



电力调度内网安全监控平台建设

袁 林,高夏生,赵田红

(国网安徽省电力公司电力调度控制中心 合肥 230022)

摘 要:电力调度内网部署大量安全防护设备,但缺乏集中监控、统计分析和统一管理手段。针对这一情况,介绍了某省电力调度内网安全监控平台的建设情况,该监控平台能够实时采集各安全防护设备的运行状态、告警和日志信息,经过标准化数据处理和分析计算,在统一监控平台上实现集中监控、综合告警、隐患提醒、统计分析、报表生成和辅助决策等功能。

关键词:电力调度;内网;安全防护;集中监控

doi: 10.3969/j.issn.1000-0801.2014.01.018

Construction of Security of Monitoring Platform in Electric Power Dispatching Internal Network

Yuan Lin, Gao Xiasheng, Zhao Tianhong

(Power Dispatching Control Center, State Grid Anhui Electric Power Company, Hefei 230022, China)

Abstract: Power dispatching internal network contains of a large amount of safety equipments, but lacks of centralized monitoring, statistical analyzing and unified managing tool. A platform for monitoring the security of electric power dispatching internal network was constructed. The platform acquires realtime security equipments operating status, alarms, and logs information, through standardized data processing, analysis and calculation, to achieve centralized monitoring, integrated alarm, hidden danger reminder, statistical analysis, report generation and decision functions.

Key words: power dispatch, internal network, security protection, centralized monitoring

1 引言

近年来,为保障电力调度内网安全运行,省调度中心(以下简称省调)及各地市调度中心(以下简称地调)、变电站陆续部署了大量安全防护设备和系统,包括横向隔离设备、纵向加密认证装置、防火墙、入侵检测系统(IDS)、防病毒系统等,二次系统安全防护水平大幅提升。但随着众多安全防护设备的投入运行,管理人员需要经常查看各个设备的日志文件,并从中发现安全隐患,工作十分繁重,且容易遗漏其中的某些重要信息。因此,如何更加有效地管理好、维护好这些设备,更全面、细致、科学地分析安全系统

的运行情况,是一个新的课题。

为解决上述问题,进一步做好电力二次系统的安全防护工作,省调在国网调度(以下简称国调)中心的支持下,积极开展电力调度内网安全监控平台的建设工作。监控平台的主要作用是,对安全防护设备的实时告警与运行状态进行监测,采取有效措施阻止恶意攻击行为;收集安全防护设备的运行日志并进行分析,指导技术人员解决问题和消除隐患;及时进行日、月、年数据汇总与统计分析,形成各种报表,为二次系统安全防护的优化、升级改造提供辅助决策。省调内网安全防护系统架构如图1所示。

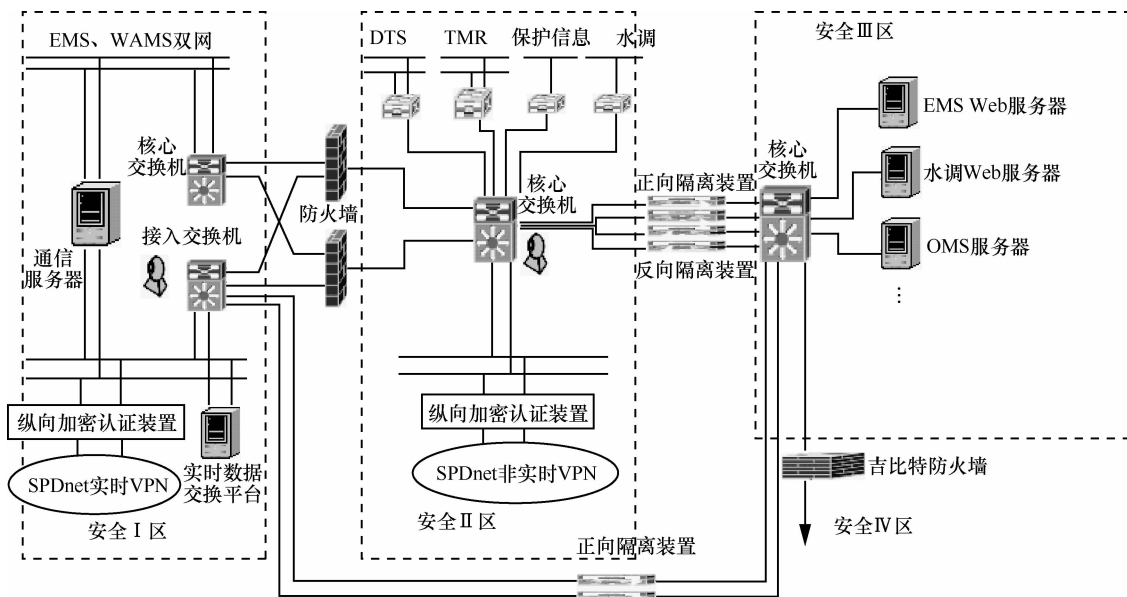


图 1 省调内网安全防护系统架构

2 系统架构

2.1 分级部署

按照“统一部署、分级管理”原则,下级监控平台需

主动向上级监控平台报送告警信息,从而实现上下级调度中心安全监控平台的级联通信。不同的地市调度中心,根据其规模大小,配置有所不同。级联方式如图 2 所示。

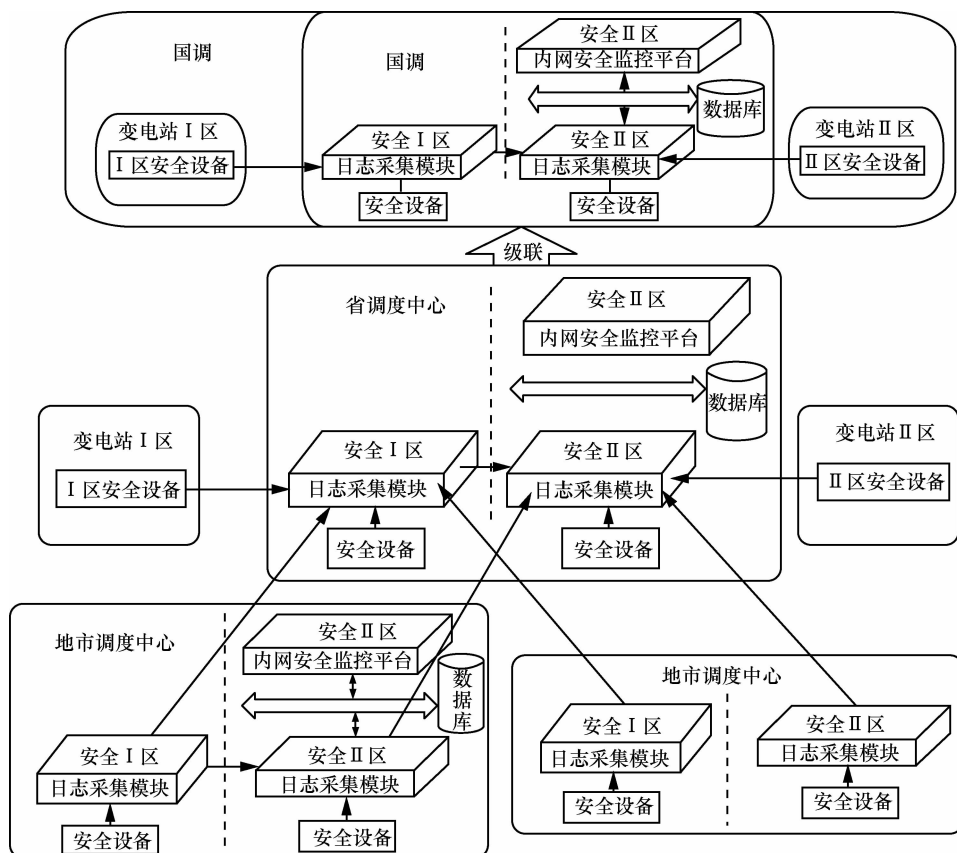


图 2 上下级监控平台级联方式

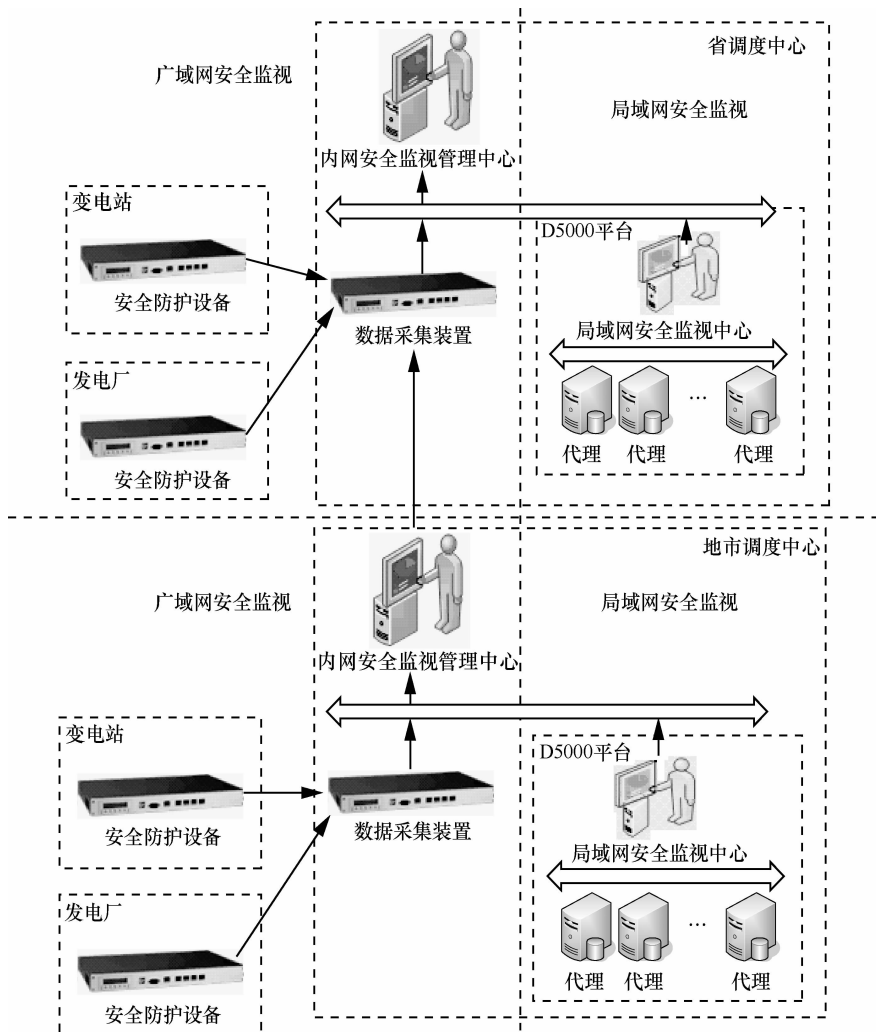


图3 电力调度内网安全监控平台总体架构

2.2 广域网与局域网

某省电力调度内网安全监控平台的总体架构分为广域网安全监控和局域网安全监控两部分,如图3所示。

广域网安全监控范围包括电力专用安全设备(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)。广域网安全监视模块负责监视二次系统安全设备(电力专用安全设备和通用安全设备),通过日志采集模块实时采集网络中存在的异常访问、非法外联等重要告警信息;局域网安全监视模块负责监视智能调度技术支持系统内部主机的安全状态,当系统内部主机发生异常或非法外联时,向内网安全监控平台发出告警。

2.3 平台功能3层架构

平台软件功能按照3层架构划分,即采集层、处理层和展现层,如图4所示。采集层主要负责采集不同类型设

备的日志事件信息;处理层对原始日志信息进行相应的处理,包括事件归并、过滤、格式转换和标准化;展现层则提供告警、设备和统计信息的实时展示。

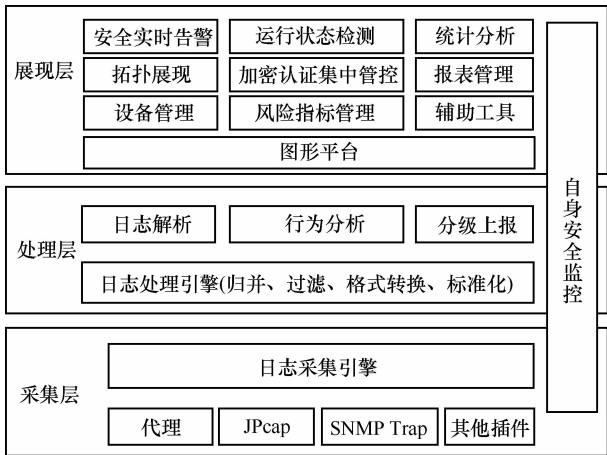


图4 平台功能3层架构

3 功能与实现方法

3.1 数据采集和发送

数据采集功能模块实现对横向物理隔离装置(正/反向)、纵向加密认证装置、防火墙、入侵监测系统、防病毒系统以及调度技术支持系统内部关键设备和应用的数据采集。

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)通过代理将日志转换为电力系统标准格式后进行采集;调度技术支持系统内部的关键设备和应用通过代理将日志转换为标准格式并发送至安全监控平台。

3.2 数据处理和分析

(1)数据标准化处理

安全监控平台的基础功能。采集端接收到原始日志数据后,首先经过协议识别,分流到各自的内容识别模块。在内容识别模块,经过内容模式匹配引擎,将数据分流到不同类型的分析模块中,进行关键字提取、内容筛选填充处理。

对于采集到的数据,根据安全监控平台设置的规则进行过滤,只保留监视范围内的、必要的、有效的数据,确保安全监控平台不保存过多冗余数据。数据的过滤规则能够通过匹配运算符设置复杂的匹配关系,匹配规则采用正则表达式算法。

(2)数据关联分析

安全监控平台支持事件类型关联、事件内容关联、资产信息关联,能够通过特定算法从大量安全事件数据中挖掘当前的安全趋势和规律。安全监控平台关联分析支持如下关联分析类型。

- 基本关联——根据事件的基本属性信息关联分析结果。
- 攻击关联——根据安全设备发出的告警事件,结合目标资产的类型生成关联分析结果。
- 位置关联——根据事件来源的位置或目标资产的物理位置,生成关联分析结果。
- 角色关联——根据事件相关用户名,结合事件基本属性生成关联分析结果。
- 因果关联——根据事件类型,结合事件行为结果生成关联分析结果。

3.3 数据展现界面

界面展现功能以图形化方式对采集的监视设备数据进行分析、查询以及图表展示,并对分析结果进行报表输出以及报表管理。可对监视设备进行资产管理,对系统本身的参数、用户权限、界面配色、地域路由、缺陷等进行配置和管理,仅以指标分析和装置管理为例进行介绍。

(1)指标分析

指标分析模块实现以下功能:设备数量统计分布饼图,可以看到每类设备所占的比例;各厂商安全设备统计柱状图;最近一周内平台设备在线运行率;紧急、重要告警量分布饼图;最近一周内平台安全指数对比柱状图;最近一周内平台告警数量统计曲线;地调地域横向对比柱状图;按照地域信息统计指定安全事件列表。

(2)装置管理

装置管理主要提供对加密装置的管理和查询功能,可以远程管理加密装置,为加密装置配置隧道和策略,并在页面上实时查看加密装置的链路情况,实现实时画面、实时监视和实时信息的即时刷新显示。

4 主要技术特点

(1)实现省地一体化运维

为满足二次系统安全防护的要求,充分发挥省、地两级专业人员的作用,平台采取省、地协同的建设方案,统一规划,两级部署。省调的安全Ⅰ区和Ⅱ区分别部署日志采集服务器,不仅负责采集省调的安全设备日志,还负责汇集地调的安全设备日志;地调的安全Ⅰ区和Ⅱ区也分别部署日志采集服务器,除负责采集地调的安全设备日志外,还负责将采集来的信息级联到省调,实现省地两级分布部署。

通过系统平台提供的用户权限管理功能,实现系统管理责任区的有效划分。省调用户查看全省范围内发生的告警和已接入的设备信息,地调用户只能查看自己地区范围内发生的告警和已接入的设备信息,不能查看其他地区的告警和设备信息。

(2)内建预案管理知识库

为保证正确、迅速处理异常情况,内网安全监控平台中建立了预案处理知识库,异常处理预案按照设备类型、告警类型、告警子类型、异常特征、处理方法等关键字段进行分类,方便专业人员检索。新型异常出现以后,专业人员



对异常处理进行总结分析,记录处理过程及处理方法,按照异常处理预案的关键要素编制描述文档,录入知识库。若系统中再次出现类似告警,即使维护人员未处理过此类异常,也可以通过检索知识库找到处理方法,正确处理。

(3)实现告警信息一体化监控

从加强二次系统安全防护设备和平台系统自身的运行维护出发,开发了告警信息输出接口,将平台系统的告警信息接入自动化报警系统中,与调度主站各系统实现统一监控。对系统的各类告警信息进行了全面梳理,优化了告警信息分类。当系统出现紧急告警时,告警信息通过接口实时输出至自动化报警监控系统,通知自动化运行值班人员,并以手机短信方式告知有关管理人员,与调度主站各系统实现一体化监控。

(4)更友好的可视化界面

系统提供的展示画面构图充分考虑了设备属性、维护习惯、设备之间的关系。按照分区概念建立拓扑结构,已接入的设备分别放置在拓扑结构的相应概念区域内,如地调 I 区的 IDS 放置在拓扑 I 区主站的概念区域内,地调 220 kV 变电站的加密装置放置在 II 区厂站的概念区域内,地调 I-II 区横向防火墙放置在 I 区主站和 II 主站之间,地调 I-III 区隔离放置在 I 区主站和 III 区之间。拓扑采用铁道线展现从主站到厂站的纵向加密隧道。

为了增强表现力,系统还增加了界面色彩配置功能,维护人员可以按照需求选择配置界面及字体的色彩,系统内置 3 种配色方案供选择使用。

(5)完善的运维操作工具

为了提高运维效率,对平台进行了大量优化,有效减轻了维护工作量,提高了工作效率,同时增强了系统的实用化水平。比如,“置告警缺陷牌”功能,即对于某些一时无法处理的告警,通过设置缺陷牌停止告警,避免对运行监视形成干扰,问题解决后解除缺陷牌确认该告警,满足运行监视的可靠性、准确性要求。

5 项目实施

建设项目由省调电力调度控制中心负责组织实施。根据调度内网规模和业务数据流量,省调主调部署整套安全监控平台和日志采集模块,省调备调及地调只部署监控平台广域网日志采集模块。部署方案架构如图 5 所示。

5.1 平台硬件配置

电力调度内网安全监控平台在省调及各地调共部署 37 台联想服务器,其中,在省调部署 3 台服务器,1 台部署在 I 区,用于采集省调 I 区内网的安全事件,接收并转发各地调和备调 I 区采集服务器上传的日志信息;另外 2 台部署在 II 区,作为平台数据库服务器和内网安全监控平台服务器,在平台服务器上同时部署日志采集模块,接收各

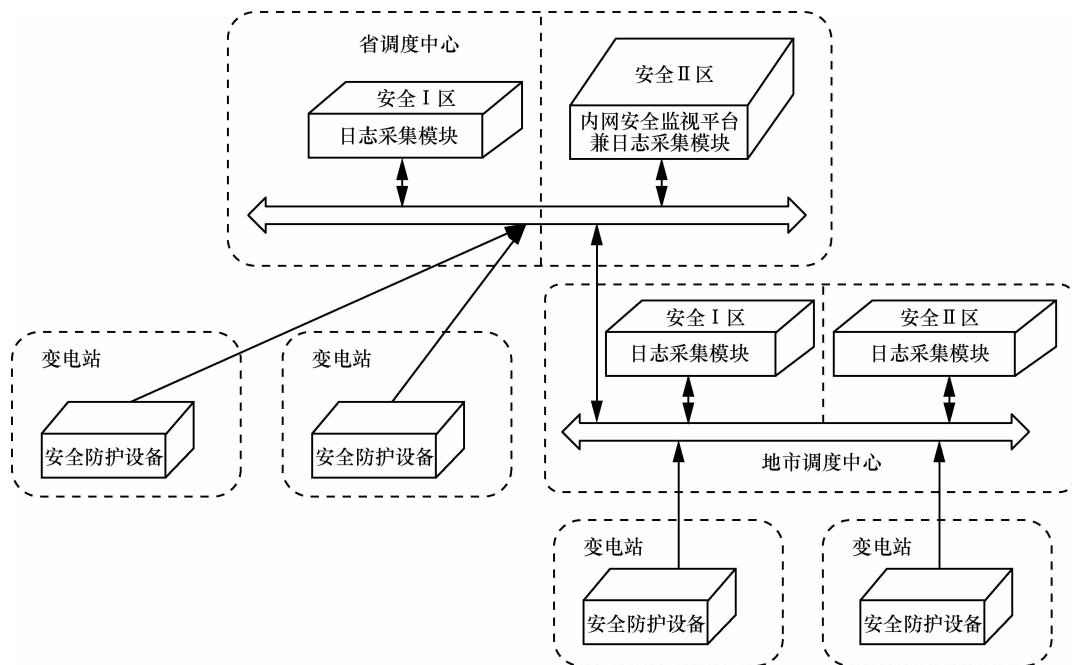


图 5 部署方案架构

地调和备调Ⅱ区采集服务器上传的日志信息,统一发送到总线并进行入库处理。在省调备调和下属16个地调部署2台服务器,分别部署在Ⅰ区和Ⅱ区,采集内网的安全事件,并上传到省调服务器。

5.2 平台软件配置

配置凝思安全操作系统37套(与硬件配置数量相对应),满足国家级保护要求中具有4级防护能力的B级操作系统,其中省调主调3套、省调备调2套、16个地调各2套。

配置金仓数据库企业版1套(25个用户,含并行处理),具备数据库的备份和恢复功能,并且可以明确划分数据库的用户权限,区分业务应用和数据库管理员的操作权限。

配置省调内网安全监控平台1套。配置日志采集模块36套,其中省调主调2套、省调备调2套、16个地调各2套,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)的日志。

6 运行情况

电力调度内网安全监控平台已完成省调、备调、16个地调及其所辖县调和220 kV变电站的共162台纵向加密装置(南瑞)、121台防火墙(东软、天融信、联想网御、启明星辰)、45台正反向隔离装置(南瑞、珠海鸿瑞)、2台防病毒(瑞星)的日志接入工作。工程涉及5家厂商的5类安全设备。

平台提供了对接入设备的在线统计分析,不仅支持对设备类型、设备厂商、设备在线率、告警数量和安全指数等的每日统计,还支持每15 min对设备在线情况进行判断。以上信息可以在线查看、在线统计和在线分析,并最终形成月报表和年报表。

平台自2012年10月投运以来,运行稳定、可靠,可以及时发现和处理安全防护设备缺陷、安全事件,取得良好效果。如隧道建立错误,宿州的双庆变纵向加密装置与远端装置之间的隧道建立错误。两台加密装置之间的隧道建立错误,即这两台装置之间的信息在网络上无法以密文的方式传输,只能以明文的方式传输,存在安全隐患。再如不符合安全策略的访问,蚌埠地调的反向隔离装置出现某个IP地址以UDP访问其他IP地址的0端口,该访问不符合安全策略。如果某个IP地址以UDP试图穿过反向隔离访

问装置另一端的IP地址的0端口成功,那么病毒通过UDP的0端口进行传播的概率增加,存在安全隐患。平台及时发现存在的安全隐患,经过及时分析处理,保证调度内网的安全。

7 结束语

部分地调早期部署的防火墙、入侵检测装置,由于版本老旧而无法接入监控平台。已制定升级改造计划,争取尽快实现全部设备的接入。省调已制定《内网安全监控平台运行管理规定》,以期通过技术和管理两个方面,全面加强二次系统安全防护;同时,也将不断完善平台功能,改进人机界面,总结运行规律,并针对新的安全问题持续改进与提高。

参考文献

- 1 胡炎,辛耀中,韩英铎.二次系统安全体系结构化设计方案.电力系统自动化,2003,27(21):63~68
- 2 秦超,张涛,林为民.基于数字证书认证的电力安全拨号认证系统.电力系统自动化,2009,33(19):52~55,100

[作者简介]



袁林,男,国网安徽省电力公司电力调度控制中心高级工程师、副总工程师,主要从事电力系统自动化、信息化工作。



高夏生,男,国网安徽省电力公司电力调度控制中心高级工程师,主要从事电力系统自动化、网络管理工作。



赵田红,女,国网安徽省电力公司电力调度控制中心高级工程师,主要从事自动化系统维护、运行管理工作。

(收稿日期:2013-08-01)