附件 2

控制系统“一条龙”应用计划申报指南

一、产业链构成

立足现有数据采集与监视控制系统（SCADA）、分散型控制系统（DCS）和地铁交通综合监控系统的基础，瞄准石油化工、轨道交通、电力电网等系统级用户，以产业链上下游供需能力为基础，应用为导向，针对关键环节重点基础产品、工艺，推动相关重点项目建设和技术突破，开发相关领域高安全要求的安全控制系统，创建安全系统的试验环境，相关环节取得国际功能安全的认证，建设高质量要求的生产线，从试点应用到逐步推广。

关键产业链条环节

序号	产业链环节		石油石化行业控制系统	轨道交通行业控制系统	电力电网控制系统
1.	控制系统安全设计			√	
2.	安全控制系统	SOC 芯片			√
3.		高性能实时总线芯片	√	√	√
4.		实时操作系统	√	√	√
5.		工业边缘计算网关及服务器	√	√	√
6.		通信协议		√	
7.		数据采集与监视控制系统（SCADA）	√		
8.		分散型控制系统（DCS）	√		
9.		安全仪表系统	√	√	
10.	安全防护系统	网络安全监管及态势感知系统	√	√	√
11.		控制系统网络安全防护系统	√	√	
12.	试验验证环境	软件与信息安全试验验证环境	√	√	√
13.		控制系统可靠性试验验证环境	√	√	√
14.	安全可靠认证体系			√	
15.	行业用户示范应用		√	√	√

二、目标和任务

（一）石油石化行业控制系统

1. 高性能实时总线芯片

（1）环节描述及任务。研究控制系统高性能实时总线芯片，以及配套编程环境；研制基于高性能实时总线芯片开发的通信协议栈和总线通信板卡；研制基于高性能实时总线芯片传统总线的协议兼容网关。

（2）具体目标。最大传输距离不低于 500 米；最大传输速率：100Mbit/s；最小循环周期不大于 8 微秒；单网段节点数不低于 256 个；单网段节点网络延时不高于 500 微秒；时间同步精度不高于 100ns；支持自动检错和纠错；支持非对称加密；支持总线和环形总线；兼容 ETHERNET/IP、PROFINET、MODBUS TCP/IP 等工业以太网协议；兼容 HART、PROFIBUS、MODBUS、CAN 等工业总线协议。

2. 实时操作系统

（1）环节描述及任务。研究能够高效支撑工业高实时应用和非实时应用的工业级操作系统，具有丰富的生态兼容支持能力和可靠的安全机制。

（2）具体目标。操作系统具有调试能力和故障诊断能力、支持底层驱动开发、集成丰富的函数库、自带 TCP/IP 等通讯协议栈，具备二次开发能力，二次开发语言支持 C/C++等通用编程语言。提供虚拟化环境下的实时保障，提供实时虚拟机对 CPU 核、外围 IO 设备的独占机制，实时虚拟机中断响应时间达到 us 级，实时虚拟机切换时间小于 5us。支持主流的 X86、ARM、龙芯等 CPU 架构。支持

主流桌面系统、实时系统同时运行，非实时系统和各实时系统独立运行、互不影响。支持不少于20个虚拟机。提供开发工具，支持对虚拟机的全生命周期管理。提供对设备整体状态及虚拟机实例状态的多维度实时状态监控。支持实时系统与非实时系统间的高速数据交换。支持外设虚拟化及直接透传。实时功能模块化，支持灵活裁剪。

3. 工业边缘计算网关及服务器

（1）环节描述及任务。研究适应于工业现场复杂恶劣环境，具备边缘计算、过程控制、运动控制、机器视觉、现场数据采集、工业协议能力的边缘计算装置。

（2）具体目标。研发设计安全的工业边缘计算服务器系统与软件，可持续迭代演进；取得与工业边缘计算服务器相关的实用新型、发明、外观等专利，并实现与之配套的运营环境及编程环境。实现多虚拟运行环境的隔离，实现高实时应用和非实时应用的隔离互不干扰，单台装置支持不少于20个完全独立的运行环境；控制计算周期支持50us~10ms的配置；支持IEC61131编程、C/C++编程，支持图形化编程；支持通用运动控制，逻辑运算、位置速度加速度控制、路径规划、闭环控制、插补运算；支持机器视觉神经网络计算架构，辅助算力不低于30TOPS；支持常用工业协议与规约，支持Modbus TCP、Ethernet/IP、CAN、S7、EtherCAT、101/104规约、IEC61850规约、IEC61375规约、MQTT、OPC-UA等10种以上典型工业协议与规约；适应恶劣工作环境，无风扇设计，-40~75°C宽温运行，IP40防护。

4. 数据采集与监视控制系统（SCADA）

（1）环节描述及任务。围绕石油石化行业用户的需求，基于 C/S 或 B/S 架构，研发具备安全控制功能的数据采集与监视控制系统，可以采集标准通讯协议以及私有通讯协议的数据报文，并实时处理，将重要数据存入历史数据库，并进行分析和处理，发现异常情况及时报警和预警。

（2）具体目标。包含数据采集、基础平台、人机界面和基础应用等子系统，支持石油石化行业共性应用开发，具备如石油或天然气长输管道管网、炼油等调度控制 SCADA 系统开发案例。单服务器实时历史库支持管理容量至少百万点；1 秒内可以完成计算实例至少 1 万点；从数据采集到人机界面显示的平均响应时间最长 1 秒；从产生开关量报警到人机界面显示的平均响应时间最长 2 秒；从产生模拟量报警到人机界面显示的平均响应时间最长 3 秒；人机界面下发命令平均响应时间最长 1 秒；实时数据最小采集周期为 50 毫秒；实时历史库中记录数据时间戳精确到毫秒位；冗余服务器的平均切换时间最长 5 秒；主备网络的平均切换时间最长 1 秒，主备中心的平均切换时间最长 10 秒。支持毫秒级精度实时数据存储和显示；支持采集器分布式部署和断线续传；数据库支持 Windows/FreeBSD/Linux 部署。HMI 支持多媒体的插入。支持脚本语言。画面实时数据刷新的速率要求不大于1秒。(按至少100个模拟量和200个开关量计算)；画面下发命令响应时间要求不大于 1 秒。

5. 分散型控制系统（DCS）

（1）环节描述及任务。围绕石油化工、炼油等用户的需求，开发制造具有安全的 DCS 控制系统，主要包括主机模块（CPU 模块）、

电源模块、输入输出 IO 模块、通信模块等组件。

（2）具体目标。具备典型石油石化工艺的应用功能，具备典型场景的 DCS 系统建设项目经验。支持指令集和标准通信协议，如 Modbus、OPC UA、Profinet、Ethernet/IP、IEC 104、IEC61850 等。在工控网络安全方面，在硬件及软件设计中应考虑网络安全的需求，能防止非较大努力实现的非法访问和破坏。开发安全、稳定、可靠的冗余方式，整体冗余切换时间要不大于 50ms。最大支持 4000 个模拟量和 6.5 万个开关量点。满足恶劣环境条件下（-20℃-70 ℃ ）的应用能力。电磁兼容性 EMC3 级抗电磁干扰能力。满足 ANSI/ISA S71.04 标准 G3 级别防腐能力。1G 加速度抗振动能力。输入输出卡件（IO）支持硬件冗余功能，稳定可靠。整体切换时间 20ms。平均无故障时间（MTBF）超过 20 万小时。

6. 安全仪表系统

（1）环节描述及任务。开发安全仪表系统安全程序编程调试开发平台软件和控制平台软件。实现集成开发或支持第三方开发的编程与运行软件、功能模块，可灵活配置，支持多重化冗余表决的主机模块（CPU 模块）、电源模块、输入输出模块、功能模块、通信模块等组件。

（2）具体目标。满足石油化工行业的紧急停车系统、火焰烟气监测系统、燃烧管理系统、压缩机控制系统、安全防护系统的需求。架构上重点解决容错架构、在线诊断、多重化冗余表决、安全失效、故障隔离、多样性设计等。采用和体现面向对象编程理念，符合 GBT15969.3(对应国际标准：IEC61131-3)标准，并支持梯形图、语句表、顺序功能图、结构化文本等多种程序描述方法，支持程序的仿

真运行，支持远程编程调试和诊断维护。支持高响应速度、高诊断覆盖率、低失效率的性能处理。输入端到输出端响应时间不大于100ms，数字量 I/O 点≥1024 点，模拟量 I/O 点不小于 512 点。支持多重化容错设计，支持表决模式、降级模式，在开发架构上，考虑工业互联网平台技术体系下安全仪表系统可能的架构改变。支持具备安全协议的现场总线和工业以太网通讯。特定单元、模块满足安全控制功能的要求，通过 IEC61508 SIL3 级认证，满足信息安全等保 3 级要求。

7. 网络安全监管及态势感知系统

（1）环节描述及任务。拥有控制系统多源数据融合分析系统，感知石油石化行业的重点区域、重点企业的工业控制系统网络安全风险，发现潜在的网络攻击，提升工业控制系统安全监测、威胁预警、攻击取证、态势呈现等能力；拥有行业性的工业控制安全防护系统，提升工业控制系统网络防护、异常监测、漏洞发现、主机加固等能力，实现密码在工业控制系统中的信息传递、主机保障等方面的深度应用；研究工控系统自主技术和密码技术在石油石化行业中应用的具体要求和技术条件，将密码与网络安全要素紧密融合在工控系统中，研制安全可控的工控系统核心部件。

（2）具体目标。具备工控协议的检测控制不少于 50 种，其中具备提供指令级工控协议控制不少于 5 种；研制工业控制安全防护系统 1 套，具备边界防护、漏洞扫描、终端防护、安全通信、异常监测、区域隔离等功能；研制安全可控的工控系统核心部件 1 套，具备工控协议识别与内容检测、数据完整性保护等功能。

8. 控制系统网络安全防护系统

（1）环节描述及任务。围绕工业行业工业控制系统的特点，研制行业性的工业控制安全防护系统，具备网络防护、异常监测、漏洞发现、主机加固等能力，实现密码在工业控制系统中的信息传递、主机保障等方面的深度应用；核心部件具备密码与网络安全要素融合在工控系统中。围绕控制系统网络体系中边缘层、工业 IaaS 层、工业 PaaS 层、工业 SaaS 层面临的突出安全风险，综合考虑管理要求和技术要求要素，应用工业互联网平台安全防护核心技术，形成抗 DDoS、虚拟机逃逸、镜像篡改、数据窃取与篡改等安全防护能力，提升工业互联网平台企业自身安全防护和态势感知能力。

（2）具体目标。具备防攻击、防病毒、防入侵、防窃密、防控制等安全防护能力；支持不少于 30 家企业设备的安全接入认证，保护接入设备安全性、隐私性。在安全评估测试以及管理运维方面，形成 1 套检测规范，2 套制度流程规范，提升企业应急响应能力和信息安全事件处理效率。

9. 控制系统软件与信息安全试验验证环境

（1）环节描述及任务。建设石油石化行业工业控制系统安全检测验证环境，打造仿真验证、攻防演练、安全培训、系统评估等基础系统，为石油石化行业工业控制系统综合防护能力提供指导工作，为技术研究、人员培训、漏洞检测、密码检验等提供基础平台。

（2）具体目标。建设工业控制系统安全检测验证实验平台，具备工控安全检测、技术研究、人才培训、成果验证、风险分析的能力。具备相关服务项目经验，针对石油石化行业开展风险评估、漏洞检测、技术培训等服务。

10. 控制系统可靠性试验验证环境

（1）环节描述及任务。具备可靠性、失效分析、电磁兼容功能性能等内容的试验验证环境。

（2）具体目标。依据产品的可靠性目标、参考相关国际标准化组织或者行业协会制定的相关标准或规范，确定所采用的测试项目及条件。具备样品制备、系统级分析、封装级分析、芯片级失效分析等流程及能力。具备辐射抗扰度、传导抗扰度、电快速瞬态（EFT）脉冲群抗扰度、芯片上电状态下的静电放电（ESD）抗扰度等测试环境及能力。

11. 石油石化行业示范应用

（1）环节描述及任务。培育炼油化工、油气管道等细分行业和领域的安全控制系统集成商或行业大用户,选择示范行业/领域，形成样板应用系统，并逐步推广和拓展。鼓励系统集成商或行业大用户与安全控制系统厂商建立紧密联系，使安全控制系统厂商具备良好的销售和工程服务网络。推动安全控制系统的大规模应用和产业化发展。

（2）具体目标。在炼油化工领域进行示范应用（DCS 系统），在应用中对系统各项指标进行综合验证。在油气管道领域进行示范应用，包括输油站和调度控制中心，对控制系统进行综合测试和性能评估。在示范应用基础上，在国内油气管道上进行推广。

（二）轨道交通行业控制系统

12. 控制系统安全设计

（1）环节描述及任务。对标 GB17859 或 61508 等标准规范，按照网络信息安全和功能安全的需要，研发控制系统编程软件，积累

形成相关工业知识和开发模块，对系统进行网络安全的加固设计。

（2）具体目标。研究高安全轨道交通列控系统产业链总体解决方案，使列控系统达到 IEC61508 规定的 SIL4 级功能安全等级，并满足相关网络信息安全等级保护标准要求。研发功能安全嵌入式实时操作系统安全设计规范，功能安全完整性达到 IEC61508 规定的 SIL3 级和 EN50128 规定的 SIL4 级。研究轨道交通列控系统网络信息安全加固方案，围绕列控主机、列控设备、列控网络和列控数据，深入分析安全防护需求，构建基于网络隔离、入侵监测、主机防护、安全核查等技术的纵深防御体系，形成防攻击、防病毒、防入侵、防窃密、防控制等安全防护能力。研究高安全等级的通信解决方案。在具备防火墙、网闸等基本信息安全功能的基础上，针对轨道交通控制应用，提出通用通信协议的加固方案及轨道交通专用安全通信协议，全面提升设备间通信安全防护能力。

13. 高性能实时总线芯片

（1）环节描述及任务。研究控制系统高性能实时总线芯片，以及配套编程环境；研制基于高性能实时总线芯片开发的通信协议栈和总线通信板卡；研制基于高性能实时总线芯片传统总线的协议兼容网关。

（2）具体目标。最大传输距离不低于 500 米；最大传输速率：100Mbit/s；最小循环周期不大于 8 微秒；单网段节点数不低于 256 个；单网段节点网络延时不高于 500 微秒；时间同步精度不高于 100ns；支持自动检错和纠错；支持非对称加密；支持总线和环形总线；兼容 ETHERNET/IP、PROFINET、MODBUS TCP/IP 等工业以太网协议；兼容 HART、PROFIBUS、MODBUS、CAN 等工业总线

协议。

14. 实时操作系统

（1）环节描述及任务。研究能够高效支撑工业高实时应用和非实时应用的工业级操作系统，具有丰富的生态兼容支持能力和可靠的安全机制。

（2）具体目标。操作系统具有调试能力和故障诊断能力、支持底层驱动开发、集成丰富的函数库、自带 TCP/IP 等通讯协议栈，具备二次开发能力，二次开发语言支持 C/C++等通用编程语言。提供虚拟化环境下的实时保障，提供实时虚拟机对 CPU 核、外围 IO 设备的独占机制，实时虚拟机中断响应时间达到 us 级，实时虚拟机切换时间小于 5us。支持主流的 X86、ARM、龙芯等 CPU 架构。支持主流桌面系统、实时系统同时运行，非实时系统和各实时系统独立运行、互不影响。支持不少于 20 个虚拟机。提供开发工具，支持对虚拟机的全生命周期管理。提供对设备整体状态及虚拟机实例状态的多维度实时状态监控。支持实时系统与非实时系统间的高速数据交换。支持外设虚拟化及直接透传。实时功能模块化，支持灵活裁剪。

15. 工业边缘计算网关及服务器

（1）环节描述及任务。研究适应于工业现场复杂恶劣环境，满足国内主流控制器、工业机器人、智能传感器等工业设备的接入和数据解析的需求，支持边缘端数据运算及通过互联网推送数据到云平台功能的网关。具备边缘计算、过程控制、运动控制、机器视觉、现场数据采集、工业协议能力的边缘计算装置。

（2）具体目标。研发设计安全的工业边缘计算服务器系统与软

件，可持续迭代演进；取得与工业边缘计算服务器相关的实用新型、发明、外观等专利，并实现与之配套的运营环境及编程环境。实现多虚拟运行环境的隔离，实现高实时应用和非实时应用的隔离互不干扰；支持同时上线运行的异构执行体不少于 3 个，实现对不同行业工业设备不少于 30 种不同设备接入和协议解析功能；3 个千兆以太网、2 个串口、1 个 USB 接口、支持无线功能，支持 2G/3G/4G 等移动网络；支持本地数据缓存、断线续传功能；支持透传或 VPN 模式远程调试与下载自动化控制程序；具备远程配置、远程升级、网关远程监控等。

16. 通信协议

（1）环节描述及任务。研发满足国际功能安全要求和安全防护能力的通信协议，包括私有协议和标准协议，满足不同行业以及不同应用场合的需求。

（2）具体目标。设计开发符合 IEC61508 规定的 SIL3 级的 TCP/IP 协议栈。针对轨道交通行业功能安全要求，协议栈针对功能安全进行优化，并进行功能安全加固，提高协议栈的稳定性和可靠性。TCP/IP 协议栈可以作为功能安全操作系统中的一个软件组件使用，也可以作为单独的组件在无操作系统的环境下使用。TCP/IP 协议栈支持 IPV4、DHCP、UDP、TCP、ICMP、ARP，支持路由功能，支持组播通信。通过国际功能安全的认证，故障安全完整性等级不低于 SIL2，支持节点数不少于 32 个，支持 Server/Client 通讯，支持 TCP 或 UDP 通讯模式。参照 EN50159 先关标准中关于封闭通信网络和开放网络传输的安全通信防护标准，能够对重复、丢失、插入、乱序、损坏、延迟、伪装等通信风险进行防范；采用 3DES、国标加密等算

法，满足开放网络的安全加密等级标准，保证数据的通信安全。安全协议采用分层设计以及灵活的可裁剪配置设计，满足不同处理能力平台的使用要求，链路层支持 HDLC、TCP、UDP、CAN 等多种方式，并且支持多点连接。

17. 安全仪表系统

（1）环节描述及任务。具备自主知识产权的安全计算机系统平台，主要包括支持多重化冗余表决的主机模块（CPU 模块）、电源模块、输入输出模块、功能模块、通信模块等组件，实现安全计算和安全输出。

（2）具体目标。开发的安全计算机系统平台，满足轨道交通列车控制系统、安全防护系统等的需求，能兼容车载和轨旁的应用。架构上重点解决容错架构、故障诊断、同步处理、多重化冗余表决、安全失效、故障隔离、多样性设计等。在性能上，支持数字量 I/O 点≥2048 点，主机模块同步相位差小于 12us，主机模块完成 I/O 的读写操作时间不大于 10ms，轮询 I/O 的周期不大于 50ms。重点解决高响应速度、高诊断覆盖率、低失效率、安全控制等功能要求。支持表决模式、降级模式，系统达到 SIL4 安全认证。

18. 网络安全监管及态势感知系统

（1）环节描述及任务。具备工业控制系统的监测、预警、审计和接入防护等技术，实现对外部攻击及内部非法操作的预警防御和应急响应，有效地实现防外及安内，防止因网络安全事件造成重大安全生产事故，保障信息系统安全。支持多源数据融合分析，感知重点区域、重点企业安全风险、潜在网络攻击，

（2）具体目标。支持自动识别网络内的资产和工控设备；设备

在线运行状态监测集中展现工控系统信息安全态势，建成工业控制系统多源数据融合分析系统 1 套，具备工控协议的检测控制不少于 50 种，其中具备提供指令级工控协议控制不少于 5 种；研制工业控制安全防护系统 1 套，具备边界防护、漏洞扫描、终端防护、安全通信、异常监测、区域隔离等功能；研制安全可控的工控系统核心部件 1 套，具备工控协议识别与内容检测、数据完整性保护等功能。

19. 控制系统网络安全防护系统

（1）环节描述及任务。围绕工业行业工业控制系统的特点，研制行业性的工业控制安全防护系统，具备网络防护、异常监测、漏洞发现、主机加固等能力，实现密码在工业控制系统中的信息传递、主机保障等方面的深度应用；核心部件具备密码与网络安全要素融合在工控系统中。围绕控制系统网络体系中边缘层、工业 IaaS 层、工业 PaaS 层、工业 SaaS 层面临的突出安全风险，综合考虑管理要求和技术要求要素，应用工业互联网平台安全防护核心技术，形成抗 DDoS、虚拟机逃逸、镜像篡改、数据窃取与篡改等安全防护能力，提升工业互联网平台企业自身安全防护和态势感知能力。

（2）具体目标。具备防攻击、防病毒、防入侵、防窃密、防控制等安全防护能力；支持不少于 30 家企业设备的安全接入认证，保护接入设备安全性、隐私性。在安全评估测试以及管理运维方面，形成 1 套检测规范，2 套制度流程规范，提升企业应急响应能力和信息安全事件处理效率。

20. 控制系统软件与信息安全试验验证环境

（1）环节描述及任务。根据国家软件测评、信息安全测评标准，参照系统使用的需求，建立试验验证方法论、试验验证环境和测评

质量管理体系，开展轨道交通行业控制系统系统测评、信息安全测评等。

（2）具体目标。参与国家信息安全相关标准制定，拥有控制系统、机器人等信息安全、软件试验验证环境。近三年开展轨道交通控制系统测评、信息安全测评项目 5 项以上。

21. 控制系统可靠性试验验证环境

（1）环节描述及任务。具备可靠性、失效分析、电磁兼容功能性能等内容的试验验证环境。

（2）具体目标。针对轨道交通行业被测对象仿真测试规模大、异构度高、实时性强、自动化要求高等需求，研究基于分布式半实物的仿真测试架构、面向复杂工程系统的建模方法、多源数据多层面可追溯性测试管理方法、自动测试、故障注入再现及分析方法、安全控制系统接口监测、测试环境资源优化配置等重大核心技术，提高被测系统缺陷纠正率和质量可信度，实现对列控系统、货运、行车指挥等系统的方案验证、功能开发、系统集成、工程实施等全生命周期各个阶段的测试验证和技术支撑。具备相关行业的试验验证项目经验。

22. 安全可靠认证体系

（1）环节描述及任务。拥有轨道交通安全控制系统全寿命周期的安全性和可靠性认证规范。具备安全控制系统故障预测模型与可靠性改进体系。拥有包括硬件可靠性设计、物料优选、可靠性仿真分析、可靠性试验、可靠性和安全性管理等可靠性保障团队。

（2）具体目标。以欧标 EN50126 和 EN50129 中的安全性和可靠性要求为基础，结合国内轨道交通安全控制系统的特点，拥有轨

道交通安全控制系统全寿命周期的安全性和可靠性认证规范。初步建立安全控制系统故障预测模型与可靠性改进体系，具备可靠性仿真分析平台和故障报告、分析和纠正措施平台。基于安全控制系统的历史数据、现场数据和应用环境数据等信息，通过可靠性仿真分析平台对控制系统可靠性进行预测和分析，寻找薄弱环节并进行改进，从而获得可靠性的提升。建立安全控制系统可靠性试验和验证平台，从设计开发、样机测试到批量生产，全方位保证并提升系统可靠性，同时制定相关可靠性试验验证标准。拥有包括硬件可靠性设计、物料优选、可靠性仿真分析、可靠性试验、可靠性和安全性管理等可靠性保障认证人员。确保安全控制系统的开发过程遵循可靠性和安全性认证规范，并符合安全可靠认证体系中的流程和标准，从而使得安全控制系统均能达到 SIL 等级 3 级或者 4 级的要求。

23. 轨道交通行业示范应用

（1）环节描述及任务。培育轨道交通、高铁列控的细分行业和领域的安全控制系统集成商或行业大用户,选择示范行业/领域，形成样板应用系统，并逐步推广和拓展。鼓励系统集成商或行业大用户与安全控制系统厂商建立紧密联系，使安全控制系统厂商具备良好的销售和工程服务网络。推动安全控制系统的大规模应用和产业化发展。

（2）具体目标。实施城市级管廊轨道交通控制系统建设项目，或拥有城市轨道交通控制系统、高铁列控系统的典型案例 2 个以上，在应用中对系统各项指标进行综合验证。在示范应用基础上，逐步在国内其他轨道交通上进行推广应用。

（三）电力电网行业控制系统

24. SoC 芯片

（1）环节描述及任务。研究 SoC 芯片集成技术，通过深入研究总线架构、高速外围接口、多电源域时钟网络等技术，使系统效能得以提升；研究自动化仿真验证平台技术，实现验证平台自动化的激励产生机制和自动化的结果对比机制，从而解决采用传统仿真验证机制导致的验证周期长、验证不充分的问题；研究基于 FPGA 的软硬件协同验证技术，对高速接口和 SoC 架构等功能进行测试和评估，并通过外部 PC 平台实现对内核的驱动和测试功能评估，从而对 SoC 芯片进行软硬件协同验证。在上述基础上研发低端电力控制 SOC 芯片和高性能电力控制 SOC 芯片。

（2）具体目标。具备多电源域时钟网络技术；具备高速外围接口；具备 FPGA 软硬件协同验证技术；研制系列化高、低端 SOC 芯片。

25. 高性能实时总线芯片

（1）环节描述及任务。研究控制系统高性能实时总线芯片，以及配套编程环境；研制基于高性能实时总线芯片开发的通信协议栈和总线通信板卡；研制基于高性能实时总线芯片传统总线的协议兼容网关。

（2）具体目标。最大传输距离不低于 500 米；最大传输速率：100Mbit/s；最小循环周期不大于 8 微秒；单网段节点数不低于 256 个；单网段节点网络延时不高于 500 微秒；时间同步精度不高于 100ns；支持自动检错和纠错；支持非对称加密；支持总线和环形总线；兼容 ETHERNET/IP、PROFINET、MODBUS TCP/IP 等工业以太网协议；兼容 HART、PROFIBUS、MODBUS、CAN 等工业总线

协议。

26. 实时操作系统

（1）环节描述及任务。研究能够高效支撑工业高实时应用和非实时应用的工业级操作系统，具有丰富的生态兼容支持能力和可靠的安全机制。

（2）具体目标。操作系统具有调试能力和故障诊断能力、支持底层驱动开发、集成丰富的函数库、自带 TCP/IP 等通讯协议栈，具备二次开发能力，二次开发语言支持 C/C++等通用编程语言。提供虚拟化环境下的实时保障，提供实时虚拟机对 CPU 核、外围 IO 设备的独占机制，实时虚拟机中断响应时间达到 us 级，实时虚拟机切换时间小于 5us。支持主流的 X86、ARM、龙芯等 CPU 架构。支持主流桌面系统、实时系统同时运行，非实时系统和各实时系统独立运行、互不影响。支持不少于 20 个虚拟机。提供开发工具，支持对虚拟机的全生命周期管理。提供对设备整体状态及虚拟机实例状态的多维度实时状态监控。支持实时系统与非实时系统间的高速数据交换。支持外设虚拟化及直接透传。实时功能模块化，支持灵活裁剪。

27. 高性能实时总线芯片

（1）环节描述及任务。研究控制系统高性能实时总线芯片，以及配套编程环境；研制基于高性能实时总线芯片开发的通信协议栈和总线通信板卡；研制基于高性能实时总线芯片传统总线的协议兼容网关。

（2）具体目标。最大传输距离不低于 500 米；最大传输速率：100Mbit/s；最小循环周期不大于 8 微秒；单网段节点数不低于 256

个；单网段节点网络延时不高于 500 微秒；时间同步精度不高于 100ns；支持自动检错和纠错；支持非对称加密；支持总线和环形总线；兼容 ETHERNET/IP、PROFINET、MODBUS TCP/IP 等工业以太网协议；兼容 HART、PROFIBUS、MODBUS、CAN 等工业总线协议。

28. 工业边缘计算网关及服务器

（1）环节描述及任务。研究适应于工业现场复杂恶劣环境，满足国内主流控制器、工业机器人、智能传感器等工业设备的接入和数据解析的需求，支持边缘端数据运算及通过互联网推送数据到云平台功能的网关。具备边缘计算、过程控制、运动控制、机器视觉、现场数据采集、工业协议能力的边缘计算装置。

（2）具体目标。研发设计安全的工业边缘计算服务器系统与软件，可持续迭代演进；取得与工业边缘计算服务器相关的实用新型、发明、外观等专利，并实现与之配套的运营环境及编程环境。实现多虚拟运行环境的隔离，实现高实时应用和非实时应用的隔离互不干扰；支持同时上线运行的异构执行体不少于 3 个，实现对不同行业工业设备不少于 30 种不同设备接入和协议解析功能；3 个千兆以太网、2 个串口、1 个 USB 接口、支持无线功能，支持 2G/3G/4G 等移动网络；支持本地数据缓存、断线续传功能；支持透传或 VPN 模式远程调试与下载自动化控制程序；具备远程配置、远程升级、网关远程监控等。

29. 网络安全监管及态势感知系统

（1）环节描述及任务。具备工业控制系统的监测、预警、审计和接入防护等技术，实现对外部攻击及内部非法操作的预警防御和

应急响应，有效地实现防外及安内，防止因网络安全事件造成重大安全生产事故，保障信息系统安全。支持多源数据融合分析，感知重点区域、重点企业安全风险、潜在网络攻击。

（2）具体目标。支持自动识别网络内的资产和工控设备；设备在线运行状态监测集中展现工控系统信息安全态势，建成工业控制系统多源数据融合分析系统 1 套，具备工控协议的检测控制不少于 50 种，其中具备提供指令级工控协议控制不少于 5 种；研制工业控制安全防护系统 1 套，具备边界防护、漏洞扫描、终端防护、安全通信、异常监测、区域隔离等功能；研制安全可控的工控系统核心部件 1 套，具备工控协议识别与内容检测、数据完整性保护等功能。

30. 控制系统软件与信息安全试验验证环境

（1）环节描述及任务。建设电力电网行业工业控制系统安全检测验证环境，打造仿真验证、攻防演练、安全培训、系统评估等基础系统，为电力电网行业工业控制系统综合防护能力提供指导工作，为技术研究、人员培训、漏洞检测、密码检验等提供基础平台。

（2）具体目标。建设工业控制系统安全检测验证实验平台，具备工控安全检测、技术研究、人才培训、成果验证、风险分析的能力。具备相关服务项目经验，针对电力电网行业开展风险评估、漏洞检测、技术培训等服务。

31. 控制系统可靠性试验验证环境

（1）环节描述及任务。具备可靠性、失效分析、电磁兼容功能性能等内容的试验验证环境。

（2）具体目标。依据芯片产品的可靠性目标、参考相关国际标准化组织或者行业协会（如 JEDEC，AEC-Q 等）制定的相关标准或

规范，确定所采用的测试项目及条件。具备样品制备、系统级分析、封装级分析、芯片级失效分析等流程及能力。具备辐射抗扰度、传导抗扰度、电快速瞬态（EFT）脉冲群抗扰度、芯片上电状态下的静电放电（ESD）抗扰度等测试环境及能力。

32. 电力电网行业示范应用

（1）环节描述及任务。在电力电网行业选择典型企业典型场景开展示范应用。培育轨道交通、高铁列控的细分行业和领域的安全控制系统集成商或行业大用户,选择示范行业/领域，形成样板应用系统，并逐步推广和拓展。

（2）具体目标。在电力电网行业控制系统、电力控制芯片及操作系统的项目应用推广，形成电力领域良好合作生态，形成上下游企业产品与服务，积极参与电力建设规划，推进标准化应用。完成 2 型电力电网用户的应用推广。

三、咨询电话

中国电子信息产业发展研究院　周 峰　010-88559882

郝 鑫　010-88559777

附：控制系统“一条龙”应用计划申报书

附

控制系统“一条龙”应用计划申报书

企业名称：_____

项目名称：_____

责任人（法人代表）：_____

项目技术负责人：_____

实施年限：20_____年_____月至20_____年_____月

填报日期：20_____年_____月_____日

中华人民共和国工业和信息化部制

二〇一　　年　月

<table>
<tr><td>单位名称</td><td colspan="2"></td><td>注册地</td><td></td><td>机构代码</td><td></td></tr>
<tr><td>项目名称</td><td colspan="2"></td><td>项目实施期</td><td colspan="3">年　月至　年　月</td></tr>
<tr><td>所属产业链</td><td colspan="6">☐ 石化行业控制系统　☐ 轨道交通控制系统　☐ 电力电网控制系统</td></tr>
<tr><td>所属产业链关键环节</td><td colspan="6">☐ 控制系统安全设计　☐ 安全控制系统开发
☐ 控制系统安全防护技术　☐ 试验验证环境构建
☐ 安全可靠认证体系　☐ 行业用户示范应用</td></tr>
<tr><td>安全控制系统</td><td colspan="6">☐ SoC 芯片　☐ 工业以太网交换芯片
☐ 高性能实时总线芯片　☐ 实时操作系统
☐ 工业边缘计算服务器　☐ 通信协议
☐ 数据采集与监视控制系统（SCADA）　☐ 分散型控制系统（DCS）
☐ 安全仪表系统硬件平台　☐ 安全仪表系统编程运行软件
☐ 实时/历史数据库　☐ 人机界面 HMI</td></tr>
<tr><td>控制系统安全防护技术</td><td colspan="6">☐ 安全监管与预警平台　☐ 基层工控环境安全管理系统
☐ 上层控制系统网络安全防护系统　☐ 信息安全数据融合分析系统
☐ 工控数据库安全审计系统</td></tr>
<tr><td>试验验证环境</td><td colspan="6">☐ 软件试验验证环境　☐ 硬件试验验证环境</td></tr>
<tr><td>实施期</td><td colspan="6">年　月至　年　月</td></tr>
<tr><td>主要负责人</td><td colspan="2"></td><td colspan="2">联系电话（手机）</td><td colspan="2"></td></tr>
<tr><td>电子邮箱</td><td colspan="2"></td><td colspan="2">传真</td><td colspan="2"></td></tr>
<tr><td colspan="7">参与单位满足所属“一条龙”环节供需概述（包括:
1.企业基本情况;
2.重点产品、工艺符合性质，与“一条龙”其他环节在产品、工艺上的直接关联性;
3.创新能力、产品技术和工艺水平领先情况;
4.对产业链上游的需求，以及对下游可提供的产品或服务；近年来企业产品和技术实际使用和应用情况;
5.近三年经营业绩，遵纪守法情况，管理制度建设情况，包括不限于以下内容
2015、2016、2017 年企业情况
<table><tr><td rowspan="2">技术</td><td>研发投入占营收比例</td></tr><tr><td>当年申请专利数，截至年底累计授权专利数</td></tr><tr><td>市场</td><td>细分领域市场份额、市场排名</td></tr><tr><td rowspan="4">财务</td><td>总资产</td></tr><tr><td>资产负债率</td></tr><tr><td>年度营业收入</td></tr><tr><td>年度净利润</td></tr></table>6.企业参与“一条龙”应用计划的运行工作机制及措施;
7.推荐的龙头企业、参与单位和示范工程;
8.存在的问题和建议等。</td></tr>
<tr><td colspan="7">项目基本情况（总投资、主要建设内容、预期效果等），并填列下表:
项目目前情况
<table><tr><td>项目成熟度</td><td>是否已经完成可研</td></tr><tr><td>项目总投资</td><td>总投资额</td></tr><tr><td>项目资本金</td><td>项目资本金额度</td></tr></table></td></tr>
<tr><td>参与单位自评意见</td><td colspan="6">本单位承诺申报内容真实有效。
法定代表人（签字）：（盖章）
年　月　日</td></tr>
</table>