典型架构及其工业应用场景

智能仪表是适用于工业过程测量和控制的新型嵌入式设备[13],具有多种智能功能,其典型架构及其工业应用场景如图 1 所示,所处工业控制现场层级结构主要包括企业层、监控层、控制层以及物理层[14]。物理层描述与工业过程相关的智能仪器或过程。控制层包括边缘管理器和智能仪表设备。监控层主要提供监控服务,确保边缘管理器以及各个仪表设备的实时运行状态;同时,将获取的实时信息上传至企业层。企业层负责控制和管理整个工业控制运行过程。与此同时,智能仪表工业应用场景具有较高的实时性和可用性需求[15],传统计算机领域中的信息安全防护无法满足其安全需求,并且各层不同安全风险内容对应的安全防护需求存在差异。

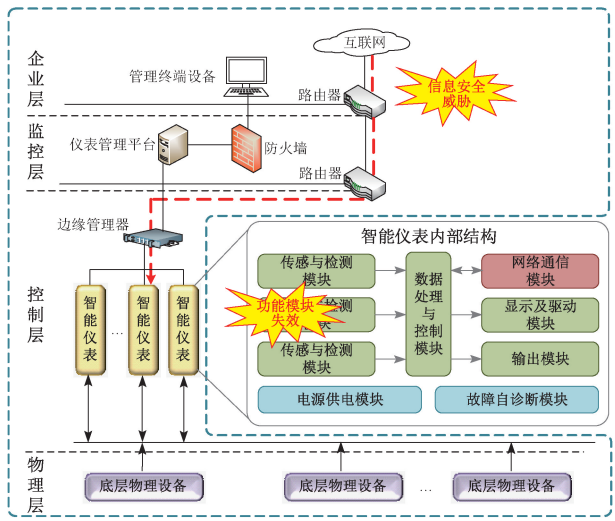

图 1 智能仪表典型架构及应用场景

Fig. 1 Typical architecture and application scenarios of intelligent instruments

由图 1 可知,智能仪表是连接底层物理设备与上层管理设备的关键设施,其具体内部结构主要包括:传感与检测模块、数据处理与控制模块、网络通信模块、显示及

驱动模块、输出模块、电源供电模块以及故障自诊断模块等模块。一方面,各功能模块均存在功能失效风险,任意模块的功能故障都极易引发智能仪表运行异常。另一方面,工业控制系统信息安全威胁一旦破坏监控层的防火墙,将逐层渗透至仪表内部功能模块导致其功能失效。由此可见,仪表内部功能安全保护及外来风险抵御对于其安全防护不可或缺。因此,充分考虑到智能仪表应用场景、内部结构以及运行特点,面向智能仪表的一体化安全防护,首先是利用防火墙过滤外部信息攻击,然后在仪表内部部署安全防护手段,确保渗透信息攻击和内部功能故障的有效防护。在安全防护手段实施之前,一体化安全失效分析是必经之路。仪表失效过程作为潜在安全风险发生的可能性表征,有利于后续安全防护手段实施,实现仪表安全可靠运行。

1.2　一体化失效分析方法框架

智能仪表功能安全与信息安全一体化失效分析主要包括对失效路径的推理和评估,方法框架如图 2 所示。一体化失效路径推理部分首先明确智能仪表常见失效原因和失效结果,然后对二者进行融合分析,接着,利用因果失效模型对仪表失效关系进行路径推理,得到失效路径集合。评估部分则综合考虑失效路径的结构重要度、概率重要度以及关键程度等重要度属性,通过对属性权重求解得到失效路径重要度结果并对其排序,以此揭示不同失效路径对仪表安全失效的影响程度。

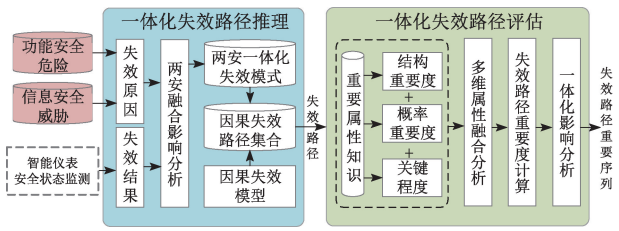

图 2　一体化失效分析方法框架

Fig. 2　Architecture of the integrated failure analysis method

目前智能仪表面临的失效情况主要分为以下两类:1)由硬件故障、环境扰动以及人为误操作等功能安全问题导致的仪表安全失效;2)信息攻击引起仪表异常行为,从而导致仪表安全失效。传统功能安全失效分析研究已经较为成熟,但是信息安全对仪表安全影响机理研究尚处于起步阶段。图 3 展示了信息攻击对智能仪表渗透影响过程。具体来说,信息安全威胁通过采取不同的攻击方式渗透作用到智能仪表各个功能模块,最终导致智能仪表失效。与此同时,信息安全问题的引入也使得原有安全防护措施部分失效,仪表本身不能够及时对信息安全风险进行管控,因此导致仪表在内的工业现场遭受严重损失。综合上述分析,本文对由功能安全引起的失效行为和由信息安全引起的异常行为进行融合分析,推理智能仪表因果失效路径并对其评估,最终实现功能安全与信息安全一体化分析过程,为后续安全防护加固提供理论支撑。

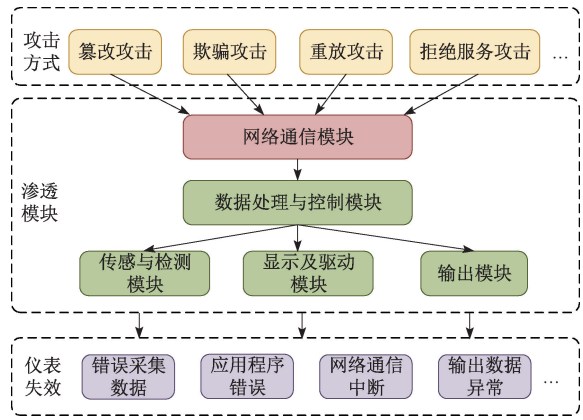

图 3　信息攻击渗透影响过程

Fig. 3　Cyber attack penetration process

2　基于动态因果图的安全失效路径推理及评估方法

2.1　动态因果图失效路径推理

智能仪表的因果失效路径推理,是将智能仪表存在的多种失效模式利用动态因果图模型表达,然后通过因果图拓扑关系推理因果失效路径。

1)基于动态因果图的失效模型

动态因果图作为图形化概率推理模型,其中图形节点表达事件发生概率或相关变量参数,有向边表示各事件/变量的因果关系。该方法简洁的知识表达和合理有效的推理原则使其在失效分析领域应用广泛[16]。

动态因果图具备传统故障攻击树和贝叶斯网络分析特点,能够定性表达变量关系以及通过事件概率量化状态转移过程,同时该方法动态分析特性能根据信息变化实时调整图形结构,克服了故障攻击树静态分析问题的局限。另外,因果回路结构解决了贝叶斯网络无法处理回路信息难题。并且该方法的布尔逻辑运算增强了对未知威胁的预测能力。基于以上特征,动态因果图能够有效融合分析智能仪表功能故障和信息攻击等失效原因与仪表安全失效表征结果,通过事件逻辑定性表达失效原因和结果间的关联关系,并利用概率描述量化失效过程,最终完成智能仪表一体化失效分析。综合看来,本文选择动态因果图失效分析方法对智能仪表一体化安全失效进行分析。

动态因果图失效模型如图 4 所示,包括 3 个要素:

(1)事件:基本事件和中间事件。

基本事件 B_i 通常被当作失效原因,它不包含输入边但必须包含至少一条输出边。中间事件 X_i 通常被当作失效结果,它至少包含一条输入边,可以不包含输出边或者包含一条及多条输出边。

(2)逻辑门:与门、或门等。

与门要求输入边输入事件 $X_i(i=1,2,\cdots,n)$ 全部发生,输出事件 x 才发生,逻辑关系为:

$$x = B_1 \cap B_2 \cap \cdots \cap B_n \tag{1}$$

或门要求输入边事件 $X_i(i=1,2,\cdots,n)$ 中任意一个或几个发生,输出事件 x 发生,相应逻辑关系为:

$$x = B_1 \cup B_2 \cup \cdots \cup B_n \tag{2}$$

(3)因果关系。

主要指事件与事件之间的连接事件变量 P_{ij},表示事件 i 向事件 j 的转移概率,即 i 到 j 因果强度。

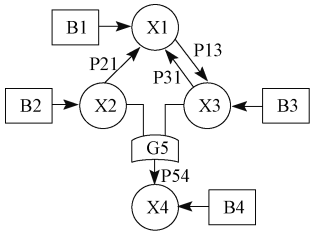

图 4 动态因果图失效模型结构

Fig. 4 Dynamic causal diagram failure model

2)失效路径推理

为了实现失效路径推理,首先需要对智能仪表存在的失效模式进行描述,本文通过三元组表示失效模式,即 $Mode = < L,P,D >$。

其中,L 表示智能仪表失效的功能模块,可分为图 1 所示 7 大功能模块;P 表示该具体功能模块失效的现象,即智能仪表具体异常行为,包括输入/输出数据格式错误,硬件故障导致功能无法正常实现等现象;D 表示对其异常行为的表述,即对该异常行为产生的潜在原因进行说明。

动态因果图失效模型里,任何一个中间事件 X_i 都能展开成以该事件为输出事件,多个输入事件共同组成的路径集合。基于动态因果图的失效路径推理主要分为以下 3 步:

(1)中间失效事件一阶割集表达式,将中间事件由相邻事件表达;

(2)中间失效事件的最终割集表达式,最终割集由基本事件和连接事件表达;

(3)中间失效事件的不交化割集表达式,若最终割集的表达式为:

$$X = \bigcup_{i=1}^{m} C_i, \text{其中 } C_i = \bigcap_{j=1}^{N} V_{ij} \tag{3}$$

则不交割集的表达式为:

$$X = C_1 + C_2\overline{C_1} + \cdots + C_m\overline{C_1C_2\cdots C_{m-1}} \tag{4}$$

动态因果图的不交割集仅包含基本事件和连接事件的最小割集表示。在智能仪表因果失效路径分析中,最小割集用于表征仪表最小失效模式,从而实现多样故障和攻击方式下仪表功能模块安全失效过程表达。因此,基于动态因果图的智能仪表失效路径推理,能有效结合功能安全威胁和信息安全危险,通过图形化方式揭示信息安全对功能安全的影响作用。

基于动态因果图失效模型,N 条一体化失效路径能够由集合 $PATH = \{Path_i, i = 1,\cdots,N\}$ 表示。对于任意一条路径,可采用三元组的形式表达为:$Path_i = < Effect_i, Cause_i, Connection_i >$。

其中,$Effect$ 表示失效结果 X,$Cause$ 表示失效原因 B,$Connection$ 表示失效原因和失效结果之间的连接关系。连接关系 $Connection$ 用 $\boldsymbol{I} \times \boldsymbol{J}$ 矩阵表示,矩阵元素 c_{ij} 定义如下:

$$c_{ij} = \begin{cases} 0, & P_{ij} \notin Path \\ 1, & P_{ij} \in Path \end{cases} \tag{5}$$

2.2 失效路径重要度评估

基于动态因果图推理智能仪表因果失效模型,将失效原因、结果及中间事件或变量的转移关系以图形拓扑结构生动的展示,能够清晰地定位导致仪表失效的功能模块以及模块间渗透作用,有利于后续防护措施的部署。然而,面对复杂多变的失效情况和多样的失效路径,针对性的安全防护控制必须明确失效影响程度。面向智能仪表对象的安全一体化失效分析,其失效路径重要度不仅反映了失效环节量化程度,更能作为风险分析环节的关键评估因素。一般来说,重要度、安全风险以及相应的安全防护需求呈正相关趋势,需要优先对重要度高的失效环节进行安全防护,从而保证智能仪表正常运行。因此本节基于重要度实现失效路径重要度的量化评估,主要包括重要属性融合分析和重要度计算两方面内容。

1)重要度属性融合分析

重要度是因果失效量化分析的关键指标[17],主要包括结构重要度,概率重要度和关键程度等 3 个重要属性,具体定义如表 1 所示。

表 1 重要度属性

Table 1 Importance attribute

属性名称	具体定义
结构重要度 *Str*	失效事件引起的局部失效以及全局失效的模块数量
概率重要度 *Pro*	基本失效事件本身发生的概率
关键程度 *Ess*	由因果图不交割集中基本事件对应的连接变量决定

一般来说,3 个重要属性足以揭示失效路径的重要性,结构重要度可以评估失效原因最终导致功能模块失效的范围;概率重要度有效揭示了失效原因本身存在的概率;关键程度揭示了因果失效路径中各个中间事件连接关系,其连接变量越多,说明失效路径渗透影响越严重。综合来讲,重要属性不仅考虑到失效路径自身造成的失效结果,而且能够结合仪表结构特征,明确不同失效路径间的关联失效影响。

2)失效路径重要度计算

由于重要度属性衡量标准不一致,在对失效路径重要度计算时,无法直接对其赋予权重进行融合计算。为避免由专家经验直接给出权重,以及灰色关联、层次分析法中的主观影响,本文采用熵权法[18]确定重要度属性权重。失效路径重要度求解具体步骤如下:

(1)确定基本失效事件 $B_i(i=1,2,\cdots,n)$ 的重要度属性;

(2)对重要度属性进行无量纲处理;设有 n 个基本事件,每个基本失效事件有 s 个重要度属性,通过步骤 1 对每个基本事件的重要度属性确定,第 i 个事件的第 j 个重要度属性值为 r_{ij}。由于 3 个基本属性于失效路径重要度呈正相关性,因此无量纲处理采用正指标公式:

$$\begin{cases} Y_{ij}=\dfrac{X_{ij}-X_{\min(j)}}{X_{\max(j)}-X_{\min(j)}}\times\alpha+(1-\alpha) \\ X_{\max(j)}=\min\limits_{i}\{X_{ij}\},X_{\min(j)}=\min\limits_{i}\{X_{ij}\} \end{cases} \tag{6}$$

其中,X_{ij} 为处理前重要度属性值,Y_{ij} 为处理后重要度属性值,且 $0<\alpha<1$,一般取 $\alpha=0.9$。

(3)计算第 j 个重要度属性下第 i 个基本事件的属性值的比重;

$$q_{ij}=Y_{ij}\Big/\sum_{i=1}^{n}Y_{ij} \tag{7}$$

(4)计算第 j 个重要度属性的熵值 e_j;

$$e_{ij}=-k\sum_{i=1}^{n}q_{ij}.\ln q_{ij},k=1/\ln n \tag{8}$$

(5)计算第 j 个重要度属性的权值 w_j;

$$w_j=\frac{1-e_j}{n-\sum\limits_{j=1}^{s}e_j},j=1,2,\cdots,s,\text{且}\sum_{j=1}^{s}w_j=1 \tag{9}$$

(6)计算第 j 个基本事件的重要度 IMP_i。

$$IMP_i=\sum_{j=1}^{s}w_{ij}\times r_{ij},i=1,2,\cdots,n,j=1,2,\cdots,s \tag{10}$$

通过以上步骤依次求解仪表所有失效路径的重要度,并基于基本失效事件进行路径重要度排序,明确具体失效原因对智能仪表安全失效结果的重要程度。失效路径的重要度值越大,则表明该失效路径及其失效原因对智能仪表正常运行情况的影响越严重。

3　智能变送器失效分析实践

3.1　智能变送器概述

智能变送器作为智能仪表常见类型,具有仪表典型结构,主要包括信号输入/输出模块,数据处理与控制模块和网络通信模块。因此,基于变送器的安全失效分析具有普适性,针对其他仪表类型均适用。本文以智能变送器为例展开面向智能仪表的一体化安全失效分析。智能变送器失效模式总结如表 2 所示。

表 2　智能变送器常见失效模式

Table 2　Common failure modes of intelligent transmitters

失效模块 L	失效现象 P	失效模式描述 D
输入/输出模块	错误采集数据	器件性能的偏移和损坏
	无法正常输出数据	器件性能的偏移和损坏
	硬件故障	电磁干扰或环境影响
数据处理模块	数据存储异常	数据丢失
	数据处理单元异常	数据运算结果错误
	数据应用程序错误	程序流错误或缓冲区溢出
	操作系统异常	系统故障或环境导致程序错误
网络通信模块	数据欺骗	恶意攻击通过数据欺骗入侵网络从而操控设备
	数据篡改	攻击者修改传输报文
	数据监听	攻击者监听并窃取工业数据
	数据破坏	总线共享、传输介质错误,或报文被干扰
	数据伪装	攻击者插入有效报文
	数据延时	攻击者攻击设备导致服务被延迟或拒绝

3.2　智能变送器一体化失效分析

1)失效路径推理分析

结合智能变送器常见失效模式,利用动态因果图对其进行失效路径推理,其一体化因果失效模型如图 5 所示。具体来说,面向智能仪表的因果失效模型基本失效事件由 B_{1-21} 表示,具体如表 3 所示。进一步地,X_{0-30} 表示仪表安全失效事件,其中 X_0 表示变送器工作异常,X_{1-4} 表示功能模块安全失效,X_{5-7} 表示维持变送器正常运行基本模块故障,而 X_{8-30} 表示各模块具体失效情况,具体描述如表 4 所示。同时,连接变量 $P_{i,j}$ 表示事件 X_i 到事件 X_j 转移概率,用于实现仪表因果失效路径中的基本失效事件和安全失效事件的关联。本文以智能变送器安全失效为最终失效结果进行分析,对基本失效事件经过多个中间状态转移最终导致变送器失效的过程展开路径推理。

失效原因 B_{12} 对失效路径 $Path_{12}$ 形式化表达结果如下所示：

失效路径 $Path_{12}=<X_0, B_{12}, Connection_{12}>$，其中 $c_{1,0}=c_{2,0}=c_{2,1}=c_{3,0}=c_{3,2}=c_{11,3}=c_{24,11}=1$，其余元素均为 0。$Path_{12}$ 在图 5 中的路径为 $B_{12}\rightarrow X_{24}\rightarrow X_{11}\rightarrow X_3\rightarrow X_2\rightarrow X_1\rightarrow X_0$。其物理意义为攻击者发起篡改攻击并渗透至变送器内部网络通信模块，使得该模块受到信息安全威胁，并且在一定概率下，会导致网络通信模块安全失效。更严重的是，由于网络通信模块与数据处理模块间双向连通，该模块安全失效可能将进一步诱发数据处理模块产生不安全行为。与此同时，该模块极易通过信号输入模块发出错误逻辑运行指令，进而导致信号输入模块功能异常。综合以上对变送器内部各模块行为分析，外部信息安全威胁可能会对变送器内部多个功能模块均造成影响，最终导致变送器安全失效。因此，对智能变送器信息安全与功能安全一体化失效路径推理对精准定位失效环节具有重要意义。

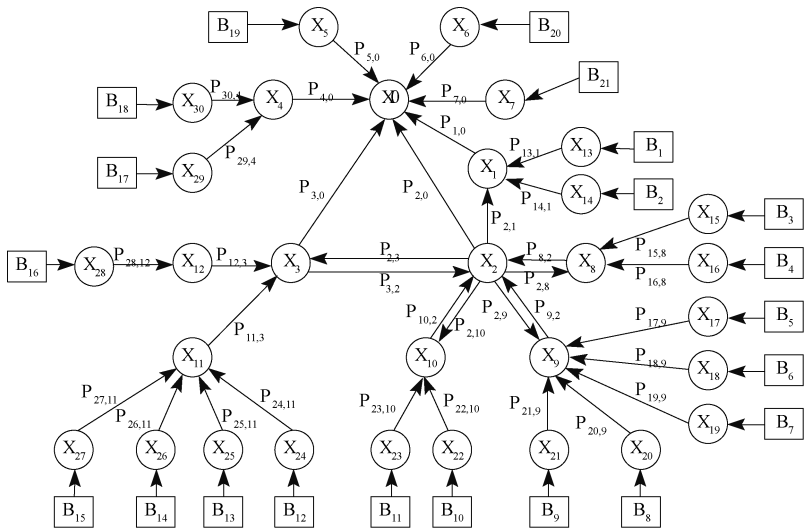

图 5 智能变送器一体化因果失效模型

Fig. 5 Integrated causal failure model of intelligent transmitter

表 3 基本失效事件描述

Table 3 Description of basic failure events

序号	描述	序号	描述
B_1	采集通道硬件损坏	B_{12}	外部发起篡改攻击
B_2	传感器性能降低	B_{13}	外部发起欺骗攻击
B_3	A/D 转换器硬件故障	B_{14}	外部发起重放攻击
B_4	A/D 转换器受到干扰	B_{15}	外部发起拒绝服务攻击
B_5	微处理器工作逻辑错误	B_{16}	网络通信模块硬件故障
B_6	微处理器计算资源占用	B_{17}	输出通道硬件损坏
B_7	微处理器内存资源占用	B_{18}	输出通道受到环境干扰
B_8	微处理器运算逻辑错误	B_{19}	硬件故障自诊断电路损坏
B_9	微处理器硬件故障	B_{20}	电源、显示及驱动等基本模块组件损坏
B_{10}	D/A 转换器硬件故障	B_{21}	冗余电路组件损坏
B_{11}	D/A 转换器受电磁干扰	–	–

表 4 安全失效事件及中间事件描述

Table 4 Description of safety failure events

序号	描述	序号	描述
X_0	智能变送器工作异常	X_{16}	A/D 转换器逻辑错误
X_1	信号输入模块安全失效	X_{17}	微处理器程序错误
X_2	数据处理模块安全失效	X_{18}	计算资源过度消耗
X_3	网络通信模块安全失效	X_{19}	存储资源过度消耗
X_4	信号输出模块安全失效	X_{20}	运算结果被篡改
X_5	故障自诊断电路工作	X_{21}	微处理器硬件损坏
X_6	电源、显示及驱动等基本模块工作异常	X_{22}	D/A 转换器不工作
X_7	冗余电路备份失败	X_{23}	D/A 转换器逻辑错误
X_8	A/D 转换器工作异常	X_{24}	网络通信模块受到篡改攻击
X_9	微处理器工作异常	X_{25}	网络通信模块受到欺骗攻击
X_{10}	D/A 转换器工作异常	X_{26}	网络通信模块受到重放攻击
X_{11}	网络通信模块遭受攻击	X_{27}	网络通信模块受到拒绝服务攻击
X_{12}	网络通信模块功能异常	X_{28}	网络通信模块通道故障
X_{13}	采集通道故障	X_{29}	输出通道故障
X_{14}	传感器工作异常	X_{30}	输出数据错误
X_{15}	A/D 转换器不工作	–	–

2）失效路径评估与分析

构建一体化因果失效模型，推理失效路径，以基本失效事件为路径起始，变送器安全失效为最终结果，对失效

路径基于基本事件重要度进行评估。首先,选取重要属性结构重要度 *Str*、概率重要度 *Pro* 和关键程度 *Ess* 信息如表 5 所示。

表 5　基本失效事件重要度属性

Table 5　Importance attributes of basic failure events

事件	*Str*	*Pro*	*Ess*	事件	*Str*	*Pro*	*Ess*
B_1	2	0.003 6	0.040 0	B_{12}	8	0.003 5	0.158 5
B_2	2	0.002 3	0.040 0	B_{13}	8	0.002 7	0.158 5
B_3	5	0.000 5	0.037 2	B_{14}	8	0.002 9	0.158 5
B_4	5	0.000 7	0.055 9	B_{15}	8	0.004 7	0.158 5
B_5	7	0.000 2	0.080 1	B_{16}	8	0.002 5	0.076 6
B_6	7	0.000 2	0.080 1	B_{17}	2	0.003 6	0.040 0
B_7	7	0.000 2	0.080 1	B_{18}	2	0.000 7	0.040 0
B_8	7	0.000 2	0.057 2	B_{19}	1	0.000 1	0.096 0
B_9	7	0.000 5	0.091 5	B_{20}	1	0.000 1	0.090 0
B_{10}	7	0.000 5	0.037 2	B_{21}	1	0.000 1	0.076 0
B_{11}	7	0.001 6	0.055 9	–	–	–	–

进一步地,利用式(6)~(9)求解重要度属性权重,结果如表 6 所示。

表 6　熵权法求解权重结果

Table 6　Results of the entropy weight method

重要度属性	信息熵值 e	权重 w
Str	0.904	0.233
Pro	0.838	0.394
Ess	0.846	0.373

最后,利用式(10)对各基本失效事件重要度 *IMP* 计算,结果如表 7 所示。

表 7　重要度计算结果

Table 7　Results of importance attributes

事件	IMP	事件	IMP	事件	IMP
B_1	0.482 4	B_8	1.652 5	B_{15}	1.925 1
B_2	0.481 9	B_9	1.665 4	B_{16}	1.893 6
B_3	1.179 1	B_{10}	1.645 1	B_{17}	0.482 4
B_4	1.186 2	B_{11}	1.652 5	B_{18}	0.481 2
B_5	1.661 0	B_{12}	1.924 6	B_{19}	0.268 9
B_6	1.661 0	B_{13}	1.924 3	B_{20}	0.266 7
B_7	1.661 0	B_{14}	1.924 4	B_{21}	0.261 5

重要度排序结果如下所示:

$<B_{15},B_{12},B_{14},B_{13},B_9,B_5,B_6,B_7,B_8,B_{11},B_{10},B_4,B_3,B_1,B_{17},B_2,B_{18},B_{19},B_{20},B_{21}>$

基于基本失效事件的失效路径重要度属性以及重要度对比如图 6~9 所示。

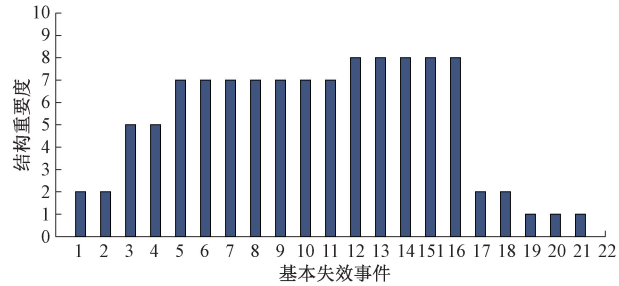

图 6　失效路径结构重要度属性 *Str*

Fig. 6　Importance attribute *Str* of failure paths

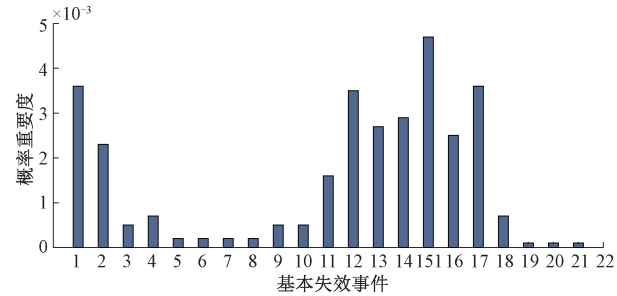

图 7　失效路径概率重要度属性 *Pro*

Fig. 7　Importance attribute *Pro* of failure paths

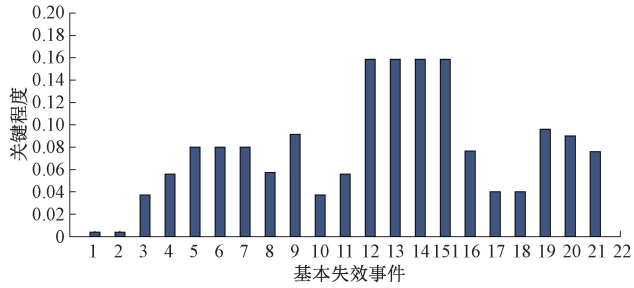

图 8　失效路径关键程度属性 *Ess*

Fig. 8　Importance attribute *Ess* of failure paths

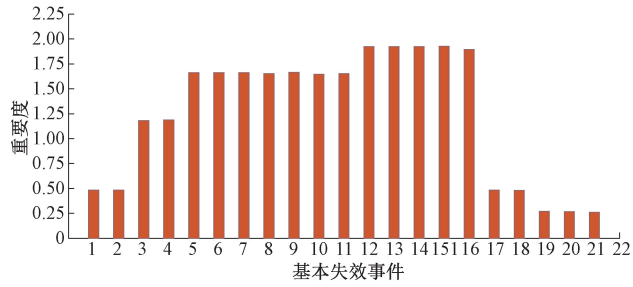

图 9　失效路径重要度结果

Fig. 9　Results of importance attributes for failure paths

对各个失效路径重要属性对比分析可以看出,基本失效事件 $B_{12\sim16}$ 的结构重要度属性 *Str* 数值最高,表明引起网络通信模块失效的信息攻击或硬件故障在变送器安全失效中,且对其他模块造成的影响最大。虽然 $B_{3\sim11}$ 的结构重要度次于 $B_{12\sim16}$ 反映了数据处理模块的失效对其他模块的渗透作用略低,但是依然存在较高风险。$B_{1\sim2,17\sim21}$ 在结构上对变送器失效影响较低。

与此同时,$B_{12\sim16}$ 概率重要度属性值 *Pro* 略高于其他基本失效事件,表明网络通信模块作为与外部信息交互的最重要模块,本身面临信息功能安全双重风险,故产生不安全行为的概率最高。此外,$B_{1,2}$ 主要通过引起信号输入模块故障来诱发变送器安全失效,其 *Pro* 偏高,表明智能变送器中输入模块与底层物理设备紧密相连,面临功能安全失效情况复杂,容易受物理环境干扰,其安全失效概率以及产生的后果都会对变送器后续行为有较大影响。类似地,B_{17} 代表输出通道硬件存在较高故障率,揭示了变送器对外输出功能具有不稳定性。因此,作为设备的薄弱环节,需要对其应该采取相应安全防护措施以保证变送器安全运行。失效事件 $B_{3\sim11,18\sim21}$ 较低的概率重要度属性值明确了这部分失效事件发生概率较低,且对整个工况影响相对较小,但是基于关键程度 *Ess* 可知,一旦 $B_{3\sim11}$ 失效,将影响其他失效路径。同理,$B_{18\sim21}$ 在 *Str* 和 *Pro* 属性值均较低的情况下,由于其 *Ess* 值较高,该部分失效路径对变送器安全失效作用也存在着不可忽视的影响。

综上所述,如果考虑单个重要属性,仅片面地得到该失效路径影响的评估结果,并不能全面揭示失效路径在变送器安全失效中的影响情况。因此,本文对多维属性进行融合分析,得到失效路径重要度评估结果如图 9 所示,说明智能变送器安全失效不仅与基本事件的失效概率有关,更与三种重要属性共同作用的结果密切相关。在变送器因果失效模型中,关键程度权重大于结构重要度,表明一体化失效路径的复杂交互关系比单个功能模块的结构位置对变送器的安全状态影响更大。最后,信息攻击由于其渗透影响范围广、失效概率较高,且作用模块结构重要,其安全失效对智能变送器安全运行状态存在严重影响。

4 结 论

本文提出了面向智能仪表的功能安全与信息安全一体化失效分析方法框架,利用动态因果图对一体化失效路径推理,并综合失效路径结构重要度、概率重要度以及关键程度等重要属性对失效路径进行评估,从而揭示了信息安全威胁对功能安全失效的影响。最后,以智能变送器为例,验证本文所提方法的有效性和可行性。本文所提的一体化失效分析方法,有助于明确智能仪表等现场设备面临的多类安全风险,以及为后续安全防护措施的部署提供理论支撑。该方法具有一定的理论研究意义和推广应用价值。

参考文献

[1] 赵剑明, 曾鹏, 刘贤达, 等. 第十讲:面向仪表两安融合的失效分析关键技术[J]. 仪器仪表标准化与计量, 2021(4): 9-12.
ZHAO J M, ZENG P, LIU X D, et al. Chapter 10: Key technology of failure analysis facing safety and security fusion of meter [J]. Instrument Standardization and Metrology, 2021(4): 9-12.

[2] 陈志瑞. 智能仪表在工业自动化控制中的应用[J]. 中国高新科技, 2021(24): 111-113.
CHEN ZH R. Application of intelligent instrument in industrial automation control[J]. China High and New Technology, 2021(24): 111-113.

[3] 赵林, 王雪, 刘佑达. 基于突变理论设冷水泵转轴功能安全完整性评估[J]. 仪器仪表学报, 2016, 37(12): 2728-2734.
ZHAO L, WANG X, LIU Y D. Functional safety integrity evaluation of the component cooling water pump shaft based on the catastrophe theory [J]. Chinese Journal of Scientific Instrument, 2016, 37(12): 2728-2734.

[4] SHU F, CHEN S T, ZHANG J Y, et al. Research on situation awareness technology in industrial control system[C]. 2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), IEEE, 2019: 1937-1940.

[5] 谷敏, 鲍宜帆. 关于物联网技术信息安全探讨[J]. 数字技术与应用, 2019, 37(2): 199,201.
GU M, BAO Y F. Discussion on information security of internet of things technology[J]. Digital Technology & Applications, 2019, 37(2): 199,201.

[6] 宋常亮, 孙博, 唐泽波, 等. 基于失效物理的多模式耦合可靠性建模方法[J]. 电子测量与仪器学报, 2021, 35(11): 124-131.
SONG CH L, SUN B, TANG Z B, et al. Multi-mode coupling reliability modeling method based on physics failure [J]. Journal of Electronic Measurement and Instrumentation, 2021, 35(11): 124-131.

[7] ASPLUND F, MCDERMID J, OATES R, et al. Rapid integration of CPS security and safety [J]. IEEE Embedded Systems Letters, 2018, 11(4): 111-114.

[8] PIETRE-CAMBACEDES L, BOUISSOU M. Cross-fertilization between safety and security engineering[J].

Reliability Engineering & System Safety, 2013, 110: 110-126.

[9] 靳江红, 莫昌瑜, 李刚, 等. 工业控制系统功能安全与信息安全一体化防护措施研究[J]. 工业安全与环保, 2020, 46(1): 53-60.
JIN J H, MO CH Y, LI G, et al. Integration technology of functional safety and cyber security for Industrial control system[J]. Industrial Safety and Environment Protection, 2020, 46(1): 53-60.

[10] NAGARAJU V, FIONDELLA L, WANDJI T. A survey of fault and attack tree modeling and analysis for cyber risk management [C]. 2017 IEEE International Symposium on Technologies for Homeland Security, IEEE, 2017: 1-6.

[11] KHAN S, KATOEN J P, BOUISSOU M. Explaining boolean-logic driven markov processes using GSPNs[C]. 2020 16th European Dependable Computing Conference (EDCC), IEEE, 2020: 119-126.

[12] WANG H, LIU L, PENG Z, et al. An overview of failure analysis expert system based on Bayesian networks[C]. 2019 IEEE 26th International Symposium on Physical and Failure Analysis of Integrated Circuits (IFPA), IEEE, 2019: 1-5.

[13] GROTTI G, CROTTI, DANIELE, et al. Industrial comparator for smart grid sensor calibration[J]. IEEE Sensor Journal, 2017, 17(23): 7784-7793.

[14] ZHOU C J, HU B W, SHI Y, et al. A unified architectural approach for cyberattack-resilient industrial control systems[J]. Proceeding of the IEEE, 2020, 109(4): 517-541.

[15] 李雪菁, 姚新红, 张进明. 高温液态金属流量在线测量方法与技术综述[J]. 仪器仪表学报, 2022, 43(1): 62-72.
LI X J, YAO X H, ZHANG J M. Review of on-line measurement methods and technologies for high temperature metal flow[J]. Chinese Journal of Scientific Instrument, 2022, 43(1): 62-72.

[16] SHI Q, LIANG X. Dynamic causality diagram in fault diagnosis[C]. 2009 International Joint Conference on Computational Science and Optimization, IEEE, 2009, 1: 225-227.

[17] POURALI M. Incorporating common cause failures in mission-critical facilities reliability analysis[J]. IEEE Transactions on Industry Applications, 2013, 50(4): 2883-2890.

[18] ZHU Y, TIAN D, YAN F. Effectiveness of entropy weight method in decision-making[J]. Mathematical Problems in Engineering, 2020.

作者简介

刘璐,2019 年于重庆大学获得学士学位,现为华中科技大学人工智能与自动化学院博士研究生,主要研究方向为工业互联网信息安全与功能安全影响分析。
E-mail: liuluddex@hust.edu.cn

Liu Lu received her B.Sc. degree from Chongqing University in 2019. She is currently pursuing her Ph.D. degree in the School of Artificial Intelligence and Automation at Huazhong University of Science and Technology. Her main research interests include security analysis and safety analysis of Industrial Internet.

杜鑫,2018 年于湘潭大学获得学士学位,现为华中科技大学人工智能与自动化学院博士研究生,主要研究方向为工控系统异常检测技术、安全控制技术、数字孪生技术。
E-mail: xdhust@hust.edu.cn

Du Xin received his B.Sc. degree from Xiangtan University in 2018. He is currently pursuing his Ph.D. degree in the School of Artificial Intelligence and Automation at Huazhong University of Science and Technology. His main research interests include the intrusion detection, control and digital twin of industrial control systems.

周纯杰(通信作者),2001 年于华中科技大学获得博士学位,现为华中科技大学人工智能与自动化学院教授,主要研究方向为工业控制系统安全控制、数字孪生技术、人工智能等。
E-mail: cjiezhou@hust.edu.cn

Zhou Chunjie (Corresponding author) received his Ph.D. degree from Huazhong University of Science and Technology in 2001. He is currently a professor in the School of Artificial Intelligence and Automation at Huazhong University of Science and Technology. His main research interests include safety and security control of industrial control systems, digital twin technology and artificial intelligence.