**工业控制系统简述**

一、定义

**系统**：实现一系列功能或目标的相互关联的一组元素。其内涵主要包括**元素**及**关系**，外延包括系统的功能或目标、与系统相互作用的**环境**与**人**等等，是一个的抽象人造概念。

**工业控制系统：**在工业中通过精确操纵一系列变量从而达到预定状态的系统。

**系统的功能或目标：**……

**环境：**系统之外的元素集合。环境元素通常会与系统产生物质、能量、信息等方面的交互。

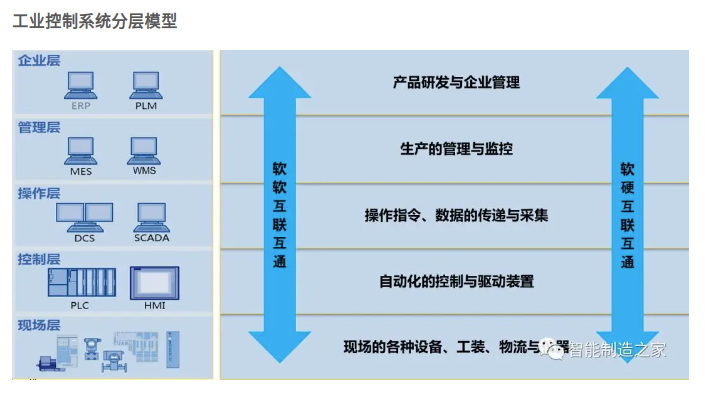
**人：**……

**其他：**……

**典型的工业控制系统要素：**测量元件（传感器）、执行元件（伺服器）、控制元件（控制器）、工业通信网络、生产资源及计划管理软件。

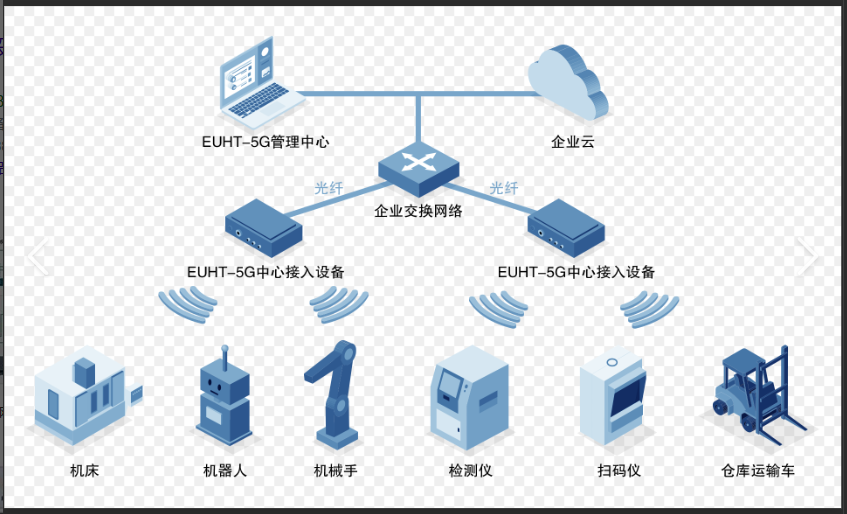


工业控制系统层次图（ISA-95，美国）



国际电工委

ISO/IEC 62264的层次结构模型



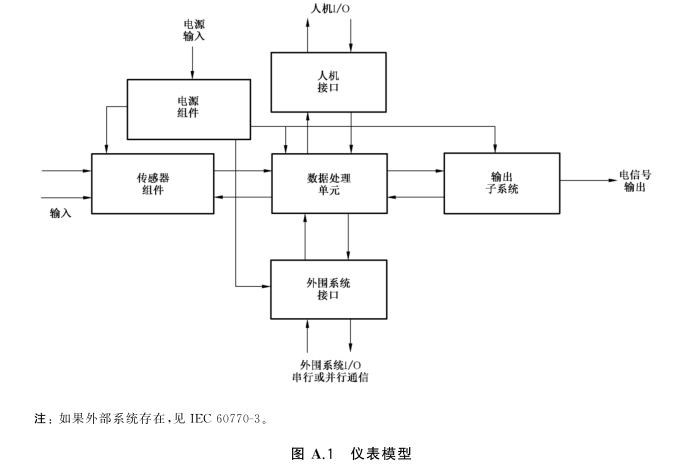
云端工业控制系统

工业控制系统体系首先是西方国家建立起来的，我国引进。由于历史、资源、市场、甚至政治等因素，造就了工业控制体系十分复杂。目前还未找到综述性文件或总论著作。可检索到的较为顶层技术文件有：美国标准协会下属的Instrumentation, System and Automation Society （仪器仪表，系统与自动化分舵）首先制订ANSI/ISA-95.00.01-2010，企业-控制系统集成；国际标准化组织借鉴前者而制订ISO/IEC 62264-1企业-控制系统集成；我国借鉴前者而制订GB/T 20720.1-2013企业控制系统集成。这三份规范文件，对工业控制系统作出了技术描述并将SCADA系统、DCS系统和PLC系统等模型的共性进行分类，共分为5个层级，依次为企业资源层、生产管理层、过程监控层、现场控制层和现场设备层，各层分别行使其抽象功能。其中第5企业资源层、第4生产管理层主要用于规范ERP、MES等软件系统的信息流。第3、2、1层个人认为是狭义的工业控制系统的模型。

五层模型是经典结构，现在市场上可供采购的工控软硬件产品大部分参考这一模型。

随着互联网技术、IoT物联网技术的发展，特别是4G/4G网络的发展，五层模型未见相应修订。我国于2022年拽出了GB/T 42021-2022，工业互联网 总体网络架构。

二、传感器



1、定义（GB/T 7665-2005，传感器术语；GB/T 7666-2005，传感器命名与代号）

传感器（sensor）能感受被测量并按照一定的规律转换成可用输出信号的器件（device）或装置（apparatus），通常由敏感元件（sensing component）和转换元件（transacting component）组成。

敏感元件指直接感受或响应被测量的部分。

转换元件指将敏感元件感受或响应的被测量转换为适宜传输或测量的电信号的部分。

输出为标准信号的传感器称为变送器（transmitter）。

2、分类（GB/T 36378.1/2/3-2018，传感器分类与代码）

2.1按照被测量将传感器分为：物理量、化学量、生物量三类。

2.1.1被测物理量可分为：力学量、热学量、光学量、磁学量、电学量、声学量、微波、射线、其他。

2.1.2被测化学量可分为：……

2.1.3被测生物量可分为：……

2.2按照转换原理将传感器分为：电阻式、电容式、电感式、压电式、磁电式、光电式、谐振式、声波式、辐射式、其他。

3、变送器

（GB/T 2900.56-2008，电工术语 控制技术）

（GB/T 2900.77-2008，电工术语 电子测量和仪器仪表）

**（GB/T 17212，工业过程测量和控制的术语和定义）**

~~（GB/T 18271，过程测量和控制装置）~~

~~（GB/T 18272，工业过程测量和控制 系统评估中系统特征的评定）~~

对于工业过程测量和控制系统常使用具有标准输出信号的传感器即变送器。变送器的输出子系统能够提供**模拟信号**（mA，V，频率）以及**数字信号**（开关信号，脉冲计数串，复杂通信协议信号）。

3.1 标准输出信号的分类

3.1.1模拟信号**（GB/T 3369.1/2-2008，过程控制系统用模拟信号）**

直流电流

直流电压

频率（未见相关规范性文件）

3.1.2 数字信号

开关信号

脉冲计数串，如编码器

复杂通信协议信号（规范性文件相当多并与工业网络相关，典型如GB/T 25105-2014 工业通信网络 现场通信总线规范系列）

3.2 智能变送器

智能变送器是一种在运行中采用数字处理和通信技术来执行其功能、保护和传送数据与信息的装置。**（GB/T 17614.1/2/3-2015，工业过程控制系统用变送器）**

4、小结

我公司开展工业物联网项目，涉及过程测量节点的传感器大概率会采用变送器或具有通信协议的智能传感器。。

4.1选择变送器的原因：

系统相对简单。

成品变送器产品丰富，易于采购，供货周期、质量有保障，售前售后支持好。

综合成本低。

易于安装实施。

4.2 选择智能变送器的原因：

特殊要求。

与现有软硬件环境兼容较好

三、伺服器

目前暂未过多涉足，待后续补充。比如步进电机、电机调速器、变频器、电动/气动阀门……

相关规范性文件后补。

四、控制器

4.1 抽象概念，主要指五层模型中的第二、三层软硬件设备，比如PLC（可编程逻辑控制器）、DCS（分布式控制系统）、SCADA（系统控制与数据采集）、SIS（安全仪表系统，侧重于安全过程控制的控制器）。据网络老司机表述，前三者功能相似（南门口、大师傅、蒋家肠旺面的区别？），由厂商、应用行业、市场不同而产生不同称谓。这类产品概念多由西方原创，我国引进。**控制器是工业控制系统的核心设备。**

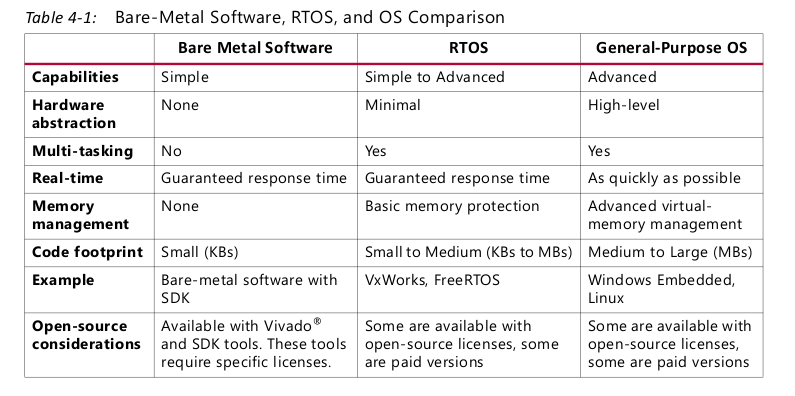
控制器的实质就是计算机系统，工业控制器是满足工业条件的工业计算机系统。

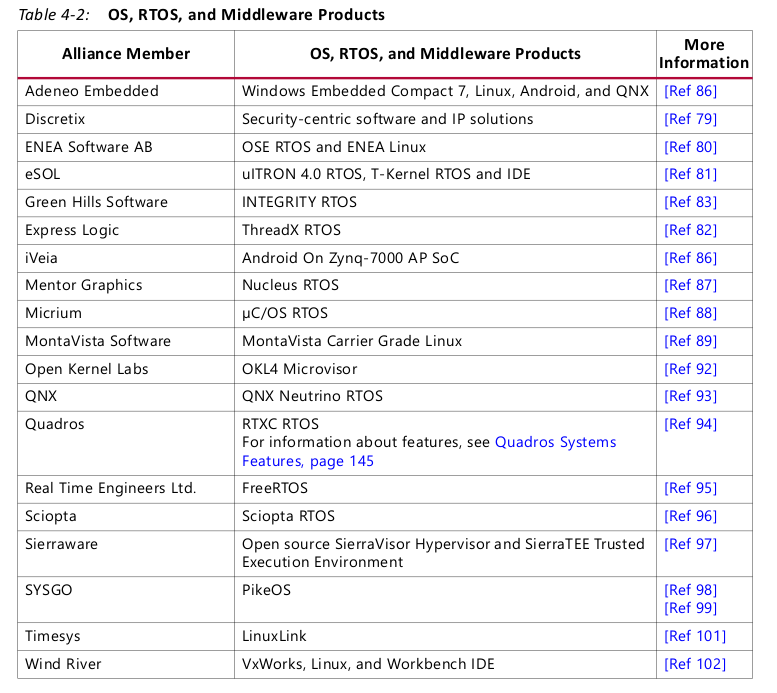
按计算机指令架构分：x86、arm、RISC-V等。

按处理能力分（比如每秒执行指令的数量）：工业控制工作站、工控机、嵌入式计算机等。

按操作系统分：无操作系统（bare metal，白板），如西门子 TIA S系列PLC。

有操作系统，如win server、unix、linux、android各式各样的嵌入式操作系统。

无超作系统、嵌入式操作系统、通用操作系统对比



千奇百怪的嵌入式操作系统

4.2 控制器关注点

工业控制器选型的关键是操作系统选择。操作系统也是后续开发工作关键分界面。

4.2.1 在此分界面以上是系统API开发设计，运用软件环境构建，运用软件开发等工作、

数据存储与展示、业务逻辑；

4.2.2 在此分界面以下是操作系统建立，硬件驱动及环境构建等嵌入式软件开发工作，上

层调用接口；

4.2.3 再下一层是硬件设计工作。

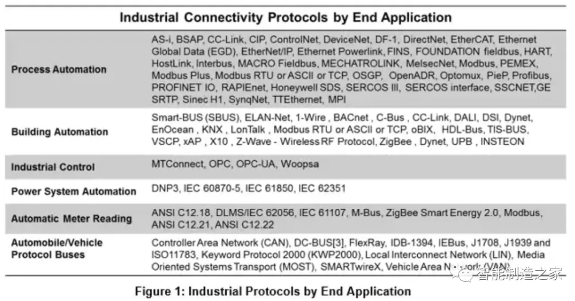
4.2.4 采购成品系统，然后集成。

4.3 相关规范性文件后补。

五、工业通信网络

5.1概述。

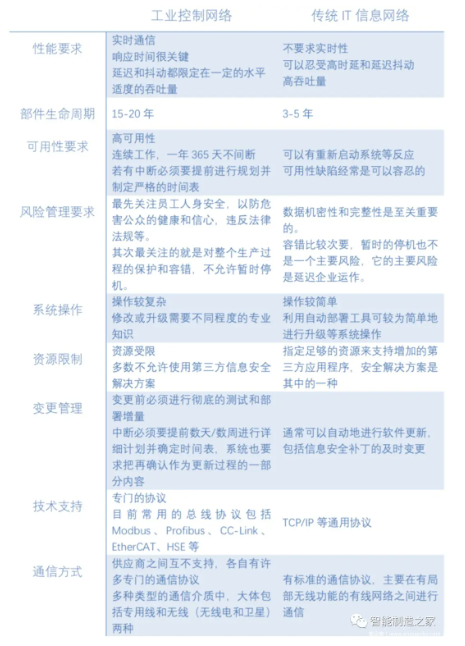
工业产品种类丰富，生产过程花样繁多。生产设备必须连成网络，方能为自动控制提供信息通路。人类工业化的历史悠久，工业通信网络会连接很多不同类的设备，而且通常会工作在恶劣的环境下，因此造就了众多的总线，接口，协议，标准。比如，目前世界上依然存在着40余种现场总线族。由于行业特性的不同，也存在着不同的总线协议运用惯例。各种各样的现场总线大都用于过程自动化、加工制造、交通运输、医药、国防、航天、农业和楼宇等领域，大概不到十种的总线占有80%左右的市场。（来源于网络）



经典工业通信网络的特点是：局域性、高可靠性、功能特征离散性、成本离散性、历史性、专有性、行业性。根据金灿荣（中国人民大学国际关系学院教授）、尤瓦尔·赫拉利（《人类简史》作者）等人的观点，18世纪60年代，人类工业革命首先在西方国家发生，随后人类进入工业文明时代，人类的工业化进程也是西方工业国对世界其他农业国侵略、殖民降维打击的过程。西方工业国除了虐夺资源外，也传播了先进的工业思想，因此经典的工业知识体系完全由西方国家主导。工业革命没有发生在中国，结果就被侵略了。中国在后续的工业化过程中只能跟随西方国家的脚步，市场上鲜有中国原创的工业产品。

但是，当前互联网、IoT、4G/5G等信息技术在中国普遍成熟运用，其成效相较于西方国家是压倒性的（表现为GDP的贡献值）。因此中国在工业互联方面首先制订了GB/T 42021-2022，工业互联网 总体网络架构。我司开展工业信息化项目的噱头也可源于此。

互联网源于计算机系统，是一个计算机信息系统网络。当其运用于工业领域，被赋予了各种特殊要求。



5.2 工业互联网 总体网络架构

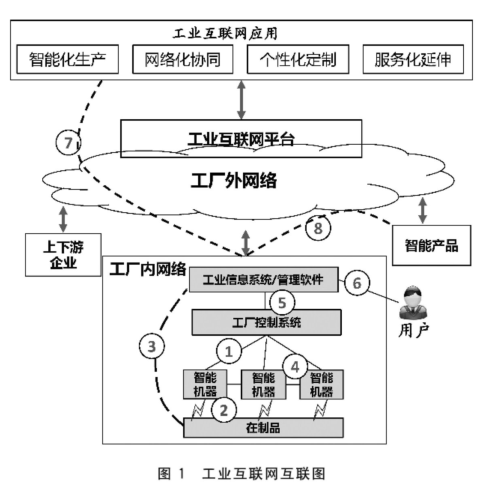
新一代信息技术与工业经济相融合的新型基础设施、运用模式和工业生态，通过对人、机、物、系统的全面连接，构建起覆盖全产业链、全价值链的全新制造和服务体系。

空间上划分为：厂内网络与厂外网络。

业务对象上划分：OT（operation technology network）网络，直接控制工业自动化功能的

网络；

IT（information technology network）网络，信息化网络。



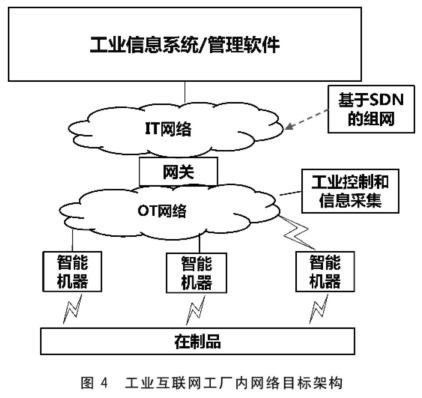
工业制造企业

工业服务企业：围绕设计、制造、供应、服务等环节提供服务的企业。

网络服务企业：电信、网络服务商，互联网企业。

5.3 厂内网络

工厂内部用于生产要素和IT系统之间连接的网络。



由上图可知，工业互联网涉及三类企业主体：GB/T 42021将IEC 62264约束在了厂内。

示例：新普能源电能优化管理系统。

变送器：温度、压强、液位……

伺服器：电机变频调速器

控制器：刘总自主研发，嵌入式win-ce控制器，软件C#语言开发，纯手工打造，性能稳

定可靠。

OT网络：有线电压信号、电流信号、Modbus-RTU现场总线、Modbus-TCP现场总线、

商用以太网

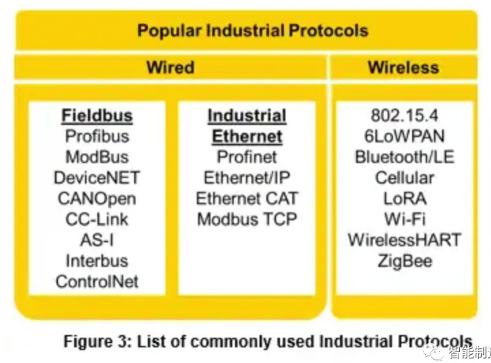
IT网络：商用以太网

OT-IT网关：windows server dell 工作站、工业电脑，实现现场设备状态数据向广域网发送，

软件系统采用B/S结构，.net环境，SQ server。该网关也兼顾人机控制界面，

现场数据库，在恶劣的工作他条件下，该网关经常出问题。

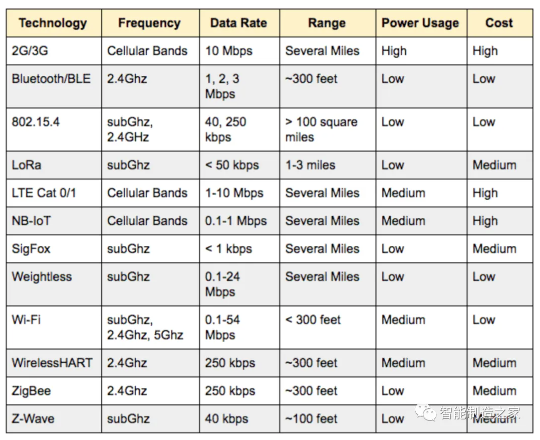
工业网络的严格要求在历史上推动了各种私有协议和应用专属协议的产生。有线和无线网络都有专属的协议集。尽管可用的协议有很多，但大多数有线协议都遵循两个标准：现场总线或者工业以太网。在当代，无线连接降低网络成本的潜力日益凸显，Wi-Fi、蜂窝网络、蓝牙以及 ZigBee 等协议都得到不同程度的应用。



现场总线（field bus）是一系列工业网络协议的总称，主要用于实时分布式控制，常用485网络和CAN网络等。现场总线相比传统I/O通信的最大优势在于它可以大幅缩减工厂的供电线路。简单可靠是现场总线最重要的特征，在工业以太网兴起之前，它成为了工业网络的首选。相关规范性文件IEC 61158，GB/T 25105-2014 工业通信网络 现场通信总线规范系列、GB/T 36417.1/2/3/4-2018 分布式工业控制网络、GB/T 38868-2020 工业控制网络通用技术要求 有线网络等。

经过多年的发展，工业以太网已经成为了主流（市场份额约64%），通过对ISO/OSI七层模型不同程度的修改，不同程度的加强可靠性、实时性，逐步蚕食现场总线的市场份额。

经过多年的发展，工业以太网已经成为了主流，最常见的工业自动化无线技术包括 802.11.x Wi-Fi、蓝牙、蜂窝网络、无需许可证的私有 ISM 频段无线电以及WirelessHART、ISA100.11a、WIA-PA 以及 ZigBee 等基于802.15.4 的协议。



国标GB/T 26790.1/2/3/4-2015 工业无线网络WIA规范

5.4厂外网络

基于现有IT网络，针对工业运用进行加强。

国际标准



国标

GB/T 40211-2021 工业通信网络 网络与系统安全 术语

GB/T 40218-2021 工业通信网络 网络与系统安全 工业自动化和控制系统信息安全技术

也比较多，还没有理清。不多赘述。

六、 传统的生产资源及计划管理软件系统

在IEC 62264界定的范围内可理解为广义的工业控制系统。

6.1 MES（制造执行生存管理系统）

6.2 ERP（企业资源管理系统）

6.3 ……

6.4 相关规范性文件后补。

七、项目可参与性

7.1 经典工业自动化项目

通常工业自动化项目建设过程为：建设单位提出需求，设计单位论证、设计，系统集成及设备供应商制安、业主及相关方验收。我司可参与部分环节工作。

7.2 工业信息化技改项目

对既有工业项目实施信息化技术改造。可分为局部改造，整体改造。

7.3 民用商业项目

对于业务流程简单的民用商业项目，可考虑整体实施。

八、面临的挑战