



中华人民共和国国家标准

GB/T 38868—2020

工业控制网络通用技术要求 有线网络

Industrial control network general technical requirements—Wired networks

2020-07-21 发布

2021-02-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义、缩略语..... 1

4 概要 3

5 工业控制网络设备通信质量保障性要求 3

 5.1 EMC 要求 3

 5.2 通信协议一致性要求 3

 5.3 网络安装要求 3

6 工业控制网络通信性能要求 4

 6.1 概述 4

 6.2 端节点数 4

 6.3 基本网络拓扑 4

 6.4 网络组件数 4

 6.5 通信速率 4

 6.6 非实时带宽 4

 6.7 响应时间 5

 6.8 时间同步精度 5

 6.9 非基于时间的同步精度 5

 6.10 冗余恢复时间 5

7 工业控制网络功能要求 5

 7.1 运行维护要求 5

 7.2 管理要求 7

 7.3 服务保障要求 7

 7.4 安全要求 7

附录 A（资料性附录） 常用工业控制网络 9

附录 B（规范性附录） 工业控制网络设备常用 EMC 检测项要求及相关标准 10

附录 C（资料性附录） PROFINET 网络性能设计示例 12

附录 D（资料性附录） 工业控制信息安全标准 15

参考文献 16

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国机械工业联合会提出。

本标准由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本标准起草单位:机械工业仪器仪表综合技术经济研究所、中国科学院沈阳自动化研究所、浙江中控技术股份有限公司、上海自动化仪表股份有限公司、北京和利时系统工程有限公司、北京东土科技股份有限公司、上海工业自动化仪表研究院、工业和信息化部电信研究院、中电科技集团重庆声光电有限公司。

本标准主要起草人:谢素芬、刘丹、张思超、虞日跃、陆卫军、薛百华、李红词、赵勇、张茂成、段世惠、郑秋平、王洲、史宝库、徐大千。

工业控制网络通用技术要求 有线网络

1 范围

本标准规定了智能制造系统中有线工业控制网络及设备在工业现场环境下,关于通信质量、工业控制网络性能以及工业控制网络功能等方面的通用要求,包括:

- a) 通信质量保障性基本要求;
- b) 工业控制网络性能要求;
- c) 工业控制网络功能要求。

本标准适用于有线工业控制网络以及网络设备的制造商、系统集成商和用户。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 17626(所有部分) 电磁兼容 试验和测量技术

GB/T 20438(所有部分) 电气/电子/可编程电子安全相关系统的功能安全

GB/T 21109(所有部分) 过程工业领域安全仪表系统的功能安全

GB/T 26336—2010 工业通信网络 工业环境中的通信网络安装

ISO/IEC 8802-3 信息技术 系统间远程通信和信息交换 局域网和城域网 具体要求 第3部分:标准以太网(Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 3:Standard for ethernet)

IEC 61784-2 工业通信网络 行规 第2部分:基于ISO/IEC 8802-3的实时网络的附加现场总线行规(Industrial communication networks—Profiles—Part 2:Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3)

IEC 61784-5(所有部分) 工业通信网络 行规 第5部分:现场总线安装[Industrial communication networks—Profiles—Part 5:Installation of fieldbuses(all parts)]

3 术语和定义、缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

工业控制网络 industrial control network

连接工业控制系统设备的网络;不同的工业控制网络可以在一个车间中共存,也可以与车间外的远程设备和资源相连。

[IEC/PAS 62443-3:2008,定义 3.1.27]

3.1.2

现场总线 fieldbus

基于串行数据传输并用在工业自动化或过程控制应用中的通信系统。

[GB/T 20830—2015, 定义 3.1.17]

3.1.3

实时以太网 **real-time ethernet**

基于 ISO/IEC 8802-3 的包含实时通信的网络。

[IEC 61784-2:2019, 定义 3.1.21]

3.1.4

嵌入式系统 **embedded system**

置入应用对象内部起信息处理或控制作用的专用计算系统。

注 1: 嵌入式系统以应用为中心, 以计算技术为基础, 软件硬件可剪裁, 其硬件至少包含一个微控制器、微处理器或数字信号处理器单元。该系统能够满足应用系统对功能、可靠性、成本、体积、功耗等严格综合性的要求。

注 2: 改写 GB/T 22033—2017, 定义 2.001。

3.1.5

一致性 **conformance**

标准与实现之间的关系, 即标准中为真(true)的条款在实现中也为真(true)。

[IEC 62443-2-1:2010, 定义 3.1.10]

3.1.6

信息安全 **security**

- a) 保护系统所采取的措施。
- b) 由建立和维护保护系统的措施而产生的系统状态。
- c) 能够免于非授权访问和非授权或意外的变更、破坏或者损失的系统资源的状态。
- d) 基于计算机系统的能力, 能够提供充分的把握使非授权人员和系统既无法修改软件及其数据也无法访问系统功能, 却保证授权人员和系统不被阻止。
- e) 防止对工业自动化和控制系统的非法或有害的入侵, 或者干扰其正确和计划内的操作。

注: 措施可以是与物理信息安全(控制物理访问计算机的资产)或者逻辑信息安全(登录给定系统和应用的能力)相关的控制手段。

[GB/T 30976.1—2014, 定义 3.1.14]

3.1.7

功能安全 **functional safety**

与 EUC 和 EUC 控制系统有关的整体安全的组成部分, 它取决于 E/E/PE(电气/电子/可编程电子)安全相关系统, 以及其他技术安全相关系统和外部风险降低设施功能的正确行使。

[GB/T 20438.4—2017, 定义 3.1.9]

3.1.8

工业控制系统 **industrial control system**

由计算与工业控制主机、设备和装置组成的系统, 计算与工业控制主机、设备和装置集成到一起以控制工业生产、传输或分布式过程。

注: 在本标准中, ICS 表示一般意义上的自动化系统, 包括监视控制和数据采集(SCADA)。

[IEC/PAS 62443-3:2008, 定义 3.1.28]

3.2 缩略语

下列缩略语适用于本文件。

EMC 电磁兼容性(Electro Magnetic Compatibility)

EMI 电磁干扰(Electro Magnetic Interference)

EMS 电磁敏感性(Electro Magnetic Susceptibility)

EUC 受控设备(Equipment Under Control)

E/E/PE 电气/电子/可编程电子(Electrical/Electronic/Programmable Electronic)

ICS 工业控制系统(industrial control system)

RTE 实时以太网(Real-Time Ethernet)

4 概要

工业生产现场环境中,由于工频干扰及设备自身的电磁辐射,电磁环境比较复杂。为保证工业控制网络设备稳定可靠地工作,应对设备电磁抗干扰能力与电磁干扰特性进行约定。工业控制网络设备实现了某种通信协议(比如现场总线及实时以太网),应对通信协议的符合性进行检测认证。还有,工业控制网络设备的安装对于通信质量也是关键影响因素,比如屏蔽、接地、等电势联接等对通信的稳定性影响较大。这三方面是保障通信质量的基本要求。

工业控制网络连接智能制造系统中的设备层与控制层,是智能制造系统中的基础通信网络。因此,除了在第5章规定工业控制网络设备通信质量保障性要求外,在第6章和第7章分别还对工业控制网络通信性能以及工业控制网络功能提出要求,以规范工业控制网络的实施与应用,为制造商、用户及集成商提供工业通信协议应用的通用导则。

常见工业控制网络通信协议参见附录A。

5 工业控制网络设备通信质量保障性要求

5.1 EMC 要求

根据应用需求和设备类型,工业控制设备应根据以下 EMI 和 EMS 各项(可选且不限于)对 EMC 性能进行评估,性能等级应符合附录B中的规定,并提供符合要求的合格证明。

EMS 性能要求项如下:

- 静电放电抗扰度;
- 射频电磁场辐射抗扰度;
- 电快速瞬变脉冲群抗扰度;
- 浪涌(冲击)抗扰度;
- 射频场感应的传导骚扰抗扰度;
- 工频磁场抗扰度;
- 电压暂降、短时中断和电压变化的抗扰度。

EMI 性能要求项如下:

- 辐射发射;
- 传导发射。

工业网络设备在受到的电磁干扰消失后,无需人为干预应能恢复正常通信。

5.2 通信协议一致性要求

按照特定工业通信协议开发的工业控制网络设备应符合工业通信协议的规定。根据不同工业通信协议要求,对于控制网络中设备的物理层、数据链路层、应用层协议实现等有协议一致性要求。对于应用在工业控制网络中的设备,应通过官方授权的检测认证实验室的测试,并提供符合性证明。

5.3 网络安装要求

有线网络的安装应符合 GB/T 26336—2010 及 IEC 61784-5 的要求,IEC 61784-5 为系列标准,宜

根据应用的通信协议种类选择使用。

6 工业控制网络通信性能要求

6.1 概述

针对不同应用,用户对工业控制网络的要求也不相同。为了更好地满足应用要求以及明确通信能力评估指标,规定本章中的通信性能要求。这些性能要求用来规范网络能力,而网络能力依赖于网络终端设备及网络部件性能,可作为制造商与用户共同参考的技术指标。工业以太网 PROFINET 网络性能设计示例参见附录 C。

本标准中不规定通用的性能指标边界值,但是,如果制造商声称其产品符合某种工业通信协议,应规定其产品的相应边界值。关于具体通信协议的通信性能见 IEC 61784-2。

6.2 端节点数

对于工业以太网,端节点数指的是一个通信行规(CP)应支持的 RTE 端节点的最大数量,交换机类的网络设备不计入端节点数。

对于现场总线,指的是一个网络中所允许的符合相关通信协议的最大节点个数。

在网络规划中,应对端节点的个数加以限制,目的是优化网络性能,确保在控制器的处理能力范围内,达到应用所需的响应及时性、延时、网络负载等指标。

6.3 基本网络拓扑

包括星型、树型、线型以及用于冗余的环形网络。

星型网络适用于在物理上受空间限制的区域,几个通信节点连接到同一个交换机则自动形成星型拓扑。这种拓扑结构中,单一网络节点失败或移除,不影响其他节点的工作。如果中央的交换机失败,所有连接的节点通信都将中断。

将几个星型拓扑连接起来即可形成树型拓扑。树型拓扑中星型交汇点的交换机作为信号分路器,该交换机基于地址路由报文。

线型拓扑中设备串接成菊花链,用于物理区域较大的自动化车间,比如传送带,也可用于小型机器应用。线型拓扑中断时(例如以太网接口设备断电),位于该设备后面的所有设备都无法正常通信。

环形拓扑可以解决线型拓扑中的上述缺陷,环网中的所有设备连接成环,其中的一个设备为冗余管理器,逻辑上不形成闭环。当其中有节点断开时,冗余管理器重新组织通信路径,从而恢复正常通信。

6.4 网络组件数

端节点间网络组件个数。网络组件对信号的传输会带来延时,应根据应用要求,限制网络组件的使用数量。

注:网络组件指交换机、中继器、路由器、集线器等。

6.5 通信速率

通信链路上单位时间内传输的数据量,通常以比特每秒(bit/s)表示。工业通信协议的物理层决定了可支持的通信速率,每种通信速率仅可达有限的通信距离,通信速率与通信距离间的要求见具体的协议规范。

6.6 非实时带宽

一个链路上用于非实时通信的带宽百分比。工业通信数据由时间关键的数据(即实时数据,比如过

程数据、报警等)以及非时间关键数据(非实时数据,比如参数、状态信息等)组成,应为非实时通信预留带宽。实时以太网带宽与非实时以太网带宽彼此关联。

6.7 响应时间

从一个节点(请求方)向另一个节点(响应方)发出请求至请求方收到来自响应方的响应所需的时间。影响响应时间的因素包括但不限于传输距离、通信拓扑、网络组件数量、经历的节点数量、响应方收到请求后的处理时间。响应时间包括传输时间、网络延时以及请求处理时间,该通信性能取决于通信协议本身及具体应用。

6.8 时间同步精度

任意两个节点时钟之间的最大偏差,根据应用不同,时间同步精度可为 ms 级、 μ s 级,甚至是 ns 级。集成了时间同步协议的工业通信协议才能用于时间同步应用中,通信协议可实现的时间同步精度与协议特性相关。

6.9 非基于时间的同步精度

任意两个节点之间的周期性行为的最大抖动。周期性行为通过网络上的周期性事件触发,该特性用于评估事件触发的数据或者动作的一致性。

6.10 冗余恢复时间

发生单一永久失效时,从失效到再次完全正常工作的最大时间。冗余形式包括多种形式,例如介质冗余、关键装置冗余、控制系统冗余。冗余恢复时间与采用的冗余协议以及相关设备的性能有关。

7 工业控制网络功能要求

7.1 运行维护要求

7.1.1 标识

7.1.1.1 一般要求

标识功能提供一组可读/写的定义良好的数据,用以标识网络设备。该组数据要求永久存储,即,可以掉电保存,同时提供该组数据的版本信息;数据中应包含制造商信息、硬件版本、软件(固件)版本、产品序列号,宜包含订货号、安装日期、位置、签名(SIGNATURE,用于信息安全);不应包含与用户应用无关的信息,比如制造商加密相关信息等。设备宜提供的标识信息见表 1。

表 1 推荐设备提供的标识信息

标识信息内容	解 释	访问属性
Manufacturer_name	制造商名称	R
Device_ID	设备 ID	R
Hardware_Revision	硬件版本	R
Firmware_Revision	固件版本	R
Serial_Number	产品序列号	R
Order_Number	订货号	R

表 1 (续)

标识信息内容	解 释	访问属性
Install_Date	安装日期	RW
Install_Location	安装位置	RW
TAG	标签	RW
SIGNATURE	签名	RW
注：R 表示可读，RW 表示可读写。		

另外，工业控制网络设备应支持物理标识、网络地址标识和应用属性标识，应具有统一的标识编码规则。

7.1.1.2 标识配置

工业控制网络应根据标识信息的不同，支持与用户现场应用相关标识信息的配置功能，可通过有线网络接口读取、修改设备各类标识。

7.1.1.3 标识识别

工业控制网络应支持标识识别功能，通过有线网络接口识别所连接的网络中各节点的身份标识和应用属性标识，解析其应用属性，将所解析出来的信息提供给组态、参数化、调试、诊断、维护、维修、固件升级、资产管理、审计跟踪等设备全生命周期各阶段使用。

7.1.2 诊断和报警

工业控制网络设备宜支持诊断和报警功能。当现场设备/模块的状态或操作、控制器等出现异常情况，或者现场设备出现故障时，应向操作站发出诊断或报警的事件报告。

工业控制网络宜检测整个网络的通信状态，检测网络是否发生异常或存在无法通信的节点，按照严重程度提供诊断或报警。

设备制造商按照事件的紧急或严重程度，区分一般诊断和报警信息：

- a) 一般诊断信息仅是报告有某个事件发生但不至于影响控制网络系统运行，例如某个生产装备环境温度较高或者寿命将近等；
- b) 报警是指发生了比较严重的异常和故障，要求控制器或操作员现场解决或报警确认。

7.1.3 日志

工业控制网络设备应支持日志功能，应包含配置管理、固件升级、诊断报警等历史记录。

工业控制网络应支持网络管理的日志功能，应包含组网设备状态、网络拓扑变化、网络状态变化、诊断报警等历史记录。

7.1.4 档案资料维护

网络拓扑图、网络维护记录、运行日志(历史记录)应纳入档案资料管理。

网络设备的说明书、相关设备物理位置图、网络规划图、备件情况、电缆等配件的相关资料宜单独保存，作为系统维护资料的一部分。

7.1.5 状态报告

工业控制网络宜支持获得实时的设备工作状态信息，设备工作状态信息包括但不限于：设备标识、

系统资源使用、固件版本、接口状态、工作环境等。

工业控制网络宜支持网络状态监视功能。网络状态监视功能应包含整体网络连接状态、网络所有节点状态、网络负荷等状态监视功能,供网络管理人员或智能网络管理软件分析统计。

7.2 管理要求

7.2.1 配置

工业控制网络的配置要求如下:

- a) 宜支持设备配置管理功能,通过有线网络接口进行设备配置管理。设备网络配置管理功能应包含但不限于:设备基本信息管理、诊断范围和报警域限管理、设备固件升级等。
- b) 宜根据身份对管理进行权限控制。

7.2.2 可扩展

工业控制网络应具备可扩展性,新接入的节点应能即插即用。

7.2.3 拓扑管理

工业控制网络提供以下拓扑管理功能:

- a) 应支持网络拓扑图生成、显示、布局功能;
- b) 宜支持设备自动发现功能;
- c) 宜支持网络拓扑管理功能,当网络结构发生变化时,可自动更新。

7.3 服务保障要求

7.3.1 冗余

工业控制网络宜具有一定的冗余措施,在部分网络出现故障时,剩余网络维持系统正常运转。工业控制网络宜包括以下冗余功能:

- a) 网络冗余:两个或以上的冗余通信网络,当其中一个网络故障时,另一个网络能够正常通信,不影响正常数据通信。或者,构建环形冗余通信网络,当环网其中一个方向网络故障时,通信数据可以通过另一个方向正常通信。
- b) 节点冗余:互为热备或冷备的冗余节点,当其中一个节点故障时,另一热备或冷备节点能够接替故障节点工作,不影响正常数据通信。

7.3.2 故障隔离

工业控制网络应支持网络故障隔离,减小故障影响。故障类型包括区域故障和单点故障,应采取包括但不限于以下措施:

- a) 工业控制网络宜进行横向分区,纵向分层设计,某区域发生故障(如网络风暴)时,故障宜被隔离,不应扩散至其他区域。
- b) 工业控制网络宜配置合适策略,网络某点发送故障时,故障被隔离至有限范围内;故障恢复时,隔离措施不影响正常通信。

7.4 安全要求

7.4.1 功能安全

根据工业控制网络的应用领域,如果网络中有功能安全关键系统(Safety-critical system),要求特

定行业应利用风险评估过程为工业控制系统设计目标安全完整性等级。

GB/T 20438 以及 GB/T 21109 是功能安全基础标准,特定行业(如核工业、铁路、机械等)具有以上述标准为基础的行业特定功能安全标准。对于工业控制系统或者部件的功能安全评估,如果具有行业特定功能安全标准,可参照行业标准,否则,宜按 GB/T 20438 要求执行。

有些通信协议提供了安全行规(如 PROFI-safe、CC-LINK Safety),制造商可通过在通信协议之上实现此安全行规作为安全层,以保证通信数据的正确性。这样的产品应对安全层进行检测认证,以及对产品研制过程是否符合 GB/T 20438 进行认证(即安全认证)。

需要明确强调,各部件/设备的安全完整性等级即使都与系统预期设计的安全完整性等级相同或者更高,也不代表由这些部件组成的系统能达到系统要求的功能安全等级。单个设备的安全完整性等级可通过在设备中实现功能安全规范,经过对设备软/硬件开发全过程的安全评估,实现预期的安全等级。系统的功能安全涉及整个生命周期,包括分析、设计、安装、确认、操作、维护、停用,需要根据功能安全标准和系统目标功能安全等级,对系统进行风险分析,确定可接受的风险,实施风险降低措施。

对于功能安全有要求的工业控制系统,应由专业功能安全评估机构根据功能安全标准,通过风险分析方法,评估整个系统的功能安全等级以确定是否符合功能安全要求。

7.4.2 信息安全

工业控制网络应提供信息安全功能,为实现信息安全可采取的措施包括管理措施和技术措施。工业控制网络的信息安全要求可参照数字化车间信息安全一般要求。

应注意的是,工业通信协议本身如果提供了信息安全技术细节,设备制造商可通过实现信息安全协议内容为设备提供部分信息安全功能。对于整个控制系统,则需要对系统进行风险分析,根据目标信息安全等级,由系统集成商/用户采取管理以及技术方面等措施来实现信息安全功能。信息安全实施及评估的国家标准或国际标准参见附录 D。



附 录 A
(资料性附录)
常用工业控制网络

IEC 61158 按照类型(Type)来区分不同的场总线和工业以太网。表 A.1 列出了工业控制网络常用通信协议。

表 A.1 工业控制网络常用通信协议

编号	IEC 61158 类型	现场总线/工业以太网类型	国家标准
1	类型 2	ControlNet/Ethernet/IP	GB/Z 26157
2	类型 3	PROFIBUS	GB/T 20540
3	类型 10	PROFINET	GB/T 25105
4	类型 12	EtherCAT	GB/T 31230
5	类型 13	Ethernet POWERLINK	GB/T 27960—2011
6	类型 16	SERCOSS III	—
7	类型 18	CC-Link	GB/T 19760
8	类型 20	HART	GB/T 29910
9	类型 1	Fieldbus Foundation	—
10	类型 15	Modbus/TCP	GB/T 19582
11	类型 23	CC-Link IE	GB/T 33537

附 录 B

(规范性附录)

工业控制网络设备常用 EMC 检测项要求及相关标准

B.1 EMC 常用检测要求

根据应用需求、设备类型及 GB/T 17626,工业控制网络设备常用 EMS、EMI 检测项和要求见表 B.1 与表 B.2(可选且不限于)。

表 B.1 工业控制网络设备常用 EMS 检测项和要求

EMS 性能检测项	试验条件	性能判据
静电放电抗扰度	接触 6 kV,空气 8 kV	B
射频电磁场辐射抗扰度	80 MHz~1 GHz,10 V/m	A
	3 V/m(1.4 GHz~2 GHz)	A
	1 V/m(2.0 GHz~2.7 GHz)	A
电快速瞬变脉冲群抗扰度	交流电源口 2 kV(5 ns~50 ns,5 kHz)	B
	信号口 1 kV(5 ns~50 ns,5 kHz)	B
浪涌(冲击)抗扰度	交流电源口,线对地 2 kV,线对线 1 kV	B
	信号口,线对地 1 kV(仅适用线缆长度超过 10 m)	B
射频场感应的传导骚扰抗扰度	交流电源口 10 V,150 kHz~80 MHz, 信号口 10 V,80%AM(1 kHz)	A
工频磁场抗扰度	30 A/m(仅适用于对磁场敏感的设备)	A
电压暂降、短时中断和电压变化的抗扰度	交流电源口 0% 0.5 周期	A
	0% 1 周期	B
	40% 10 周期	B
	70% 25 周期	B
	0% 250 周期	C

表 B.2 工业控制网络设备常用 EMI 检测项和要求

EMI 性能检测项	试验条件	性能判据
辐射发射	30 MHz~1 GHz	A 类限值
传导发射	150 kHz~30 MHz 交流电源口和网口	A 类限值

B.2 常用 EMC 标准

工业控制常用 EMC 标准见表 B.3。

表 B.3 工业控制常用 EMC 标准

标准号	标准名称
GB/T 17625	电磁兼容 限值
GB/T 17626	电磁兼容 试验和测量技术
GB/T 17799	电磁兼容 通用标准
GB/T 18039	电磁兼容 环境
GB/T 15969.2—2008	可编程序控制器 第 2 部分:设备要求和测试
GB/T 9254—2008	信息技术设备的无线电骚扰限值和测量方法
GB 4824—2019	工业、科学和医疗设备 射频骚扰特性 限值和测量方法



附 录 C

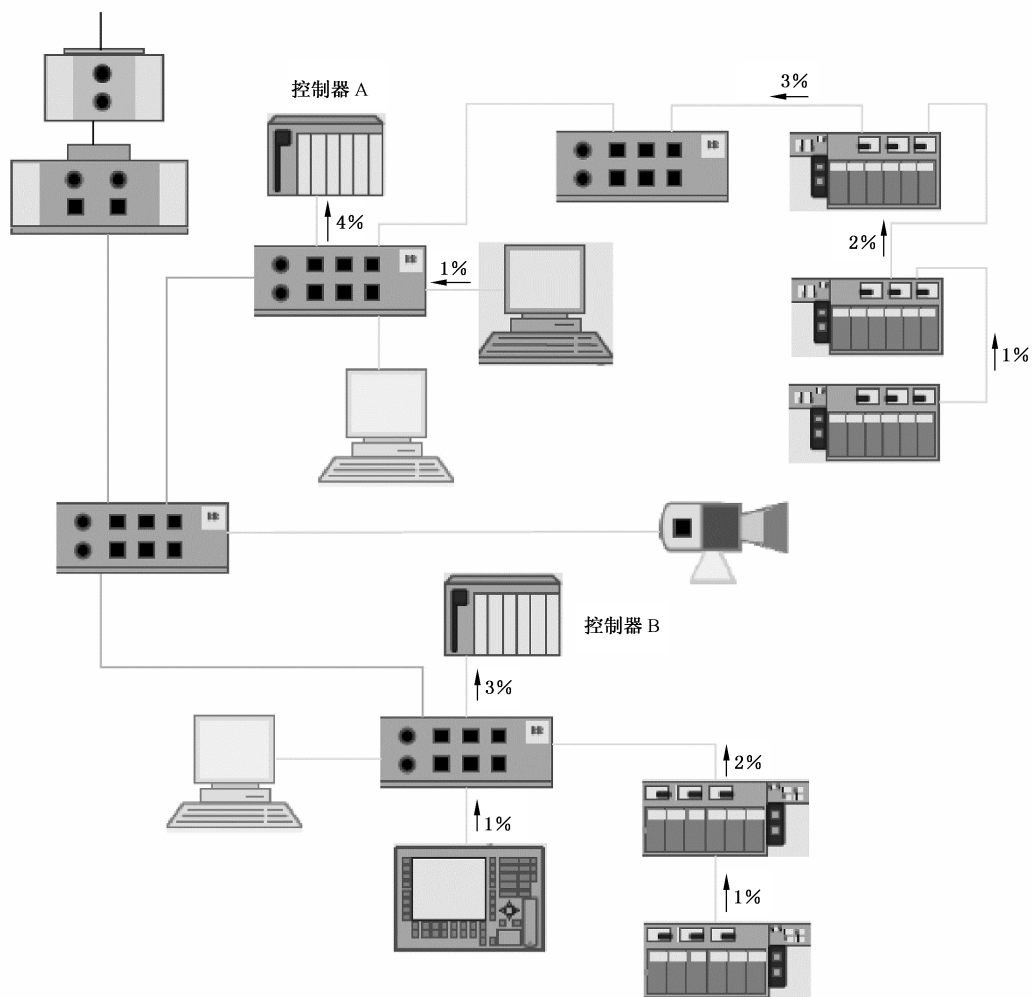
（资料性附录）

PROFINET 网络性能设计示例

C.1 概述

根据环境条件和自动化任务的要求,选择 CC-B 设备。

按照物理区域、控制对象、数据量,将控制设备划分为两个控制域,构成两个控制子网,如图 C.1 所示。



注: 图中的百分数是网络负载, 即已使用的带宽与最大可用带宽的比。

图 C.1 网络规划图

C.2~C.5 各条针对影响 PROFINET 网络关键性能的因素进行分析设计。

C.2 拓扑选择

整个控制系统根据应用需求采用混合拓扑,现场 IO 设备通过线型拓扑连接,再连接至交换机,与控制器、操作面板及监视器构成星型拓扑。

现场 IO 设备距离交换机较远,线型拓扑连接可以节省线缆。

C.3 update time 确定

update time 指一个设备在其应用中形成一个变量,通过线缆传送给另一个设备并供此设备使用,这一过程所耗费的时间。同一车间中 PROFINET 设备的 update time 可能不同,传输周期由其中 update time 最慢的设备确定,在一个传输周期中,所有的 PROFINET 设备至少接收或发送数据一次。

一个传输周期被划分为几个阶段,每个阶段的时间为 31.25 μs 的整数倍,该倍数即 SendClockFactor(来自设备的 GSD 文件),用公式表示如下:

$$T_p = \text{SendClockFactor} \times 31.25 \mu\text{s}$$

update time 的值 T_a 不一定是传输时钟,其值可通过如下公式获得:

$$T_a = \text{ReductionRatio} \times \text{SendClockFactor} \times 31.25 \mu\text{s}$$

上述公式中的 ReductionRatio 来自设备的 GSD 文件,一般有多个可选值。

注:传输时钟(transmission clock)是数据包发送的最小时钟,在 IO 控制器中设置。通常,控制器中设置的传输时钟对应于设备的最小 update time。

宜使用较小的传输时钟,目的是分散网络负载,降低集中度。因此,如果要更改设备的 update time,宜先考虑修改 ReductionRatio,而不是控制器的传输时钟。

如果使用较小的 update time 值,则数据更新间隔更短,因此能以更快的速度提供数据用以处理。但是,一定时间内网络中传输的数据量即网络负载就会增加。

以常见 PROFINET 包的大小 108 字节(60 字节有效负载数据)为例,网络负载与 update time 以及网络节点数的函数关系如图 C.2 所示。

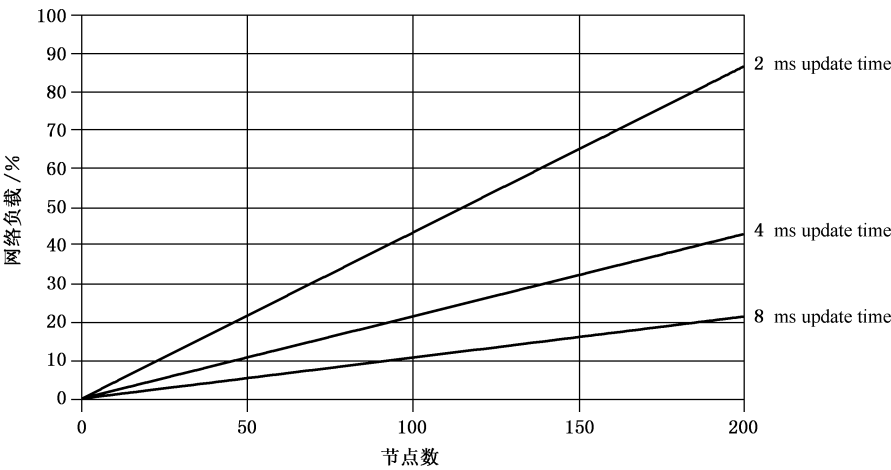


图 C.2 网络负载与 update time 以及网络节点数的函数关系

当周期实时通信网络负载增加时,其他通信可用带宽下降。

update time 越小,周期实时通信占用带宽越大;update time 越大,响应时间越长。因此,宜在符合应用对响应时间的要求下,尽量选择较大的 update time。

C.4 网络负载

网络负载是指使用的带宽与可用最大带宽的比值。假设每个设备在设备至控制器方向产生 1% 的网络负载,最大负载发生在交换机与控制器之间。

通信同时在发送和接收方向进行,仅分析负载较高的一个方向即可。

网络规划要求确定最高网络负载的点,对该点进行负载限值的核算,推荐的网络负载限值见表 C.1。

表 C.1 推荐的网络负载限值

网络负载	推荐的措施
<20%	无需动作
20%~50%	检查网络负载规划
>50%	采取适当措施降低网络负载

为了识别出负载最高的位置,需要知道每个 PN 设备产生的循环网络负载,这取决于 update time 和数据量,设备的网络负载计算可采用专用工具计算。

另外,应检查非实时网络负载。例如在网络规划图中,针对摄录机这样大量数据的设备,应采用单独的链路,避免通过控制链路传输数据。

C.5 line depth 检查

line depth 指 IO 设备至控制器之间的交换机数量,由于交换机会引入延时,因此在规划拓扑时应考虑 line depth 值的影响。大的 line depth 影响响应时间。“存储并转发交换机”以及“直通”交换机带来的延时不同,下面分别给出特定 update time 时,两种交换机分别对应的最大允许 line depth 见表 C.2 和表 C.3。

表 C.2 “存储并转发”交换机最大允许 line depth

update time	1 ms	2 ms	4 ms	8 ms
line depth	7	14	28	58

表 C.3 “直通”交换机最大允许 line depth

update time	1 ms	2 ms	4 ms	8 ms
line depth	64	100	100	100

如果 IO 设备与控制器间混合使用了两种交换机,则都按“存储并转发”型交换机计算 line depth。

附 录 D
(资料性附录)
工业控制信息安全标准

常用信息安全标准如下:

GB/T 30976.1—2014 工业控制系统信息安全 第1部分:评估规范

GB/T 30976.2—2014 工业控制系统信息安全 第2部分:验收规范

GB/T 33007—2016 工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序

GB/T 33008.1—2016 工业自动化和控制系统网络安全 可编程控制器(PLC) 第1部分:系统要求

GB/T 33009.1—2016 工业自动化和控制系统网络安全 集散控制系统(DCS) 第1部分:防护要求

GB/T 33009.2—2016 工业自动化和控制系统网络安全 集散控制系统(DCS) 第2部分:管理要求

GB/T 33009.3—2016 工业自动化和控制系统网络安全 集散控制系统(DCS) 第3部分:评估指南

GB/T 33009.4—2016 工业自动化和控制系统网络安全 集散控制系统(DCS) 第4部分:风险与脆弱性检测要求

IEC/TS 62443-1-1 工业通信网络 网络和系统安全 第1-1部分:术语、概念和模型(Industrial communication networks—Network and system security—Part 1-1: Terminology, concepts and models)

IEC 62443-3-1 工业通信网络 网络和系统安全 第3-1部分:工业自动化与控制系统的信息安全技术(Industrial communication networks—Network and system security—Part 3-1: Security technologies for industrial automation and control systems)

IEC 62443-3-3 工业通信网络 网络和系统安全 第3-3部分:系统安全要求和信息安全等级(Industrial communication networks—Network and system security—Part 3-3: System security requirements and security levels)

参 考 文 献

- [1] GB/T 19582(所有部分) 基于 Modbus 协议的工业自动化网络规范
- [2] GB/T 19760(所有部分) CC-Link 控制与通信网络规范
- [3] GB/T 20540(所有部分) 测量和控制数字数据通信 工业控制系统用现场总线 类型 3: PROFIBUS 规范
- [4] GB/T 20830—2015 基于 PROFIBUS DP 和 PROFINET IO 的功能安全通信行规-PROFIsafe
- [5] GB/T 22033—2017 信息技术 嵌入式系统术语
- [6] GB/T 25105(所有部分) 工业通信网络 现场总线规范 类型 10: PROFINET IO 规范
- [7] GB/Z 26157(所有部分) 测量和控制数字数据通信 工业控制系统用现场总线 类型 2: ControlNet 和 EtherNet/IP 规范
- [8] GB/T 27960—2011 以太网 POWERLINK 通信行规规范
- [9] GB/T 29910(所有部分) 工业通信网络 现场总线规范 类型 20: HART 规范
- [10] GB/T 31230(所有部分) 工业以太网现场总线 EtherCAT
- [11] GB/T 33537(所有部分) 工业通信网络 现场总线规范 类型 23: CC-Link IE 规范
- [12] IEC 61158(all parts) Industrial communication networks—Fieldbus specifications
- [13] IEC 61784-1 Industrial communication networks—Profiles—Part 1: Fieldbus profiles
- [14] IEC TR 62390 Common automation device—Profile guideline
- [15] IEC 62443-2-1 Industrial communication networks—Network and system security—Part 2-1: Establishing an industrial automation and control system security program
- [16] IEC/PAS 62443-3 Security for industrial process measurement and control—Network and system security