窄带无线SCADA系统安全解决方案

卫士通信息产业股份有限公司

2018年11月

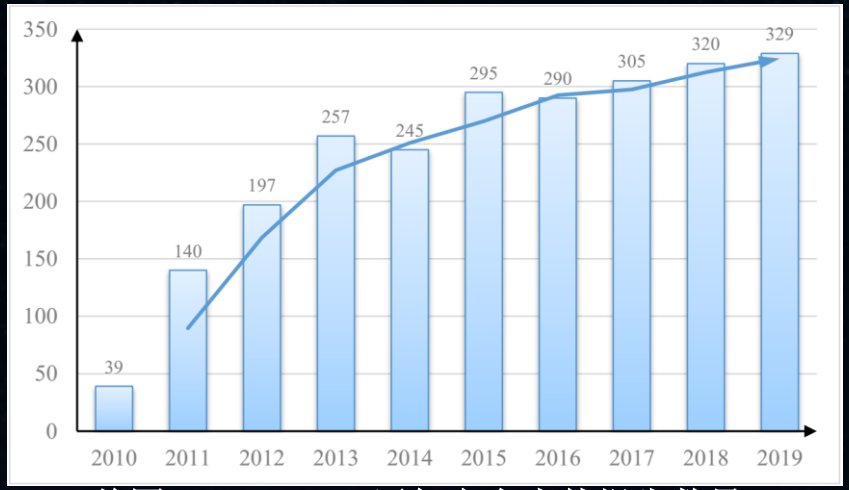
王亮 13808189086

目 录

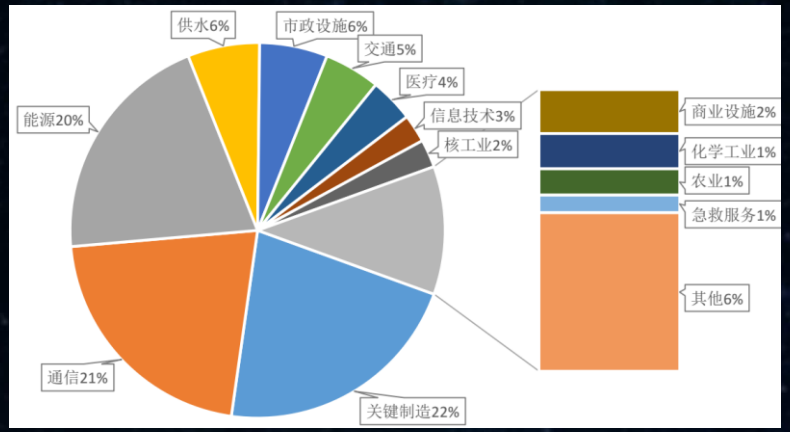
CONTENTS

工控安全形势严峻

近年来，工业控制领域的信息安全事件的数量呈现上升趋势，涉及关键制造、通信、能源、供水和市政设施等重要领域的关键信息基础设施，工控信息安全成为影响国家关键基础设施安全和工控行业健康发展的重要因素。



美国 ICS-CERT 历年安全事件报告数量



工控安全事件发生所在行业分布情况

数据来源：美国 ICS-CERT，国家工业信息安全产业发展联盟整理

国家对工控安全高度重视

2015 年5 月8 日，《中国制造2025》提出，要加强智能制造工业控制系统网络安全保障能力建设，健全综合保障体系。

2016 年10 月17 日，工业和信息化部印发了《工业控制系统信息安全防护指南》，对全国工业企业工控安全防护和保障工作进行指导和管理。

2016 年12 月27 日，国家互联网信息办公室发布了《国家网络空间安全战略》。该战略提出要坚决维护国家安全，保护关键信息基础设施。

2017年12月29日，《工业控制系统信息安全行动计划（2018-2020年）》，指出“工业控制系统信息安全（以下简称工控安全）是实施制造强国和网络强国战略的重要保障。”，同时强调“坚持落实企业主体责任。确立企业工控安全主体责任地位，强化责任意识，把工控安全作为工业生产安全的重要组成部分，将安全要求纳入企业生产、经营、管理各环节。”

采购和使用要求

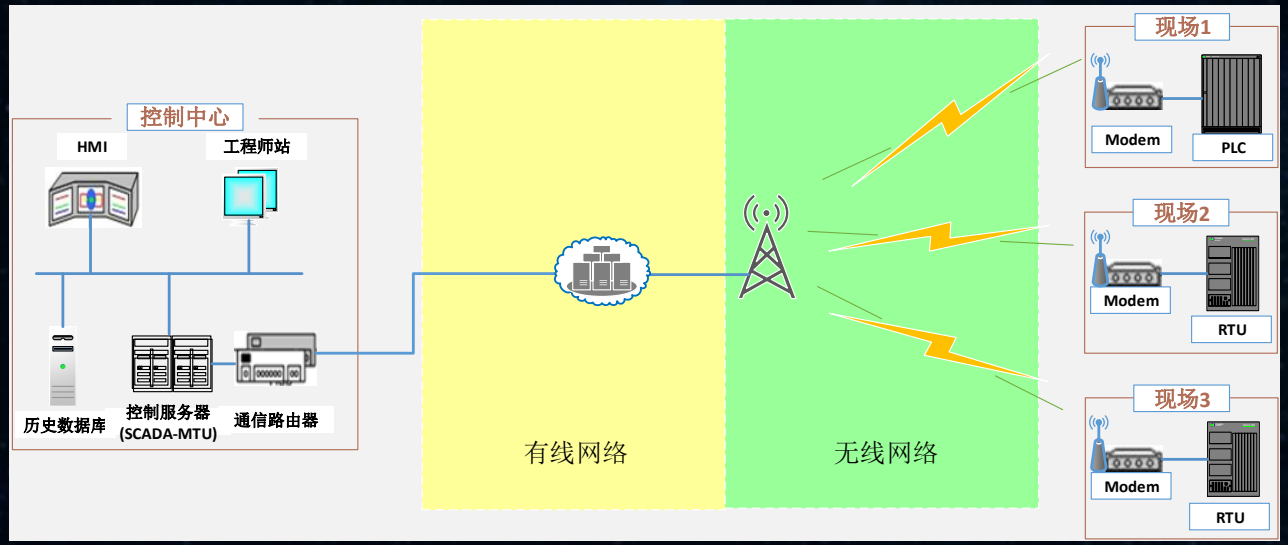
等保2.0《信息安全技术 信息系统安全等级保护基本要求 第5部分 工业控制安全扩展要求》中明确要求：

“工控控制系统重要设备及专用信息安全产品应通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测后方可采购使用。”

目 录

CONTENTS

典型SCADA系统架构及信息安全风险



控制中心的安全风险

- 控制中心的敏感信息泄露
- 控制中心的控制指令被篡改
- 控制中心的控制逻辑被篡改
- 非法使用、配置控制软件

通信网络的安全风险

- 传输的敏感信息泄露
- 控制指令或采集数据被篡改

设备的安全风险

- 设备的敏感信息泄露
- 设备软件和数据被篡改
- 设备被非法配置、调试

信息安全对功能安全的影响

信息安全

功能安全

指令和采集数据被篡改、伪造

控制逻辑错误；设备被损坏；基础设施遭受破坏

敏感数据泄露

国家、企业利益受到损害

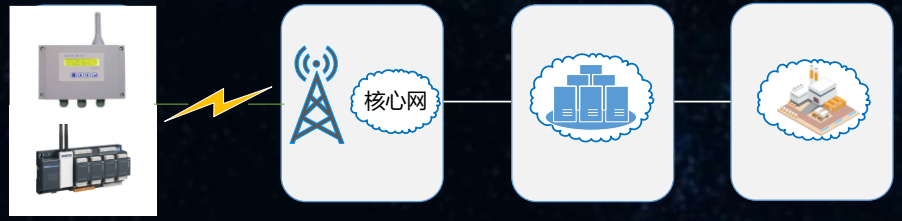
外接安全装置的问题

对于现场设备端的安全，通常采用外接硬件安全装置的方式解决。但是这种方式在物理上存在被旁路的风险，同时在可靠性上也存在一定隐患。另外，在某些工控现场，没有条件安装外置式安全装置，需要一种嵌入设备内部的安全方案。

RTU　　安全装置　　通信网络

无线低功耗广域网技术带来的新问题

NB-IoT技术在工业领域的应用日益广泛，其低功耗运行机制对信息安全技术的实现带来了新的问题。



- 需要基于UDP协议的轻量级身份认证和安全传输协议
- 安全机制需要适应“服务器无法主动连接终端”的应用场景
- 安全机制和安全产品需要满足低功耗要求

目 录

CONTENTS

总体思想

安全

控制指令和采集数据的真实、完整；
保护敏感数据的传输安全和存储安全。

可用

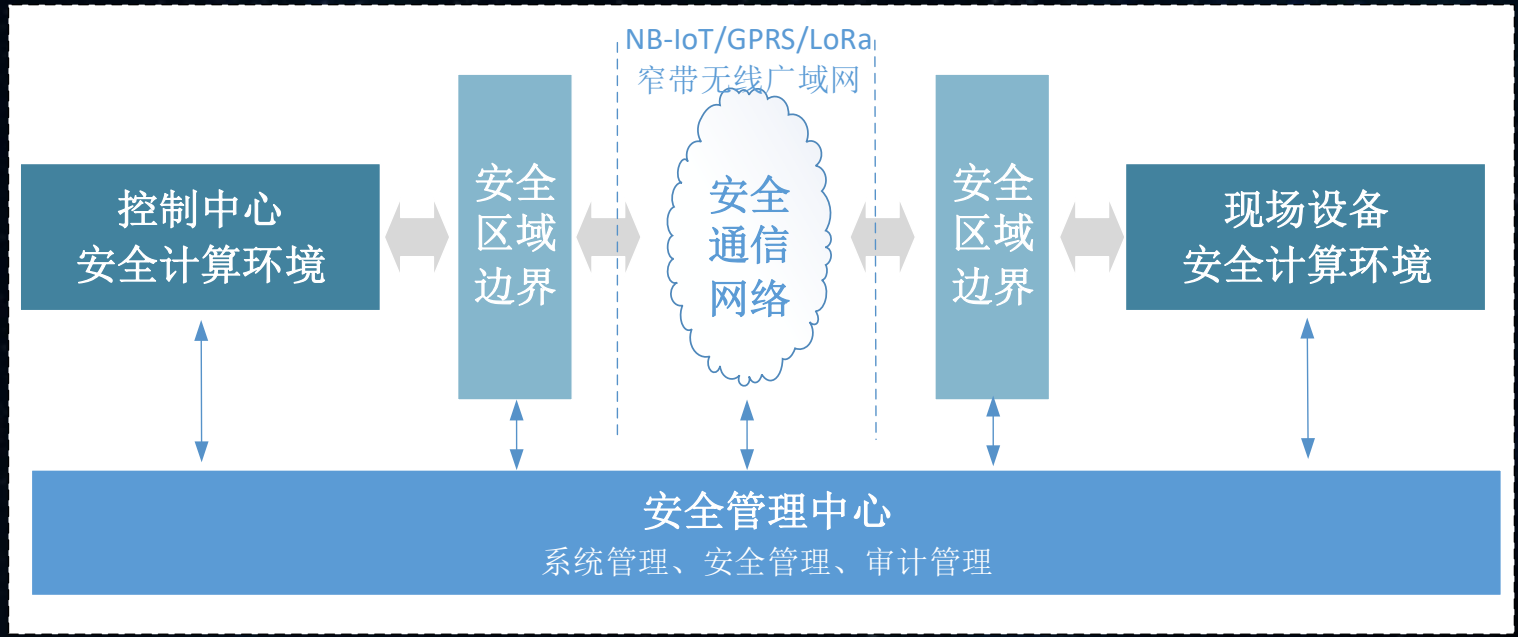
减少引入安全功能对应用系统的影响；
采取轻量化、低功耗的安全机制。

易用

降低应用厂商集成和实现安全功能的难度。

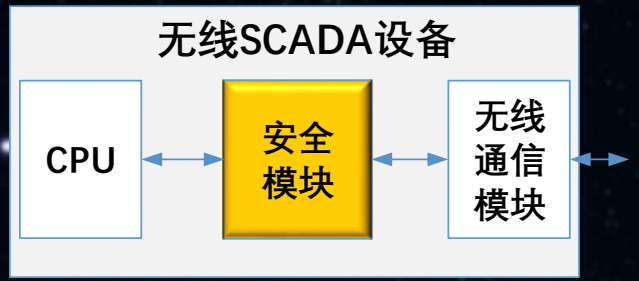
安全防护总体框架

按照等保2.0的思想，构建在安全管理中心支持下的计算环境、区域边界、通信网络三重防御体系。



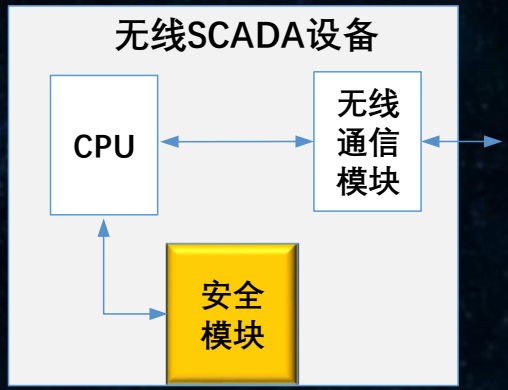
主要安全措施

采用将硬件安全模块集成到SCADA设备内部的方式，通过UART串口与CPU或无线通信模块连接，为设备提供安全防护能力，形成一体化的安全SCADA设备。



门卫式

安全性更高



调用式

应用灵活，成本更低，功耗更低

可支撑的安全功能

■ 身份认证及访问控制

确保网络通信双方的身份可信。确保本地使用、调试人身份可信。在身份认证的基础上，按照权限、角色实现对资源访问的控制。

■ 安全传输协议

确保无线传输的指令和采集数据的真实可信、无法篡改、信息保密。

■ 设备数据安全存储

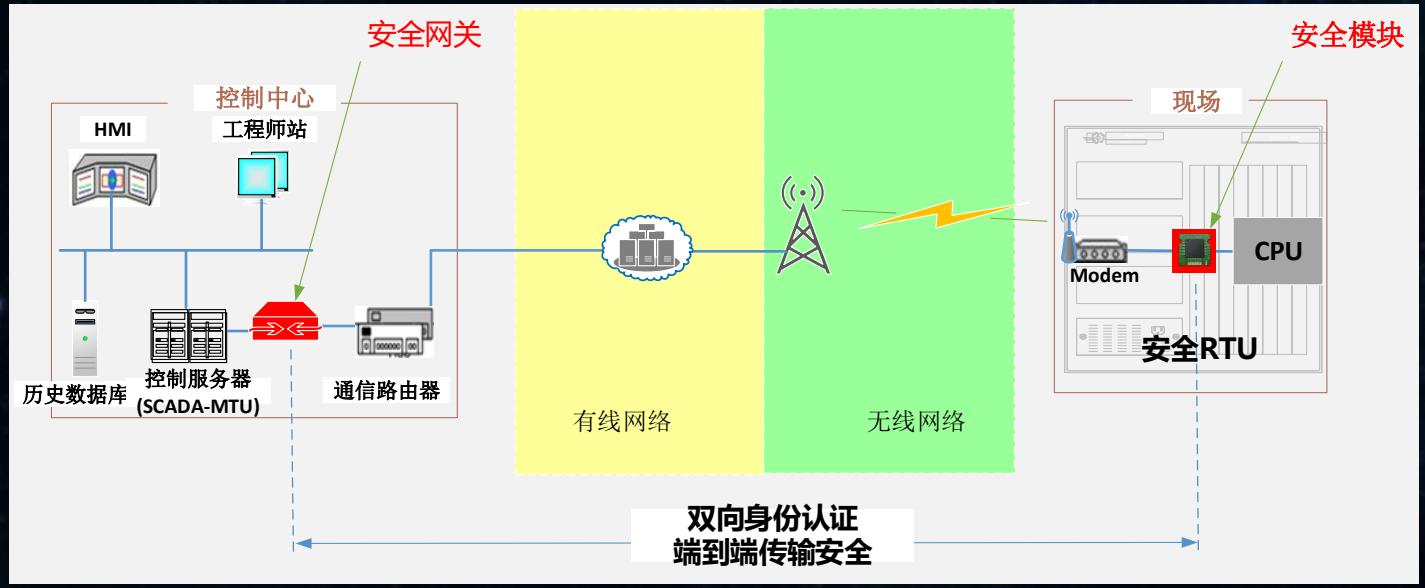
保障本地敏感数据的存储安全，信息保密。

■ 设备代码签名验证

可验证设备代码是否完整且未被篡改。

端到端的通信安全方案

建立从SCADA设备到控制中心服务器之间的端到端的通信安全防护机制，为指令、采集数据、在线升级文件、配置参数等信息的安全传输提供保障。



整体安全防护框架

SCADA 控制中心安全防护		窄带无线广域网 边界和通信网络防护	SCADA 设备安全防护
身份认证	访问控制	网络侧身份认证	身份认证
终端防护	协议过滤	网络侧访问控制	访问控制
区域隔离	数据流分析	传输加密	存储加密
漏洞扫描	态势感知		代码验证
安全管理中心			

目 录
CONTENTS

方案特色

- 适合低功耗窄带无线应用场景；
- 硬件安全模块与SCADA设备集成，提升安全性、可靠性；
- 工控厂商“零信安知识”集成，接口易用，便于快速实现；
- 设备端支持两种硬件架构，适应不同的应用及安全需求。

公司实力

卫士通信息产业股份有限公司（卫士通，002268）成立于1998年，国内知名密码产品、网络安全产品、互联网安全运营、行业安全解决方案综合提供商，首批商密产品研发、生产、销售资质单位，是国内第一家上市的信息安全企业，是十二大军工集团之一——中国电子科技集团公司旗下唯一的网络信息安全上市平台。

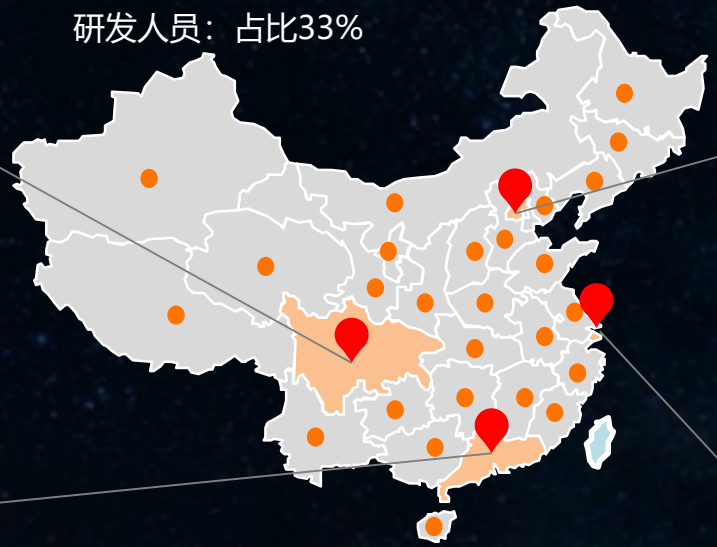
卫士通积累了大量密码及信息安全核心技术，能够满足用户从硬件到软件、从底层到应用层、从端到云的一体化安全需求，帮助用户有效解决基础设施防护、智慧城市、移动办公、安全应用、工业控制、商业秘密保护、云计算、信任服务等各类场景中面临的信息安全问题。

公司实力

全国化的服务布局

4大区域营销服务中心，29个办事处，遍布全国范围的本地化营销服务体系。

在职员工：2000多人
本科以上：占比83%
技术人员：占比67%
研发人员：占比33%



成 都
管理总部
产品研发中心
产品生产基地

北 京
营销总部
解决方案创新中心
前沿技术研发中心

广 州
行业华南营销服务中心

上 海
行业华东营销服务中心

公司实力

政府部委

全国人民代表大会 The National People's Congress of the People's Republic of China

中华人民共和国最高人民法院 The Supreme People's Court of the People's Republic of China

中华人民共和国最高人民检察院 The Supreme People's Procuratorate of the People's Republic of China

中共中央纪律检查委员会

中华人民共和国外交部 Ministry of Foreign Affairs of the People's Republic of China

中华人民共和国国家发展和改革委员会 National Development and Reform Commission

中华人民共和国财政部 Ministry of Finance of the People's Republic of China

中国科学院 CHINESE ACADEMY OF SCIENCES

国家海洋局 State Oceanic Administration People's Republic of China

中国证券监督管理委员会 CHINA SECURITIES REGULATORY COMMISSION

金融

中国人民银行 THE PEOPLE'S BANK OF CHINA

中国银联 China UnionPay

国家开发银行 CHINA DEVELOPMENT BANK

中国进出口银行 THE EXPORT-IMPORT BANK OF CHINA

中国工商银行 INDUSTRIAL AND COMMERCIAL BANK OF CHINA

中国农业银行 AGRICULTURAL BANK OF CHINA

中国银行 BANK OF CHINA

中国建设银行 China Construction Bank

交通银行 BANK OF COMMUNICATIONS

中国光大银行 CHINA EVERBRIGHT BANK

中信银行 CHINA CITIC BANK

招商银行 CHINA MERCHANTS BANK

华夏银行 HUAXIA BANK

能源

国家电网公司 STATE GRID CORPORATION OF CHINA

中国南方电网 CHINA SOUTHERN POWER GRID

中国石油

中国石化 Sinopec

中国国电集团公司 CHINA GUODIAN CORPORATION

中国华能 CHINA HUANENG

中国电力投资集团公司 CHINA POWER INVESTMENT CORPORATION

中国华电集团公司 CHINAHUADIANCORPORATION

神华集团有限责任公司 SHENHUAGROUP CORPORATION LIMITED

国家电网 STATE GRID 中国电力科学研究院 CHINA ELECTRIC POWER RESEARCH INSTITUTE

中国长江电力股份有限公司 China Yangtze Power Co.,Ltd.

军工

中国核工业集团公司 China National Nuclear Corporation

中国核工业建设集团公司 CHINA NUCLEAR ENGINEERING GROUP CO

中国航天科技集团公司 China Aerospace Science and Technology Corporation

中国航天科工集团公司 CHINA AEROSPACE SCIENCE & INDUSTRY CORP.

中国航空工业集团公司 AVIATION INDUSTRY CORPORATION OF CHINA

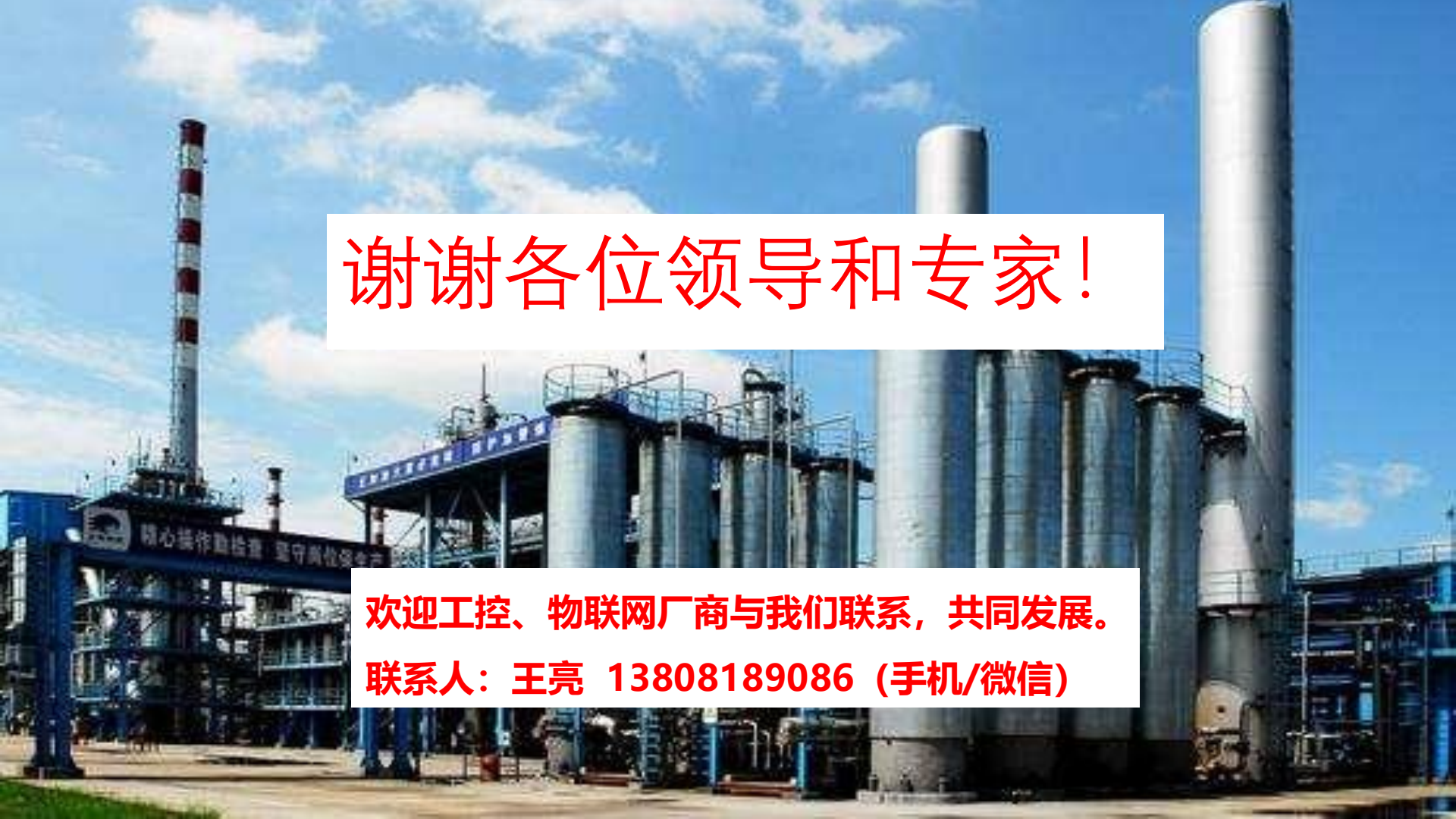
中国船舶工业集团公司 CHINA STATE SHIPBUILDING CORPORATION

中国船舶重工集团公司 CHINA SHIPBUILDING INDUSTRY CORPORATION

中国兵器工业集团公司 CHINA NORTH INDUSTRIES GROUP CORPORATION

中国兵器装备集团公司 China South Industries Group Corporation

CETC 中国电子科技集团公司 China Electronics Technology Group Corporation


谢谢各位领导和专家！
欢迎工控、物联网厂商与我们联系，共同发展。
联系人：王亮 13808189086（手机/微信）