CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

http: //d2.cigre.org
/

2017 Colloquium
September 20 to 22, 2017
Moscow – RUSSIA

PS2

基于大数据的网络安全态势感知及预警分析

Big Data Based Network Security Situation Awareness and Early Warning Analysis

刘建明 张波

Chinese Society for Electrical Engineering Information Special Committee/
Chinese National Committee of CIGRE
China
ljming@263.net，zhangbo@geiri.sgcc.com.cn

随着智能电网建设速度的越来越快，电网数字化和智能化程度越来越高，给电力系统网络与信息安全工作带来了新的机遇和挑战。

本文介绍了中国国家电网公司近年来基于大数据的网络安全管理，包括信息收集、数据采集、大数据分析、网络安全态势感知、预警分析和应急处置等工作。在数据采集上，开展了实时数据采集和历史数据的集中管理和存储。在数据分析上，建立了场景分析、统计分析、安全处理视图界面分析。在网络安全态势感知和预警分析上，利用大数据技术以及场景主题建模，进行多维展示，监测各下属单位的网络安全信息、安全威胁，进行预警分析。

通过以上举措，实现“可管可控、精准防护、可视可信、智能防御” 的策略。论文最后介绍了中国电力系统 2017-2020 年计划开展的电力信息安全工作。

State Grid Corporation of China is vigorously promoting the construction of a strong smart grid and the global energy Internet. The increasing digital and intelligent power grid has brought new opportunities and challenges to the network and information security work in the power system.

This paper introduces the Big-data-based network security protection management system of State Grid Corporation of China, including information collection, data collection, large data analysis, network security situation awareness, early warning analysis and emergency response. In the data collection, the system implements real-time data collection and historical data centralized management and storage. In the data analysis, the system constructs the scene analysis, statistical analysis and security management view interface analysis. In the network

situation awareness and early warning analysis, the system uses the big data technology and scene theme modeling for the multi-dimensional displaying, and to help the subordinate units monitoring the network information and security threats for making early warning analysis.

Through the above approaches, the system implements the strategy of controllability, manageability, precise protection, visual credibility and intelligent defense . Finally, the paper introduces the power information security work planned by China Power System 2017-2020.

Instructions to be deleted when sending the file:

The file name shall be as follows CC_PSn_AUTHOR.ext
Where *CC* is the ISO country code with 2 characters
***n* is the number of the Preferential Subject, i.e. 1, 2 or 3**
***AUTHOR* is the name of the author in capitals letters**
***ext* is the extension of the file (either pdf, doc or docx)**

The synopsis is to be submitted before the 2016-11-19