DOI:10.12158/j.2096-3203.2022.03.002

计及网络攻击影响的安全稳定控制系统风险评估方法

钱胜[1]，王琦[1]，颜云松[2]，封科[2]，夏海峰[2]
（1. 东南大学电气工程学院，江苏 南京 210096；
2. 南瑞集团（国网电力科学研究院）有限公司，江苏 南京 211106）

摘 要：安全稳定控制系统（稳控系统）是保证电网可靠运行的重要防线，针对稳控系统的网络攻击会造成严重的物理后果。为了量化评估稳控系统遭受网络攻击的影响，解决现有风险评估方法未充分考虑网络攻击易发性的问题，文中提出一种计及网络攻击影响的稳控系统风险评估方法。文中首先分析了稳控系统的层次结构；然后，从攻击对象、攻击方式、攻击后果 3 个角度分析了稳控装置本体与稳控装置站间通信的网络攻击风险点；其次，基于模糊层次分析法对网络攻击易发性进行量化，并结合由 Petri 网建立的网络攻击防护单元模型建立针对稳控系统的网络攻击成功概率模型；最后，结合物理后果和攻击成功概率，对标准系统和实际系统进行风险评估，计算了正常运行和网络攻击 2 种情况下的风险值，验证了所提模型的有效性。

关键词：安全稳定控制系统；网络攻击；易发性；模糊层次分析法；Petri 网；风险评估
中图分类号：TM715 **文献标志码**：A **文章编号**：2096-3203（2022）03-0014-08

0 引言

随着能源互联网的不断发展，信息系统的安全对于物理系统愈发重要[1—2]。针对信息系统的网络攻击具有低成本、易实施和影响范围广的特点，逐渐成为敌对国家、组织对电力系统进行破坏的重要手段[3—4]。安全稳定控制系统（稳控系统）作为保证电网可靠运行的重要防线，呈现出大型化、广域化和复杂化的趋势。由于其控制节点多、控制链条长，若遭遇网络攻击导致系统误动、拒动，可能给电网造成巨大的运行风险[5—8]，因此研究稳控系统遭受网络攻击的风险评估方法具有重要意义。

根据攻击目的的不同，电力系统的攻击行为可划分为破坏可用性、破坏完整性以及破坏保密性的网络攻击[9—11]。针对电力系统网络攻击的研究主要采用攻击图、复杂网络理论、攻击树和 Petri 网等方法。（1）攻击图模型通过分析攻击者对存在的安全漏洞进行攻击的行为，找到所有能达到攻击目标的攻击路径。文献[12]提出了一种改进的电力信息物理系统连锁故障失效评估的攻击图模型，但缺乏对信息系统攻击成功的可能性分析；文献[13—15]采用攻击图的方法研究工业物联网的脆弱性，但缺乏对攻击后果的分析；文献[16]考虑网络攻击对电力系统的影响，基于攻击图建立了网络攻击成功概率模型，量化评估网络攻击对电力系统的影响，但求取网络攻击成功概率时仅考虑了通信路径上防御措施的漏洞。（2）复杂网络理论能从局部和整体的视角分析电网系统安全风险传播行为。文献[17]采用复杂网络理论进行电力系统风险评估，从安全漏洞和防御措施 2 个方面建立概率模型，但是该模型以物理网络的连通能力作为风险指标，对电力系统的物理本质考虑不足。（3）攻击树模型使用树形结构描述对系统的网络攻击，将攻击总目标作为根节点，将总目标分为多个子目标，并将其作为子节点，逐步细分，从根节点到子节点的路径表示一次完整的攻击过程。文献[18]基于攻击树的方法对工业控制系统进行风险评估，应用多属性效应理论计算网络攻击成功概率，但缺乏对网络攻击行为的易发性建模且主观性较强。（4）Petri 网通过定义库所、变迁、弧和令牌等元素构成攻击过程模型，可体现出攻击当前状态、攻击动作和进程，清晰表述动作和状态的意义并量化计算，适用于对离散事件动态系统建模[19]。如何评估网络攻击事件的易发性及成功概率，合理量化网络攻击对稳控系统的影响仍有待研究。

网络攻击易发性评估属于多目标决策问题，在评估过程中容易存在主观性较强的缺点。模糊层次分析法结合层次分析法和模糊数学的特点，可以有效分析目标准则体系层次之间的非序列关系，提高多因素下针对目标事件评估的可靠性。

基于以上分析，文中首先分析了稳控系统的层次结构；然后从攻击对象、攻击方式和攻击后果 3 个角度分析了稳控装置本体与稳控装置站间通信的

收稿日期：2022-01-12；修回日期：2022-03-27
基金项目：国家重点研发计划资助项目（2017YFB09030）；国家电网有限公司总部科技项目（5100-202040440A-0-0-00）

风险点;其次,基于模糊层次分析法对网络攻击易发性进行量化,并结合由 Petri 网建立的网络攻击防护单元模型,建立网络攻击成功概率模型;最后,以标准系统和实际系统为算例验证了所提风险评估方法的有效性。

1 稳控系统层次结构及风险点分析

稳控系统是为了保证电力系统在遇到大扰动时安全稳定运行而在重要发电厂或变电站内装设的控制设备,是实现紧急切机组、切负荷、直流功率紧急提升或回降等功能的二次控制系统。

1.1 稳控系统的组成结构

稳控系统一般由多套稳控装置经通信通道连接配合构成。一个系统中一般设置 1 个稳定控制主站,其余为控制子站和执行站,各站之间通过复用 2M 通道或专用光纤通道连接,稳控系统典型三层结构如图 1 所示。MS 为控制主站;SS1—SS4 分别为 4 个控制子站;ES1—ES7 分别为 7 个执行站。

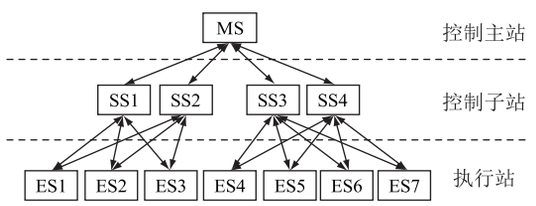

图 1 稳控系统典型三层结构示意

Fig.1 Schematic diagram of typical three-layer structure of security and stability control system

不同层级的稳控装置具有不同的功能。控制主站主要负责控制策略的决策,汇集本站和下属站点的信息,采用离线预定或者在线决策的控制策略,向下属站点下达控制命令;控制子站主要负责对本地信息采样以及汇集下属站点的采样信息,是控制主站和执行站之间信息和命令传递的关键枢纽;执行站主要负责执行控制主站发过来的远方控制命令,采集并上传本地信息。

1.2 稳控业务面临的网络攻击风险点分析

稳控装置是保证稳控业务正确执行的重要设备,文中主要从装置本体以及装置站间通信 2 个方面来分析稳控业务面临的网络攻击风险点。

1.2.1 装置本体结构风险点分析

(1) 攻击对象。针对稳控装置本体的网络攻击对象主要有 3 种:装置硬件层,主要包括装置芯片、核心板卡模块;装置系统层,主要包括装置嵌入式系统、数字信号处理系统和 VxWorks、Linux 操作系统;应用层,主要包括各种安全稳定控制决策功能模块、通信功能模块、出口功能模块等应用模块。

(2) 攻击方式。针对装置硬件层、装置系统层及应用层的木马攻击:攻击者将木马故意植入电子系统中的特殊模块以及电路,或者设计者无意留下的缺陷模块以及电路。这种模块或电路一般潜伏在原始电路中,但在特殊条件触发下,能被攻击者利用以对原始电路进行有目的性的修改,实现破坏性功能。

(3) 攻击后果。攻击后果主要分为 2 个等级:① 造成稳控系统控制功能整体失效,当控制主站或子站装置遭受网络攻击后,会产生错误提升或回降的直流功率,大量误切机组或负荷,破坏电网稳定;② 造成稳控系统控制功能局部失效,执行站遭受网络攻击后,导致预先设定的动作措施不能正常执行,仅影响电网一次系统的局部范围,一般能保证电网稳定运行。

1.2.2 稳控装置站间通信风险点分析

(1) 攻击对象。针对稳控系统装置站间通信的网络攻击对象主要分为装置与通信接口装置、通信接口装置与同步数字体系(synchronous digital hierarchy,SDH)、SDH 与 SDH 通信通道。

(2) 攻击方式。针对装置与通信接口装置、通信接口装置与 SDH、SDH 与 SDH 通信通道的主要攻击方式有网络风暴、窃听和篡改等。一方面,攻击者可以利用通信协议漏洞发起网络风暴,令稳控系统中的设备瘫痪,失去服务能力;另一方面,攻击者通过物理层接入电力通信专网,串入攻击设备,实现对光通信系统的窃听或接管通信网络篡改正常的数据,进而对稳控系统发动攻击。

(3) 攻击后果。通过对稳控装置站间传输发动攻击,可造成量测数据或控制数据的错误,通过向变电站内稳控装置发送非正常控制指令,可造成误切机或切负荷动作,导致直流换流站的稳控装置误提升或回降直流,此类攻击会给电网的安全稳定运行造成巨大威胁。

2 稳控业务遭受网络攻击的风险评估方法

稳控业务遭受网络攻击的风险评估方法包含 3 个步骤:首先基于模糊层次分析法建立网络攻击易发性模型;其次结合网络攻击传播过程的 Petri 网模型,建立网络攻击成功概率模型;最后结合网络攻击物理后果,提出相应的风险评估方法。

2.1 针对稳控业务的网络攻击易发性评估模型

考虑稳控系统和网络攻击的特点,构建了 3 层评估指标体系,如图 2 所示。从攻击方水平(S_1)、设备管理(S_2)和设备安全(S_3)3 个角度,全面地对

网络攻击事件易发性进行评估。攻击方水平方面主要考虑攻击方知识(I_1)、攻击成本(I_2)以及攻击被发现的可能性(I_3);设备管理方面主要考虑设备重要度(I_4)、软硬件故障(I_5)以及工作员操作(I_6);设备安全方面主要考虑设备漏洞(I_7)、身份认证(I_8)以及加密算法(I_9)。

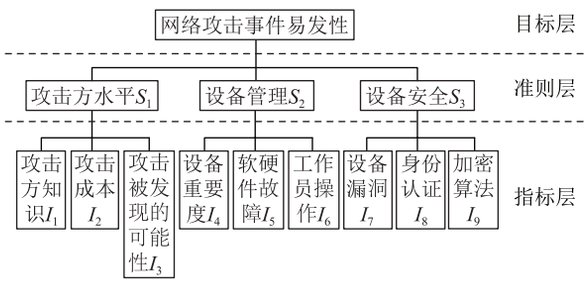

图 2 网络攻击事件易发性模型

Fig.2 Susceptibility model of cyber attack incident

攻击方水平、设备管理和设备安全指标的评分标准见表 1—表 3。

表 1 攻击方水平评分标准

Table 1 Evaluation criteria of attacker level index

攻击方知识 I_1	攻击成本 I_2	攻击被发现的可能性 I_3	等级
专业黑客	>5	很容易	5
复杂系统知识	2~5	容易	4
网络工程师	1~2	中等	3
掌握常规攻击	0.5~1	难	2
了解系统结构	<0.5	很难	1

表 2 设备管理评分标准

Table 2 Evaluation criteria of equipment management

设备重要度 I_4	等级	软硬件故障 I_5	等级	工作员操作 I_6	等级
很重要	1	很难	5	极其规范	5
重要	2	难	4	十分规范	4
稍微重要	3	中等	3	稍微规范	3
一般	4	容易	2	规范	2
不重要	5	很容易	1	不规范	1

表 3 设备安全评分标准

Table 3 Evaluation criteria of equipment safety

设备漏洞 I_7	等级	身份认证 I_8	等级	加密算法 I_9	等级
极多	1	很难	5	很难	5
很多	2	难	4	难	4
部分	3	中等	3	中等	3
很少	4	容易	2	容易	2
极少	5	很容易	1	很容易	1

基于模糊层次分析法分配指标层以及准则层权重,具体方法可参考文献[20]。在文中的研究中,网络攻击事件易发性概率模型为:

$$P_{\mathrm{h}} = W_{\mathrm{a}} \sum_{k=1}^{3} W_k U(x_k) + W_{\mathrm{b}} \sum_{l=1}^{3} W_l U(x_l) + W_{\mathrm{c}} \sum_{o=1}^{3} W_o U(x_o) \quad (1)$$

式中:W_{a},W_{b},W_{c}分别为准则层 3 个方面的权重系数;W_k,W_l,W_o分别为攻击方水平、设备管理及设备安全 3 个准则所对应的第 k,l,o 个指标的权重系数;$U(x)$为对应指标参数的效用值,取 $U(x)=\mathrm{e}^{-x}$。

2.2 基于 Petri 网的网络攻击防护单元建模

目前稳控系统针对网络攻击的防护研究还在起步阶段,其中加密和认证是稳控系统针对网络攻击的主要防护手段。

2.2.1 加密模型

密码模型主要由两部分组成:登录尝试概率和响应速度。登录尝试概率为所有动作中入侵尝试动作的概率,可由失败日志记录数得到;响应速度为中央处理器(central processing unit,CPU)时钟运行速度。加密模型如图 3 所示,其中,灰色矩形表示瞬时变迁;白色矩形表示时延变迁;λ_{S} 为重复登陆间的时延;P_{f} 为密码模型入侵失败的概率;P_{S}为密码模型成功入侵目标系统的概率,可由式(2)估计得到。

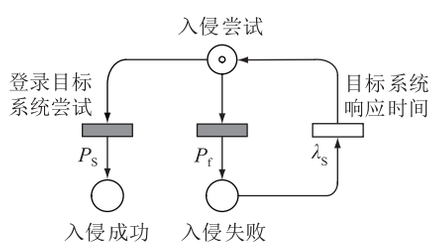

图 3 加密模型

Fig.3 Password model

$$P_{\mathrm{S}} = \frac{f_{\mathrm{S}}}{N_{\mathrm{S}}} \quad (2)$$

式中:f_{S} 为入侵成功数;N_{S} 为总记录数。

2.2.2 认证模型

认证加密方案在具体实现中可能有不同手段,其中硬件加密具有兼容性好、速度快的特点,被广泛使用。基于硬件加密的身份认证过程如下:

(1) 初始化阶段。客户端和服务器端共享一个加密硬件。

(2) 客户端向服务器发出一个验证请求,然后服务器端产生随机数并通过网络传输给客户端。

(3) 客户端将收到的随机数与存储在加密硬件中的密钥进行散列运算,并将结果作为认证证据传给服务器。

(4) 服务器端对传递过来的随机数进行散列运

算,得到服务器端的信息摘要,并与客服端的信息摘要比较,相同则认证成功。

依据此过程,身份认证模型如图 4 所示。其中,λ_d 为以各种手段偷取一个系统内已在使用的加密硬件所需要的时间;λ_e 为复制一个新的加密硬件所需要的时间;λ_t 为系统更换加密硬件的周期;λ_q 为成功获取到一个服务器发来的随机数所需要的时间;λ_g 为服务器校验终端发回信息所需要的时间。

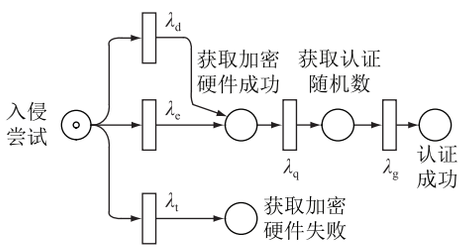

图 4　身份认证模型

Fig.4　Identity authentication model

2.2.3　网络攻击成功概率模型

一次成功的网络攻击一般须要突破加密和认证环节,因此将密码模型和身份认证模型进行串联,建立网络攻击传播过程的 Petri 网模型,如图 5 所示。由于攻击者发动重复攻击时只须要获得一次硬件便可以多次使用,因此图中用瞬时变迁代替身份认证模型中的时延变迁,在模型图里将这一环节简化为瞬时变迁表示的概率。P_d,P_e分别为偷取加密硬件和复制加密硬件的成功概率。

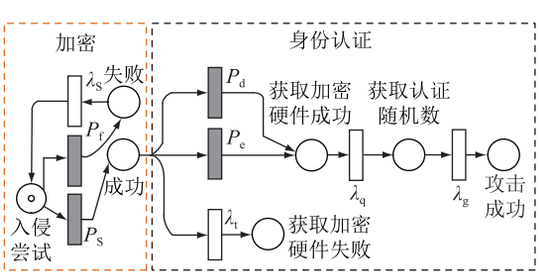

图 5　网络攻击过程模型

Fig.5　Process model of cyber attacks

结合 2.1 节网络攻击事件的易发性模型和网络攻击过程模型,建立网络攻击成功概率模型为:

$$P_s = P_h P_J \tag{3}$$

式中:P_J 为采用 Petri 网仿真软件得到的网络攻击传播模型的仿真结果。

2.3　考虑网络攻击的稳控业务风险评估方法

考虑网络攻击的稳控业务风险评估方法如图 6 所示,具体步骤如下。

步骤 1:通过外部循环实现对各个执行站中稳控业务遭受网络攻击的考虑,每次针对一个执行站中稳控业务遭受网络攻击的情景进行计算。

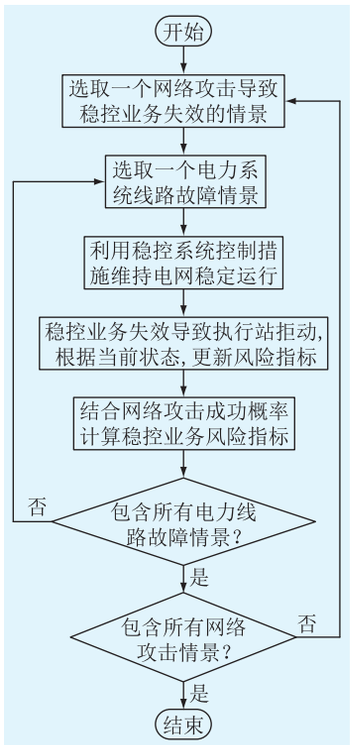

图 6　考虑网络攻击的稳控业务风险评估流程

Fig.6　Flow chart of the risk assessment of a stable business considering cyber attacks

步骤 2:通过内部循环实现对电力系统故障情景的考虑。

步骤 3:利用稳控系统控制措施维持电网运行。针对标准系统可以采用最优减载算法[21]得到控制措施;针对实际系统可以根据已知故障场景得到控制措施后,采用电力系统分析软件仿真得到故障后果。如果稳控业务因网络攻击失效,导致执行站拒动,将对当前状态重新计算风险指标。

步骤 4:结合网络攻击成功概率,稳控业务遭受网络攻击后,执行站 i 的风险指标 R_i 为:

$$R_i = P_s P_l M_i \tag{4}$$

式中:P_l为电力线路故障场景发生概率;M_i为网络攻击和电力线路故障同时发生后执行站 i 的评估指标。

3　算例分析

采用 IEEE 30 标准系统以及实际系统对文中所提方法进行验证,在 IEEE 30 系统每个负荷不为 0 的节点安装执行站装置。实际系统以及对应的稳控系统控制架构参见文献[21]。

3.1　网络攻击成功概率计算

通过 2.1 节分析可知,针对稳控装置本体实施网络攻击,一般应熟悉芯片、操作系统或应用软件内部信息,难度极大且成本极高,因此文中主要考

虑针对稳控装置站间通信通道的网络攻击。

假设通过访问变电站并偷取一个加密硬件，访问周期为 30 d，偷取成功概率为 0.1。复制一个加密硬件所需要的时间为 90 d，复制成功概率为 0.1。假设加密硬件的更换周期是 360 d。基于图 5 所示网络攻击过程模型，采用 YASPER Petri 网仿真软件进行 10 000 次仿真，仿真得到 P_J 为 0.038。

网络攻击事件的具体赋值由专家在实际情况中根据特定条件和经验打分，如表 4—表 8 所示。

表 4 准则层模糊评判矩阵

Table 4 Fuzzy evaluation matrix of criterion layer

指标	S_1	S_2	S_3
S_1	0.50	0.85	0.60
S_2	0.15	0.50	0.35
S_3	0.40	0.65	0.50

表 5 攻击方水平模糊评判矩阵

Table 5 Fuzzy evaluation matrix of attacker level index

指标	I_1	I_2	I_3
I_1	0.50	0.82	0.65
I_2	0.18	0.50	0.32
I_3	0.35	0.68	0.50

表 6 设备管理模糊评判矩阵

Table 6 Fuzzy evaluation matrix of equipment management

指标	I_4	I_5	I_6
I_4	0.50	0.71	0.55
I_5	0.29	0.50	0.42
I_6	0.45	0.58	0.50

表 7 设备安全模糊评判矩阵

Table 7 Fuzzy evaluation matrix of equipment safety

指标	I_7	I_8	I_9
I_7	0.50	0.62	0.56
I_8	0.38	0.50	0.42
I_9	0.44	0.58	0.50

表 8 网络攻击事件评分等级

Table 8 Evalution level of cyber attack events

事件	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9
1	5	4	5	1	3	5	5	4	4
2	4	4	3	2	2	3	3	4	4
3	4	4	2	3	3	4	5	4	4

结合式(1)、式(3)及表 8，事件 1 表示网络攻击对象为装置与通信接口装置，攻击成功概率为 0.001 4；事件 2 表示网络攻击对象为通信接口装置与 SDH，攻击成功概率为 0.001 6；事件 3 表示网络攻击对象为 SDH 与 SDH 通信通道，攻击成功概率为 0.001 5。

3.2 针对标准系统的故障仿真

采用最优减载算法计算切负荷量，评估指标 M_i 如式(5)所示。

$$M_i = \frac{1}{m}\sum_{i}^{m}\sum_{j=1}^{n} L_{i,j} \tag{5}$$

式中：m 为执行站数量；n 为电力线路数量；$L_{i,j}$ 为第 j 条线路故障后执行站 i 的切负荷量。

计算切负荷量的结果如表 9 所示，其中切负荷量 L 为不考虑网络攻击时的评估指标，切负荷量 K 为考虑网络攻击时的评估指标。从表中可以看出，不考虑网络攻击时，除了 ES1、ES2、ES3、ES6、ES7、ES8、ES9、ES16、ES17 执行站在线路发生故障时并未产生切负荷量，其他执行站均有切负荷量，且最高切负荷量为 24.40 MW，占全部负荷的 12.91%。

表 9 各执行站的切负荷量

Table 9 Load shedding of each execution station

执行站	切负荷量 L/MW	切负荷量 K/MW	执行站	切负荷量 L/MW	切负荷量 K/MW
ES1	0	28.21	ES11	2.81	14.42
ES2	0	3.12	ES12	1.27	5.39
ES3	0	9.88	ES13	2.98	15.27
ES4	24.40	53.23	ES14	1.26	4.08
ES5	20.46	58.78	ES15	9.50	31.93
ES6	0	7.54	ES16	0	4.16
ES7	0	14.56	ES17	0	11.31
ES8	0	8.06	ES18	3.50	4.67
ES9	0	10.66	ES19	0.68	3.79
ES10	0.19	4.75	ES20	2.32	16.05

当电力系统发生 $N-1$ 故障，考虑网络攻击导致稳控业务失效时，执行站的切除负荷量明显增加。其中执行站 ES5 的切负荷量最多，高达 58.78 MW。这是因为执行站 ES5 对应电力节点 8，其负荷需求最大，当线路发生故障且执行站无法正常切除负荷时，容易导致其他线路潮流过载而断开，此时根据电网当前状态重新计算切负荷量时，故障后果明显增加。例如当电力线路 6—8 故障时，执行站 ES5 应切负荷 19.46 MW，但由于装置拒动，使线路 6—28 以及 8—28 因过载而断开，节点 8 上的负荷全部丢失，增加了线路故障的影响后果。

图 7 为不同故障情景下执行站的切负荷量，更加清晰直观地展现出考虑网络攻击时，稳控业务失效造成的故障后果。各执行站切负荷量相比稳控业务正常时切负荷量明显增加，其中执行站 ES5 切负荷量增加最多，ES18 切负荷量增加最少。

基于 2.3 节考虑网络攻击的稳控业务风险评估

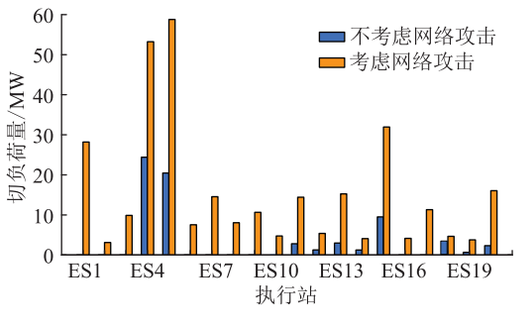

图 7 不同故障情景下执行站的切负荷量

Fig.7 Load shedding of execution stations under different failure scenarios

方法及式(4),其中线路的故障概率为 0.14%,计算后果经归一化后如图 8 所示。

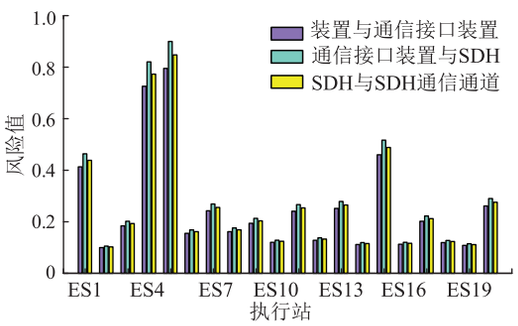

图 8 不同网络攻击场景下执行站的风险值

Fig.8 Risk value of execution stations under different cyber attack scenarios

从图 8 可以看出,执行站 ES4、ES5 的风险值比其他装置高。而当同一个执行站遭受网络攻击后,攻击通信接口装置与 SDH 所造成的风险最大,这是因为风险值不仅与网络攻击事件成功概率有关,还和攻击所造成的影响相关。这 3 种网络攻击事件都导致稳控业务失效,造成的拒动后果相同,而针对通信接口装置与 SDH 的网络攻击成功概率最高,因此其风险值最大。

3.3 针对实际系统的故障仿真

以某实际特高压交直流混联系统[21]的稳控系统作为研究对象,分析不同执行站因网络攻击而拒动对暂态频率的影响。故障场景为某条直流双极闭锁,损失功率为 3 100 MW。此时为了保持系统频率稳定,执行站 ES1—ES5 分别提升直流 550 MW,250 MW,100 MW,250 MW,50 MW,并且执行站 ES6—ES11 分别切除负荷 300 MW,375 MW,275 MW,250 MW,300 MW,300 MW。若稳控业务遭受网络攻击失效后,频率跌落最大量为 0.552 4 Hz。针对执行站进行 N-1 故障遍历,并以频率跌落量为评估指标,即式(4)中的 M_i。该指标由 BPA 仿真计算得到,仿真时间设置为 60 s。网络攻击各执行站对系统频率的影响见表 10。

表 10 网络攻击各执行站对系统频率的影响

Table 10 The impact of cyber attacks on various execution stations on system frequency

执行站	M_i/Hz	执行站	M_i/Hz
ES1	0.043 00	ES7	0.036 98
ES2	0.034 05	ES8	0.033 85
ES3	0.033 94	ES9	0.033 91
ES4	0.034 44	ES10	0.035 13
ES5	0.028 98	ES11	0.035 10
ES6	0.035 19		

由表 10 可知,考虑网络攻击时,执行站发生 N-1 故障,系统频率跌落量在 0.028 98~0.043 00 Hz 范围内,系统频率保持在安全范围内。系统频率跌落量不仅和执行站的执行量有关,也和执行站的位置相关。

假设电力系统中直流双极闭锁的故障概率为 0.01%,针对各执行站的网络攻击风险计算后果经归一化后如图 9 所示。

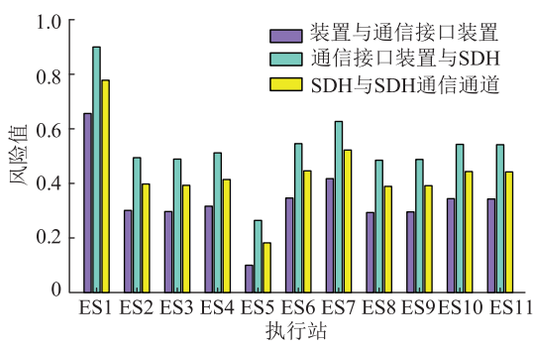

图 9 考虑网络攻击时实际系统中各执行站的风险值

Fig.9 Risk value of execution stations in the actual system considering cyber attacks

从图 9 可以看出,相较其他执行站,针对 ES1 的网络攻击风险值较大。主要是因为 ES1 拒动时,系统频率跌落量较大。相较其他 2 种方式,针对通信接口装置与 SDH 的网络攻击风险值较大,这是因为针对通信接口装置与 SDH 的网络攻击成功概率最高,同一稳控业务失效造成的后果一样。

4 结语

稳控系统存在较多网络安全隐患,攻击者可利用信息传输过程中的安全漏洞,实现对稳控业务的网络攻击。据此,文中基于模糊层次分析法建立了网络攻击易发性概率模型,并结合由 Petri 网建立的网络攻击防护单元模型,提出了一种针对网络攻击的稳控业务风险量化评估方法,克服了已有方法只能定性分析或缺乏物理后果分析的不足,比较了不

同网络攻击事件对稳控业务风险值的影响大小。通过开展信息安全风险评估工作，可以发现稳控系统信息网络中存在的主要问题，帮助运维人员找出系统薄弱的环节，为稳控系统信息网络防护措施提供参考依据。

文中研究的稳控系统是基于主站—子站—执行站的集中式控制模式，在后续工作中，可考虑灵活的分布式控制，研究不同运行方式和表决模式下的稳控系统风险评估方法，以此来适应未来大电网发展的实际需求。

参考文献：

[1] 汤奕，李梦雅，王琦，等. 电力信息物理系统网络攻击与防御研究综述：(二)检测与保护[J]. 电力系统自动化，2019，43(10)：1-9，18.
TANG Yi，LI Mengya，WANG Qi，et al. A review on research of cyber-attacks and defense in cyber physical power systems：part two detection and protection[J]. Automation of Electric Power Systems，2019，43(10)：1-9，18.

[2] 王琦，李梦雅，汤奕，等. 电力信息物理系统网络攻击与防御研究综述：(一)建模与评估[J]. 电力系统自动化，2019，43(9)：9-21.
WANG Qi，LI Mengya，TANG Yi，et al. A review on research of cyber-attacks and defense in cyber physical power systems：part one modelling and evaluation[J]. Automation of Electric Power Systems，2019，43(9)：9-21.

[3] 王子骏，刘杨，鲍远义，等. 电力系统安全仿真技术：工程安全、网络安全与信息物理综合安全[J]. 中国科学：信息科学，2022，52(3)：399-429.
WANG Zijun，LIU Yang，BAO Yuanyi，et al. Power system security simulation technologies：engineering safety，network security and cyber-physical integrated security[J]. ScientiaSinica (Informationis)，2022，52(3)：399-429.

[4] 邓松，张建堂，祝展望. 网络攻击下能源互联网数据容侵评估技术综述[J]. 电力信息与通信技术，2021，19(1)：11-19.
DENG Song，ZHANG Jiantang，ZHU Zhanwang. Overview of energy internet data intrusion tolerance assessment technology under cyber attack[J]. Electric Power Information and Communication Technology，2021，19(1)：11-19.

[5] 李满礼，倪明，颜云松，等. 面向恶意攻击的安全稳定控制系统信息物理协调防御方法[J]. 电力系统自动化，2021，45(18)：113-121.
LI Manli，NI Ming，YAN Yunsong，et al. Cyber-physical coordinated defense method against malicious attacks for security and stability control system[J]. Automation of Electric Power Systems，2021，45(18)：113-121.

[6] 罗剑波，董希建，崔晓丹，等. 关于大型安全稳定控制系统可靠性研究的探讨[J]. 电力系统保护与控制，2018，46(8)：65-72.
LUO Jianbo，DONG Xijian，CUI Xiaodan，et al. Discussion on reliability of large scale security and stability control system[J]. Power System Protection and Control，2018，46(8)：65-72.

[7] ZHAO L L，LI X M，NI M，et al. Review and prospect of hidden failure：protection system and security and stability control system[J]. Journal of Modern Power Systems and Clean Energy，2019，7(6)：1735-1743.

[8] 彭云豪，董希建，周海强，等. 电网安全稳定控制系统可靠性评估[J]. 电力系统保护与控制，2020，48(13)：123-131.
PENG Yunhao，DONG Xijian，ZHOU Haiqiang，et al. Reliability evaluation of power grid security and stability control system[J]. Power System Protection and Control，2020，48(13)：123-131.

[9] 汤奕，王琦，倪明，等. 电力信息物理融合系统中的网络攻击分析[J]. 电力系统自动化，2016，40(6)：148-151.
TANG Yi，WANG Qi，NI Ming，et al. Analysis of cyber attacks in cyber physical power system[J]. Automation of Electric Power Systems，2016，40(6)：148-151.

[10] 徐飞阳，薛安成，常乃超，等. 电力系统自动发电控制网络攻击与防御研究现状与展望[J]. 电力系统自动化，2021，45(3)：3-14.
XU Feiyang，XUE Ancheng，CHANG Naichao，et al. Research status and prospect of cyber attack and defense on automatic generation control in power system[J]. Automation of Electric Power Systems，2021，45(3)：3-14.

[11] DENG R L，ZHUANG P，LIANG H. CCPA：coordinated cyber-physical attacks and countermeasures in smart grid[J]. IEEE Transactions on Smart Grid，2017，8(5)：2420-2430.

[12] 王宇飞，高昆仑，赵婷，等. 基于改进攻击图的电力信息物理系统跨空间连锁故障危害评估[J]. 中国电机工程学报，2016，36(6)：1490-1499.
WANG Yufei，GAO Kunlun，ZHAO Ting，et al. Assessing the harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph[J]. Proceedings of the CSEE，2016，36(6)：1490-1499.

[13] VELLAITHURAI C，SRIVASTAVA A，ZONOUZ S，et al. CPIndex：cyber-physical vulnerability assessment for power-grid infrastructures[J]. IEEE Transactions on Smart Grid，2015，6(2)：566-575.

[14] LAW Y W，ALPCAN T，PALANISWAMI M. Security games for risk minimization in automatic generation control[J]. IEEE Transactions on Power Systems，2015，30(1)：223-232.

[15] WANG H，CHEN Z F，ZHAO J P，et al. A vulnerability assessment method in industrial Internet of Things based on attack graph and maximum flow[J]. IEEE Access，2018，6：8599-8609.

[16] 陈德成，付蓉，宋少群，等. 基于攻击图的电网信息物理融合系统风险定量评估[J]. 电测与仪表，2020，57(2)：62-68.
CHEN Decheng，FU Rong，SONG Shaoqun，et al. Quantitative risk assessment for cyber physical power system based on attack graph[J]. Electrical Measurement & Instrumentation，2020，57(2)：62-68.

[17] 伍志韬，杜伟，刘蕾蕾，等. 恶意攻击下的电力耦合网络风险传播模型研究[J]. 电网技术，2020，44(6)：2045-2052.

WU Zhitao, DU Wei, LIU Leilei, et al. Risk propagation model of power coupled networks under malicious attack[J]. Power System Technology, 2020, 44(6): 2045-2052.

[18] 孙卓,刘东,肖安洪,等. 基于攻击树模型的数字化控制系统信息安全分析[J]. 上海交通大学学报,2019,53(S1):68-73.
SUN Zhuo, LIU Dong, XIAO Anhong, et al. Information security analysis of digital control system based on attack tree model [J]. Journal of Shanghai Jiao Tong University, 2019, 53(S1): 68-73.

[19] 乐成利,高秀峰. 基于 Perti 网的移动 Ad Hoc 网络改进攻击网建模方法研究[J]. 兵器装备工程学报,2020,41(4):148-155.
LE Chengli, GAO Xiufeng. Research on improved attack net modeling method based on Perti network for mobile Ad Hoc network [J]. Journal of Ordnance Equipment Engineering, 2020, 41(4): 148-155.

[20] 张晶晶,许修乐,丁明,等. 基于模糊层次分析法的变压器状态评估[J]. 电力系统保护与控制,2017,45(3):75-81.
ZHANG Jingjing, XU Xiule, DING Ming, et al. A condition assessment method of power transformers based on fuzzy analytic hierarchy process[J]. Power System Protection and Control, 2017, 45(3): 75-81.

[21] 薛禹胜,李满礼,罗剑波,等. 基于关联特性矩阵的电网信息物理系统耦合建模方法[J]. 电力系统自动化,2018,42(2):11-19.
XUE Yusheng, LI Manli, LUO Jianbo, et al. Modeling method for coupling relations in cyber physical power systems based on correlation characteristic matrix [J]. Automation of Electric Power Systems, 2018, 42(2): 11-19.

作者简介:


钱胜

钱胜(1996),男,硕士在读,研究方向为电力系统稳定分析与控制(E-mail:220192835@seu.edu.cn);

王琦(1989),男,博士,副教授,研究方向为电力系统稳定分析与控制、电网信息物理系统等;

颜云松(1981),男,硕士,高级工程师,从事电力系统稳定分析与控制工作。

Risk assessment method of security and stability control system considering the impact of cyber attacks

QIAN Sheng[1], WANG Qi[1], YAN Yunsong[2], FENG Ke[2], XIA Haifeng[2]

(1. School of Electrical Engineering, Southeast University, Nanjing 210096, China;
2. NARI Group (State Grid Electric Power Research Institute) Co., Ltd., Nanjing 211106, China)

Abstract: The security and stability control system is an important defense line to ensure the reliable operation of the power grid. Serious physical consequences can be caused by cyber attacks against the security and stability control system. In order to quantitatively evaluate the impact of cyber attacks on security and stability control system and solve the problem that the existing risk assessment methods do not fully consider the susceptibility of cyber attacks, a risk assessment method of security and stability control system considering the impact of cyber attacks is proposed. Firstly, the hierarchical structure of the security and stability control system is analyzed. Then, the risk points of cyber attacks on the stability control device body and device's interstation communication from the three perspectives of attack object, attack methods, and attack consequences are analyzed. Secondly, the susceptibility of cyber attacks is quantified based on the fuzzy analytic hierarchy process, and a successful probability model of cyber attacks for security and stability control system is established combined with the defense unit model of cyber attacks built by Petri nets. Finally, the risk assessment is carried out on the standard and actual systems combined with the physical consequences and the probability of successful attacks. The risk values under two conditions of normal operation and cyber attack are calculated to verify the validity of the proposed model.

Keywords: security and stability control system; cyber attacks; susceptibility; fuzzy analytic hierarchy process; Petri net; risk assessment

(编辑 陆海霞)