

PLC

网络系统配置指南

WANGLUO XITONG PEIZHI ZHINAN

宋伯生 编著

厂各部门间
信息网络

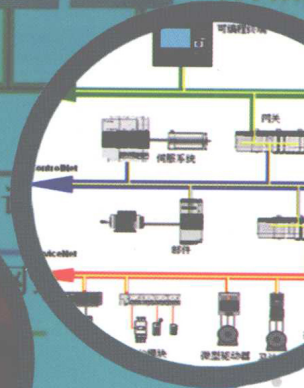
工厂内
控制系统
网络

生产线内
现场总线
网络

设备内
网络

243-2 277 241 243-1243-1 IT
* Email
* HTML

模拟电话



机械工业出版社
CHINA MACHINE PRESS

PLC 网络系统配置指南

宋伯生 编著



机械工业出版社

前 言

PLC 网络的广泛应用是进入 21 世纪以来 PLC 技术进步的重要标志。PLC 连网已是当今 PLC 硬件的必要配置。正是 PLC 网络的广泛应用, PLC 控制系统已越来越成为工厂信息系统不可分割的组成部分, 再也不是孤立的“信息孤岛”。可以这么说, 当今已是“无 PLC 不连网”, 差别只是连的是什么网络, 以及是常态连网还是临时连网。试想, 当今 PLC 不连网怎么编程? 不编程又怎么能工作?

处理 PLC 连网有两个基本问题要解决好: 一是系统配置, 二是通信编程。前者是组建(设计、采购、安装)网络与配置(设置、组态)网络, 为后者提供平台。后者要使网络正常运转, 实现站点间数据交换、信息交流, 达到连网的目的。这两者缺一不可, 但各有各的着重点。一般来讲, 从事系统集成的更重视前者, 总要尽量把网络组建好。而网络使用人员则更关心后者, 力求使组建好的网络为控制优化与信息交流所用。本书着重介绍系统配置, 至于通信编程将另有专著介绍。

本书共 5 章。之前还有简短的绪论。由于至今对 PLC 网络还没有公认的定义, 所以, 在此先对本书要讨论的 PLC 网络的有关概念做一些介绍, 以便理解后续章节的内容。

本书第 1 章介绍 PLC 网络基础知识。从技术的基本点上讲, PLC 网络与计算机网络是完全相同的。所以, 本章介绍的 PLC 网络基础知识也包含有很多计算机网络的知识。此外, 本章还对 PLC 网络的概况及通信实现作了说明。

第 2 章介绍 PLC 串口网络配置。先是介绍串口常用标准, 继而介绍各种常用品牌 PLC 的串口特点及网络配置实例。串口网络虽是最简单、最基本, 也是 PLC 使用最早、最常见的网络。但它的技术也在发展, 功能也在增加。通过串口, 实现计算机、人机界面与 PLC 连网、通信是最廉价, 也是最方便的。在相同品牌 PLC 之间, 使用它很容易连网, 并可实现多种方式的数据交换与相互操作。在不同品牌 PLC 之间, 如必要, 也可对其中一个串口做适当转换便可连网, 并利用好相关通信指令也可通信。至于现场设备, 只要配置有串口, PLC 也可与其连网、通信。所以, 本书介绍 PLC 网络首先对串口网络做了较详细的说明。

第 3 章介绍 PLC 设备网配置。PLC 设备网是用以实现 PLC 与地处远程的操作器、传感器这样的底层工业设备通信的网络, 是 PLC 实现远程分布控制的基础, 已用得越来越多。考虑到这类网络的普及情况及发展前景, 这里主要介绍 AS-i、CC-Link/LT 及 CompoNet3 种开放的标准设备网络。

第 4 章介绍 PLC 控制网配置。PLC 控制网主要用于 PLC 站点间的数据交换与相互操作, 也可用于 PLC 对远程控制的控制, 既是 PLC 最重要的网络, 也是 PLC 实现控制网络化的基础。特别是随着 PLC 控制地域的扩展, 控制规模的扩大, 其应用也越来越多。

过去 PLC 控制网络多是专有的，一家一个样，而如今已有了很多公认的开放标准网络。而且，有实力的 PLC 厂家的新机型多在使用自身专有控制网络的同时，也逐步与开放网络标准兼容。一些 PLC 厂家，如和利时、ABB 公司干脆就直接采用这些标准，以使自身的产品可以加入这些网络，从而扩展自身产品的应用。为此，本书在介绍 PLC 控制网络时，就只介绍几个流行的开放标准网络，具体是 CC-Link、DeviceNet、ControlNet 及 Profibus 等。

第 5 章介绍 PLC 信息网配置。当今 PLC 信息网用的几乎全以太网。这与以太网的技术优势、发展快速与应用广泛有关。原先 PLC 以太网主要是用于与企业高层计算机联网。但由于工业以太网的出现，其环境的适应性、通信的实时性及信息的安全性都有极大进步，已使它也可用于 PLC 间的链接数据及与分布设备间的 I/O 数据的实时交换，以至于进一步发展还可用于安全与运动控制。如 AB 公司等开发的 EtherNet/IP/西门子公司等开发的 Profinet 及三菱公司等开发的 CC-Link IE 等工业以太网就已经或即将实现这些目标。人们盼望已久的“一（E，EtherNet）网到底”或“一（E，EtherNet）网打尽”的局面开始显现。为此，本章先对以太网的有关发展及其技术优势做介绍，接着介绍上述 3 种工业以太网。

本书对上述网络的介绍都是先简要介绍其组成、协议、机理、结构及特点，进而结合有关厂家的产品介绍一些典型的配置实例。对具体网络的叙述，本书则在一般概括与具体介绍两个方面做了努力。前者是为了能全面理解这些网络的结构与特点，把握 PLC 网络系统的全貌，便于通过对比组建网络。后者是为了能分类了解这些网络的应用与使用，弄清 PLC 网络组态的思路，便于按照步骤设置好网络。

相比已有介绍 PLC 网络的专著，像本书这样抓住 PLC 网络的当今主流，把握 PLC 网络的发展趋势，从网络机理到应用配置做系统说明，对各个品牌 PLC 网络做全面介绍，似乎还未曾有过。这里的主流、趋势、系统、全面也正是本书追求的目标。

但毕竟网络配置的细节很多，特别是网络具体产品的类型、型号、版本、规格及安装的细节很多，还有网络的测试及排故障的内容更多，由于本书篇幅有限，实难一一顾及。何况 PLC 网络还在发展，很多新技术也很难一一概括。加上本人水平、精力及条件所限，书中不足之处，以至于存在差错也在所难免。在此，望广大读者不吝赐教！本人将诚恳采纳大家的意见，向着本书追求的目标，把本书修改好，以使其成为您进行 PLC 网络系统配置的好向导。

本书涉及了各种 PLC 网络协议及各厂家的 PLC。使用术语相同，但含义可能不完全一样，还可能用不同的术语，但含义却是相同的。所以，建议读者阅读时多加留意，从实质上去理解就好处理了。

宋伯生 2010 年 12 月 于沈阳

目 录

前言

绪论 1

第 1 章 PLC 网络基础知识 13

1.1 PLC 网络物理连接 13

1.1.1 网络通信媒体 13

1.1.2 网络通信组件 19

1.1.3 网络拓扑结构 21

1.2 PLC 网络通信技术 24

1.2.1 通信方式 24

1.2.2 通信数据 27

1.2.3 数字传输 30

1.2.4 模拟传输 34

1.2.5 通道复用 37

1.3 网络结构模型与相应协议 39

1.3.1 OSI/RM 模型与相应协议 40

1.3.2 TCP/IP 模型与相应协议 45

1.3.3 企业网络模型 47

1.4 计算机局部网络与 PLC 网络

协议标准 48

1.4.1 计算机局部网络标准 48

1.4.2 PLC 网络行业标准 57

1.4.3 PLC 网络事实标准 61

1.5 PLC 网络及其配置 65

1.5.1 PLC 网络概况 65

1.5.2 PLC 网络特点 76

1.5.3 PLC 网络配置 78

1.6 PLC 网络通信实现 80

1.6.1 自动通信 80

1.6.2 对话通信 83

1.6.3 专用软件通信 84

1.6.4 互联网通信 86

1.6.5 利用公网通信 87

第 2 章 PLC 串口网络配置 88

2.1 计算机标准串口 88

2.1.1 RS-232C 接口 88

2.1.2 RS-422A 接口 92

2.1.3 RS-485 接口 92

2.1.4 USB 口 93

2.1.5 IEEE1394 口 95

2.1.6 通信口转换 95

2.1.7 串口设定 97

2.2 LM 机串口网络 97

2.2.1 LM 机串口配置 97

2.2.2 LM 机串口功能 99

2.2.3 LM 机串口设置 99

2.2.4 LM 机串口连网配置实例 99

2.3 OMRON PLC 串口网络 100

2.3.1 OMRON PLC 串口配置 100

2.3.2 OMRON PLC 串口功能 105

2.3.3 OMRON PLC 串口设置 108

2.3.4 OMRON PLC 串口连网实例 111

2.4 西门子 PLC 串口网络 115

2.4.1 西门子 PLC 串口配置 115

2.4.2 西门子串口通信协议 119

2.4.3 西门子 PLC 串口网络设定 121

2.4.4 西门子 PLC 串口网络配置实例 127

2.5 三菱 PLC 串口网络 129

2.5.1 三菱 PLC 串口配置 130

2.5.2 三菱 PLC 串口功能 131

2.5.3 三菱 PLC 串口设定 132

2.5.4 三菱 PLC 串口使用实例 133

第 3 章 PLC 设备网及其配置 136

3.1 PLC 设备网概述 136

3.1.1 PLC 远程 I/O 网 136

3.1.2 现场总线 138

3.1.3 PLC 设备网 141

3.2 AS-i 142

3.2.1 AS-i 简介 142

3.2.2 西门子 PLC AS-i 网络组件 149

3.2.3 西门子 PLC AS-i 网络配置 实例 156

3.2.4 三菱 PLC AS-i 网络及其配置 实例 159

3.3 CC-Link/LT	168	4.5.4 其他 PLC 公司 Profibus 组件	320
3.3.1 CC-Link/LT 简介	169	第 5 章 PLC 信息网配置	326
3.3.2 三菱 CC-Link/LT 组件	172	5.1 以太网发展	326
3.3.3 三菱 CC-Link/LT 配置过程及 实例	180	5.1.1 传统以太网	326
3.4 CompoNet	185	5.1.2 快速以太网	327
3.4.1 CompoNet 简介	185	5.1.3 交换以太网	330
3.4.2 OMRON CompoNet 组件	191	5.1.4 工业以太网	335
3.4.3 OMRON CompoNet 配置实例	196	5.1.5 PLC 以太网	337
第 4 章 PLC 控制网配置	201	5.2 和利时 PLC 以太网配置	338
4.1 PLC 控制网概述	201	5.2.1 LM 机以太网模块特性	338
4.1.1 专用 PLC 控制网	201	5.2.2 LM 机以太网模块功能	339
4.1.2 基于标准的 PLC 控制网	203	5.2.3 LM 机以太网设置	340
4.2 CC-Link	203	5.2.4 LM 机以太网使用实例	342
4.2.1 CC-Link 简介	204	5.3 AB PLC 以太网配置	342
4.2.2 三菱 CC-Link 组件	215	5.3.1 Ethernet/IP 简介	343
4.2.3 三菱 CC-Link 配置实例	219	5.3.2 AB 以太网组件	345
4.3 DeviceNet	230	5.3.3 AB 以太网配置实例	347
4.3.1 DeviceNet 简介	230	5.4 OMRON PLC 以太网配置	354
4.3.2 AB DeviceNet 组件及配置实例 ..	237	5.4.1 以太网组件	354
4.3.3 OMRON DeviceNet 组件及配置 实例	248	5.4.2 以太网功能	357
4.3.4 三菱 DeviceNet 组件及配置 实例	255	5.4.3 以太网设置	362
4.4 ControlNet	256	5.4.4 以太网配置实例	368
4.4.1 ControlNet 简介	256	5.5 西门子 PLC 以太网配置	371
4.4.2 AB ControlNet 组件及配置实例 ..	264	5.5.1 Profinet 简介	371
4.4.3 OMRON Controller Link	277	5.5.2 西门子以太网组件	378
4.5 Profibus	293	5.5.3 西门子 PLC 以太网配置实例	382
4.5.1 Profibus 简介	294	5.6 三菱 PLC 以太网配置	400
4.5.2 西门子 PLC Profibus 组件及配置 实例	298	5.6.1 CC-Link/IE 简介	400
4.5.3 和利时 PLC Profibus 组件及配置 实例	316	5.6.2 三菱 CC-Link IE 组件及配置 实例	405
		5.6.3 三菱信息网组件及其配置实例 ..	410
		参考文献	414
		后记	415

绪 论

1. PLC 网络概念

PLC 网络是指分布在不同地理位置上、各自独立工作的 PLC、计算机或现场设备，通过通信组件与通信介质进行物理连接，并在网络软件及通信程序管理与协调下，实现数据通信、信息交流的集成系统。PLC 网络是计算机、PLC、现场设备及现代通信技术发展的产物，并随着这些技术的进步而日趋完善！与单一的 PLC 控制系统相比，它可实现更大规模、更广范围的实时控制，更全面、更精确的信息处理。同时，由于控制的网络化、分散化，控制出现故障的风险也将减少。

在 PLC 网络中，各个独立工作的 PLC、计算机或现场设备称为网络站点（node），简称站点或节点。

PLC 网络站点的多少，取决于网络的规模。多的有几十，甚至更多。少的只有几个、十几个，甚至于仅两个。如仅拥有两个站点的网络有时也称链接。

PLC 网络还可互连。指的是，通过专用的网络互连组件或同时连接在不同网络上的站点，使不同网络相互连接，从而实现不同网络站点之间的通信。互连后的网络是网络的网络，称互连网（也称互联网，internet 或 inter network 或 interconnection network），其实质也是网络。

这里对 PLC 网络的界定强调了它是“集成系统”。也就是由一些单一的系统所集成。显然比前者要复杂得多。具体讲，构成 PLC 网络有 3 个要点：

（1）应有物理连接

目的是在站点间建立通信通道。为此要做到：

1) 要选用好通信媒体或介质。通信介质可以有线的，如电缆、光缆；也可以是无线的，如无线电波、光波、红外线。类型很多，到底选用什么介质，则与网络的站点最大距离、网络站点数目、分布情况以及工作要求及环境有关。

2) 要选用好网络组件，主要是配置与使用好网络模块或相应接口。以便使用它通过通信介质实现站点间的物理连接。

对计算机，如串口连网，可使用串口或 USB 口；如果接入其他类型的 PLC 网络，那就要插入相应的网卡。

对 PLC，如串口连网，可使用 CPU 单元上的外设口、串口或 USB 口，也可用串口模块；如果连接其他类型的网络，那就要配置相应的网络插件或模块。

对现场设备，如串口连网，可使用串口或 USB 口；如果要连接其他类型的网络，那就要配置相应的专用网络接口。

当网络站点之间的距离很大时，为确保数据正确传输，需增设相关通信组件，以进行信号放大或数据中转。而为了网络互连，则还要有相应的网络组件。

（2）应有数据通信

目的是进行站点间信息交流。

对于 PLC 网络,信息主要有两个方面:一是状态信息,它包含自身工作及控制对象工作的状况;二是命令信息,它包含通信命令发送、应答及工作命令下达。

状态信息交流可使各个 PLC 站点的控制得以协调,进而提高控制能力。同时,状态信息,特别是所收集的对象状态信息,还可上传,为企业的信息管理提供原始数据。

命令信息的传送及应答,是各站点相互操作的需要。这也是 PLC 网络所特有的。如 PLC 控制变频器的输出频率就可用传送命令信息实现。再如计算机控制 PLC 工作,或 PLC 主站控制其从站工作,用的也是命令信息。

数据通信进行信息交流要做到以下两点:

1) 要有网络管理软件,以进行网络配置与管理。对 PLC 网络,PLC 厂家的编程软件多可进行这个配置与管理。如站点编址、通信参数设定、使用数据区指定等。此工作也称为网络组态或设置(定),是使用网络必须做好的工作。此外,有的厂家也还提供有专门网络管理软件,也可用以对网络的组态及管理。

2) 要有通信程序,以进行通信数据的准备、传送、接收、处理及使用,进而达到交流信息、传送命令的目的。对 PLC 网络,这个程序必须由用户编写,要依据控制进程以及交流信息的需要编写。

(3) 应有 PLC 站点

PLC 应该是网络的核心。

PLC 网络的数据通信主要是在 PLC 与计算机、PLC 与 PLC 以及 PLC 与现场设备间进行。在这 3 种通信中,唯一不能缺少的就是 PLC。显然,如果网络中没有 PLC,只有计算机,那只是计算机网络。如果连计算机都没有,那可能是电信或电视网络。

各站点都能独立工作也是必要的。计算机、PLC 独立工作比较好理解。而这里的现场设备则强调要有智能,即不仅要有通信接口,还要有简单的控制功能。否则,只是 PLC 的远程 I/O 系统,与计算机与打印机之类的设备连网一样,虽也是网络,但从控制风险分散的角度看,似乎不是真正意义上的网络。真正意义上的网络,应保证即使网络数据通信瘫痪,但由于各站点都能独立工作,都可实施自身简单的控制,还可确保系统工作的安全。

总之,物理连接、数据通信及有独立工作的 PLC 站点是 PLC 网络的 3 个要点。缺少其中一个都不能称为 PLC 网络。

2. PLC 网络类型

PLC 网络的类型是很多的,可以说是一个 PLC 公司一个样。而且相互多不兼容。有的即使是同一公司的网络,但网络类型不同,PLC 机型不同,网络也不完全相同,也不兼容。这也是 PLC 网络的悲哀!当然,事情也在变化。由于 PLC 网络标准化的推进,各 PLC 厂家的网络,已逐渐向若干公认的标准靠近。有的厂家还生产有可接入这些公认网络的模块。有了它,也可使自身的 PLC 接入这些公认网络。

尽管 PLC 网络千差万别,但还是可从实现功能及站点角色上对其作分类说明。

(1) 从网络功能角度分类

1) 设备网(Field),也称现场网络,有的称现场通信网或现场总线(有的也把一些控制网归类到现场总线中)。主要用于 PLC 与现场设备及传感器/执行器之间的通信,以实现 PLC 对现场设备及智能装置的数据采集与工作控制。有了设备网,可以减少硬接线,减少安装时间及安装费用。同时,还便于实施对现场及现场设备实时诊断。

设备网处于企业网络的下层，交换数据量小。但通信的可靠性、实时性要求高。即使短时间的数据交换停止，将影响 PLC 控制功能的实现。

2) 控制网 (Control)，相当于车间级或生产线级的网络，有的称为数据及现场通信网，主要用于 PLC 间的连网、通信，以实现 PLC 对多台设备或生产线控制的协调，以扩大 PLC 的控制范围，增强 PLC 的控制能力。

控制网处于企业网络的中层。它交换数据量也不大，但通信的可靠性、实时性要求也很高。一般讲，即使短时间的数据交换停止也是不允许的。

3) 信息网 (Information)，也就是企业级网络，有的称为数据通信网，主要用于 PLC 与计算机连网通信。以使 PLC 与计算机或计算机与计算机交换信息、传达命令，以实现企业的供、产、销的信息共享，及人、财、物的资源管理。在此，PLC 起到对生产一线的数据采集、上传，管理命令下达等不可代替的作用。

信息网也是企业的局域网，是小范围的网络，覆盖范围可在十几千米以内，结构简单，布线容易。但它处于企业网络的上层，其通信的数据量大，要求通信的速度高。但通信的实时性要求可低些。即使较长时间停止数据交换也是允许的。

这 3 层网络还可互连。其办法是有的站点有两个通信接口。分别与不同层的网络相连。由于有这样网络互连，可很容易把工厂底层的信息上传到信息层；或把信息层的命令下达到现场。

要指出的是，这样划分也是相对与变化发展的。如控制网，虽主要用在 PLC 之间的通信、交换数据，但也可在计算机与 PLC 以及 I/O 设备与 PLC 之间通信、交换数据。再如信息网，情况也类似。特别是随着以太网技术的应用以及以太网技术的进步，除了以太网自身的网速高、组网简单、成本低廉、软件丰富、互连容易、使用方便、应用广泛这些固有的优点外，它在工业应用中的环境适应性、组装方便性、工作可靠性、信息安全性以及通信实时性也都有很大长进。因而已出现“e 网包打天下”的局面。极有这可能，在未来 PLC 的 3 种网络中，都使用以太网。果真那样，也许 PLC 的组网将会变得更简单、更方便与更低廉，其应用也更广泛、更普及与更有效。那将是控制自动化、信息化、网络化发展的幸事！

(2) 从站点角色分工分类

1) 主从网 (Master/Slave, M/S)。在这样网络中，多数站点为从站，只有一个或个别几个站为主站。主站管理从站，并发起通信。而从站则接受管理，响应通信。PLC 网络大多数为此类网络。如 Profibus-DP 网，就有主站、从站之分。

主、从网较复杂，在组网时，要进行相应组态或设定。但是它较易实现集中管理与监控，安全性高，较适合作为控制网与设备网。

2) 客户机、服务器网 (Client/Server, C/S)。在这种网络中，多数站点为客户机 (Client)，只有一个或个别几个站为服务器。

计算机网络很多是这样系统。这里的服务器 (Server) 一般为高性能的计算机。客户机一般是指普通计算机，也可称网络工作站。服务器运行网络操作系统，进行网络管理，提供共享资源。处理各个网络工作站的服务请求。如访问服务器硬盘上的文件系统、申请共享打印服务等。客户机，也即网络工作站，是用户使用网络的接口，也是用户工作的平台。它接受网络服务器管理与服务，共享网络的资源。

PLC 网络的 C/S 系统，服务器则多为 PLC，用以采集数据，而计算机则可能是工作站，

用以访问 PLC，读取数据。将要介绍的 SCADA 系统就是这么处理的。

3) 网站 (网页)、浏览器网 (Browser/Server, B/S)。将要提到的因特网就是这样的网络。在这种网络上，有无限多的站点。但这些站点大致可分为两类：一类是提供服务的，另一类是接受服务的。前者设有网址，以网页的形式提供数据、画面或多媒体数据，供后者访问。后者使用通用的浏览器，通过登录访问前者，接收前者服务。

PLC 网络的 B/S 系统，服务器也多为 PLC。这时，PLC 要有可以提供生成网页的以太网模块。用它可建立 PLC 实时数据网页，以让计算机通过浏览器访问。这比用 SCADA 更为简便，成本也较低。只是由于 B/S 产品人机交互界面比较差，远程打印瓶颈问题，还有报表设计问题，安全问题、接入速度问题等等，制约了 B/S 产品的普及。

4) 对等网。在这种网络中，各个站点不分主次。每个站点都可以对等地与其他站点通信。此类网络比较简单，组网方式灵活方便。著名的以太网就是对等网。PLC 串口自由协议通信，通信双方也是对等的。

在对等网中，各方都可共享彼此的信息资源和硬件资源。但是它较难实现集中管理与监控，安全性也低。

5) 链接网。使用各个站点间指定数据区共享、运用数据链接自动通信。在通信时，各个站点也是对等的。但与对等网不同的是，它要通过网络设定，指定有一个管理主站，以实施对网络管理。

(3) 从网络覆盖范围分类

如仅考虑计算机站点构成的网络，其覆盖范围相差很大，类型很多。最小的是个人网络，仅供一个人使用。例如，通过无线网络，将一台计算机与它的鼠标、键盘和打印机连接起来，就是这样的网络。最大的可以覆盖整个地球，可供全球人员使用。例如因特网。表 0-1 所示为站点之间距离、所处位置及网络例子。但是，PLC 网络覆盖范围变化不大。

表 0-1 计算机网络的不同覆盖范围

站点之间的距离	站点所在的位置	例子
1m	1m 见方的范围内	个人区域网
10m	同一房间	局域网
100m	同一建筑物内	
1km	同一校园	
10km	同一城市	城域网
100km	同一国家	} 广域网
1000km	同一个洲	
10000km	同一个行星	Internet

1) 广域网 (Wide Area Network)。可覆盖一个省、几个省、一个国家或几个国家的计算机网络。PLC 无此网络，但可接入此网络。

2) 城域网 (Metropolitan Area Network)。可覆盖一个城市的计算机网络。目前，我国许多城市已建立或正在建立这样的网络。PLC 多无此网络，但也可接入此网络。如特殊情况需要，也可建立此网络。例如，笔者曾参与编程的，山东威海市自来水公司组建的调度中心计算机，通过串口无线 Modem 与多个水站的西门子 S7-200PLC (其串口也连接无线 Modem)，

通过无线信道连网就是一例。该网覆盖的地域就是整个威海市，也是典型的城域网。

以上两个网络可以是公用的，公众付费即可使用这个网络。也可是专用的，如金融网络，虽也是城域网、广域网，但并不是任何计算机用户都可以接入。

显然，如果采集现场数据的 PLC 与读取 PLC 所采集的数据计算机都接入此公用网，也就可实现计算机对 PLC 数据的远程读取，实际也就是 PLC 的广域网或城域网。

3) 局域网 (Local Area Network)。覆盖地域不大的网络。以上介绍的企业信息网即为此网络。PLC 常要接入此网络。

4) 因特网 (Internet, 这里字母 i 是大写!)。是互联网 (internet) 的一种，指世界范围互联网，也是最大的广域网。其前身是 1969 年诞生在美国的阿帕网 (ARPANET)。它用 TCP/IP 网络协议将各种不同类型、不同规模、位于不同地理位置的计算机网络连接成一个整体，提供有万维网、文件传输、电子邮件、远程登录等服务。而万维网则是它的最重要的应用。PLC 也常要接入此网络。

这里的所谓万维网，是指环球信息网 (World Wide Web, WWW)，简称 3W，有时也叫 Web，是欧洲粒子物理实验室 (CERN) 于 1989 年研制的。它创建了超文本 (hypertext) 标记语言 (HTML)，使用“超级链接”，把因特网上的所有信息，如图像、动画、声音、3D 世界等，连接在一起，形成巨大的分布资源，使得任何连接因特网的用户都可通过 Web 浏览器，访问这些资源，共享这些信息。

文件传输、电子邮件是人们上网很常见的使用。至于远程登录，是指通过因特网，允许一个用户登录到一个远程计算机系统中，就好像用户端直接与远程计算机相连一样。一般人使用不多。

提示：习惯上往往把因特网、万维网统称为互联网。

5) 接入网 (Access Network)。是指计算机或局域网到因特网之间的中介。一般由因特网服务商 (ISP) 提供。ISP 提供的接入网有 3 种：

① 电话网络接入。低速的可以用调制解调器 (Modem) 拨号入网；高速的可用 ADSL 宽带入网。

② 有线电视网络 (混合光纤电缆系统, HFC) 接入。用 Cable Modem 入网。由于有线电视的普及，这种接入目前已用得很多。

③ 移动网络。计算机使用无线网卡，通过 ISP 供应商提供的账号接入因特网。这为笔记本电脑用户提供了很大方便。只是这样的 ISP 是很多的。也是多层次的。最高层次的 ISP 才拥有专用通信通道直接接入因特网。

当配置以太网模块或接口的 PLC 接入因特网后，也可设置网址，供用户远程访问。有的还可制成网页，用户利用浏览器即可直接读取 PLC 的数据。这样，就可以使 PLC 控制的状态信息传递到世界的任何可接入因特网的地方。也可从世界任何可接入因特网的地方得到 PLC 所需要的命令信息。PLC 控制再也不是信息的孤岛了。这对实现控制信息化、网络化、远程化，提高 PLC 控制效益提供了很大的方便。

(4) 从网络传输介质分类

1) 有线网络。网络站点之间的物理连接均使用电缆或光缆这样的有线传输介质，是最常见的，也是最常用的 PLC 网络。

2) 无线网络。网络站点之间的物理连接不完全使用有线传输介质，还使用电磁波、光

波、红外线这样的传输介质。

计算机的无线网络类型很多。小的如系统无线连网，它用蓝牙技术实现计算机组件之间的连接，如键盘、鼠标与主板连接。大的有无线局域网（WLAN），这种网络的每个站点都用一个无线调制解调器及通信天线做物理连接，进而实现相互通信。更大的也可使用基于基站（基站间用有线通信）的移动通信以组成广域网，这是因为移动通信早已从模拟通信发展为数字通信，所以它除了传送语音，也可用于数据交换。此外，还可利用无线路由器，或移动网络接入因特网，其通信范围将不受限制。

无线网络接线简单，站点还可移动，网络站点接入、退出灵活，为它的广泛使用提供了很大方便，目前在 PLC 网络中也已用得越来越多。

3. PLC 网络功能

PLC 网络功能是实现 PLC 与 PLC、计算机（还有人机界面）及现场设备之间通信。而通信则各有其目的。

（1）PLC 与计算机、人机界面通信的目的

1) 实现 PLC 编程及程序调试。这也是 PLC 与计算机通信的最基本目的。PLC 编程是较麻烦的。若用手持编程器，通过助记符编程则更麻烦。但若用计算机与 PLC 连网，再使用相应编程软件，则可使用梯形图或流程图语言编程，甚至于还可使用其他高级语言编程，较为方便。

而且用计算机编程，还可对所编的程序进行语法检查，以便于发现与查找程序中的语法错误。同时，还可进行程序仿真，可对输入点的状态进行强制置位或复位，可模拟现场情况，进而可发现与解决程序中语义方面的问题。

此外，计算机编程还可存储、打印 PLC 程序，或把程序写入 ROM 中等，便于 PLC 程序的移植及重用。

所以与计算机连网进行 PLC 编程已是一个趋势。有的厂家高级的 PLC 编程器，实质就是笔记本式个人计算机。

2) 实现计算机控制系统的监控与数据采集 SCADA（Supervisory Control and Data Acquisition）。具体是：

① 读取 PLC 工作状态及 PLC 所控制的 I/O 点及内部数据的状态，并显示在计算机的屏幕上，以便于人们了解 PLC 及所控制设备的工作状态。

② 通过向 PLC 写数据，改变 PLC 所控制的设备工作状态，或改变 PLC 的工作模式，实现人们对控制的必要干预。

③ 读取由 PLC 所采集的数据，并进行处理、存储、显示及打印，便于人们使用。

3) 实现人机界面的监控及管理。人机界面（HumanMachineInterface）实质是工业现场用的简易计算机。具有信息处理、数据录入、采集及显示功能。近来已用得越来越多。

它与 PLC 连网通信，可从 PLC 读取数据，并予以显示。也可向它写数据，再传输给 PLC，改变 PLC 的状态或数据，实现对 PLC 或系统的控制。

虽然它的功能不如计算机，但它的体积小、工作可靠，可安装在工业现场。所以用起来是很方便的。在一定程度上也可起到计算机的 SCADA 作用。

4) 实现远程诊断与维护。有的 PLC 配备有远程诊断与维护系统。可通过连网，甚至互连网，利用厂家提供的通信模块与专用软件，实施远程数据采集与故障诊断，并实施相应维

护，如下载新版本的 CPU 操作系统及有关硬件驱动等。

(2) PLC 与 PLC 的通信目的

1) 扩大控制地域及增大控制规模。PLC 多安装于工业现场，用于当地控制。但如果进行连网通信，则可实现远程控制。距离近的可以为几十、几百米，远的可达几千米或更远，可大大扩大 PLC 的控制地域。

连网后还可增加 PLC 控制的 I/O 点数。这里，尽管每台 PLC 控制的 I/O 点数不变（有的 PLC 加远程单元后，也可增加 I/O 点数），但由于连网后，为多台 PLC 参与控制。其控制总点数为参与连网的 PLC 控制点数之和。显然，其控制的规模要比单个 PLC 的规模大。

不少事实说明，两个或若干个中、小型 PLC 连网，也可达到一个大型机的控制规模，而费用则比大型机要低得多。因而用中、小型 PLC 连网，去替代大型 PLC，已成为一个趋势。

2) 实现系统的综合及协调控制。用 PLC 实现对单个设备的控制是很方便的。但如果有若干个设备要协调工作，用 PLC 控制，较好的办法是连网通信。单个设备各由各自的 PLC 控制，而设备间的工作协调，则依靠连网通信后 PLC 间的数据交换解决。

这样连网通信，可使 PLC 控制，从设备一级提升到对生产线一级。便于实现工厂的综合自动化。

3) 提高 PLC 工作的可靠性。连网通信后各 PLC 还是独立工作的。只要协调好，即使个别站点出现故障，并不影响其他站工作，更不至于全局瘫痪。故可降低系统的故障风险。

4) 连网通信更便于实现冗余配置。工作 PLC 与热备用 PLC 使用连网通信处理转换，用起来非常方便，系统也非常可靠。是当今冗余配置的一个趋势。

(3) PLC 与现场设备通信目的

1) 简化系统布线。工业现场的普通开关量及模拟量输入、输出信号，都是通过信号线与 PLC 的 I/O 点相连。连线很多，布线也很复杂。特别是一些远离 PLC 的输入、输出点多时，则更为复杂。而如果用连网通信传送输入、输出信号，则简单得多。因为通信线仅用两根或几根，就可传送很多输入、输出信号。尽管这样处理有一定延时，但由于网络传送及信号处理速度的不断提高，这点时延，对一般的控制过程是不会有影响的。

2) 便于系统维修。输入、输出信号用连网通信处理，布线简单了。这既可节省硬件开销，还便于系统维修。可以设想，在一大堆的输入、输出接线中，真有个别出现问题，在现场查找是很不易的。

3) 实施对现场设备的管理。目前很多现场设备都有自身的 CPU、内存及通信接口。自身可采集、处理或使用数据。但是，如果没有连网通信，它们还只是“信息孤岛”。无法与其他控制协调，或实现信息共享。而如果与 PLC 连网通信，则将可使这些装置不再是“信息孤岛”了。

特别要强调的是，信息化已是当今信息社会的潮流。已给世界带来了巨大的社会效益与经济效益。而企业的信息化，推行企业资源计划（ERP）、信息执行系统（MES），甚至于产品生命周期计划（PLM），更是给企业带来了不可估量的效益。

而企业信息化的基础是准确的生产一线数据。PLC 连网通信后，这些数据可自动采集，

避免了人为干扰，因而是客观的、准确的，而且是完整的、及时的。这就为建立智能工厂、透明工厂、全集成系统或 e 自动化等的成功提供了基础。

总之，从根本上讲，PLC 连网通信主要是用好信息技术。目的是协调控制，进而实现系统控制的自动化、网络化、远程化、信息化、智能化。

4. PLC 网络性能

PLC 网络是用于站点间数据通信的。为此，要求这个通信做到速度快、实时性好、可靠性高、出错率低、传输数据量大。同时，网络还要便于使用、维护。而且建网及使用的费用要低廉。为了反映网络的这些特性，可以使用一些指标予以衡量。这些指标也是人们对 PLC 网络的配置与使用的要求。这些指标主要是：

(1) 网络规模

指的是网络可连接的最多站点数。PLC 网络站点少的仅 2、3 个，多的有 8、16、32、64、128 个不等。功能强的网络，最多站点数也将多些。

网络规模还要看网络互连的情况。网络互连得多，网络规模也大。

(2) 网络覆盖

指网络中站点间最大的距离。PLC 网络最大站点间距离差别很大。小的几米、十几米，甚至也可能同在一个电气柜内。大的可以是几百米、几千米，甚至几十千米。功能强的通信媒体使用光纤的站点间的距离则大些。

PLC 网络规模及覆盖比起计算机网络要小得多。不大可能有什么城域网、广域网。即使企业级的 PLC 网络，主要也是用以实现 PLC 与计算机信息交流。纯 PLC 站点的网络最多也只是车间级的。

(3) 帧的大小

帧是网络数据传送的单位。一般以二进制位或一个字符计。这里“帧的大小”是指，一个帧的最大二进制位数或字符数（两者都是以字节计）。这个指标与网络的性能有关。性能强的网络，帧的最大字节数多，如几 K 字节。性能差的网络，有的只有几十字节或 100 多个字节。

由于帧的大小是受限制的。所以如果一次要传送的数据（即报文），很大，一般要把它分解成若干个帧，按帧分别传送。

(4) 网络速度

指网络数据信号发送或接收的速率。常用的有两个指标：一是比特率，又称为信息速率，简称数据率。比特是二进制数的一个位。比特率 S 是指每秒平均传输比特的个数，其单位是每秒位（bit/s），或每秒千位（kbit/s），或每秒兆位（Mbit/s）。

二是信号码元（信号波形）传输速率，即波特率。指每秒可传送的波形数量。信号波形是承载信息的基本信号单位，也是信号编码的单位。波特率 B 与波形持续的周期 T 有关。两者互为倒数。

比特率和波特率及其携带的信息量有关。其关系可以按下式计算：

$$S = B \log_2 n$$

这里， n 代表信号波形中包含的信息量，即波形可反映多少数值有关。如为 2，即仅反映 0、1 两种状态，则 S 与 B 完全相等。如为 4，可反映 00、01、10、11 等 4 种状态，则 $S = 2B$ 。多数 PLC 网络信号波形的信息量为 2，所以，波特率与比特率总是相等的。

波特率也可比比特率大。如 10M 以太网, 其比特率为数据率为 10Mbit/s。但它使用曼彻斯特编码。这意味着发送的每一位要有两个信号周期。所以, 其码元传输速率即为波特率, 是数据率的两倍, 即 20M 波特。

网络速率有时也用带宽 (bandwidth) 表示。带宽本是模拟信号通信线路传输能力的术语, 指传输信号所包含成分的频率范围。如电话线路, 可传输话音信号, 其范围为 3.1Hz (从 3.1 ~ 3.4Hz)。当今, 也用它近似代表通道传输数字信号的最高速率。因为带宽的下限是很小的。带宽的单位与比特率相同。

(5) 通信时延 (delay 或 latency)

通信时延指一个帧的数据从网络的一个站点传输到另一个站点所需的时间。由发送时延、传输时延及处理时延三部分组成。

发送时延指发送站点把一个帧数据发送进入传输媒体所需要的时间。它与帧大小及信号发送速率 (transmission 或 transmit) 有关。即

$$\text{发送时延} = \frac{\text{帧大小}}{\text{信号发送速率}}$$

传输时延指信号在介质上的传输时延, 与信号在传输介质上的传输速率 (propagation 或 propagate) 及信道长度有关。即

$$\text{传输时延} = \frac{\text{信道长度}}{\text{信号传输速率}}$$

信号传输速率与介质的特性有关。如在粗同轴电缆上传播, 约为 200m/μs (相当于光在真空中传播速度的 2/3)。

处理时延指通信站点或网络组件处理通信数据所需的时间。与站点或组件特性及数据的多少有关。但不好量化计算。

PLC 网络时延不能太长。特别是它的设备网与控制网, 只能以 ms (毫秒) 计, 否则将影响控制的及时性。进而也将影响控制精确度。

还有一个指标叫抖动, 指数据报 (帧) 之间延时差异。当然这个值应尽可能小为好。

(6) 通信质量

通信质量一般用差错率, 也即误码率衡量。其值为

$$\text{误码率 (Pe)} = (\text{接收方出现差错的码元数 (位数)} / \text{总的传输码元数 (位数)}) \times 100\%$$

误码率是一个统计平均值, 在统计和测试时应采用统计学的方法, 在足够时间和足够统计的数量后方可正确得出。

计算机网络通信系统中, 要求误码率低于 10^{-6} 。如果实际传输的不是二进制信号, 需折合成二进制信号计算。PLC 控制与设备网络要求误码率更小。一般讲, 任何出现误码都是不允许的。或一旦出现误码, 也要有相应的应对措施。

(7) 网络可靠性

可用可靠度衡量。即

$$\text{可靠度} = \frac{\text{全年 (或全月) 正常工作时间}}{\text{全年 (或全月) 总工作时间}} \times 100\%$$

影响可靠度的因素很多, 主要是网络的软、硬件可靠性及操作人员的水平。

PLC 网络的可靠性还可用 RAS, 即 Reliability (可靠性)、Availability (有效性)、Serviceability (可维护性) 衡量, 并设定有响应的评价指标。

(8) 通信安全

主要指数据的安全。要有必要的措施, 确保数据不能被无关人员盗用, 也不能让黑客入侵。

(9) 网络兼容

网络兼容也是必要的。目前, PLC 网络的兼容性很差。随着技术的发展及协调, 这个不兼容的局面必然会有所改变的。

(10) 网络经济性

指组建网络与使用、维修网络的费用。在其他性能相同或相近似, 应选择此费用尽可能低的解决方案。

网络经济性还有一个指标是带宽的利用率。带宽是指在一个信道上用于传输信息的可用频率范围。它是用来表示信道传输能力的指标。因此带宽越宽, 电路能够传输的信息量就越大。带宽的单位一般用频率使用的单位, 即 Hz 或 MHz; 也可用传输速率的单位比特率, 即 bit/s; 如果频率很高, 如传输媒体用光纤, 也有用波长 (光速/频率), 即 km 来表示的。

可以用带宽利用率衡量。利用率可用下式计算:

$$\eta = \frac{R_b}{B}$$

式中 R_b ——比特率 (bit/s);

B ——信道的带宽。

η 值大, 说明带宽得到充分的利用。因而, 也可获得更大的经济效益。

5. PLC 网络发展

如果说计算机网络是计算机技术进步与通信技术发展相结合的成果。那么, PLC 网络则是随着 PLC 技术的进步及计算机网络的发展而快速发展与逐步成熟起来的。

最初, 与计算机一样, PLC 也没有网络。只有外设接口连接手持编程器, 以编写、调试 PLC 程序, 以及进行人机交互。

进一步发展, 出现了图形编程器, 显示屏尺寸加大, 可用梯形图符号进行 PLC 编程。有的 PLC 的图形编程器实质就是当今的笔记本电脑。因而运用它, 实际上就是计算机与 PLC 的链接。也许这就是 PLC 最初形态 PLC 与计算机连网。

再进一步发展是由于个人电脑价格大幅度降低及广泛应用, 致使 PLC 编程几乎都是使用个人电脑加 PLC 编程软件。也就是说, PLC 与计算机的链接是很平常的事。

为了实现远程控制。PLC 还发展有远程单元。有远程主单元及远程从单元。主单元放置在当地的机架上, 接受 PLC CPU 的管理。从单元放置在远程机架上, 管理远程的 I/O 模块。

主、从单元通过通信介质实现物理相连, 并进行通信, 周期地交换远程 I/O 数据。把 CPU 对输出 (O) 的控制传送给远程输出模块, 同时, 把远程的输入模块的输入 (I) 传送给 CPU。这样, PLC CPU 处理远程 I/O 与处理当地 I/O 相比, 所不同的只是时间略有延时 (增加主、从模块间的通信时间)。

这样的远程控制, 可扩大 PLC 的控制地域范围, 还简化了 I/O 点的接线。对提供 PLC 的控制效能提到了重要作用。因此, 这样的 PLC 远程控制, 在 PLC 系统中至今仍然还在广泛应用。只是, 这样的远程的控制系统, 它的远程从站没有 CPU, 不能独立工作, 不是独

立站点。控制的风险要大些。而且严格说它只是分布控制系统，还不能算是网络。

这样远程系统的进一步发展，还出现了在从站中，也可接入小型 PLC 的情况。这也就出现 PLC 主、从控制网了。

以上可以说是 20 世纪 80 年代末期的情况。之后，各个 PLC 厂家都加快了 PLC 网络的开发，出现各种不同的 PLC 网络。

OMRON 有 Host Link 网（用于计算机与 PLC 通信）、PLC Link 网（用于 PLC 与 PLC 通信）、SYSMAC Link 网（用于 PLC 与计算机以及 PLC 通信）、SYSMAC NET 网（用于 PLC 与计算机以及 PLC 通信）、ComBoBus/S 及 ComBoBus/D 网（用于 PLC 与现场设备以及 PLC 通信）、ControlLink 网（用于 PLC 与计算机以及 PLC 通信）、以太网（用于 PLC 与计算机以及 PLC 通信）等。

西门子 S5 系列机网络且不论，S7 机除了可用 RS-485 串口建立 PPI 网、MPI 网进行一对一，或一对多的主从网络，还有 AS-i 网（用于设备层）、Profibus 网（用于控制层）、工业以太网（用于信息层）。

三菱 PLC 可用标准通信串口 RS-232C 口或 RS-485 口，进行 1:1 或 1:N 通信。此外还有 CC-Link 网、CC-Link/LT 网、MELSECNET/10、MELSECNET（II）、MELSECNET/B、MELSECNET/H、MELSECI/O-LINK、MELSECNETFX-PN 及以太网。

Allen-Bradley、GE 及施耐德等公司的 PLC 网络也很多。

可以说，20 世纪 90 年代，是 PLC 网络百花齐放，越来越多的年代。

进入 21 世纪，情况则有所变化。出现了 4 个特点：

1. PLC 网络兼容在进步

经过实际使用比较及商业竞争、优胜劣汰，加上 PLC 标准化的推进，在 PLC 网络中，性能低的、兼容性差的逐步被淘汰了。各厂家的网络开始趋同或出现兼容。特别是新推出的 PLC，网络类型都向主流网络靠近，以致与旧机型的网络都不兼容了。

以信息网为例，当今各 PLC 厂家都是使用工业以太网。先是用 10M 以太网，继而用 100M 以太网、1000M 以太网，甚至速度更快的以太网也都在研发中。尽管各家以太网的具体细节不完全相同，但物理连接上各家基本都是相同的。此外，也出现了几个公认的上层协议。

再以设备网及个别控制网为例，当今各个厂家 PLC 都向现场总线靠近。公认有 Profibus-DP、DeviceNet 及 CC-Link。几乎各个厂家新型的 PLC 都提供接入这些网络的接口。

只是多数厂家的控制网差别大些，不大好兼容。但有厂家也提供有可接入两种不同网络的接口产品。有的类似网关，一边接入一家网络，利用它的收、发转换，间接实现了不同控制网的互连；还有的类似接口转换器，可在不同的网络间进行转换。也许这将是 PLC 网络发展的亮点。

2. PLC 网络功能在加多

以常用的标准串口连网为例。早期 OMRON PLC 只能作为从站，被动地与计算机通信；后来由于开发了串口指令，不仅可主动发起与计算机通信，而且还可与其他 PLC 或现场设备通信；同时还可实现多台 PLC 间的链接通信，也具有原先 PLC Link 网的功能。西门子的 S7-200 机用 RS-485 口多站点连网，早期只能是一个主站，而今也可配置为多个主站。再如以太网，近期的不仅速度快了，功能也有所加多。有的还可实现网页的功能等。