

现场总线Fieldbus简析

版本：v1.2.0

Crifan Li

摘要

此文主要介绍的现场总线的基础知识,以及现场总线的规范的简介和现场总线的一些特性,并且对简单介绍了常见的现场总线的基本架构和相关知识点,包括Profibus,Profinet,Ethernet/IP,HART,Foundation Fieldbus,还包括一些常见问题的思考



本文提供多种格式供：

在线阅读	HTML ¹	HTMLs ²	PDF ³	CHM ⁴	TXT ⁵	RTF ⁶	WEBHELP ⁷
下载（7zip压缩包）	HTML ⁸	HTMLs ⁹	PDF ¹⁰	CHM ¹¹	TXT ¹²	RTF ¹³	WEBHELP ¹⁴

HTML版本的在线地址为：

http://www.crifan.com/files/doc/docbook/fieldbus_intro/release/html/fieldbus_intro.html

有任何意见，建议，提交bug等，都欢迎去讨论组发帖讨论：

http://www.crifan.com/bbs/categories/fieldbus_intro/

修订历史

修订 1.0	2011-10-03	crl
1. 简述现场总线的基本知识 2. 对于常见的一些现场总线技术进行了简单介绍		
修订 1.2.0	2015-05-26	crl
1. 通过Docbook发布 2. 添加部分profinet内容		

¹ http://www.crifan.com/files/doc/docbook/fieldbus_intro/release/html/fieldbus_intro.html

² http://www.crifan.com/files/doc/docbook/fieldbus_intro/release/htmls/index.html

³ http://www.crifan.com/files/doc/docbook/fieldbus_intro/release/pdf/fieldbus_intro.pdf

⁴ http://www.crifan.com/files/doc/docbook/fieldbus_intro/release/chm/fieldbus_intro.chm

⁵ http://www.crifan.com/files/doc/docbook/fieldbus_intro/release/txt/fieldbus_intro.txt

⁶ http://www.crifan.com/files/doc/docbook/fieldbus_intro/release/rtf/fieldbus_intro.rtf

⁷ http://www.crifan.com/files/doc/docbook/fieldbus_intro/release/webhelp/index.html

⁸ http://www.crifan.com/files/doc/docbook/fieldbus_intro/release/html/fieldbus_intro.html.7z

⁹ http://www.crifan.com/files/doc/docbook/fieldbus_intro/release/htmls/index.html.7z

¹⁰ http://www.crifan.com/files/doc/docbook/fieldbus_intro/release/pdf/fieldbus_intro.pdf.7z

¹¹ http://www.crifan.com/files/doc/docbook/fieldbus_intro/release/chm/fieldbus_intro.chm.7z

¹² http://www.crifan.com/files/doc/docbook/fieldbus_intro/release/txt/fieldbus_intro.txt.7z

¹³ http://www.crifan.com/files/doc/docbook/fieldbus_intro/release/rtf/fieldbus_intro.rtf.7z

¹⁴ http://www.crifan.com/files/doc/docbook/fieldbus_intro/release/webhelp/fieldbus_intro.webhelp.7z

现场总线Fieldbus简析:

Crifan Li

版本 : v1.2.0

出版日期 2015-05-26

版权 © 2015 Crifan, <http://crifan.com>

本文章遵从 : [署名-非商业性使用 2.5 中国大陆\(CC BY-NC 2.5\)](#)¹⁵

¹⁵ http://www.crifan.com/files/doc/docbook/soft_dev_basic/release/html/soft_dev_basic.html#cc_by_nc

目录

术语表	1
正文之前	iii
1. 此文目的	iii
1. 现场总线的基础知识	4
1.1. 什么是现场总线	4
1.2. 为什么需要现场总线	4
1.3. 现场总线的连接方式	4
1.4. 现场总线的网络拓扑	4
2. 现场总线规范简介	6
2.1. IEC 61158规范简介	6
2.2. IEC 61158规范的内容	6
2.3. IEC 61158规范的众多的实现标准	7
3. 现场总线的一些特性	8
3.1. 现场总线的优点	8
3.2. 现场总线的缺点	8
3.3. 现场总线的安全性	8
3.4. 现场总线的市场和前景	8
4. 一些常见的现场总线的简介	10
4.1. PROFIBUS	10
4.1.1. 背景和现状	10
4.1.1.1. Profibus DP	10
4.1.1.2. Profibus PA	10
4.1.2. Profibus架构简介	10
4.1.2.1. 应用层	11
4.1.2.2. 数据链路层=安全层	11
4.1.2.3. 物理层=比特位传输层	11
4.2. PROFINET	11
4.2.1. Profinet CBA = components	16
4.2.2. Profinet IO = peripherals	16
4.2.3. Profinet领域内的一些名词术语	16
4.3. Ethernet/IP	17
4.3.1. Ethernet/IP的架构	17
4.4. HART	18
4.5. Foundation Fieldbus	18
5. 关于现场总线的一些思考	20
常见问题	20
问：为何现场总线都是实时的？	20
问：为何现场总线协议都只包含了OSI模型的1,2,7三层，而没有全部包含？	20
参考书目	21

插图清单

4.1. Profinet的CNC设备 : Challenger的Microcut	13
4.2. Profinet的CNC设备 : Biglia B465Y2	14
4.3. Profinet的CNC设备 : MillMatic III	15
4.4. Ethernet/IP的架构	17
4.5. 基于FF的控制系统的框架图	19

表格清单

1.1. 工业自动化控制系统的架构组成	4
2.1. IEC 61158标准的8种类型	6
2.2. ICE 61158协议组成	6
2.3. 现场总线部分特性和性能对比	7
4.1. 以OSI为参考模型的PROFIBUS协议架构	10
4.2. HART数据包的结构	18

术语表

ASIC (ASIC)	Application Specific Integrated Circuit 特定用途的集成电路
DCS (DCS)	Digital/Distributed Control System 数字化或分布式的控制系统
EIA (EIA)	Electronic Industrial Alliance 美国电子工业联合会
Ethernet/IP (Ethernet/IP)	Ethernet Industrial Protocol 以太网工业协议
FDL (FDL)	Fieldbus Data Link 现场总线数据链路 (层)
FF (FF)	Foundation Fieldbus 基金会现场总线
FPGA (FPGA)	Filed Programmable Gate Arrays 现场可编程门阵列
HART (HART)	Highway Addressable Remote Transducer 可寻址远程传感器高速通道协议
HMI (HMI)	Human Machine Interface 人机交互界面 可以简单理解为图形界面，方便用户操作对应的系统
IEC (IEC)	International Engineering Consortium 国际电工委员会 IEC负责电工，电子领域的国际标准化工作，于此对应的ISO，负责其他领域的国际标准。
IRT (IRT)	Isynchronous Real Time 等时式实时
LAN (LAN)	Local Area Network 局域网

	一种计算机网络，实现，在一个有限的范围内，所有的计算机互联
MBP (MBP)	Manchester Bus Powered 曼彻斯特总线供电
PLC (PLC)	Programmable Logic Controller 可编程逻辑控制器
Profibus (Profibus)	PROcess FieldBUS 过程现场总线
Profibus DP (Profibus DP)	Profibus Decentralized Peripherals 分散性外围设备过程现场总线
Profibus PA (Profibus PA)	Profibus Process Automation 过程自动化过程现场总线
SD (SD)	Start Delimiter 起始分隔符

正文之前

1. 此文目的

此文主要是简述现场总线的一些基本知识，包括现场总线的历史，为何需要现场总线，以及对应的IEC 61158规范的相关知识和对应此规范的实现协议有哪些。

第 1 章 现场总线的基础知识

1.1. 什么是现场总线

现场总线，是一组工业计算机协议的总称。这些协议是用于实时的分布式控制方面的。

现在标准化为 IEC 61158

1.2. 为什么需要现场总线

对于一个复杂的工业自动化控制系统，比如制造生产线，常常需要一个有良好的系统架构，才能更好地实现，控制系统去控制对应的功能模块。

而这套控制系统架构，一般包含了上层的人机交互界面HMI，以便操作者监视和操作系统，这一层，往往又通过一个对时间不是很敏感的（non-time-critical）通讯系统，比如Ethernet，与下面的PLC的中间层相连接。在控制系统的最底层，就是对应的现场总线，将PLC连接到对应的实际工作的功能组件上，比如传感器（sensor），制动器（actuator），电动机（electric motor），灯光控制（console light），开关（switch），阀门（valve），接触器（contactor）。

所以，需要现场总线，将控制系统的上层HMI+中间层PLC，连接到实际工作的模块，以实现对应的控制功能。

下表简要概括了，常见的工业自动化控制系统中，各个层次之间的关系：

表 1.1. 工业自动化控制系统的架构组成

层次	包含的内容	解释
上层	HMI人机交互界面	用户操作和控制的界面
通讯系统（比如Ethernet等）		
中间层	PLC或者控制器	
现场总线（比如Ethernet/IP, FF, Profibus等）		
底层	被控制的功能模块	比如传感器，电动机等

1.3. 现场总线的连接方式

最开始，两个计算机之间，都是以RS232连接的。但是缺点是只能在2个设备之间连接通信。

此连接方式等价于现在所用的“4-20 mA通讯方案”（4-20 mA communication scheme），其要求，每一个设备在控制器层面上，都有其自己的通讯端口，而现场总线等价于当前的LAN类型的网络连接。其只要求在控制器的级别上，有一个通讯端口，然后允许同时连接成百上千的模拟的和数字的模块。此方案，即降低了对电缆长度的要求，又减少了对电缆数目的需求。

再者，由于设备通过现场总线连接的话，需要一个微处理器，所以同一个设备可以提供多个端点。有些现场总线现在支持一种PID控制方案，在设备端实现控制功能，而不需要控制器端去处理。

1.4. 现场总线的网络拓扑

即现场总线中，各个组件之间，是什么样的连接方式，有这些网络拓扑形式：

- 菊花链（daisy chain）
- 星形（star）
- 环形（ring）

- 分支型 (branch)
- 树形 (tree)

第 2 章 现场总线规范简介

现场总线技术1988年左右就出现了，后来经过漫长的时期，才发展为最初的IEC 61158标准，其包含了8个不同的协议集合，此处叫做“类型（type）”：

表 2.1. IEC 61158标准的8种类型

类型	名称
Type 1	Foundation Fieldbus H1
Type 2	ControlNet
Type 3	PROFIBUS
Type 4	P-Net
Type 5	FOUNDATION fieldbus HSE (High Speed Ethernet)
Type 6	SwiftNet (a protocol developed for Boeing, since withdrawn)
Type 7	WorldFIP
Type 8	Interbus

此种形式的标准，最初是为欧洲经济共同体（European Common Market）所开发的，主要重点不在通用性，公平性，而在于实现其主要目的，即取消各个贸易国之间的贸易壁垒。

而关于通用性的问题，则是留给了那些负责支持现场总线标准类型的国际公会联盟。几乎是自从“八国首脑”成立后，此IEC标准开发工作就停止了，委员会也解散了。一个新的IEC委员会 SC65C/MT-9成立了，旨在解决不同形式的标准之间的冲突和维护4000多页的IEC 61158协议标准。

原先的协议类型基本已完成，而新的协议，例如安全现场总线（safety fieldbus）或者是基于以太网的实时的现场总线，也被吸收接纳进入此国际版的现场总线标准中了。维护此协议的时间，基本算是5年一个周期。

目前，在过程控制领域，不论是新的开发还是主要的改装，FF（Foundation Fieldbus）和Profibus技术已经得到广泛实现和应用了。

2.1. IEC 61158规范简介

现场总线技术，有很多种。因此，没有实现其最原始的期望，即希望用一个通讯机制统一所有的应用。而这点，不是没有预料到，而且是因为现实的实际情况是，不同的应用领域，的确需要不同的规范的实现。比如，汽车制造方面的现场总线，从功能上，就和工厂的生产线的控制，不一样。

最终的IEC61158标准，则允许8种实现技术。对于自动化协议，这其中也内含一些层次关系。

2.2. IEC 61158规范的内容

IEC 61158规范，标题是 用于测量和控制领域的数字化数据通讯-现场总线，用于工业控制系统，其包含了以下部分：

表 2.2. ICE 61158协议组成

组成部分	协议内容
Part 1	IEC 61158系列协议的概述和一些指导意见
Part 2	物理层的规范和服务的定义
Part 3	数据链路层的服务定义
Part 4	数据链路层的协议规范

组成部分	协议内容
Part 5	应用层的服务定义
Part 6	应用层的协议规范

2.3. IEC 61158规范的众多的实现标准

现场总线标准的实现，有很多种，而不同的协议有不同的特性和性能。

而由于其之间，数据传输方法的极大差异，使得也没有一个通用的比较模式去比较它们之间的性能区别。

下表，以对应的现场总线通常是否支持1ms或更快的数据更新周期为例，进行了简单的比较：

表 2.3. 现场总线部分特性和性能对比

Fieldbus	Bus power	Cabling redundancy	Max devices	Synchronisation	Sub millisecond cycle
AS-Interface	Yes	No	62	No	No
CANOpen	No	No	127	Yes	No
CompoNet	Yes	No	384	No	Yes
ControlNet	No	Yes	99	No	No
CC-Link	No	No	64	No	No
DeviceNet	Yes	No	64	No	No
EtherCAT	No	Yes	65536	Yes	Yes
Ethernet Powerlink	No	Optional	240	Yes	Yes
EtherNet/IP	No	Optional	Almost unlimited	Under development	No
Interbus	No	No	511	No	No
LonWorks	No	No	32000	No	No
Modbus	No	No	246	No	No
PROFIBUS DP	No	Optional	126	Yes	No
PROFIBUS PA	Yes	No	126	No	No
PROFINET IO	No	Optional	Almost unlimited	No	No
PROFINET IRT	No	Optional	Almost unlimited	Yes	Yes
SERCOS III	No	Yes	511	Yes	Yes
SERCOS interface	No	No	254	Yes	Yes
Foundation_Fieldbus_H1	Yes	No	240	No	No

第 3 章 现场总线的一些特性

3.1. 现场总线的优点

和"4-20 mA通讯方案"相比，现场总线只需少得多的电缆即可实现互联。

因此，许多设备，可以通过一拖多的方式，共享同一组的电缆，而4-20mA的连接，对每一个设备，都需要一组特定的电缆。

而且，现场总线网络，在单次通信中可以传送多个参数，而4-20mA的连接，一次只能传送一个参数。

3.2. 现场总线的缺点

与4-20mA的模拟信号标准的方案相比，现场总线也有一些缺点：

1. 现场总线显得更加复杂，所以需要用户有足够的知识和受到专业的培训后，方能应用。
2. 现场总线的组件，价格更高些
3. 和4-20mA中用来读取或模拟信号的万用表相比，现场总线的测试设备，也更复杂。
4. 不同的现场总线的系统，反馈信号所需时间也不同，不过相比4-20mA要稍微长一些。
5. 设备制造商必须为不同的现场总线标准，为同一设备，提供多个不同版本。这会增加设备成本设备选择方面的难度。
6. 在众多的现场总线标准中，其中很少的一些，会随着时间发展，逐渐占领大部分的市场，而其他一些，则会逐渐地淘汰。这对于投资去实现现场总线，也是一个要考虑的风险。

3.3. 现场总线的安全性

对于一些必须满足一些安全性标准，如IEC 61508或EN 954-1，的系统来说，现场总线，也是适用的。

取决于实际所用的不同的协议，现场总线，也可以支持一些评测特性，比如计数器，CRC校验，回显，超时，发送者或接受者的ID的唯一性，交叉校验。

Ethernet/IP和SERCOS III，都使用CIP安全协议，Ethernet Powerlink使用openSAFETY，而FF和Profibus，都有各自的一些兼容安全协议的变体。

3.4. 现场总线的市场和前景

目前，现场总线协议，在过程控制系统中，用的最多的是FF和PROFIBUS PA。

两种技术都使用相同的物理层，即双线的31.25KHz的曼彻斯特编码的电流调制，

关于选择哪类现场总线，概括地说就是：

- 通过PLC来控制 and 监视方面的应用，倾向于用Profibus
- 通过数字化或分布式的控制系统DCS来监视和控制的应用，倾向于用FF

近来，出现了一些基于以太网的工业通讯系统，其中多数都是属于原系统在在实时通讯方面的扩展，从长远看，这些系统会逐渐取代现有的现场总线技术的。

如下列举了一部分这类新的，基于以太网的工业通讯系统：

- EtherCAT

- EtherNet/IP
- Ethernet Powerlink
- PROFINET IO
- PROFINET IRT
- SafetyNET p
- SERCOS III
- TTEthernet
- VARAN

第 4 章 一些常见的现场总线的简介

4.1. PROFIBUS

4.1.1. 背景和现状

1987年，德国，21个公司和组织，发起了一个项目计划，叫做“现场总线”，并成立了一个协会，目的是，实现和传播，基于现场设备接口的基本需求，而产生的“串行位”的现场总线的应用。为了实现这一目的，成员国达成一致，愿意支持一种通用的技术概念，用于生产和过程自动化。

最初，制定出的第一个规范是Profibus FMS（现场总线消息规范，Field Bus Message Specification），其经过裁剪用于要求较高的任务间通讯。在接下来的1993年，又制定出了更加简单，速度也更快的协议，Profibus DP（分散性外围设备）协议。

Profibus FMS用于Profibus主控(Master)之间的非确定性的数据通信；

Profibus DP用于Profibus主控和其远程的从设备的IO之间的确定性的数据通信。

目前Profibus主要有两类，用的最多的是Profibus DP，其次是，和应用相关的Profibus PA。

4.1.1.1. Profibus DP

在生产自动化应用中，通过一个中央化的控制器，用此Profibus DP，去操作传感器和制动器。

许多标准的诊断方法，也主要是针对这方面的应用。

4.1.1.2. Profibus PA

在过程自动化应用中，用Profibus PA，通过过程控制系统，去监测设备。此技术主要是用于爆炸性的和对人体有害（Ex-zone 0 and 1）的环境中。

物理层，比如电缆，符合IEC 61158-2的规范，其支持现场的设备通过总线供电的同时由于电流很小，所以即使出现故障，也不会产生爆炸。也因此，总线上连接的设备的数目是比较有限的。

PA的数据传输速率有31.25Kbit/s，但是PA却是和DP用同一种协议，可以通过一个耦合器与DP进行连接。而速度相对较快的DP，则是起到一个主干网的作用，将过程信号数据传输到控制器端。这就意味着，DP和PA可以紧密地协同地工作，尤其是在那些过程和工业自动化，都是各自为政的混合型的应用中。

4.1.2. Profibus架构简介

下表为以OSI为参考模型的Profibus的协议架构：

表 4.1. 以OSI为参考模型的PROFIBUS协议架构

OSI-Layer		PROFIBUS			
7	Application	DPV0	DPV1	DPV2	Management
6	Presentation				
5	Session				
4	Transport	---			
3	Network				
2	Data Link	FDL			

OSI-Layer		PROFIBUS		
1	Physical	EIA-485	Optical	MBP

4.1.2.1. 应用层

为了实现对应的功能，定义出了DP协议中的各种服务：

1. DP-V0
用于周期性的数据交换和设备诊断
2. DP-V1
用于周期和非周期的数据交换和警报处理
3. DP-V2
用于等时模式和数据交换广播（从设备到从设备的通讯）

4.1.2.2. 数据链路层=安全层

此处的FDL (Fieldbus Data Link) 层也叫做安全层，其将令牌环传递模式和主从模式合并而成为混合访问模式。在Profibus DP的网络中，控制器或者是过程控制系统，是主设备端，传感器和制动器，是从设备端。

其是用各种不同类型的报文，每种报文有各自不同的起始分隔符（SD，start delimiter）。

4.1.2.3. 物理层=比特位传输层

比特位传输（Bit-transmission）层，包含了三种方式：

1. EIA-485
即RS-485，根据EIA-485的电信号传输标准，在总线拓扑中使用电阻是150欧姆的双绞线。可用的比特率是从9.6kbit/s到12Mbit/s。两个中继器之间的电缆长度限制是在100米到1200米，具体长度取决于比特率。传输方法主要是用Profibus DP。
2. 光纤
如果是通过光线传输，那么拓扑结构可选用为星形，总线型，环形。中继器之间的长度最大可达15km。环形拓扑可以冗余式地对应延长
3. MBP
根据MBP (Manchester Bus Powered) 传输技术，可用同一电缆实现供电和数据传输。由于极大地降低了供电，使得可以应用在易爆炸和对人体有害的场合中。总线拓扑结构，可以长达1900米，以及最长分支可达60米。此处比特率是固定的31.25kbit/s，此拓扑结构是专为Profibus PA用于过程自动化领域而设计的

4.2. PROFINET

TODO：对于：

[【整理】SIEMENS SINUMERIK 828D简介和CNC的含义¹](#)中关于SINUMERIK 828D的，和

<http://www.industry.siemens.com/topics/global/en/magazines/special-editions/Documents/MotionWorld-2012-IMTS-en.pdf>

http://www.industry.siemens.com/topics/global/en/cnc4you/cnc_downloads/cnc4you-magazine/Documents/cnc4you_2012_1_en.pdf

¹ http://www.crifan.com/industrial_automation_cnc_meaning_and_siemens_sinumerik_828d/

[视频: 西门子 Siemens SINUMERIK 828D](#) ²

[Tutorial Programming Sinumerik 828D and 840D sl with ShopTurn](#) ³

中的截图，应用案例，整理出来。

TODO：去看

[SINUMERIK 828D BASIC CNC Control](#) ⁴

[SINUMERIK 828D Simple Setups](#) ⁵

可以对于CNC数控机床有个更直观的了解：了解CNC如何控制机械去操作设备的

TODO：

有空再去研究：

[SINUMERIK 828D rear](#) ⁶

中的很多应用案例。

下面是一些相关的产品图片供参考，以便了解对应的该领域内的设备大概长啥样：

² http://v.youku.com/v_show/id_XMjE2MDc1Mjgw.html

³ <http://www.youtube.com/watch?v=it4pa1wLdR4>

⁴ <http://www.youtube.com/watch?v=1vUOmYjonYw>

⁵ <http://www.youtube.com/watch?v=82ng1BqvSck>

⁶ http://www.google.com.hk/search?newwindow=1&safe=strict&client=firefox-a&rls=org.mozilla:zh-CN:official&q=SINUMERIK+828D+rear&um=1&ie=UTF-8&hl=zh-CN&tbm=isch&source=og&sa=N&tab=wi#facrc=_&imgdii=_&imgrc=VvjhL1sAcF6diM%3A%3B6o_TlJN_dgN9ZM%3Bhttp%253A%252F%252Fbernardandcompany.files.wordpress.com%252F2013%252F02%252F01_biglia.jpeg%253Fw%253D614%3Bhttp%253A%252F%252Fbernardandcompany.wordpress.com%252Fcategory%252Fsiemens-machine-tools%252Fpage%252F%252F%3B614%3B350

图 4.1. Profinet的CNC设备：Challenger的Microcut



图 4.2. Profinet的CNC设备：Biglia B465Y2



图 4.3. Profinet的CNC设备：MillMatic III



Profinet是一个开放式的，Profibus & PI在自动化领域的工业以太网方面的标准。

Profinet使用TCP/IP和IT协议标准，是一个实时的以太网。

Profinet特点在于是一个模块化的架构，因此，用户可以自定义地去选择每一层所用何功能。

与Profinet一起的还有另外两个，Profinet CBA和Profinet IO。

Profinet CBA适用于通过TCP/IP的基于组件之间的通讯，和在模块化的系统中的，实时的通讯。此两种通讯，都可以并行使用。

Profinet IO是为分散的外设之间的实时RT和等时实时IRT的通讯，而设计的。

指定的RT和IRT，仅仅描述了Profinet IO中通讯的实时的特性而已。

在同一总线系统中，同一时刻，可以允许Profinet CBA和Profinet IO同时通讯。他们可以分别或合并起来操作，这样的话，从系统层次看的话，Profinet IO子系统就像是一个Profinet CBA系统。

为了实现这些功能，定义了三种层次的协议：

1. TCP/IP协议
用于Profinet CBA和工厂的试运行，反馈时间在100ms级别
2. RT实时协议
用于Profinet CBA和Profinet IO应用，时间周期是10ms级别
3. IRT等时式实时协议
用于Profinet IO应用的驱动系统中，时间周期在1ms级别

4.2.1. Profinet CBA = components

一个Profinet CBA系统，包含了众多的自动化组件。每个组件都涵盖了机械，电子，和IT方面的参数。组件可以通过标准编程工具生成出来。组件是用XML格式的PCD (Profinet Component Description) 文件来描述的。

使用配置工具，就可以从这些描述文件中载入对应的配置，并启用这些组件之间的逻辑的内部连接，以实现一个工厂。

此模型主要是受到了IEC 61499规范的启发而得。

4.2.2. Profinet IO = peripherals

通过Profinet IO来实现外设之间的交互。Profinet IO定义了现场连接的设备之间的通讯。

其基本思想是层级式的实时概念。Profinet IO定义了在主控制器与从设备之间的整个的数据交换，以及参数设置和如何调试诊断。

Profinet IO遵循供给者-消费者的模型，设计是用于基于以太网的现场设备之间的快速的数据交换。

Profinet IO包括了如下设备：

1. IO控制器
其控制自动化任务的实现
2. IO设备
现场设备，受IO控制器的监视和控制。单个的IO设备可能会包含多个模块或子模块
3. IO监控者
软件实现，常为基于PC端的软件，用于设置参数和调试单个的IO设备

在IO控制器和IO设备之间，会建立起一个应用关系 (AR, Application Relation)，这类AR是用于在参数传输，周期性的数据交换，警报处理等不同的特性之间，去定义对应的通讯关系 (CR, Communication Relation)。

IO设备的特性，是通过设备制造商的通用配置描述符 (GSD, General Station Description) 来描述的。用于此描述的语言是一个基于XML的GSDML (GSD标记语言)。GSD文件提供监视软件，作为去规划配置一个Profinet IO的系统提供一个基础。

4.2.3. Profinet领域内的一些名词术语

- PC/PG或PG/PC
可以在：

http://www.automation.siemens.com/doconweb/pdf/SINUMERIK_SINAMICS_04_2010_E/828D_SH.pdf

中看到PG/PC，含义是：Programming Device/Personal Computer

- PPU==Panel Processing Unit=面板处理单元

[【整理】PROFINET应用实例：SIEMENS的SINUMERIK 828D系统框架示例连接图：SINUMERIK 828D+MCP 483C PN+PP 72/48D PN+其他⁷](#)

中已有整理：

PPU==Panel Processing Unit=面板处理单元

4.3. Ethernet/IP

Ethernet/IP，以太网工业协议，主要用于过程控制和工业自动化应用领域。

Ethernet/IP是一个应用层的标准，其将网络中的所有设备都视为一系列的对象object。

Ethernet/IP是基于广泛使用的CPI协议的，其可以无缝地实现去访问来自ControlNet和DeviceNet的对象。

Ethernet/IP利用现有的网络架构，即Ethernet网络。

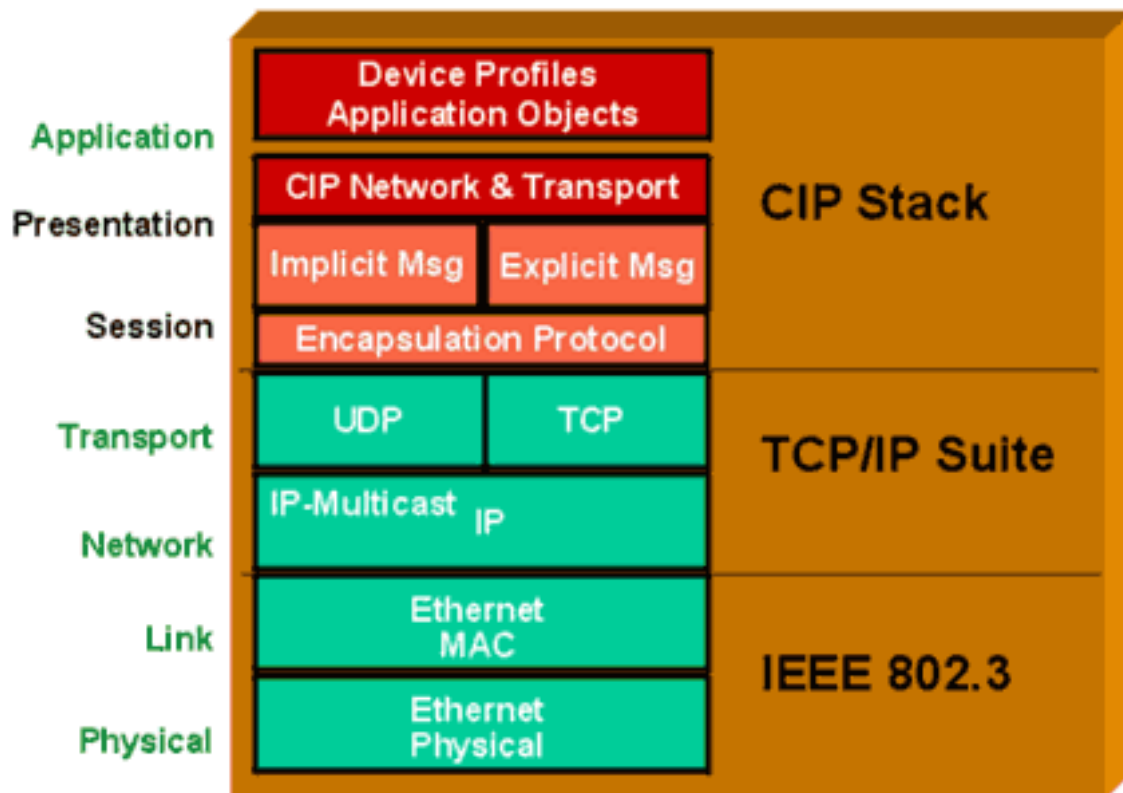
整个的Ethernet/IP协议栈，都可以通过微处理器之上的软件来实现，而不再需要特定的硬件（比如ASIC，FPGA等）。

Ethernet/IP，是基于TCP/IP协议栈之上，用到了全部的OSI的7层模型。

4.3.1. Ethernet/IP的架构

Ethernet/IP的架构，可以用下图很清晰的表示出来：

图 4.4. Ethernet/IP的架构



⁷ http://www.crifan.com/profinet_siemens_sinumerik_828d_system_arch_and_mcp_483c_pn/

4.4. HART

HART, Highway Addressable Remote Transducer Protocol, 可寻址远程传感器高速通道协议, HART是作为数字化工业自动化协议的现场总线的最早期的实现。

其最引人注目的特点是, HART可以在旧的4-20mA的模拟仪表配线上, 共享使用双绞线, 进行通讯。由于过去的大量的系统是基于4-20mA的方案, 也使得HART协议成为现在最流行的工业协议之一。

对于习惯使用旧的4-20mA的信号系统的人来说, 想要去实现更加智能化的协议。HART算是提供了一个很好的协议转换。目前工业界中, 使用Profibus DP/PA和FF的, 越来越多了, 因为对于用户来说, 越来越熟悉这些技术了, 也愿意使用性能更好的调试功能。

HART有两种操作模式, 对等模式(模拟/数字模式)和多支路(Multidrop)模式。

1. 对等(peer-to-peer = analog/digital)模式
数字信号重叠与4-20mA的环路电流之上。

对于设备来说, 数字信号和4-20mA的电流, 都是有效的输出。轮训的设备地址设置为0.对于每一个仪器的电缆的信号对来说, 只能放置一个设备。单个用户指定的信号, 作为4-20mA的信号, 另外的信号, 在4-20mA信号之上, 作为数字信号发送。例如, 压力参数可以通过4-20mA信号, 表示压力的范围, 而温度可以通过同一信号线, 作为数字信号传送

2. 多分支(multidrop)模式
只用数字信号。

模拟的环路电流是固定的4mA。在multidrop模式中, 单个信号线缆, 可能会接多个仪器。HART的3到5版本中, 允许轮训仪器地址的范围是1-15.第6版即之后的HART, 最大寻址达63.每个仪表都有个独一无二的地址。

HART的数据包的结构为:

表 4.2. HART数据包的结构

域名	长度(字节)	用途
Preamble	5-20	同步和载波检测
Start Byte	1	指定主设备号
Address	1-5	指定注从设备, 指定突发模式
Command	1	数字值, 用于要执行的命令
Number of Data Bytes	1	指定数据域的大小
Status	Master (0) Slave (2)	执行和健康状况回应
Data	0-253	和命令相关的数据
Checksum	1	异或所有的字节, 从起始字节到倒数第二个字节, 而得到的校验值

4.5. Foundation Fieldbus

Foundation Fieldbus, 一般简称为FF, 是一个全数字化的, 串行的, 双向的通讯系统。

其在工厂或生产自动化环境中, 起到一个基础的网络功能。

FF主要用于过程工业领域。

FF主要分两类:

1. H1
工作在31.25kbit/s，常连接到现场设备上。通过标准的双绞线供电和实现数据通信。HI是目前用的最多的
2. HSE
High Speed Ethernet，高速以太网，工作在100Mbit/s，常通过标准的以太网电缆，连接到IO子系统，主机系统，连接服务，网关，和现场设备。目前来说，不支持通过电缆供电。与FF HSE对应的规范是IEC 61804

下图是一个基于FF HSE的控制系统的框架图：

图 4.5. 基于FF的控制系统的框架图

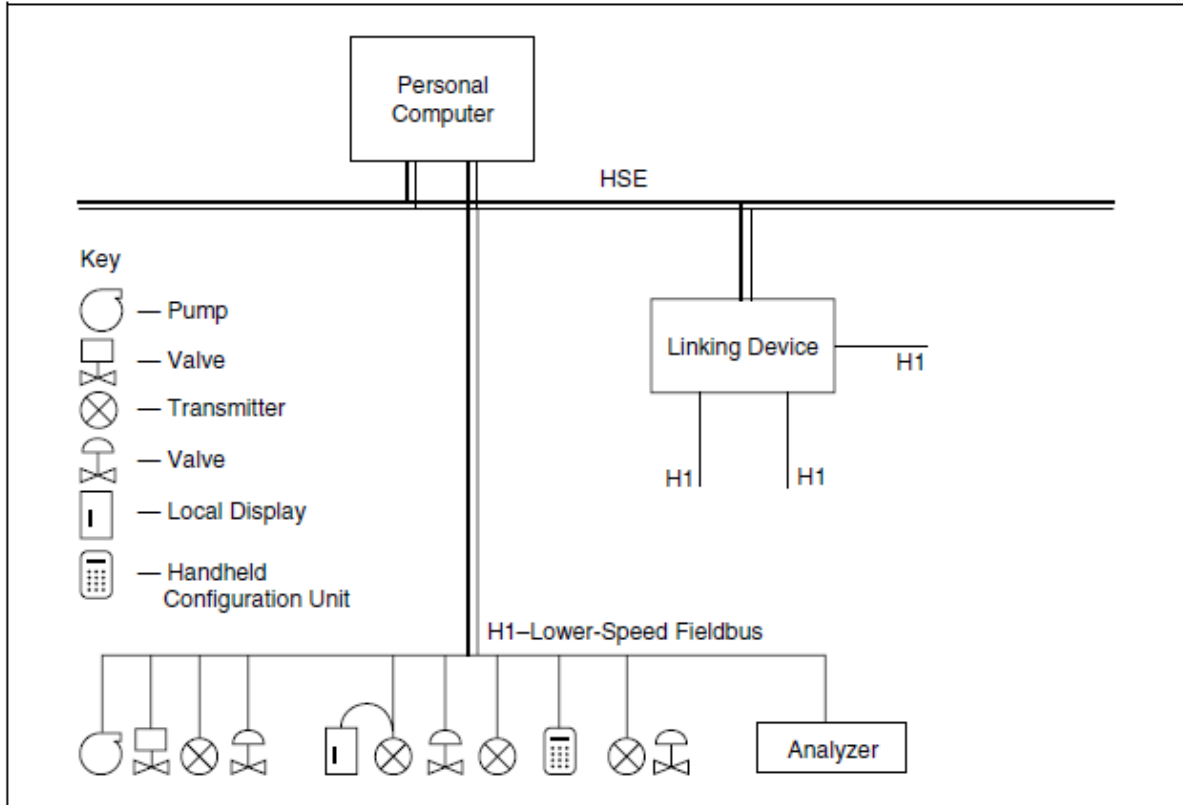


Figure 1-1. Foundation Fieldbus-Based Control System

第 5 章 关于现场总线的一些思考

问：为何现场总线都是实时的？

答：由于工业控制等领域中，系统要去控制这些工作模块，往往都需要精准的时间，所以，现场总线也必须是实时的。

即在既定的时间内，就必须将控制信息等数据传送到对应的被控设备中，以实现对其控制。

如果通过现场总线传输数据的过程中，耗时太长，或者延迟超过特定的限制，那么很可能就会失去对设备的控制，在设备出现异常等情况的时候，也无法及时有效地控制设备做出必要的响应。因此，现场总线，必须是实时的。

问：为何现场总线协议都只包含了OSI模型的1,2,7三层，而没有全部包含？

答：首先，对于此问题的解释，如果是问现场总线所实现出来的协议来说的话，那么，由于对应的协议是由对应的现场总线的规范而决定的，所以，此问题的答案很简单，就是现场总线的规范的定义中，表面上看，就只定义了OSI的1,2,7层，所以对应的实现的现场总线的协议，也因此只包含了OSI的1,2,7层。

而如果继续问，为何现场总线规范中，只实现了OSI的1,2,7层，而没有实现所有的层次，那么答案是：

OSI的模型中，分了7层，而现场总线虽然表面上看只实现了1,2,7三层，但是实际上：

现场总线的2,7层=OSI的2,3,4,5,6,7层，

即功能上，都是已经实现了，只是没有细分出来而已。

为何没有细分出来，主要原因还是在于：

实际的现场总线的应用环境中，不需要这么多层次。将层次简化了，显得结构更加紧凑，可以使得降低各层次之间的通信的开销，以实现更低的通信延迟，更快的速度，更利于实现现场总线的实时特性。

那么再来细看现场总线的这1,2,7三层：

- 第一层，物理层
关于物理电路特性，比如电压是3.3V还是5V等，这个，肯定是必须的
- 第二层，数据链路层
关于数据是如何组织的，也是需要说明清楚的
- 第七层，应用层
表明了具体的应用

此三层，算得上是最精简的了，也很难再简化了。

参考书目

- [1] [Fieldbus](#)¹
- [2] [Profibus](#)²
- [3] [Profinet](#)³
- [4] [Local area network](#)⁴
- [5] [SERCOS III](#)⁵
- [6] [现场总线通信模型的特点](#)⁶
- [7] [为什么大多数现场总线协议只包含OSI的1,2,7层](#)⁷
- [8] [EIA-485](#)⁸
- [9] [国际电工委员会](#)⁹
- [10] [Ethernet/IP](#)¹⁰
- [11] [Ethernet/IP](#)¹¹
- [12] [Highway Addressable Remote Transducer Protocol](#)¹²
- [13] [FOUNDATION fieldbus](#)¹³
- [14] [Foundation Fieldbus Overview](#)¹⁴
- [15] [【整理】PROFINET应用实例：SIEMENS的SINUMERIK 828D系统框架示例连接图：SINUMERIK 828D+MCP 483C PN+PP 72/48D PN+其他](#)¹⁵

¹ <http://en.wikipedia.org/wiki/Fieldbus>

² <http://en.wikipedia.org/wiki/Profibus>

³ <http://en.wikipedia.org/wiki/PROFINET>

⁴ http://en.wikipedia.org/wiki/Local_area_network

⁵ http://en.wikipedia.org/wiki/SERCOS_III

⁶ <http://bbs.cechina.cn/thread-141333.html>

⁷ <http://zhidao.baidu.com/question/244236780.html>

⁸ <http://en.wikipedia.org/wiki/EIA-485>

⁹ <http://www.ccsa.org.cn/organization/intro.php?org=IEC>

¹⁰ http://www.anybus.cn/technologies/ethernet_ip.shtml

¹¹ <http://en.wikipedia.org/wiki/EtherNet/IP>

¹² http://en.wikipedia.org/wiki/Highway_Addressable_Remote_Transducer_Protocol

¹³ http://en.wikipedia.org/wiki/FOUNDATION_fieldbus

¹⁴ <http://www.ni.com/pdf/manuals/370729a.pdf>

¹⁵ http://www.crifan.com/profinet_siemens_sinumerik_828d_system_arch_and_mcp_483c_pn/