



基于电力应用的 PTN 安全综合评价

高丽丹¹, 孙凤杰¹, 刘国军², 李建岐²

(1. 华北电力大学, 北京 102206; 2. 全球能源互联网研究院, 北京 102209)

摘要:传统的基于 SDH 的多业务传送网对数据业务突发性和灵活性的适应性越来越低, PTN 技术弥补了原有 SDH 网络的不足, 是 SDH 网络的良好补充。针对 PTN 设备的安全性能要求, 通过参考相关标准规范, 研究多指标综合评价技术与理论, 提出电力 PTN 安全性能测试关键评价指标。最后, 采用层次分析和模糊评价的安全性能评价体系对 3 款 PTN 设备的安全性能进行了评判, 验证了评价体系的可行性。

关键词: PTN; 安全性能; 关键指标; 评价

中图分类号: TN915.08

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2015381

Power PTN security comprehensive evaluation based on power application

GAO Lidan¹, SUN Fengjie¹, LIU Guojun², LI Jianqi²

1. North China Electric Power University, Beijing 102206, China

2. Global Energy Interconnection Research Institute, Beijing 102209, China

Abstract: Traditional multi service transport network based on SDH has a low adaptability to the data service and flexibility. PTN technology which makes up the deficiency of the original SDH network is a good supplement to SDH network. According to the requirements of security performance in PTN equipment, the technology and theory of multi index comprehensive evaluation was studied by referring to the relevant standards, the key evaluation index of power PTN security performance test was put forward. Finally, the security performance of the three models was evaluated by using the analytic hierarchy process and fuzzy evaluation system, and the feasibility of the evaluation system was verified.

Key words: PTN, security performance, key index, evaluation

1 引言

随着智能电网、物联网、云计算等新技术在电网的大力推广与应用, 电网业务逐步呈现出 IP 化、宽带化等特点, 传统的基于 SDH 的多业务传送网对数据业务突发性和灵活性的适应性越来越低, 而传统的面向非连接的 IP

网络难以严格保证重要业务的运行质量和安全性要求, PTN 技术对于 IP 大颗粒业务的传输弥补了原有 SDH 网络的不足, 是 SDH 网络的良好补充, 也在国家电网进行了小范围的试点与应用。

目前已建立与应用的 PTN, 主要用来同时承载电网调度生产业务和管理信息化业务, 用于满足电网业务接入灵

收稿日期: 2015-09-25; 修回日期: 2015-11-17

基金项目: 国家电网公司科技项目“电力分组传输网安全及 IPv6 可信通信网络研究”(No.SGRIXTKJ[2015]406)

Foundation Item: The Science and Technology Project of State Grid Corporation of China “Research on Security of Power Packet Transport Network and IPv6 Trusted Communication Network”(No.SGRIXTKJ[2015]406)

活性、多样性和经济性需求,但存在安全性问题。电力系统 SDH/MSTP 网络综合承载各安全分区业务,能通过不同纤芯、波长和时隙进行物理隔离,而软隔离效果、抗网络安全攻击能力、传送/控制/管理平面通信安全性等问题还需要进一步研究,尚未形成电力行业的分组传送网相关规范。

因此,PTN 在电网作为业务承载的网络尚不成熟,对于 PTN 设备的各种性能指标要求和功能要求(如时延、同步、业务数、L3 功能、网管功能、可靠性功能等)也没有明确的认识,在 PTN 试运行阶段存在网络组织经验缺乏、业务组织经验不足以及业务承载安全性等一系列问题。因此,需要建立一套完整的 PTN 安全评价指标体系,通过安全性测试与评价来验证 PTN 技术在电力通信网中大规模运用的可靠性和适用性。

目前在 PTN 安全性能评价方面的研究如下所示。

- 参考文献[1]针对 PTN 技术构建的智能配电通信网隔离度的大小,提出了一种数学评估模型来评估智能配电通信网的隔离效果。所提方法在估计隔离度方面具有良好的可行性和有效性,为评估网络隔离提供了一种可量化的方法。
- 参考文献[2]针对现有网络运行质量评估方法不能同时反映指标重要性和决策者偏好性的问题,提出了采用 WOMA 算子的网络运行质量模糊综合评估方法,该方法能够得出正确的评估结果。
- 参考文献[3]介绍了衡量通信网络可靠性的相关指标及目前配电通信网络的可靠性评估现状,鉴于目前评估方法尚存在不足之处,提出选用灰色关联分析法来分析配电通信网可靠性。该评估方法是通过定量分析两个因素之间的相互关联程度,避开了主观因素对评估结果的影响。

2 PTN 安全综合评价指标体系构建

基于电力应用的 PTN 安全综合评价指标体系采用自上而下的分析法进行构建,建立具有 3 层结构的指标体系框架:一级指标是 PTN 安全性综合评价总体目标的分解或分类;二级指标是实现一级指标目标的关键因素;三级指标是实现二级指标关键因素的基础指标。针对一级指标,从 PTN 系统组成部分来看,包括设备、网络、业务、(网管)系统等,为保证基于电力应用的 PTN 安全评价的全面性,一级指标设置设备安全、网络安全、业务安全、网管安全和系统安全共 5 个指标。

在一级指标确定的基础上,设备安全方面重点考虑设备

保护能力、设备抗攻击能力和设备电磁兼容抗扰度能力 3 方面的影响因素,原因一方面是电力生产控制业务对设备可靠性要求较高;另一方面是 PTN 设备通常部署于电磁环境恶劣的变电站中,对设备电磁抗扰度要求较高。网络安全主要从网络生存性、OAM 安全和 DCN 安全 3 方面考虑,保障基于电力应用的 PTN 运行的可靠性。业务安全重点考虑隔离能力、业务性能、关键电网业务承载能力等影响因素,主要考虑到 PTN 技术需要考虑不同分区业务的共同承载安全问题以及电网控制业务对 TDM 业务的时延与误码要求很高,如用于继电保护的通信通道单向时延应不大于 10 ms,用于线路纵差保护的光纤通道应确保双向路由一致;网管安全主要考虑网管系统的用户鉴权、账号与口令、数据库备份等安全功能要求;系统安全主要从端口漏洞、系统后门、系统完整性 3 方面来体现。指标体系中涉及的具体三级指标见表 1。

3 PTN 安全综合评价方法

在构建基于电力应用的 PTN 安全综合评价指标体系的基础上,结合定性评价与定量评价,本文采用层次分析法+模糊综合评价法对应用于电力的各厂商 PTN 设备的安全性进行了评价。其中层次分析法确定指标体系中各层级指标的相对权重^[4],用模糊综合评价法建立模糊评判数学模型,对各指标进行评价,最终得到评价结果。

3.1 层次分析法计算各层指标权重

层次分析法主要流程与思路如下。

(1)采用比例九标度评分标准,通过两两比较,得到电力 PTN 安全性能评价指标体系每一层的判断矩阵。计算矩阵 A 的最大特征值 $\lambda_{\max}$ 及特征向量 W ,可采用递归或方根法求解。

(2)对特征向量 W 进行归一化,得到每个成对判断矩阵的权向量 $\bar{W}$ 。

(3)对判断矩阵进行一致性检验, $R.I.$ 为同阶次的平均随机一致性指标, $C.R.$ 为一致性比率, $C.I.$ 为判断矩阵一致性指标,通常 $C.R.<0.1$,说明判断矩阵的一致性是可以接受的。

其中 $\lambda_{\max} = \sum_{i=1}^n \frac{(AW)_i}{nW_i}$, $C.I. = \frac{\lambda_{\max} - n}{n-1}$, $C.R. = \frac{C.I.}{R.I.}$ 。

(4)用同样的方法可以计算出下一层各指标相对于上层的权重值,计算最低层指标综合权重值 w 。例如一级指标 a_1 、二级指标 b_1 、三级指标 c_1 权重值分别为 w_1 、 w_2 、 w_3 ,综合权重值 $w = w_1 \times w_2 \times w_3$ 。

3.2 模糊评判数学模型

模糊综合评价法根据模糊数学的隶属度理论把定性



表 1 基于电力应用的 PTN 安全综合评价指标体系

一级指标	二级指标	三级指标
业务安全	隔离能力	PW 隔离测试
		隧道标签隔离测试
		设备端口隔离测试
		以太网业务隔离测试
	业务性能	TDM 双向时延测试
		TDM 业务双向时延差测试
		TDM 和以太网业务混合承载的长期误码/分组丢失性能
		双向时延差对线路纵差保护业务的影响
	关键电网业务承载能力	网络负载对线路纵差保护的影响
		网络保护倒换对线路纵差保护的影响
		PTN 设备电源保护测试
		PTN 设备主控板保护测试
设备安全	设备保护能力	PTN 设备交换板保护测试
		ARP 防欺骗
		防 ARP 泛洪攻击
		防 IGMP 泛洪攻击能力
	设备抗攻击能力	防 IGMP 畸形报文攻击能力
		静电放电抗扰度
		电快速瞬变脉冲群抗扰度
		浪涌(冲击)抗扰度
	设备电磁兼容抗扰度能力	电压瞬降和短时中断抗扰度
		PTN 内的 1:1 LSP /PW 线性保护功能测试
		PTN 内的 Wrapping 环网保护功能测试
		SDH 和 PDH 接入链路 OAM 功能测试
网络安全	网络生存性	以太网接入链路 OAM 功能测试
		通信数据安全性
		DCN 的路由协议安全认证
		DCN 的安全
	OAM 安全	按权限增加不同用户
		账号锁定和解锁
		口令复杂度能力测试
		新旧口令不相同,口令有效期
网管安全	用户鉴权	日志备份
		配置数据备份
		业务数据备份
		网管脱管对业务运行影响
	账号与口令	网管脱管对业务运行影响
		管理端口漏洞扫描
		业务端口进行主机软件漏洞扫描
		管理端口操作系统后门排查
系统安全	数据库备份	业务端口操作系统后门排查
		软件包(含补丁包及发布文档)业界主流软件扫描
		验证设备是否具有完整性校验机制

评价转化为定量评价,对受到多种因素制约的事物或者对象做出一个总体的评价。在 PTN 安全性评价指标体系中,许多定性指标的标值概念与确定性定量指标不同,不能用单一数值来描述。需要根据评价等级集确定的指标向量对具体的指标赋值。指标向量中每一元素为该指标的隶属度,由指标向量构成的矩阵称为模糊关系矩阵。

模糊排序综合评价过程大致包括以下几个环节。

- 根据综合评价目标要求,确定综合评价指标体系。按模

糊数学的提法,指标体系构成了模糊评判的因素论域,通常记为 U 。若有 p 个指标,则 $U=\{U_1, U_2, U_3, \dots, U_p\}$ 。

- 根据对评价对象价值水平的概念判断,将评价对象的价值水平划分为若干个等级,如“安全性能很强”、“安全性能较强”、“安全性能一般”、“安全性能较弱”、“安全性能很弱”5个等级。按照模糊数学的提法,此类等级称为“评价等级论域”,通常记为 V 。设有 M 个评语等级,则 $V=\{V_1, V_2, V_3, \dots, V_M\}$ 。

表 2 基于电力应用的 PTN 安全性综合评价结果

一级指标 (权重值)	二级指标(权重值)	三级指标(权重值)	综合权重	PTN 设备 A 评分	PTN 设备 B 评分	PTN 设备 C 评分
业务安全 (0.216 4)	隔离能力 (0.637)	PW 隔离测试(0.3)	0.041 4	90	90	90
		隧道标签隔离测试(0.3)	0.041 4	90	90	90
		设备端口隔离测试(0.3)	0.041 4	90	90	90
		以太网业务隔离测试(0.1)	0.013 8	90	90	90
	业务性能 (0.258 3)	TDM 双向时延测试(0.428 6)	0.024 0	80	80	60
		TDM 业务双向时延差测试(0.142 9)	0.008 0	0	60	90
		TDM 和以太网业务混合承载的长期误码/分组丢失性能测试(0.428 6)	0.024 0	90	90	90
	关键电网业务承载能力(0.104 7)	双向时延差对线路纵差保护业务的影响(0.714 3)	0.016 2	0	60	90
		网络负载对线路纵差保护的影响(0.142 9)	0.003 2	60	70	70
		网络保护倒换对线路纵差保护的影响(0.142 9)	0.003 2	0	60	90
设备安全 (0.2164)	设备保护能力(0.428 6)	PTN 设备电源保护测试(0.428 6)	0.039 8	90	90	90
		PTN 设备主控板保护测试(0.428 6)	0.039 8	90	90	90
		PTN 设备交换板保护测试(0.142 9)	0.013 3	90	90	90
	设备抗攻击能力(0.142 9)	ARP 防欺骗(0.25)	0.007 7	90	90	90
		防 ARP 泛洪攻击(0.25)	0.007 7	90	90	90
		防 IGMP 泛洪攻击能力(0.25)	0.007 7	90	90	90
		防 IGMP 畸形报文攻击能力(0.25)	0.007 7	90	90	90
	设备电磁兼容抗扰度能力(0.428 6)	静电放电抗扰度(0.25)	0.023 2	90	90	90
		电快速瞬变脉冲群抗扰度(0.25)	0.023 2	0	60	90
		浪涌(冲击)抗扰度(0.25)	0.023 2	0	70	70
		电压瞬降和短时中断抗扰度(0.25)	0.023 2	60	70	70
网络安全 (0.418 3)	网络生存性 (0.428 6)	PTN 网络内的 1:1 LSP/PW 线性保护功能测试(0.833 3)	0.149 4	90	90	90
		PTN 网络内的 Wrapping 环网保护功能测试(0.166 7)	0.029 9	0	90	60
	OAM 安全 (0.428 6)	SDH 和 PDH 接入链路 OAM 功能测试(0.75)	0.134 5	90	90	90
		以太网接入链路 OAM 功能测试(0.25)	0.044 8	90	90	90
	DCN 安全 (0.142 9)	通信数据安全性(0.5)	0.029 9	90	90	90
		DCN 的路由协议安全认证(0.5)	0.029 9	0	60	90
网管安全 (0.101 1)	用户鉴权 (0.166 7)	按权限增加不同用户(0.5)	0.008 4	90	90	90
		账号锁定和解锁(0.5)	0.008 4	90	90	90
	账号与口令 (0.166 7)	口令复杂度能力测试(0.5)	0.008 4	90	90	90
		新旧口令不相同、口令有效期(0.5)	0.008 4	90	90	90
	数据库备份 (0.166 7)	日志备份(0.333 3)	0.005 6	90	90	90
		配置数据备份(0.333 3)	0.005 6	90	90	90
		业务数据备份(0.333 3)	0.005 6	90	90	90
	网管脱管影响(0.5)	网管脱管对业务运行影响(1)	0.050 6	90	90	90
系统安全 (0.047 9)	端口漏洞 (0.323)	管理端口漏洞扫描(0.5)	0.007 7	90	90	90
		业务端口进行主机软件漏洞扫描(0.5)	0.007 7	90	90	90
	系统后门 (0.566 6)	管理端口操作系统后门排查(0.5)	0.013 6	90	90	90
		业务端口操作系统后门排查(0.5)	0.013 6	90	90	90
	系统完整性 校验(0.110 4)	软件包(含补丁包及发布文档)业界主流软件扫描(0.5)	0.002 6	90	90	90
		验证设备是否具有完整性校验机制(0.5)	0.002 6	90	90	90



- 确定每一指标的重要性权数,记为 W ,即 $W=\{w_1, w_2, w_3, \dots, w_p\}$ 。
- 建立模糊关系矩阵 $R=(r_{ij})_{p \times m}$, r_{ij} 表明被评价单位第 i 项指标隶属于第 j 级的程度。
- 计算模糊合成值 $B, B=W \odot R$ 写成矩阵形式,即:

$$B=(b_1 \ b_2 \ \dots \ b_m)=(w_1 \ w_2 \ \dots \ w_m) \odot \begin{bmatrix} r_{11} & \dots & r_{1m} \\ \vdots & \ddots & \vdots \\ a_{p1} & \dots & a_{pm} \end{bmatrix} \quad (1)$$

其中, $\odot$ 称为模糊算子,这里采用普通乘与加运算 $(\cdot, +)$ 。

最后得到的结果是被评价对象在全部因素(整个指标体系)上隶属于各个评语等级的总程度。

4 实例计算与结果分析

目前,PTN 技术在电网方面通常应用于电力四级骨干通信网或县域通信网,分为核心层、汇聚层和接入层。这里选取应用于汇聚层的 3 种不同 PTN 设备进行安全性综合评价。首先,在 PTN 安全综合评价指标体系的基础上(见表 1),采用层次分析法计算各层指标权重值,求出最低层指标综合权重值 W 。其次,依据参考文献[5]的相关测试方法,对 PTN 安全综合评价指标体系的 3 级指标测试项开展测试工作,根据测试结果得到评语等级,建立模糊关系矩阵 R 。例如,电力线路纵差保护业务对 E1 业务双向时延差要求很高,如果双向时延差大于 1 ms,会影响继电保护动作的准确性。可定义当双向时延差小于 0.5 ms,该项指标评语值为 90;大于 1 ms 时,评语值为 0。计算的最低层指标综合权重值与三级指标测试评语值见表 2。最后,通过式(1)求得模糊评价值 $B=W \times R=(76.96, 86.37, 87.41)$ 。由此可知,PTN 设备 B 与设备 C 安全性综合评价价值较高,PTN 设备 A 的安全性综合评价价值较低,其原因主要体现在双向时延差不满足要求,对继保业务影响加大,电磁抗扰度不满足变电站电磁环境要求。

5 结束语

本文提出的 PTN 安全综合评价指标体系及综合评价方法结合了定性定量评价优势,对电力应用的 PTN 通信系统进行安全性综合评价。PTN 安全综合评价指标体系综合考虑了 PTN 多电网业务承载隔离性、电网关键业务承载可行性、网络生存性、设备可靠性、网管安全性等关键因素。采用模糊综合评价法克服评价过程中主观因素影响过大的问题。实例分析表明,本文提出的 PTN 安全综合评

价指标体系及综合评价方法,一方面可从整体性评价各厂商、各型号 PTN 设备安全性;另一方面可从关键指标模糊评价价值方面分析不安全因素。

参考文献:

- [1] 薛金,余江,常俊,等.基于 PTN 技术的配电通信网隔离度评估研究[J].电力系统保护与控制,2013(16): 60-65.
XUE J, YU J, CHANG J, et al. Isolation evaluation research of power system protection and control of distribution communication network based on PTN technology [J]. Power System Protection and Control, 2013(16): 60-65.
- [2] 夏靖波,罗赞骞. IP 网络运行质量模糊综合评估方法研究[J]. 电子科技大学学报, 2011, 40(2): 267-272.
XIA J B, LUO Y Q. IP network operation quality fuzzy synthetic assessment method [J]. Journal of University of Electronic Science and Technology, 2011, 40(2): 267-272.
- [3] 黄留燕. 基于 PTN 配电通信网的实时性与可靠性研究[D]. 昆明: 云南大学, 2012.
HUANG L Y. The communication of PTN distribution network in real time and reliability[D]. Kunming: Yunnan University, 2012.
- [4] 余明辉,郭锡泉. 网络安全综合评价的 AHP 可拓分析方法[J]. 电信科学, 2010, 26(12): 110-114.
YU M H, GUO X Q. AHP extension comprehensive evaluation for network security [J]. Telecommunications Science, 2010, 26(12): 110-114.
- [5] 分组传送网(PTN)设备测试方法[EB/OL]. [2013-05-15]. http://www.nova.net.cn/news_detail.aspx-i d=372.htm.
Packet transport network (PTN) equipment test methods[EB/OL]. [2013-05-15]. http://www.nova.net.cn/news_detail.aspx-i d=372.htm.

[作者简介]



高丽丹 (1992-), 女, 华北电力大学硕士生, 主要研究方向为电力通信网。

孙凤杰 (1961-), 男, 华北电力大学教授, 主要从事通信与信息系统及数字图像处理的教学与研究工作。

刘国军 (1983-), 男, 全球能源互联网研究院高级工程师, 主要从事电力通信安全、网络评估等研究工作。

李建岐 (1969-), 男, 全球能源互联网研究院教授级高级工程师, 主要从事电力通信网、电力线通信等研究工作。



基于 CBR 的电力事故应急辅助决策方法

门永生^{1,2}, 刘山葆³

(1. 北京科技大学土木与环境工程学院, 北京 100083;

2. 国网智能电网研究院, 北京 102209; 3. 广东省通信管理局, 广东 广州 510080)

摘要:应用案例推理方法生成电力事故应急决策与处置方案, 可以为电力事故应急决策者提供科学的辅助决策支持。通过对电力事故应急处置过程的分析, 给出电力事故案例总体情况、处置流程、实施效果 3 个方面的特征属性表示框架。应用相似度计算和归纳式检索两种方法进行相似案例检索, 提出通过专家打分确定模糊属性的隶属函数, 应用隶属函数计算模糊属性的相似度。探讨了案例修正与案例学习方法, 并给出了基于案例推理的电力事故应急辅助决策过程。

关键词:电力事故; 案例推理; 应急; 辅助决策

中图分类号: X921

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2015385

Power emergency assistant decision methods based on CBR

MEN Yongsheng^{1,2}, LIU Shanbao³

1. Civil and Environment Engineering School, University of Science & Technology Beijing, Beijing 100083, China

2. State Grid Smart Grid Research Institute, Beijing 102209, China

3. Guangdong Communication Management Bureau, Guangzhou 510080, China

Abstract: Application of case-based reasoning (CBR) to generate grid infrastructure accidents emergency disposal scheme, can provide auxiliary decision scientific method for emergency people. Through investigation and analysis of the electric accident case, conclude basic situation, disposal process, disposal effect in three aspects of the characteristic attributes presentation framework of power accidents. Search similar case in two methods by means of inductive retrieval and similarity calculation. The determination of membership function of fuzzy attributes by using expert scoring was put forward. Fuzzy attribute similarity by membership functions was calculated and the power accidents case-based reasoning emergency disposal of the auxiliary decision-making process were given.

Key words: power accident, case-based reasoning, emergency, assistant decision

1 引言

我国电力工业正处于高速发展时期, 各类自然灾害及电力系统突发事件频发, 对电网设施安全运行造成严重威胁^[1]。2009 年南方雨雪冰冻灾害、2013 年四川雅安

特大地震等都对变电站、输电线路等电网设施造成了灾难性打击, 给人民群众生活与社会稳定带来巨大影响^[2]。电力事故应急处置要求标准较高, 在紧急情况下利用科学的方法与智能化的手段辅助决策者进行科学决策, 成为当前电力安全与应急工作迫切希望得到解决的问题, 而基于案例