工业互联　智造转型

2017 中国工业互联网大会

iSESOL云平台及安全实践

智能云科信息科技有限公司

张晓

关于智能云科

iSESOL：i-Smart Engineering & Services Online

智能云科信息科技有限公司（简称“智能云科”）由沈阳机床集团联合神州数码控股、光大金控于2015年共同投资设立。

公司以“中国制造2025”战略与“互联网+”理念为指导，制造装备互联为基础，基于“工业互联+云服务+智能终端”创新模式， 秉承“让制造更简单”理念，打造iSESOL云制造服务平台。

核心业务分为制造数据云、交易智选云、区域协同云、金融合作云、人才汇聚云与个性定制云六大版块 。

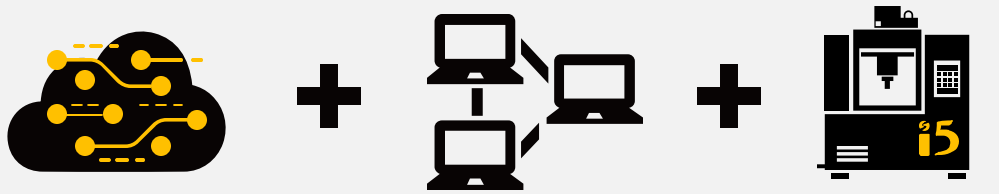
iSESOL-“互联网+智能制造”运营模式

iSESOL平台实质——“+ 智能终端 +工业互联网+ 云服务 ”的商业服务平台

通过布局智能终端设备，连接利益相关者的增值网络，
通过云计算等技术手段释放大数据潜力，形成制造新生态。

智能装备联网

基于i5机床及装备的广泛使用



云
云计算
大数据

网
工业互联网
物联网

端
i5智能机床及
制造装备

基于i5智能装备，使工业智能网有了承载终端
中国工业4.0有了创新的生产方式

安装量上**百万**
改变制造生产方式

安装量上**十万**
形成稳定盈利模式

安装量上**万**
初步形成网络布局

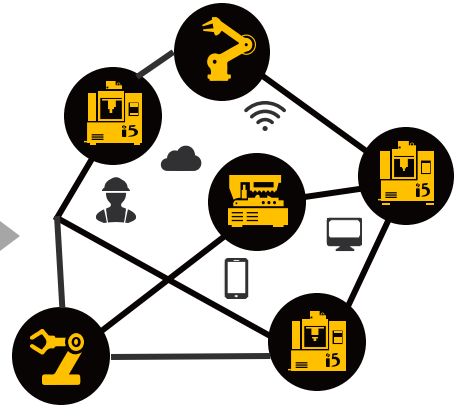
iSESOL-搭建“互联网+智能制造”新生态

iSESOL平台为制造行业互联网化应运而生

单机智能

- 制造数据最小单元
- 独立结算体
- 可按工作量租赁
- 软硬件可做针对性调试
- 不用对冗余功能买单

智能车间



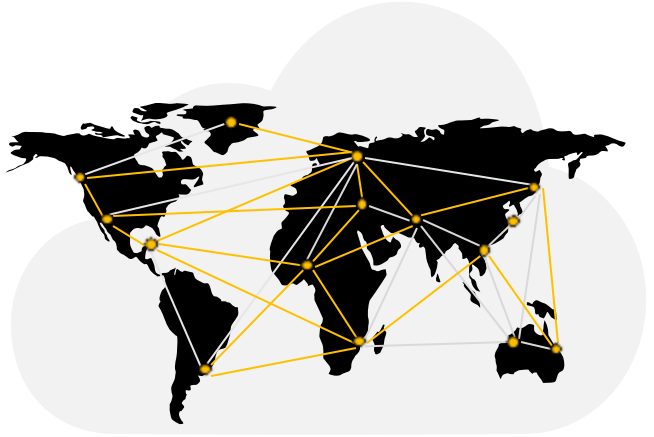
- 通过网络形成智能生产环境
- 生产状态实时监控
- 过程数据透明化
- 定制生产柔性化
- 实现智能生产

iSESOL平台

智能区域协同

- 企业间产能盈缺互助
- 上下游产能协同互补
- 区域内稀缺资源共享
- 行业内资源弹性组合
- 民间创造创新力共享

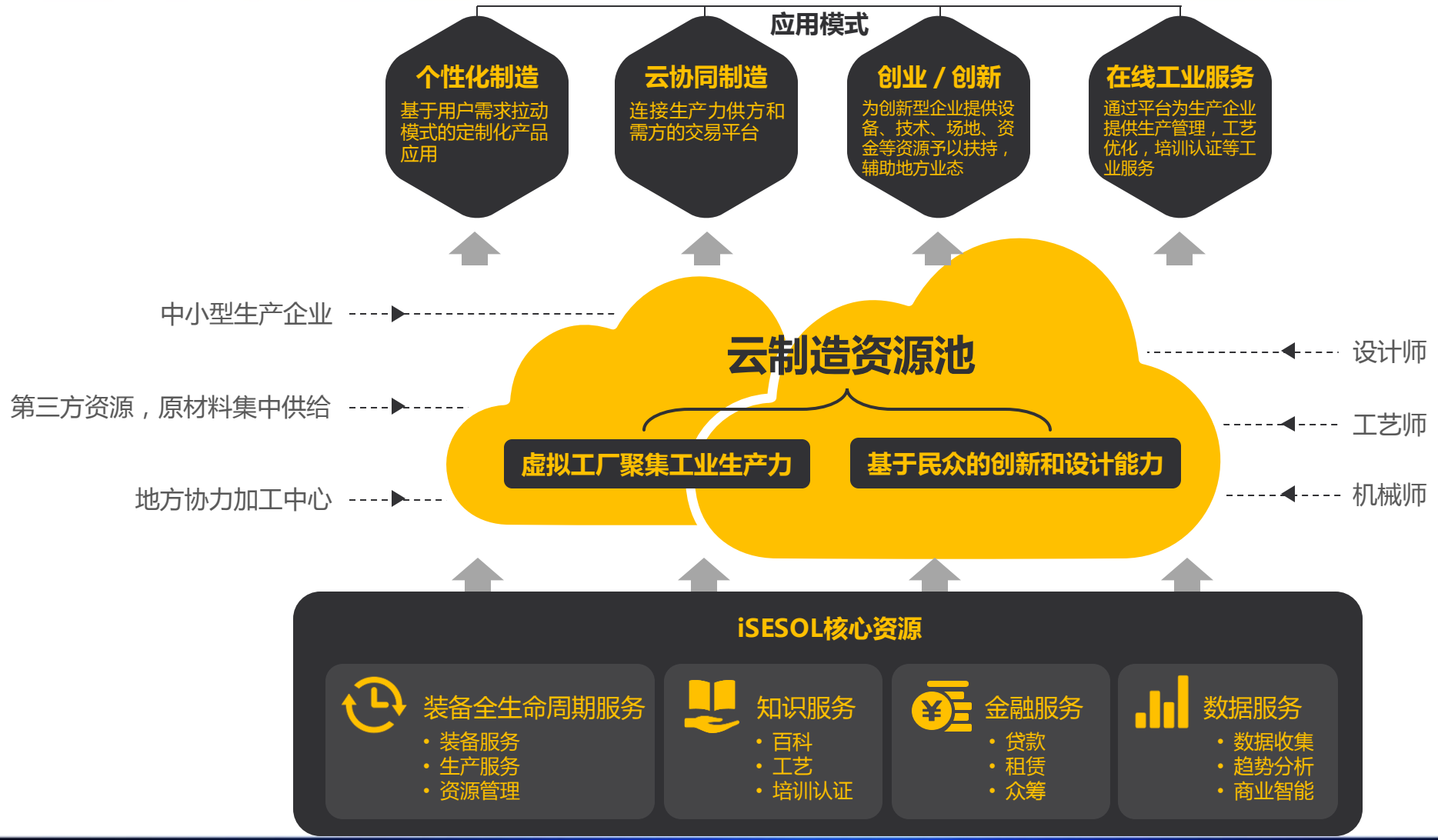
智能制造新业态



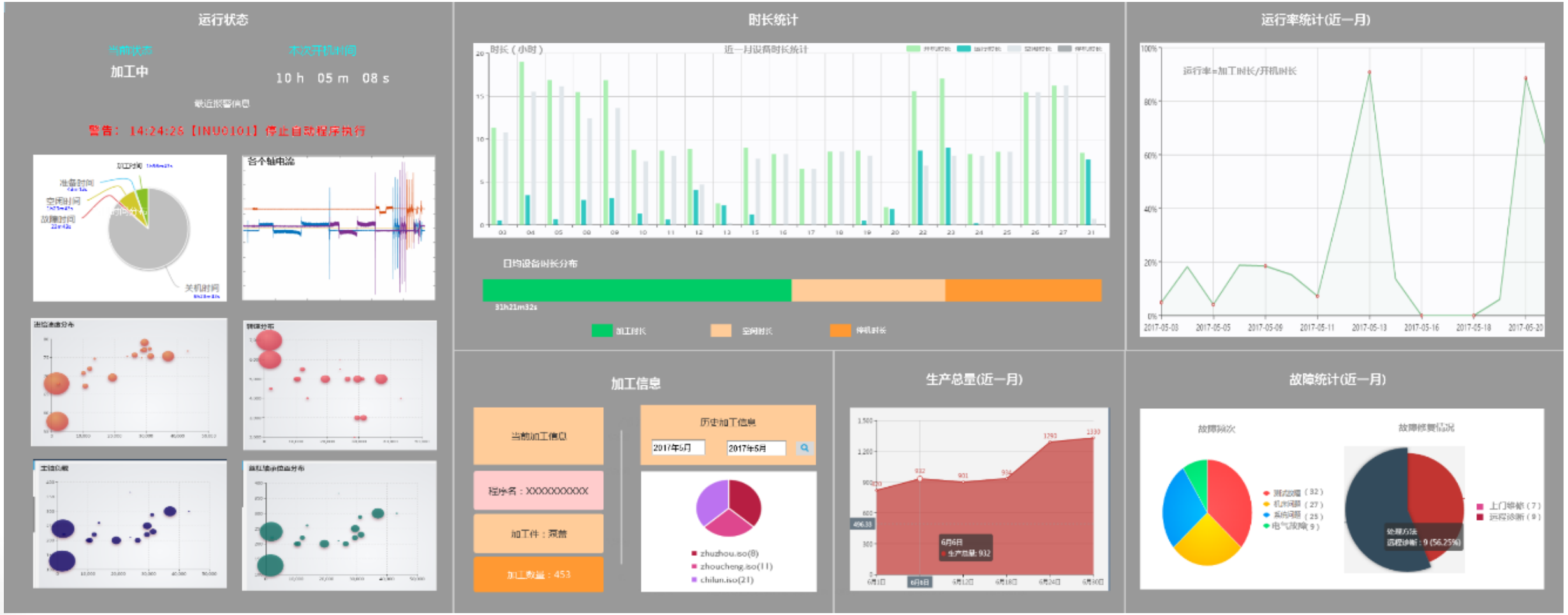
- 跨区域、跨行业协同
- 成就万能工厂
- MindShare

机床是制造业的基础，具备大量的市场存量、广泛的产业应用和跨行业特征，通过广泛联网形成社会工业网络，从而使中国工业互联网找到了突破口。

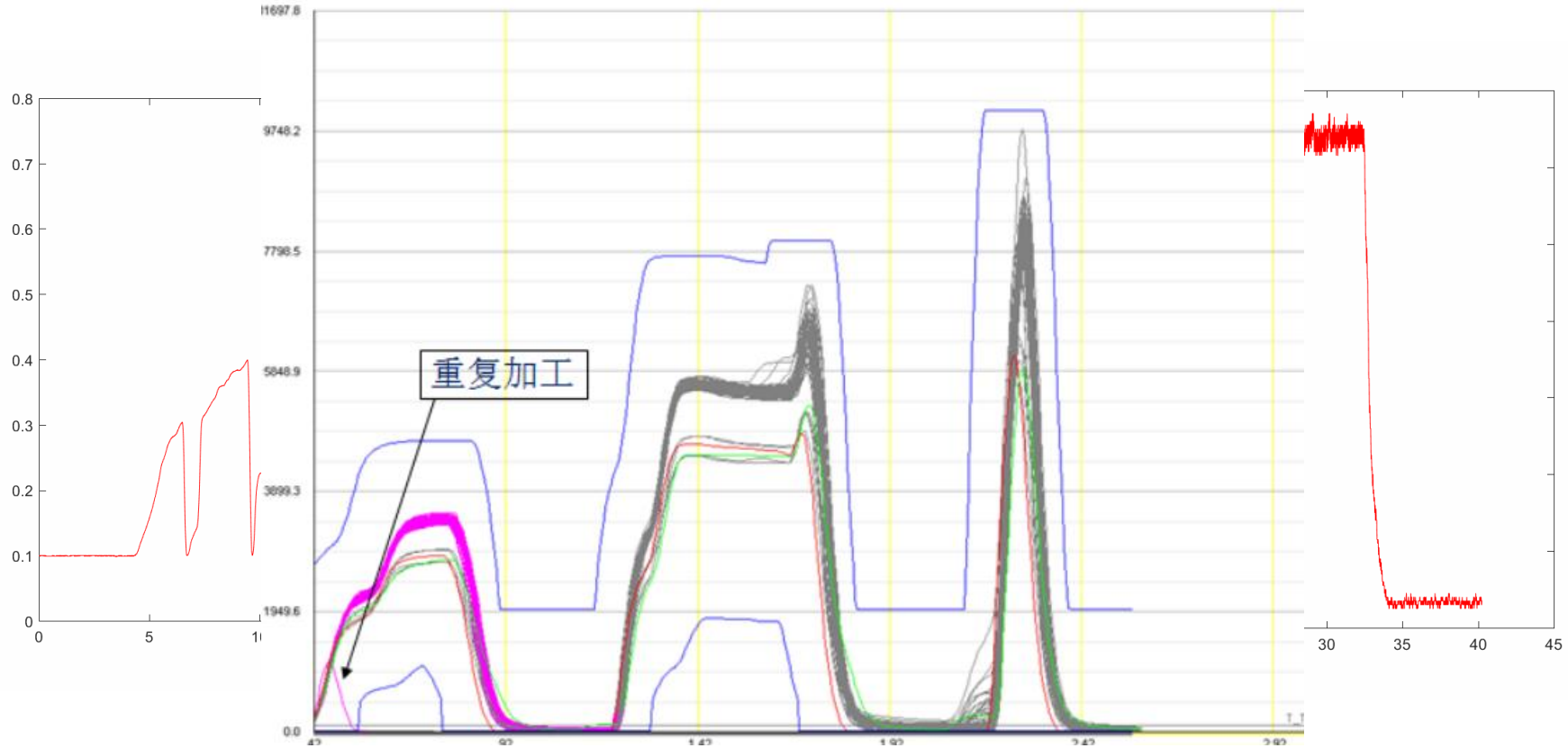
iSESOL-致力于打造社会制造的多赢业态



大数据分析可以从多个维度反映机床的状态



通过实时高频数据采集和大数据分析对加工方案进行多维度量化评价



- 基于加工过程状态数据提供加工方案的多维量化评价
- 可以进行刀具损耗分析
- 横坐标上加入运行的G代码指令，进行更加具体的分析

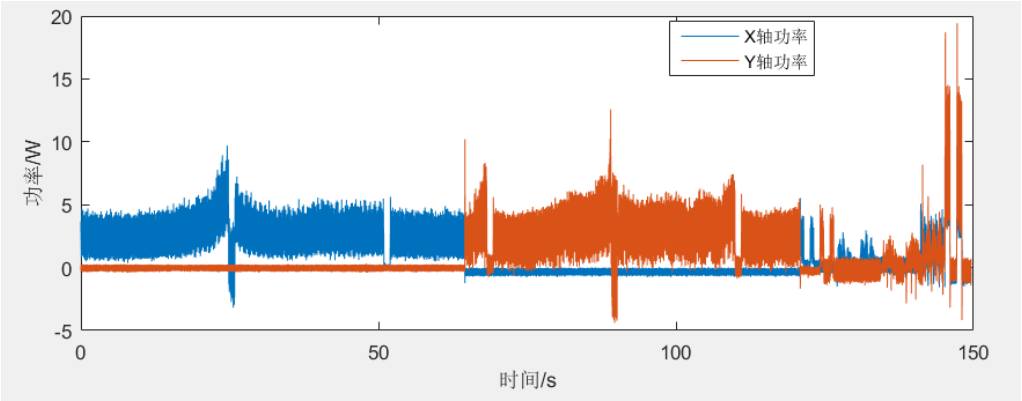
利用大数据进行机床体检

主要功能：

运行标准测试程序并云端采集分析数据

测试内容

- 丝杠受力分析测试程序
- 单轴测试
- 圆弧测试
- 双轴测试
- 主轴空转测试



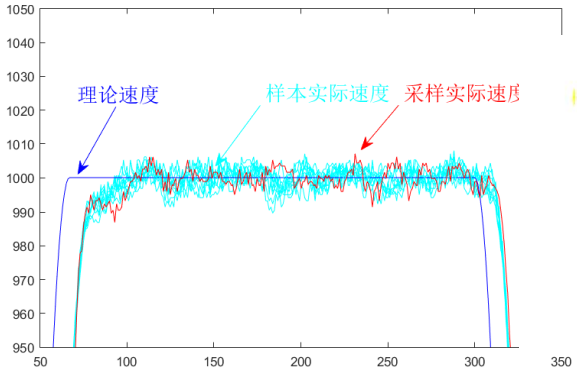
采集信号

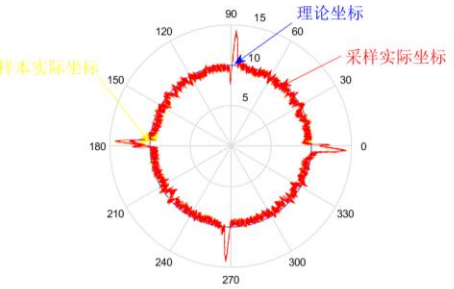
外部传感器

- 主轴功率信号
- 伺服电机功率信号
- 工作台加速度信号
- 主轴加速度信号

内部伺服数据

- 进给轴理论速度
- 进给轴实际速度
- 进给轴理论坐标
- 进给轴实际坐标
- 进给电机电流





丰富的应用 | 运动控制底层 | 云平台功能基础设施 | 可靠的硬件载体

铝合金机身

机加工成型，可回收

适用各类工业环境

无风扇，全密封设计，防水防尘

RFID刷卡区

基于云平台的用户权限管理系统，
多种登录方法的实现

应用桌面

访问所有可用的应用程序

经过严格测试的按键

通过EMC测试，高达100万次的使用寿命，2~3N的按键力控制

人性化设计

更友好、更直观、更简洁

i5OS开放的设计原则，创造生态链的共同利益

在保护i5核心技术的前提下尽可能的**开放i5系统接口及资源**

专业的人做专业的事，i5OS要与设备制造商及APP开发者**区别定位**

确保i5OS生态链条的整体利益，各个环节相互支撑相互依存

基于i5App的运动控制操作系统 打造智能制造的AppStore

i5OS

提供运动控制领域的操作系统平台：

向主机厂商/自动化方案提供商/自动化设备制造商提供运动控制核心软件平台，提供开放的APP框架，统一的开发平台，使其能够快速基于i5运动控制核心技术进行面向各自领域的自动化集成方案开发，行成专业领域的APP。

i5 APP

提供基于i5OS的基础APP模块：

- 提供各类面向运动控制及自动化领域的基础APP应用；
- 帮助用户专注高价值应用开发；
- 标准的i5 APP可以组合搭建起面向数控机床的完整解决方案。

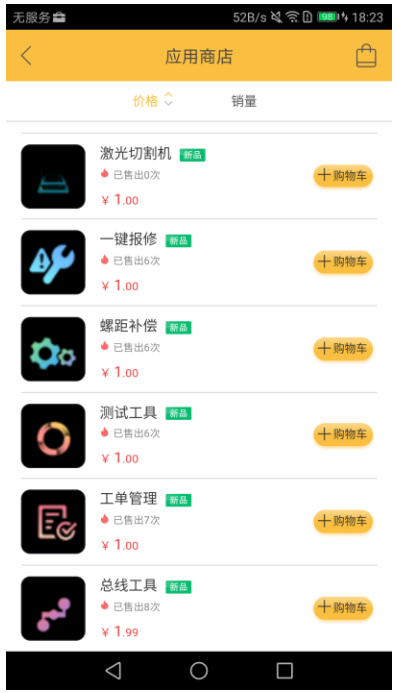
i5OS APP Store

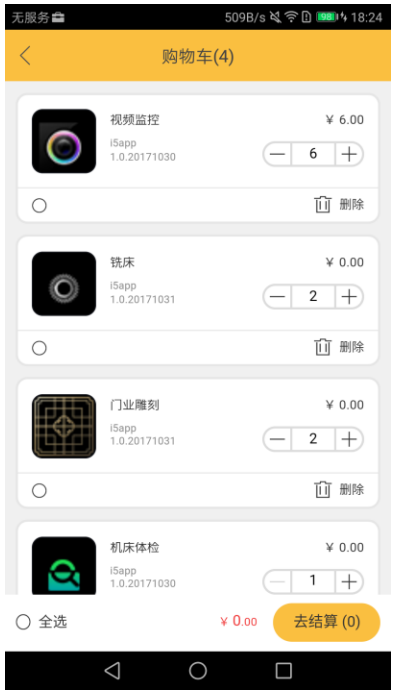
提供运动控制领域的应用分享及推广平台：

- 针对i5OS应用的专业开发商所开发的APP，提供APP商店，使其能够在自身推广网络之外获得快速的推广、复用，帮助i5OS用户快速获取面向不同专业领域的APP；
- i5充当APP验证的角色，确保平台上APP的稳定性和可靠性。

2017年11月i5OS即将正式发布——工业控制系统从“功能机”时代跨入“智能机”时代

通过手机端应用商城，购买和授权使用不同的App





通过APP组合配置快速构建面向不同行业的智能系统

支撑更多的行业领域


搬运和装配技术
半导体设备
木材加工机械
印刷和造纸机械
LED制造加工检测设备
自动装配设备
流水线控制
门窗加工机械
半导体切割
点胶机
贴标机
塑料机械
数控机床
打标机
光纤光栅
电子产品自动化加工设备
电子产品自动化测试设备
插件机
组装机
光通讯设备
LCD自动加工设备
电子产品自动化装配设备
包装机械
运动控制
钣金设备
焊接机
电子装配自动检测
离子束焊接
电子装配和检查
等离子火焰切割
上下料机械手
切割机
运动模拟器
图像复制
空间坐标测量
绘图仪
3C设备
激光打标设备
关节机器人
包装设备
钻孔机
固晶机
生物医学取样和处理设备
医疗设备
激光雕刻设备
薄膜制造
掩膜矫正
绕线机
LCD自动检测设备
激光切割设备
锂电池设备
光纤矫正
检测机
雕刻机
冲孔机
印刷设备
电子显微镜
印刷自动检测

i5OS + iSESOL共同打造工业互联网生态的基础平台

有别于Predix、MindSphere，我们提供“终端+云端+商业模式”完全贯通的工业互联网生态解决方案

i5OS帮助各个领域从“功能机”步入“智能机”时代

i5OS提供基础平台，借助i5OS，发烧友可以利用APP快速构建工具链，结合云平台和运动控制技术，快速地构建出智能化的、面向行业的应用。

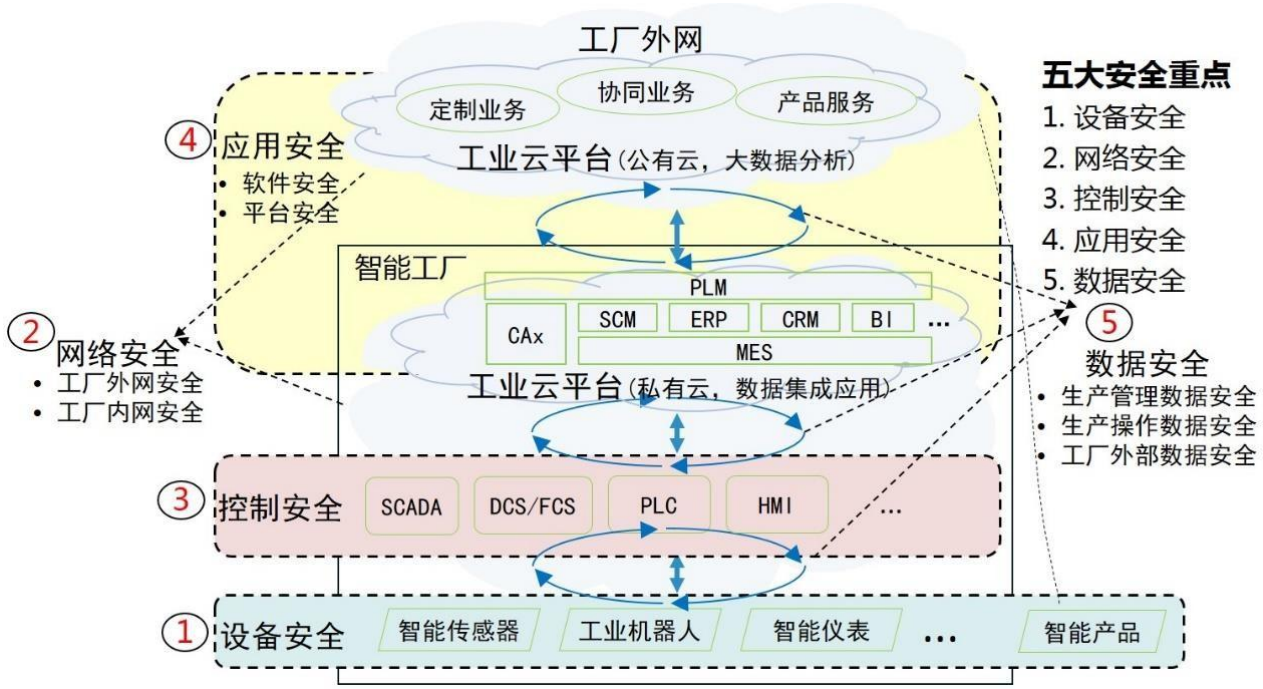
用户可以借助i5OS中的i5 APP store，以最低的使用成本，获得最多的应用服务，使得专家端的成果得到放大，单个软件的使用成本得到降低。制造商利用i5OS，打造出具有行业特色的，具有差异化的应用场合，解决原有的产品同质化、结构单一的、研发投入成本高的难题。

基于iSESOL平台，制造业用户及设备制造商可以分享iSESOL平台的渠道、人力资源、设计资源，基于工业互联网的商业模式可以获得快速的复制。

iSESOL帮助制造业快速与创新的商业模式对接

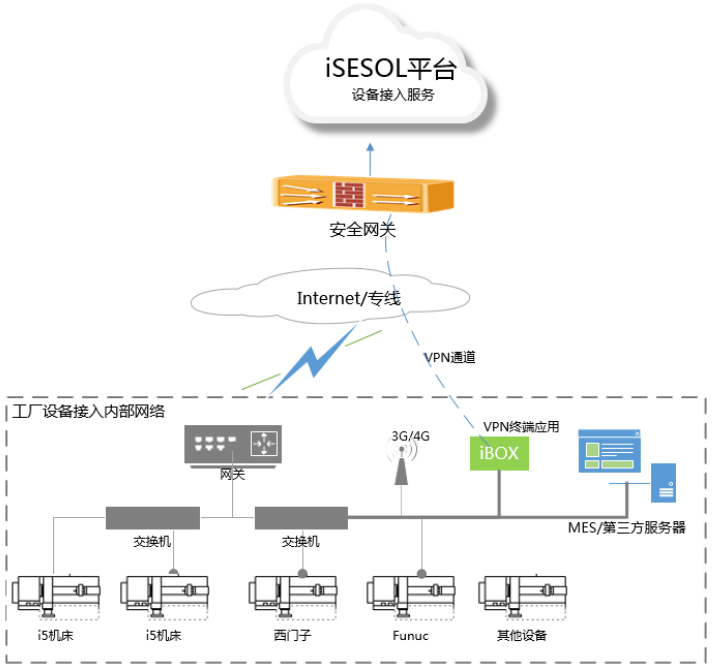
在平台整体安全领域，我们按照工业互联网架构-安全的体系框架进行整体设计，打造安全的工业互联网平台

工业大数据的应用覆盖工业生产的全流程和产品的全生命周期。工业大数据的作用主要表现为状态描述、诊断分析、预测预警、辅助决策等方面，在智能化生产、网络化协 同、个性化定制和服务化延伸四类场景下发挥着核心的驱动作用。

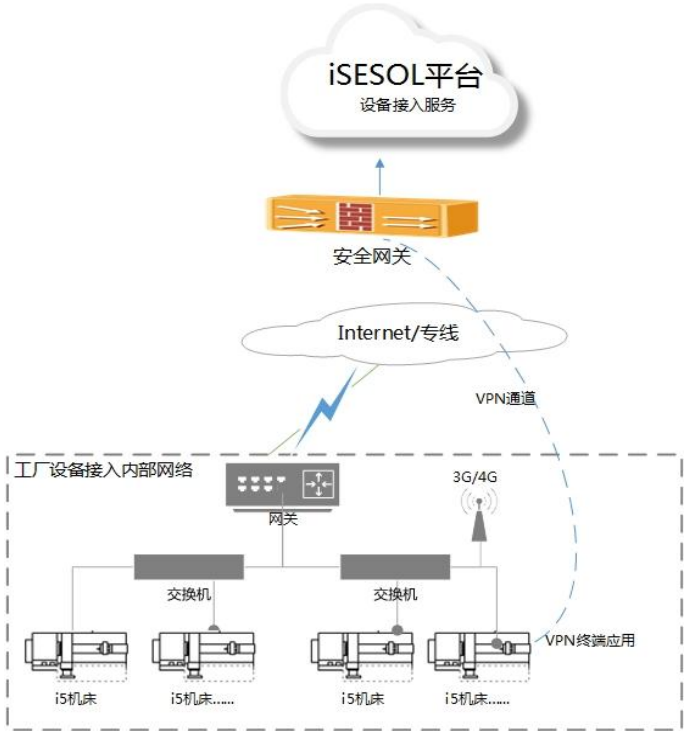


- 设备内嵌安全机制
- 动态网络安全防御机制
- 信息安全与功能安全融合机制
- 面向工业应用的灵活安全保障能力
- 工业数据分类分级保护机制

分别为智能机床直接联网及通过网关接入场景



设备通过采集网关模式：通过采集器接入模式适用于应用功能在云端，并且设备满足平台标准接入协议，有本地信息化系统与设备通信的要求；设备通过内部网络，连接到采集器终端，通过采集器终端实现数据与本地信息化系统的对接与数据定制要求，同时具备采集器与云平台构建通讯VPN隧道，保障通讯安全



设备直连模式：设备直接联网的接入模式适用于应用功能在云端，并且设备满足平台标准接入协议，也无本地信息化系统与设备通信的要求；设备通过内部网络，可以通过有线/无线方式与云平台互联，采用安全网关构建终端设备与云平台之间的通讯VPN隧道，保障通讯安全

工控网络及平台的安全现状

- 高精尖数控设备绝大多数为进口设备，无法进行自主维护，依赖国外厂商。

- DNC工业控制网络防护建设不够完善，仅通过传统防火墙、防病毒软件等进行防护。

- 缺乏对工控安全问题的高度重视，对企业核心技术知识和国家机密的信息安全风险并未有足够的认识。

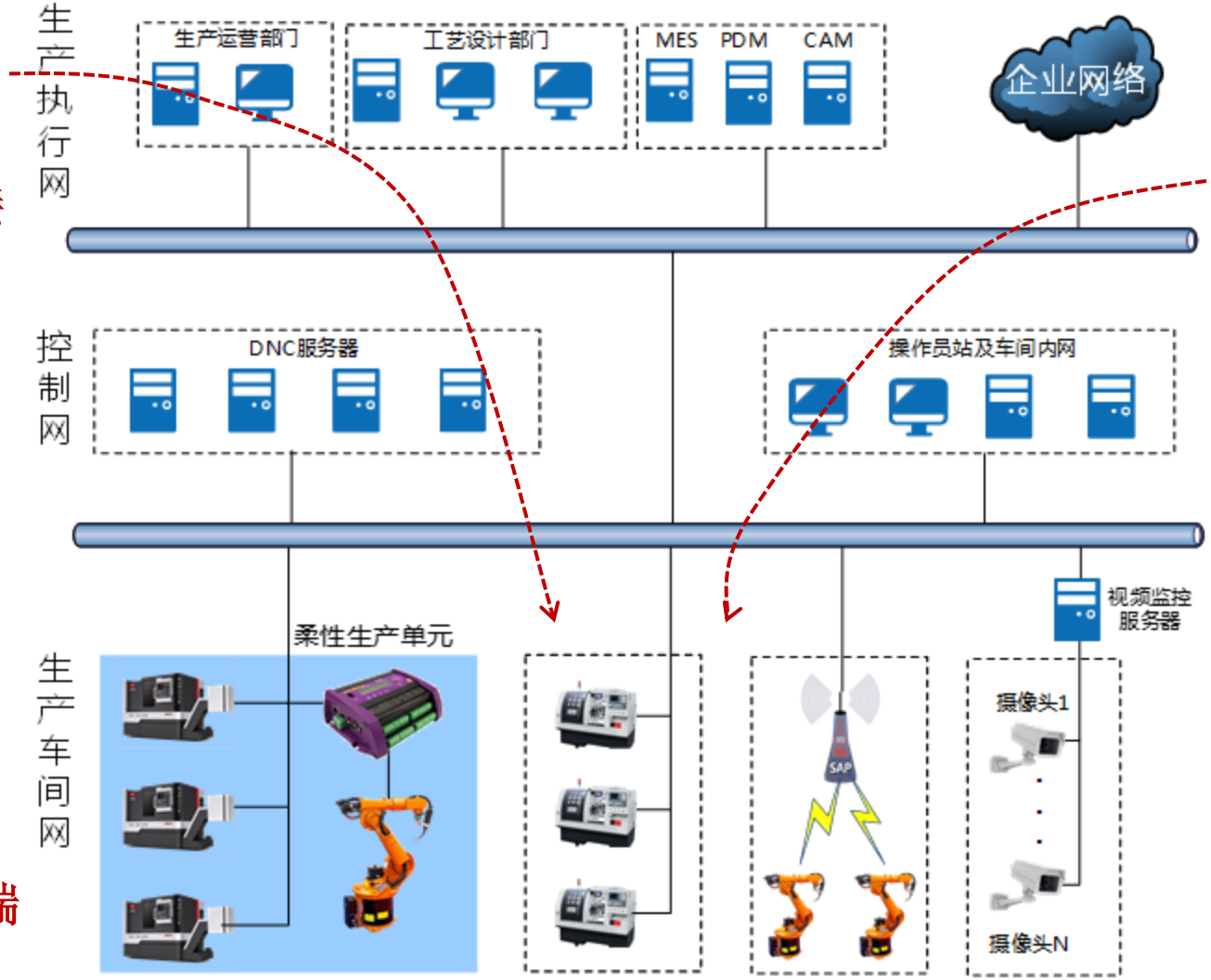
- 国务院、工信部、国家保密局、国防科工局、总装备部对数控系统与管理网络的链接进行了严格规定。

智能制造工控网络存在多种入侵途径

WIFI无线连接

远程维护通道

手机等智能终端



企业办公网

USB移动存储介质

心怀不满的恶意员工

工业控制系统“白环境”解决方案理念

方案核心安全理念

提出了建立工控系统的**可信任网络白环境**和**工控软件白名单**的理念为客户构筑工控系统“安全白环境”整体防护体系，保护国家基础设施安全。

- 只有可信任的**设备**，才能接入控制网络
- 只有可信任的**消息**，才能在网络上传输
- 只有可信任的**软件**，才允许被执行

技术亮点及创新点

- 从“黑”到“白”
- 从“被动防御”到“主动防护”

基于相关标准及要求，考虑智能终端的安全设计

DNC网络工控安全解决方案设计依据

- 《工业控制系统信息安全防护指南》
- 《GB / T26333-2010　工业控制网络安全风险评估规范》
- 《信息安全技术 网络安全等级保护基本要求　第5部分：工业控制系统安全扩展要求》
- 《信息安全技术 网络安全等级保护测评要求　第5部分：工业控制系统安全扩展要求》
- 《信息安全技术 网络安全等级保护安全设计技术要求　第5部分：工业控制系统安全扩展要求》

本方案重点解决以上政策标准中的核心问题

工业互联网的安全防护的实施框架

1、控制系统与信息系统之间，部署防火墙；

2、工厂内外部云平台的访问应部署防火墙及防御措施；

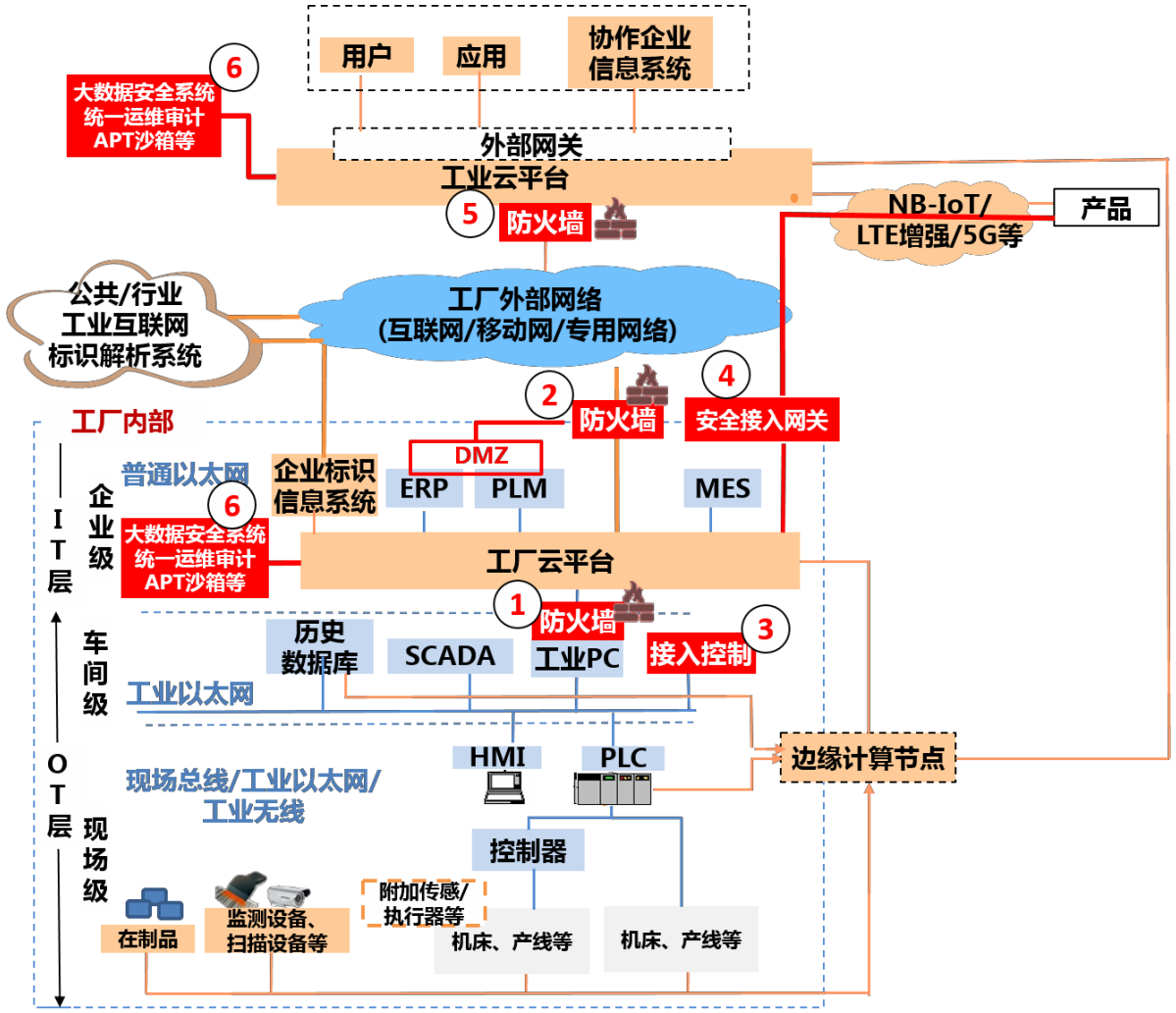
3、工厂内的设备接入系统都需进行接入控制；

4、工厂外的设备及系统接入工厂内均需通过网关控制；

5、访问外部应用均需通过防火墙的控制；

6、应该工厂云平台及工业云平台部署大数据安全系统；

7、在数据传输上，要采用SSL加密通道，同时，对于影响安全生产的重要数据，如智能设备执行的脚本，命令等需要进行**数字签名**等验证措施，确保数据安全。

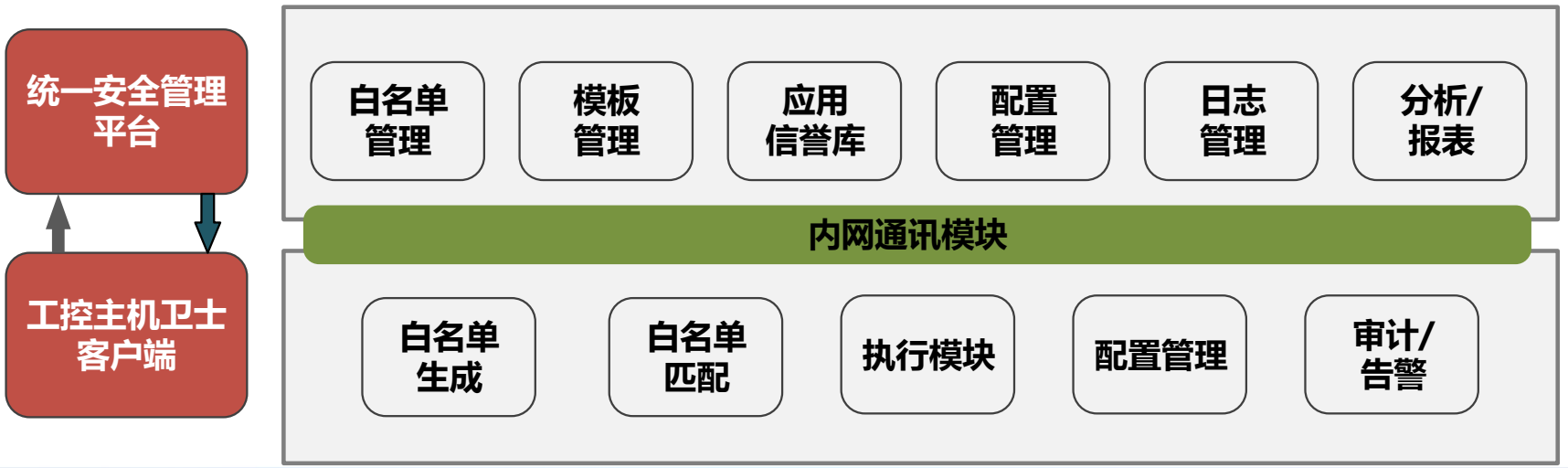


通过工业互联网安全监测公共服务平台，进行安全监测和威胁预警

- 工
  -
- 病
  -
- D
  - 发现：企业DDOS
- 高级攻击监测
  -
- 工
  -

在智能终端上采用安全卫士，确保终端的安全

- **统一安全管理平台**：进行状态监控及策略配置和下发，收集、汇总、更新、同步单独客户端的白名单数据信息，统一收集单独客户端的审计信息，并进行大数据分析，统一管理企业消息推送；
- **工控主机卫士客户端**：监控分析应用程序和人工操作的行为特征，生成白名单，阻止恶意程序和操作的执行。



威努特
安全卫士

工业互联　智造转型

2017 中国工业互联网大会

iSESOL 智能云科　i5OS

谢谢大家