电力二次系统内网安全监视功能的研究与实现

陈茂源[1], 孙 炜[2], 梁 野[1], 李 勃[1], 谷丰强[1]
(1. 北京科东电力控制系统有限责任公司,北京 100192;2.国家电力调度控制中心,北京 100031)

摘 要:电力二次系统安全监视功能通过对安全防护设备的日志实现标准化采集,实现对安全设备的实时告警与运行状态监测,及时发现安全体系中存在的各类安全隐患和异常访问行为。通过研究日志采集技术,形成电力二次系统安全日志采集规范;通过研究上下级调度中心监视功能的级联通信,实现功能分级部署;通过研究调度主站 D5000 主机的安全状态,实现对 D5000 的安全监视。

关键词:内网监视; 网络安全; D5000; 关联分析
中图分类号:TM769 **文献标志码**:B **文章编号**:1009-0665(2014)03-0031-04

电力二次系统安全监视功能通过对二次安全防护设备的日志实现标准化采集,实现对安全设备的实时告警与运行状态监测,及时发现安全体系中存在的各类安全隐患和异常访问行为。电力二次系统安全监视功能实现安全防护设备的资产管理和对各类参数的动态管理,大幅减少系统管理员的工作量。同时与智能电网调度技术支持系统(简称 D5000)结合,实现内网安全事件的集中收集、统一管理,为基础平台提供有效的安全保障[1-3]。

1 内网安全监视功能的范围

内网安全监视功能通过收集安全日志,实现安全监视,监视范围包括电力专用安全防护设备、通用安全防护设备和调度技术支持系统内关键进程。

1.1 电力专用安全防护设备

此类设备包括横向隔离设备和纵向加密装置,将按照 Syslog 日志规范主动向内网安全监视功能发送其运行状态和告警数据。为便于日志收集分析,此类设备日志报文采用自定义电力二次系统标准 Syslog 日志格式:< 告警级别 >< 空格 > 告警时间 < 空格 > 设备名称 < 空格 > 设备类型 < 空格 > 内容描述。

1.2 通用安全防护设备

此类设备包括:防火墙、入侵检测装置、防病毒系统等, 采用 Syslog 与 Agent 相结合方式实现数据采集。由于此类设备涉及厂家众多,且其工作原理和实现技术差异较大,无法规定其采用统一的 Syslog 日志格式。因此,采用日志采集代理 Agent 的方式到达规范其日志格式的目标。在采集 Agent 程序中,输入内容为上述各类设备的原始 Syslog 日志,输出内容为电力二次系统定义的标准格式 Syslog 日志。

1.3 调度技术支持系统内关键进程

随着 D5000 的逐步完善和建设, 内网安全监视功能已纳入智能调度技术支持系统。根据《智能调度技术支持系统总体设计方案》的要求,D5000 的关键进程也将纳入监视范围。由于 D5000 运行环境相对固定,操作系统主要采用国产安全操作系统, 因此, 将采用 Agent 方式实现关键进程的数据采集功能。

2 内网安全监视关键功能的研究及实现

2.1 日志采集功能

安全监视功能主要使用 Syslog 方式采集安全设备的日志信息。电力系统专用安全设备(横向物理隔离装置、纵向加密认证装置)使用 Syslog 方式直接采集;通用安全设备(防火墙、入侵监测系统、防病毒系统)经 Agent 代理将日志转换为符合电力系统标准格式的日志后采集; 调度技术支持系统内部的关键设备和应用通过 Agent 代理将日志转换为标准格式发送至安全监视功能。

Syslog 采用用户数据报协议(UDP)作为其底层传输层机制。Syslog 的默认端口是 514 端口,端口可以根据实际情况重新配置。日志采集流程如 1 所示。

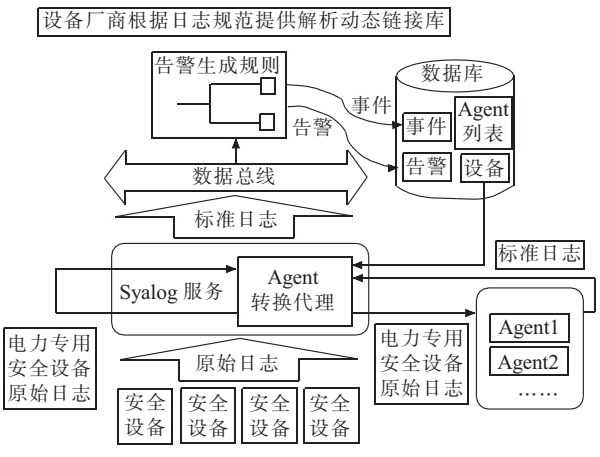

图 1 日志采集流程

2.1.1 广域网日志采集功能

广域网日志采集模块作为安全监视功能重要辅助

收稿日期:2013-12-10;修回日期:2014-01-27

模块,可以广泛地部署各级调度机构和变电站 ,负责采集电力专用安全设备(横向物理隔离装置、纵向加密认证装置)和通用安全设备(防火墙、防病毒系统、入侵检测系统)的运行日志和告警信息,并将处理后的信息发送至电力二次系统内网安全监视功能, 进行集中分析和展示。

广域网日志采集模块具有预处理功能, 包括事件接收、事件过滤、事件压缩、事件报送等功能。

(1) 事件接收。广域网日志采集模块使用 Syslog 方式接收事件内容,范围包括电力专用安全设备、通用安全设备。

(2) 事件过滤。广域网日志采集模块将接收到大量安全事件,但并非所有事件都需要关注,过滤功能将不重要的事件信息过滤掉。

(3) 事件压缩与归并。对重复事件进行压缩,所有重复事件只显示一次, 同时记录重复告警事件的第一次发生时间、最后一次发生时间和发生次数。

(4) 事件报送。广域网日志采集模块将事件处理后得到的重要事件信息报送至安全监视功能。

2.1.2 局域网日志采集功能

局域网安全监视模块负责监视主站 D5000 内部关键设备和应用,采集系统的运行状态和告警信息,并将处理后的告警信息发送至电力二次系统内网安全监视功能。局域网日志采集模块具有如下功能。

(1) 采集系统外接设备。采集主机的外接设备情况(USB 接口、串口、并口),根据安全监视代理的配置文件,当有不符合安全策略的外接设备接入时发出告警。

(2) 采集系统关键进程运行情况。采集系统内主要业务的关键进程的运行情况,当出现非法进程、进程异常或非法退出时发出告警。

(3) 日志发送。当系统内发生异常、非法操作、非法访问或外连时,以 Syslog 格式向监视功能发送告警信息。

2.2 运行状态阈值告警机制

内网监视功能对采集的运行状态数据进行阀值告警处理,主要的告警现象包括:

(1) 越界。规定数值的合理取值范围,当不在该范围,越界条件成立。如某主机的 CPU 负载率超过定义的最大值或动态阈值;硬盘使用率达到 100%,无可用空间等。

(2) 跳变。规定数值在给定时间间隔的变化幅度,如超出,跳变条件成立。如 oracle 数据库的某个表空间增长过快;交换机的流量异常增长等。

(3) 不刷新。规定一个时间间隔,如数值在该时间段结束时,未改变,不刷新条件成立。如 D5000 某个关键值长时间不变化等。

2.3 安全日志数据分析处理

2.3.1 事件标准化

按照管理需要对原始事件中包含的信息进行事件的重定义标准化,具体内容包括:将信息进行相关的修改定义,将事件的内容、描述信息、级别等进行修改,从而标准化事件信息,便于事件的处理。需要对事件的内容,如级别、故障类型、描述等进行标准化定义,如图 2 所示。

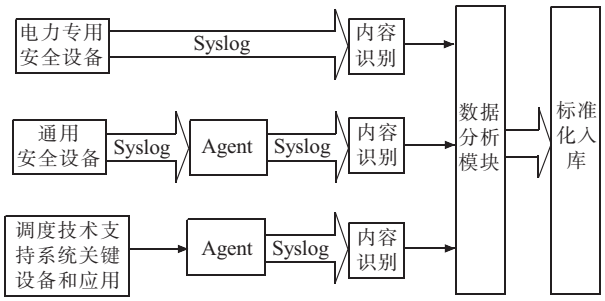

图 2 数据标准化处理流程

2.3.2 事件压缩与归并

对重复事件进行压缩, 所有重复事件只记录和显示一条, 同时提供告警事件的第一次发生的时间和最后一次发生的时间以及次数。

系统提供按照标准化事件的所有属性进行过滤归并策略设置。按照如下条件进行规则设定:监视对象、事件类型、紧急程度、发生时间、事件刷新的时间间隔。

2.3.3 事件过滤

在采集事件的同时,通过对模板的定义,可以对指定的事件进行过滤, 从而提高事件的处理效率和时效性;根据事件采集的规则,将不需要的事件在采集层直接过滤,可以减少管理服务器的处理事件量[4]。

2.3.4 风险管理

内网安全监视功能具有针对二次系统安全风险的评估指标体系,包括运行类和安全类两类指标。运行类指标体现防护体系中安全设备的总体运行状况, 安全类指标体现防护体系中的安全可靠程度。运行类指标包括:设备在线运行率、纵向加密的密通可用率等;安全指标是功能当前风险值。

针对电力二次系统安全防护设备告警日志的特点,采用基于层次式聚类的多特征关联算法,实现告警信息的分类和聚合功能,通过 IP 地址与资产信息的关联,快速定位告警信息来源,同时分析告警内容,按照属性相似度进行关联,有效精简了报警数量,解决了系统中安全事件描述信息过于冗余庞杂的问题。

2.4 监视功能级联管理

安全监视功能可以向上级单位报送高级别的安全事件、本级功能自身运行指标以及统计后的告警信息。上级安全监视功能通过设备统一编码识别安全事件的

来源。根据电力二次系统采用通信专网的特点,监视功能采用 syslog 报文及文件的方式实现功能的级联管理功能。具体系统架构如图 3。

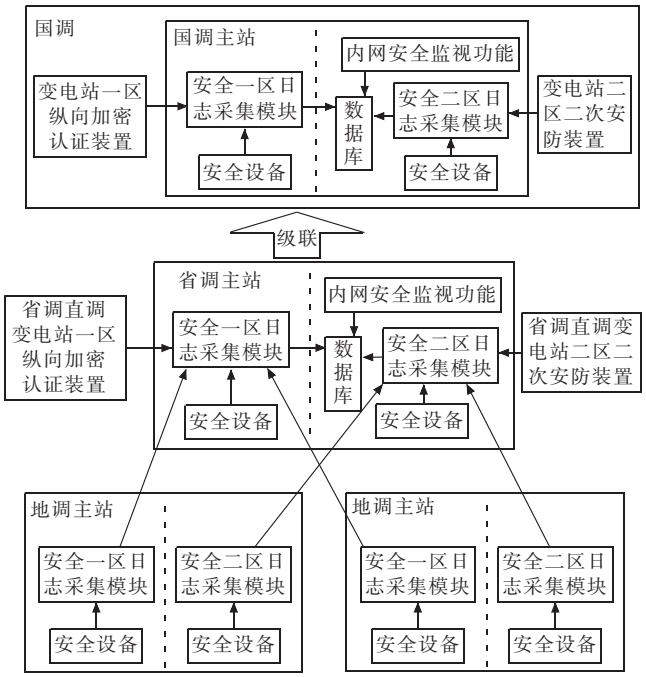

图 3 级联管理架构

2.4.1 高级别安全事件上报

高级别安全事件上报指下级监视功能向上级监视功能转发告警级别为紧急的安全事件。当本级功能发生告警级别为紧急的安全事件后，本级功能除记录该安全事件外，会将该条告警的告警级别降一级后以 syslog 的形式上报给上级功能，上级功能解析并存储该条告警,产生对应的告警事件。

2.4.2 本级功能自身运行指标上报

本级功能自身运行指标上报指每 5 min 以 syslog 形式上报一次运行状态。内容包括:安全指标数值、紧急告警数量、重要告警数量、次要告警数量、通告告警数量、功能数据流量(kb/s)以及按照设备类型分布的告警数量。

2.4.3 本级功能统计分析信息上报

本机功能统计分析信息上报指每天零点以 E 文件的形式向上级功能报送过去一天的运行状态。内容包括:本级功能的告警数量、安全设备统计信息、指定安全事件、安全设备在线运行率、纵向装置密通可用率、按照设备类型和设备厂商划分归并后的告警数量、未归并日志数量。

内网安全监视功能结合电力系统的五级调度机制,以及安全分区特点,实现了适合电力系统的内网安全监视功能级联通信功能。该功能为上级平台及时准确地了解下级功能运行状态提供支持，提供最及时的告警功能。最大限度降低紧急安全事件对全网的安全威胁，同时也为上级调度单位对下级调度单位的二次安全防护工作提供一个有效的考核方法。

3 内网安全监视功能研究成果

3.1 内网安全监视功能结构

内网安全监视功能的逻辑架构分为 3 层，由下至上依次为数据采集层、数据处理分析层、图形界面展现层三层,架构图如图 4 所示[5,6],各层功能说明如表 1 所示。

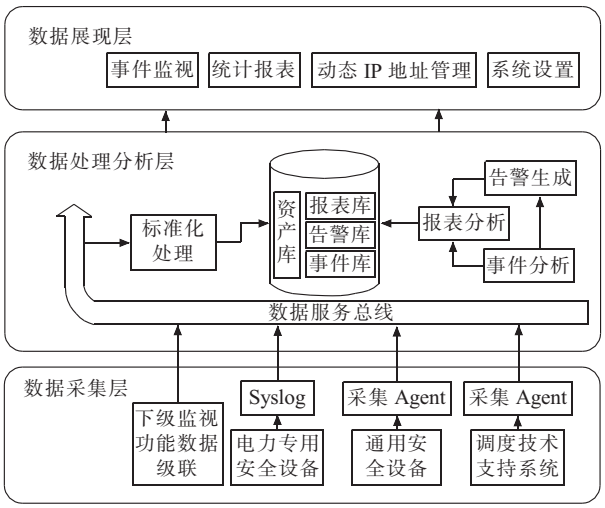

图 4 功能架构

表 1 监视功能结构表

技术结构	主要模块和功能
图形界面展现层	事件监视(事件检索、告警管理) 统计报表(Top10 统计,报表管理) IP 地址动态管理及资产管理 系统管理(系统参数、用户权限)
事件处理和分析层	标准化处理(压缩、归并、标准化入库) 数据存储(事件库、资产库、报表库) 统计分析(实现多种维度的统计分析) 事件告警
数据采集层	电力专用安全设备以 Syslog 方式直接采集 通用安全设备通过 Agent(接收器->转换代理(设备厂商实现)->发送器)转发收集 D5000 关键主机通过 Agent 方式收集

3.2 内网安全监视与 D5000 系统的有机结合

根据《智能调度技术支持系统总体设计》、《智能调度技术支持系统主机安全监视功能规范》要求,结合智能调度技术支持系统的特点,实现 D5000 安全监视功能。该功能充分利用了 D5000 系统的消息总线、服务总线、数据总线的应用机制,结合 D5000 系统人机界面的表格编辑器、饼图、棒图、实时曲线,使用画面浏览器、实时库数据、历史数据库进行内网安全监视功能的展示,如图 5 所示。

4 推广应用情况

该功能可完全应用在国家电网公司二次系统安全

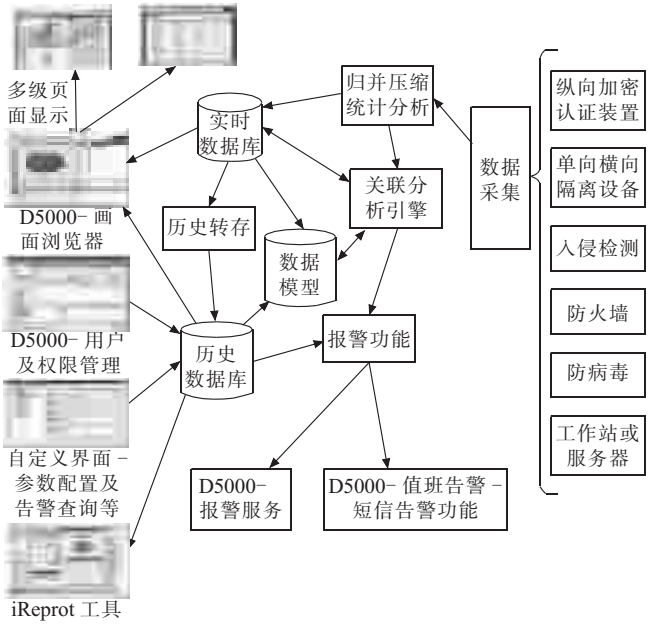

图 5 内网监视功能与 D5000 结合展示

防护体系的建设中，为构建智能电网环境中的智能主动安全防御体系奠定坚实的基础。同时，在电力二次系统安全防御体系基础上，通过对电力二次系统安全监视的研究、开发并实施电力二次系统内网安全监视功能，提高电力二次系统安全运行管理水平，健全完善电力二次系统安全防护体系，保障电力二次系统的安全稳定可靠运行。

电力二次系统内网安全监视功能已经在 2010 年完成江西和陕西试点的建设，并在各分中心、省调中逐步推广建设。2011 年完成国调中心、华北、华中分中心，河北、福建、江苏、重庆、安徽、四川省调等 9 个单位的建设工作，并在 2012 年底完成全公司其他省级及以上调度机构的建设工作。

5 结束语

通过日志数据采集技术、安全日志数据分析处理技术、数据关联分析技术，以及 D5000 安全监视技术的研究，解决了 D5000 对关键安全设备、服务器的日志集中采集和统一管理问题，实现对安全设备的实时告警与运行状态监测，及时发现安全体系中存在的各类安全隐患和异常访问行为。电力二次系统内网安全监视功能的建设有助于电力二次系统安全防护体系由边界防护向纵深防御发展，解决调度技术支持系统对关键安全设备、服务器的日志集中采集和统一管理问题，实现对电力专用设安全设备和通用安全设备在统一的功能下实现实时告警与运行状态监测，为 D5000 提供全面的安全基础支撑，对于及时掌握电力二次系统存在的安全隐患，保障电网安全稳定运行具有重要意义。由于功能收集了大量安全设备告警信息，存在海量信息问题，不能迅速从海量告警信息中发现二次系统安全事件，亟需告警信息二次分析；在日志过程中，一些告警并不合理，告警级别存在过高问题，需要根据紧急程度重新调整。

参考文献：

[1] 李 澄，陈 颢，宁 艳. 二次设备时间同步状态在线监测系统研究[J]. 江苏电机工程，2012，31(1)：9-11.
[2] 胡 炎，辛耀中，韩英铎. 二次系统安全体系结构化设计方法[J]. 电力系统自动化，2003，27(S21)：63-68.
[3] 陈建亚. 现代通信网监控与管理[M]. 北京：北京邮电大学出版社，2000：56.
[4] 彭雪娜，闻英友，赵 宏. 网络安全信息关联与分析技术的研究进展[J]. 计算机工程，2006，32(17)：1-3.
[5] 刘金龙. drools 规则引擎模式匹配效率优化研究及实现[D].成都：西南交通大学，2007.
[6] 金学成，孙 炜，梁 野，等. 电力二次系统内网安全监视平台的设计与实现[J]. 电力系统自动化，2011，35(16)：99-104.

作者简介：
陈茂源(1984)，男，山东枣庄人，工程师，从事电力二次系统安全防护工作；
孙 炜(1977)，男，北京人，高工，从事电力二次系统安全防护工作；
梁 野(1980)，男，辽宁沈阳人，北京人，高工，从事电力二次系统安全防护工作；
李 勃(1978)，男，辽宁盘锦人，工程师，从事电力二次系统安全防护工作；
谷丰强(1982)，男，河南郑州人，工程师，从事电力二次系统安全防护工作。

Research and Implementation of Power System Secondary Network Security Monitoring

CHEN Maoyuan[1], SUN Wei[2], LIANG Ye[1], LI Bo[1], GU Fengqiang[1]
(1. Beijing Kedong Electric Power Control System Co. Ltd., Beijing 100192, China;
2. National Electric Power Dispatching Control Center, Beijing 100031, China)

Abstract: Through standardize the sampling of data of safety equipment, power system secondary security monitoring can achieve real-time warning and operating status monitoring for the safety equipment, and detect the presence of various types of security system risks and abnormal access behavior. With the studying of log collection technology, a norm for power system secondary security log collection is formed. With the research of cascade communications between upper and lower dispatch monitor center, a hierarchical deployment of functions is achieved. Through studying the security state of D5000 host in dispatch center, the security monitoring on D5000 is achieved.

Key words: network security monitoring; network security; D5000; correlation analysis