引用格式: 张磊, 李延, 谷思庭, 等. 新型电力系统配电自动化安全可信防护模型及评价体系[J]. 微电子学与计算机, 2023, 40(12): 70-80. [ZHANG L, LI Y, GU S T, et al. Security and trustworthy protection model and evaluation system of distribution automation under the new power system[J]. Microelectronics & Computer, 2023, 40(12): 70-80.]**DOI:** 10.19304/J.ISSN1000-7180.2022.0696

新型电力系统配电自动化安全可信防护模型及评价体系

张 磊[1], 李 延[1], 谷思庭[1], 袁艳芳[1], 王振林[1], 房 牧[2], 由新红[2]

(1 北京智芯微电子科技有限公司, 北京 102200;
2 国网山东省电力公司 电力科学研究院, 山东 济南 250000)

摘 要: 电力物联网是当前新型电力系统发展的一个重要方向. 电力物联网天然在运行方式、拓扑形态等方面可以很好地支撑主动配电网的建设,但由于配电网运行环境复杂,既要基于配电物联网来实现物联和全景感知,也要直接面对由于物联网灵活多样的接入环境和方式、数量庞大的终端造成的配电网结构和边界的动态多变,以及面临的更高安全风险,亟需开展里外兼顾、多维融合的配电自动化安全可信防护研究. 本文首先介绍了新型电力系统下配电自动化系统的架构,提出了配电自动化安全可信防护模型;其次,建立了基于可信计算的等保指标评价体系,分析其应用于配电自动化系统安全的可行性;再次,对提出的配电自动化安全可信防护模型做出评价,分析其完整性度量和可信网络连接过程;最后,对该架构下的安全性进行了简要总结.

关键词: 可信计算; 电力安全防护; 电力物联网; 配电自动化; 评价体系; 综合评价; G1 法

中图分类号: TM769 **文献标识码:** A **文章编号:** 1000-7180(2023)12-0070-11

Security and trustworthy protection model and evaluation system of distribution automation under the new power system

ZHANG Lei[1], LI Yan[1], GU Siting[1], YUAN Yanfang[1],
WANG Zhenlin[1], FANG Mu[2], YOU Xinhong[2]

(1 Beijing Smart-Chip Microelectronics Technology Co., Ltd., Beijing 102200, China;
2 State Grid Shandong Electric Power Research Institute, Ji′nan 250000, China)

Abstract: The ubiquitous power Internet of Things(IoT) is an important direction for the development of the current new power system. The ubiquitous power IoT can naturally support the construction of active distribution networks in terms of operation mode and topology. However, due to the complex operating environment of the distribution network, it is necessary to realize the ubiquitous IoT and panoramic views based on the distribution IoT. In terms of perception, it is also necessary to directly face the dynamic changes in the distribution network structure and boundary caused by the flexible and diverse access environments and methods of the IoT, a large number of terminals, and the higher security risks faced. It is urgent to take into account the inside and outside, multi-dimensional integration of power distribution automation security and trusted protection research. This paper firstly introduces the architecture of the distribution automation system under the new power system, and proposes a trusted protection model for distribution automation security; secondly, establishes an evaluation system of equal protection indicators based on trusted computing, and analyzes the feasibility of its application to the security of distribution automation systems; Furthermore, the proposed distribution automation security trusted

收稿日期: 2022-11-03; **修回日期:** 2023-01-31
基金项目: 国家电网有限公司科技项目 (5400-202116144A-0-0-00)

protection model is evaluated, and its integrity measurement and trusted network connection process are analyzed. Finally, the security under this architecture is briefly summarized.

Key words: trusted computing; electrical safety protection; power internet of things; distribution automation; evaluation system; comprehensive evaluation; G1 method

1　引言

随着计算机通信技术的发展,面向电力行业的信息管理系统也有了广泛的应用[1]. 面向电力营销、调度、巡检等的各种信息系统在近年来完成了从传统分布式到开放式的升级,电力行业的 IT 系统愈发庞大[2]. 配电网运行环境复杂,既要基于配电物联网来实现物联和全景感知,也要直接面对由于物联网灵活多样的接入环境和方式、数量庞大的终端造成的配电网结构和边界的动态多变,以及面临的更高安全风险,亟需开展里外兼顾、多维融合的配电网可信安全防护体系研究[3].

近几年来,在“网络空间安全”国家重点研发计划中也均涉及了云计算、天地一体化通信等领域的“内生安全”课题的研究[4];一些文献也已提出了构建具有动态重构和可信免疫的配电物联网可信防护体系的建议[5];同时,国家电网公司也将可信计算和区块链等技术列为支撑“三型两网”建设的支撑技术[6].

本文提出一种基于可信计算的配电自动化安全防护模型,通过建立指标体系评价配电网系统安全性能,分析模型的完整性度量,实现配电自动化的可信安全防护.

2　配电自动化安全可信防护模型

2.1　现有配电自动化安全防护架构

随着通信技术和网络技术的快速发展,安全问题得到了越来越多的重视. 在电力系统安全防护建设上,国家电网已经有了一定的建设基础[7]. 2014 年国家发展改革委发布的《电力监控系统安全防护规定》(以下简称《防护规定》) 中提到[8],电力系统安全防护工作应当落实国家信息安全等级保护制度,按照国家信息安全等级保护的有关要求,坚持“安全分区、网络专用、横向隔离、纵向认证”的原则[9],保障电力系统安全. 以此为基础,按照电力系统中建设的技术路线为标准,建立配电网安全防护架构层次模型,如图 1 所示,分为主站层、网络层、终端层 3 个层次[10].

主站层包括配电生产控制大区、配电信息管理

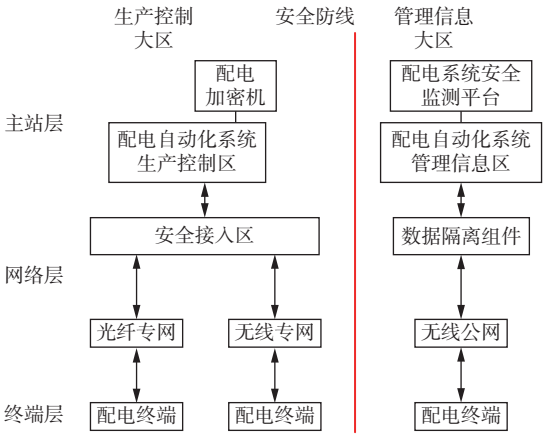

图 1　配电自动化安全防护架构

Fig. 1 Distribution automation safety protection framework

大区.生产控制区是电力系统安全防护最重要的大区,它直接实现对电力一次系统的实时监控. 配电信息管理大区是指生产控制大区以外的电力企业管理业务系统的集合,其典型业务包括电力企业数据网、生产管理系统等. 生产控制大区和信息管理大区之间设置正反向安全隔离装置,保障信息交互的安全性[11].

网络层由子站系统及通信网络构成.子站系统负责将感知层终端采集的海量数据汇总上传以及实现平台层控制指令的下达,由主机、路由等设备构成,子站系统分为监控功能子站和通信汇集功能子站[12]. 通信网络中包含纵向加密装置、防火墙等安全装置,保障配电网通信的安全性.

终端层由主动配电网的终端设备 (如智能电表、故障检测仪、智能传感器等) 构成,承担起主动配电网数据感知和信息采集工作[13],支撑配电网管理控制系统构建.

2.2　基于可信计算的配电网安全防护模型

随着配电网的深入发展,配电网终端设备种类复杂,数量繁多,其性能和工作性质也大不相同,其安全需求也有较大差距,为此需要提出一种统一的安全架构模型[14],保障配电网内生安全.

配电网系统由配电主站、通信网络层和配电终端组成,为实现配电物联网安全可信的信息交互,提出基于可信计算的配电物联网安全管控架构[15],实现各层之间的可信认证和各设备自身的完整性度量,其具体架构如图 2 所示.

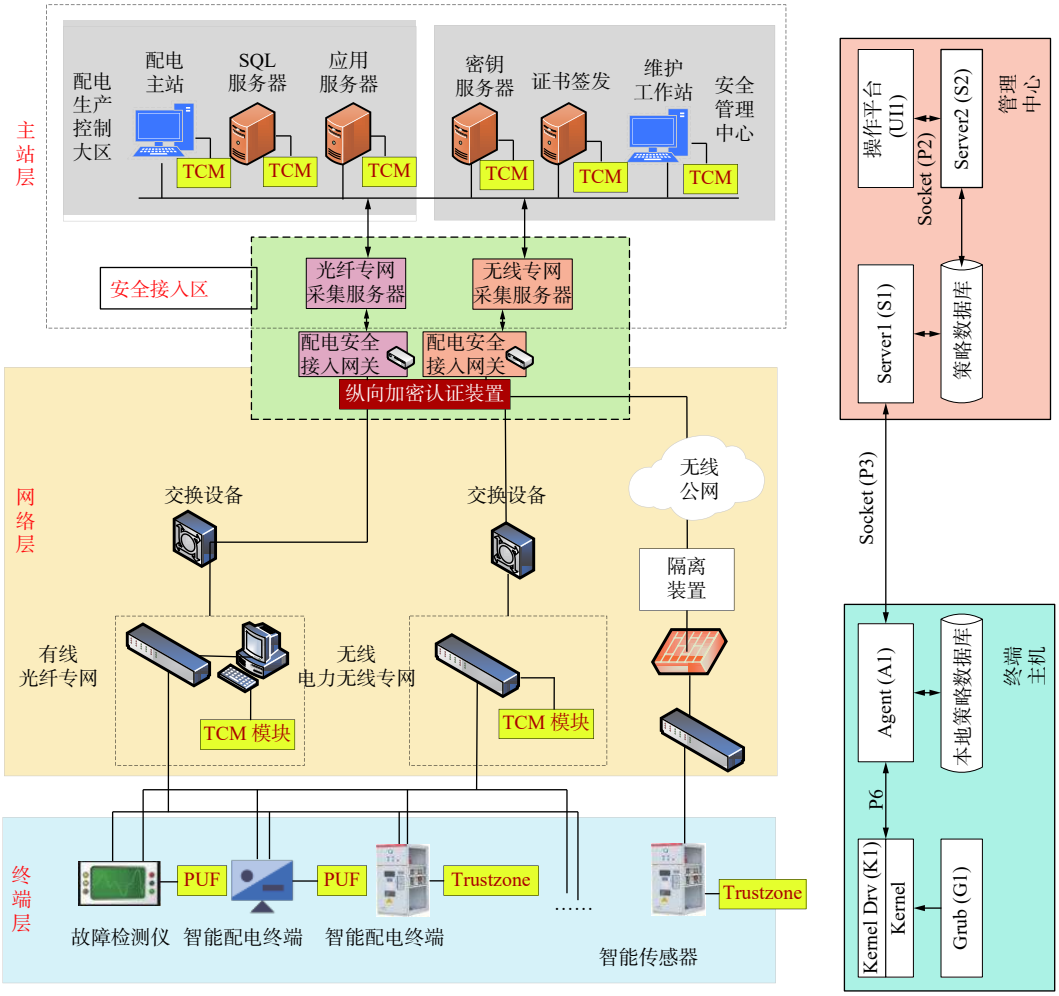

图 2 基于可信计算的配电网安全防护模型

Fig. 2 Distribution network security protection model based on trusted computing

将可信计算技术融入配电网架构,依照电力系统层次结构分为主站层、网络层、终端层. 主站层由配网主站、数据库服务器、应用服务器等构成,其主要功能是实现主站对配电网的统筹控制. 同时与配网主站处于同一层次的还有安全管理中心 (Certificate Authority,CA),主要作为安全认证的第三方参与配电网安全管控. 网络层包括配电网通信网络及配电子站,子站作为中继站实现对感知层终端的控制及信息交互[16]. 感知层有智能配电终端 (DTU/FTU/TTU)、智能传感器等控制和感知设备,也有故障检测仪、智能电表等轻量级感知设备,承担起配电网终端控制及信息采集的工作.

随着可信计算的发展,可信计算技术实现方式从原来单一的硬件芯片形式发展为多样化的软硬件形式,特别是在计算和存储资源有限的移动设备、嵌入式设备中[17]. 如,基于 Advanced RISC Machines(ARM) 的 Trustzone 通过处理器分区实现设备的可信;物理不可克隆函数(Physical Unclonable Functions,PUF),通过其物理安全特征的唯一性实现可信认证、密钥管理等功能,且因其轻量级、易实现等特性,常用于物联网、移动网络、可穿戴设备等场景中. 可信计算作为一种保障信息系统可预期性的技术,用在配电网终端安全通信研究上,既可实现设备自身完整性验证,也可实现设备之间可信接入[18]. 为将可信计算引入配电网内,需要在各设备平台配备可信根可信密码模块 (Trusted Cryptography Module,TCM),可以有以下 3 种方式:

(1) 针对计算性能偏弱的嵌入式平台,可以采用软 TCM 设计,只实现基本的 TCM 功能命令即可,包括:完整性度量、密码学计算;

(2) 针对 ARM 配有 Trustzone 且对 TCM 性能要求低的平台,可以使用 Trustzone 构建一个较完整功能的 TCM 功能区,进而构建该平台的可信根;

(3) 像主机平台一样,通过系统主板总线接口内置/外置一个 TCM 安全芯片,进而构建完整的 TCM 可信根功能.

考虑到配电网设备数量庞大、种类繁多、接入方式复杂,本文构想采用多种平台可信根设计,灵活使用可信计算,实现配电网终端的安全性和可靠性.

在本架构中对感知层设备的可信计算应用采取第二种和第三种可信根 TCM 构建方式. 在子站设备引入基于 ARM 系统的 Trustzone 结构构建一个具有完整功能的 TCM 功能区,或者像主机平台一样,通过系统主板总线接口内置/外置一个 TCM 安全芯片,进而构建完整的 TCM 可信根功能,实现子站层设备自身的完整性度量及设备与配电子站之间安全可信通信.

由于部分感知层终端的计算能力较低、性能偏弱,所以在本架构中,这类终端主要通过物理不可克隆技术 PUF 实现软 TCM 设计,只实现基本的 TCM 功能命令 (包括完整性度量、密码学计算). 由此也可实现终端设备自身的完整性度量以及终端与主站的安全可信通信.

终端侧的可信逻辑如图 3 所示,芯片为可信安全硬件,操作系统是 Linux,白名单为应用程序.主站侧的可信计算支撑平台如图 4 所示,计算机系统的应用软件与可信密码支撑平台双向互通,可信计算密码支撑平台由 TCM 服务模块与可信密码模块构成,密码算法引擎有 SM2、SM3、SM4 和随机数发生器等.

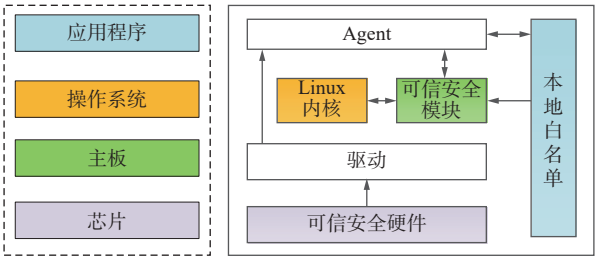

图 3　终端侧可信逻辑

Fig. 3 Terminal side trusted logic

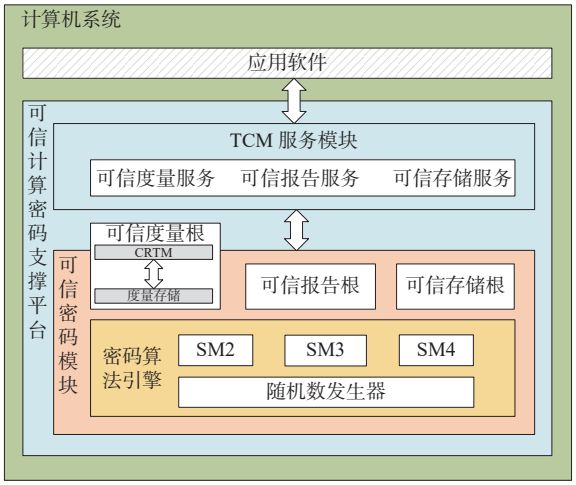

图 4　主站侧可信逻辑

Fig. 4 Master station side trusted logic

3　配电自动化可信防护评价指标

本文主要研究电力信息系统,结合等级保护 2.0 标准、《电力信息安全水平评价指标 (GB/T 32351-2015)》和《电力信息系统安全检查规范 (GB/T 36047-2018)》构建电力信息系统安全性评估指标体系[19]. 该指标体系分为 3 层:目标层 (B)、一级指标 (C)、二级指标 (D).

本文主要对电力信息系统的技术部分进行安全评估,按照等级保护 2.0 进行构建,技术部分包含 5 类一级指标:安全物理环境 (C_1)、安全通信网络 (C_2)、安全区域边界 (C_3)、安全计算环境 (C_4)、安全管理中心 (C_5);管理部分包含 5 类一级指标:安全管理制度 (C_6)、安全管理机构 (C_7)、安全管理人员 (C_8)、安全建设管理 (C_9)、安全运维管理 (C_{10}). 各类一级指标下,还细分若干二级指标,二级指标依据等级保护 2.0 以及电力行业相关标准提取建立.

由于等级保护 2.0 的安全测评全部采用主观判定的方式进行评价,为此,本文参照等级保护 2.0 标准、电力行业相关标准对二级指标进行整合优化,保障安全评估的全面性. 本文主要针对基于可信计算的安全防护评估,因此,仅选取可信相关指标,如图 5 所示.

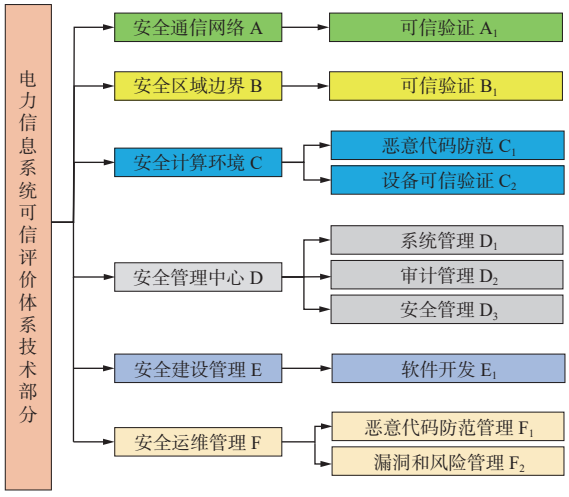

图 5　配电自动化可信防护评价体系

Fig. 5 Reliable protection evaluation system for distribution automation

可信指标体系的评价要素对应关系见表 1.

3.1　安全通信网络指标

安全通信网络指标包括 3 项二级指标:通信网络架构D_3、通信传输D_4、可信验证D_5. 本文仅选取安全通信网络可信验证指标进行评价.

表 1 可信指标对应评价要素

Tab. 1 Corresponding evaluation elements of credible indicators

评价指标	评价要素
安全通信网络	对通信网络层设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证
安全区域边界	系统边界和区域边界,包括网闸、防火墙、交换机、路由器等系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证
安全计算环境	电力信息系统的所有对象,包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等进行可信验证
安全管理中心	对网络运行日志、操作系统日志、数据库访问日志、业务应用系统运行日志、安全设备和系统运行日志的集中收集、定期分析
安全建设管理	实现开发测试环境与实际生产运行环境物理分离,并对开发人员的活动范围和行为实施管控
安全运维管理	按照恶意代码管理制度要求进行恶意代码监测程序和可更新恶意代码库的更新；针对关键业务系统建立补丁升级测试环境,或建立获取已测试补丁的有效渠道

安全通信网络可信验证主要要求:可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证,并在应用程序的关键执行环节进行动态可信验证,在检测到其可信性受到破坏后进行报警,并将验证结果形成审计记录送至安全管理中心.

3.2 安全区域边界指标

依据等级保护 2.0 要求,安全区域边界针对电力信息系统网络边界提出了安全控制要求,主要对象为系统边界和区域边界,包括网闸、防火墙、交换机、路由器等,涉及的安全控制点包括边界防护、访问控制、人侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等多方面内容. 为保证指标评价的效率,本文仅针对安全区域边界可信验证D_8进行评价.

安全区域边界可信验证主要要求:可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证,并在应用程序的关键执行环节进行动态可信验证,在检测到其可信性受到破坏后进行报警,并将验证结果形成审计记录送至安全管理中心.

3.3 安全计算环境指标

安全计算环境针对边界内部提出了安全控制要求,主要对象为电力信息系统的所有对象,包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等,涉及的安全控制点包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份与恢复、剩余信息保护和个人信息保护. 本文针对恶意代码防范D_{10}、安全计算环境可信验证D_{11}进行评估.

(1) 恶意代码防范D_{10}

恶意代码防范的主要要求:应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为,并将其有效阻断.

主动免疫可信验证机制是指在可信根的支撑下,对在计算节点上的所有可执行代码在执行前进行可信验证,计算可信执行代码的哈希值与基准值的比对结果,从而对未知的执行代码进行控制；另一方面,可信验证的动态验证通过周期性或关键行为触发性对业务的执行环境进行可信验证,一旦发现环境受到破坏,如系统调用表、中断表、syscall等内存关键数据被篡改也会触发控制机制进行阻断控制；由此实现对入侵和病毒行为的及时识别和有效阻断.

(2) 可信验证D_{11}

安全计算环境可信验证主要要求:可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证,并在应用程序的关键执行环节进行动态可信验证,在检测到其可信性受到破坏后进行报警,并将验证结果形成审计记录送至安全管理中心.

3.4 安全管理中心指标

安全管理中心是等级保护 2.0 相对 1.0 版本中新增的技术要求,强化安全管理中心的概念,突出安全管理中心在信息安全等级保护建设中的重要性. 安全管理中心可以有效对安全节点进行管理,从安装到运行维护都可以体现安全管理中心的有效管理作用.

参照等级保护 2.0,本文考虑系统管理D_{13}、审计管理D_{14}、安全管理D_{15}这 3 项指标进行评价.

(1) 系统管理D_{13}

系统管理主要要求:应通过系统管理员对系统的资源和运行进行配置、控制和管理,包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备备份与恢复等.

该控制项主要是安全管理中心中系统管理员对系统进行系统资源配置,其中包括“系统资源配置、系统加载和启动”这一条里面就包括对系统可执行的程序和业务软件的配置,这里面涉及在系统启动和加载过程中的可执行代码、程序、业务软件、驱动、函数库、BIOS 程序、操作系统加载器等,涉及对这些可信预期值采集过程,采集的预期值可作为后面安全管理员配置安全管理的依据.

(2) 审计管理D_{14}

审计管理主要要求:应通过审计管理员对审计记录应进行分析,并根据分析结果进行处理,包括根据安全审计策略对审计记录进行存储、管理和查询等.

该控制项主要是审计管理员对系统审计记录进行分析,审计记录包含可信验证过程中的结果记录,包含对启动过程中可信验证的结果记录和对关键执行环节动态可信验证的结果记录. 审计管理员能够制定审计策略,能够对可信验证等安全策略制定相应的审计,例如:全审计、部分审计、审计导出位置频率等.

(3) 安全管理D_{15}

安全管理主要要求:应通过安全管理员对系统中的安全策略进行配置,包括安全参数的设置,主体、客体进行统一安全标记,对主体进行授权,配置可信验证策略等.

该控制项主要是可信安全管理中心中安全管理员对系统进行安全策略配置,其中包括配置可信验证策略,也即是对计算环境、通信网络和区域边界中计算节点的可信验证功能进行策略配置. 可信验证功能由可信根和可信软件基两部分共同完成,所以策略配置涉及可信根的策略配置和可信软件基的策略配置,从而实现在管理中心侧由安全管理员对系统可信验证策略的配置和统一管理. 安全管理中心也是计算节点应该具备可信根支撑的可信验证功能.

3.5　安全建设管理指标

安全建设管理指标包括 3 项二级指标:方案设计及产品使用D_{24}、软件开发D_{25}、测试验收及系统交付D_{26}. 本文仅选取软件开发指标进行评价.

软件开发主要要求如下:应将开发环境与实际运行环境物理分开,测试数据和测试结果受到控制;应制定软件开发管理制度,明确说明开发过程的控制方法和人员行为准则;应制定代码编写安全规范,要求开发人员参照规范编写代码;应具备软件设计的相关文档和使用指南,并对文档使用进行控制;应保证在软件开发过程中对安全性进行测试,在软件安装前对可能存在的恶意代码进行检测;应对程序资源库的修改、更新、发布进行授权和批准,并严格进行版本控制.

3.6　安全运维管理指标

安全运维管理指标包括 4 项二级指标：资产管理D_{27}、设备维护管理D_{28}、恶意代码防范管理D_{29}、漏洞和风险管理D_{30}. 本文仅选取恶意代码防范管理指标与漏洞和风险管理指标进行评价.

(1) 恶意代码防范管理主要要求:应提高所有用户的防恶意代码意识,对外来计算机或存储设备接入系统前进行恶意代码检查等;应定期验证防范恶意代码攻击的技术措施的有效性.

(2) 漏洞和风险管理主要要求:应采取必要的措施识别安全漏洞和隐患,对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补;应定期开展安全测评,形成安全测评报告,采取措施应对发现的安全问题.

4　实例分析

4.1　G1 评价方法

(1) 指标项a_j序关系确认

将指标项$a_j, j=1,2,\cdots,M$进行重要度排序,假设指标项重要度由大到小依次为$a_1 > a_2 > \cdots > a_M$,表示重要度左侧>右侧.

(2) 确定序关系间隔

令$r_{(j-1,j)}=\omega_{(j-1)}/\omega_j$,称$r_{(j-1,j)}$为指标项$\alpha_{(j-1)}$与$\alpha_j$的间隔,衡量指标项间的重要度差值,规定$r_{(j-1,j)}$取值为[1.0　1.2　1.4　1.6　1.8],分别表示指标项$\alpha_{(j-1)}$与α_j相比[同等重要　稍重要　较重要　很重要　极重要]

(3) 建立方程组求解$\omega_j, j=1,2,\cdots,M$,得出各重要度指标项的主观权重. 如式 (1) 所示：

$$\begin{cases}\begin{bmatrix} r_{(1,1)} & r_{(1,2)} & r_{(1,3)} & \cdots & r_{(1,M)} \\ 0 & r_{(2,2)} & r_{(2,3)} & \cdots & r_{(2,M)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & r_{(M-1,M-1)} & r_{(M-1,M)} \end{bmatrix}\begin{bmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_M \end{bmatrix}=\begin{bmatrix} n\omega_1 \\ (M-1)\omega_2 \\ \vdots \\ 2\omega_{(M-1)} \end{bmatrix} \\ \omega_1+\omega_2+\cdots+\omega_M=1 \end{cases} \tag{1}$$

4.2 实例分析

本文相关指标的专家排序及关系间隔如表 2 所示.

表 2 各指标的专家排序及关系间隔

Tab. 2 Expert ranking and relationship interval of each indicator

项目	专家编号	排序	r_2	r_3	r_4	r_5	r_6
一级指标	1	A>C>B>D>E>F	1.8	1.6	1.4	1.2	1.2
	2	A>B>C>E>D>F	1.6	1.4	1.4	1.2	1.2
	3	A>C>B>D>F>E	1.8	1.6	1.4	1.4	1.2
安全通信网络(A)	1	A_1					
	2	A_1					
	3	A_1					
安全区域边界(B)	1	B_1					
	2	B_1					
	3	B_1					
安全计算环境(C)	1	$C_1>C_2$	1.2				
	2	$C_2>C_1$	1.2				
	3	$C_1>C_2$	1.4				
安全管理中心(D)	1	$D_1>D_3>D_2$	1.4	1.6			
	2	$D_3>D_1>D_2$	1.2	1.4			
	3	$D_1>D_3>D_2$	1.2	1.4			
安全建设管理(E)	1	E_1					
	2	E_1					
	3	E_1					
安全运维管理(F)	1	$F_1>F_2$	1.2				
	2	$F_1>F_2$	1.2				
	3	$F_2>F_1$	1.2				

由 G1 法可得,二级指标权重为

$$\omega=\{0.382\,2,0.220\,4,0.080\,4,0.063\,7,0.044\,2,0.034\,9,0.023\,9,0.081\,9,0.037\,2,0.031\,0\} \quad (2)$$

即指标重要度排序为

$$A_1>B_1>E_1>C_1>C_2>D_1>F_1>D_2>F_2>D_3 \quad (3)$$

根据计算结果可知,安全通信网络可信验证指标所占权重最大,为 0.382 2,对系统的重要程度最高. 安全管理指标所占权重最小,为 0.023 9,对系统重要程度最低.

3 个专家分别对该系统的各项指标打分,取出平均值为 92、90、90、86、92、88、94、92、90、88. 则该方案的最终得分为

$$Score=weight\times indexscore=90.69$$

4.3 基于可信计算的配电网安全可信防护机制

4.3.1 设备自身可信验证机制

(1) 基于 Trustzone 的设备自身可信验证

从设备可信根出发,基于密码学和可信验证技术实现整个设备的逐级度量,实现设备自身可信验证,即设备完整性度量[20]. 在 Trustzone 结构下的可信计算完整性度量如图 6 所示,ARM 处理器分为安全世界和非安全世界[21],TCM 功能区位于安全世界中. 其完整性度量过程如图 6 所示.

当系统启动时,先给 TCM 上电,将其内部的可信度量根 (Root of Trust for Measurement,RTM) 作为设备自身可信验证起点,首先对 Boot ROM 进行度量,然后度量 Monitor[22]. 随后分别对安全世界和非安全世

界的 Bootloader、操作系统、软件应用进行度量,逐级传达信任链,实现整个设备的自身可信. 度量结果由 TCM 功能区的平台配置寄存器 (Platform Configuration Register,PCR) 记录,并通过与预存 PCR 值比较,可以判断设备的可信链是否正常扩展,从而达到完整性认证的目的[23].

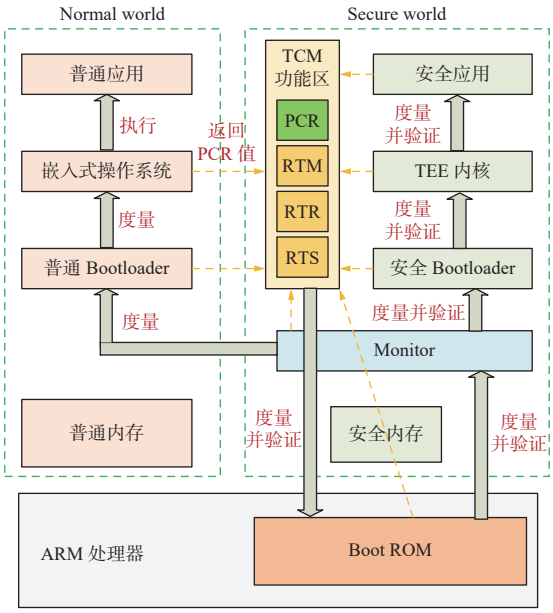

图 6　Trustzone 完整性度量图

Fig. 6 Trustzone integrity measurement diagram

(2) 基于物理不可克隆函数 PUF 的设备自身可信验证

物理不可克隆函数 PUF 利用每个设备芯片独特的物理特性构建不可复制的激励-响应对(Challenge Response Pair,CRP),CRP 可以用于实现轻量级密码学服务. 例如,本文中智能电表、故障检测仪等轻量级设备中,无法外置 TCM 芯片实现完整的可信服务时,可利用 PUF 函数作为唯一标识,确保系统自身可信验证. 在该设计中,针对的是计算能力弱、无内置/外置的 TCM 安全芯片的轻量级终端,其完整性度量过程如下:

当终端设备启动时,终端将设备运行信息作为 PUF 函数的激励 X,将通过 PUF 函数所得结果作为响应 Y,将对应的 $x_i \in X, y_i \in Y$ 记为一个激励-响应对 CRP. 在设备内部,构建一个预设 CRP 集合,通过实时计算激励-响应对与预存值进行对比,若对比一致,则表明设备状态可信,由此可验证基于 PUF 的终端设备的完整性.

4.3.2　设备间可信验证机制

参照可信计算 3.0 中可信网络连接的三元三层架构,搭建出配电网可信网络连接下的三元三层结构,如图 7 所示,其中三元包括连接请求设备、连接应答设备以及安全管理中心.

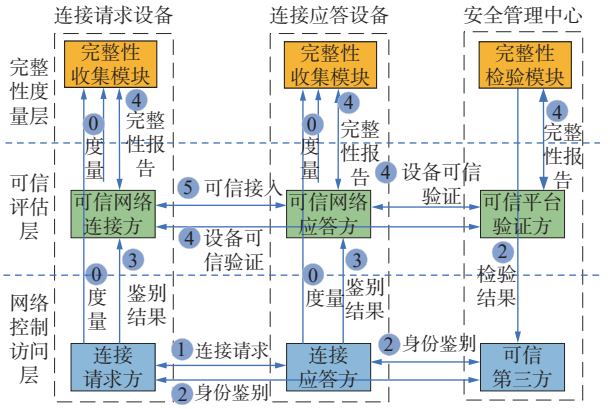

图 7　三元三层可信网络连接

Fig. 7 Three-element three-layer trusted network connection

连接请求设备是请求接入到网络的一方,连接应答设备是应答方. 在可信网络连接建立之前,由双方设备将自身可信报告上传至安全管理中心,安全管理中心依据其内部制定的设备评估策略,验证连接请求设备和连接应答设备的 PKI 证书有效性、平台完整性,并依据验证结果生成身份鉴别和可信平台评估报告及证书. 应答设备依据安全管理中心下发的验证结果及证书判定是否接纳连接请求设备[24]. 该三元三层可信网络连接的具体描述步骤如下:

步骤 1　连接请求设备和连接应答设备依照设备自身可信验证机制生成可信报告 (步骤 3 备用).

步骤 2　在建立可信网络连接之前,先构建用于保密通信的会话通道. 该通道目前仅用于双方实现可信网络连接必要信息的交互,处于受限状态. 连接请求设备向连接应答设备发送访问请求,连接应答设备回应请求,并协商出通信密钥.

步骤 3　连接应答设备在接收访问请求后,由安全管理中心对应答设备和请求设备进行身份鉴别,其中安全管理中心作为第三方可信单位.

步骤 4　连接请求设备将自己身份信息和身份密钥发送给安全管理中心进行比对;连接应答设备将自己身份信息和身份密钥发送给安全管理中心进行比对,安全管理中心根据比对结果反馈身份鉴别结果. 连接双方需依据用户身份鉴别结果对会话通道进行控制.

步骤 5　当连接请求方和连接应答方成功建立通信信道后,双方设备分别将自己身份信息和完整性度量报告发送给安全管理中心进行验证,安全管理中

心执行其内部制定的设备评估策略对双方进行可信评估,完成设备身份鉴别和完整性校验.

步骤 6　安全管理中心最终生成连接请求设备和连接应答设备的可信平台评估结果发送给双方. 连接请求设备和连接应答设备依据安全管理中心的校验结果,判定是否建立可信连接.

5　结束语

针对等保 2.0 落地实施的配电自动化安全防护方案,本文从技术指标和管理指标两个角度,对配电自动化系统安全防护进行了评价. 为了进一步评估出基于可信计算的方案安全性,建立了考虑可信计算的指标综合评价体系,本文采用 G1 赋权法对各项指标进行评价. 最后,基于以上网架模型和评价方法,通过算例分析得出了所建立的各项指标的重要度排序,通过专家对该模型各指标的打分,结合指标项的权重,给出该防护方案的最终评价,验证了模型的合理性,可为今后的新型电力系统安全防护方案提供重要参考依据.

参考文献:

[1] 方禹.《网络安全法》的成就与未来[J]. 中国信息安全, 2020(6): 42-44. DOI: 10.3969/j.issn.1674-7844.2020.06.011.
FANG Y. The achievements and future of the cybersecurity law[J]. China Information Security, 2020(6): 42-44. DOI: 10.3969/j.issn.1674-7844.2020.06.011.

[2] LAVIN A, GILLIGAN-LEE C M, VISNJIC A, et al. Technology readiness levels for machine learning systems[J]. Nature Communications, 2022, 13(1): 6039. DOI: 10.1038/s41467-022-33128-9.

[3] FAN M Y, LIU S Y, XU L Q, et al. Credible pigeon permissioned blockchain traceability platform integrated with IoT based on HACCP[J]. Scientific Reports, 2022, 12(1): 22363. DOI: 10.1038/s41598-022-27065-2.

[4] 郭启全, 张海霞. 关键信息基础设施安全保护技术体系[J]. 信息网络安全, 2020, 20(11): 1-9. DOI: 10.3969/j.issn.1671-1122.2020.11.001.
GUO Q Q, ZHANG H X. Technology system for security protection of critical information infrastructures[J]. Netinfo Security, 2020, 20(11): 1-9. DOI: 10.3969/j.issn.1671-1122.2020.11.001.

[5] 肖安南, 朱宏, 张蔚翔, 等. 电力物联网环境下网络安全防护研究[J]. 电气自动化, 2021, 43(4): 94-97. DOI: 10.3969/j.issn.1000-3886.2021.04.027.
XIAO A N, ZHU H, ZHANG W X, et al. Research on network security protection in the power internet of things[J]. Electrical Automation, 2021, 43(4): 94-97. DOI: 10.3969/j.issn.1000-3886.2021.04.027.

[6] 周泽元, 班秋成, 陶佳冶. 电力系统信息安全的重要性及防护探微[J]. 网络安全技术与应用, 2021(4): 151-152. DOI: 10.3969/j.issn.1009-6833.2021.04.094.
ZHOU Z Y, BAN Q C, TAO J Y. The importance and protection of power system information security[J]. Network Security Technology & Application, 2021(4): 151-152. DOI: 10.3969/j.issn.1009-6833.2021.04.094.

[7] 杨延栋, 刘威麟, 於湘涛. 关于电力监控系统安全防护问题的思考[J]. 通信电源技术, 2018, 35(2): 267-268. DOI: 10.19399/j.cnki.tpt.2018.02.120.
YANG Y D, LIU W L, YU X T. Thinking about the safety and protection of electric power monitoring system[J]. Telecom Power Technology, 2018, 35(2): 267-268. DOI: 10.19399/j.cnki.tpt.2018.02.120.

[8] 方圆, 张永梅, 郭洋. 电力行业移动互联网应用与安全防护分析[J]. 智能城市, 2020, 6(16): 54-55. DOI: 10.19301/j.cnki.zncs.2020.16.025.
FANG Y, ZHANG Y M, GUO Y. Mobile internet applications in the power industry and safety protection analysis[J]. Intelligent City, 2020, 6(16): 54-55. DOI: 10.19301/j.cnki.zncs.2020.16.025.

[9] 陈旭壮. 网络安全等级保护2.0安全体系构建[J]. 中国新通信, 2019, 21(22): 76-77. DOI: 10.3969/j.issn.1673-4866.2019.22.066.
CHEN X Z. Construction of network security level protection 2.0 security system[J]. China New Telecommunications, 2019, 21(22): 76-77. DOI: 10.3969/j.issn.1673-4866.2019.22.066.

[10] 陈晓, 代琪怡. 等级保护2.0下的物联网安全防护措施[J]. 科学技术创新, 2020(3): 80-81. DOI: 10.3969/j.issn.1673-1328.2020.03.047.
CHEN X, DAI Q Y. IoT security protection measures under clarified protection of cybersecurity 2.0[J]. Scientific and Technological Innovation, 2020(3): 80-81. DOI: 10.3969/j.issn.1673-1328.2020.03.047.

[11] 范博, 龚钢军, 孙淑娴. 基于等保2.0的配电物联网动态安全体系研究[J]. 信息网络安全, 2020, 20(11): 10-14. DOI: 10.3969/j.issn.1671-1122.2020.11.002.
FAN B, GONG G J, SUN S X. Research on dynamic security system of distribution IoT based on classified protection of cybersecurity 2.0[J]. Netinfo Security, 2020, 20(11): 10-14. DOI: 10.3969/j.issn.1671-1122.2020.11.002.

[12] 马民虎，赵光. 等级保护与关键信息基础设施保护的竞合及解决路径[J]. 西安交通大学学报(社会科学版)，2018，38(4)：16-22. DOI: 10.15896/j.xjtuskxb.201804003.
MA M H，ZHAO G. The solution of the co-opetition of the gradated protection and the critical information infrastructure protection system[J]. Journal of Xi'an Jiaotong University (Social Sciences)，2018，38(4)：16-22. DOI: 10.15896/j.xjtuskxb.201804003.

[13] 陈广勇，祝国邦，范春玲.《信息安全技术网络安全等级保护测评要求》(GB/T 28448-2019)标准解读[J]. 信息网络安全，2019(7)：1-7. DOI: 10.3969/j.issn.1671-1122.2019.07.001.
CHEN G Y，ZHU G B，FAN C L. Information security technology—evaluation requirement for classified protection of cybersecurity (GB/T 28448-2019) standard interpretation[J]. Netinfo Security，2019(7)：1-7. DOI: 10.3969/j.issn.1671-1122.2019.07.001.

[14] 张伟. 网络安全等级保护在工业控制系统中的应用[J]. 自动化博览，2019，36(S2)：14-18. DOI: 10.3969/j.issn.1003-0492.2019.z1.008.
ZHANG W. Application of cyber security level protection in industrial control system[J]. Automation Panorama，2019，36(S2)：14-18. DOI: 10.3969/j.issn.1003-0492.2019.z1.008.

[15] 詹雄，郭昊，何小芸，等. 国家电网边缘计算信息系统安全风险评估方法研究[J]. 计算机科学，2019，46(S2)：428-432.
ZHAN X，GUO H，HE X Y，et al. Research on security risk assessment method of state grid edge computing information system[J]. Computer Science，2019，46(S2)：428-432.

[16] 贺海，刘海峰，成金爱. 云计算平台安全能力评估体系和评估指标研究[J]. 信息安全研究，2020，6(11)：990-995. DOI: 10.3969/j.issn.2096-1057.2020.11.005.
HE H，LIU H F，CHENG J A. Research on evaluation system and index of cloud computing platform security capability[J]. Journal of Information Security Research，2020，6(11)：990-995. DOI: 10.3969/j.issn.2096-1057.2020.11.005.

[17] 张博凡，郑波，李佳亭. 基于等级保护2.0的电力物联网信息安全质量评估研究[C]//2020中国网络安全等级保护和关键信息基础设施保护大会论文集. 北京：公安部第一研究所，2020：4.
ZHANG B F，ZHENG B，LI J T. Research on information security quality assessment of electric powerIoT[C]//Proceedings of China Clarified Protection of Cybersecurity and Key Information Infrastructure Protection Conference. Beijing：The First Research Institute of the Ministry of Public Security，2020：4.

[18] 李常刚，李华瑞，刘玉田，等. 大电网动态安全风险智能评估系统[J]. 电力系统自动化，2019，43(22)：67-75. DOI: 10.7500/AEPS20190507003.
LI C G，LI H R，LIU Y T，et al. Intelligent assessment system for dynamic security risk of large-scale power grid[J]. Automation of Electric Power Systems，2019，43(22)：67-75. DOI: 10.7500/AEPS20190507003.

[19] HUANG K X，ZHOU C J，TIAN Y C，et al. Application of Bayesian network to data-driven cyber-security risk assessment in SCADA networks[C]//Proceedings of the 27th International Telecommunication Networks and Applications Conference. Piscataway：IEEE，2017：1-6. DOI: 10.1109/ATNAC.2017.8215355.

[20] 龚斯谛，王磊. 基于AHP与信息熵的工控系统信息安全风险评估研究[J]. 工业控制计算机，2017，30(4)：11-12,15. DOI: 10.3969/j.issn.1001-182X.2017.04.005.
GONG S D，WANG L. Cyber security risk assessment for industrial control system based on AHP and information entropy[J]. Industrial Control Computer，2017，30(4)：11-12,15. DOI: 10.3969/j.issn.1001-182X.2017.04.005.

[21] AKSU M U，DILEK M H，TATLI E İ，et al. A quantitative CVSS-based cyber security risk assessment methodology for IT systems[C]//Proceedings of 2017 International Carnahan Conference on Security Technology. Piscataway：IEEE，2017. DOI: 10.1109/CCST.2017.8167819.

[22] 李涛，张驰. 基于信息安全等保标准的网络安全风险模型研究[J]. 信息网络安全，2016(9)：177-183. DOI: 10.3969/j.issn.1671-1122.2016.09.036.
LI T，ZHANG C. Research on network security risk model based on the information security level protection standards[J]. Netinfo Security，2016(9)：177-183. DOI: 10.3969/j.issn.1671-1122.2016.09.036.

[23] 宁华，荣晓燕，刘海峰，等. 网络安全等级保护下的零信任SDP评估方法[J]. 网络安全技术与应用，2021(7)：2-5. DOI: 10.3969/j.issn.1009-6833.2021.07.002.
NING H，RONG X Y，LIU H F，et al. Zero trust SDP evaluation method under clarified protection of cybersecurity[J]. Network Security Technology & Application，2021(7)：2-5. DOI: 10.3969/j.issn.1009-6833.2021.07.002.

[24] 赵小林，曾冲寒，薛静锋，等. 基于TOPSIS的多维网络安全度量模型研究[J]. 北京理工大学学报，2021，41（3）：311-321. DOI: 10.15918/j.tbit1001-0645.2019.269.
ZHAO X L，ZENG C H，XUE J F，et al. A multi-dimensional network security metrics model based on TOPSIS[J]. Transactions of Beijing Institute of Technology，2021，41（3）：311-321. DOI: 10.15918/j.tbit1001-0645.2019.269.

作者简介：

张　磊　男,(1982-),硕士,工程师. 研究方向为电力安全技术.

谷思庭(通讯作者)　男,(1983-),硕士,工程师. 研究方向为电力安全技术. E-mail: xingzhou120@163.com.