(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113434866 B
(45)授权公告日 2022.05.20

(21)申请号 202110737559.2

(22)申请日 2021.06.30

(65)同一申请的已公布的文献号
申请公布号 CN 113434866 A

(43)申请公布日 2021.09.24

(73)专利权人 华中科技大学
地址 430074 湖北省武汉市洪山区珞喻路1037号

(72)发明人 周纯杰 郭伟杰 刘璐 杜鑫 张岳 梁旭清 秦元庆

(74)专利代理机构 华中科技大学专利中心 42201
专利代理师 刘洋洋

(51)Int.Cl.
G06F 21/57(2013.01)
G06Q 10/06(2012.01)
G06F 30/20(2020.01)
G06F 17/18(2006.01)

(56)对比文件
CN 105631698 A,2016.06.01
CN 109117637 A,2019.01.01
CN 108183897 A,2018.06.19
CN 105045251 A,2015.11.11
EP 3282668 A1,2018.02.14
US 2007011113 A1,2007.01.11
US 10868825 B1,2020.12.15
US 2020244691 A1,2020.07.30
CN 108833416 A,2018.11.16
徐丙凤 等.基于状态时间的故障树的信息物理融合系统风险建模.《计算机科学》.2019,

审查员 彭玢

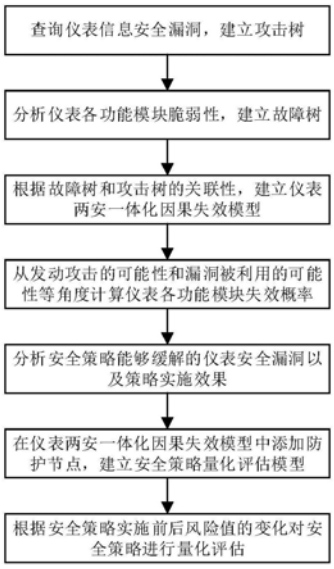
权利要求书4页 说明书11页 附图3页

(54)发明名称

仪表功能安全和信息安全策略的统一风险量化评估方法

(57)摘要

本发明公开了一种仪表功能安全和信息安全策略的统一风险量化评估方法，本发明方法具体包括结合攻击树和故障树建立仪表一体化因果失效模型；通过分析攻击发生的可能性、漏洞被利用的可能性等方式计算仪表各功能模块的失效概率；根据安全策略的属性，分析仪表功能安全和信息安全策略能够缓解的仪表安全漏洞以及对应的策略实施效果；在仪表一体化因果失效模型中添加防护节点，建立仪表安全策略评估模型；通过对仪表各功能模块进行专家打分，根据安全策略实施前后风险值的变化对仪表功能安全和信息安全策略进行量化评估。本发明能够对仪表设计过程中安全策略的部署提供一定的理论依据，相比于目前各安全标准中的定性评估，提高了准确性。



CN 113434866 B

1.一种仪表功能安全和信息安全策略的统一风险量化评估方法,其特征在于,所述方法包括以下步骤:

(1)查询仪表信息安全漏洞,分析攻击者会采取的攻击路径,建立攻击树;

(2)分析仪表功能模块脆弱性,推演功能失效过程,建立故障树;

(3)根据信息安全事件和功能失效事件之间的关联性,基于攻击树和故障树建立仪表一体化因果失效模型;基于攻击树和故障树建立仪表一体化因果失效模型包括:分析故障树的基本事件节点和攻击树的攻击目标节点之间是否存在相同节点,一旦存在相同节点,将相同的故障树基本节点作为攻击目标,添加攻击路径,得到仪表一体化因果失效模型;

(4)从实施攻击的概率和漏洞被利用的概率量化仪表功能模块的失效概率;

(5)从安全功能、策略关联、安全等级以及安全目标的角度对仪表功能安全和信息安全策略进行安全属性分析;

(6)在仪表一体化因果失效模型中添加安全属性关联的防护节点,建立安全策略的评价模型;

(7)结合仪表各功能模块资产,根据风险量化公式对仪表功能安全和信息安全策略进行量化评估;

所述步骤(4)具体包括:

(41)实施攻击的概率为:

$$P(A_i)=W_{cost}\times U(cost_{A_i})+W_{diff}\times U(diff_{A_i})+W_{det}\times U(det_{A_i})$$

其中,A_i表示任意一个攻击节点,即攻击者发起的攻击事件;P(Ai)表示攻击节点发生的概率;$cost_{Ai}$表示发起攻击事件所需的成本;$diff_{A_i}$表示发起攻击事件的难易程度;det_{Ai}表示攻击事件可能被发现的等级;W_{cost}表示攻击成本参数的权重;W_{diff}表示攻击难度参数的权重;W_{det}表示被发现的可能性参数的权重,且$W_{cost}+W_{diff}+W_{det}=1$;$U(cost_{A_i})$表示攻击成本参数的效用值;$U(diff_{A_i})$表示攻击难度参数的效用值;$U(det_{A_i})$表示攻击被发现可能性参数的效用值;

漏洞被利用的概率=攻击途径得分×攻击复杂度得分×认证得分×((机密性影响得分×机密性权重)+(完整性×完整性权重)+(可用性×可用性权重));

(42)将实施攻击的概率和漏洞被利用的概率结合仪表一体化因果失效模型,量化仪表各功能模块的失效概率:

$$P(F_i)=P(F_i|V_i=T,A_i=T)\times P(V_i=T)\times P(A_i=T)+P(F_i|V_i=T,A_i=F)\times P(V_i=T)\times P(A_i=F)+P(F_i|V_i=F,A_i=T)\times P(V_i=F)\times P(A_i=T)+P(F_i|V_i=F,A_i=F)\times P(V_i=F)\times P(A_i=F)$$

其中,$P(F_i)$为智能仪表功能模块F_i失效概率,$P(F_i|V_i,A_i)$表示智能仪表功能模块失效条件概率,$P(V_i=T)$表示漏洞节点被利用概率,$P(V_i=F)$表示漏洞节点未被利用概率,$P(A_i=T)$表示攻击节点发生概率,$P(A_i=F)$表示攻击节点未发生概率;

所述步骤(7)具体包括:

(71)对安全相关功能模块资产进行重要性交互打分,安全相关功能模块资产包括仪表传感与检测、数据处理与控制、电输出与驱动、网络通信;

(72)结合安全策略实施后通过仪表安全策略评价模型得到的仪表各安全相关功能模

块失效概率，运用量化公式对仪表的功能安全策略和信息安全策略进行量化评估；

量化公式为：

$$\Delta R=\sum_{i=1}^{n}\left(\mathrm{P}(\mathrm{F}_i)-\tilde{\mathrm{P}}(\mathrm{F}_i)\right)\mathrm{W}_i$$

其中，ΔR为安全策略实施前后仪表风险变化值，W_i为基于交互打分的仪表各功能模块的价值分数；n为仪表安全相关功能模块数量；

实施功能安全策略后的功能模块失效概率$\tilde{\mathrm{P}}(\mathrm{F}_i)$计算公式为：

$$\tilde{\mathrm{P}}(\mathrm{F}_i)=\mathrm{d}_j\times\mathrm{P}(\mathrm{F}_i)$$

实施信息安全策略后的功能模块失效概率$\tilde{\mathrm{P}}(\mathrm{F}_i)$计算公式为：

$$\begin{aligned}\tilde{\mathrm{P}}(\mathrm{F}_i)=&\mathrm{P}(\mathrm{F}_i\mid\mathrm{V}_i=\mathrm{T},\ \mathrm{A}_i=\mathrm{T})\times d_j\times\mathrm{P}(\mathrm{V}_i=\mathrm{T})\times d_j\times\mathrm{P}(\mathrm{A}_i=\mathrm{T})\\&+\mathrm{P}(\mathrm{F}_i\mid\mathrm{V}_i=\mathrm{T},\ \mathrm{A}_i=\mathrm{F})\times d_j\times\mathrm{P}(\mathrm{V}_i=\mathrm{T})\times\mathrm{P}(\mathrm{A}_i=\mathrm{F})\\&+\mathrm{P}(\mathrm{F}_i\mid\mathrm{V}_i=\mathrm{F},\ \mathrm{A}_i=\mathrm{T})\times\mathrm{P}(\mathrm{V}_i=\mathrm{F})\times d_j\times\mathrm{P}(\mathrm{A}_i=\mathrm{T})\\&+\mathrm{P}(\mathrm{F}_i\mid\mathrm{V}_i=\mathrm{F},\ \mathrm{A}_i=\mathrm{F})\times\mathrm{P}(\mathrm{V}_i=\mathrm{F})\times\mathrm{P}(\mathrm{A}_i=\mathrm{F})\end{aligned}$$

其中，d_j为能够缓解仪表安全漏洞对应安全策略的关联防护节点的防护系数。

2.根据权利要求1所述的一种仪表功能安全和信息安全策略的统一风险量化评估方法，其特征在于，所述步骤(5)具体包括：

(51)基于步骤(1)和步骤(2)中仪表信息安全漏洞和仪表功能模块脆弱性，查询安全标准，选择适用于仪表的功能安全策略和信息安全策略；

(52)根据安全标准中对仪表的功能安全策略和信息安全策略的定性描述，结合安全策略的安全功能、策略关联和安全目标属性，分析安全策略能够缓解的信息安全漏洞和功能模块脆弱性；

根据安全策略的安全等级属性，对安全策略进行分级，确定策略实施效果。

3.根据权利要求1所述的一种仪表功能安全和信息安全策略的统一风险量化评估方法，其特征在于，所述步骤(6)具体包括：

(61)根据仪表安全策略实施能够缓解的仪表功能模块安全漏洞，在仪表一体化因果失效模型中连接攻击节点和漏洞节点的逻辑门后，以及功能失效节点后添加防护节点；

(62)根据仪表安全策略的等级，对关联防护节点设置不同的防护系数，建立仪表安全策略评价模型。

4.一种仪表功能安全和信息安全策略的统一风险量化评估系统，其特征在于，所述系统包括以下部分：

第一模块，用于查询仪表信息安全漏洞，分析攻击者会采取的攻击路径，建立攻击树；

第二模块，用于分析仪表功能模块脆弱性，推演功能失效过程，建立故障树；

第三模块，用于根据信息安全事件和功能失效事件之间的关联性，基于攻击树和故障树建立仪表一体化因果失效模型；基于攻击树和故障树建立仪表一体化因果失效模型包括：分析故障树的基本事件节点和攻击树的攻击目标节点之间是否存在相同节点，一旦存在相同节点，将相同的故障树基本节点作为攻击目标，添加攻击路径，得到仪表一体化因果失效模型；

第四模块，用于从实施攻击的概率和漏洞被利用的概率量化仪表功能模块的失效概率；

第五模块，用于从安全功能、策略关联、安全等级以及安全目标的角度对仪表功能安全和信息安全策略进行安全属性分析；

第六模块，用于在仪表一体化因果失效模型中添加安全属性关联的防护节点，建立安全策略的评价模型；

第七模块，用于结合仪表各功能模块资产，根据风险量化公式对仪表功能安全和信息安全策略进行量化评估；

所述第四模块具体包括：

第一单元，用于分析实施攻击的概率，具体为：

$$P(A_i)=W_{cost}\times U(cost_{A_i})+W_{diff}\times U(diff_{A_i})+W_{det}\times U(det_{A_i})$$

其中，A_i表示任意一个攻击节点，即攻击者发起的攻击事件；P(Ai)表示攻击节点发生的概率；$cost_{Ai}$表示发起攻击事件所需的成本；$diff_{A_i}$表示发起攻击事件的难易程度；det_{Ai}表示攻击事件可能被发现的等级；W_{cost}表示攻击成本参数的权重；W_{diff}表示攻击难度参数的权重；W_{det}表示被发现的可能性参数的权重，且$W_{cost}+W_{diff}+W_{det}=1$；$U(cost_{A_i})$表示攻击成本参数的效用值；$U(diff_{A_i})$表示攻击难度参数的效用值；$U(det_{A_i})$表示攻击被发现可能性参数的效用值；

漏洞被利用的概率＝攻击途径得分×攻击复杂度得分×认证得分×((机密性影响得分×机密性权重)+(完整性×完整性权重)+(可用性×可用性权重))；

第二单元，用于将实施攻击的概率和漏洞被利用的概率结合仪表一体化因果失效模型，量化仪表各功能模块的失效概率：

$$\begin{aligned}P(F_i)=&P(F_i\mid V_i=T,\ A_i=T)\times P(V_i=T)\times P(A_i=T)\\&+P(F_i\mid V_i=T,\ A_i=F)\times P(V_i=T)\times P(A_i=F)\\&+P(F_i\mid V_i=F,\ A_i=T)\times P(V_i=F)\times P(A_i=T)\\&+P(F_i\mid V_i=F,\ A_i=F)\times P(V_i=F)\times P(A_i=F)\end{aligned}$$

其中，$P(F_i)$为智能仪表功能模块F_i失效概率，$P(F_i\mid V_i,A_i)$表示智能仪表功能模块失效条件概率，$P(V_i=T)$表示漏洞节点被利用概率，$P(V_i=F)$表示漏洞节点未被利用概率，$P(A_i=T)$表示攻击节点发生概率，$P(A_i=F)$表示攻击节点未发生概率；

所述第七模块具体包括：

重要性打分单元，用于对安全相关功能模块资产进行重要性交互打分，安全相关功能模块资产包括仪表传感与检测、数据处理与控制、电输出与驱动、网络通信；

量化评估单元，用于结合安全策略实施后通过仪表安全策略评价模型得到的仪表各安全相关功能模块失效概率，运用量化公式对仪表的功能安全策略和信息安全策略进行量化评估；

量化公式为：

$$\Delta R=\sum_{i=1}^{n}\left(P(F_i)-\tilde{P}(F_i)\right)W_i$$

其中，ΔR为安全策略实施前后仪表风险变化值，W_i为基于交互打分的仪表各功能模块的价值分数；n为仪表安全相关功能模块数量；

实施功能安全策略后的功能模块失效概率$\tilde{P}(F_i)$计算公式为：

$$\tilde{P}(F_i)=d_j\times P(F_i)$$

实施信息安全策略后的功能模块失效概率$\tilde{P}(F_i)$计算公式为：

$$\begin{aligned}\tilde{P}(F_i)=&P(F_i\mid V_i=T,\ A_i=T)\times d_j\times P(V_i=T)\times d_j\times P(A_i=T)\\&+P(F_i\mid V_i=T,\ A_i=F)\times d_j\times P(V_i=T)\times P(A_i=F)\\&+P(F_i\mid V_i=F,\ A_i=T)\times P(V_i=F)\times d_j\times P(A_i=T)\\&+P(F_i\mid V_i=F,\ A_i=F)\times P(V_i=F)\times P(A_i=F)\end{aligned}$$

其中，d_j为能够缓解仪表安全漏洞对应安全策略的关联防护节点的防护系数。

5.根据权利要求4所述的一种仪表功能安全和信息安全策略的统一风险量化评估系统，其特征在于，所述第五模块具体包括：

查询模块，用于基于第一模块和第二模块中仪表信息安全漏洞和仪表功能模块脆弱性，查询安全标准，选择适用于仪表的功能安全策略和信息安全策略；

分析单元，用于根据安全标准中对仪表的功能安全策略和信息安全策略的定性描述，结合安全策略的安全功能、策略关联和安全目标属性，分析安全策略能够缓解的信息安全漏洞和功能模块脆弱性；

根据安全策略的安全等级属性，对安全策略进行分级，确定策略实施效果。

6.根据权利要求4所述的一种仪表功能安全和信息安全策略的统一风险量化评估系统，其特征在于，所述第六模块具体包括：

防护添加单元，用于根据仪表安全策略实施能够缓解的仪表功能模块安全漏洞，在仪表一体化因果失效模型中连接攻击节点和漏洞节点的逻辑门后，以及功能失效节点后添加防护节点；

评价模型建立单元，用于根据仪表安全策略的等级，对关联防护节点设置不同的防护系数，建立仪表安全策略评价模型。

仪表功能安全和信息安全策略的统一风险量化评估方法

技术领域

[0001] 本发明属于仪表安全防护领域，更具体地，涉及一种仪表功能安全和信息安全策略的统一风险量化评估方法。

背景技术

[0002] 随着微型计算机技术和网络通信技术的快速发展，具有测量、运算、控制、执行、通信、诊断等功能的智能仪表在工业控制系统现场设备中得到了广泛运用。然而，相比于传统仪表，智能仪表给生产运行带来极大便利的同时，也面临着功能失效因素不断增多和信息攻击加速渗透等威胁。因此，智能仪表存在功能安全和信息安全防护的迫切需求。如何在功能安全和信息安全防护需求下对仪表安全防护策略进行有效的统一量化评估，从而给后期部署仪表功能安全和信息安全防护策略提供理论指导是目前需要解决的一大难题。

[0003] 现阶段仪表功能安全和信息安全策略有独立的有效性评估方法，而不同的安全标准缺乏对安全策略的统一评估方法和指标。现有技术中有对功能安全策略的目标和功能进行了定性描述，还由对信息安全策略所缓解的漏洞以及目前存在的问题等方面进行定性评估。上述方法都是通过定性方法对安全防护策略进行评估描述，缺乏准确性，目前尚没有一种评估方法能定量评估仪表的安全风险。

发明内容

[0004] 针对现有技术的以上缺陷或改进需求，本发明提供了一种仪表功能安全和信息安全策略的统一风险量化评估方法，其目的在于基于风险的角度通过定量方法对仪表功能安全和信息安全策略进行统一评估，相比于目前的定性方法，提高了准确性。

[0005] 为实现上述目的，本发明提供了一种仪表功能安全和信息安全策略的统一风险量化评估方法，所述方法具体包括以下步骤：

[0006] (1)查询仪表信息安全漏洞，分析攻击者会采取的攻击路径，建立攻击树；

[0007] (2)分析仪表功能模块脆弱性，推演功能失效过程，建立故障树；

[0008] (3)根据信息安全事件和功能失效事件之间的关联性，基于攻击树和故障树建立仪表一体化因果失效模型；

[0009] (4)从实施攻击的概率和漏洞被利用的概率量化仪表功能模块的失效概率；

[0010] (5)从安全功能、策略关联、安全等级以及安全目标的角度对仪表功能安全和信息安全策略进行安全属性分析；

[0011] (6)在仪表一体化因果失效模型中添加安全属性关联的防护节点，建立安全策略的评价模型；

[0012] (7)结合仪表各功能模块资产，根据风险量化公式对仪表功能安全和信息安全策略进行量化评估。

[0013] 进一步地，所述步骤(4)具体包括：

[0014] (41)实施攻击的概率为：

[0015] $P(A_i)=W_{cost}\times U(cost_{A_i})+W_{diff}\times U(diff_{A_i})+W_{det}\times U(det_{A_i})$

[0016] 其中，A_i表示任意一个攻击节点，即攻击者发起的攻击事件；P(Ai)表示攻击节点发生的概率；$cost_{Ai}$表示发起攻击事件所需的成本；$diff_{A_i}$表示发起攻击事件的难易程度；det_{Ai}表示攻击事件可能被发现的等级；W_{cost}表示攻击成本参数的权重；W_{diff}表示攻击难度参数的权重；W_{det}表示被发现的可能性参数的权重，且$W_{cost}+W_{diff}+W_{det}=1$；$U(cost_{A_i})$表示攻击成本参数的效用值；$U(diff_{A_i})$表示攻击难度参数的效用值；$U(det_{A_i})$表示攻击被发现可能性参数的效用值；

[0017] 漏洞被利用的概率＝攻击途径得分×攻击复杂度得分×认证得分×((机密性影响得分×机密性权重)+(完整性×完整性权重)+(可用性×可用性权重))；

[0018] (42)将实施攻击的概率和漏洞被利用的概率结合仪表一体化因果失效模型，量化仪表各功能模块的失效概率：

[0019] $P(F_i)=P(F_i|V_i=T,A_i=T)\times P(V_i=T)\times P(A_i=T)+P(F_i|V_i=T,A_i=F)\times P(V_i=T)\times P(A_i=F)+P(F_i|V_i=F,A_i=T)\times P(V_i=F)\times P(A_i=T)+P(F_i|V_i=F,A_i=F)\times P(V_i=F)\times P(A_i=F)$

[0020] 其中，$P(F_i)$为智能仪表功能模块F_i失效概率，$P(F_i|V_i,A_i)$表示智能仪表功能模块失效条件概率，$P(V_i=T)$表示漏洞节点被利用概率，$P(V_i=F)$表示漏洞节点未被利用概率，$P(A_i=T)$表示攻击节点发生概率，$P(A_i=F)$表示攻击节点未发生概率。

[0021] 进一步地，所述步骤(5)具体包括：

[0022] (51)基于步骤(1)和步骤(2)中仪表信息安全漏洞和仪表功能模块脆弱性，查询安全标准，选择适用于仪表的功能安全策略和信息安全策略；

[0023] (52)根据安全标准中对仪表的功能安全策略和信息安全策略的定性描述，结合安全策略的安全功能、策略关联和安全目标属性，分析安全策略能够缓解的信息安全漏洞和功能模块脆弱性；

[0024] 根据安全策略的安全等级属性，对安全策略进行分级，确定策略实施效果。

[0025] 进一步地，所述步骤(6)具体包括：

[0026] (61)根据仪表安全策略实施够缓解的仪表功能模块安全漏洞，在仪表一体化因果失效模型中连接攻击节点和漏洞节点的逻辑门后，以及功能失效节点后添加防护节点；

[0027] (62)根据仪表安全策略的等级，对关联防护节点设置不同的防护系数，建立仪表安全策略评价模型。

[0028] 进一步地，所述步骤(7)具体包括：

[0029] (71)对安全相关功能模块资产进行重要性交互打分，安全相关功能模块资产包括仪表传感与检测、数据处理与控制、电输出与驱动、网络通信；

[0030] (72)结合安全策略实施后通过仪表安全策略评价模型得到的仪表各安全相关功能模块失效概率，运用量化公式对仪表的功能安全策略和信息安全策略进行量化评估；

[0031] 量化公式为：

[0032] $$\Delta R=\sum_{i=1}^{n}\left(P(F_i)-\tilde{P}(F_i)\right)W_i$$

[0033] 其中，ΔR为安全策略实施前后仪表风险变化值，W_i为基于交互打分的仪表各功能

模块的价值分数；

[0034] 实施功能安全策略后的功能模块失效概率$\tilde{P}(F_i)$计算公式为：

[0035] $$\tilde{P}(F_i) = d_j \times P(F_i)$$

[0036] 实施信息安全策略后的功能模块失效概率$\tilde{P}(F_i)$计算公式为：

[0037] $$\begin{aligned}\tilde{P}(F_i) = {} & P(F_i \mid V_i = T,\ A_i = T) \times d_j \times P(V_i = T) \times d_j \times P(A_i = T) \\ & + P(F_i \mid V_i = T,\ A_i = F) \times d_j \times P(V_i = T) \times P(A_i = F) \\ & + P(F_i \mid V_i = F,\ A_i = T) \times P(V_i = F) \times d_j \times P(A_i = T) \\ & + P(F_i \mid V_i = F,\ A_i = F) \times P(V_i = F) \times P(A_i = F)\end{aligned}$$

[0038] 其中，d_j为能够缓解仪表安全漏洞对应安全策略的关联防护节点的防护系数。

[0039] 另一方面，本申请还实现了一种仪表功能安全和信息安全策略的统一风险量化评估系统，所述系统包括以下部分：

[0040] 第一模块，用于查询仪表信息安全漏洞，分析攻击者会采取的攻击路径，建立攻击树；

[0041] 第二模块，用于分析仪表功能模块脆弱性，推演功能失效过程，建立故障树；

[0042] 第三模块，用于根据信息安全事件和功能失效事件之间的关联性，基于攻击树和故障树建立仪表一体化因果失效模型；

[0043] 第四模块，用于从实施攻击的概率和漏洞被利用的概率量化仪表功能模块的失效概率；

[0044] 第五模块，用于从安全功能、策略关联、安全等级以及安全目标的角度对仪表功能安全和信息安全策略进行安全属性分析；

[0045] 第六模块，用于在仪表一体化因果失效模型中添加安全属性关联的防护节点，建立安全策略的评价模型；

[0046] 第七模块，用于结合仪表各功能模块资产，根据风险量化公式对仪表功能安全和信息安全策略进行量化评估。

[0047] 进一步地，所述第四模块具体包括：

[0048] 第一单元，用于分析实施攻击的概率，具体为：

[0049] $$P(A_i) = W_{cost} \times U(cost_{A_i}) + W_{diff} \times U(diff_{A_i}) + W_{det} \times U(det_{A_i})$$

[0050] 其中，A_i表示任意一个攻击节点，即攻击者发起的攻击事件；P(Ai)表示攻击节点发生的概率；$cost_{Ai}$表示发起攻击事件所需的成本；$diff_{A_i}$表示发起攻击事件的难易程度；det_{Ai}表示攻击事件可能被发现的等级；W_{cost}表示攻击成本参数的权重；W_{diff}表示攻击难度参数的权重；W_{det}表示被发现的可能性参数的权重，且$W_{cost}+W_{diff}+W_{det}=1$；$U(cost_{A_i})$表示攻击成本参数的效用值；$U(diff_{A_i})$表示攻击难度参数的效用值；$U(det_{A_i})$表示攻击被发现可能性参数的效用值；

[0051] 漏洞被利用的概率＝攻击途径得分×攻击复杂度得分×认证得分×((机密性影响得分×机密性权重)+(完整性×完整性权重)+(可用性×可用性权重))；

[0052] 第二单元，用于将实施攻击的概率和漏洞被利用的概率结合仪表一体化因果失效

模型，量化仪表各功能模块的失效概率：

[0053] $P(F_i)=P(F_i|V_i=T,A_i=T)\times P(V_i=T)\times P(A_i=T)+P(F_i|V_i=T,A_i=F)\times P(V_i=T)\times P(A_i=F)+P(F_i|V_i=F,A_i=T)\times P(V_i=F)\times P(A_i=T)+P(F_i|V_i=F,A_i=F)\times P(V_i=F)\times P(A_i=F)$

[0054] 其中，$P(F_i)$为智能仪表功能模块F_i失效概率，$P(F_i|V_i,A_i)$表示智能仪表功能模块失效条件概率，$P(V_i=T)$表示漏洞节点被利用概率，$P(V_i=F)$表示漏洞节点未被利用概率，$P(A_i=T)$表示攻击节点发生概率，$P(A_i=F)$表示攻击节点未发生概率。

[0055] 进一步地，所述第五模块具体包括：

[0056] 查询模块，用于基于第一模块和第二模块中仪表信息安全漏洞和仪表功能模块脆弱性，查询安全标准，选择适用于仪表的功能安全策略和信息安全策略；

[0057] 分析单元，用于根据安全标准中对仪表的功能安全策略和信息安全策略的定性描述，结合安全策略的安全功能、策略关联和安全目标属性，分析安全策略能够缓解的信息安全漏洞和功能模块脆弱性；

[0058] 根据安全策略的安全等级属性，对安全策略进行分级，确定策略实施效果。

[0059] 进一步地，所述第六模块具体包括：

[0060] 防护添加单元，用于根据仪表安全策略实施够缓解的仪表功能模块安全漏洞，在仪表一体化因果失效模型中连接攻击节点和漏洞节点的逻辑门后，以及功能失效节点后添加防护节点；

[0061] 评价模型建立单元，用于根据仪表安全策略的等级，对关联防护节点设置不同的防护系数，建立仪表安全策略评价模型。

[0062] 进一步地，所述第七模块具体包括：

[0063] 重要性打分单元，用于对安全相关功能模块资产进行重要性交互打分，安全相关功能模块资产包括仪表传感与检测、数据处理与控制、电输出与驱动、网络通信；

[0064] 量化评估单元，用于结合安全策略实施后通过仪表安全策略评价模型得到的仪表各安全相关功能模块失效概率，运用量化公式对仪表的功能安全策略和信息安全策略进行量化评估；

[0065] 量化公式为：

[0066] $$\Delta R=\sum_{i=1}^{n}\left(P(F_i)-\tilde{P}(F_i)\right)W_i$$

[0067] 其中，ΔR为安全策略实施前后仪表风险变化值，W_i为基于交互打分的仪表各功能模块的价值分数；

[0068] 实施功能安全策略后的功能模块失效概率$\tilde{P}(F_i)$计算公式为：

[0069] $$\tilde{P}(F_i)=d_j\times P(F_i)$$

[0070] 实施信息安全策略后的功能模块失效概率$\tilde{P}(F_i)$计算公式为：

[0071]
$$\begin{aligned}\tilde{P}(F_i) = {} & P(F_i \mid V_i = T,\ A_i = T) \times d_j \times P(V_i = T) \times d_j \times P(A_i = T) \\ & + P(F_i \mid V_i = T,\ A_i = F) \times d_j \times P(V_i = T) \times P(A_i = F) \\ & + P(F_i \mid V_i = F,\ A_i = T) \times P(V_i = F) \times d_j \times P(A_i = T) \\ & + P(F_i \mid V_i = F,\ A_i = F) \times P(V_i = F) \times P(A_i = F)\end{aligned}$$

[0072] 其中，d_j为能够缓解仪表安全漏洞对应安全策略的关联防护节点的防护系数。

[0073] 总体而言，通过本发明所构思的以上技术方案与现有技术相比，具有以下有益效果：

[0074] (1)本发明提出的上述仪表功能安全和信息安全策略统一风险量化评估方法，克服了传统安全标准中对功能安全和信息安全策略定性描述的局限性，能够有效分析仪表功能安全和信息安全策略的实施效果；

[0075] (2)本发明首先根据仪表功能安全和信息安全策略的安全目标、安全功能以及策略关联属性分析仪表安全策略能够缓解的仪表功能模块漏洞，然后根据仪表安全策略的安全等级属性分析安全策略实施效果，最后将安全属性关联到安全策略评价模型中的防护节点，为仪表功能安全策略和信息安全策略基于统一尺度分析提供了可能；

[0076] (3)本发明从风险的角度对仪表功能安全和信息安全策略进行统一量化评估，相比于定性方法，提高了准确性以及为安全策略的部署提供了一定的理论依据。

附图说明

[0077] 图1是本发明方法的流程示意图；

[0078] 图2是本发明实施例中仪表攻击树示意图；

[0079] 图3是本发明实施例中仪表故障树示意图；

[0080] 图4是本发明实施例中仪表一体化因果失效模型示意图；

[0081] 图5是本发明中仪表功能安全和信息安全策略属性提取分析流程示意图；

[0082] 图6是本发明中仪表功能安全和信息安全策略评价模型示意图。

具体实施方式

[0083] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。此外，下面所描述的本发明各个实施方式中所涉及到的技术特征只要彼此之间未构成冲突就可以相互组合。

[0084] 本发明提供了一种仪表功能安全和信息安全策略统一风险量化评估方法，其流程如图1所示，包括如下步骤：

[0085] 步骤1：查询仪表信息安全漏洞，分析攻击者可能采取的攻击路径，建立攻击树。

[0086] 步骤1.1：通过执行漏洞扫描或查询信息安全漏洞库，获得仪表安全漏洞列表，然后根据仪表安全漏洞列表，结合已知的攻击策略，分析所有可能的攻击场景。

[0087] 查询信息安全漏洞库，找到仪表常见信息安全漏洞CNVD-2021-07490，CNVD-2021-17406，CNVD-2020-10538，攻击者可利用这些漏洞发起拒绝服务攻击，导致网络通信接口功能模块失效；可以借助通用的便携式手操器或者仪表管理通信软件的组态、校验管理、调试

等功能，通过调试接口等，对智能仪表的固件或操作系统进行篡改，甚至注入恶意代码，导致智能仪表数据处理与控制模块功能失效；攻击者还可通过未授权的外部设备或者通信组态软件接入智能仪表时，可以实现对智能仪表量程的恶意篡改、零点漂移、停止工作等操作。

[0088] 步骤1.2：将攻击事件节点和漏洞节点作为叶子节点，分析通过利用漏洞发动信息攻击可能导致的功能失效事件，并将功能失效事件作为根节点，自底向上建立攻击树。攻击树如图2所示。

[0089] 步骤2：分析仪表功能模块脆弱性，推演功能失效过程，建立故障树。

[0090] 步骤2.1：结合过程潜在失效模式及后果分析表或咨询现场工程人员，分析仪表各安全相关功能模块的脆弱性，确定仪表常见失效的功能模块，过程潜在失效模式及后果分析表参见表1所示。

[0091] 表1

[0092]

失效类别	潜在的失效模式	潜在的失效后果	潜在的失效原因	防护措施
功能安全	传感与检测功能模块失效	输出驱动模块功能模块失效	零点漂移	故障自诊断
	输出驱动模块失效	二次仪表无法正常显示	检测模块或数据处理与控制模块失效	故障自诊断

[0093]

	数据处理与控制功能模块失效	仪表不正常工作	程序异常	时序与逻辑监视
	……	……	……	……
信息安全	仪表无法正常工作	工况异常	未授权设备接入	访问控制
	无法收发数据	工况异常	遭受 DOS 攻击	入侵检测
	数据被篡改	工况异常	遭受欺骗攻击	入侵检测
	……	……	……	……

[0094] 步骤2.2：将仪表某个功能模块失效事件作为顶层事件节点，结合仪表工作运行原理，将引起顶层事件发生的功能模块失效事件作为基本事件节点，通过逻辑门和有向边将顶层事件节点和基本事件节点连接起来，自顶向下建立故障树。

[0095] 智能仪表的输入信号要经过开关量输入通道电路或模拟量输入通道电路进行变换、放大、整形、补偿等处理。对于模拟量信号，需经A/D转换器转换成数字信号，再通过接口

送入微控制器。由微控制器对输入数据进行加工处理、计算分析等一系列工作，通过接口送至显示器或打印机，也可输出开关量信号或经模拟量通道的D/A转换器转换成模拟量信号，还可通过串行接口(例如RS-232等)实现数据通信，完成更复杂的测量、控制任务。因此一旦传感检测模块或者数据处理与控制模块功能失效，输出驱动模块以及网络通信模块也将失效。基于上述失效场景，自顶向下建立故障树，故障树如图3所示。

[0096] 步骤3：分析故障树的基本事件节点和攻击树的攻击目标节点之间是否存在相同节点，一旦存在相同节点，将相同的故障树基本节点作为攻击目标，添加攻击路径，得到仪表一体化因果失效模型。仪表一体化因果失效模型如图4所示。

[0097] 步骤4：从实施攻击的可能性和漏洞被利用可能性等角度分析仪表功能模块失效事件发生的可能性。

[0098] 步骤4.1：从攻击成本、攻击难度以及攻击被发现的可能性分析发起攻击的可能性，通过CVSS漏洞评分标准分析漏洞被利用的可能性。

[0099] 考虑攻击者发起攻击的可能性跟攻击成本、攻击难度以及攻击被发现的可能性有关，在计算攻击节点的可能性时，给每个攻击节点赋予这三个属性值。运用多属性效用理论，将以上属性转换成其实现目标的效用值。则计算攻击者发起攻击可能性的公式如下：

[0100] $$P(A_i)=W_{cost}\times U(cost_{A_i})+W_{diff}\times U(diff_{A_i})+W_{det}\times U(det_{A_i}) \quad (1)$$

[0101] 其中：A_i表示任意一个攻击节点，即攻击者发起的攻击事件；$P(A_i)$表示攻击节点发生的概率；$cost_{A_i}$表示发起攻击事件所需的成本；$diff_{A_i}$表示发起攻击事件的难易程度；det_{Ai}表示攻击事件可能被发现的等级。W_{cost}表示攻击成本参数的权重；W_{diff}表示攻击难度参数的权重；W_{det}表示估计被发现的可能性参数的权重，且这三个权重系数之和为1。$U(cost_{A_i})$表示攻击成本参数的效用值；$U(diff_{A_i})$表示攻击难度参数的效用值；$U(det_{A_i})$表示攻击被发现可能性参数的效用值。

[0102] 通过公式(1)求解攻击事件发生的概率$P(A_i)$涉及到三个属性，因此需要制定相应的评分标准对它们进行评价。本发明采用的等级评分标准参见表2所示。

[0103] 表2

[0104]

攻击成本		攻击难度		攻击被发现的可能性	
成本	等级	难度	等级	可能性	等级
很高	5	很难	5	很难	1
高	4	难	4	难	2
中等	3	中等	3	中等	3
低	2	容易	2	容易	4

[0105]

很低	1	很容易	1	很容易	5

[0106] 为了计算攻击者发起攻击事件的概率，需要计算效用值$U(cost_{A_i})$、$U(diff_{A_i})$、$U(det_{A_i})$。通过分析可知，$cost_{A_i}$、$diff_{Ai}$、det_{A_i}与$U(cost_{A_i})$、$U(diff_{A_i})$、$U(det_{A_i})$成反比例关系。为了计算，三组之间的对应关系均取为$U(x)=1/x$。运用式(1)即可求出攻击事件发生的概率$P(A_i)$。

[0107] Common Vulnerability Scoring System(CVSS),即“通用漏洞评分系统”,是一个“行业公开标准,其被设计用来评测漏洞的严重程度,主要目的是帮助人们建立衡量漏洞严重程度的标准,便于分析漏洞的严重程度。本发明通过CVSS计算仪表信息安全漏洞被利用的可能性。CVSS包括基本得分,临时得分和环境得分这三个要素,这里仅需考虑基本得分,基本得分评价指标参见表3。

[0108] 表3

[0109]

	要素	可选值	评分
1	Access Vector(攻击途径)	本地/远程	0.7/1
2	Access Complexity(攻击复杂度)	高/中/低	0.6/0.8/1
3	Authentication(认证)	需要/不需要	0.6/1
4	Confidentiality Impact(机密性影响)	不受影响/部分/完全	0/0.7/1
5	Integrity Impact(完整性影响)	不受影响/部分/完全	0/0.7/1
6	Availability Impact(可用性影响)	不受影响/部分/完全	0/0.7/1
	权值倾向	平均/机密性/完整性/可用性	各0.333/权值倾向要素0.5另外两个0.25

[0110] 基本得分＝攻击途径得分*攻击复杂度得分*认证得分*((机密性影响得分*机密性权重)+(完整性*完整性权重)+(可用性*可用性权重))

[0111] 步骤4.2:分析历史数据或咨询现场工程人员分析仪表各功能模块失效的条件概率,结合公式(1)中的攻击者发动攻击的概率和漏洞被利用的概率,得到仪表各功能模块的失效概率。

[0112] 步骤5:从安全功能、策略关联、安全等级、安全目标等角度对仪表功能安全和信息安全策略进行安全属性特征量化分析。安全策略的属性分析量化流程示意图参见图5所示。

[0113] 步骤5.1:根据步骤1和步骤2得到的仪表常见信息安全漏洞和功能模块失效机理,通过查询相关安全标准,选择适用于仪表的功能失效控制策略和信息安全防护策略。

[0114] 智能仪表作为现场物理层的设备,面临的信息安全威胁主要包括DOS攻击,未知设备的接入,篡改等,本发明根据IEC62443信息安全标准选取了访问控制、入侵检测、日志管理、权限控制、身份验证策略,考虑仪表主要通过传感与检测、数据处理与控制、电输出与驱动以及网络通信接口功能模块实现仪表的采集、运算、输出以及通信功能,一旦某功能模块失效,将极大影响仪表作用价值。本发明根据IEC61508选取了微处理器单元诊断、采集诊断、输出诊断、时序和逻辑监视以及多重化技术策略。

[0115] 步骤5.2:根据相关安全标准中对仪表的功能安全和信息安全策略的定性描述,根据仪表安全策略的安全功能、策略关联、安全目标属性,分析安全策略能够缓解的仪表功能

模块安全漏洞以及安全策略实施效果。

[0116] 以权限控制为例，权限控制是保护工业控制系统及其关键资产不受意外破坏的第一步。权限控制决定相关角色应该被允许进入或离开一个系统的过程。一旦确定了这些信息，就可以实施纵深防御访问控制措施，以验证只有经过授权的人员和设备才能真正访问工业控制系统。因此权限控制能够缓解未知设备接入漏洞。相比于传统的权限控制，基于角色的权限控制通过基于用户角色或工作职责的访问克服了动态环境中难以及时更新角色权限的问题，具有更好的漏洞防护效果。

[0117] 步骤6：在因果失效模型中添加安全属性关联的防护节点，建立安全策略的评价模型。

[0118] 步骤6.1：根据仪表安全策略实施能够缓解的仪表功能模块安全漏洞，在仪表一体化因果失效模型中连接攻击节点和漏洞节点的逻辑门后以及功能失效节点后添加防护节点。

[0119] 根据步骤五分析得出信息安全策略实施能够缓解的漏洞，在相应的攻击路径中添加防护节点，根据步骤五分析得出的功能安全策略实施能够缓解的功能模块脆弱性，在相应的失效路径中添加防护节点。仪表功能安全和信息安全策略关联防护节点参见表4所示。

[0120] 表4

[0121]

		关联防护节点			关联防护节点
功能安全策略	访问控制	D_1，D_2	信息安全策略	微处理器单元诊断	D_3
	日志管理	D_1，D_2，D_5		采集诊断	D_4
	入侵检测	D_3，D_4，D_6，D_7		输出诊断	D_6
	权限控制	D_2		多重化技术	D_3，D_4
	身份验证	D_1		时序和逻辑监视	D_3

[0122] 步骤6.2：根据仪表安全策略的实施效果，对防护节点设置不同的防护系数，建立仪表安全策略评价模型。

[0123] 对于功能安全和信息安全策略安全等级属性，本发明设置了两种不同等级，安全策略等级属性表参见表5所示。

[0124] 表5

[0125]

策略安全等级	定义	防护节点 D_i 取值
LV=0	未实施安全策略	1
LV=1	一定程度上缓解仪表安全漏洞	0.67
LV=2	能够有效缓解仪表安全漏洞	0.33

[0126] 基于上述步骤，建立仪表安全策略评价模型。仪表安全策略评价模型中各节点的含义参见表6所示。

[0127] 表6

[0128]

节点符号	含义
V_1	CNVD-2021-07490
V_2	CNNVD-2019-02
V_3	CNVD-2021-17406
A_1	攻击者借助仪表管理通信软件的组态对智能仪表的处理单元注入恶意代码
A_2	攻击者通过未授权的仪表通信组态软件对仪表测量功能模块进行攻击
A_3	攻击者发动拒绝服务攻击
F_1	数据处理与控制功能模块失效
F_2	传感与检测功能模块失效
F_3	电输出与驱动功能模块失效
F_4	网络通信接口功能模块失效

[0129] 步骤7：结合仪表各功能模块资产，根据风险量化公式对仪表功能安全和信息安全策略进行量化评估。

[0130] 步骤7.1：考虑仪表传感与检测、数据处理与控制、电输出与驱动、网络通信等安全相关功能模块资产，根据功能模块的重要性进行专家打分；

[0131] 步骤7.2：结合安全策略实施前后仪表各功能模块失效概率的变化值$\Delta P(F_i)$，运用量化公式对仪表的功能安全和信息安全策略进行量化评估。

[0132] $$\Delta R=\sum_{i=1}^{n}\Delta P(F_i)W_i \qquad (2)$$

[0133] 其中，ΔR为安全策略实施前后仪表风险变化值，n为仪表安全相关功能模块数量，W_i为基于专家打分的仪表各功能模块的价值分数。

[0134] 通过分析历史数据或咨询现场工程人员获得F_1，F_2，F_3节点的条件概率$P(F_1|A_1,V_1)$，$P(F_2|A_2,V_2)$，$P(F_3|F_1,F_2)$，$P(F_4|F_1,A_3,V_3)$，结合攻击事件节点A_1，A_2，A_3的发生概率$P(A_1)$，$P(A_2)$，$P(A_3)$，以及漏洞节点的发生概率$P(V_1)$，$P(V_2)$，$P(V_3)$。进而能够计算出各功能模块失效概率$P(F_1)$，$P(F_2)$，$P(F_3)$，$P(F_4)$。

[0135] 通过实施安全策略，在安全防护节点的作用下，得到新的攻击事件节点发生概率$\tilde{P}(A_1)$，$\tilde{P}(A_2)$，$\tilde{P}(A_3)$，新的漏洞节点的发生概率$\tilde{P}(V_1)$，$\tilde{P}(V_2)$，$\tilde{P}(V_3)$，进而得到各功能模块失效事故新的概率$\tilde{P}(F_1)$，$\tilde{P}(F_2)$，$\tilde{P}(F_3)$，$\tilde{P}(F_4)$，结合功能模块的价值分数W_i，i＝1,2,3,4，最终得到风险变化值公式

[0136] $$\Delta R=\sum_{i=1}^{4}\left(P(F_i)-\tilde{P}(F_i)\right)W_i \qquad (3)$$

[0137] 根据公式(3)计算出的各安全策略实施前后的风险值的变化，对仪表的功能安全和信息安全策略进行量化评估。

[0138] 实施功能安全策略后的功能模块失效概率$\tilde{P}(F_i)$计算公式为：

[0139] $$\tilde{P}(F_i) = d_j \times P(F_i) \tag{4}$$

[0140] 实施信息安全策略后的功能模块失效概率$\tilde{P}(F_i)$计算公式为：

[0141] $$\begin{aligned}\tilde{P}(F_i) = {} & P(F_i \mid V_i = T,\ A_i = T) * d_j * P(V_i = T) * d_j * P(A_i = T) \\ & + P(F_i \mid V_i = T,\ A_i = F) * d_j * P(V_i = T) * P(A_i = F) \\ & + P(F_i \mid V_i = F,\ A_i = T) * P(V_i = F) * d_j * P(A_i = T) \\ & + P(F_i \mid V_i = F,\ A_i = F) * P(V_i = F) * P(A_i = F)\end{aligned} \tag{5}$$

[0142] d_j为能够缓解仪表安全漏洞对应安全策略的关联防护节点的防护系数。

[0143] 以上内容本领域的技术人员容易理解，以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

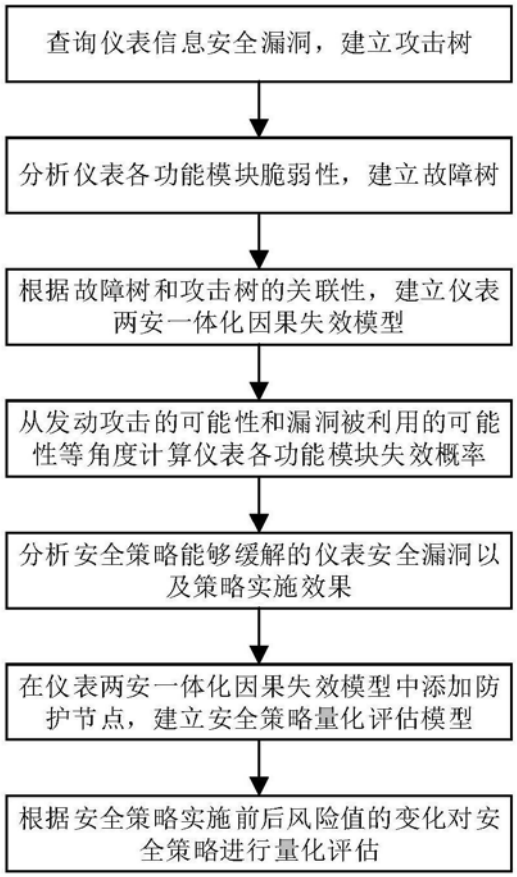

查询仪表信息安全漏洞，建立攻击树
分析仪表各功能模块脆弱性，建立故障树
根据故障树和攻击树的关联性，建立仪表两安一体化因果失效模型
从发动攻击的可能性和漏洞被利用的可能性等角度计算仪表各功能模块失效概率
分析安全策略能够缓解的仪表安全漏洞以及策略实施效果
在仪表两安一体化因果失效模型中添加防护节点，建立安全策略量化评估模型
根据安全策略实施前后风险值的变化对安全策略进行量化评估

图1

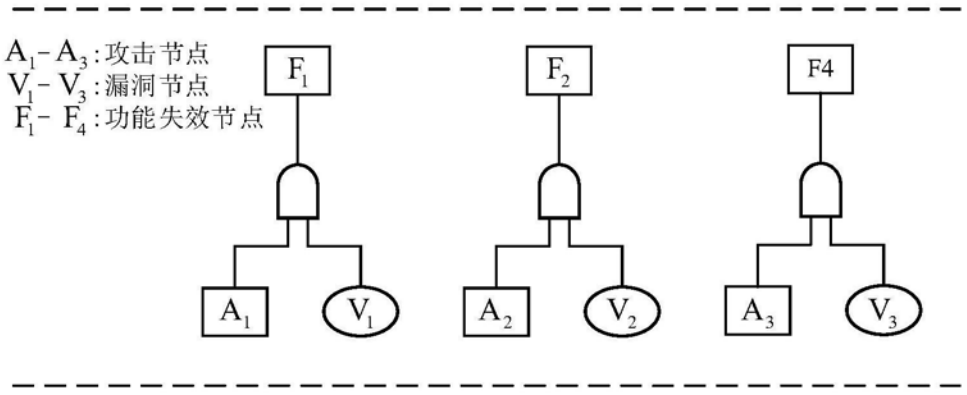

A1-A3:攻击节点
V1-V3:漏洞节点
F1-F4:功能失效节点
F1
F2
F4
A1
V1
A2
V2
A3
V3

图2

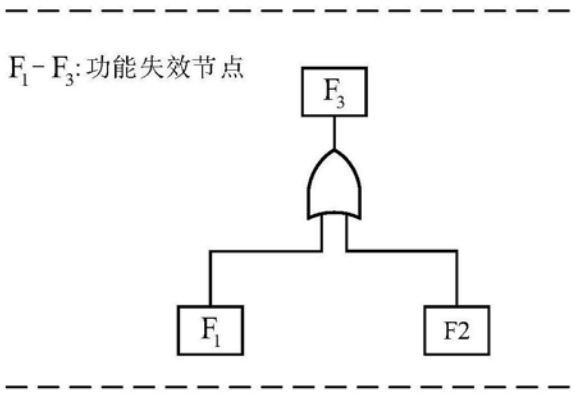

F1-F3:功能失效节点
F3
F1
F2

图3

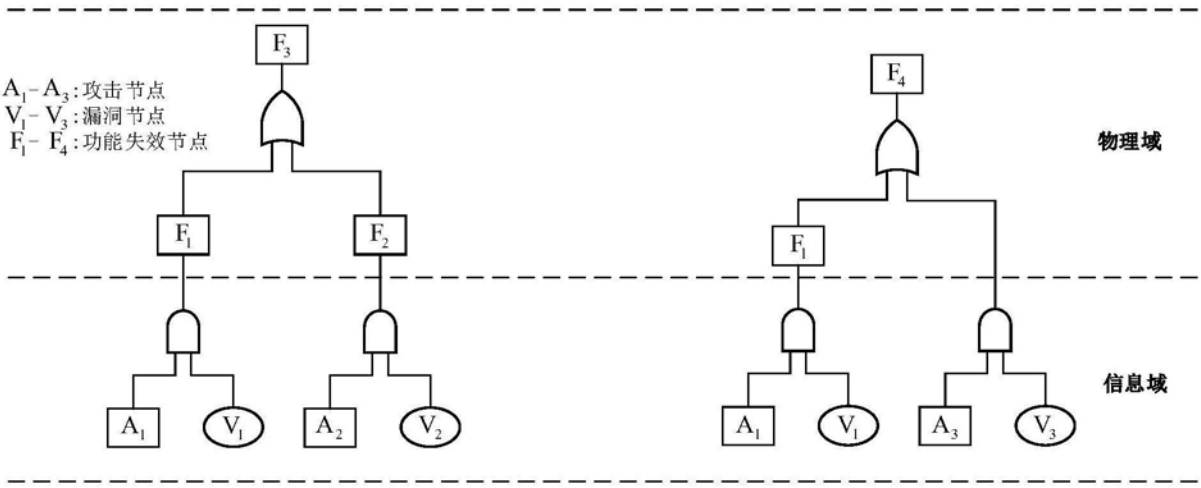

A1-A3:攻击节点
V1-V3:漏洞节点
F1- F4:功能失效节点
F3
F1
F2
A1
V1
A2
V2
F4
F1
A1
V1
A3
V3
物理域
信息域

图4

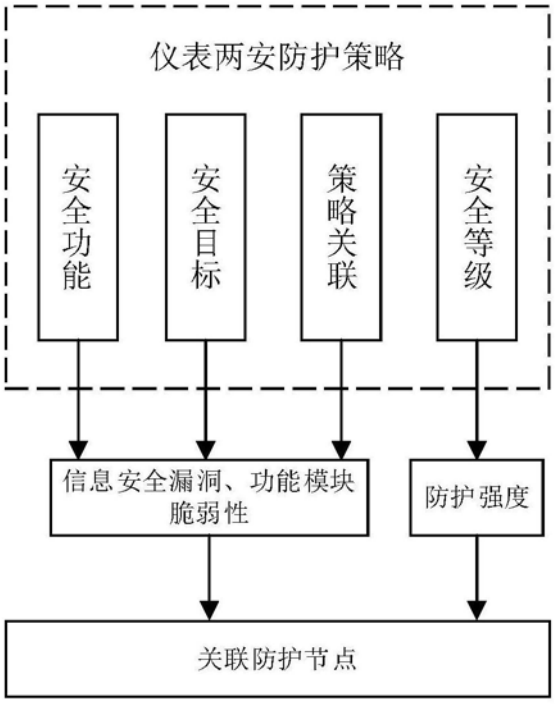

仪表两安防护策略
安全功能
安全目标
策略关联
安全等级
信息安全漏洞、功能模块脆弱性
防护强度
关联防护节点

图5

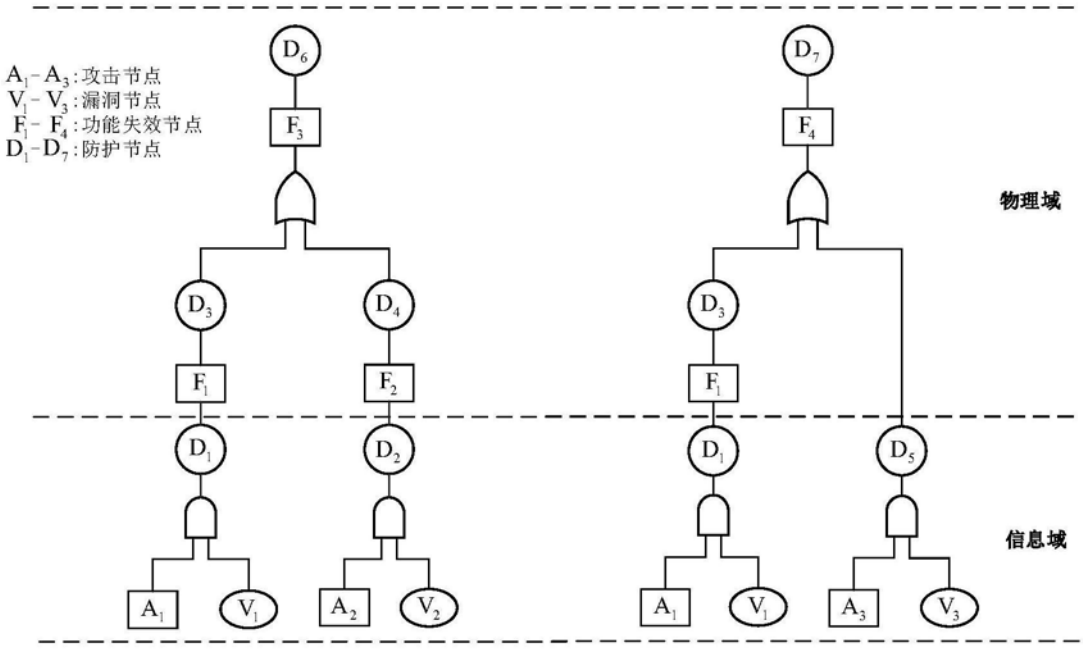

A1-A3:攻击节点
V1-V3:漏洞节点
F1-F4:功能失效节点
D1-D7:防护节点
D6
F3
D7
F4
物理域
D3
D4
D3
F1
F2
F1
D1
D2
D1
D5
信息域
A1
V1
A2
V2
A1
V1
A3
V3

图6