《多功能智能杆　网络安全等级保护规范》解读

一、制定背景

标准是构成国家核心竞争力的基本技术要素，是规范经济和社会发展的重要技术制度。习近平总书记提出：“标准决定质量，有什么样的标准就有什么样的质量，只有高标准才有高质量。”

当前，智慧城市的建设与发展迅速，作为近年来新兴的城市公共设施，多功能智能杆整合城市各类基础设施与新型设施，融合多种城市功能，并通过运用信息和通信技术手段感测、分析、整合城市运行系统的各项关键信息，实现城市服务与城市管理的智慧化，是智慧城市的重要载体。

2021 年 2 月 10 日，为了规范多功能智能杆基础设施的管理，有效利用资源，提高城市管理效能和公共服务水平，提升城市品质，维护智慧城市感知网络安全，根据有关法律法规、规章等规定，深圳市人民政府下发《深圳市人民政府关于印发深圳市多功能智能杆基础设施管理办法的通知》(深府规〔2021〕3 号)。通知要求充分发挥深圳信息产业发展特别是 5G 率先独立组网全覆盖的先发优势，坚持高标准规划建设、高水平运营管理，推进多功能智能杆建设，进一步提升城市管理水平，加快实现万物感知、万物互联、万物智能，努力为打造一流智慧城市提供有力支撑。

近年来，随着 5G 技术的迅速发展与新基建进程的加速，多功能智能杆建设正在全国各地蓬勃开展，各地纷纷出台相关建设标准，但是现阶段，多功能智能杆在信息系统安全管理方面尚无相关标准。本文件将为多功能智能杆信息系统安全提供依据，防范对多功能智能杆

网络的攻击、侵入、干扰、破坏和非法使用以及意外事故提出防范应对措施，提升多功能智能杆系统网络数据的完整性、保密性、可用性的能力，助力多功能智能杆产业高质量发展。该标准的编制将对完善我国智慧城市标准体系，助力智慧城市建设具有重要现实意义。

二、目的和意义

“让城市更聪明一些、更智慧一些，是推进城市治理体系和治理能力现代化的必由之路，前景广阔。”习近平总书记的讲话为未来城市的发展指明了道路和方向。

智慧城市是在物联网、云计算、大数据等新一代信息技术快速发展背景下产生的城市发展新模式，通过“更加透彻的感知、更加深入的计算和更加广泛的连接”，改变着物与物之间、人与物之间的联系方式，改变着我们的生存环境，也深刻改变着人类的思维方式和生活模式。

多功能智能杆作为新基建的重要组成和智慧城市建设的入口，也是未来承载5G基站布点的载体，它通过深度整合城市各类资源，实现资源的共享、集约和统筹，降低城市建设成本，提升城市运维效率，将为城市治理的快速发展带来多重效益。

2018年深圳出台《深圳市多功能智能杆建设发展行动计划（2018—2020年）》，成为国内首个政府出台的顶层行动计划。

2019年9月，《深圳市人民政府关于印发率先实现5G基础设施全覆盖及促进5G产业高质量发展若干措施的通知》印发，要求加快推进多功能智能杆建设。

2020年4月，国家发改委明确“新基建”范围主要包括：包含以

5G、物联网为代表的信息基础设施，以大数据、人工智能等技术深度应用的融合基础设施和以支撑科学研究、技术开发等的创新基础设施。随着我国物联网新型基础设施建设的全面推进，多功能智能杆的产业发展步入快车道。

2021 年我国多功能智能杆建设的最大特点是从北上广深延伸到了全国各地，2021 年度共有 28 个省（自治区、直辖市）新增了多功能智能杆建设项目，新增项目总量达到 350 个，新增多功能智能杆拟建数量达到 12.8 万根。

多功能智能杆系统包括杆体及其搭载的感知终端（各类设备和传感器），它是集智慧照明、视频监控、交通管理、环境监测、无线通信、应急求助等多功能于一体的信息基础设施。梳理和分析多功能智能杆系统之间的数据流通路径，将系统中不同设备、软件、数据、资源、分不同重要等级进行分等级保护显得尤为重要。

近年来，网络安全形势不容乐观，世界各国均高度重视网络安全，例如美国发布了《网络安全信息共享法》，欧盟发布了《一般数据保护法案》、德国发布了《联邦数据保护法》、英国发布了《数据保护法》等；十九届四中全会，我国首次增列“数据”作为生产要素，数据安全与国家安全息息相关。我国国家数据安全相关法律法规有《中华人民共和国网络安全法》《中华人民共和国数据安全法》及《中华人民共和国个人信息保护法》等；国内数据安全标准有 GB/T 35273—2020《信息安全技术　个人信息安全规范》、GB/T 37988—2019《信息安全技术　数据安全能力成熟度模型》等。

习近平总书记高度重视信息网络安全工作，多次提出：没有网络

安全就没有国家安全，没有信息化就没有现代化；网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进。

多功能智能杆系统网络是指由计算机及其相关和配套的挂载设备、设施构成的，按照一定的应用目标和规则对信息进行存储、传输、处理的系统或者网络；信息是指在信息系统中存储、传输、处理的数字化信息。

多功能智能杆系统网络安全是指在政府主导和社会参与下，综合运用技术、法律、管理、教育等手段，在信息空间积极应对敌对势力攻击、网络犯罪和意外事故等多种威胁，有效保护信息基础设施、信息系统、信息应用服务和信息内容的安全，为经济发展、社会稳定、国家安全提供安全保障的活动。

三、主要内容

本文件包括9章，8个附录，分别为范围、规范性引用文件、术语和定义、缩略语、基本要求、第一级安全要求、第二级安全要求、第三级安全要求、第四级安全要求、附录A（规范性） 安全要求的选择和使用 、附录B（规范性） 等级保护对象整体安全保护能力的要求、附录C（规范性） 等级保护安全框架和关键技术使用要求、附录D（规范性） 管理平台应用要求、附录E（规范性） 移动互联应用场景要求、附录F（规范性） 挂载设备应用场景要求 、附录G（规范性） 密码模块安全技术要求、附录H（规范性） 可信验证要求。

1 范围

本文件规定了多功能智能杆的网络安全等级保护的基本要求、第一级安全要求、第二级安全要求、第三级安全要求和第四级安全要求。

本文件适用于多功能智能杆非涉密对象的网络安全等级的建设和运营管理。

2 规范性引用文件

本文件在制定过程中规范性引用了下列标准：

GB/T 20269—2006 信息安全技术 信息系统安全管理要求

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 28181—2022 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 37025—2018 信息安全技术 物联网数据传输安全技术要求

GB/T 37092—2018 信息安全技术 密码模块安全要求

GB/T 37932—2019 信息安全技术 数据交易服务安全要求

GB/T 39477—2020 信息安全技术 政务信息共享 数据安全技术要求

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

GA/T 1049.3—2013 公安交通集成指挥平台通信协议 第3部分：交通视频监视系统

GA/T 1400.4—2017 公安视频图像信息应用系统 第4部分：接口协议要求

DB4403/T 271—2022 公共数据安全要求

3 术语和定义

3.1 多功能智能杆

通过挂载各类设备提供智能照明、移动通信、城市监测、交通管理、信息交互和城市公共服务等多种功能，并可通过管理平台进行远程监测、控制、管理、校时、发布信息的杆。

3.2　多功能智能杆系统网络

集智能照明、视频采集、移动通信、交通管理、环境监测、气象监测、无线电监测、应急求助和信息交互等诸多功能于一体的复合型公共基础设施网络。

3.3　安全保护能力

能够抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态等的程度。

3.4　管理平台

根据多功能智能杆应用场景和数据业务以及安全要求的不同，对各挂载设备业务进行汇聚和分配、远程集中管理、控制、运行监测、数据分析、查询和定位，实现统一管理和运维，保障设备安全运行的系统。

3.5　平台服务商

多功能智能杆管理平台的供应方。

3.6　平台服务客户

为使用管理平台服务同平台服务商建立业务关系的参与方。

3.7　宿主机

运行虚拟机监视器的物理服务器。

3.8　移动互联

采用无线通信技术将移动终端接入有线网络的过程。

3.9　移动终端

在移动业务中使用的终端设备。

3.10　无线接入设备

采用无线通信技术将移动终端接入有线网络的通信设备。

3.11　移动应用软件

针对移动终端开发的应用软件。

3.12　等级保护对象

多功能智能杆网络安全等级保护工作直接作用的对象。

3.13　外部网络

多功能智能杆网络中等级保护对象之外的网络。

3.14　公共数据

公共管理和服务机构及处理大量个人信息的服务平台在依法履行公共管理职责或者提供公共服务过程中产生、处理的数据。

3.15　敏感数据

被不当处理或泄露将对个人、组织或社会造成严重危害的数据。

3.16　数据安全

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

3.17　挂载设备

挂载在多功能智能杆上，对物体或环境进行信息采集和/或执行操作，或能联网进行通信的装置。

3.18　边缘控制器

将挂载设备所采集的数据进行汇总、适当处理或数据融合，并进

行转发通信的装置。

3.19　密码模块

能完成密码运算功能并提供调用接口，相对独立的软件或硬件装置。

4　缩略语

列出了本文件中使用的AP、BIOS、COM、CPU、DDoS、HTTPS、IaaS、IP、IPv4、IPv6、PaaS、RJ45、SaaS、SPI、SSH、SSID、TCB、TCP、TPCM、UDP、VPN、WEP、WPS共23个缩略语。

5　基本要求

5.1　等级保护对象定级

本条规定了多功能智能杆网络安全四个安全保护等级的划分要求。

5.2　不同等级的安全保护能力

本条规定了多功能智能杆网络安全四个安全保护等级的安全保护能力。

5.3　安全通用要求

本条规定了多功能智能杆网络安全四个安全保护等级的安全通用要求。

5.4　安全扩展要求

本条规定了多功能智能杆网络安全四个安全保护等级的安全扩展要求。

5.5　密码模块安全要求

本条规定了多功能智能杆网络安全四个安全保护等级的密码模块安全要求。

6 第一级安全要求

6.1 安全通用要求

本条规定了安全通用要求中的安全通信网络、安全区域边界和安全计算环境的具体要求。

6.2 管理平台安全要求

本条规定了管理平台安全中的安全通信网络、安全区域边界和安全计算环境的具体要求。

6.3 移动互联安全要求

本条规定了移动互联安全中的安全区域边界和安全计算环境的具体要求。

6.4 挂载设备安全要求

本条规定了挂载设备安全中的安全物理环境、安全区域边界和安全运维管理的具体要求。

6.5 公共数据基本安全要求

本条规定了公共数据基本安全中的数据收集基本安全、数据存储基本安全、数据传输基本安全、数据使用基本安全、数据加工基本安全、数据开放共享基本安全、数据交易基本安全、数据出境基本安全和数据销毁与删除基本安全的具体要求。

7 第二级安全要求

7.1 安全通用要求

本条规定了安全通用要求中的安全通信网络、安全区域边界和安全计算环境的具体要求。

7.2 管理平台安全要求

本条规定了管理平台安全要求中的安全通信网络、安全区域边界和安全计算环境的具体要求。

7.3　移动互联安全要求

本条规定了移动互联安全要求中的安全区域边界和安全计算环境的具体要求。

7.4　挂载设备安全要求

本条规定了挂载设备安全要求中的安全物理环境、安全区域边界和安全运维管理的具体要求。

7.5　公共数据基本安全要求

本条规定了公共数据基本安全中的数据收集基本安全、数据存储基本安全、数据传输基本安全、数据使用基本安全、数据加工基本安全、数据开放共享基本安全、数据交易基本安全、数据出境基本安全和数据销毁与删除基本安全的具体要求。

8　第三级安全要求

8.1　安全通用要求

本条规定了安全通用要求中的安全通信网络、安全区域边界、安全计算环境和安全管理中心的具体要求。

8.2　管理平台要求

本条规定了管理平台安全要求中的安全通信网络、安全区域边界、安全计算环境和安全管理中心的具体要求。

8.3　移动互联安全要求

本条规定了移动互联安全要求中的安全区域边界和安全计算环境的具体要求。

8.4　挂载设备安全要求

本条规定了挂载设备安全要求中的安全物理环境、安全区域边界、安全计算环境和安全运维管理的具体要求。

8.5　公共数据基本安全要求

本条规定了公共数据基本安全中的数据收集、数据存储、数据传输、数据使用、数据加工、数据开放共享、数据交易、数据出境和数据销毁与删除的具体要求。

8.6　公共数据三级增强安全要求

本条规定了公共数据三级增强安全中的数据收集、数据存储、数据传输、数据使用、数据加工、数据开放共享、数据交易、数据出境和数据销毁与删除具体要求。

9　第四级安全要求

9.1　安全通用要求

本条规定了安全通用要求中的安全通信网络、安全区域边界、安全计算环境和安全管理中心的具体要求。

9.2　管理平台要求

本条规定了管理平台安全要求中的安全通信网络、安全区域边界、安全计算环境和安全管理中心的具体要求。

9.3　移动互联安全要求

本条规定了移动互联安全要求中的安全区域边界和安全计算环境的具体要求。

9.4　挂载设备安全要求

本条规定了挂载设备安全要求中的安全物理环境、安全区域边界、

安全计算环境和安全运维管理的具体要求。

9.5　公共数据基本安全要求

本条规定了公共数据基本安全中的数据收集、数据存储、数据传输、数据使用、数据加工、数据开放共享、数据交易、数据出境和数据销毁与删除的具体要求。

9.6　公共数据四级增强安全要求

本条规定了公共数据四级增强安全中的数据收集、数据存储、数据传输、数据使用、数据加工、数据开放共享、数据交易、数据出境和数据销毁与删除具体要求。

附录A（规范性）　安全要求的选择和使用

本附录规定了网络安全等级保护中的保护对象的差异、定级结果的组合、保护措施的选择、安全要求的标识和安全要求的调整和补充的具体要求。

附录B（规范性）　等级保护对象整体安全保护能力的要求

本附录规定了网络安全等级保护对象整体安全保护能力的总体要求和安全措施要求。

附录C（规范性）　等级保护安全框架和关键技术使用要求

本附录规定了网络安全等级保护安全框架和关键技术使用中的总体要求、工作内容要求、等级保护安全要求和关键技术使用要求。

附录D（规范性）　管理平台应用要求

本附录规定了不同管理平台的服务模式架构图、不同服务模式下管理平台的组成、安全管理责任。

附录E（规范性）　移动互联应用场景要求

本附录规定了移动互联应用场景中的移动互联应用场景架构和移动互联应用场景安全扩展要求。

附录F（规范性）　挂载设备应用场景要求

本附录规定了挂载设备应用场景中的多功能智能杆应用场景、多功能智能杆部件组成、管理平台架构和挂载服务的具体要求。

附录G（规范性）　密码模块安全技术要求

本附录规定了密码模块安全技术要求中的安全一级、安全二级、安全三级和安全四级的具体要求。

附录H（规范性）　可信验证要求

本附录规定了可信验证要求中的功能框架和可信验证硬件改造示例。