

基于电力系统的信息安全综合评价体系研究

徐 晖¹ 梁承东² 程俊春³

(海南电网公司 海口 570203)¹ (广东省南方信息安全等级保护服务中心 广州 510635)²

(中国南方电网公司 广州 510623)³

摘 要 为了解决目前电力系统中的综合信息安全程度次优化问题,以协同论机理为基础,结合电力系统信息化架构的特定环境,设计出一种信息安全综合评价体系结构。该结构联动了电力系统信息安全体系中的技术、管理、规范、监测、调控等5个变量因子,评价了变量因子之间的发展协同程度。通过分析可知,只有保证变量因子全面联动与协同发展,才能高效优化电力系统综合信息安全水平。

关键词 信息安全,协同论,评价体系,电力系统

中图分类号 TP309 **文献标识码** A

Comprehensive Evaluation Research of Information Security Based on Power System

XU Hui¹ LIANG Cheng-dong² CHENG Jun-chun³

(Hainan Power Grid Corp, Haikou 570203, China)¹

(Guangdong Southern Information Security Classified Protection Service Center, Guangzhou 510635, China)²

(China Southern Power Grid Corp, Guangzhou 510623, China)³

Abstract In order to effectively solve the suboptimal problems of comprehensive information security based on power system, this paper combined with the specific environmental of power system, and designed a comprehensive evaluation architecture of information security. This architecture links these variable factors that contain technology, management, strategy, system, monitor, and evaluates the develop synergistic degree of these variable factors. Analysis shows that only ensuring synergetic development of these variable factors can optimize the information security level of power system efficiently.

Keywords Information security, Synergetics, Evaluation architecture, Power system

电力系统作为国家最重要的基础建设项目工程系统之一,其信息安全问题一直备受关注。随着计算机网络攻防技术以及电力系统信息化规模的不断发展,其电力系统受到的安全威胁以及潜在不安全因素日益增多,如电力数据信息泄露、电力设备安全配置不均衡、员工安全意识单薄、信息安全管理不规范、技术手段缺乏、电力人才流失等。因此,如何提高电力系统中综合信息安全能力以及如何综合评价电力系统信息安全变得极其重要^[1]。

1 相关概述

对电力系统信息安全的研究主要从以下5方面入手:

(1)技术。电力系统信息安全问题的首要威胁就是攻防技术的创新与更新,其电力系统采用的信息安全技术具体包括以下几种类型:(a)物理层安全技术,如防电磁、防辐射等;(b)网络层安全技术,如防火墙、安全认证、数字加密、入侵检测、虚拟专用网(VPN)等;(c)应用层安全技术,如安全协议分析、中间件安全管理等。

(2)管理。从电力系统信息化架构出发,信息安全问题根本源头绝大多数出自于管理,其中人员因素是其重要的一环^[2-4]。所以,非常有必要加强内部管理,做出正确的、合理的

人员规划架构体系。该部分具体包括以下几种类型:(a)管理战略与政策的制定。对于电力系统而言,信息安全是一种战略与政策规划,是必须启动并实施的。与此同时,必须提前综合考虑其信息安全规划过程中的预算与收益问题。(b)塑造信息安全意识与文化体系。电力系统内部信息化部门岗位职责各异,信息安全应成为一种意识载体附着在每一个岗位中,积极培育一种信息安全文化氛围。(c)业务流程规范管理。有效疏通电力系统信息安全流程规范,从细节入手,环环相扣,避免业务流程方面的失误处理与操作。

(3)规范。随着电力系统对信息安全技术、管理等方面关注度的增强,电力系统信息安全规范性逐渐制度化^[3],其规范措施应具体包括以下几个类型:(a)标准规范化。以满足电力行业内部信息安全标准、国家 GB/Z 信息安全相关标准、ISO/IEC 国际信息安全相关标准等为原则,积极推进电力系统信息安全标准化进程。(b)认证规范化。电力行业信息安全从业者应具备一定的认证资格,如 ISC、CISA、ISO、CIW 以及 CISP 相关认证等,从人员认证方面整体提高信息安全水平,实现电力系统信息安全统一认证化。

(4)监测。电力系统信息安全事件的发生关乎数以亿计的企业与个体客户的用电需求,所以需要对其进行实时监测,

一般是引入第三方组织完成相关工作,具体包括:(a)行业信息安全动态监测;(b)电力系统内部信息安全监测;(c)政府内部文件监测以及信息安全法律知识、动态调查等^[5]。

(5)调控。信息安全调控机制一般作为电力系统的中轴核心,用于协调技术、管理、规范、监测等变量因子之间的均衡与优化^[6]。

综上所述,基于电力系统的信息安全研究具体均是从技术、管理、规范、监测、调控等单方面或多方面进行分析^[7],但保证电力系统综合信息安全需要技术、管理、规范、监测、调控等多层次、全面性的联动,才能使得电力系统信息安全能力达到次优化状态。由此,本文以协同论机理为基础,结合电力系统信息化架构的特定环境,设计出一种信息安全综合评价体系结构。该结构联动了电力系统信息安全体系中的技术、管理、调控、规范、监督等 5 个变量因子,评价了变量因子之间的发展协同程度。通过分析可知,只有保证变量因子全面联动与协同发展,才能高效优化电力系统综合信息安全水平。

2 电力系统信息安全综合评价

2.1 协同联动机制

协同论^[8]具体包括序参量与役使原理两种概念。序参量是明确系统变化进程的根本变量,从电力系统信息安全架构出发,其技术、管理、规范、监测、调研等 5 个方面就是协同论中的序参量,亦称变量因子。役使原理是指系统演化过程中,在接近临界点时,发展迅速的序参量由于变化太快,以致在对系统施加影响以前就消失或变化了,因此极少数变化相对缓慢的序参量成为支配和主宰系统演化的主要因素。可知,其役使原理如同“木桶效应”的翻版。因此,其技术、管理、规范、监测、调研均可能成为役使原理的核心元素^[8]。保障电力系统信息安全是需要各种序参量协同联动的,也就是说需要技术、管理、规范、监测、调研 5 个变量因子的互相协同、互相影响的结果。正如役使原理所述,变量因子中最短板的部分将决定电力系统信息安全的综合水平,如图 1 所示。

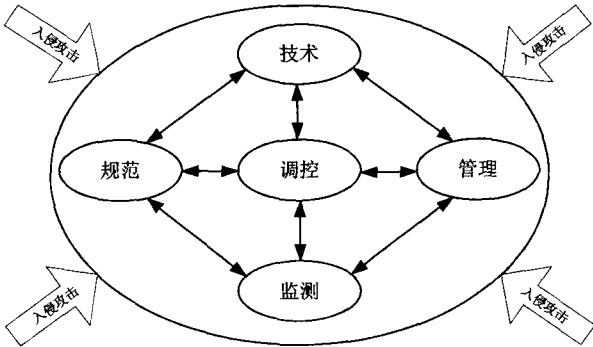


图 1 电力系统信息安全协同联动模型

2.2 指标体系构建

以上一节的信息安全协同联动机制为基础,能够构建电力系统信息安全技术、管理、规范、监测与调控等多种变量因子之间协同联动水准的评价指标与结构模型。

预定条件:电力系统信息安全统一化为一个系统,即 $S=\{S_1, S_2, S_3, S_4, S_5\}$ (其中 S_k 是影响电力系统信息安全的变量因子,具体包括技术、管理、规范、监测、调控; $k=1, 2, 3, 4, 5$),

序参量参数 $t_k=(t_{k1}, t_{k2}, \cdots, t_{kn})$, 其中 $k=(1, 2, 3, 4, 5)$, n 为大于等于 1 的正整数, $\beta_{ki} \leq t_{ki} \leq \alpha_{ki}, i \in [1, n]$ 。

由预定条件进行电力系统综合信息安全评价指标体系构建工作,如表 1 所列。

表 1 电力系统综合信息安全评价指标体系

系统 S	变量因子 S_k	序参量分子 t_{ki}
电力系统 信息安全	技术 S_1	物理层安全技术 t_{11}
		网络层安全技术 t_{12}
		应用层安全技术 t_{13}
	管理 S_2	管理战略与政策的制定 t_{21}
		塑造信息安全意识与文化体系 t_{22}
		业务流程规范管理 t_{23}
	规范 S_3	标准规范化 t_{31}
		认证规范化 t_{32}
	监测 S_4	行业信息安全动态监测 t_{41}
		系统内部信息安全监测 t_{42}
	调控 S_5	政府内部文件监测 t_{43}
		信息安全优化机制 t_{51}

2.3 综合评价体系结构

构建电力系统综合信息安全评价指标体系的目的是为了形成一种基于电力系统的统一信息安全有序模型,将其变量因子按照序参量分子顺序依次引入至综合评价体系结构中。本文在综合评价体系结构中添加了一种能够协调系统统一有序性的协同参数 Q ,从而有效地优化电力系统综合信息安全性能。

(1) 电力系统信息安全统一有序性结构

说明 1 对于变量因子 S_K ,序参量分子 t_{ki} 的信息安全统一有序性参数值(其中 $k=\{1, 2, 3, 4, 5\}$)表示如下:

$$Q_k(t_{ki})=\begin{cases} \frac{t_{ki}-\beta_{ki}}{\alpha_{ki}-\beta_{ki}}, & i \in [1, j] \\ \frac{\alpha_{ki}-t_{ki}}{\alpha_{ki}-\beta_{ki}}, & i \in [j+1, n] \end{cases}$$

其中,有序性参数 $Q_k(t_{ki})$ 与序参量分子 t_{ki} 对变量因子 S_k 的价值是成正比关系的。

说明 2 对于变量因子 S_K ,序参量 t_i 的信息安全统一有序性参数值(其中 $k=\{1, 2, 3, 4, 5\}$)表示如下:

$$Q_k(t_i)=\sqrt[n]{\prod_{i=1}^n Q_k(t_{ki})}$$

其中,有序性参数 $Q_k(t_i)$ 与序参量 t_i 对变量因子 S_k 的价值是成正比关系的。

说明 3 对于变量因子 S_K ,系统信息安全统一有序性参数值(其中 $k=\{1, 2, 3, 4, 5\}$)表示如下:

$$Q=\sqrt[n]{\prod_{i=1}^n Q_k(t_i)}$$

其中,有序性参数 Q 与系统综合信息安全水平是成正比关系的。

(2) 电力系统信息安全协同程度优化结构

电力系统信息安全协同程度优化结构兼顾了技术、管理、规范、监测、调控等变量因子的相互协同关系,从架构上说明了电力系统信息安全综合水准。预定在某一时间点 M_0 ,信息安全统一有序性参数值是 $Q_k^0(t_k)$,那么在某一时间点 M_1 ,若信息安全统一有序性参数值是 $Q_k^1(t_k)$,电力系统的整体有序性协同参数值是 Q^{M_1} ,则有如下所示:

说明 4 信息安全协同程度优化参数:

$$h=r \cdot Q^M_k \cdot \sqrt{\prod_{i=1}^5 [Q^i(t_i)-Q^p(t_i)]}$$

$$r=\frac{\min_i [Q^i(t_i)-Q^p(t_i)]}{|\min_i [Q^i(t_i)-Q^p(t_i)]|}$$

其中, $i=k$ 并且 $Q^i(t_i)-Q^p(t_i) \neq 0$, 有: (a) 优化参数 h 与其协同程度成正比关系; (b) 参数内部分子 r 明确了电力系统信息安全中 5 个变量因子的协同联动方向, $r=1$ 与 $r=-1$ 时分别说明了变量因子的完全同向与反向特征。 (c) 说明中统一分析了 5 个变量因子对电力系统信息安全的影响程度, 即技

术、管理、规范、监测以及调控的相关价值比。只要有单一变量因子出现短板, 其电力系统综合信息安全能力也会相应出现短板, 因此, 保证电力系统信息安全次优化协同状态, 必须保持各个变量因子之间协同程度满足要求。

3 实验分析

通过 Delphi 分析法对一般化电力系统信息安全中的技术、管理、规范、监测与调控 5 个变量因子进行协同实验, 如表 2 所列。

表 2 一般化电力系统信息安全指标数据列表

时间点	信息安全序参量分子											
	t ₁₁	t ₁₂	t ₁₃	t ₂₁	t ₂₂	t ₂₃	t ₃₁	t ₃₂	t ₄₁	t ₄₂	t ₄₃	t ₅₁
M ₀	2.32	2.63	4.77	3.16	4.29	5.22	5.13	3.86	5.11	4.18	6.02	4.32
M ₁	2.55	2.94	4.79	3.82	4.37	5.25	5.19	4.01	5.62	4.27	6.26	5.81
M ₂	3.41	3.72	5.13	3.91	5.11	5.83	6.37	4.47	5.81	4.36	6.31	5.94
M ₃	3.72	4.01	6.27	4.51	5.38	6.17	6.53	4.82	6.07	4.91	6.68	6.37
M ₄	3.98	4.37	6.83	4.72	5.39	6.39	6.93	5.06	6.42	5.38	6.91	6.81
M ₅	4.13	4.89	6.89	5.85	5.74	6.71	7.27	5.79	6.77	5.71	7.04	7.19
M ₆	5.68	5.78	7.22	6.72	6.04	7.09	7.42	6.03	7.24	5.95	7.46	7.47
M ₇	6.17	6.36	7.46	7.01	6.92	7.28	7.58	6.79	7.33	6.69	7.82	7.53

通过信息安全指标数据, 从说明 1、2 分别可计算出序参量分子 t_{ki} 以及序参量 t_i 的信息安全统一有序性参数值, 然后依据上述结果与说明 3 可知一般化电力系统从 M_0 到 M_7 时间段的信息安全统一有序性参数值。依次计算, 最后又可知一般化电力系统从 M_0 到 M_7 时间段的信息安全协同程度优化参数, 如图 2、图 3 所示。

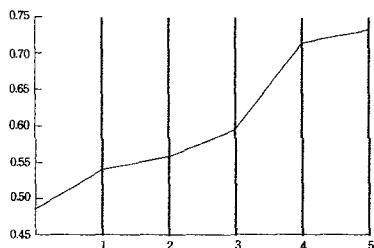


图 2 电力系统信息安全统一有序性协同参数趋势

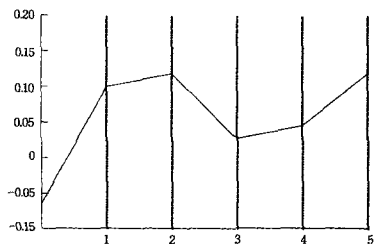


图 3 电力系统信息安全协同程度优化参数趋势

从图 2 中可知, 尽管一般化电力系统信息安全统一有序性参数逐渐提高, 但是其对应图 3 中的一般化电力系统信息安全协同程度优化参数却相应先下滑后上升, 其根本原因是变量因子中规范不完善, 出现一定短板, 尽管电力系统中其他 5 个变量因子都较为完善, 但是正如协同联动体系结构所述, 电力系统综合信息安全水平取决于最差变量因子。

结束语 针对目前电力系统中综合信息安全程度次优化

尚未得到完善解决等问题, 本文以协同论为基础, 结合电力系统信息化架构的特定环境, 首先设计出一种协同联动机制, 具体联动了电力系统信息安全体系中的技术、管理、规范、监测、调控等 5 个变量因子, 评价了变量因子之间的发展协同程度; 其次对其信息安全指标体系进行了构建; 最后详细分析了信息安全综合评价体系结构。通过分析可知, 只有保证变量因子全面联动与协同发展, 才能高效优化电力系统综合信息安全水平。下一步的研究重点就是将次优化的信息安全综合评价体系结构进行实际应用并拓展。

参 考 文 献

- [1] 李丈武, 游文霞, 王先培. 电力系统信息安全研究综述[J]. 电力系统保护与控制, 2011, 39(10): 140-147
- [2] Anderson E E, Choobineh J. Enterprise information security strategies [J]. Computers & Security, 2008, 27: 22-29
- [3] 罗嘉, 李连友. 基于协同学的金融监管协同度研究 [J]. 财贸经济, 2009, (8): 15-19
- [4] Colwill C. Human factors in information security: The insider threath Who can you trust these days ? [J]. Information Security Technical Report, 2009, 14: 186-196
- [5] 陶长琪, 陈文华, 林龙辉. 我国产业组织演变协同度的实证分析——以企业融合背景下的我国 IT 产业为例[J]. 管理世界, 2007 (12): 67-72
- [6] 彭端旭. 浅谈电力应急管理建设重点[J]. 东北电力大学学报, 2007(5): 11-12
- [7] 张鑫, 陈雪华, 刘新. 电力系统信息安全基线标准体系的构建 [J]. 电力信息与通信技术, 2013, 11(11): 110-114
- [8] Ashenden D. Information Security management: A human challenge [J]. Information Security Technical Report, 2008, 13: 195-201