



中国地质大学（武汉）

计算机网络与工业互联网课程报告

学 院： 自动化学院

课 程： 计算机网络与工业互联网

指导老师： 熊永华

学 号： 20201000128

班 级： 231202

姓 名： 刘瑾瑾

2022 年 10 月 30 日

现代工业控制网络应用调研

一、工业控制网络的基本架构和组网原理

CAN 是 Controller Area Network 的缩写（以下称为 CAN），是 ISO 国际标准化的串行通信协议。在汽车产业中，出于对安全性、舒适性、方便性、低功耗、低成本的要求，各种各样的电子控制系统被开发了出来。由于这些系统之间通信所用的数据类型及对可靠性的要求不尽相同，由多条总线构成的情况很多，线束的数量也随之增加。为适应“减少线束的数量”、“通过多个 LAN，进行大量数据的高速通信”的需要，1986 年德国电气商博世公司开发出面向汽车的 CAN 通信协议。此后，CAN 通过 ISO11898 及 ISO11519 进行了标准化，在欧洲已是汽车网络的标准协议。

CAN 的高性能和可靠性已被认同，并被广泛地应用于工业自动化、船舶、医疗设备、工业设备等方面。现场总线是当今自动化领域技术发展的热点之一，被誉为自动化领域的计算机局域网。它的出现为分布式控制系统实现各节点之间实时、可靠的数据通信提供了强有力的技术支持。

CAN 是一种用于实时应用的串行通讯协议总线，它可以使用双绞线来传输信号，是世界上应用最广泛的现场总线之一。CAN 协议用于汽车中各种不同元件之间的通信，以此取代昂贵而笨重的配电线束。CAN 协议的特性包括完整性的串行数据通讯、提供实时支持、传输速率高达 1Mb/s、同时具有 11 位的寻址以及检错能力。

CAN 总线用户接口简单，编程方便。网络拓扑结构采用总线式结构。这种网络结构简单、成本低，并且采用无源抽头连接，系统可靠性高。通过 CAN 总线连接各个网络节点，形成多主机控制器局域网(CAN)。信息的传输采用 CAN 通信协议，通过 CAN 控制器来完成。各网络节点一般为带有微控制器的智能节点完成现场的数据采集和基于 CAN 协议的数据传输，节点可以使用带有在片 CAN 控制器的微控制器，或选用一般的微控制器加上独立的 CAN 控制器来完成节点功能。传输介质可采用双绞线、同轴电缆或光纤。如果需要进一步提高系统的抗干扰能力，还可以在控制器和传输介质之间加接光电隔离，电源采用 DC-DC 变换器等措施。这样可方便构成实时分布式测控系统。微控制器，或选用一般的微控制器加上独立的 CAN 控制器来完成节点功能。传输介质可采用双绞线、同轴电缆或光纤。如果需要进一步提高系统的抗干扰能力，还可以在控制器和传输介质之间加接光电隔离，电源采用 DC-DC 变换器等措施。这样可方便构成实时分布式测控系统。

CAN 总线使用串行数据传输方式，可以 1Mb/s 的速率在 40m 的双绞线上运行，也可以使用光缆连接，而且在这种总线上总线协议支持多主控制器。CAN 与 I2C 总线的许多细节很类似，但也有一些明显的区别。

当 CAN 总线上的一个节点(站)发送数据时，它以报文形式广播给网络中所有节点。对每个节点来说，无论数据是否是发给自己的，都对其进行接收。每组报文开头的 11 位字符为标识符，定义了报文的优先级，这种报文格式称为面向内容的编址方案。在同一系统中标识符是唯一的，不可能有两个站发送具有相同标识符的报文。当几个站同时竞争总线读取时，这种配置十分重要。

当一个站要向其它站发送数据时，该站的 CPU 将要发送的数据和自己的标识符传送给本站的 CAN 芯片，并处于准备状态；当它收到总线分配时，转为发送报文状态。CAN 芯片将数据根据协议组织成一定的报文格式发出，这时网上的其它

站处于接收状态。每个处于接收状态的站对接收到的报文进行检测，判断这些报文是否是发给自己的，以确定是否接收它。

由于 CAN 总线是一种面向内容的编址方案，因此很容易建立高水准的控制系统并灵活地进行配置。我们可以很容易地在 CAN 总线中加进一些新站而无需在硬件或软件上进行修改。当所提供的新站是纯数据接收设备时，数据传输协议不要求独立的部分有物理目的地址。它允许分布过程同步化，即总线上控制器需要测量数据时，可由网上获得，而无须每个控制器都有自己独立的传感器。

二、工业控制网络的难点问题

工业控制网络主要存在以下五个难点问题：

1、工业机理模型数字化问题

工业互联网平台是软硬融合平台，工业软件在工业互联网平台数字化、网络化和智能化控制以及商业模式创新中发挥着核心作用，工业产品的数字设计、验证和测试，工业装备的数字化控制，都离不开工业软件支撑。工业软件绝非一般的普通软件，是工业机理模型数字化封装和复用，需要对工业工艺、技术和机理等长期积累。

目前，国际主流常用的各领域工业软件有超过 150 余款，涵盖研发设计、生产控制、测试验证等环节，几乎都是国外企业提供，且软件封闭不开源不开放。我国工业各细分领域国产工业软件全链条缺失，影响了国内企业工业互联网集成工业软件，已经成为了我国企业部署工业互联网平台最大障碍。

2、数字工业设备集成互联问题

完善接口标准是工业互联网平台发挥平台系统集成、资源汇聚、信息共享等作用的关键。工业数字化设备网络接入、工业软件互联互通等标准不统一，不同厂商提供工业数字化设备、工业软件也就无法综合集成和互联互通,更无法建成一体化的工业互联网平台，互联工厂和智能工厂也就无从谈起。

例如，目前市场上常用工业现场总线种类就超过 20 多种，由不同国际主要工业数字化设备厂商主导着，工业数字化设备五花八门，严重地影响了工业互联网平台对工业设备的综合集成。

3、数字工业设备高速互联问题

提供满足工业应用场景需求的工业网络接入服务，是工业互联网平台畅通内外信息流通渠道必要保障。固定光纤网络无法解决工业设备移动化应用场景需求，传统室内 WiFi 无法满足海量设备接入、大场景移动漫游、多路数据高速率并发传输等需求，工业 WiFi 设备存在大场景部署无法弹性伸缩等问题。

需要根据工业应用场景特殊需求，按照 5G 网络服务能力，为工业应用场景量身定制能解决网络接入痛点、技术切实可行、性价比高的 5G 专用网络部署方案。

4、工业网络化服务商业价值问题

商业模式创新是工业互联网平台发展的价值所在。企业数字化转型绝对不是简单的技术层面推动设备上云上平台，是通过商业模式创新来重塑工业企业在数字化条件下的物资链、服务链、价值链。没有商业模式重构的工业互联网平台建设，只能算是企业内部管理信息系统，难以从根本上推动企业数字化转型和变革。

目前，绝大部分工业企业在建设工业互联网平台过程中，都遭遇到了商业模式可行性问题。

5、数字工业设备可管可控问题

工业互联网平台遭受病毒等网络攻击，产生的危害更为巨大。当前工业互联网平台安全风险来自多个不同层次，需要保障来自不同工业互联网平台服务厂商的硬软件安全，确保不出现漏洞；需要保障网络接入安全，确保接入安全可信网络；需要保障数据使用安全，严格按照工业数据分级分类要求管理和使用数据。

目前面对工业设备全方位的安全保障体系由于技术、制度等原因尚未全面建立起来。

解决方法及措施：

1、多措并举推进工业软件普及应用和跨越发展

引导和支持工业软件服务商服务化转型，推进工业软件网络化和平台化服务，提高模块定制化服务能力，满足工业互联网平台综合集成需要。创新工业软件推进模式，鼓励和支持各领域行业龙头企业强强联合，创新合作推进机制，成立工业软件开发和运营公司，推动领域内工业软件的攻关突破和商业化应用。

2、加快建立涵盖工业软硬件的互联互通标准体系

加快建立工业网络接入标准，组建工业网络接入联盟，以主流工业网络协议为基础，制定统一的工业网络接入行业标准，适时上升为国家强制标准。建立数字工业设备接口标准，发展方便易用的工业设备连接器、转接器、连接线等连接设备，促进工业设备集成互联。建立工业软件关键数据共享标准，方便数据导入导出、共享交换、迭代更新和挖掘分析。

3、加快发展面向工业应用场景的网络接入服务

推进 5G 在工业应用场景的应用，根据工业应用场景特殊需求，选择合适的网络部署和组网模式，量身定做满足接入需求、性价比高的专用网络接入服务，提高大移动场景下网络接入服务能力。持续优化工业 WiFi，推进工业 WiFi 在工业应用场景的应用，提升移动部署和弹性伸缩服务能力，满足中小工业企业应用场景接入需求。

4、深化工业和互联网融合创新

加快推进企业上云步伐，按照先易后难、先外部后内部、促进业务创新等原则，做好企业上云规划，谋划好云端业务信息系统部署需求和部署方式，积极推进已建信息系统通过升级改造向云平台迁移，鼓励采购成熟的 SAAS 云业务系统服务和大型 PAAS 云平台开展企业业务系统建设。构建企业大数据中心，统筹规划企业数据资源，推进各类业务信息系统数据和系统分离，构建企业数据开发利用统一支撑平台，以数据应用创新推动业务创新变革。适应社会运行模式的转变，大力拓展网络空间新服务，提供数字化、网络化和智能化服务。

5、构建面向数字工业应用场景的安全保障体系

加快建立工业互联网网络接入、平台运行、数据使用等安全保障措施，增强入侵检测、电子认证、安全审计、角色管理等技术防护措施，加强产品安全测试和认证。完善技术、网络、平台、应用、人员等安全管理制度，建立工业互联网平台安全应急预案。

三、工业控制网络的发展趋势

工业控制网络的发展历程是分步骤的，从传统的控制网络发展到较为先进的现场总线，再后来随着科技文明的进步，发展为现在研究热点工业以太网以及到无线网络控制。未来工业网络的发展需要扩展以太网作为工业控制总线，提高控制总线的通信带宽，从通信的实时性、安全性和可靠性来努力，并且努力实现多总线路集成以及实时异构网络。

1、以太网作为现场控制总线

以太网作为现场总线的发展趋势其最大的优势在于它应用的广泛性。作为 IT 领域主流网络技术的以太网,经过十几年的发展,已经形成了十分巨大的硬件、软件资源,很多成熟的技术和产品都可以在工业以太网上直接加以借鉴或移植,另一方面,从事该领域研发和应用的人员与从事现场总线技术领域的技术人员比起来要多得多,这就为工业以太网的研究、开发、设计、运行和维护以及它的日益广泛的普及提供了非常坚实的基础。此外,与现场总线产品相比,以太网低廉的价格也是它逐渐得到广泛重视的一个重要原因。更为重要的是采用以太网作为现场总线技术,可以使现场总线技术的发展融入计算机网络技术的发展潮流当中,形成二者相互促进的局面,从而打破自动化控制领域任何垄断的企图,实现彻底的技术开放,使自动化领域产生新的生机和活动。

2、更高的带宽

更高的带宽是高性能工业控制网络的要求,要增加带宽,首先要分散控制数据,在将来的几年里,分散控制系统会产生增加二十到三十倍的制造信息。同样地,PLC 从场地设备采集的信息预计也会增加一二十倍。在自动化控制和通信设施中,如果总使用新的处理体系和技术,网络很可能无法承载,离散的网络组织也可能产生瓶颈效应从而对网络变成透明的、覆盖企业范围的应用实体产生阻碍。以太网的标准带宽是 10Mbps,近期研究高速以太网,其速度能达到百兆甚至千兆,从而能够成为企业大范围内的主干网络。在这种状况下,只有以太网能满足需要,这同时也促进了多样控制网络的出现。

3、高标准的通信要求

工业控制领域对于通信的实时性、安全性和可靠性要求较高,提高通信的质量将会为工业互联网的发展注入新的活力,从而提高生产的效率并保障安全性。未来可通过提高操作系统和交换技术以支持实时通信。此外,也可通过改善网络的拓扑结构或者优化 MAC 层上的数据传输调度方法用以提高实时性。安全性意味着能预防危险,如系统故障、电磁干扰、高温辐射以及恶意攻击等因素所带来的威胁。IEC 61508 针对安全通信提出了黑通道机制并制定了安全完整性等级 SIL。提高工业通信的安全性,以满足 SIL 高级别的要求,是工业控制网络安全性发展的趋势。工业控制网络基于不同的网络交换技术,需进行不同类型网络站点之间的通信,因此通信的可靠性显得尤为重要。

4、多总线集成

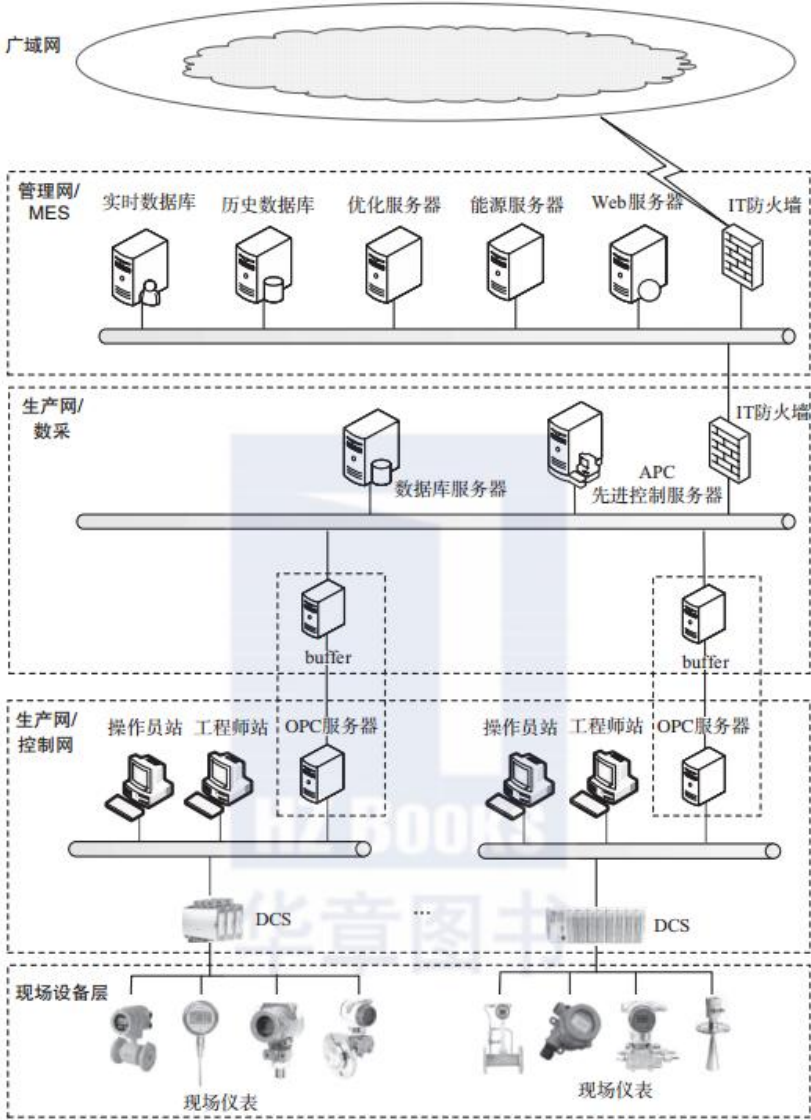
多总线并存且相互竞争的局面由来已久,在未来相当长的时间内这种局面还将继续。多总线集成协同完成工业控制任务,是未来发展的趋势,可通过使用代理机制,将单一总线系统中的设备映射到基于工业以太网的工业控制网络中。

5、实时异构网络

无线通信进入工业控制领域的趋势无可置疑。通过有线网络与无线网络融合、广域网与局域网集成来构建实时异构网络,是未来发展的趋势。在工业自动化领域,有成千上万的感应器,检测器,计算机,PLC,读卡器等设备,需要互相连接形成一个控制网络,通常这些设备提供的通信接口是 RS-232 或 RS-485。无线局域网设备使用隔离型信号转换器,将工业设备的 RS-232 串口信号与无线局域网及以太网信号相互转换,符合无线局域网 IEEE802.11b 和以太网 IEEE802.3 标准,支持标准的 TCP/IP 网络通信协议,有效的扩展了工业设备的联网通信能力。

四、典型应用

典型情形下，现有的炼化厂生产控制系统的网络拓扑图如图所示。大型石油化工产业控制系统庞大，安全要求高，现场由多个控制系统完成控制功能。大型石油化工工程全厂 DCS 采用大型局域网架构，网络架构较为复杂。现场的主要控制功能都是由 DCS 来完成的，其他系统的集中控制在某种程度上可以完全由 DCS 监控。DCS 含有大量的数据接口，是构建企业信息化的数据来源与执行机构。除



DCS 外的其他系统一般对外并没有数据接口（无生产数据），且相对独立，网络结构简单。

图 1 典型炼化厂网络结构拓扑图

主要控制系统的功能如下所示：

1、分布式控制系统（DCS）

DCS 完成生产装置的基本过程控制、操作、监视、管理、顺序控制、工艺联锁，部分先进过程控制也在 DCS 中完成。大型石油化工工程全厂 DCS 采用大型局域网架构。根据生产需求、系统规模和总图布置划分为若干独立的局域网，确保每套生产装置独立开停车和正常运行。

2、安全仪表系统（SIS）

SIS 设置在现场机柜室（FAR），与 DCS 独立设置，以确保人员及生产装置、重要机组和关键设备的安全。SIS 按照故障安全型设计，与 DCS 实时数据通信，在 DCS 操作员站上显示。大型石油化工工程全厂 SIS 采用局域网架构。根据生产需求、系统规模和总图布置划分为若干独立的局域网，确保采用 SIS 的生产装置独立开停车和安全运行。

3、可燃/有毒气体检测系统（GDS）

生产装置、公用工程及辅助设施内可能泄漏或聚集可燃、有毒气体的地方分别设有可燃、有毒气体检测器，并将信号接至 GDS。

4、压缩机控制系统（CCS）

压缩机控制系统完成压缩机组的调速控制、防喘振控制、负荷控制及安全联锁保护等功能，并与装置的 DCS 进行通信，操作人员能够在 DCS 操作员站上对机组进行监视和操作。

5、转动设备监视系统（MMS）

MMS 用于主要透平机、压缩机和泵等转动设备参数的在线监视，同时对转动设备的性能进行分析和诊断，对转动设备的故障预测维护进行有力的支持。

6、可编程逻辑控制系统（PLC）

操作控制相对比较独立或特殊的设备的控制监视和安全保护功能原则上采用独立的 PLC 控制系统。与 DCS 进行数据通信，操作人员能够在 DCS 操作员站上对设备的运行进行监视与操作。

7、在线分析仪系统（PAS）

在线分析仪（工业色谱仪、红外线分析仪等）应包括采样单元、采样预处理单元、分析器单元、回收或放空单元、微处理器单元、通信接口（网络与串行）、显示器（LCD）单元和打印机等。

具有如下特点：

- 1、自动化：自动化是减轻人的劳动，强化、延伸、取代人的有关劳动的技术或手段，石化工厂中生产的基础手段逐渐从手工操作发展到自动控制，从低级的单回路控制发展到高级复杂系统控制，从单元先进控制到区域集成优化。
- 2、数字化：数字化表现为可计算性和可度量性，是计算机、多媒体技术、软件技术、智能技术的基础，也是信息化的技术基础。
- 3、可视化：可视化的含义是将生产状态、工业视频等各类信息高度集中和融合，，加强对空间信息的管理，为操作和决策人员提供对现场环境的感知，确保迅速准确地掌握所有信息和快速的决策。
- 4、模型化：模型化是指通过利用生产运行数据和专家知识，将石化工厂的行为和特征的知识理解固化成各类工艺、业务模型和规则，实现人与制造系统的融合及人在其中智能的充分发挥。
- 5、集成化：集成化是指石化工厂中的系统与现有石化生产过程的工艺过程和管理业务流程高度集成，实现石化生产各个管理环节和各工序间紧密衔接与集成，从全局角度实现整体优化。