



# 基于openeuler的工控行业可信解决方案

---

[www.linux-info.com](http://www.linux-info.com)

北京凝思软件股份有限公司



# 01 / 简介

## 简介

凝思基于欧拉系统推出了面对工控行业的可信解决方案，实现了操作系统层面的可信安全增强，满足通用服务器、嵌入式设备等终端设备的可信计算需求，提升了系统整体的安全性和合规性。





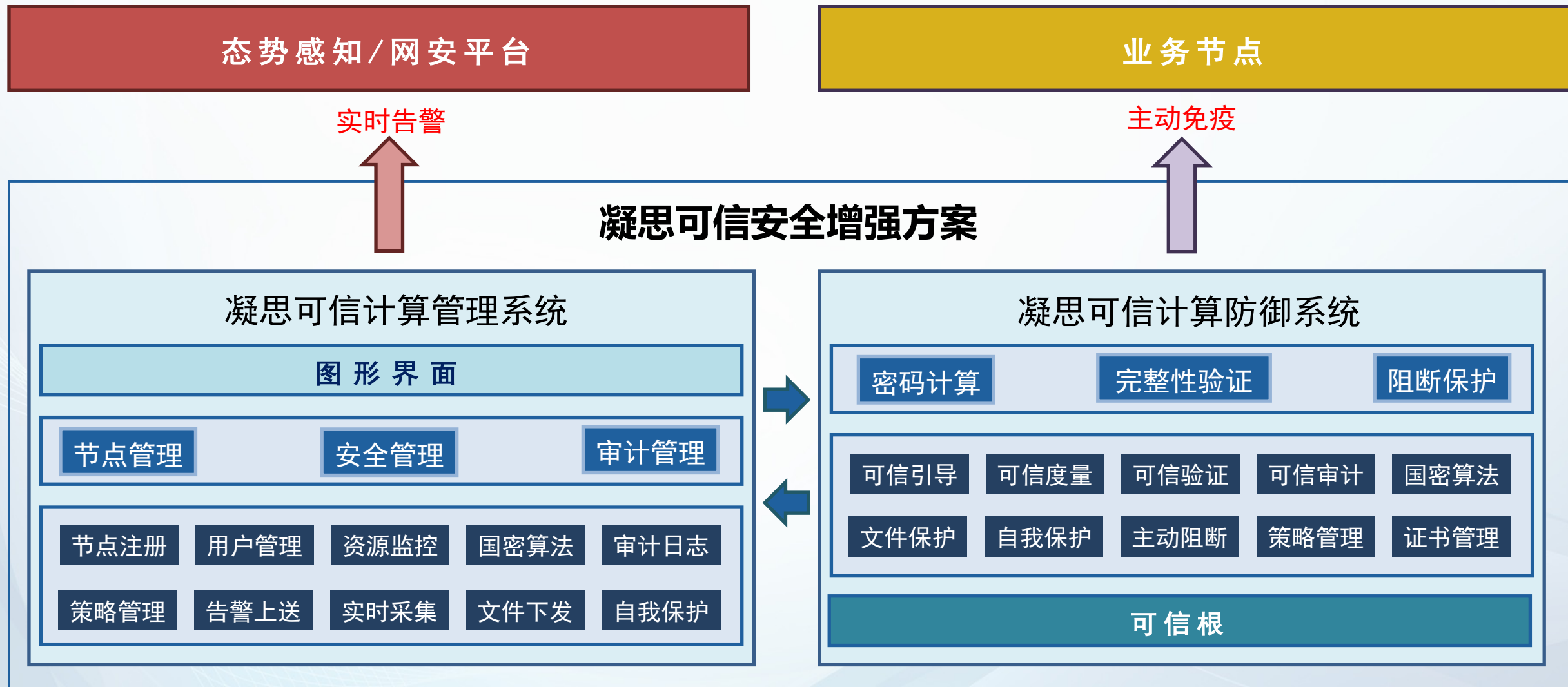
# 02 / 方案介绍

## 方案介绍

凝思的可信解决方案以可信计算为核心技术，通过在系统层部署凝思自研的可信计算防御系统软件，在核心终端上构建操作系统层面的可信环境，实现基于密码计算的系统完整性保护，保障操作系统从引导到系统服务和应用程序启动全过程的可信度量与验证。支持主动阻断并告警危险行为，为业务终端提供主动防御机制，提升系统整体的安全性、稳定性和合规性。



# 架构






# 03 / 功能介绍




# 凝思可信计算防御系统




## 可信根

支持软件可信根和硬件可信根




## 可信引导

对操作系统引导阶段时关键文件、启动盘、程序进行可信验证，验证失败，阻止系统启动



## 静态度量

所有类型文件皆可静态度量，主动阻断篡改、删除操作行为，形成审计和告警信息




## 动态度量

周期验证程序运行时代码段、只读数据段，验证失败，根据策略阻止运行或继续运行，形成审计记录并告警



## 可信白名单

可信白名单功能实现了对未知程序的免疫，在可信白名单外的程序尝试运行时，阻止其运行。



## 签名验签

支持签名验证，基于数字证书签名的应用程序验证成功后即自动添加可信属性




## 实时备份

备份关键文件，并实时更新，确保安全的同时，内容保持同步



## 基准库保护

可信基准库具有持久化存储能力，基于国密算法加密存储，避免可信自身关键数据出现安全隐患




## 独立运行

可信节点离线管理平台时，支持策略单独配置，同时依然能正常提供可信度量和验证




# 凝思可信计算防御系统




## 可信根

支持软件可信根和硬件可信根




## 可信引导

对操作系统引导阶段时关键文件、启动盘、程序进行可信验证，验证失败，阻止系统启动



## 静态度量

所有类型文件皆可静态度量，主动阻断篡改、删除操作行为，形成审计和告警信息




## 动态度量

周期验证程序运行时代码段、只读数据段，验证失败，根据策略阻止运行或继续运行，形成审计记录并告警



## 可信白名单

可信白名单功能实现了对未知程序的免疫，在可信白名单外的程序尝试运行时，阻止其运行。



## 签名验签

支持签名验证，基于数字证书签名的应用程序验证成功后即自动添加可信属性




## 实时备份

备份关键文件，并实时更新，确保安全的同时，内容保持同步



## 基准库保护

可信基准库具有持久化存储能力，基于国密算法加密存储，避免可信自身关键数据出现安全隐患



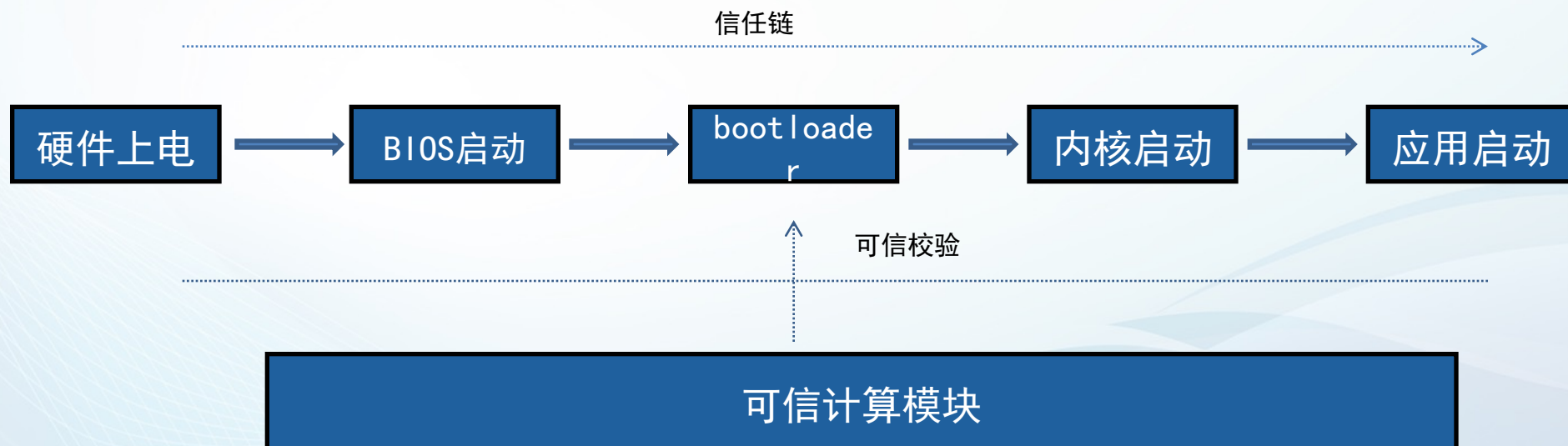
## 独立运行

可信节点离线管理平台时，支持策略单独配置，同时依然能正常提供可信度量和验证

## 可信根与可信引导

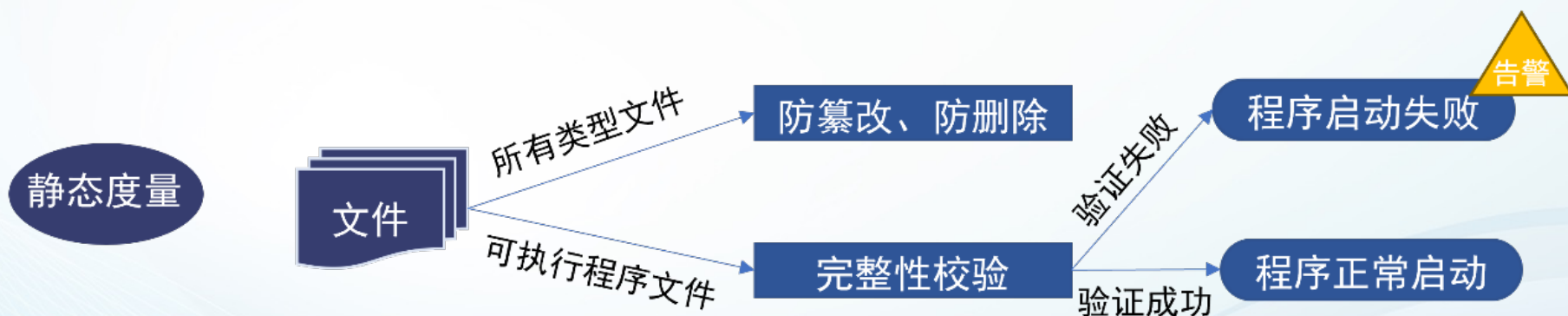
系统在开始启动阶段时，要确保操作系统引导程序、启动盘以及内核在可信任环境下进行启动和运行，构建计算机环境的可信闭环。

可信根是可信引导的重要模块，分为软件和硬件两种方式，对外提供完整性度量、安全存储、密码计算等服务，硬件可信根使用TCM/TPM硬件芯片或支持密码计算的PCIe卡，实现上述功能。



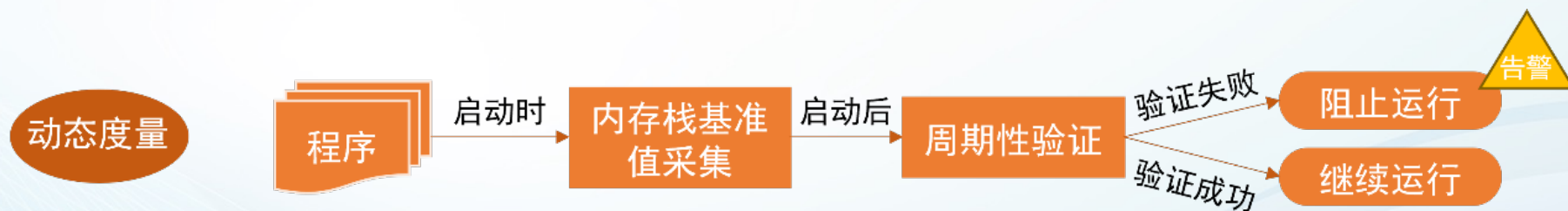
## 静态度量

静态度量指可信验证模块对配置静态度量的文件进行可信基准值采集，统一生成基准库，根据基准值对文件进行完整性校验，提供事后文件变动验证依据，同时主动阻断文件篡改、删除行为。



## 静态度量

程序在运行时会以进程形式存在内存中，程序每一次启动与运行，内存栈都会动态变化，因此可信验证模块会在程序每一次启动时采集内存栈的可信基准值，在程序运行时周期性验证内存栈，确保该程序运行范围的安全可控。





# 凝思可信计算管理系统

## 集中管理



集中管理和配置所有可信节点的可信功能注册、监控、配置、验证、关闭、退出等全生命周期的行为

## 直观展示



弹窗告警紧急事件，统一展示可信节点的所有文件及目录、可信策略、审计日志、运行情况等关键信息

## 一键配置



支持将程序依赖的动态库、可执行文件自动加入可信属性，简化因关联文件过多导致的大量操作；



## 远程下发



远程批量下发文件和策略，自动识别文件类型，可执行程序下发后正常运行，无需单独配置相关策略

## 离线补发



可信节点离线平台恢复后，审计信息自动回传补发

## 上送告警



结合电网业务调度场景，支持告警信息上送到态势感知或网安平台



# 04 / 方案优势

## 方案优势



更高的性能：对可信计算过程进行了针对性的优化，确保安全性的同时降低可信计算对系统造成的性能影响。



安全合规：开发基于GB/T20272、GB/T22239等国家标准，满足等保2.0对可信验证的要求。



良好兼容性和广泛适用性：支持主流国产硬件，具有广泛的适用性。



易用性强：提供友好的用户界面和便捷的集中管理工具，降低用户使用和维护的难度。





# 05 / 总结



## 总结

凝思工控行业可信解决方案通过结合多种先进技术，为工控系统提供了全面的安全防护和可信保障。实现针对系统的控制器、服务器、网络设备、边界设备等核心终端进行可信安全增强。同时满足等保2.0标准安全通用要求对可信验证的要求，实现可信安全与合法合规并举。

# 谢谢观看

# 谢谢观看

# 谢谢观看