Smart Grid 智能电网, 2020, 10(5), 225-230
Published Online October 2020 in Hans. http://www.hanspub.org/journal/sg
https://doi.org/10.12677/sg.2020.105025

配电物联网的信息安全方案分析

戴　铭，王　宇，赵金平

北京智芯半导体科技有限公司，北京
Email: daim0802@163.com

收稿日期：2020年9月8日；录用日期：2020年10月2日；发布日期：2020年10月9日

摘　要

随着配电物联网建设的不断推进，在提升配网运行效能的同时，作为连接输电与用电的关键环节，其安全可靠的运行问题同样值得关注。本文针对配电物联网“云－管－边－端”四层逻辑架构，分析了目前配电物联网所面临的安全问题，并形成了针对配电物联网的安全防护方案体系。

关键词

配电，物联网，安全

Analysis of Information Security Scheme of Power Distribution Internet of Things

Ming Dai, Yu Wang, Jinping Zhao

Beijing Smartchip Semiconductor Technology Company Limited, Beijing
Email: daim0802@163.com

Received: Sep. 8th, 2020; accepted: Oct. 2nd, 2020; published: Oct. 9th, 2020

Abstract

With the continuous progress of the construction of the distribution network of things, while improving the operation efficiency of the distribution network, as a key link connecting transmission and electricity consumption, its safe and reliable operation problem also deserves attention. Aiming at the four-layer logic architecture of “cloud-pipe-side-end” of the distribution network of

文章引用: 戴铭, 王宇, 赵金平. 配电物联网的信息安全方案分析[J]. 智能电网, 2020, 10(5): 225-230.
DOI: 10.12677/sg.2020.105025

things, this paper analyzes the security problems faced by the distribution network of things at present, and forms a security protection scheme system for the distribution network of things. In order to improve the safety of the power distribution Internet of Things, a reliable solution is provided.

Keywords

Power Distribution, The Internet of Things, Safety

1. 引言

随着物联网应用越发普及，能源互联网战略部署的建设与推进，配电网的架构也随着物联网(Internet of Things, IoT)技术、人工智能技术、大数据存储技术、云计算技术、5G 通信技术等新兴技术的应用而不断演进。配电物联网建设将极大程度提升配网运行状态的全面感知能力，保障分布式能源的友好接入，提高对新型负荷的弹性承载力，满足用户多样性用能需求。配电网作为连接输电与用户的关键环节，其安全可靠运行对电力系统稳定以及用户体验的重要性不言而喻。

针对信息安全防护问题，电力系统以网络边界隔离保护为主的安全防护体系，制定了“安全分区、网络专用、横向隔离、纵向认证”的安全防护策略，当前配电物联网的建设、发展及其信息安全防护仍处于探索阶段，本文首先介绍当前配电物联网当前建设架构，其次对配电物联网的安全问题和主要安全防护技术进行分析，最后展望配电物联网未来安全防护发展趋势。

2. 配电物联网架构

物联网技术在广义上说，可以把它理解成利用信息传输系统，把物品的相关信息与互联网相连接，从而实现物质信息置换通讯，完成智能识别、定位、跟踪和监管的一种现代化信息技术，其架构通常可分为三个逻辑层次，其从上至下依次为：应用层(application)、传输层(transport)和感知层(sensing) [1] [2]。而配电网作为连接电网与用户的桥梁，相较于电力系统其他环节更具有面向社会服务的特性，通过物联网技术对整个配电系统中的各项设备进行精准的感知，让其中的各项设备之间都有信息的传递，而且还可以根据需要进行相互间的操作，形成“云(应用层) - 管(平台层) - 边(网络层) - 端(感知层)”的四个层次的逻辑架构，如图 1 所示，对整个电网中的各种细节都可以进行感知，对配电网络的管理可以更加的高效。

感知层由感知层网关和二维码、智能装置以及 RFID 等感知设备组成，能够完成数据的收集和处理工作，感知层提供配电网的运行状态、设备状态、环境状态以及其它辅助信息等基础数据需求[3]；应用层具备行业应用、公众应用、数据存储、数据管理以及标识解析等多种功能，其功能主要基于海量配网运行数据，完成配电网中低压业务信息处理和分析，其物理形态表现为基于物联网的配电自动化主站；网络层是平台层和感知层的桥梁，为两个阶层提供了专用网、异构网以及移动互联网等数据传输路线，利用了从云平台到网络边缘计算节点、直至终端单元的计算、存储、通信、管理等功能，形成了从云到端的连续服务区域[4]。

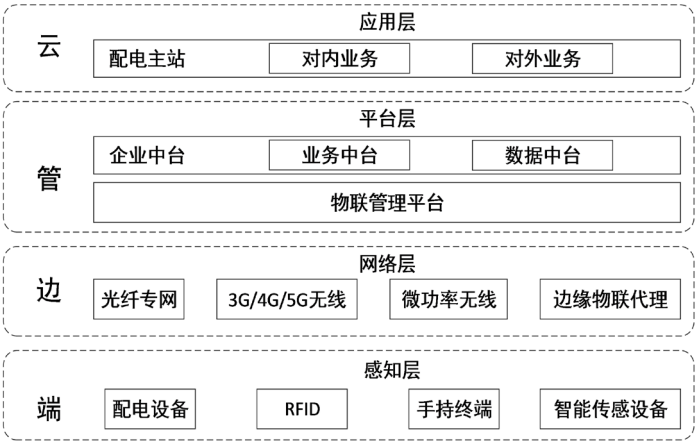

Figure 1. Distribution Internet of Things logic architecture
图 1. 配电物联网逻辑架构

3. 配电物联网安全风险分析

近年来全球工控网络信息安全事件频发，2010 年“震网”病毒席卷全球超过 45,000 个网络，以伊朗遭到的攻击最为严重，造成伊朗布什尔核电站推迟发电。2014 年 12 月德国一家钢铁厂遭受高级持续性威胁(ATP)网络攻击，导致工控系统的控制组件和整个生产线被迫停止运转。2015 年乌克兰停电事件，以终端为攻击跳板瘫痪电力控制系统导致，成为全球首例公开报道的因黑客攻击导致大范围停电事件。2018 年 8 月，台积电部分台机受病毒感染，造成三大厂区大规模停产。2019 年 3 月 7 日，包括首都加拉加斯在内，委内瑞拉一度同时有 20 个州大面积停电超 24 h，2019 年 3 月 8 日凌晨，各州陆续恢复供电。2019 年 4 月 11 日，全国第二次大面积停电。委内瑞拉国家总人口量约为 3085 万，整体发电量约为 117,000 GWh，造成停电事故的主要原因是发电量占全国用电量近四成的古里水电站遭受网络攻击进而发生故障。攻击者预先植入恶意代码，在设备采购的供应链环节植入震网病毒变体，适时诱导病毒发作；通过电子战飞机攻开 WiFi 密码，然后以此为入口，进行目标渗透，致使失去对绝大部分变电站的监测及控制导致古里水电站的计算机系统中枢和加拉加斯控制中枢严重受损[5]。

以上安全事件表明针对工业网络的各种攻击日益增多且方式多样，配电物联网需要一套完整的安全防护方案。

应用层直接面向用户提供应用服务，包括各类服务器、工作站等设备，针对用户操作首先存在身份是否合法问题，其次是否超出权限范围问题，还有操作行为是否合规问题。针对应用服务是否能正常为用户提供正常响应，所部署系统是否存在漏洞，开放的端口可能被攻击利用，主机是否被植入病毒木马等安全问题。

平台层承载着配电网运行的大量数据，针对数据防护需考虑所存储数据是否被越权访问导致关键数据泄露，管理的数据是否被篡改或恶意删除造成上层应用做出错误的判断和操作，数据库系统存在被入侵风险，所接入的智能终端设备的身份是否正确等安全问题。

网络层主要负责安全高效地传递感知层收集到的信息，主要面临传输的业务数据被非法监听或篡改，短距离无线通信被侵入恶意利用，部分采用电池供电保持短距离通信设备易受到 DOS 攻击造成设备电量耗尽停止工作等问题。

感知层主要负责数据收集，海量智能终端互联互通导致网络开放性扩大引入网络攻击渗透破坏风险，终端自身安全防护措施不足易被病毒、木马等网络攻击利用，嵌入式系统与核心芯片的自主可控程度低也增加安全风险。

4. 配电物联网安全防护体系

针对配电物联网感知层、网络层、平台层和应用层 4 个层面的安全问题，构建全层次的网络安全防护体系如表 1 所示[5]。

Table 1. Safety protection system for Internet of Things distribution
表 1. 配电物联网安全防护体系

防护思路		重点防护方向	
应用层数据的价值创造安全	业务安全基础上，重点实现应用的全景监测和智能处理	数据安全 (数据分类授权、防泄漏)	应用安全 (应用审计、安全交互)
		威胁主动预警	等保合规
平台层数据的管理安全	云安全基础上，重点实现物联网数据和应用安全交互	动态安全感知	工控专用情报库、漏洞库、病毒库
		云平台安全	
网络层数据的传输安全	流量监测基础上，重点实现信息内网和外网的智能防御	电力无线专网安全防护	通信协议规范
		内外网融合防护	全流量监测
感知层数据的采集安全	端到端可信互联基础上，重点实现终端的统一感知	终端安全管控 (安全策略管控、物联代理安全)	安全身份认证 (基础密码服务、身份标识认证)

在配电物联网的安全防护下，主要应用的安全防护主要有以下几方面。

1) 数据安全

数据加密技术提高数据的安全性和保密性，按照作用的不同，数据加密技术可分为数据存储加密技术、数据传输加密技术、数据完整性的鉴别技术和密钥管理技术[6] [7]。

a) 数据存储加密技术是防止在存储环节上的数据失密，数据存储加密技术可分为密文存储和存取控制两种。前者一般是通过加密算法转换、附加密码、加密模块等方法实现；后者则是对用户资格、权限加以审查和限制，防止非法用户存取数据或合法用户越权存取数据。

b) 数据传输加密技术的目的是对传输中的数据流加密，使用两种加密方式，一种为线路加密如 VPN 通道，另一种为端与端之间的数据加密，指信息由发送端自动加密，对协议报文进行数据报封装，然后作为不可阅读和不可识别的数据穿过网络，在到达目的地时将被重组、解密，而成为可读的数据。

c) 数据完整性鉴别技术的目的是对介入信息传送、存取和处理的人的身份和相关数据内容进行验证，一般包括口令、密钥、身份、数据等项的鉴别。系统通过对比验证对象输入的特征值是否符合预先设定的参数，实现对数据的安全保护。

d) 密钥管理技术包括密钥的产生、分配、保存、更换和销毁等各个环节上的保密措施，密钥管理可服务于身份认证技术，智能终端设备接入，在装置中嵌入灌装密钥安全模块，作为接入的凭证。

2) 应用安全

信息安全审计主要是指对系统中与安全有关的活动的相关信息进行识别、记录、存储和分析。信息安全审计可以访问网络、主机和数据库，监控审计用户使用行为和信息内容，为判断信息的真实性、可靠性提供依据。信息监控审计技术实时监控网络流量，在发现问题时及时切断链接并保留审计日志，对网络信息进行“内容消毒”[8]。

3) 平台安全

a) 主机安全加固技术从提高主机操作系统本身的安全性出发，以可信认证为基础、访问控制为核心，

利用“三权分立”的管理机制，通过对文件、目录、进程、注册表和服务的强制访问控制，有效制约和分散原有系统管理员的权限，结合文件和服务的完整性检测、防缓冲区溢出等功能，将普通操作系统透明提升为安全操作系统，增强主机安全性[9]。

b) 主机病毒防范技术针对应用层的服务器、工作站等主机操作系统及时更新、打补丁，同时部署主机防护软件，管控 U 盘接入所带来的恶意代码、病毒，启动文件级白名单策略，实时监控运行的程序，防止恶意代码、病毒、非法软件执行，并定期对主机进行全盘进行恶意代码、病毒查杀[5]。

c) 入侵检测技术是计算机的监视系统，通过实时监视系统，一旦发现异常情况就发出警告，根据信息来源分为主机入侵检测和网络入侵检测，对各种事件进行分析，从中发现违反安全策略的行为[10]。

4) 终端安全

终端可信计算技术针对配电终端特性研究基于电力专用芯片的配电终端可信根，实现对电力终端操作系统、业务应用程序的可信量度，保证终端状态的可信。设计以可信根为基础、以嵌入式微控制单元为应用的终端可信逻辑硬件架构，研究端口安全访问机制和接口驱动安全机制，实现终端的主动免疫能力[11]。

5) 网络安全

处于生产控制大区内的某些业务系统或其模块需使用公共通信网络、无线通信网或任何非可控的网络设备与终端进行通信时，如其自身安全防护水平明显低于同大区内的其他系统，则须建立安全接入区。在安全接入区内加设用于进行数据采集的公网数据采集服务器，接入区与其他区块之间需加装横向隔离装置。安全接入区使用公共通信网络或无线通信网络时应使用加密认证，以此达到主站与业务终端之间安全隔离、身份认证等目的[12] [13]。

6) 身份认证

身份验证是信息安全中最基本的一项，对配电主站等关键业务系统采用多因子认证技术进行身份认证，是一种计算机访问控制的方法，通过静态或动态密码 + UKey 的方式相结合对登陆者的身份进行验证，未来还会增加指纹等更多身份识别因子[12]。

5. 总结

关于配电物联网的安全防护强度逐步提升，但随着配电物联网的不断发展，新技术持续引入，配电物联网现有的安全防护方案已具备相当安全防护能力，但随着物联网及新技术的不断发展，轻量级安全机制、区块链技术的应用[14] [15]、自主可控芯片[12]等新技术的研究也应不断深化，然而潜在安全风险仍不容忽视，只有尽快发现并解决配电物联网安全研究的诸多难点，才能更有效抵御愈发严重攻击，使配电物联网更加安全、可靠、高效地运行。

参考文献

[1] 张亚健, 杨挺, 孟广雨. 泛在电力物联网在智能配电系统应用综述及展望[J]. 电力建设, 2019, 40(6): 1-12.

[2] 张玉清, 周威, 彭安妮. 物联网安全综述[J]. 计算机研究与发展, 2017, 54(10): 2130-2143.

[3] 易斌, 梁崇淦, 赵伟, 赵赫. 基于低压配电台区运行特性的储能控制策略[J]. 智能电网, 2020, 10(3): 121-130.

[4] 张冲, 王凯, 王宇恒. 电力配网自动化系统的运行监控安全保护探讨[J]. 电气技术与经济/研究与开发, 2018(6): 1-2.

[5] 王海峰, 李朝阳, 吕政权, 陈怡君, 彭道刚. 泛在电力物联网环境下网络安全攻击研究[J]. 浙江电力, 2019, 38(12): 76-81.

[6] 黄河明. 数据加密技术及其在网络安全传输中的应用[D]: [硕士学位论文]. 厦门: 厦门大学, 2008.

[7] 巴斯替, 骆德汉. 智能电网的网络安全: 概述与挑战[J]. 产业与科技论坛, 2019, 18(10): 43-45.

[8] 刘文. 信息安全审计问题与应用创新策略研究[J]. 信息安全研究, 2017, 3(10): 946-953.

[9] 廖翼, 王涛, 施武作, 陈婷婷. 配网智能终端无线网络接入电力系统安全技术研究[J]. 机电信息, 2019(21): 26-28.

[10] 余俊. 内网安全防护技术的研究与实现[D]: [硕士学位论文]. 南京: 南京航空航天大学, 2010.

[11] 刘积芬. 网络入侵检测关键技术研究[D]: [博士学位论文]. 上海: 东华大学, 2013.

[12] 方明伟. 基于可信计算的移动智能终端安全技术研究[D]: [博士学位论文]. 武汉: 华中科技大学, 2012.

[13] 张涛, 赵东艳, 薛峰, 张波, 章锐. 电力系统智能终端信息安全防护技术研究框架[J]. 电力系统自动化, 2019, 43(19): 1-8.

[14] 江秀臣, 罗林根, 余钟民, 等. 区块链在电力设备泛在物联网应用的关键技术及方案[J]. 高电压技术, 2019, 45(11): 3393-3400.

[15] 吉斌, 谭建成. 利用区块链技术的配电侧分布式微电能交易初探[J]. 现代电力, 2019, 36(1): 29-36.