



中华人民共和国国家标准

GB/T 20171—2006

用于工业测量与控制系统的 EPA 系统结构与通信规范

EPA system architecture and communication specification for use
in industrial control and measurement systems

2006-05-08 发布

2006-11-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会

发布

中 华 人 民 共 和 国
国 家 标 准
用于工业测量与控制系统的
EPA 系统结构与通信规范

GB/T 20171—2006

*

中国标准出版社出版发行
北京西城区复兴门外三里河北街16号

邮政编码:100045

<http://www.spc.net.cn>

电话:(010)51299090、68522006

2006年11月第一版

*

书号:155066·1-28093

版权专有 侵权必究
举报电话:(010)68522006

目 次

前言	IX
引言	X
1 范围	1
2 规范性引用文件	1
3 术语和定义	4
3.1 GB/T 9387 中的术语	4
3.2 GB/T 16262—1996 中的术语	4
3.3 GB/T 17967—2000 中的术语	5
3.4 IEC 61158-5 中的术语	6
3.5 IEC 61804-2 中的术语	9
3.6 本标准规定的术语	10
4 符号和缩略语	12
5 约定	14
5.1 对象定义约定	14
5.2 服务定义约定	15
5.3 协议状态机的约定	16
6 EPA 系统结构	17
6.1 概述	17
6.2 EPA 结构	17
6.3 网络拓扑结构	21
6.4 EPA 设备间的通信过程	25
6.5 EPA 系统组态和启动	27
7 EPA 数据链路层协议	29
7.1 概述	29
7.2 数据链路层模型	29
7.3 EPA 通信调度规程	30
7.4 EPA 通信调度管理实体 PDU 结构	37
7.5 EPA 通信调度管理实体 PDU 编码	38
8 EPA 应用层服务定义	40
8.1 概念	40
8.2 数据类型 ASE	52
8.3 通信模型规范	59
8.4 EPA 应用层服务一览	104
9 EPA 应用层协议规范	104
9.1 语法描述	104
9.2 传输语法	115
9.3 协议状态机概述	139
9.4 系统管理实体协议状态机	140

9.5	应用访问实体协议状态机	149
9.6	套接字映射实体协议状态机	160
10	基于 XML 的 EPA 设备描述	162
10.1	概述	162
10.2	EPA 可扩展设备描述文件概述	163
10.3	设备描述文件结构定义	167
10.4	组态软件接口	179
	附录 A(规范性附录)EPA 网络安全导则	180
	附录 B(规范性附录)基于以太网的物理层附加要求	185
	附录 C(规范性附录)工业以太网设计和安装指导	191
	参考文献	196
表 1	服务原语格式示例	16
表 2	状态机转换表的约定	16
表 3	EPA 对 ISO/OSI 模型的映射	17
表 4	EPA 通信调度管理实体 EPA_CSME 状态转换表	32
表 5	EpaPeriodicDataSendingSuc 函数描述	34
表 6	EpaNonPeriodDataAnnunciation 函数描述	34
表 7	EpaPeriodicDataSending 函数描述	34
表 8	EpaNonPeriodDataSendingSuc 函数描述	34
表 9	EpaFirstNonPeriodDataSending 函数描述	34
表 10	EpaNonPeriodDataPriority 函数描述	35
表 11	EpaNonPeriodDataTimeEnough 函数描述	35
表 12	EpaNonPeriodDataSending 函数描述	35
表 13	EpaEndofNonPeriodDataSending 函数描述	35
表 14	EpaIsDeviceConfigured 函数描述	36
表 15	EpaCountOffsetTime 函数描述	36
表 16	EpaDataSendingTiming 函数描述	36
表 17	EpaRecEndofNonPeriodDataSending 函数描述	36
表 18	NonPeriodDataAnnunciation 报文编码表	38
表 19	非周期数据发送结束声明报文编码表	39
表 20	EPA 报文编码表	39
表 21	EPA 管理信息库 EPA MIB	61
表 22	EPA 系统管理实体服务	73
表 23	EM_FindTagQuery 服务参数	74
表 24	EM_FindTagReply 服务参数	75
表 25	EM_GetDeviceAttribute 服务参数	76
表 26	EM_DeviceAnnunciation 服务参数	78
表 27	EM_SetDeviceAttribute 服务参数	79
表 28	EM_ClearDeviceAttribute 服务参数	81
表 29	域 ASE 支持的服务	82
表 30	域的存取组	82
表 31	域的存取权限	83

表 32	域下载服务的参数	84
表 33	域上载服务参数	86
表 34	事件管理服务	87
表 35	事件对象的存取组	88
表 36	事件对象的存取权限	88
表 37	事件通知服务参数	89
表 38	事件通知确认服务参数	90
表 39	改变事件条件监视服务参数	91
表 40	变量访问服务	92
表 41	域的存取组	93
表 42	域的存取权限	93
表 43	域的存取组	95
表 44	域的存取权限	95
表 45	变量读服务参数表	96
表 46	变量写服务参数表	97
表 47	信息分发服务参数表	98
表 48	EPA 应用层服务一览	104
表 49	Boolean 数据类型取值为 True 时的编码	115
表 50	Boolean 数据类型取值为 False 编码	115
表 51	Unsigned8 数据类型编码	115
表 52	Unsigned16 数据类型编码	115
表 53	Unsigned32 数据类型编码	116
表 54	Unsigned64 数据类型编码	116
表 55	Int8 数据类型编码	116
表 56	Int16 数据类型编码	116
表 57	Int32 数据类型编码	117
表 58	Int64 数据类型编码	117
表 59	Real 数据类型编码	117
表 60	VisibleString 数据类型编码	117
表 61	OctetString 数据类型编码	118
表 62	BitString 数据类型编码	118
表 63	TimeOfDay 数据类型编码	118
表 64	BinaryDate 数据类型编码	119
表 65	TimeDifference 数据类型编码	119
表 66	EPAMIBHeader 对象编码表	120
表 67	EPADevice Descriptor 对象编码表	120
表 68	Sync and Scheduling 对象编码表	121
表 69	MAX Response Time 对象编码表	121
表 70	Communication Schedule Management 对象编码表	122
表 71	Device Application Information 对象编码表	122
表 72	FB Application Information Header 对象编码表	122
表 73	Domain Application Information Header 对象编码表	123
表 74	Link Object Header 对象编码表	123

表 75	FB Application Information 对象编码表	124
表 76	Link Object 对象编码表	124
表 77	Domain Application Information 对象编码表	125
表 78	域 Domain 对象编码表	125
表 79	简单变量 Variable 对象编码表	126
表 80	事件 Event 对象编码表	126
表 81	EPA 套接字映射对象	127
表 82	EPA 套接字映射定时器对象编码表	127
表 83	差错对象 ErrorType 编码表	128
表 84	报文结构描述	128
表 85	EM_FindTagQuery 服务报文编码表	129
表 86	EM_FindTagReply 服务报文编码表	129
表 87	EM_GetDeviceAttribute 服务请求编码表	130
表 88	EM_GetDeviceAttribute 服务正响应编码表	130
表 89	EM_GetDeviceAttribute 服务负响应编码表	131
表 90	EM_DeviceAnnunciation 服务请求报文编码表	131
表 91	EM_SetDeviceAttribute 服务请求报文编码表	132
表 92	EM_SetDeviceAttribute 服务正响应报文编码表	133
表 93	EM_SetDeviceAttribute 服务负响应报文编码表	133
表 94	EM_ClearDeviceAttribute 服务请求报文编码表	133
表 95	EM_ClearDeviceAttribute 服务负响应报文编码表	134
表 96	EM_ClearDeviceAttribute 服务负响应报文编码表	134
表 97	域下载请求服务报文编码表	134
表 98	域下载服务正响应报文编码表	134
表 99	域下载服务负响应报文编码表	135
表 100	域上传请求服务报文编码表	135
表 101	域上传请求服务正响应报文编码表	135
表 102	域上传请求服务负响应报文编码表	136
表 103	事件通知服务报文编码表	136
表 104	事件通知确认服务报文编码表	136
表 105	事件通知确认服务正响应报文编码表	136
表 106	事件通知确认服务负响应报文编码表	137
表 107	改变事件条件监视服务报文编码表	137
表 108	改变事件条件监视服务正响应报文编码表	137
表 109	改变事件条件监视服务负响应报文编码表	137
表 110	变量读请求服务报文编码表	138
表 111	变量读请求服务报文正响应编码表	138
表 112	变量读请求服务报文负响应编码表	138
表 113	变量写请求服务报文编码表	138
表 114	变量写请求服务正响应报文编码表	139
表 115	变量写请求服务负响应报文编码表	139
表 116	信息分发服务报文编码表	139
表 117	应用层用户向系统管理实体发布的原语	140

表 118	系统管理实体向应用层用户发布的原语	140
表 119	系统管理实体与应用层用户之间交换的原语所用的参数	141
表 120	系统管理实体发布给套接字映射实体的原语	141
表 121	套接字映射实体发布给系统管理实体的原语	141
表 122	系统管理实体与套接字映射实体之间交换的原语所用的参数	141
表 123	管理实体状态转换表	142
表 124	EpaRcvNewIpAddress 函数描述	145
表 125	EpaAttribute_Set 函数描述	145
表 126	EpaRestoreDefaults 函数描述	146
表 127	EpaNewAddress 函数描述	146
表 128	Restart_EPAREpeatTimer 函数描述	146
表 129	EpaClear_DuplicatePdTagFlag 函数描述	146
表 130	EPAREpeatTimerExpire 函数描述	147
表 131	EpaSend_EM_ReqRspMessage 函数描述	147
表 132	EpaSend_EM_CommonErrorRsp 函数描述	147
表 133	EpaSntpSyncLost 函数描述	147
表 134	EpaIPAddressCollision 函数描述	147
表 135	EpaRecvMsg 函数描述	148
表 136	EpaQueryMatch 函数描述	148
表 137	EpaMessageIDMatch 函数描述	148
表 138	EpaDevId_Match 函数描述	148
表 139	EpaPdTag_Match 函数描述	149
表 140	EpaSet_Attribute_Data 函数描述	149
表 141	EpaSet_DuplicatePdTagFlag 函数描述	149
表 142	应用层用户向应用访问实体发布的原语	149
表 143	应用访问实体向应用层用户发布的原语	150
表 144	应用访问实体和应用层用户之间交换的原语所用的参数	150
表 145	应用访问实体和套接字映射实体发布的原语	150
表 146	套接字映射实体向应用访问实体发布的原语	150
表 147	应用访问实体和套接字映射实体之间交换的原语所用的参数	150
表 148	应用访问实体状态描述	151
表 149	应用层状态表——发送方状态转换	151
表 150	应用层服务状态表——接收方状态转换	152
表 151	ServiceType 函数描述	153
表 152	事件通知者向事件对象发布的原语	153
表 153	事件对象向事件通知者发布的原语	153
表 154	事件管理的状态取值表	154
表 155	事件状态转换表	154
表 156	域状态取值	155
表 157	域管理状态转换表	156
表 158	Domain_DownloadSucceed 函数描述	159
表 159	Domain_WriteBuffer 函数描述	159
表 160	IncrementInvokeDomainCounter 函数描述	159

表 161	DecrementInvokeDomainCounter 函数描述	160
表 162	传输层和套接字映射实体之间交换的原语	160
表 163	传输层和套接字映射实体之间交换的原语所用的参数	160
表 164	套接字映射实体状态描述	160
表 165	套接字映射实体状态表——发送方事务处理	161
表 166	套接字映射实体状态表——接收方事务处理	161
表 167	ServiceType 函数描述	162
表 168	根元素	167
表 169	设备描述文件信息体描述元素	167
表 170	设备描述结构体描述元素	168
表 171	设备标识描述结构体描述元素	168
表 172	功能块描述结构体描述元素	169
表 173	功能块结构体描述元素	169
表 174	功能块基本信息描述结构体描述元素	170
表 175	简单变量参数描述元素	172
表 176	枚举变量参数描述子元素	174
表 177	数组变量参数描述子元素	176
表 178	结构参数变量描述子元素	178
表 179	域对象描述元素	179
表 A.1	域、事件和变量对象的存取组	182
表 A.2	域、事件和变量对象的存取权限	183
表 B.1	工业以太网通信线缆选用	185
表 B.2	工业环境通用要求	186
表 B.3	工业防护级别	186
表 B.4	铜缆选择通用要求	186
表 B.5	铜缆直径选择	187
表 B.6	光纤机械特性要求	187
表 B.7	光纤类型	188
表 B.8	连接器通用要求	188
表 B.9	环境对连接器的要求	189
表 B.10	铜缆连接器通用要求	189
表 B.11	不同环境对铜缆连接器的要求	189
表 B.12	光纤连接器通用要求	190
表 B.13	不同环境对光纤连接器的要求	190
表 C.1	根据电磁兼容性的电缆分类	192
表 C.2	机壳外部电缆与干扰源最小距离	192
表 C.3	机壳内部电缆与干扰源最小距离	192
图 1	EPA 通信协议模型	19
图 2	EPA 测量与控制系统模型	20
图 3	EPA 系统网络拓扑结构示例图	21
图 4	无线局域网 EPA 现场设备接入模型	23

图 5	蓝牙 EPA 现场设备接入的协议模型	24
图 6	EPA 设备间的通信	25
图 7	EPA 链路关系	26
图 8	数据链路层模型	29
图 9	EPA 通信调度示意图	30
图 10	EPA 通信调度管理实体 EPA_CSME 状态转换图	31
图 11	EPA 报文标识	37
图 12	非周期数据声明 PDU 格式	37
图 13	非周期数据发送结束声明 PDU 格式	37
图 14	EPA 报文 PDU 格式	38
图 15	与 OSI 基本参考模型的关系	40
图 16	EPA 应用层的体系结构位置	41
图 17	客户机/服务器交互作用	43
图 18	推模型交互作用	43
图 19	EPA 应用层传输的 APO 服务	44
图 20	应用实体结构	45
图 21	EPA 应用层 ASE 示例	46
图 22	EPA 应用层对象管理	47
图 23	ASE 服务传送	47
图 24	定义和建立 AREP	49
图 25	EPA 应用层体系结构组件	50
图 26	数据类型类层次示例	53
图 27	EPA 应用实体	59
图 28	AR ASE 在 AP 之间传递 APDU	99
图 29	EPA 接收到的报文流向	102
图 30	协议状态机之间交换的原语	140
图 31	EPA 管理实体协议状态机	142
图 32	应用访问实体状态转换图	151
图 33	事件管理协议状态机	154
图 34	域管理协议状态机(Server)	155
图 35	套接字映射实体状态转换图	161
图 36	XDDL 模型	163
图 37	XDDL 可扩展设备描述文件结构	163
图 C.1	屏蔽层接地法	194
图 C.2	保证屏蔽层的连续性	194
图 C.3	星形接地法	195

前 言

本标准的附录 A、附录 B、附录 C 为规范性附录。

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和控制标准化技术委员会第四分技术委员会归口。

本标准起草单位：浙江大学、浙江中控技术股份有限公司、中国科学院沈阳自动化研究所、重庆邮电学院、大连理工大学、清华大学。

本标准参加起草单位：机械工业仪器仪表综合技术经济研究所、上海工业自动化仪表研究所、北京华控技术有限责任公司。

本标准起草人：褚健、金建祥、王宏、冯冬芹、徐皓冬、王平、仲崇权、杨佃福、缪学勤。

本标准参加起草人：梅恪、陈小枫、欧阳劲松、王忠锋、李卓函、魏剑崑、刘丹、张利、马万里、张鑫龙。

引 言

当前,以太网和无线通信技术在工业企业综合自动化系统中的信息管理层、监控级网络得到了广泛应用,并有直接向下延伸,应用于工业测量与控制系统的现场设备级网络的趋势。

从 ISO/OSI 开放系统互连参考模型来看,以太网和无线通信规范只映射为其中的物理层和数据链路层;而在网络层和传输层,目前以 TCP/IP 协议为主(已成为基于以太网的“事实上的”标准)。而对较高的层次,会话层、表示层、应用层等没有作技术规定。如果只有 Ethernet、TCP/IP 这低四层协议规范,只能保证连接到以太网上的设备进行互连,不能保证它们之间的信息互访,因此有必要定义应用层规范,以实现基于以太网和无线技术的工业测量和控制仪表与系统之间的可互操作。同时,还需要定义相应的机制,实现基于以太网和无线通信的确定性通信。

GB/T 20171—2006《用于工业测量与控制系统的 EPA 系统结构与通信规范》针对工业测量与控制系统网络通信特点,以工业控制为应用对象,以以太网和无线通信、TCP/IP 为基础,在 MAC 层与网络层之间定义了 EPA 通信调度管理实体,同时还定义了应用层服务与协议规范,实现了工业自动化系统中各网络层次上的信息集成。

用于工业测量与控制系统的 EPA 系统结构与通信规范

1 范围

本标准定义了基于 GB/T 15629.3—1995、IEEE Std 802.11、IEEE Std 802.15:2002 以及 RFC 791、RFC 768 和 RFC 793 等协议的 EPA(Ethernet for Plant Automation)系统结构、数据链路层协议、应用层服务定义与协议规范以及基于 XML 的设备描述规范。

本标准适用于工业自动化控制领域。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

- GB 4208—1993 外壳防护等级(IP 代码)(eqv IEC 60529:1989)
- GB/T 5271(所有部分) 信息技术词汇(eqv ISO/IEC 2382)
- GB/T 9387(所有部分) 信息技术 开放系统互连 基本参考模型(idt ISO 7498)
- GB 14050—1993 系统接地的型式及安全技术要求
- GB/T 15629.2—1995 信息处理局域网 第 2 部分:逻辑链路控制(idt ISO 8802-2:1989)
- GB/T 15629.3—1995 信息处理局域网 第 3 部分:带碰撞检测的载波侦听多址访问(CSMA/CD)的访问方法和物理层规范(idt ISO 8802-3:1990)
- GB/T 16262—1996 信息处理系统 开放系统互连 抽象语法记法一(ASN.1)规范(idt ISO/IEC 8824:1990)
- GB/T 16263—1996 信息处理系统 开放系统互连 抽象语法记法一(ASN.1)基本编码规则规范(idt ISO/IEC 8825:1990)
- GB/T 17176—1997 信息技术 开放系统互连 应用层结构(idt ISO/IEC 9594:1994)
- GB 17859—1999 计算机信息系统 安全保护等级划分准则
- GB/T 17963—2000 信息技术 开放系统互连 网络层安全协议(idt ISO/IEC 11577:1995)
- GB/T 17967—2000 信息技术 开放系统互连 基本参考模型 OSI 服务定义约定(idt ISO/IEC 10731:1994)
- GB/T 18018—1999 路由器安全技术要求
- GB/T 18019—1999 信息技术 包过滤防火墙安全技术要求
- GB/T 18020—1999 信息技术 应用级防火墙安全技术要求
- GB/T 18336.1—2001 信息技术 安全技术 信息技术安全性评估准则 第 1 部分:简介和一般模型(idt ISO/IEC 15408-1:1999)
- GB/T 18336.2—2001 信息技术 安全技术 信息技术安全性评估准则 第 2 部分:安全功能要求(idt ISO/IEC 15408-2:1999)
- GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第 3 部分:安全保证要求(idt ISO/IEC 15408-3:1999)
- GB 50311—2000 建筑与建筑群综合布线系统工程设计规范