MOSES
海天煒業
服 務 提 升 價 值

智能制造中的工控信息安全框架设计

——让生产更安全

刘安正

2016年8月

目录

CONTENTS

公司概况及前期成果介绍

发展历程与技术能力

建立工控系统集成与运维中心；
Honeywell、Emerson、
Yokogawa、ABB、Siemens
施耐德、中控、和利时等

建立工业信息安全研发中心；
取得石油化工设备检维修资质

推出Guard工业防火墙

联合中科院软件所共同研制工控可信计算安全防护技术

新三板挂牌

股票代码：836296

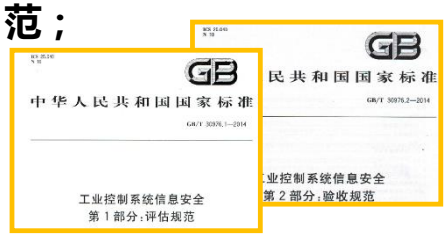
股票简称：海天炜业

2003 | 2009 | 2011 | 2012 | 2014 | 2015 | 2016

国内首家专业的工业信息安全解决方案提供商；

大型生产企业安全项目：
石油化工行业
电力行业
冶金、烟草行业
……

国家发改委工控信息安全专项《支持多协议的分布式工业防火墙及产业化》；
制定《工业控制系统信息安全评估规范/验收规范》
输油气管道监控与数据采集（SCADA）系统安全防护规范；



引入功能安全技术体系；

工信部2015年智能制造专项“功能安全和工业信息安全标准研究和验证平台”；

青岛市工控系统安全工程技术中心

MOSES 海天煒業
服 務 提 升 價 值

发展历程与技术能力

- HAZOP分析
- SIL评估咨询及服务
- 功能安全产品认证
- 功能安全与信息安全结合
- 功能安全工程师培训

功能安全 Safety　信息安全 Security

安全

- 工业信息安全整体解决方案
- 工控信息安全产品研发
- 控制系统信息安全项目集成
- 控制系统信息安全评估
- 工业信息安全培训
- 工业网络信息安全实验室

- 10余年自动化系统整体运维经验
- 大型自动化系统集成能力
- 工业信息化数据采集解决方案及项目经验
- 工控设备检修及系统集成资质

海天炜业、exida战略合作签约

功能安全业务

艾思达（青岛）

exida 咨询 LLC

咨询

过程安全（IEC61511
IEC62061
ISO26262）
报警管理ISA18.2
网络信息安保（ISAS99）

培训

过程安全
网络信息安保
Onsite
Offsite
Web
安全审核

exida 认证

产品认证

功能安全（IEC61508）
控制系统网络安全
网络的鲁棒性（阿基里斯）

专业认证

CFSE
CFSP
FSP
功能安全专家

exida 产品

工程工具

exSILentia
(PHA，HAZOPA，SILA，LOPA SRS SIS确认）
SILstat
SILAlarm
PHAx
SERH Viewer

参考资料

SERH安全设备可靠性数据库
FSE教程
教科书
参考书
市场研究

产品认证经验

- exida完成的认证项目大部分是针对全球主要的自动化公司
- exida 最终用户委员会修订了所有的程序，并提出由exida强制执行的额外要求(发送申请到 info@exida.com成为一员)

参与国家标准制定

国家标准研制：

- 《工业控制系统信息安全 第一部分：评估规范》
- 《工业控制系统信息安全 第二部分：验收规范》
- 信息安全技术、信息系统等级保护 、工业控制系统安全设计技术指南（正在制定中）
- 国家工信部智能制造课题 “功能安全和工业信息安全标准研究和验证平台”

行业标准：

- 输油气管道监控与数据采集（SCADA）系统安全防护规范
- 工业过程测量和控制安全 网络和系统安全 IEC62443-3（计划号：2011-1108T-JB）
- 工业通信网络 网络和系统安全 第1-1部分 ：术语、概念和模型（计划号：2011-1120T-JB）
- 工业通信网络 网络和系统安全 第3-1部分：工业自动化和控制系统信息安全技术（计划号：2011-1121T-JB）
- 可编程逻辑控制器（PLC）系统信息安全要求
- 集散控制系统（DCS）安全防护标准；
- 其它.....

智能制造工控信息安全框架设计

几点说明：

- 1. 面向对象：离散制造领域的生产控制网络，同时由于这个领域的行业也包含众多，因此该框架仅是指引；
- 2. 框架内容：从安全厂商角度出发，没有包含物理安全的内容；
- 3.工控信息安全体系主要分为管理和技术两部分；
- 4. 信息安全没有绝对，不能依靠一个产品，一次性投入解决信息安全问题。
- 5. 信息安全没有止境，是可接受风险与投资的平衡。
- 6. 工控信息安全评估/调研是制定工控信息安全的方案的重要步骤。
- 7. 在工控信息安全评估中，针对由信息安全能导致的生产事故，但无法用信息安全防护手段解决的风险，需要考虑增加功能安全设计；

2016工控网络安全框架指引-管理

- 1.书面安全策略或程序文件
- 2.工控网络资产梳理
- 3.工业控制系统安全培训和安全意识培养
- 4.工业控制系统设备（包含网络设备）操作指南
- 5.控制系统的内置安全配置策略（安全基线）
- 6.控制系统边界及内部安全产品管理（安全策略及日志）
- 7.控制系统相关软、硬件脆弱性管理
- 8.工控系统维护及配置变更管理
- 9.工控系统安全审计
- 10.工控系统信息安全灾难恢复计划及应急响应体系

2016工控网络安全框架指引-技术

网络层

- 1.网络架构设计；
- 2.边界访问控制-防火墙；
- 3.内部区域隔离-防火墙
- 4.应用审计-安全审计
- ……

主机层

- 1.防病毒；
- 2.进程管理；
- 3.USB管理；
- 4.账户密码
- ……

监控层

- 安全管理平台（中心）
- 工控网络异常监测
- ……

服务层

- 评估咨询；
- 漏洞挖掘、渗透测试；
- 安全运维及分析；
- ……

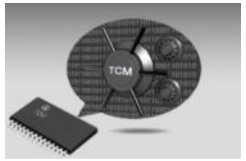
公司工控信息安全产品及服务体系

工业信息安全
ICS Information Security

Gurad工业防火墙/ 审计/网关…

网络层

Intrust工控可信计算平台/USB…



主机层

SMP安全管理中心

监控层

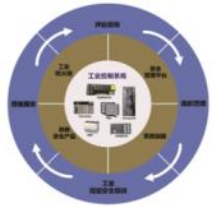
工业控制系统安全评测咨询

服务层

工业控制系统信息安全实验室

服务层

全生命周期解决方案



服务层

油气开采及储运；
石油石化；
煤化工及一般化工
钢铁及冶炼；

电力（火电、水电、
核电，新能源）
智能/先进制造；
国防军工

水利及水处理；
烟草
城市燃气及管网；
智能交通

服务行业

（一）Guard工业防火墙

IFW2400-11

IFW2400-12

IFW2400-14

TSA220

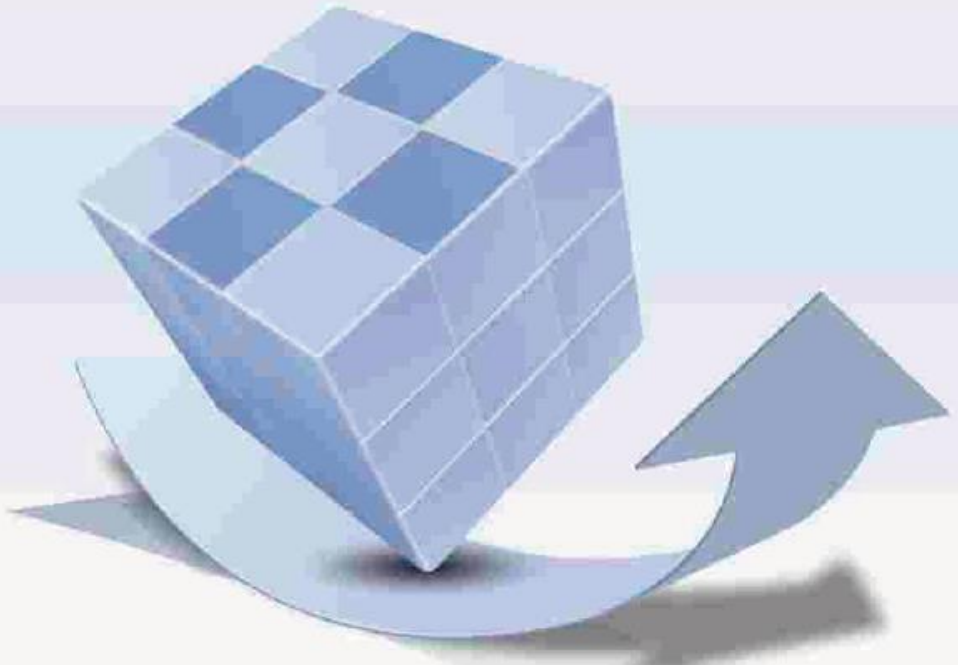
产品优势

- 内置多种常见工业通讯协议和控制器模型
- 无IP连接技术，让入侵者无从发现攻击目标
- 工业协议深度包检测
- 网络通讯透视镜功能，智能预警分析
- 在线实施，无需停车，无需更改原有网络结构
- 自身强大的安全性

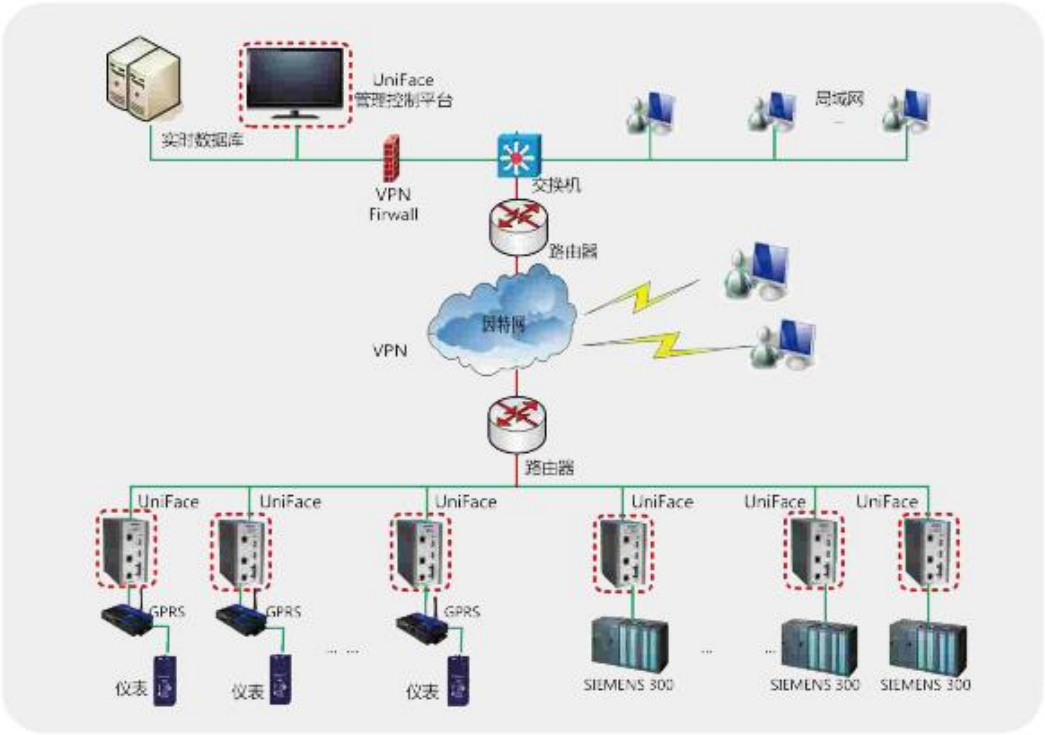
Guard工业防火墙

典型应用

- 生产控制网与管理网的隔离
- 控制网络区域隔离
- SCADA系统防护
- 工业以太环网防护
- SIS安全仪表系统、关键控制器、服务器的保护
- APC先控防护
- 工程师站隔离
- Modbus TCP通讯深度防护
- OPC通讯深度防护



（二）Uniface安全数采网关



环境监测数采架构图

- 支持上百种自动化设备及仪表的通讯协议，轻松解决接口种类繁多的问题
- 独有的数据缓存及断点续传功能，保证生产数据的完整性
- IP保护、MAC绑定等安全防护，保护暴露于因特网的控制系统不被攻击
- 支持标准工业通信协议（OPC、Modbus等），与第三方软件实现无缝连接
- 设备监控管理功能大大降低系统维护成本
- 友好的人机界面，系统组态、工程制作、升级与维护简单、易学、易操作

（三）工控网络安全审计与异常监测

核心功能：

- ❖ 工控网络数据海量存储；
- ❖ 工控网络通讯指令实时解析；
- ❖ 工控网络异常动态分析；
- ❖ 工控网络安全事件溯源；
- ❖ 工控网络资产运维；

- 自定义规则告警展示：

2016-03-04 10:09:38	TCP_关键资产访问超出白名单	非攻击	TCP	10.1.1.13	3894	10.1.1.16	135	自定义规则
2016-03-04 10:09:38	TCP_关键资产访问超出白名单	非攻击	TCP	10.1.1.13	3856	10.1.1.16	135	自定义规则
2016-03-04 10:09:38	TCP_关键资产访问超出白名单	非攻击	TCP	10.1.1.13	3856	10.1.1.16	135	自定义规则
2016-03-04 10:09:38	Modbus_特定时间内出现异常状态码	非攻击	MODBUS	192.168.1.25	502	192.168.1.19	49169	自定义规则
2016-03-04 10:09:38	Modbus_特定时间内出现异常状态码	非攻击	MODBUS	192.168.1.25	502	192.168.1.19	49169	自定义规则
2016-03-04 10:09:38	Modbus_特定时间内出现异常状态码	非攻击	MODBUS	192.168.1.19	49169	192.168.1.25	502	自定义规则

参数展示

原始内容 转为十六进制

connection is out of bounds : ip.src=10.1.1.13 and ip.dst=10.1.1.16

参数展示

原始内容 转为十六进制

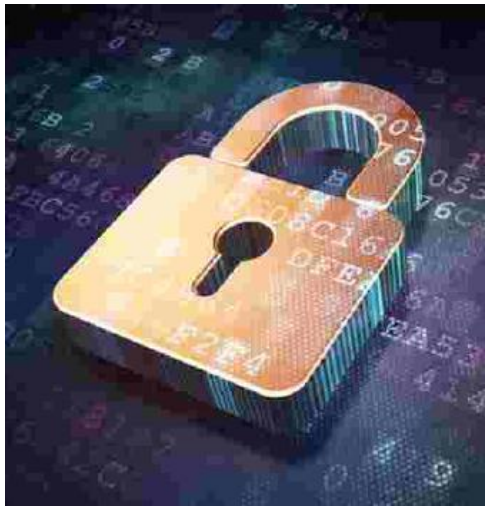
modbus.funccode=1modbus.data=8\x00

100000018	iec104返回信息
100000020	TCP_Honeywel_未知IP访问IPC
100000021	TCP_服务器主动向其它IP发送请求
100000022	TCP_关键资产访问超出白名单
100000023	Modbus_工作时间开关机
100000024	Modbus_特定时间内出现异常状态码
100000025	TCP_Honeywel_IPC访问未知ip

（四）Intrust工控可信计算安全平台

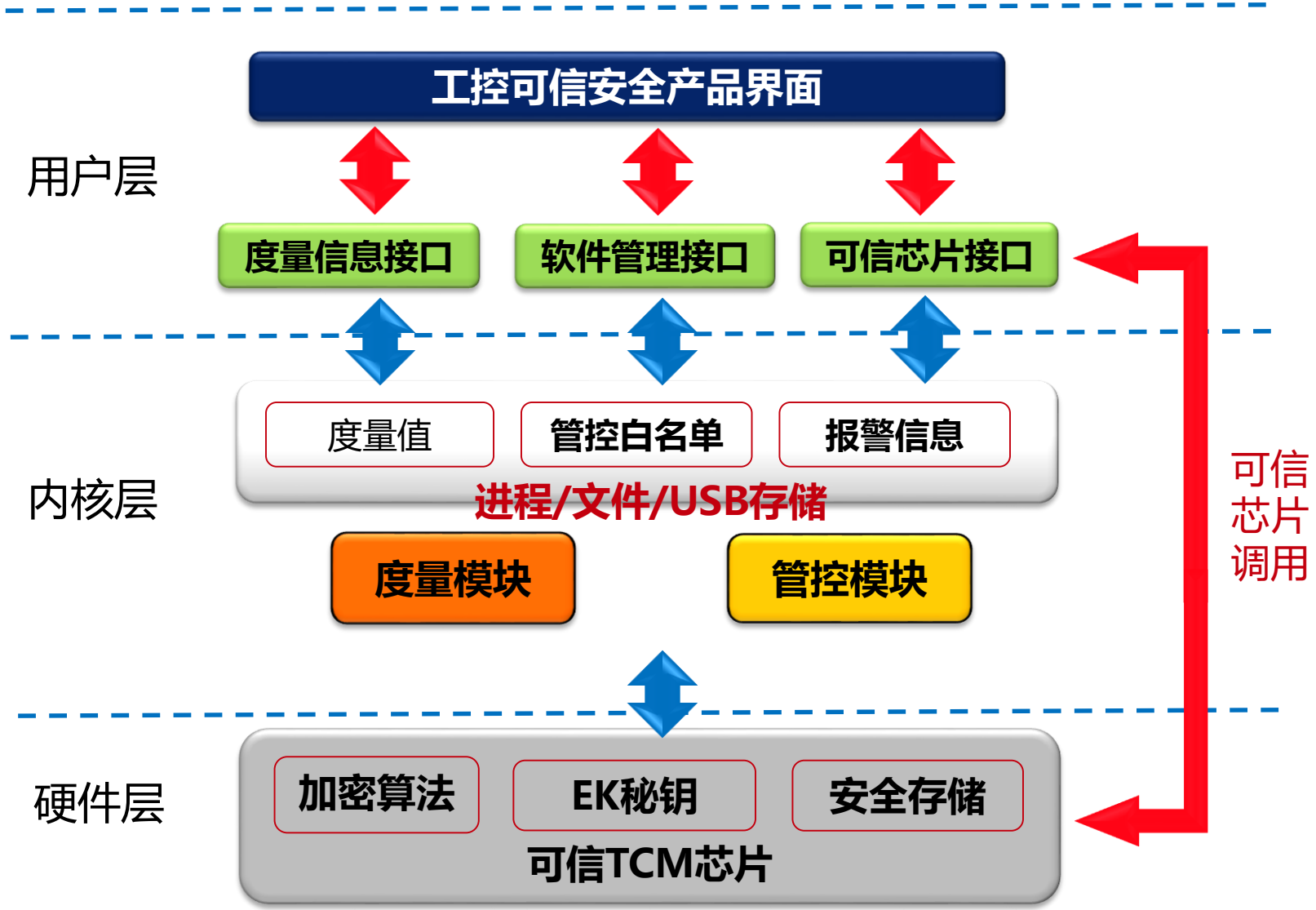
可信计算技术实现主机防护、加固

提高工控系统终端自身免疫力



- 基于TCM，首创可信计算在工控领域的创新应用
- 由**授权服务器（Intrust-S2400）**和安全**客户端（Intrust-C2400）**两部分组成
- 客户端对保护计算机系统所有进程进行全面度量，并将度量信息提交至授权服务器端
- 服务器对这些信息进行编辑后生成白名单，供客户端下载
- 客户端依据所下载的白名单对系统进行管控

工控可信计算安全产品原理

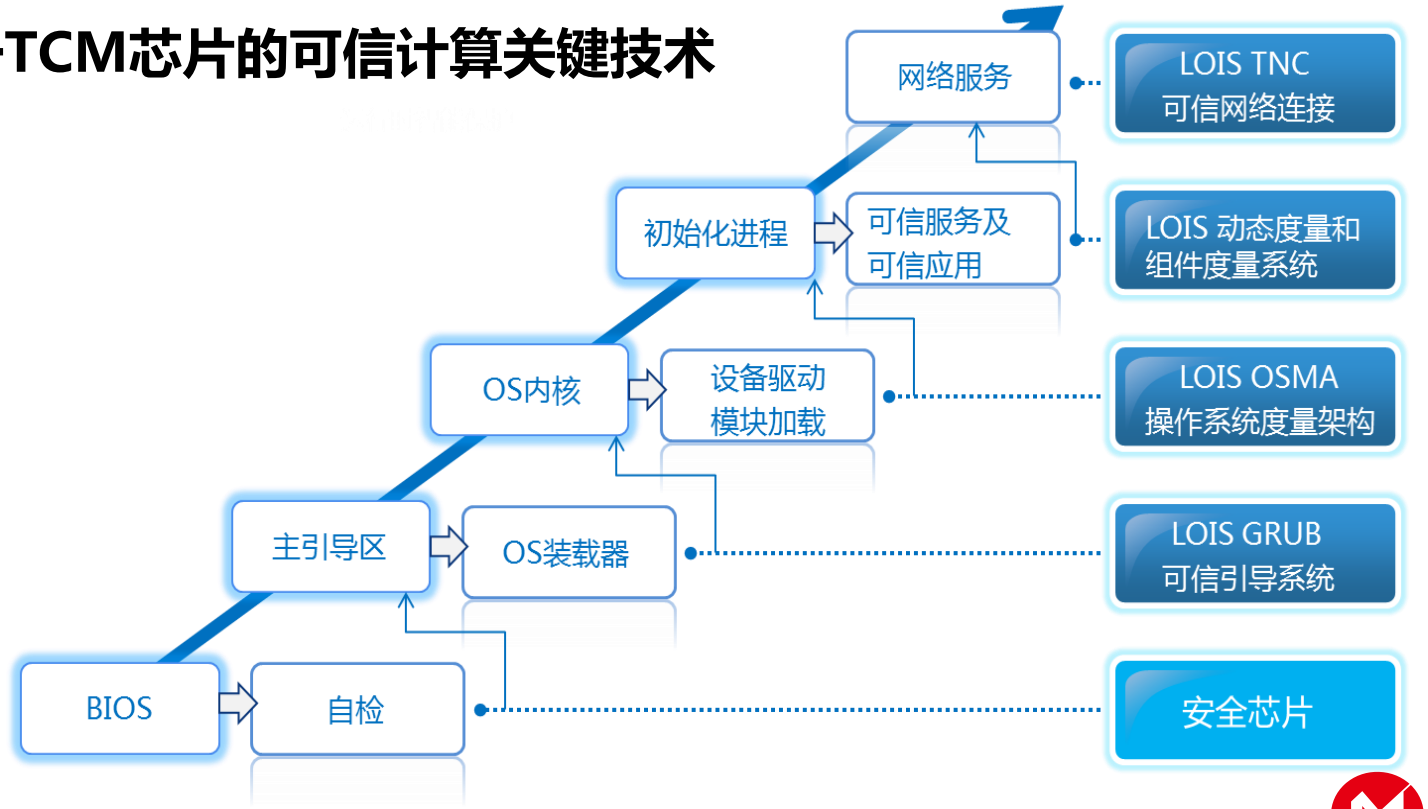


- **建立信任链**

1)从信任根开始，到硬件平台，到操作系统，再到应用软件；

2)一级度量认证一级，一级信任一级，把这种信任扩展到整个计算机系统。

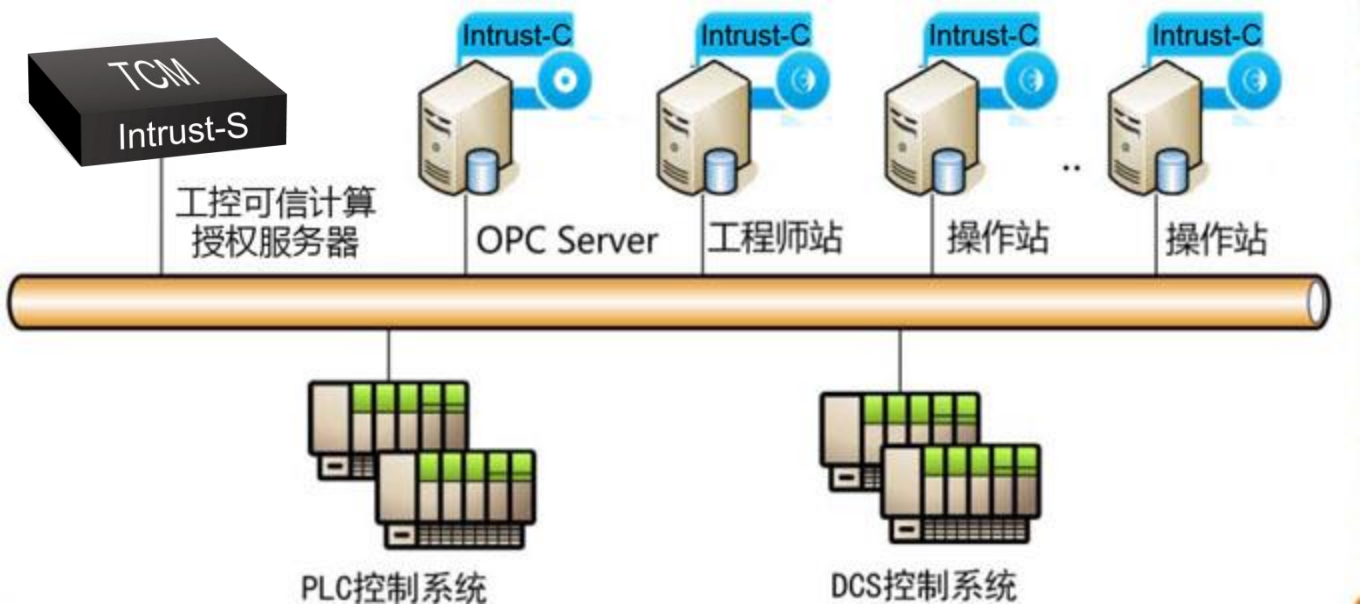
- **基于TCM芯片的可信计算关键技术**



Intrust工控可信计算安全平台

典型应用

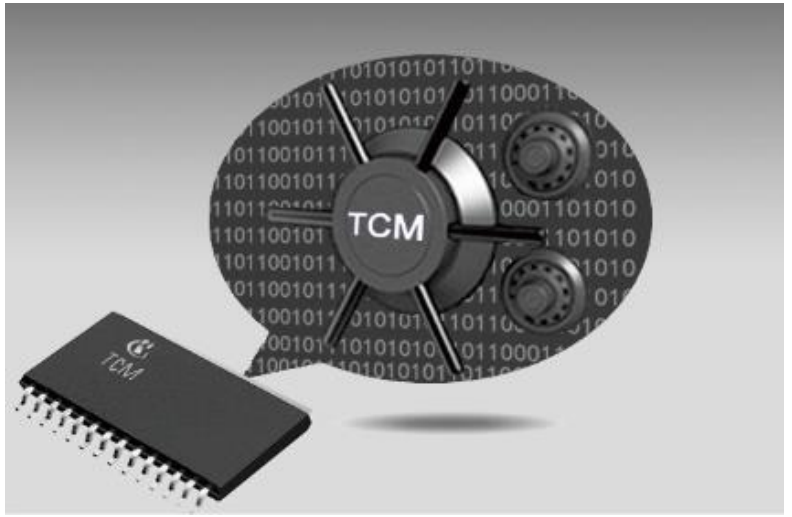
- 工控可信计算授权服务器
- 工控可信安全平台客户端软件



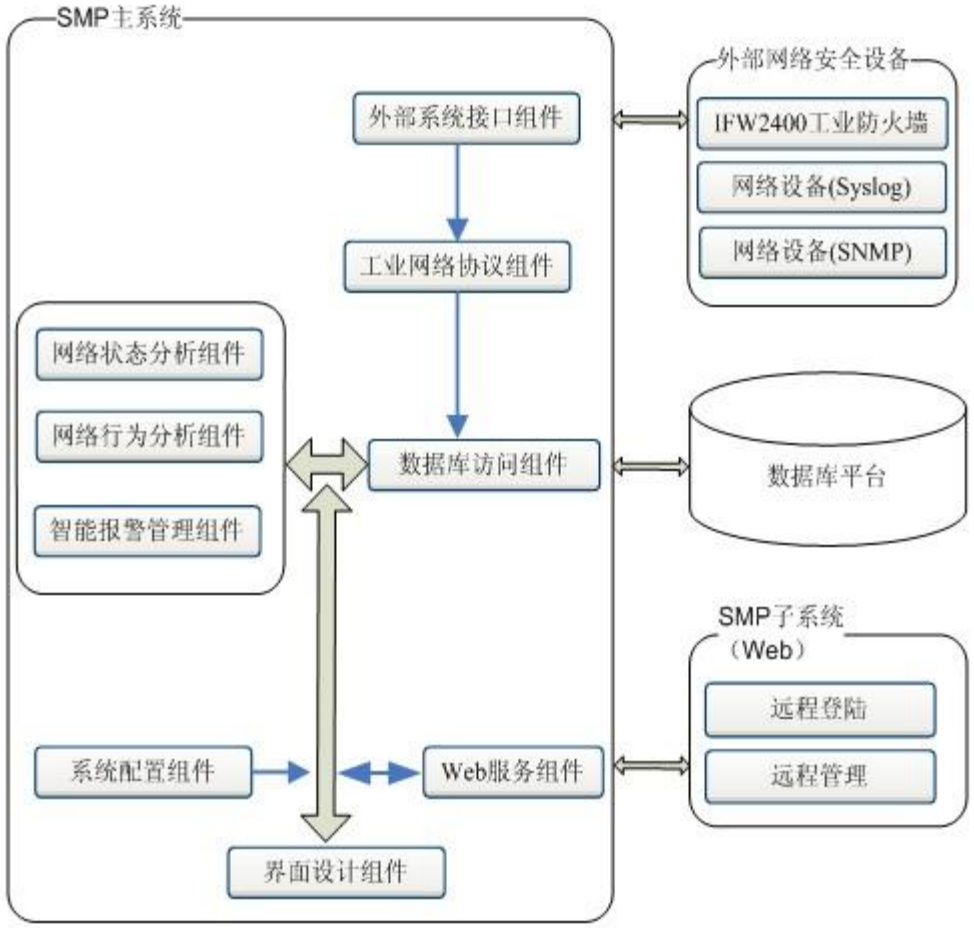
Intrust工控可信计算安全平台

产品优势

- 基于TCM芯片，独有的加密算法
- 专业为工控环境开发
- 可升级的工控系统知识库功能模块，方便用户对系统的部署
- 基于白名单模式，从底层BIOS开始管控所有进程
- 实时监控系统中的可信进程，杜绝未知恶意程序启动
- **强大的USB等可移动设备管控功能**
- B/S架构模式，保证系统自身的易管理性和安全性
- 独有的内核驻留程序，即使关闭软件也能正常执行管控功能



（五）安全管理中心SMP



安全管理中心总体结构图

- 安全管理中心以底层工业防火墙、审计平台、可信计算平台、恶意软件动态分析平台及其它第三方网络设备为探针
- 利用内置的“工业控制网络通讯行为模型库”核心模块，智能监控、分析控制网络行为，及时检测工业网络中出现的工业攻击、非法入侵、设备异常等情况
- 利用数据库存储、分析和挖掘技术，对危及系统网络安全的因素做出智能预警分析
- 给管理者提供决策支持，以总揽大局的方式为工厂网络信息安全故障的及时排查、分析提供了可靠的依据。

网络监控画面及实时报警

网络监控画面及实时报警

（六） 工业信息安全培训

培训内容

- 工业网络和安全概述
- 工厂网络结构
- 工厂网络设备及应用
- 工业网络通讯协议
- 工厂安全事件与漏洞分析
- 工控信息安全关键技术
- 系统风险评估
- 工控信息安全国际防护先进理念
- 我国安全等级保护标准在工控领域的应用

（七） 工控系统安全评估与咨询

- 结合工控信息安全的独特性，将应用功能安全HAZOP分析方法对工控系统信息安全进行评估；
  - Hazard *and* Operability （危险性与操作性）
  - 英国帝国化学公司ICI在60年代提出
  - 是所有工艺危害分析/安全评价方法中系统性、全面性最好的方法
- 常规IT测试方法仅用于离线测试或者实验室仿真验证；
- 密切结合国内标准规范为依据，最终给出评估报告；
  - **GB/T 30976.1-2014 工业控制系统信息安全评估规范**

- 能够识别潜在由信息安全攻击导致的生产过程风险；（哪里有问题）

评估方法概述

- 评估分成系统级（风险）和节点设备级（漏洞及脆弱性）分别进行

- 系统级离线评估软件具备
  - 智能化网络节点库（积累各类工控系统模型）
  - 智能化网络安全威胁库（HAZOP分析方法下的威胁分析列表）
  - 工控设备漏洞库（融合国际和自身积累形成）

- 节点设备级测试
- 基于验证环境的设备测试，应用阿杰里斯WurldTech等专业测试设备

系统-产品-人员-认证服务

- **Functional Cyber-Security**
  - Achilles Level 1-2
  - ISA Secure Levels 1 – 3
  - IEC 62443 Series
- **Functional Safety Certification**
  - IEC 61508
  - IEC 61511
  - IEC 62061 / ISO 13849
  - IEC 26262
  - EN 50271
  - EN 50128/50129*

ACLASS

CERTIFICATE OF ACCREDITATION

ANSI-ASQ National Accreditation Board/ACLASS
500 Montgomery Street, Suite 625, Alexandria, VA 22314, 877-344-3044

This is to certify that

exida.com, LLC
64 N. Main Street
Sellersville, PA 18960

has been assessed by ACLASS
and meets the requirements of international standard

ISO/IEC 17025:2005

while demonstrating technical competence in the field(s) of

TESTING

Refer to the accompanying Scope(s) of Accreditation for information regarding the types of tests to which this accreditation applies.

AT-1531
Certificate Number

ACLASS Approval

Certificate Valid: 03/24/2011-03/24/2013
Version No. 001 Issued: 03/24/2011

This laboratory is accredited in accordance with the recognized International Standard ISO/IEC 17025:2005. This accreditation demonstrates technical competence for a defined scope and the operation of a laboratory quality management system (*refer to joint ISO-ILAC-IAF Communiqué dated January 2009*).

CERTIFICATE of ACCREDITATION
PRODUCT CERTIFICATION

The American National Standards Institute hereby affirms that

exida.com L.L.C
64 North Main Street, Sellersville, PA 18960, USA

ACCREDITATION ID# 1004

meets the ANSI accreditation program requirements and those set forth in

ISO/IEC Guide 65: 1996 General Requirements for Bodies Operating Product Certification Systems
EDSA-100 ISA Security Compliance Institute - Embedded Device Security Assurance - ISASecure certification scheme Version

for programs within the following

SCOPE OF ACCREDITATION

GRANTED 2011-11-30
ISASecure Embedded Device Security Assurance (EDSA)

ANSI
ANSI Accredited Program PRODUCT CERTIFICATION

2013-12-01

The manufacturer may use the mark:

Report:
GEE 09-08-29 R001 v11 IEC 61511 Design Basis Approval 109FB A16 SS

Validity:
This Design Basis Approval is valid for 109FB Gas Turbine & A16 Steam Turbine Single Shaft – Gas and Liquid option and includes all development steps up to and including the Factory Acceptance Test / First Article Test.

This assessment is valid until April 30, 2013.
Revision 1.1 April 26, 2010

exida
Certification Services

Certificate / Certificat
Zertifikat / 合格証

GEE 090829 C002

exida hereby confirms the Design Basis Approval of the:

109FB Gas Turbine & A16 Steam Turbine Single Shaft – Gas and Liquid Fuel
GE Energy
Greenville, SC
USA

The 109FB Gas & A16 Steam Turbine Single Shaft, its engineering process, the engineering process deliverables, and the Factory Acceptance Test / First Article Test have been evaluated and assessed per the relevant requirements of:

IEC 61511 Part 1

The assessment concludes that the 109FB Gas & A16 Steam Turbine Single Shaft was designed and developed in accordance with this standard up to and including the Factory Acceptance Test / First Article Test.

As a result a

Design Basis Approval

is issued.

Application Restrictions:
The unit must be properly installed and maintained per the Safety Manual requirements.

Product Assessor

Auditor

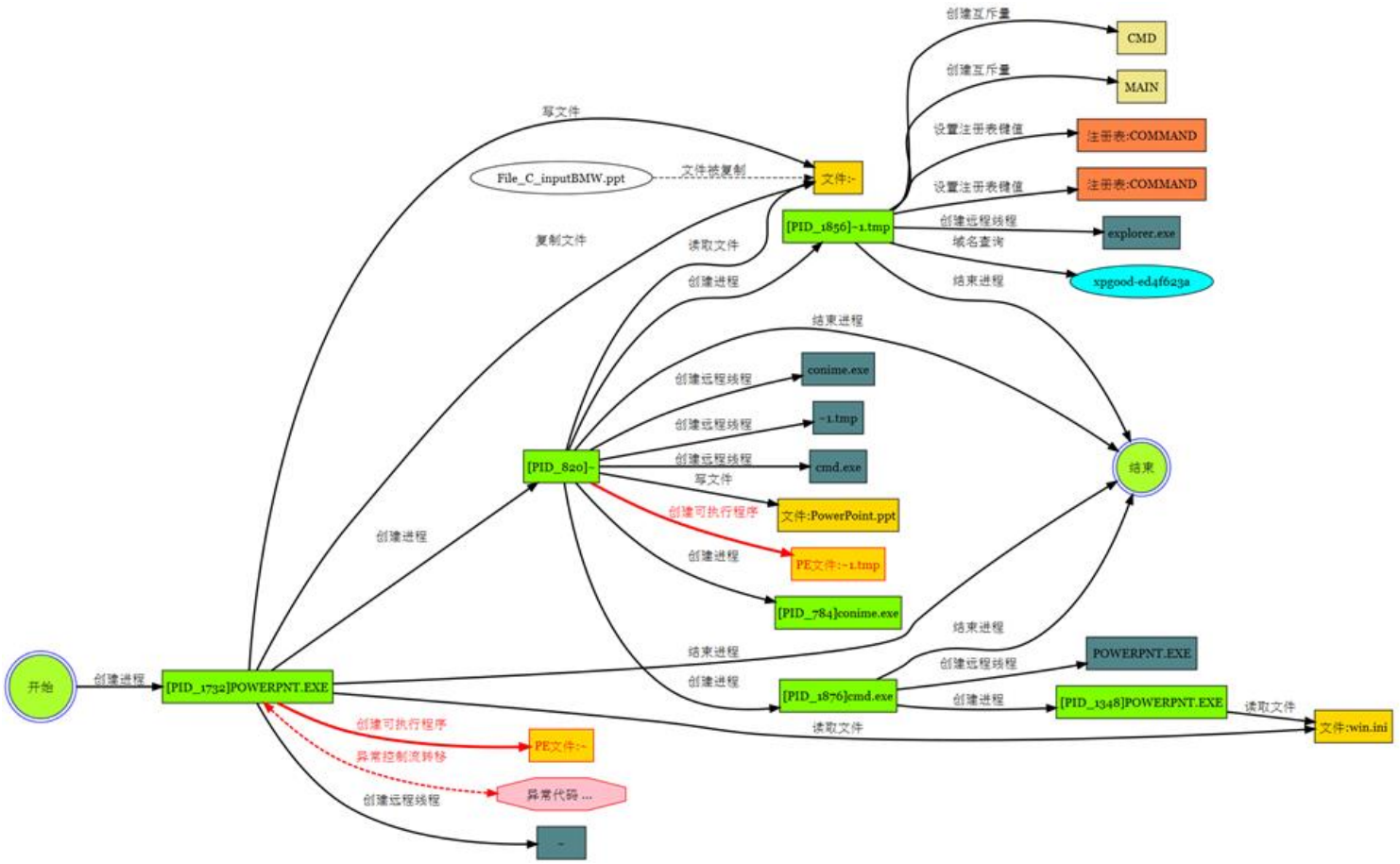
（八） 工业信息安全实验室

海天炜业拥有业内规模领先，设备完善的工业网络安全实验室，配备有HONEYWELL、SIEMENS、Yokogawa、Emerson、AB-Rockwell、Schneider、安控、中控、和利时等主流工控系统，以及专业网络测试仪、高负荷稳定性测试系统、高低温测试仪等测试分析设备。

功能展示

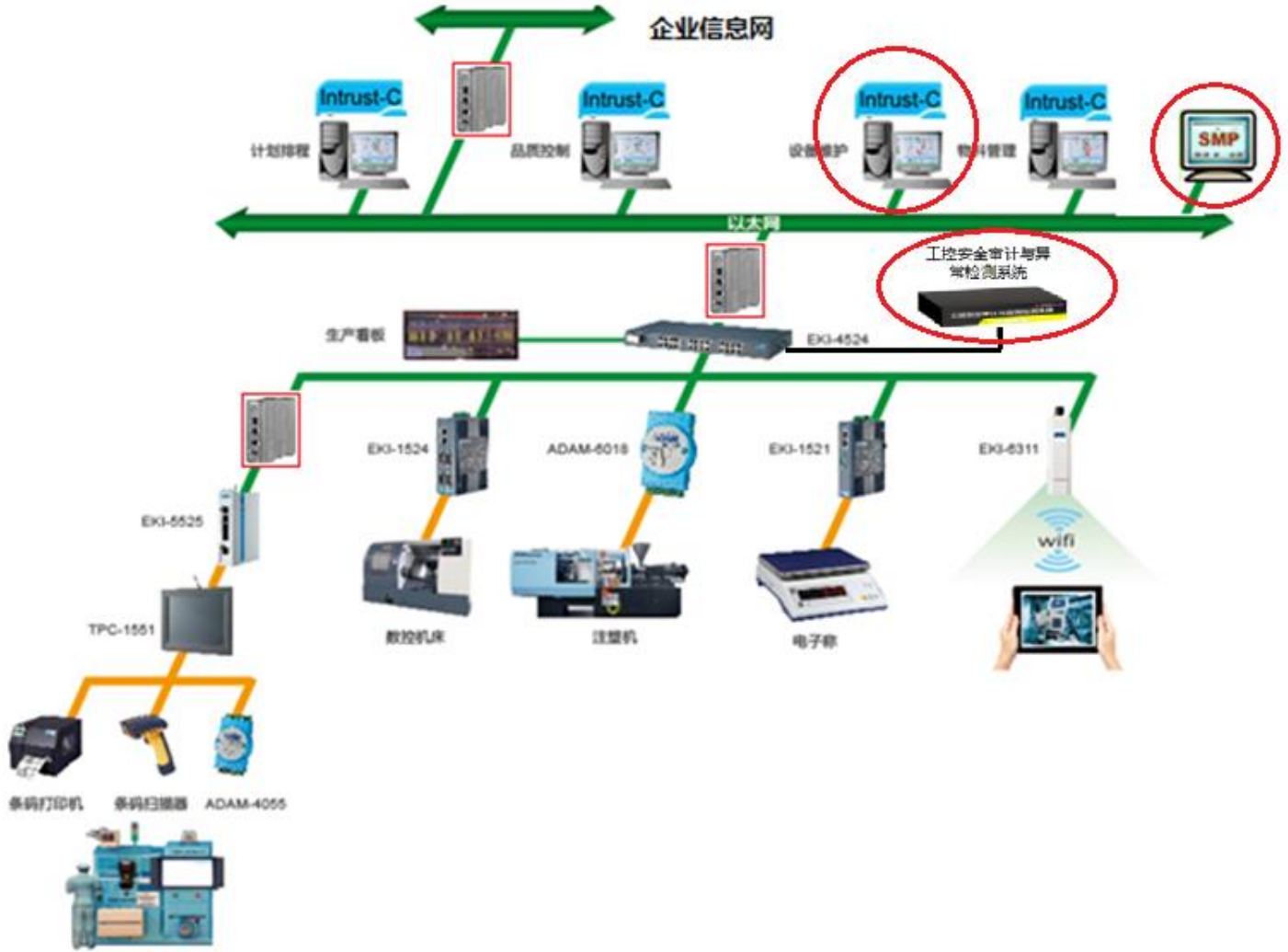
- 工控系统漏洞挖掘及防护研究
- 工业信息安全设备测试
- 工业信息安全事件搜集与分析
- 工业信息安全实验平台搭建
- 工业攻防演练
- 技术展示
- 安全测试
- 技术交流
- 资源共享

实验室--工控信息安全应急响应应中心



为用户提供安全应急响应及基于样本恶意代码分析服务

产品整体解决方案示意图



MOSES 海天煒業
服 務 提 升 價 值

MOSES

海天煒業

服 務 提 升 價 值

www.mosesceo.com

谢 谢！