长擎安全操作系统 24

产品白皮书

北京长擎软件有限公司

二〇二四年十二月

目 录

1 产品概述

“十四五”规划指出坚持创新在我国现代化建设全局中的核心地位，把科技自立自强作为国家发展的战略支撑。习近平总书记强调，核心技术是国之重器，要下定决心、保持恒心、找准重心，加速推动信息领域核心技术突破。

在我国，由于工业控制系统基础弱，大部分控制系统被国外垄断，受制于人，国外厂商完全有能力、有手段对正在我国运行的工业控制系统进行远程操控，或者获取机密数据。再加上新基建下的工业互联网的大力发展，必然导致工业控制系统的广泛互联，如果不进行安全有力的保障措施必然给国外的黑客组织、敌对势力带来攻击的机会。

操作系统是管理计算机和网络的中枢神经，是整个信息系统大厦的墙基，是网信产业的地基。根基不牢，地动山摇，重要性、挑战性不言而喻。可喜的是，经过 30 年的持续深耕和产业化道路探索后，国产操作系统已经在天问一号、嫦娥五号等“大国重器”中交出了满意的答卷!

长擎安全操作系统 24 是北京长擎软件有限公司推出的工控安全操作系统品牌。长擎安全操作系统 24 基于 linux 内核 5.10.92 版本，依据 GB/T20272 -2019 第四级安全保护需求，遵循软件工程开发过程思想，采用 Flask 安全体系结构实现系统安全功能的结构化、复杂度最小化，打造工控领域系统安全底座。

2 产品特点

长擎安全操作系统 24 结合了操作系统安全技术与可信计算技术，具有高安全级的保障措施，系统实现了：身份标识与鉴别、细粒度的自主访问控制、强制访问控制、基于角色访问控制、可信路径、禁止客体重用、安全审计、安全数据保护、文件完整性检查等安全机制。此外，系统还实现了基于国密 TPM2.0 的可信引导、可信启动、进程运行控制、基于国密 TPM2.0 的身份认证等可信功能，并设计实现了安全控制中心，用于管理配置这些安全功能。

1. 升级移植身份标识与鉴别、细粒度自主访问控制、基于角色的强制访问控制、基于 IAC 的强制访问控制、基于 MLS 的强制访问控制、可信路径、禁止客体

重用、安全审计、文件完整性检查等安全功能。

2. 基于国密 TPM2.0 的系统可信引导。在 grub 阶段采用国密 TPM2.0 芯片对系统内核镜像、initrd 和启动配置文件进行度量；同时也可采用国密 TPM2.0 芯片在 grub 阶段通过 CPU 和国密 TPM2.0 对内核镜像、initrd 和启动配置文件进行度量，保证启动系统的可信性。
3. 系统可信启动。通过可信内核模块在启动过程中对启动的所有进程的可执行文件进行度量，并扩展到可信芯片 PCR 中，并保证各程序启动顺序一样，实现系统启动后整个系统运行环境的可信。
4. 进程运行控制，通过可信内核模块在所有程序运行之前度量可执行文件的内容是否被更改，若被更改则拒绝程序运行，并提供可恢复该文件的功能。
5. 基于国密 TPM2.0 的可信身份认证，登录认证利用国密 TPM2.0 可信芯片实现三权用户的本地登录，其中使用了可信芯片的杂凑运算和 NV 存储功能。其把传统的登录认证方式和国密 TPM2.0 可信芯片结合起来。登录认证把密码信息由传统的文件存储转为由可信芯片的 NV 空间存储，并且实现利用可信芯片对密码信息进行杂凑运算。
6. 系统实现了多种 CPU 架构支持，同源兼容 x86_64、LoongArch64、AArch64、sw_64、MIPS64 等架构。

3 产品系统结构

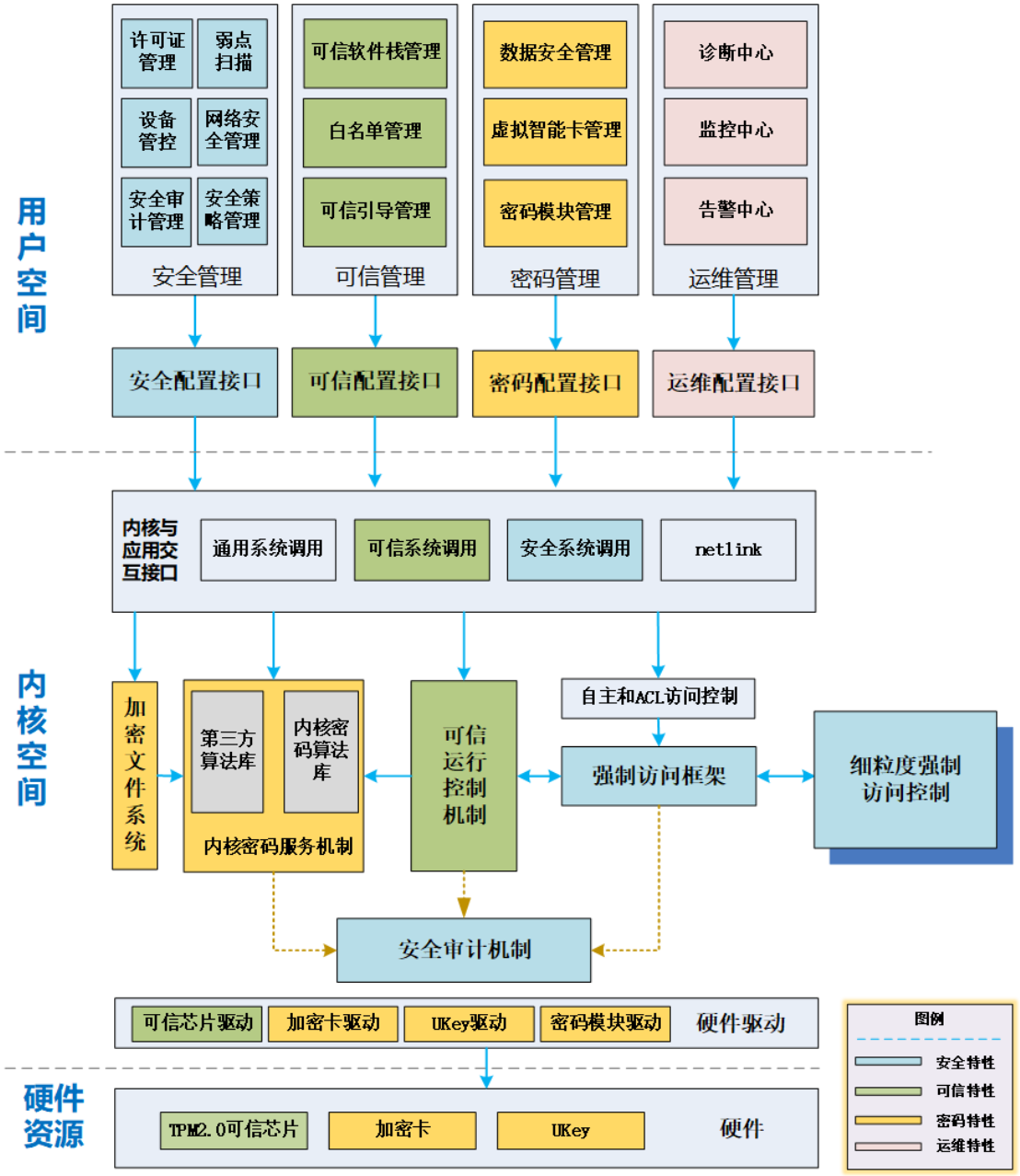

图 1 系统结构

产品系统结构如上图所示，系统基于底层国密 TPM2.0 可信硬件实现对系统的安全增强。在系统内核层实现可信运行控制机制检测所有应用的完整性，同时也为应用提供了可信支撑接口用于调用可信芯片资源来增加应用自身安全性。在系统上层提供了安全管理、可信管理、密码管理、运维管理等。

4 产品功能

长擎安全操作系统 24 参照标准《GB/T 20272-2019 操作系统安全技术要求》进行设计开发。为了从根本上完善系统安全措施，系统针对网络化环境下信息安全攻击技术特点，研究能有效防御缓冲区溢出攻击、病毒攻击的特色技术，并采取缺省安全、简化安全配置等措施，增强安全操作系统的易用性。保障信息处理系统的安全是长擎安全操作系统 24 的主要任务。长擎安全操作系统 24 在安全设计方面采用内核与应用一体化的安全机制，采用多策略与动态策略的安全框架，支持以模块化方式实现安全策略，提供多种访问控制策略的统一平台。

长擎安全操作系统 24 从多个方面提供安全保障，提供了身份认证、细粒度的自主访问控制、安全标记、最小特权、客体重用、可信路径、三权分立、强制访问控制和安全审计等安全功能，为用户提供了从内核到应用的全方位安全防护。

长擎安全操作系统 24 符合 Posix 系列标准，并兼容 Linux 目标代码，Linux 平台上的大型应用如图形环境、oracle 数据库服务等都可以直接运行在长擎安全操作系统 24 平台上，有力拓广了长擎安全操作系统 24 的应用面。长擎安全操作系统 24 可应用在能源、管网、电力等领域，有效保证了控制系统的底层安全。

4.1 安全子系统

安全子系统是操作系统中的重要组成部分，长擎安全操作系统从多个方面提供安全保障，保护系统不受恶意软件和攻击的影响，以及确保数据的完整性和机密性。长擎安全操作系统提供了身份认证、细粒度的自主访问控制、三权分立、安全标记、最小特权、客体重用、强制访问控制、设备安全管控、和安全审计等安全功能，为用户提供了从内核到应用的全方位安全防护。

4.1.1 身份认证

身份认证是长擎安全操作系统的主要安全机制之一，身份认证必须准确鉴别用户的身份，以便为访问控制和安全审计打下坚实的基础。长擎安全操作系统采用了多种系统登录限制手段加强系统的安全性，其中最主要的手段就是通过口令和 Ukey 相结合的双重认证机制来判定一个用户是否是合法的系统用户。其主要

设计思想是，系统利用 PAM 可插入模块验证机制，把密码和 Ukey 验证模块组合成一套成熟的验证体系，使得系统在登录验证时先后通过密码和 Ukey 的身份认证。双重身份认证中如有一项验证不通过，则系统就会判定登录失败。

4.1.2 用户能力

CAP 能力机制的主要思想在于分割 root 用户的特权，即将 root 的特权分割成不同的能力。每一种能力代表一定的特权操作，如 CAP_SYS_MODULE 表示能够加载（或卸载）内核模块操作的特权操作，CAP_SETUID 表示能够修改进程用户身份的特权操作。在 CAP 能力机制中，系统将根据进程拥有的特权来进行特权操作的访问控制。

CAP 策略模块的结构，包括 CAP 属性存储、CAP 能力计算、CAP 访问控制，并提供外部接口，供 RBAC 框架和安全管理工具使用；其中 CAP 属性存储是核心，它为 CAP 能力计算和访问控制提供依据，同时外部接口也是针对 CAP 属性存储。

4.1.3 强制访问控制

访问控制是操作系统安全重要的组成部分，系统在自主访问控制（DAC）基础上结合完整性访问控制（IAC）、基于角色的访问控制（RBAC）和多级安全策略（MLS）的强制访问控制，采用混合模型全面保障系统安全。

系统整个访问控制流程如下图所示：

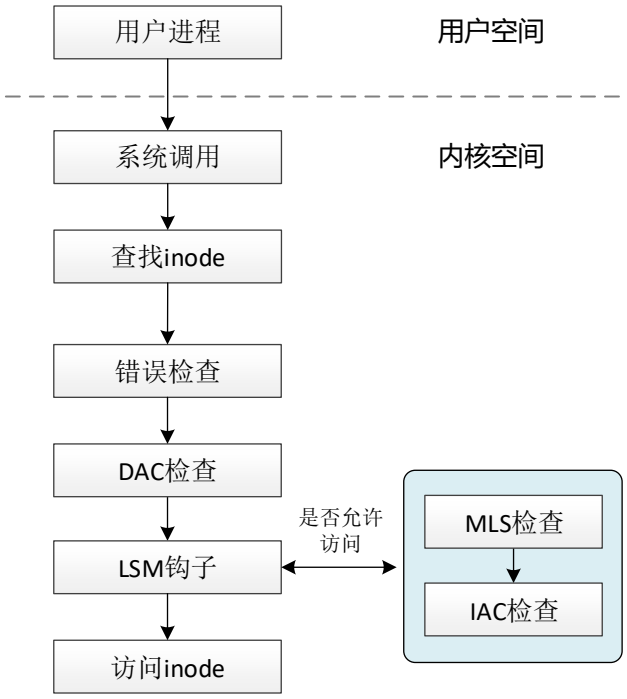

图 2 访问控制流程

当主体访问客体时需要经过一系列的检查之后才能访问成功，用户进程通过系统调用查找到客体的 inode 节点，基本的错误检查通过后，再经自主访问控制（DAC）的权限检查，之后又通过 LSM 进程强制访问控制检查，其中先检查 MLS 机密性，再检查 IAC 完整性，只有所有的检查都通过后，最后才能访问这个客体。

4.1.4 安全审计

安全审计系统提供了一种记录系统安全信息的方法，为审计管理员在用户违反系统安全法则时提供及时的警告信息。审计系统可以将记录系统内部发生的事件的信息根据用户的需求，提供不同的报表功能，从而实现对系统信息的追踪、审查、统计和报告等功能。审计系统的审计信息包括：可被审计的事件名称、事件状态（成功或失败）和安全信息等。

4.1.5 设备管控

为了对操作系统中的设备进行统一配置管理，以及增加设备的可扩展性，在设备管控决策模块引入了设备统一管理配置操作模型。设备管控通过多种机制实现对设备的全域管控能力。

4.1.6 许可证

激活码：激活码由用户购买产品后获得，可以在安装操作系统时导入，也可以在操作系统就绪后导入，激活码附带用户的使用权限、用户、时间等信息。证书：证书通过激活码换取，由证书携带更复杂的信息，通过证书校验来激活操作系统。

二维码：通过终端界面 unicode 展示操作系统二维码信息，用户可以使用手机等具有网络与摄像头功能的设备，直接扫描二维码获取证书。

批量激活：只需要部署批量激活程序的服务器与总服务器能够通信，便可通过提供的批量激活软件一次性激活一定数量的设备。

4.2 可信子系统

可信子系统是操作系统的核心组成部分之一，旨在确保操作系统运行在安全可信的环境内，并为操作系统中的用户提供基于可信计算的数据安全功能。本文档将详细描述可信子系统的各个方面，包括可信引导、可信度量和可信加密文件系统。

4.2.1 可信路径

为防止因计算机启动相关文件被篡改而导致的系统破坏，BootLoader 可信引导模块提供对启动过程中涉及的引导程序和引导文件进行度量验证，防止使用不可信的配置程序或文件启动。同时提供初始化、更新启动过程相关的预期度量值功能，允许用户关闭 BootLoader 可信引导模块。

BootLoader 可信引导模块使用 TPM2.0 可信芯片存储度量基准值，并对加载的内核镜像、根文件系统镜像以及设备描述信息进行完整性度量验证，保证操作系统引导过程中的安全可信。

4.2.2 可信度量

可信度量模块基于预编写的策略工作，在基准数据库生成时，会根据策略文件中的规则读取指定的文件，同时生成该文件的数字签名并存贮在可信度量模块的数据库中。可信度量模块提供了国密 SM3 算法用来生成签名。进行完整性检查时，可信度量模块会根据策略文件中的规则对指定的文件重新生成一次数字签

名，并将此签名与存贮在数据库中的签名做对照。如果完全匹配，则说明文件没有被更改。如果不匹配，说明文件被改动了。

4.2.3 可信加密文件系统

可信加密文件系统，利用 ecryptfs 文件系统实现，利用 TPM2.0 可信芯片和国密算法，实现密码合规以及安全可信的加密文件系统功能。

该功能的主要功能特点如下：

（1）可信加密文件系统的密钥信息由 TPM2.0 可信芯片进行加密保护，提高了加密文件系统的破解难度；

（2）可信加密文件系统中的文件由 SM4 国密算法进行加密保护，满足密码合规性要求。

4.3 密码子系统

密码技术已经是国家网络信息安全重要的“护城河”，而密码国产化，也就成为具有战略意义的大事。特别是在关系到国计民生的工业控制领域，采用国密算法或行业自主密码体制已经逐渐成为一种趋势，它对于维护国家主权安全、维护客户利益、保护数据安全、防止各种针对性网络攻击，推动我国信息安全产业发展具有十分重要的意义。

为实现工控领域密码算法的自主可控，防止采用国际公开算法而导致的安全风险，通过将国密算法默认集成到操作系统中，内核层支持 SM3 和 SM4 国密算法，应用层 OpenSSL 支持国密算法调用、虚拟智能卡模拟以及类 SDF 算法库接口调用，从而为工控应用全面提供安全可靠的国密算法支撑。

4.3.1 虚拟智能卡

虚拟智能卡用软件来模拟 IC 卡功能，它参照 PKCS15 规范和 ISO7816 规范进行设计实现。其借助 TPM2.0 物理芯片创建虚拟的 Smart Card 智能卡设备，并在用户层提供相应的接口。

虚拟智能卡主要实现以下功能：

（1）使用 TPM2.0 物理芯片来虚拟智能卡设备；

（2）提供管理虚拟智能卡的系统服务；

（3）提供 APDU 指令集接口和二次开发接口。

4.3.2 类 SDF 算法库

类 SDF 算法库参照 GM/T 0018-2012《密码设备应用接口规范》接口，使用 openssl 和操作系统内核提供的随机数熵文件，为操作系统中的用户或者应用程序提供完整的国密 SDF 调用接口。

类 SDF 库算法模块通过 SDF 密码设备的虚拟化机制，为操作系统应用层提供完整的国密 SDF 密码设备调用接口。通过利用并发调度计算、随机数产生池、软件算法模块、安全内存以及加密通信等技术实现。

4.4 运维子系统

运维组件设计建立一个集群运维监控系统，集成各种监控、告警、故障分析等功能，以实现自动化和智能化的运维管理。该组件应具备预警、快速定位故障、实时监控等功能。

4.4.1 系统管理

采用 RBAC（Role-Based Access Control）权限模型，通过用户关联角色，角色关联权限的方式间接赋予用户权限，增加权限设置的扩展性。不同的账户登录系统能看到不同的页面，执行不同的功能。

4.4.2 安全中心

安全中心模块主要包含漏洞及修复管理功能，同时提供了一键扫描和统计功能，以方便管理员快速了解系统的安全状况。

安全中心模块主要实现漏洞信息爬取、主机漏洞扫描和主机漏洞修复等功能。

（1）漏洞库配置：通过前端界面配置漏洞库地址，系统可从该地址获取漏洞详细信息；

（2）漏洞扫描流程：通过扫描主机，发现主机存在的漏洞，然后获取相应的漏洞补丁信息；

（3）漏洞修复：通过 ssh 命令调用漏洞修复指令：dnf update --cve {} -y；

4.4.3 诊断中心

诊断中心模块提供了对系统健康和性能的全方位诊断功能，以便管理员及时发现并解决可能影响系统稳定性和性能的问题。

4.4.4 监控中心

监控中心提供被管系统各项性能指标数据，以便管理员能够掌握被管系统的运行状况，以及异常问题历史回溯。

4.4.5 告警中心

告警中心提供对关键性能指标阈值告警，管理员可以自定义告警阈值以及配置邮箱转发规则，当达到阈值时，告警中心产生告警并且通过邮件转发告警。

4.4.6 备份管理

备份管理主要针对本组件的数据库进行定时备份操作，包含全量备份、增量备份和定时任务设置。

主要通过 mysqldump 进行全量备份，mysqladmin 进行增量备份。然后通过定时任务进行调用相关的备份操作，然后把相关的备份记录到数据库中。

4.5 产品服务

北京长擎软件有限公司已建立北京、郑州等地区域原厂服务中心，为用户提专业化的技术服务。能够满足用户快速响应、及时处理并修复问题的要求，还可以按照用户的个性化需求提供订制服务，满足不同用户在各复杂业务应用场景的需要。

服务类型	服务范围
远程服务	升级服务：定期发布系统安全与功能升级补丁； 在线服务：网络热线直连或留言响应； Bug 修复服务：在线 Bug Case 报告与

	跟踪支持； 电话支持服务：5×8 或 7×24 小时电话响应； 邮件支持服务：响应用户反馈邮件。
现场服务	部署服务：批量部署服务支持； 巡检服务：定期用户使用情况巡检； 应急服务：现场应急响应与事件处理。
培训服务	使用培训：长擎安全操作系统 24 的用户使用培训； 管理培训：面向服务器操作系统管理员的安装、运维、排错等技能培训 ； 研发培训：基于国产与开源操作系统下的多种研发技术培训。
定制服务	系统定制服务：根据用户需求对操作系统镜像进行定制； 迁移研发服务：其他操作系统到长擎安全操作系统 24 的应用迁移研发级支持。

5 联系我们

北京长擎软件有限公司

Beijing Changqing Software Co.,Ltd

地址：北京市海淀区闵庄路 3 号四季慧谷 3#3 层

官网：https://www.cqsoftware.com.cn/