



中华人民共和国国家标准

GB/T 21099.1—2007/IEC/CDV 61804-1:2003

过程控制用功能块 第1部分：系统方面的总论

Function blocks for process control—Part 1: Overview of system aspects

(IEC/CDV 61804-1:2003, IDT)

2007-10-11 发布

2007-12-01 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

目 次

前言	V
引言	VI
1 范围	1
2 规范性引用文件	2
3 术语和定义	3
3.1 基本定义	3
3.2 基于 IA/IM-通道的定义	8
3.3 缩略语	8
4 工程需求	9
4.1 概述	9
4.2 设计阶段的需求	9
5 关于兼容性等级的定义	10
5.1 概要	10
5.2 不兼容性	11
5.3 共存性	11
5.4 可互连性	11
5.5 可协作性	11
5.6 可互操作性	11
5.7 可交换性	12
6 功能需求	12
6.1 概要	12
6.2 系统(或通道或设备)状态	12
6.3 有效性指数(VI)	13
6.4 信号处理	13
6.5 测量信息处理	13
6.6 设备诊断和测试支持	14
6.7 本地接口附属装置	15
6.8 设备(系统和通道)管理	15
7 功能块应用需求	18
7.1 系统概述	18
7.2 基本 FB 类型概述	20
7.3 FB 需求	21
7.4 从 I&C 派生的功能块的初始集	22
7.5 FB 环境需求	27
7.6 通信需求	28
8 附加需求	28
8.1 与外部应用协作	28
8.2 附加特性需求	31

8.3 一致性要求	32
9 设备描述语言	32
9.1 背景	32
9.2 基本要求	33
9.3 一般要求	34
附录 A (资料性附录) 系统生命周期	35
附录 B (资料性附录) FB 功能性需求:用户视图	54
附录 C (资料性附录) GB/T 21099 和 GB/T 19769.1—2005 间的关系	68
附录 D (资料性附录) 模拟输入 FB 到 GB/T 19769 的映射	78
附录 E (资料性附录) AME 需求	90
参考文献	95
图 1 应用交互	V
图 2 GB/T 21099 的影响	2
图 3 功能设备兼容性等级	10
图 4 系统(或通道或设备)状态	12
图 5 功能块设备的组成	18
图 6 过程工业用功能块应用的设备结构	20
图 7 传感器功能层次:实例	26
图 8 非功能块应用数据接口	28
图 A.1 从过程回路到 FRD 的生命周期	36
图 A.2 包含两个过程基本操作的 PFD	37
图 A.3 控制功能在扩展 P&ID 上的明确表示	38
图 A.4 来自扩展 P&ID 的控制功能的提取	39
图 A.5 控制功能和 AB 的需求	39
图 A.6 控制功能需求的结构化文档	40
图 A.7 Folio 的四部分	40
图 A.8 从控制层次图中选择 Folio	41
图 A.9 控制功能“控制泵”详细需求的 Folio	41
图 A.10 FRD 的示例	42
图 A.11 独立于 I&C 系统实现的功能需求图	42
图 A.12 标准功能块语言的需要	43
图 A.13 标准 EFB 库	44
图 A.14 从功能需求图到 I&C 系统和设备	45
图 A.15 一个执行的设计及其来自现货供应的执行设备的 AB	45
图 A.16 来自现货供应执行设备的执行 AB 的内部特性设计	46
图 A.17 AB 的内部块与控制功能的上游和下游 EFB 和 AB 的网络	46
图 A.18 执行 AB 的图形符号和不清晰的内部描述	47
图 A.19 使用 GB/T 19769.1—2005 系统模型的开/关(OFF/ON)阀执行 AB	47
图 A.20 使用 GB/T 19769.1—2005 系统模型的 OFF/ON 执行 AB	48
图 A.21 三取二安全切换 AB 的示例	48
图 A.22 使用 GB/T 19769.1—2005 系统模型的三取二切换 AB	49
图 A.23 使用 GB/T 19769.1—2005 系统模型的从 FRD 到程序设计方案	49

图 A.24	泵 AB 的内部块分布	50
图 A.25	分布 EFB 和控制功能“控制泵”的 AB 到 I&C 结构	51
图 A.26	控制功能在 I&C 设备中的实现	51
图 A.27	使用 GB/T 19769.1—2005 的控制功能“控制泵”的分布	52
图 A.28	从 FRD 到程序设计方案	52
图 B.1	系统属性	56
图 B.2	IA/IM-通道校验	57
图 B.3	分布式自动控制系统的参考功能结构	59
图 B.4	每个 IAM 功能的主要功能成分的用户视图	60
图 B.5	IM 通道/CMM 交互:用户视图	61
图 B.6	使用现场总线的分布式平台:物理组成	62
图 B.7	智能传感器参考模型	63
图 C.1	GB/T 19769.1—2005 功能块结构	68
图 C.2	GB/T 19769.1—2005 功能块的类型细节	69
图 C.3	实施细节方面	69
图 C.4	分布式应用和分布式操作系统	70
图 C.5	过程控制功能块的基本概念	71
图 C.6	过程控制 FB 中的功能成分	72
图 C.7	一个过程控制 FB 的 GB/T 19769.1—2005 图形表示	72
图 C.8	EFB 的完整结构(示例)	73
图 C.9	GB/T 19769.1—2005、GB/T 21099 以及其他标准化活动的关系	74
图 D.1	模拟输入块的参数概要	78
图 D.2	模拟输入块的仿真、模式和状态图	79
图 D.3	模式和状态产生条件	79
图 D.4	模拟输入块的状态机	80
图 D.5	模拟输入块实例	83
图 D.6	AI-FB 图形表示	84
图 D.7	AI-FB ECC	84
图 E.1	命名和寻址方法	91
表 1	功能性特征	11
表 2	初始 FB 集	22
表 3	EFB 一般列表	24
表 C.1	GB/T 19769.1—2005 功能块特征概述	70
表 C.2	GB/T 19769.1—2005 和 GB/T 21099 间的模型构件参考	76
表 D.1	实际模式计算的条件和结果	80
表 D.2	计算输出参数的状态的条件和结果	80
表 D.3	模拟输入块参数属性	81
表 D.4	过程参数描述	82
表 D.5	报警参数描述	82
表 D.6	仿真	83

前 言

GB/T 21099《过程控制用功能块》分为如下几部分：

- 第 1 部分：系统方面的总论；
- 第 2 部分：功能块概念和电子设备描述语言规范；
- 第 3 部分：电子设备描述语言；
- 第 4 部分：EDD 互操作指南。

本部分为 GB/T 21099 的第 1 部分。

本部分等同采用 IEC/CDV 61804-1:2003《过程控制用功能块 第 1 部分：系统方面的总论》(英文版)。

本部分根据 IEC/CDV 61804-1:2003 翻译。

为便于使用,对 IEC/CDV 61804-1:2003 做了下列编辑性修改：

- a) “本国际标准”一词改为“本部分”；
- b) 删除 IEC/CDV 61804-1:2003 的前言；
- c) 对文中明显错误的编号进行了纠正；
- d) IEC/CDV 61804-1:2003 的附录 E(资料性附录)的内容明显错误,给予了删除；
- e) 将 IEC/CDV 61804-1:2003 的附录 F 改为了本部分的附录 E。

本部分的附录 A、附录 B、附录 C、附录 D 和附录 E 均为资料性附录。

本部分由中国机械工业联合会提出。

本部分由全国工业过程测量和控制标准化技术委员会第二分技术委员会归口。

本部分负责起草单位：西南大学。

本部分参加起草单位：机械工业仪器仪表综合技术经济研究所、上海自动化仪表股份有限公司、中国四联仪器仪表集团、浙江大学、北京机械工业自动化研究所、上海工业自动化仪表研究所。

本部分主要起草人：刘枫、赵亦欣、黄伟、张渝、庄夏。

本部分参加起草人：冯晓升、包伟华、刘进、冯冬芹、谢兵兵、陈诗恩。

本部分为首次发布。

引言

本部分是一个最终用户驱动的基于功能块(FB)的分布式过程控制系统的需求规范。本部分及其与之相关的功能块标准(GB/T 21099.2)源自电力工业领域。本部分经过了石油和燃气、石油化工、医药和精细化工、造纸、食品和饮料、污水处理厂、冶金和其他领域中的应用的验证。对于其他工业领域,将有其他的一般需求标准和相关规范。

当前和未来的数字过程控制系统需要满足下列需求:

- 增加保密性和安全性;
- 缩短上市时间;
- 被可用的工具支持;
- 降低开发和技术支持的成本;
- 最小化培训费用;
- 支持分布式控制应用的集成;
- 支持实现的集成方法;
- 增加可维护性、可更改性、敏捷性、可升级性、灵活性、有效性、可访问性、可用性、支持工具的兼容性、多厂商设备/应用的兼容性、知识和设计的可重用性、软件组件的可重用性;
- 数字过程控制系统由数字设备组成,这些设备相互间是兼容的、可协作的、可互连的、可互操作的和可互换的。

在过程控制系统的体系结构和在生命周期所有阶段中的操作都需要满足这些需求。设计过程控制系统公认的基本概念是用 FB 描述所有必要的与实现相关的功能。FB 是提供特定功能的数据和算法的封装,它具有自主性。过程控制系统可以包含多个不同 FB 的多个实例,它们运行在提供公共服务(例如通信)以及到其他应用的接口的环境中。见图 1。

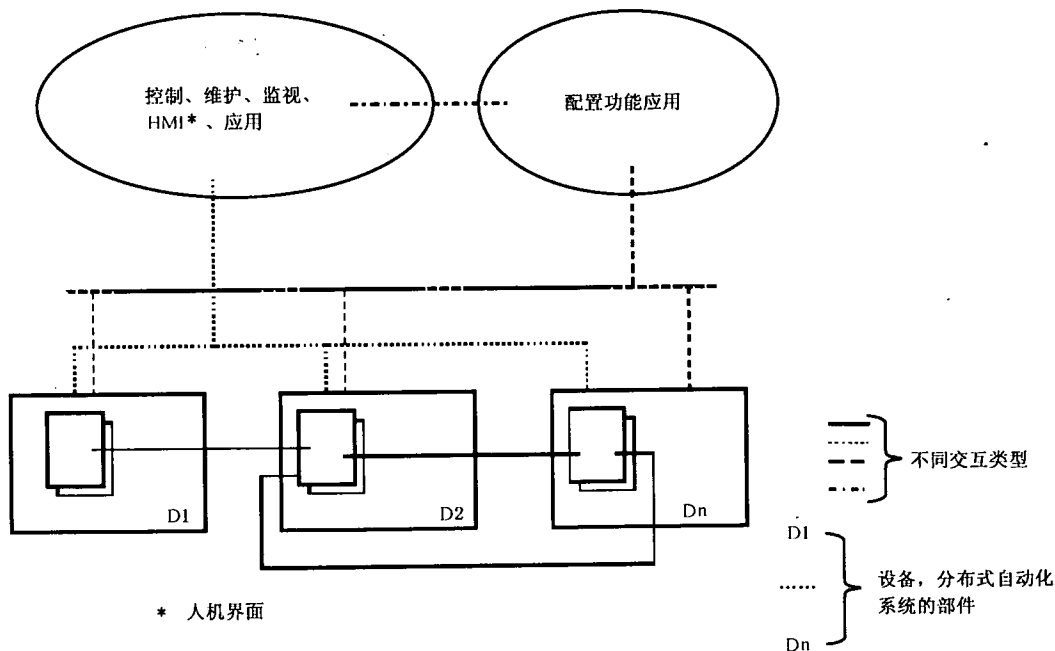


图 1 应用交互

过程控制用功能块

第 1 部分：系统方面的总论

1 范围

GB/T 21099 的本部分以通用指南的方式为供应商提供了一个规范,以满足数字过程控制系统不断发展的需求。通过本规范,用户可以确保他们所选择的设备的兼容性、可协作性、可互连性、可互操作性和可互换性。本部分给出了总的需求。为了更好地理解,本部分在附录中给出了背景信息和示例。

本部分为 FB 定义了需求,以提供控制、方便维护和技术管理的应用,这些应用与测量设备和执行机构进行交互:

- 控制包含使过程达到并保持所期望的特性的必要功能;
- 维护包含采集过程设备的状态信息和自动化设备的状态信息以及对其进行调整的功能,例如校准一个有漂移的传感器;
- 处理过程优化信息的技术管理。

主要关心的是过程和工厂设备的经济性。与安装期间工厂或设备的某项的性能和可靠性的衡量,以及与来自不同提供商,在同一操作环境中执行相同功能的某项的性能和可靠性的比较,有特别的关系。性能的示例有,来自于不同提供商的两个阀,在发生故障之前所达到的循环次数。这样,允许生成详细的、有效的统计分析,以支持决策管理和工厂设备的更改。

设计、实现和运行一个基于 FB 的过程控制系统的一个先决条件是工具、设备及其他组件遵循基于通用规范的同一体系结构。这一体系结构用来定义系统的组件,例如功能块、设备、数据、数据连接,以及这些组件之间的关系。与本部分相关的 GB/T 19769 的通用功能块模型能够提供过程控制用功能块的这些基本组件。GB/T 19769 需要补充的是在设备中实现的 FB 的参数和功能的规范。

必须规定的功能块的体系结构和范围在 7.4 中描述。7.4 含有过程工业所需的最小功能块集。它们出现在两个不同的章节,一个涉及“高级”功能块,它包含像控制回路(例如,比例、积分、微分——PID)的多数过程工业所需的复杂但通用的功能,另一个包含 EFB(Elementary FB)集,如所需的布尔函数,可组成特定的和唯一的功能性。

FB 应用于过程控制系统的整个生命周期,可以从不同方面来观察。这在附录 A 中详细说明。工艺流程设计从管道和仪表图(P&ID)开始,它以纯功能的角度给出了过程控制和仪表的需求。通过 P&ID,过程控制系统期望的特性被抽象为功能需求图(FRD),而没有考虑基本设备的详细行为。FRD 由应用块(AB)组成,AB 表示了设计阶段的数据和算法。在过程工程师和自动控制工程师(最终用户和系统集成者)进行讨论之后,通过使用市面上可用的设备及其互连以及这些设备的配置的若干设计,将 FRD 转换为应用的详细设计。这样,在 P&ID 上所示的 PID 回路将被转换为在特定现场和/或控制室设备中可实现的功能块。应当注意过程工业的许多部分,特别是那些具有许多相似和相关的简单过程的情况(例如水处理工业),并不使用 FRD 的概念或术语,而是直接从 P&ID 转换到可实现的功能块,并且使用不同的名称来描述过程和所产生的设计文档。本部分使用 FRD 的方法是因为它表示了设计阶段最正式的视图并以图解说明了在生命周期最初阶段的功能块使用。第 4 章从生命周期的角度总结了这种需求。

本部分规定了一种系统(基于分布式 FB 应用的工业过程测量和控制系统)。以体系结构、模型和生命周期来描述这种系统。体系结构是命名组件和提出系统结构的“路线图”。模型描述了组件的细节,即,它们在系统中的功能。生命周期使组件在不同的生命阶段的使用期间如何一起工作成为可见

的,即,使运行成为可见的。

图 2 以自顶向下和自底向上的角度给出了对于 GB/T 21099 的不同影响、基本规范和技术支持。

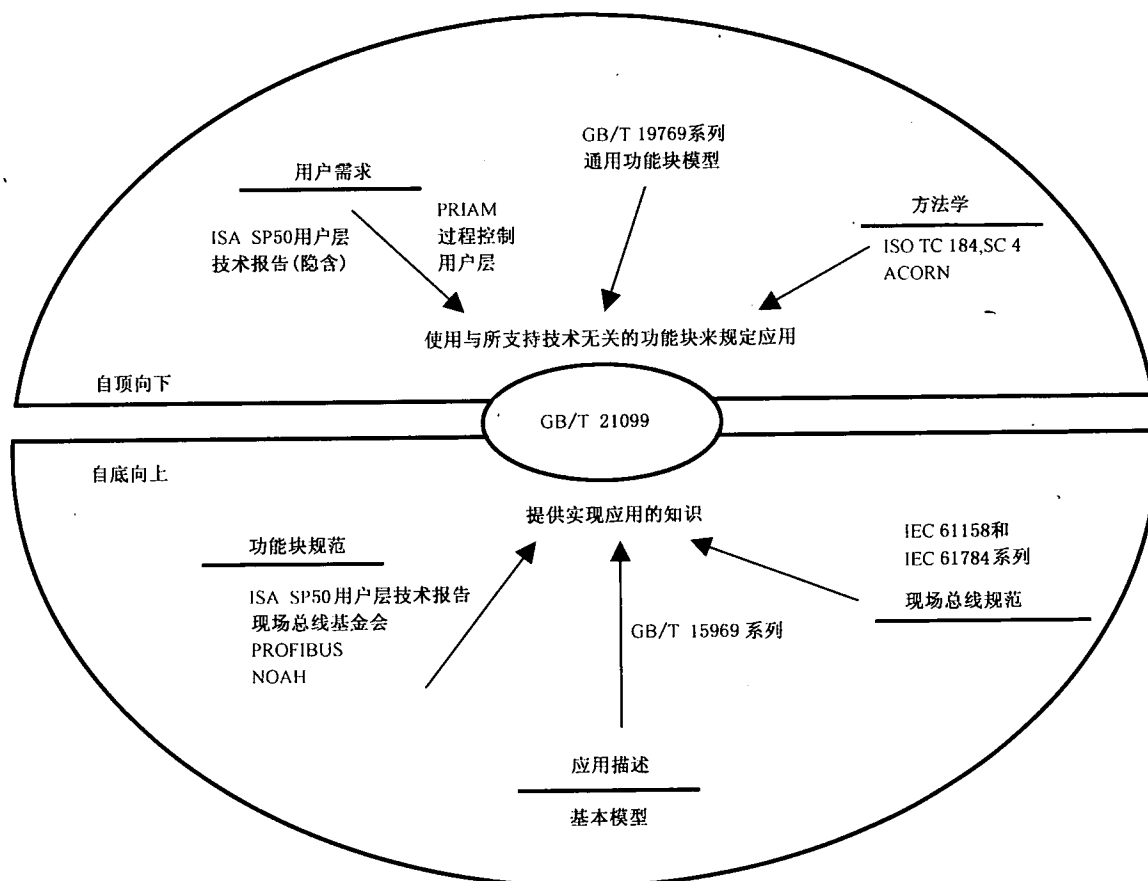


图 2 GB/T 21099 的影响

GB/T 21099 影响到涉及相同领域的国家标准和项目。这些标准或者是与技术无关的,支持自顶向下的方法;或者专注于某一技术,如可编程控制器或现场总线。两者一起构成了 GB/T 21099 所规定的标准的基础。

本部分的主要目的是使最终用户、系统供应商及设备制造商的不同角度、模型和出发点保持一致。它将是引导制定后续规范期间的讨论和指导 GB/T 21099.2 读者的参考文档。

2 规范性引用文件

下列文件中的条款通过 GB/T 21099 的本部分的引用而成为本部分的条款。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部分,然而,鼓励根据本部分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部分。

GB/T 2900.56—2002 电工术语 自动控制(IEC 60050-351:1998,IDT)

GB/T 5271.1—2000 信息技术 词汇 第 1 部分:基本术语(eqv ISO/IEC 2382-1:1993)

GB/T 5271.4—2000 信息技术 词汇 第 4 部分:数据的组织(eqv ISO/IEC 2382-4:1987)

GB/T 5271.6—2000 信息技术 词汇 第 6 部分:数据的准备与处理(eqv ISO/IEC 2382-6:1987)

GB/T 5271.8—2001 信息技术 词汇 第 8 部分:安全(idt ISO/IEC 2382-8:1998)

GB/T 5271.9—2001 信息技术 词汇 第 9 部分:数据通信(eqv ISO/IEC 2382-9:1995)

- GB/T 5271.11—2000 信息技术 词汇 第 11 部分:处理器(eqv ISO/IEC 2382-11:1987)
- GB/T 5271.12—2000 信息技术 词汇 第 12 部分:外围设备(eqv ISO/IEC 2382-12:1988)
- GB/T 5271.20—1994 信息技术 词汇 第 20 部分:系统开发(eqv ISO/IEC 2382-20:1990)
- GB/T 5271.23—2000 信息技术 词汇 第 23 部分:文本处理(eqv ISO/IEC 2382-23:1994)
- GB/T 5271.24—2000 信息技术 词汇 第 24 部分:计算机集成制造(eqv ISO/IEC 2382-24:1995)
- GB/T 5271.25—2000 信息技术 词汇 第 25 部分:局域网(eqv ISO/IEC 2382-25:1992)
- GB/T 5271.27—2001 信息技术 词汇 第 27 部分:办公自动化(eqv ISO/IEC 2382-27:1994)
- GB/T 5271.28—2001 信息技术 词汇 第 28 部分:人工智能 基本概念与专家系统(eqv ISO/IEC 2382-28:1995)
- GB/T 5271.29—2006 信息技术 词汇 第 29 部分:人工智能 语音识别与合成(ISO/IEC 2382-29:1999,IDT)
- GB/T 5271.34—2006 信息技术 词汇 第 34 部分:人工智能 神经网络(ISO/IEC 2382-34:1999,IDT)
- GB/T 9387.1—1998 信息技术 开放系统互连 基本参考模型 第 1 部分:基本模型(idt ISO/IEC 7498-1:1994)
- GB/T 15969.3—2005 可编程序控制器 第 3 部分:编程语言(IEC 61131-3:2002,IDT)
- GB/T 16682.1 信息技术 国际标准化轮廓的框架和分类方法 第 1 部分:框架(GB/T 16682.1—1996,eqv ISO/IEC TR 10000-1:1992)
- GB/T 19769.1—2005 工业过程测量和控制系统用功能块 第 1 部分:结构(IEC/CD 61499-1:2003,MOD)
- GB/T 19892.1—2005 批量控制 第 1 部分:模型和术语(IEC 61512-1:1997,IDT)
- IEC 61784:2001 测量和控制数字数据通信 工业控制系统用现场总线 连续和离散制造业的规范装置
- EN 50170:1995 通用现场总线通信系统

3 术语和定义

下列术语和定义适用于 GB/T 21099 的本部分。

3.1 基本定义

3.1.1

接口 interface

根据功能特性、信号特性或其他特性作相应定义的两个功能单元之间的共享界面。

[GB/T 2900.56—2002,351.11.19]

3.1.2

系统 system

在限定范围内被看成是一个整体并与周围环境隔离的一组相互关联的元件。

[GB/T 2900.56—2002,351.11.01]

注 1: 此类元件可以是物体,也可以是概念和概念的产物(如:体系结构、数学方法、编程语言)。

注 2: 系统被认为由一假想面使之与周围环境及其他外部系统隔开,切断该系统与周围和外部系统之间的联系。

3.1.3

数据类型 data type

值的集合及其允许的操作的集合。

[GB/T 5271 系列]

3.1.4

数据连接 data connection

功能单元之间为传递数据建立起来的联系。

[GB/T 19769.1—2005, 1.3.2.22]

3.1.5

数据 data

事实、概念或指令按某一格式化方式的一种表示,适用于人或自动装置进行通信、解释或处理。

[ISO 修订¹⁾]

3.1.6

功能单元 functional unit

能够完成特定任务的硬件或软件或两者的实体。

[GB/T 5271 系列]

3.1.7

硬件 hardware

相对于程序、过程、规则和有关文档编制而言的物理设备。

[ISO/AFNOR 计算机科学词典]

3.1.8

映射 mapping

一种与另一集合中的量或值具有确定对应关系的所有值的集合。

[GB/T 5271 系列]

3.1.9

参数 parameter

一种为专用应用程序而给定一个常数值的变量,而且它可以表示该应用程序。

[GB/T 5271 系列]

3.1.10

算法 algorithm

为在有限操作步数内求解问题而明确定义的规则的有限集合。

[GB/T 19769.1—2005, 1.3.2.5]

3.1.11

应用 application

为解决工业过程测量和控制中的问题的特定软件功能单元。

注:一个应用可以分布在多个资源中,并可与其他应用通信。

[GB/T 19769.1—2005, 1.3.2.6]

3.1.12

应用块 application block

在一个 FRD 中用于表示一个或多个(高级)功能块的设计模式。

3.1.13

属性 attribute

实体的特性或特征。例如,功能块类型规范的版本标识。

[GB/T 19769.1—2005, 1.3.2.7]

注:为了得到可互操作性,应规定属性的形式化描述。GB/T 19769.1—2005 并不规定像 FB Type-Info 那样的某些

1) 凡是后面带有标注[ISO 修订]的定义表示该定义出自“ISO/AFNOR Dictionary of Computer Science”并且已被修订。

属性。GB/T 19769.1—2005 给出了定义属性的一般规则,GB/T 21099.2 则为过程控制规定了像那些可以规定其自身的其他类型的属性。规则要避免出现非唯一的属性名。

3.1.14

配置(系统或设备) configuration(of a system or device)

系统设计中的一步:选择功能单元、指定它们的位置并且定义它们的互连。

[GB/T 19769.1—2005,1.3.2.17]

3.1.15

设备 device

独立的物理实体。具有在特定环境中执行一个和多个规定功能的能力,并由其接口分隔开。

[GB/T 19769.1—2005,1.3.2.26]

3.1.16

设备管理应用 device management application

其基本功能是管理设备内多个资源的应用。

[GB/T 19769.1—2005,1.3.2.27]

3.1.17

基础 FB elementary FB

提供具有异常处理能力的逻辑-数学功能的一种 FB 或功能。

注:FRD 中使用的 EFB 和在运行应用中的 FB 可能有区别。

3.1.18

实体 entity

特定的事物,如:一个人、地点、过程、对象、概念、联系或事件。

[GB/T 19769.1—2005,1.3.2.28]

3.1.19

事件 event

瞬时发生的事情,对算法执行的调度有意义。

[GB/T 19769.1—2005,1.3.2.29]

注:算法的执行可以使用与事件相关的变量。

3.1.20

异常 exception

导致正常执行中止的事件。

[GB/T 19769.1—2005,1.3.2.35]

3.1.21

执行 execution

完成算法规定操作序列的过程。[ISO]

注:被执行的操作序列随功能块实例调用的不同而不同,取决于功能块算法规定的规则和功能块数据结构中变量的当前值。

[GB/T 19769.1—2005,1.3.2.36]

3.1.22

功能 function

实体的特定目的或它的特有活动。

[GB/T 19769.1—2005,1.3.2.42]

3.1.23

功能块(功能块实例) FB(FB instance)

由相应功能块类型规定的数据结构的一个独立的、有副本和相关操作所组成的软件功能单元。

注:功能块典型的操作包括在相关数据结构中数据值的修改。

[GB/T 19769.1—2005, 1.3.2.43]

3.1.24

实现 implementation

使系统的硬件和软件成为可运行的开发阶段。

[ISO 修订]

3.1.25

输入变量 input variable

由数据输入提供其值的一种变量,可在功能块的一个或多个操作中使用。

注: GB/15969.3—2005 中定义的功能块输入参数是输入变量。

[GB/T 19769.1—2005, 1.3.2.48]

3.1.26

实例 instance

由带有所定义类型的属性的独立、有名实体组成的功能单元。

[GB/T 19769.1—2005, 1.3.2.49]

3.1.27

实例名 instance name

与实例相联系,并标明该实例的标识符。

[GB/T 19769.1—2005, 1.3.2.50]

3.1.28

实例化 instantiation

规定类型的实例的创建。

[GB/T 19769.1—2005, 1.3.2.51]

3.1.29

内部操作(功能块) internal operations (of a FB)

与功能块算法相关的操作,带有其执行控制或相关资源的功能性。

[GB/T 19769.1—2005, 1.3.2.52]

3.1.30

内部变量 internal variable

值由功能块的一个或多个操作使用或修改,但不由数据输入提供也不提供给数据输出的一种变量。

[GB/T 19769.1—2005, 1.3.2.53]

3.1.31

调用 invocation

启动算法所规定的操作序列执行的过程。

[GB/15969.3—2005 修订]

3.1.32

管理功能块 management FB

基本功能是管理资源中的应用的功能块。

[GB/T 19769.1—2005, 1.3.2.56]

3.1.33

管理资源 management resource

基本功能是管理其他资源的资源。

[GB/T 19769.1—2005, 1.3.2.57]

3.1.34

模型 model

真实世界中过程、设备或概念的表示。

[GB/T 19769.1—2005, 1.3.2.60]

3.1.35

操作 operation

一种完全明确的动作,该动作作用于任何已知实体的允许组合时,产生一个新的实体。

[GB/T 2900.56—2002]

3.1.36

输出变量 output variable

其值由功能块的一个或多个操作建立并提供给数据输出的变量。

注: GB/T 15969.3—2005 中定义的功能块的输出参数是输出变量。

[GB/T 19769.1—2005, 1.3.2.60]

3.1.37

资源 resource

一种有独立的操作控制的功能单元,为应用提供多种服务,包括算法的调度和执行。

注1: GB/T 15969.3—2005 中定义的 RESOURCE 是一种编程语言元件,与上述定义的资源相对应。

注2: 一个设备包含一个或多个资源。

[GB/T 19769.1—2005 修订]

3.1.38

资源管理应用 resource management application

主要功能是管理单个资源的应用。

[GB/T 19769.1—2005, 1.3.2.66]

3.1.39

调度功能 scheduling function

选择要执行的算法和操作并启动和终止其执行的功能。

[GB/T 19769.1—2005, 1.3.2.70]

3.1.40

服务 service

资源可使用的功能性,可以用服务原语序列来模型化。

[GB/T 9387.1—1998 修订]

3.1.41

软件 software

知识产物,包含与系统操作有关的程序、过程、规则以及任何相关的文档。

[ISO 修订]

3.1.42

事务 transaction

将来自请求者的请求或可能的数据传送到响应者并且也可将来自响应者的响应或可能的数据传回到请求者的服务单元。

[GB/T 19769.1—2005, 1.3.2.79]

3.1.43

类型 type

规定所有该类型实例所共享的公共属性的软件元件。

[GB/T 19769.1—2005, 1.3.2.80]

3.1.44

类型名 type name

与类型相联系,并标明该类型的标识符。

[GB/T 19769.1—2005, 1.3.2.81]

3.1.45

变量 variable

在不同时间可具有不同值的软件实体。

注1:变量的值通常限于某种数据类型。

注2:变量可分为输入变量、输出变量和内部变量。

[ISO 修订]

3.2 基于 IA/IM-通道的定义

3.2.1

执行(测量)通道 actuation(measurement) channel

按照用户需要完成每一执行(测量)所需的所有各项的总和。其物理组成从过程的附属装置一直延伸到阀门、电机、执行机构(传感器、变送器)、网络、计算机中的补码处理。

注:IA/IM-通道表示对每一需要的执行/测量的所有需求的智能执行/测量的解决方案。智能在这里表示按照用户需要提供所有的功能性。

3.2.2

系统(或通道或设备)状态 system(or channel or device) status

相关项(系统或通道或设备)的实际状况。换句话说,系统划分为几个层次:整个系统、系统的每一IA/IM-通道、构成通道的每个设备。

注:详细说明见6.2。

3.2.3

有效性指数 validity index; VI

附加在信息上的限定词,可以作为质量指数。

注:详细说明见6.3。

3.2.4

测量的不确定度 measurement uncertainty

与实际测量结果相关的一个参数,它表征了值的离差,这种离差可能是由测量引起的。

注1:“不确定度”这个词表示“怀疑”,因此“测量的不确定度”最明确的含义就是表示对测量结果的正确性和精确性的怀疑程度。

注2:例如,不确定度可以是标准偏差或置信区间的宽度。

注3:不确定度可以用一个可数学处理的数据来表示,如果其组成部分的直接测量的不确定度已知,则间接测量的不确定度可以计算出来。

3.2.5

行规 profile

一个或多个基本标准和/或国际标准行规(ISP)的集合,以及适用范围、所选分类的标识、一致性子集,这些基本标准的选项和参数,或实现特定功能所需的国际标准行规。

[GB/T 16682.1]

注:国际标准行规可以包含除国际标准之外的规范性引用文件。

3.3 缩略语

AB

应用块(Application Block)

AME

应用管理实体(Application Management Entity)

CHD	控制层次图(Control Hierarchy Diagram)
DCS	分布式控制系统(Distributed Control System)
DFBAP	分布式功能块应用进程(Distributed FB Application Process)
EFB	基础 FB(Elementary FB)
FB	功能块(Function Block)
FRD	功能需求图(Functional Requirement Diagram)
HMI	人机界面(Human Machine Interface)
IA/IM-channel	IA/IM-通道(Intelligent Actuation/Intelligent Measurement-channel)
ISP	国际标准行规(International Standard Profile)
MIB	管理信息库(Management Information Base)
MGT	管理(Management)
PFD	工艺流程图(Process Flow Diagram)
PID	比例、积分、微分(Proportional, Integral, Derivative)
PRIAM	智能执行和测量的预规范需求 (Prenormative Requirements for Intelligent Actuation and Measurement)
P&ID	管道和仪表图(Piping & Instrumentation Diagram)
SCADA	监督配置和数据采集(Supervision Configuration And Data Acquisition)
SM	系统管理(System Management)
ST	结构化文本(Structured Text)
VI	有效性指数(Validity Index)

4 工程需求

4.1 概述

本章期望读者具有某些分布式 FB 系统的工程知识。背景信息可参阅附录 A。它通过设计、工程、运行支持和维护从概念上为读者给出了面向控制系统的 FB 的生命周期的概述。这些阶段的每一个都有实际 FB 实体的不同环境和自身特定的需求。

4.2 设计阶段的需求

- a) 要识别作为特定功能需求图(FRD)中的一部分或分布式现场设备系统中某些应用块(AB)的一部分的 FB,要求 FB 能够带有特定 FRD 块的标识。

注:要求是一个可被称为 STRATEGY 的参数。基于这一参数的工程系统可以识别分布式的 FB,为了逆向工程的目的,这些功能块在 FRD 中被组合成一个 FB。

- b) 为了识别 FB 类型,需要类型名。要求类型名在库中是唯一的,但是可以有多个实例。通过这一信息,工程工具可以导向一个联机帮助文件。
- c) 为了识别拥有一个或多个 FB 的设备,需要一个设备类型标识符,以允许设备描述类型到该设备类型的连接。为了在设计阶段支持可交换性,要求设备类型标识符基于行规而不是提供商的特定类型。
- d) 要求设备类型的图形表示在设备描述中作为选项被引用。这种图标并不用于 FB 图表或 P&ID 中,而只用于现场设备的拓扑图中。在本部分中对这种表示没有要求。
- e) 为了识别控制层次图(CHD)中的元素,这些元素与 IEC 61512-1 批处理过程兼容,要求根据该批处理标准来定义某些参数。

示例:

FB 带有这些参数。FB 内没有必须的算法。EFB 不带这些参数;

- 1) 处理 ID(BATCH_ID);

- 2) 单元过程或单元处方号;
 - 3) 操作处方号;
 - 4) 阶段处方号。
- f) 要求调度功能支持 FB 的循环时间片调用。
- g) 对现场设备以及它们的基于 AB 的 FB 没有要求。
- h) 要求 EFB 被定义并集中在一个库中,一个 EFB 是一种重复的数学-逻辑处理,嵌入在 FB 中或者嵌入在 GB/T 15969 系列标准定义的功能中。EFB 是限于过程控制域的处理模块。EFB 不能被拆分。要求所有的 FB(不是功能)都带有库名。FB 名和库名的组合是功能块唯一标识符。这意味着,当在混合了 FB 分支或应用特定库的设备中,实例化 FB 类型的时候,为了识别该 FB 类型,可将其识别为 IEC EFB,这对于版本控制,连接到在线帮助等是必要的。EFB 行为的规范化内部描述要求使用 GB/T 15969.3—2005 规定的语言,如结构化文本语言(ST)、梯形图或指令列表(Instruction List)。ST 中缺少的元素必须用一些语句来编程,并且对于实例的异常处理结果可能引入附加的参数。
- i) 有必要通过选择 EFB 的动态参数来组成人机界面。人机界面建立了可视化过程、允许改变参数操作和储存数据的信息基础。对于这种选择,GB/T 15969 系列标准中没有语法定义。对于过程控制的属性,作为 GB/T 15969 的补充在结构化文本语言定义的注释字段中被定义。
- j) 对于维护和技术管理工具,有必要规定或预定义 EFB 的参数属性和 FB 属性。对于这种选择,GB/T 15969 系列标准中没有语法定义。对于过程控制的属性,作为 GB/T 15969 的补充在结构化文本语言定义的注释字段中被定义。

5 关于兼容性等级的定义

5.1 概要

在基于 FB 的设备之间存在着某些兼容性等级和协作的一致性等级,这些等级依赖于定义明确的通信和应用特征。见图 3 和表 1。



图 3 功能设备兼容性等级

用于兼容性等级定义的主要特征如下:

表 1 功能性特征

特征	描述
通信行规	
通信协议	该特征由 OSI 参考模型的 1~7 层的所有协议来定义,即,从物理媒体访问到应用层协议。
通信接口	该特征由包含了服务和参数参数的应用层通信服务定义来定义。可能需要其他的映射机制。通信系统的动态性能是该特征的一部分。
应用行规	
数据类型	该特征由块的数据输入、数据输出或参数的数据类型来定义。
参数语义	该特征由数据的典型特征来定义,它可以是数据名、数据描述、数据范围、数据的替代值、默认值、失电和恢复电源后的数据保持。
应用功能性	该特征由块内变量间的遵从关系和一致性规则来定义,并在数据描述部分或在单独的特性部分中完成。
动态性能	该特征由时间约束来定义,时间约束影响数据或一般的设备特性。例如,过程值的更新速率影响到块的算法

关于这些功能特征,以下的兼容性等级名称用于设备的分类。用于分布式功能块应用的本部分为来自不同制造商的使用功能块的设备提供了(但并不要求)共存性、可互连性、可协作性、可互操作性和可交换性。这就允许用户去选择一个设备作为新系统的一部分或作为替换,并理解这种选择的结果。

5.2 不兼容性

指在同一分布式应用中两个及多个设备无法一起工作。

注:应用的功能性、数据语义、数据类型、通信接口,甚至受影响设备所使用的通信协议的差异可能导致不兼容。如果不兼容设备置于同一分布式应用网络中,可能会干扰或妨碍相互间的正常通信或功能(甚至可能是破坏性的)。

5.3 共存性

指两个或两个以上的设备,不论是否是同一制造商,在同一通信网络中相互独立地运行,或使用相同通信协议的部分或全部一起运行,而不影响网络上其他设备的功能。

注:对于通信服务至今还没有一个共识,为了使共存设备在同一分布式应用中一起工作,通常需要在一方或两方设备中进行应用和系统的特定编程。

5.4 可互连性

指两个或两个以上的设备,不论是否是同一制造商,使用相同的通信协议和通信接口互相一起运行的能力。

注:这些设备允许交换数据类型不一致的数据,数据类型的转换可能需要。为了使可互连的设备在同一分布式应用中共同发挥作用,通常需要在一方或两方设备中进行统一的应用特定的编程。

5.5 可协作性

两个或两个以上的设备,不论是否是同一制造商,在拥有数据输入、数据输出和参数等数据类型的设备间支持设备参数传送的能力。

注:如果一个设备被另一制造商类似的设备所替换,可能需要对应用重新编程。在实现时必须设计分布式应用,以考虑所使用的可协作设备的特有的功能性和动态响应。

5.6 可互操作性

两个或两个以上的设备,不论是否是同一制造商,在一个或多个分布式应用中一起工作的能力。数据输入、数据输出、参数、它们的语义和每一设备相关功能性的应用程序定义之后,如果任一设备被另一制造商类似的设备所替换,除了动态响应可能会有不同之外,包括被替换设备的所有分布式应用仍会如替换前一样继续运行。

注:当现场设备和系统两者都支持同一标准的强制和可选部分的相同组合时,可获得可互操作性,在现场设备或系统中来自不同制造商的特有的扩展会妨碍可互操作性。

5.7 可交换性

两个或两个以上的设备,不论是否是同一制造商,在一个或多个分布式应用中使用相同的通信协议和接口一起工作的能力,每个设备的数据和功能性定义之后,如果任一设备替换,包括被替换设备的所有分布式应用仍会如和替换前一样继续运行,包括同样的分布式应用的动态响应。

6 功能需求

6.1 概要

以下表述的功能需求定义在一个适当的抽象层面上,以便最终用户和提供商都能很好地理解。

这一抽象层面不同于由提供商和系统集成商直接使用的 FB 抽象层面。

本部分定义的“功能需求”和 GB/T 21099.2 所定义的 FB 概念之间不必是一一对应的关系,可以是一对一,一对多或多对一。

在每一功能模块的定义中,对于这里的描述所包含的功能需求部分,需要提供一个清晰的关系。

要完整地理解和使用以下需求需要先阅读附录 B。

设备功能需求明确地描述了现场设备(如传感器、变送器等)中的测量通道。要求执行通道的现场部分(如阀门、执行机构、定位器等)具有相似的需求。

6.2 系统(或通道或设备)状态

原则上,状态有三种主要的值(如图 4 所示),适合的项(item)为:

- a) 有效性;
- b) 可接受的下降;
- c) 退出服务(不可接受的下降)。

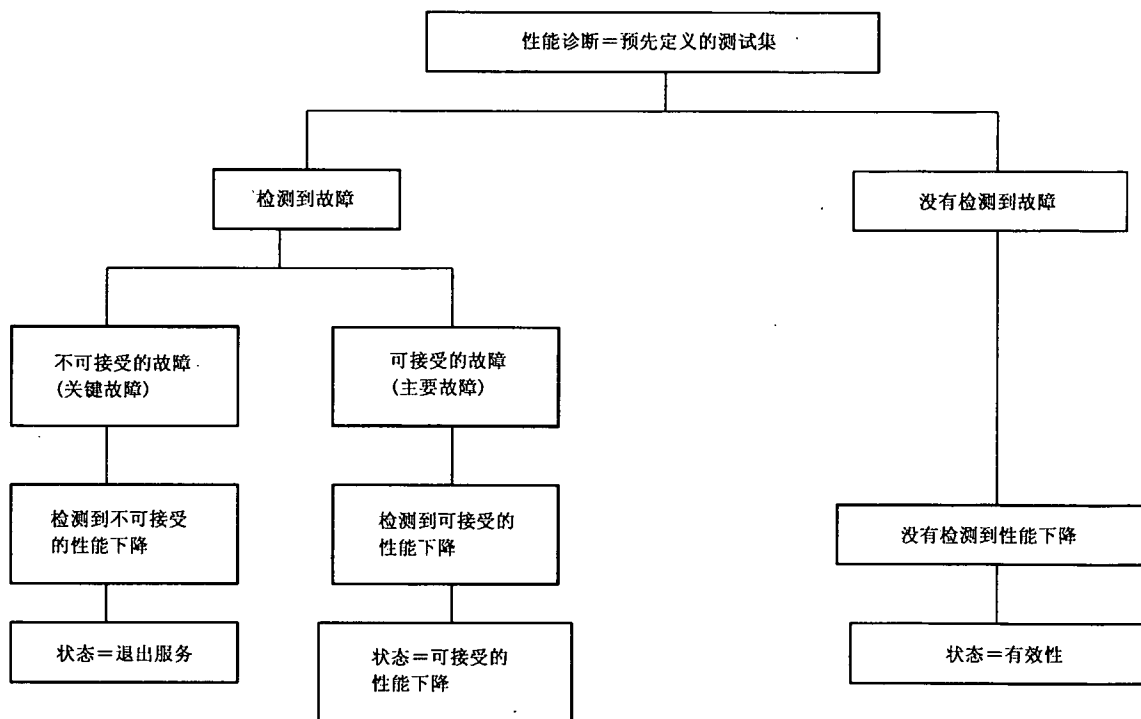


图 4 系统(或通道或设备)状态

下降定义为系统(或设备)的用户根据自己特定的需要和支持的诊断,认为是可以接受的(一些)性能降级。

就实际用途来说,用户需要这一状态的两种信息:只有一个的“综合状态”和几个“详细状态”,每一“详细状态”针对不同操作员的每一任务的需要。

a) 综合状态

综合状态表明了装备(设备或系统或通道)执行所需功能的实际能力,这一信息用以支持用户为了系统的控制、维护和技术管理而指定的直接动作。

b) 详细状态

详细状态信息为系统(或设备)维护和技术管理提供所需的明确详细的诊断信息。从用户角度看,至少要包含如下三种所需的信息:

- 1) 记录每一可替换组件的行为的详细信息,用于指导对该组件的干预;
- 2) 帮助诊断故障部分的信息并提供正确修复故障部分(这种诊断通常要求更详细的信息被记录)的有用的所有详细信息;
- 3) 同 b)1)和 2),但此处是,为了技术管理的目的,正确判断每个组件行为所需的详细信息。

6.3 有效性指数(VI)

质量是相对的质量,是以达到预先定义的要求为基础来评价的,这些要求是为产生信息的通道的属性所定义的。质量标准的基本集被认为是:

- a) 精确性和不确定性标准(测量中的不确定性参见 ISO Guide);
- b) 及时标准;
- c) 好/差标准;

在实际实施中,必须明确地陈述用来产生 VI 的标准。

VI 的目的是允许合格信息的即时并且正确的使用。

考虑到生产信息的整个通道的实际诊断和验证的结果,VI 要实时产生。因此,当故障被检测到并改正后,VI 使信息的使用者,对不同操作条件,正常和异常,导致的实际情况(决定性 VI)有明确的认识。

6.4 信号处理

产生原始测量和数据的功能,这些测量和数据作为测量信息处理和设备管理的输入。

- a) 传感器限定阈值(专用于故障管理支持的诊断);
- b) 传感器量程;
- c) A/D 转换器控制;
- d) 数据质量的决定(硬件诊断的结果导致的 A/D 转换之后,VI 与原始测量关联);
- e) 影响量的补偿(硬件);
- f) 过程附属装置和传感器诊断(运行时自动测试);
- g) 支持按需的维护测试。

6.5 测量信息处理

6.5.1 概述

它处理由测量信号处理所提供的信息。

信息处理组件的主要目的是提供更高级的测量通道,这种通道带有与测量处理紧密关联的 VI。要求知道由测量设备传递的测量和验证信息的完整语义。(要求知道参与处理的所有功能单元。)

验证是测量处理的一个本质部分,它决定测量处理的每一步所转递的测量的可信度。为了允许测量信息正确地用于其涉及的内容,通过在每一步处理中递增而获得的验证信息,是测量本身的一个基本部分。

另一个重要的方面是,通过 VI 和设备状态的使用,设备可以工作在降级的条件下,由更高级的管理来决定数据的使用。从这种意义上讲,变送器的容错特性包括了故障诊断以及对测量(VI)和设备性能(设备状态)的削弱程度的指示。

测量信息处理必须包含的功能在此后给出。

6.5.2 容错行为处理

故障的识别和限制。有利于相应测量 VI 处理的信息。

6.5.3 VI 处理

a) 测量验证

这个处理是随测量处理的每一阶段一道完成的,不是独立的。这样可以保证数据和 VI 之间的一致性。

可能包括对时间冗余的处理,这种处理是基于在为应用程序定义的采样周期中,连续抽取相同数量的许多连续采样之间的比较之上的。

b) 不确定性处理

参数(不确定性)可能是,例如,标准的偏差(或给定的倍数),或一个确定置信级区间的半个宽度。

一般地说,测量的不确定性包含许多组成部分。其中的一部分可由系列的测量结果的分布统计来评估,并且可由实验标准偏差来表征。其他部分,也可以由标准偏差表征,可以通过基于经验或其他信息的假设概率分布来评估。测量结果是被测值的最佳估计,不确定性的所有组成部分都促成离差的产生,包括那些系统效应引起的部分,如与校正和参考标准相关联的部分。

6.5.4 测量通道处理功能

- a) 标度转换;
- b) 线性化;
- c) 影响量补偿(软件);
- d) 滤波;
- e) 转储;
- f) 工程单位转换;
- g) 限制阈值(关于处理警报应用)和所有相关数据的处理;
- h) 变送后的测量处理;
- i) 测量时间戳;
- j) 测量安全值(通常将最后有效值复制给采样);
- k) 测量趋势处理。

注:可能存在其他的功能。

6.6 设备诊断和测试支持

6.6.1 概述

以下条款涉及到产生与设备状态相关的信息的功能。

6.6.2 设备诊断

- a) 加电自检;
- b) 运行自检。

6.6.3 维护相关处理信号和计算所有对执行设备降级分析有用的事件

目的是允许能够预见设备整体降级或部分降级的算法在维护系统中执行。制造商有必要定义重要的参数并在设备中包括必要的 FB。这些 FB 能够识别这些情况,并将它们的发生信息报告给维护系统和技术管理系统。

已发现的这些有用的参数示例包括:

- a) 耗费在额定工作条件之外的操作时间(通过如温度限制、压力限制等来定义);
- b) 异常事件的数量(如 P、DP 变送器的压力峰值);

c) 已定义特性的电子冲击量。

注：可能还存在其他的参数。

6.6.4 按需测试的支持(远程或本地发起)

由于执行和测量远程或本地测试(如,校准)的需要,这种支持分为以下两类:

- 介入测试:这类测试的执行会干扰设备/通道的正常操作(例如,要求关闭过程的附属装置);
- 非介入测试:这类测试的执行不会干扰设备/通道的正常操作。

根据请求的测试,需要必要的授权,并且必须将设备/通道置于相应的操作模式。

要求的功能性有:

a) 介入设备测试执行:

1) 对校准过程的支持(支持基本的和变换的测量)

该项功能的目的在于给予负责设备校准的维护操作员最大的帮助。当对许多不同制造商的许多不同设备进行校准时,可通过以下途径获得所需的帮助:

- 使用已经可用的标准术语;
- 应用可应用的标准过程;
- 直接利用电子表格形式的校准报告和结果,以便通过网络或电子支持传送到维护系统。

2) 对照参考输入的测量处理测试;

3) 过程附属装置的介入诊断测试。

b) 非介入设备测试执行

1) 过程附属装置的非介入诊断测试;

2) 对照参考输入的测量处理测试(如果在控制操作员同意的时间段内的运行时是可执行的,如一段时间的冗余部分测试)。

c) 测试结果检索

1) 设备测试结果的检索(相关信息:自诊断,测试结果和维护干扰);

2) 关于自诊断直接可用的实际信息,测试结果和维护干预采用电子表格形式,以便通过网络或电子支持传送到维护系统。

6.7 本地接口附属装置

通过合适的终端,本地可以获得:

- a) 访问权限管理功能(见 6.8.10);
- b) 信息的预定义列表;
- c) 预定义命令输入;
- d) 所要求的本地访问,以支持现场操作者的干预。

6.8 设备(系统和通道)管理

6.8.1 概述

以下的功能是系统管理员和设备管理功能协作活动的预期结果。当然,设备代理管理员的作用属于设备功能单元。

从这点来看,一个通道就是一个子系统。

6.8.2 设备标识功能

- a) 与供应商相关的设备信息检索。设备用户所需的,沿着其生命周期与设备发生交互的信息(如设备组件的零件登记号、材料、软件和硬件版本、工作范围等)。
- b) 与用户相关的设备信息检索(通常在试运行期间所撰写的补充信息,如设备标记、安装日期等)。

上述信息是在设备生命周期的相关阶段,由供应商操作员和试运行操作员用以下功能写入设备的:

- c) 与供应商相关的设备信息修改。
- d) 与用户相关的设备信息修改。

6.8.3 配置功能(和系统配置的帮助)

当变送器可编程时,变送器的处理和采集部分的特定功能的软件,必须从配置系统中下载。例如,如果一个 DP 变送器作为液位或流量传送仪使用时,需要下载特定的软件。当然,这种逻辑动作可能需要几个实际的操作(如 EPROM 替换,预装功能的选择等)。

配置包括支持不同任务所需的所有软件组件。这些任务被赋予变送器,如测量、诊断、测试例程等。特定用户的需求是指按需报告的可用性,允许操作员检查实际的配置(与指定配置相对的一致性检查)。在设备的生命周期中,不同用户可利用以下的功能:

- a) 供应商配置修改;
- b) 用户配置修改(从可用的功能中选择所需的功能);
- c) 配置检索;
- d) 读取可用的功能;
- e) 读取供应商配置修订;
- f) 读取用户配置修订;
- g) 读取已选择的(活动的)功能。

6.8.4 参数化功能

为了满足工厂的应用,该功能主要在于设定参数,以完整地定义通用的功能。

处理功能参数化取决于在配置期间选择/下载的功能;要求将这些参数保存为非易失参数,并且要求不断地检查它们的完整性。

设置的参数有,如范围、被测变量的偏移量和工程单位、警告和报警级别、采样频率,滤波时间常量等。特定用户需求是指可用的需求报告,允许操作员检查实际的参数化(与指定参数化的一致性检查)。

设备参数分为以下两类:

- 介入参数:这些参数的修改会干扰设备的正常操作;
- 非介入参数:这些参数的修改不会干扰设备的正常操作。

根据请求的参数修改,需要必要的授权,并且必须将设备/通道置于相应的操作模式。

要求的功能有:

- a) 介入设备参数化修改(单个的参数/已定义组的参数);
- b) 非介入相关设备参数化修改(单个的参数/已定义组的参数);
- c) 设备参数化检索。

6.8.5 测量管理功能

该功能是设备管理的一部分,它与系统管理的关系将在接下来的部分予以阐明。

该功能产生每种测量执行时序所需的适合的执行事件。通过合适的网络机制,系统管理员产生几个设备管理员之间的同步。

测量管理功能根据需要产生以下的服务:

- a) 周期异步测量(即,没有同步于系统参考时间)的执行事件。
它是测量所需的执行事件。这种测量的使用是周期性、异步的。在保证特定应用的数据一致性所必需的时间内,对于所有的用户该测量都是周期性可用的。
周期同步测量(即,同步于系统参考时间)的执行事件。
它是测量所需的执行事件。在接收到同步命令后,这种测量的使用是周期性、同步的。在特定应用所需的时间内,对于所有的用户该测量都是可用的。
- b) 具有异步启动和停止的周期测量。
它是测量所需的执行事件。这种测量的使用是周期性、异步的。在保证特定应用的数据一致

性所需时间内,对于所有用户该测量都是周期性可用的。

测量的获取和分发不是连续的,而是在特定命令后启动,或在某个异步事件后停止。

c) 按需测量的执行事件。

在用户发出一个特定命令后,获取该测量。在测量的用户发出数据请求命令后,该测量是可用的。

d) 检测逻辑值变化的执行事件。

e) 二进制数据值改变的事件通知。

6.8.6 系统时间管理功能

系统时间管理功能是协调每个设备的几个时间管理器的工作。

在一些应用中,例如,要求带有时间戳的测量和/或带有绝对时间信息的事件。要求系统(主)时钟和所有的设备都有一个与主时钟保持同步的内部时钟。通过明确定义的时钟精度和网络同步操作来保证应用要求的精度。

系统时间管理功能协调几个设备的管理员,以共享:

a) 绝对时间,具有被要求的精度(典型为 1 ms);

b) 相对时间,具有被要求的精度(典型为至少 1 ms);

c) 时间同步命令,由主时钟以已定义的速率传送,以保证所要求时间的精确性。

6.8.7 及时确认支持

该功能检查通过通信接口传送或接收的数据总是具有指定的时间性。

这个处理有助于数据验证的处理。

6.8.8 设备故障管理

设备故障管理用于支持设备故障的适当管理。

a) 故障检测

它适当考虑设备诊断和测试支持所提供的所有详细诊断信息。使用这些信息来执行故障检测活动,并生成内部活动所需的,由测量通道状态管理功能处理的设备状态(设备详细状态和设备综合状态)。测量通道状态管理功能处理所有的这些信息,将应用要求的信息提供给不同的用户。它是适应最终用户的。

b) 设备判定(容错过程)

在接收到管理高层的请求后,或者在设备内部自动激活后,它执行内部程序来限定检测到的故障(以防局部的故障引起系统的故障)。

它包含处理传感器和过程附属装置可能的冗余的过程。

6.8.9 操作管理功能(访问权限管理的扩展)

它是管理在几种操作模式之间转换的系统管理功能。特别地,它管理不同的人或自动操作员之间的资格转换过程。这样就可以支持现场设备的干预过程,以实现人类组织所认可的干预计划。当然,要实现上述功能,设备管理需要和系统管理协作。

由于设备中嵌入了智能以及设备之间新的通信方式,可以简化以前在工厂中使用纸质文档实现操作管理的过程。

对于每一个操作员和分布式系统之间的交互,要求设备管理使能所需的设备功能,禁止其他的功能。必须建立管理过程,将资格赋给不同的操作员,以访问在需求达成一致的基础上定义的功能或设备。这样可以防止未授权特性和可能的错误(见访问资格 qualification access)。

根据几种需要的交互来定义的、由系统管理支持的典型操作模式有:

a) 远程自动控制(相关操作员:控制设备);

b) 远程手动控制(相关操作员:远程控制操作员);

c) 本地(手动)控制(相关操作员:本地控制操作员);

- d) 远程维护(相关操作员:远程维护操作员);
- e) 本地维护(相关操作员:本地维护操作员);
- f) 远程试运行(相关操作员:远程试运行操作员);
- g) 本地试运行(相关操作员:本地试运行操作员);
- h) 参数化(相关操作员:参数化操作员);
- i) 自身(相关操作员:无;设备与现场总线失去连接)。

注:还可能存在其他的操作模式。

6.8.10 访问权限管理功能

访问权限管理功能检查对正常设备功能的每个访问的资格。

在每一操作模式中,设备自身会授权哪些操作员可以在设备上执行某种预定义的活动。

很明显,例如,当要求测量处理功能为活动(如在控制操作模式中)时,禁止配置、参数化和按需测试对设备的写访问是非常重要的。

这项设备需求是系统级相应需求的补充。

7 功能块应用需求

7.1 系统概述

前面部分是从终端用户的角度来描述的系统需求。本条从体系结构的角度来关注系统。

过程控制系统是控制过程的应用(基于 FB 的应用)、执行维护的应用、监控、HMI、试运行功能和设备中硬件及应用软件配置功能的应用的结合,也称为系统管理功能,见图 5。通过 FB 应用执行过程控制的设备必须提供允许在 FB 设备之间进行交互的所有功能和可互操作的的外部应用。因此,必须定义系统和设备的组成部分以及它们的关系。本条只涉及基于 FB 的设备。设备和系统的体系结构是基于 GB/T 19769.1—2005 中的定义之上的。

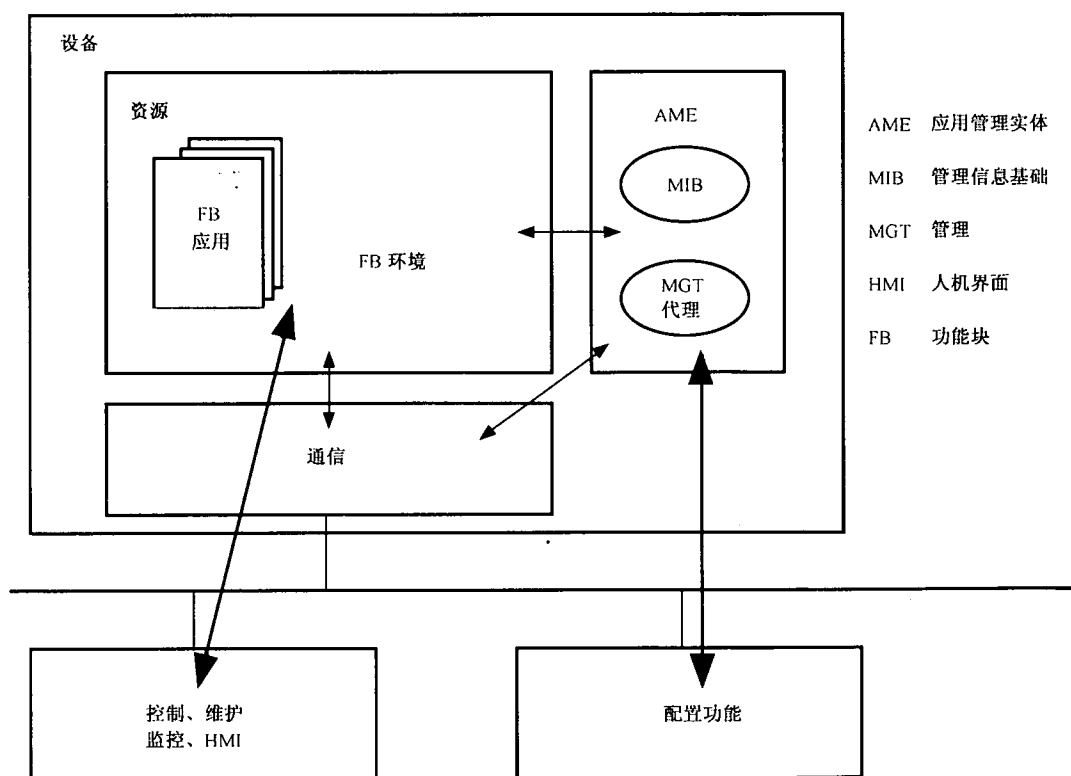


图 5 功能块设备的组成

在实际的设备或资源中,仅有数据和功能(程序)代码以及通信、过程和 HMI 接口。只有通过通信

系统,这些数据 and 程序代码才能被配置工具或设计工具视为功能块、管理代理或数据连接。设备模型的规范是设备实现的外部视图,设备模型详细描述了整个系统的体系结构。

设备模型是实际设备的抽象。

——执行 FB 应用的设备的基本组件是 FB(见图 6);

——FB 由数据和事件的输入和输出、内部数据、被包含的数据和算法组成,它们具有以下一般性要求。

注:术语 FB 是一般的块(功能、设备和技术块)以及特殊 FB 的同义词。

7.3 中有更多的描述。

a) FB 环境

FB 嵌入在以 FB 环境给出的运行环境中。FB 环境执行特殊的过程控制功能,这些功能是无需程序设计活动即可先前获得的应用部分,如报警。外部应用自主地使用 FB 环境功能,独立于 FB 应用,即与 FB 应用并行(见 7.5)。

注:功能块环境的通用功能和数据也可以封装在功能块中,如趋势。

b) 应用管理实体(AME)

从功能的角度来看,许多过程控制设备需要采用以前使用的硬件配置。例如,必须配置模块化设备中可使用的 FB,或者模型版本带有或不带有测量补偿的一个附加输入。这将导致添加或删除功能块。这些功能将会由 AME 启动,即,设备中的附加功能修改它们的应用软件。IEC 61158 系列的框架中定义了 AME。附录 E 描述了管理的要求。

注:AME 包含了所谓的系统和网络管理功能性。

c) 通信

通信服务和协议必须支持 FB 之间的数据转移,FB/FB 环境与维护之间的交互、HMI 监控以及 FB 环境/AME 与配置功能之间的交互。在 IEC 框架中,通信系统包含在 IEC 61158 系列标准和 IEC 61784 标准的范围内,FB 和 FB 环境的规范是独立于通信系统的。FB 环境和通信系统之间的子层映射将适应于不同的应用和通信。

FB 应用进程、系统和网络管理应用进程(即 AME)中的参数、块、对象和功能都需要有效地映射到基本的通信协议和服务。要求特别设计应用于 FB 应用过程、系统和网络管理应用过程的通信协议和服务,以与分布式应用进程一起使用,并且要求提供这些应用所要求的服务。

要求考虑三种不同类型的通信需求:

● 时间严格通信

要求 FB 应用进程使用的通信服务和协议支持时间严格通信的统一要求,包括:

- 1) 确定性的传输;
- 2) 传输的空间一致性;
- 3) 传输的时间一致性。

● 要求(Demand)通信

要求 FB 应用进程使用的通信服务和协议支持可用时间(time-available)通信的统一要求,包括大数据块的分段传输。要求 FB 应用进程使用的通信服务和协议支持“异常报告”通信的统一要求。

● 事件通信

要求 FB 应用过程使用的通信服务和协议支持事件通信的统一要求,并特别地设计以:

- 1) 在静止时段最小化装载;
- 2) 在高度活跃时段防止过载。

d) 资源

资源被认为是设备的软件(也许是硬件)结构的逻辑子部分。资源独立控制其自身的操作。

在一个设备内,可以对一个资源定义进行修改,而不影响其他资源。根据使用资源的应用的規定,资源接收和处理来自过程和/或通信接口的数据和/或事件,并返回数据和/或事件到过程和/或通信接口。通过设备资源提供应用的可互操作的网络视图。每个资源指定了一个或多个本地应用(或分布式应用的某些部分)的网络可见部分。

7.2 基本 FB 类型概述

7.2.1 概述

可以被其相关资源访问的基本 FB 类型在以下列出,见图'6,它们是:

- 资源块;
- 技术块;
- 功能块;
- 视图块;
- 趋势块;
- 报警块。

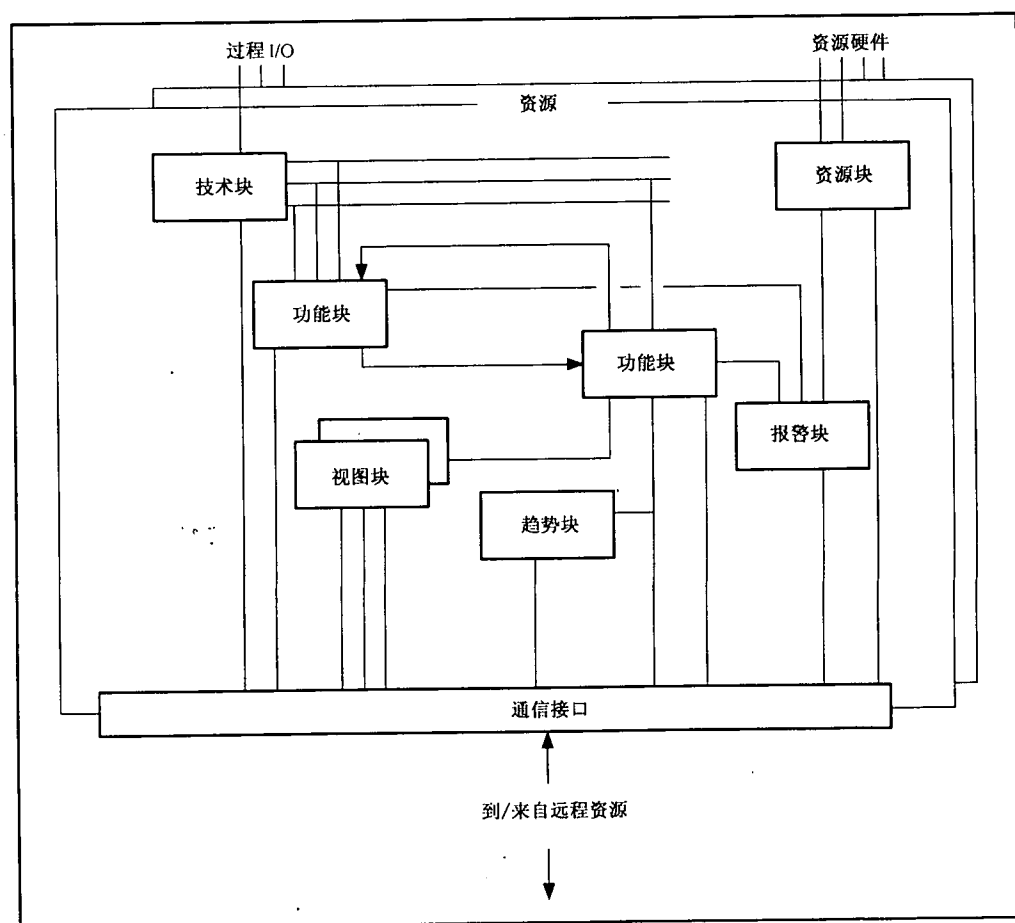


图 6 过程工业用功能块应用的设备结构

7.2.2 资源块

与资源相关的物理子组件的特性可由包含变量的资源块集合来描述。同功能块及技术块一样,资源块也可以包含变量,如设置故障-安全。这些变量在设备块中定义(见 7.4.4)。术语“设备块”和“资源块”是可交换的。

7.2.3 技术块

技术块使 FB 和 I/O 设备(如传感器、执行器和开关)的特性隔开。技术块通过为 FB 使用而定义的

独立于设备的接口来控制对 I/O 设备的访问。技术块也执行处理 I/O 数据的功能,如校准和线性化,以转换为独立于设备的表示。它们到 FB 的接口被定义为一个或多个独立于 I/O 通道的实现。

7.2.4 FB

FB 是 FB 应用中定义监控和控制的主要方法。FB 表示由应用所执行的基本自动化功能,该功能尽可能独立于 I/O 设备和网络的特性。每个 FB 根据指定的算法和一组内含的变量来处理输入变量和技术块输入。它们产生输出变量并输出到技术块。

基于处理的算法,可能要提供期望的监控、计算或控制功能。FB 执行的结果可由包含在操作或诊断信息功能块中的变量来反映。此外,处理结果可由到技术块的输出来反映,或由到一个或多个输出变量的输出来反映(见 7.3)。这些输出变量可以连接到其他 FB。

7.2.5 视图块

FB 环境包括了数据结构定义,以允许成组地访问相关的块参数,称之为视图块。当查看功能块数据时,视图块有助于操作员得到快速的响应。

为每一组以下参数定义了每一种 FB 类型和视图功能块。

- a) 操作动态参数;
- b) 操作静态参数;
- c) 所有动态参数;
- d) 其他静态参数。

7.2.6 趋势块

要求 FB 包括数据结构的定义,以允许成组地访问单个块参数的带有时间戳的连续采样集,称之为趋势块。趋势块消除了为了形成趋势而对参数高速扫描所需的通信和系统处理开销。要求趋势对象的定义包括标准采样类型及其相关采样功能(如局部采样、综合平均、最大、最小等)的定义。

7.2.7 报警块

报警是对一个块离开某个特定的状态及何时返回该状态的检测。检测到的报警状态的时间作为时间戳包含在报警消息中。同样,要包含优先级,以指示该警报是忠告性的或者是关键性的。

要求 FB 环境包括数据结构和相关资源的定义以及 FB 功能,以允许报警和时间信息在系统内受控地转移,称之为报警块。在系统内,报警块预测并有效地将报警和事件路由到选定的目的地。

报警块的定义包括用于初始化、发送和确认报警对象报告的标准交换协议的定义,确认报警、解释标准和自定义原因代码的定义,以及报警功能(如报警关键字、报警优先级、报警自动确认等)配置的定义。

当检测到警报时,资源块、技术块和功能块使用报警来传播通知消息。

7.3 FB 需求

7.3.1 FB 类型规范

要求过程 FB 包括:

- a) 标准化的数据结构;
- b) 标准化的语义;
- c) 与标准化数据相关的公共行为;
- d) 基本输入、输出和控制功能的标准化定义。

7.3.2 FB 正常和异常的操作需求

FB 执行正常和异常的操作,见 C.2.6。在稳定运行期间(运行点),在过程和自动化设备的设定条件下,FB 执行正常的操作。初始化、热或冷启动以及更高级的操作,如进入安全位置,是过程控制 FB 的附加功能。这些操作是 FB 的固定部分,默认连接到相关的事件。这些操作被称为异常操作或异常处理。

7.3.3 FB 功能性需求

对离散和连续控制都有效的 FB 功能性需求是：

- a) 功能块实例名被定义为块标签。在一个工厂站的一个系统范围内,标签是无歧义的。标签名在语法规则上可能与控制语言规则不一致(如长度、特殊字符)。
- b) 状态是与流经 FB 应用的主过程信号硬性结合的,即,要求 FB 输入和输出,不是内含参数,具有状态。
- c) 要求在级联的控制结构中使用的 FB 包括输入和输出的返回计算参数,以运载已定义的标准级联初始化、输出限制和输入或输出值状态信息。
- d) 要求 FB 功能性规范包括已定义的标准“无扰”控制模式,当检测到错误的输入、输出或转换值时,或当检测到初始化请求或来自返回计算参数的控制限制时,分离(shedding)和恢复动作。
- e) 要求 FB 功能性规范包括已定义的标准,当检测到错误输入、输出或转换值时的故障-安全动作,或者 FB 应用进程资源的故障-安全命令。当块执行其故障-安全动作时,要求通过报警块发送报警消息。要求故障-安全报警消息包括可以识别触发了什么故障-安全动作的原因编码。
- f) 要求 FB 功能性规范包括已定义的标准设定点和输出跟踪特性。要求功能块功能性规范包括已定义的标准偏差和比率设定斜坡特性。
- g) 要求 FB 包括参数,当观察实际的输入和/或输出及其状态时,以便模拟输入和/或输出及其状态(“模拟参数”),并包括可以使能或禁止每一模拟参数的参数。要求功能块功能性规范包括已定义的标准模拟参数的特性和模拟使能/禁止参数的特性。要求已定义的标准使能/禁止特性与强制的模拟禁止硬件跳线或开关适应。
- h) 要求 FB 包括过程测量(PV)和偏离报警(DV)的参数和标准化的功能定义。
- i) 要求 FB 具有控制从输入到输出的功能块内部信息流和功能块运算变化的模式。
- j) 要求 FB 包括每个块的初始化和重启的标准化功能定义。要求为以下操作环境定义行为：
 - 1) 新设备；
 - 2) 冷重启(长期的电源失效)；
 - 3) 热重启(短时的电源失效)；
 - 4) 从设备故障-安全返回。

7.4 从 I&C 派生的功能块的初始集

7.4.1 从 AB(高级 FB)派生的功能块的最小集

下例给出了过程自动化 FB 的最小集,见表 2,以确保底层控制的完整性并确保过去 10 年中,在现场总线标准化工作得到的大部分经验仍然有效。当然,最小化集是可扩展的。

表 2 初始 FB 集

功能块名称	描述	为什么包括在最小列表中
回路控制(PID)	带有以下配置的 PID: 偏差比例、测量值变化比例、速率和位置输出比例; 交互和非交互算法; 包括简单设定值的斜坡选项; 包括设定值输入的比率偏差; 包括均方偏差和非线性选项	在相同配置和调整参数的情况下,确保所有的 PID 以相同的方式操作;这有助于保证将最大回路数调节到最优。 将促进对不同整定工具所需的理解;将促进标准的整定工具和方法
控制输出选择器	多输入高/低选择器,带有初始化和状态传递	允许普通的继承和带有安全初始化和休眠终止预防的限制控制实施

表 2(续)

功能块名称	描述	为什么包括在最小列表中
测量选择器	三路测量选择器的最高、最低、平均和中等	用于不可靠测量(如,分析)的三取二投票及特别的安全
分路器	用于分离量程控制	支持初始化和无扰传输跟踪的返回计算,支持终止预防
模拟输入	扫描线性化质量检查	确保扫描和转换工作保持在最小程度,并都以同一种方式执行。在所有的实施中,允许所有控制模式中的操作以浮点工程单位进行
模拟输出	带有互锁、核对、回读 非线性值的线性化	确保公共术语、故障安全操作、限制控制和输出检查在所有的执行中以同一种标准方式执行
输出扇出	用自动、手动开关扇出控制器输出	确保公共术语、故障安全操作、限制控制和输出检查在所有的执行中以同一种标准方式执行
离散变量/脉冲输入	单一和多状态输入	确保公共术语、故障安全操作、检查、计数在所有的实施中以同一种标准方式执行
离散变量输出	单一和多数字控制输出	确保公共术语、故障安全操作、检查、计数在所有的实施中以同一种标准方式执行
超前滞后	第一顺序滞后和超前功能	允许带有安全初始化的公共前馈和限制控制的实施
空载时间	表驱动的空载时间	允许带有安全初始化的公共预测程序、前馈和限制控制的实施
控制/增量求和	对增量算法的输出求和或合并控制器输出	允许带有安全初始化的公共前馈和限制控制的实施
控制比率	带有初始化的控制器比率输出	允许带有安全初始化的公共前馈和限制控制的实施
输入切换	事件发生时,切换输入	允许带有安全初始化的公共预测、前馈和限制控制的实施
特征化	以内插值替换双向特征化块的 20 个点	允许简单的特征化,如回路耦合和线性化
定时器	通用的定时器,执行时间功能、计时、产生时间延迟脉冲等	允许带有安全初始化的简单的批量/顺序功能的实施
积分器	大量电力流量的积分器,如带有重启和行程功能	允许带有安全初始化的简单的批量功能的实施
连续变量警告/报警	带有故障安全活动、死区、忽略、计数、动态漂移和时间戳过滤的通用报警块“hi”,“hi-hi”,“lo”,“lolo”	确保带有初始化和审计追踪的公共报警功能的安全执行
离散变量警告和报警	带有故障安全活动、死区、忽略、计数、动态漂移和时间戳过滤的通用离散变量报警块	确保带有初始化和审计追踪的公共报警功能的安全执行

表 2(续)

功能块名称	描述	为什么包括在最小列表中
设备控制块	带有启动、停止、打开、关闭、停止、已启动、已打开、已关闭、巡回、故障状态的,控制电机驱动设备、阀、泵等的通用块	确保带有故障安全、初始化和审计追踪的公共电机控制和其他离散输出控制功能的安全执行,并确保标准已测试的功能代码的最大可重用
连续变量手动入口	带有检查和初始化的模拟变量的操作员入口的通用块	确保带有初始化和审计追踪的入口功能的安全执行
离散变量手动入口	带有检查和初始化的离散变量的操作员入口的通用块	确保带有初始化和审计追踪的入口功能的安全执行
设定值斜坡	批量类型循环的通用 16 点斜坡保持块	确保通用代码的最大重用,并强行初始化和审计追踪

附录 D 给出了模型化模拟输入 FB 的实例。

7.4.2 从 EFB 派生的功能块

EFB 为变量的信息处理包含了逻辑-数学算法。在过程控制领域中,由于安全方面的原因,这些算法的实现需要一些附件。其他的算法提供在设备冷启动或热启动之后的默认值、初始化之后的值或某种算法成功的状态(例如被零除的错误)。这些附加成分对于启动使过程处于安全状态的应用部分是必需的。一般地说,功能块应用中的过程相关变量和每一算法必须与一个状态结合,该状态提供算法执行和变量值的可信度。主算法是决定输出计算的等式。附加算法决定状态、默认值及其他。表 3 给出了共同使用的 EFB 的总览。

表 3 EFB 一般列表

分类	描述	建议用名	相似功能块	
			GB/T 15969.3	VDI/VDE 3696
arithm., 1 input	绝对值	ABS	ABS	ABS_
	余弦弧	ACOS	ACOS	ACOS_
	正弦弧	ASIN	ASIN	ASIN_
	正切弧	ATAN	ATAN	ATAN_
	余弦	COS	COS	COS_
	指数函数	EXP	EXP	EXP_
	自然对数	LN	LN	LN_
	以 10 为底的对数	LOG	LOG	LOG_
	正弦	SIN	SIN	SIN_
	平方根	SQRT	SQRT	SQRT_
	正切	TAN	TAN	TAN_
	死区	DEADZ	—	—
	限幅器	LIMIT	LIMIT	LIMIT_
	线性比例	SCAL	—	SCAL
	非线性(支持点)	NL_SUP	—	NONLIN_
	非线性(多项式)	NL_POL	—	—
	分割范围控制器	SPLIT	—	(in OUT_A)

表 3(续)

分类	描述	建议用名	相似功能块	
			GB/T 15969.3	VDI/VDE 3696
arithm. , ≥ 2 inp.	加法	ADD	ADD	ADD_
	除法	DIV	DIV	DIV_
	取幂	EXPT	EXPT	EXPT_
	模运算	MOD	MOD	MOD_
	乘法	MUL	MUL	MUL_
	减法	SUB	SUB	SUB_
	N 个信号平均值	AVER_N	—	—
	经 P,T 校正的流动速率	FCOR	—	Y_FCOR
boolean + edge	逻辑和	AND	AND	AND_
	否(非)	NOT	NOT	NOT_
	逻辑或	OR	OR	OR_
	逻辑异或	XOR	XOR	XOR_
	下限测定	F_TRIG	F_TRIG	FTRIG
	上限测定	R_TRIG	R_TRIG	RTRIG
counter, flip-flops	通用记数	CT	CTUD	CT
	双稳态(重起支配)	RS	RS	RSFF
	双稳态(设置支配)	SR	SR	SRFF
	大于或等于	GE	GE	GE_
	大于	GT	GT	GT_
	不等于	NE	NE	NE_
	小于或等于	LE	LE	LE_
	小于	LT	LT	LT_
	开关(+警告或信息)	SAM	—	SAM
dynamic and control	1 信号的平均运行	AVER_1	—	AVER
	(滤波)微分	DIF	—	DIF
	高/低/带滤波	—	—	(FIO/SEO)
	脉冲宽度调节器	PWM	—	PWM
	速率限制	RLIMIT	—	—
	动态二阶	SEO	—	SEO
selection	把 1/n 字节转换成数字	BIT_N	—	BIT_N
	信号分路器	DEMUX	—	DEMUX_x
timer	逻辑“关闭”延时	TOF	TOF	TOF1
	逻辑“开启”延时	TON	TON	TON1
	逻辑脉冲	TP	TP	TP1
	死区时间	DEADT	—	—
trend storage	记录(存储趋势)	R or TREND	—	R

7.4.3 技术块

- a) 技术块是执行将物理信号转换为数字信号,反之亦然,功能的特殊功能块。包括模-数/数-模转换线性化以及其他更多功能。技术块功能的定义伴随有多种参数。技术块代表了执行和测

量的类型。所有测量和执行原则指定的功能和参数都封装在技术块中。
图 7 给出了测量相关 FB 的功能性分类。

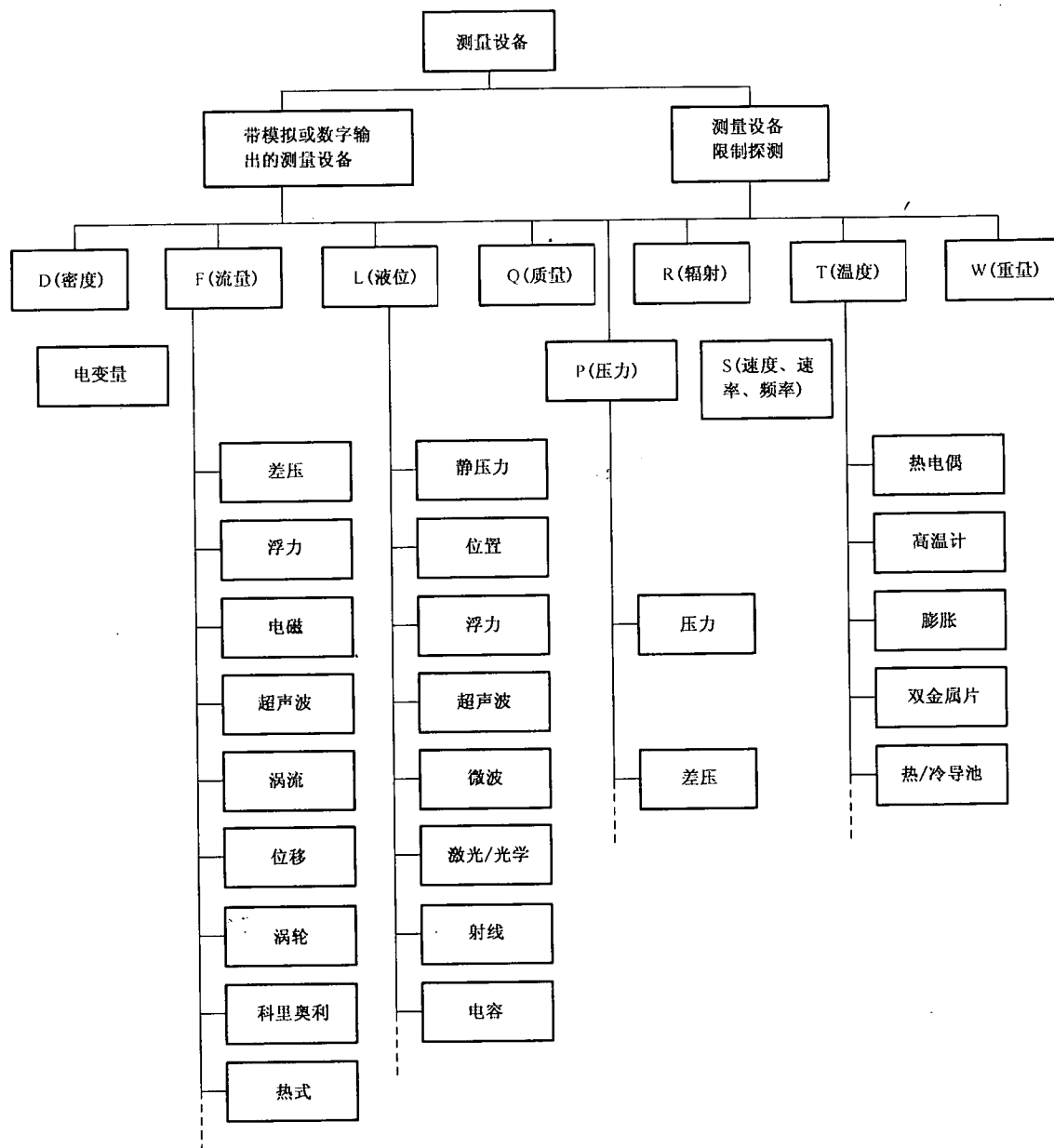


图 7 传感器功能层次:实例

b) 要求指出树的每一路径和层次、特征和要求的属性、参数以及功能。

注: FB类型的功能性分类的界限有时比较模糊,要求提供允许用户辨别 FB主要作用的支持。

c) 要求技术块包括一个 CHANNEL 参数,该参数是在资源内将数据连接到其他块所需要的。要求 CHANNEL 参数作为技术块的“标签”,而要求技术块内的其他参数被表示为“CHANNEL. Parameter”。

7.4.4 设备块

- 为了服务的目的,如日期认证或消息维护的存储空间,设备块是包含识别设备本身(设备盘)所必需的所有参数和功能的特殊 FB。设备块代表了一般的设备硬件和软件。
- 要求设备块包含含有 FB 应用进程的物理部分的描述,包括资源标签参考、资源设备描述参考和资源对象词典。

- c) 要求设备块包含管理功能块应用资源所需的信息,包括资源状态控制、动态存储空间分配和非永久性存储器更新。
- d) 要求设备块提供设备和资源所支持的可选择的 FB 应用进程特性的识别,包括串编码(ASCII 或 Unicode)和输入-输出硬件类型。
- e) 要求设备块参数和功能规范包括资源故障-安全命令,当设置该命令时,要求引起资源中的所有技术和功能块执行各自定义的故障-安全动作。
- f) 要求设备块参数和功能规范包括资源故障-安全的禁止功能,该功能被激活时,要求禁止资源中的所有技术和功能块的故障-安全动作。每当故障-安全禁用功能被激活时,要求设备块通过警告对象发出故障-安全禁用警告(见 7.2.7),且以用户配置的频率重复地发出。
- g) 要求设备块参数和功能规范包括与资源隔离的计时器功能,如果该功能被激活,要求对资源中超出“失效计数限制(stale count limit)”的计数功能块求和。在及时的通讯恢复之前,当这个总数超过了配置的值,要求资源中所有的技术和功能块强制执行已定义的故障-安全动作。该功能允许二级级联,在执行其配置的故障-安全动作前,等待相对长度的时间。

7.5 FB 环境需求

7.5.1 对象词典

要求 FB 环境包括对象词典,它含有对设备中所有块和对象的描述。设备的外部应用通过通信系统,利用对象词典来获取设备中块和对象的描述,并决定参数的内部存储索引。

7.5.2 连接对象

要求 FB 环境包括数据结构定义和相关功能,以将资源和 FB 参数映射到通信关系,称为连接对象。

7.5.3 FB 服务

FB 环境要求某些服务,这些服务执行到和来自于其他资源或设备中其他功能块环境的通信,以提供与制造商无关的系统中所有设备的一致操作。它们也提供功能块和系统管理应用进程之间的协调。

7.5.4 FB 调度

- a) 要求 FB 环境指定一个或多个标准的方法来控制 FB 的执行,要求这个或这些指定的方法与以下块执行同步:
 - 1) 块输入和块输出通信;
 - 2) 其他块的执行。
- b) 控制通信和 FB 执行的调度的参数的计算,可由在功能块环境范围之外的(即“离线”)应用执行。一旦调度建立了,要求功能块环境按照调度所定义的资源参数,控制和维护 FB 的执行。
- c) 要求块执行与块输入和输出通信之间的同步适应网络传输的时间。
- d) 要求块执行与其他块执行之间的同步适应设备资源的加载。
- e) 要求 FB 环境适应非标准或“制造商特有”的方法,以控制设备内 FB 的执行。
- f) 要求提供一种方法,以辨识设备内 FB 执行控制的方法(如“标准”或“制造商特有”)。要求这种辨识方法是可扩展的,以允许多个“标准”执行控制方法(如,允许未来对标准的补充)。

7.5.5 修正管理

FB 环境需要为设备内的所有软件和可配置参数的修订控制规定参数、功能和协议。主要参数有:

- a) 设备行规;
- b) 设备行规修订;
- c) 静态数据修订;
- d) 写锁定;
- e) 访问允许的参数;

7.5.6 维护块

要求 FB 环境包括数据结构定义和相关资源功能,以允许在设备中保持以及在维护信息系统内受

控地转换,称为维护块。

维护块的主要参数包括与设备特性和维护事件相关的以下信息:

- a) 湿件和物料代码;
- b) 制造商-输入的文本字符串;
- c) 用户购物-输入的文本字符串;
- d) 用户域-输入的字符串;
- e) 用户定义的维护活动代码;
- f) 制造商定义的交互式校准程序的结果。

7.6 通信需求

- a) 要求 FB 环境、系统和网络管理应用进程中的参数、块、对象和功能有效地映射到下层的通信协议和服务。
- b) 为了分布式应用进程的使用,要求特别设计 FB 环境、系统和网络管理应用进程使用的通信协议和服务,并要求提供这些应用所要求的服务。
- c) 要求 FB 环境使用的通信协议和服务支持时间严格通信的统一需求,包括:
 - 1) 确定性传输;
 - 2) 传输的空间连贯性;
 - 3) 传输的时间连贯性。
- d) 要求 FB 环境使用的通信协议和服务支持可用时间(time-available)通信的统一需求,包括大数据块的分段传输。
- e) 要求 FB 环境使用的通信协议和服务支持“异常报告”通信的统一需求。
- f) 要求 FB 环境使用的通信协议和服务支持通信事件的统一需求,而且被特地设计,以:
 - 1) 最小化静态期间的装载;
 - 2) 防止高度活跃期间的过载。

8 附加需求

8.1 与外部应用协作

一个全面的自动化应用包括非严格时间要求的控制操作(如监控、维护和配置),这些操作可能没有按照 FB 来说明。这些操作也可能应用于与非 FB 过程控制系统的协作。非 FB 应用需要对 FB 的变量和参数以及其他设备特定信息进行在线数据访问,见图 8。

该条提供了关键要求的概述。

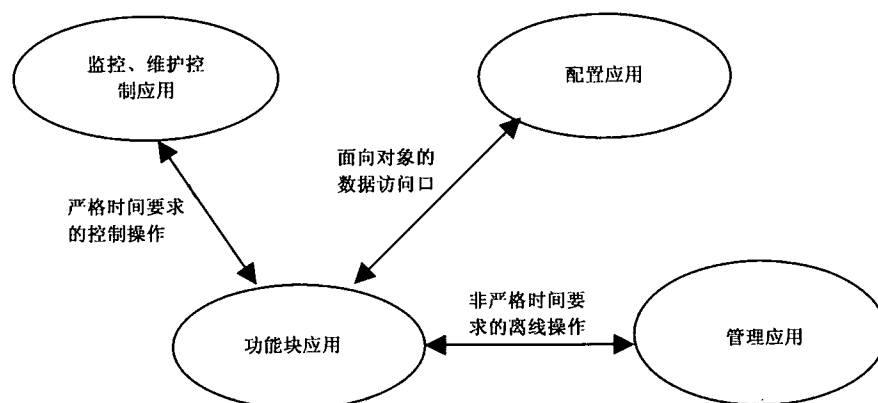


图 8 非功能块应用数据接口

8.1.1 与控制、维护和监控应用协作

8.1.1.1 概述

注：有些需求与在 FB 应用中出现的需求重复。然而，该规范必须同时考虑这两种观点。

与控制、维护和监控应用的协作需要一组公共的应用功能（数据访问、数据报告、数据记录、控制功能等），这些功能在大多数实时自动化设备中存在，特别是在基于 FB 的应用中。一组标准化的应用服务的使用允许：

- a) 将建模工作从通信细节中隔离出来；
- b) 应用高度的可互操作性，不仅在于报文的语法，也在于数据交换的语义；
- c) 降低集成的成本，因为，对所有的实时数据有一致的访问和表示机制。

8.1.1.2 终端系统的分布

要求与控制、维护和监控应用的协作支持：

- a) 位于工厂内任何地方的终端设备和处理器包含在公司设施中、在控制中心中、单元内以及用户设备中。
- b) 与过程控制系统的外部系统的通信，包括公共的通信系统和公共的因特网。
- c) 一个总体的系统环境，包括高速通信通道、低速通道、共享通道以及具有统一传输特性的媒介，如无线电、移动无线电、卫星、电力线等。
- d) 现在以及未来的网络配置，可能包括子网络层次、子网内的点对点通信以及跨企业的完全点对点通信。

8.1.1.3 设备/处理器能力

与控制、维护和监控应用的协作要求：

- a) 特定设备的处理、计算和存储能力的范围可能有功能强大的设备、简单计算设备和内存受限设备。
- b) 在同一网络或子网上，可以支持一个到数百个的设备。

8.1.1.4 对话特性

要求与控制、维护和监控应用的协作：

- a) 支持不同的通信对话和数据流要求，包括：
 - 1) 仅单向的；
 - 2) 双向交替（如层级结构）；
 - 3) 由网络协议或媒介管理的双向（如现场总线、令牌环、CSMA/CD 及基于无线电的“智能”媒介，用以处理未经请求的报告）；
 - 4) 同时双向（如全双工的 WAN）。
- b) 支持消息流经多个中间设备、本地子网和 WAN 连接。
- c) 支持同类设备之间的多并发通信。
- d) 支持消息的优先级和/或中断长消息的能力。
- e) 支持应用级安全。
- f) 通过支持有效编码和数据压缩技术来最大化网络吞吐量。

8.1.1.5 设备寻址

要求与控制、维护和监控应用的协作支持：

- a) 在同一网络中，数量从几个到数百个的设备的寻址；
- b) 在只有短地址合法的本地子网内，当允许通过广域网访问这些地址时，处理短地址的寻址方案；
- c) 处理广播和组播要求的寻址方案。

8.1.1.6 网络流量特性

要求与控制、维护和监控应用的协作支持:

- a) 以超低速(10 bit/s 或更低)到超高速(吉比特/s)之间的数据速率来传送信息和潜在的图像和图形;
- b) 不同的数据传输速率,范围从非常低频传输(一或两次/年)到高频传输(ms),再到超高频传输(特殊情况下每 50 μ s 传输一次);
- c) 传输范围从几个字节数据到非常大文件的报文。

8.1.1.7 时序问题

要求与控制、维护和监控应用的协作:

- a) 支持设备的时钟同步。
- b) 支持至少精确到 1 ms 的时间戳。
- c) 最小化时间测量偏移,至少精确到 1 ms。

8.1.1.8 应用服务需求

要求与控制、维护和监控应用的协作支持:

- a) 多个用户对系统的并发访问;
- b) 调度的和非调度的数据交换;
- c) 客户所需的远程数据检索;
- d) 未经请求的数据报告,由服务器的事件驱动;
- e) 发布者-订阅者数据交换;
- f) 数据异常传输报告,仅传输已改变了的数据;
- g) 远程设备控制命令(支持控制执行前的限制:立即控制、特殊情况控制,如设定值在限值之间或设定值被限制到特定的配置值,等等);
- h) 要求远程设备控制命令支持多个客户,客户被允许在任意时候连接到服务器;
- i) 通过一个时刻只有一个操作者或信号量(semaphore)机制来预防并发控制命令;
- j) 远程事件记录和事件日志;
- k) 广播和组播数据到设备;
- l) 远程程序控制;
- m) 设备配置文件的上传和下载;
- n) 错误管理和报告。

8.1.1.9 应用数据格式

要求与控制、维护和监控应用的协作支持:

- a) 面向对象的数据结构和功能;
- b) 与 FB 应用相同的数据类型;
- c) 数据的自定义命名约定。

8.1.1.10 操作要求

要求与控制、维护和监控应用的协作支持:

- a) 网络管理要求,包括:
 - 1) 网络协议统计记录,如临时和永久连接故障的数目、数据重发数目、连接利用数目;
 - 2) 为网络上的所有适当用户进行监控、检测和通知关键性的网络故障;
 - 3) 动态带宽分配;
 - 4) 远程网络设备的在线重配置;
 - 5) 对网络用户或部门再分配成本的 charge-back 服务;
 - 6) 第三方网络设施使用的计算管理设施;

- 7) 安全服务和机制的管理,以确保维护总体网络系统的安全。
- b) 目录服务,包括:
 - 1) 应用、处理器、设备和数据对象的标识;
 - 2) 与外部目录服务的集成,如公共的电子邮件提供者;
 - 3) 信息限制给授权用户;
 - 4) 搜索和分类能力。
- c) 安全机制,以确保:
 - 1) 机密性,防止所传输的数据被非授权用户解密;
 - 2) 完整性,检测所传输的数据的修改、插入、删除或重发;
 - 3) 数据源(data-origin)鉴定,通过说明传输数据的来源是所声明的;
 - 4) 不可拒绝性,防止发送者或接收者拒绝参与通信;
 - 5) 用户鉴别,通过说明用户的身份是所声明的;
 - 6) 访问控制,通过防止对资源的非授权访问,包括试图以不恰当的方式使用资源。

8.1.2 与配置应用协作

在这种上下文关系中,要求配置(系统或设备)被理解为系统或设备设计的带有以下活动的一个步骤:

- a) 选择功能单元;
- b) 分配存储单元;
- c) 定义它们之间的互连。

要求与配置应用的协作执行与以下设备进行协作:

- a) 远程创建数据类型、FB类型和实例以及FB实例间的数据连接;
- b) 远程删除数据类型、FB类型和实例以及FB实例间的数据连接;
- c) 远程启动、停止、取消应用程序和FB;
- d) 远程查询所有的数据类型、FB类型、FB实例、数据连接和变量。

注1:这种上下文关系中,远程意味着:协作需要一种应用协议(与应用层相反,如现场总线)。这种协议定义所有将要交换的信息、它的含义以及信息交换的顺序和序列。另外,该协议还需要一种简洁和完整的、由接收到所交换的信息发起的过程的定义集合。该协议也定义了协作期间可能出现的任何异常。

注2:在线配置和在线控制具有重叠部分。例如,设定点时的设置可以使用在线配置或在线控制来实现。

8.2 附加特性需求

8.2.1 概述

本条中的过程控制用户需求阐明了以下考虑:

- a) FB环境;
- b) 通信功能;
- c) 修正管理。

本条中列出的许多条目表现为技术上的实施细节,而不是用户需求。无论如何,由于预定系统的多供货商本性,用户需要这些技术细节的标准化实施,以产生可操作的系统。另外,用户需要某种技术细节的特定实施,因为应用进程的分布式本性要求特定的实施,以产生可操作的系统。最后,基本的特定实施细节需求是数十年来不同系统提供商的经验,以及对大多数过程控制应用中什么性能最好的广泛理解。

8.2.2 多供应商系统

过程控制用户应用,称为FB环境,要求适应多供应商系统的结构和操作。要求这种应用模型能够使用户容易地确定设备之间的兼容程度。设备兼容性要求用某种方法描述,该方法能清楚地表示设备是互连、协作、互操作或互换的。

要求这种应用模型定义标准的数据结构、特性、FB 和通常作为在使设备互交换之前的重要步骤而使用的过程控制功能和设备的规范。也要求该模型包括标准的和自定义的数据结构、特性、FB 以及使设备互连、协作和互操作的规范的结合。

8.2.3 可扩展

要求过程控制应用模型可扩展为新的标准的和制造商特定的数据结构、特性、FB 及设备规范。要求符合过程控制应用模型的扩展满足多供应商的用户需求。要求过程控制应用模型包括设备描述语言以支持所要求的扩展。

8.2.4 分布式应用

8.2.4.1 概述

该应用模型提供分布在不同设备中的过程控制应用。

8.2.4.2 分布式控制通信

分布式过程控制应用有统一的通信需求,即要求能被嵌入式通信协议满足。包括分布式应用之间安全的通信关系、应用事件和功能的同步功能、时间严格通信规定、数据及事件的时间戳、报警和事件的标准处理、分布式原操作的执行和大数据集合的分段与重组。

8.2.4.3 为现场总线的优化

要求过程控制应用模型与现场通信标准(如 IEC 61158 系列、EN 50170 等)一起使用。要求优化过程控制应用模型,以在低速、本质安全和基于现场总线的系统中,最大化利用可获得的带宽。要求定义在应用模型中的数据结构 and 通信功能有效地映射到现场总线通信的服务和协议。

8.2.4.4 与 ISO/OSI 模型的一致性

要求过程控制应用模型与各种开放的系统通信网络一起使用,因此要求与数据通信的 ISO/OSI 模型一致。过程控制应用模型提供通用应用在 OSI 模型上下文关系中的使用语义。过程控制应用模型具有统一的通信服务需求。它们包括,但不限于,时间严格通信、系统管理服务以及协议速度和效率。要求指定这些通信服务要求,以使用户能够容易地辨别特定 OSI 一致性协议与一致性过程控制应用的一致性程度。

8.3 一致性要求

8.3.1 机构支持

要求过程控制应用模型得到技术开发者、设备供应商和终端用户的活动机构的支持,该机构负责实际系统的实施和维护。

8.3.2 正在进行的改变和增加

没有过程控制应用可以是完整的和不变的,而继续满足实际应用变化着的需求。要求标准的过程控制应用模型得到有效率和有效果的发起机构的支持,并且能够实施周期性和实时性的添加、删除和改变,以适应过程工业变化的需求。

8.3.3 一致性检查和确认

实际应用中实际系统的有效率和有效果的实施要求无歧义地辨识符合标准过程控制应用模型的设备和系统。要求该模型包括独立测试机构所需的客观的和可测量的标准,以确定设备和系统的一致性。

8.3.4 培训和支持

开发者、供应商和终端用户都需要解释和培训的资料,以支持符合标准过程控制应用模型的实际系统的实施。要求该模型得到有能力提供这种培训的、有效率和有效果的发起机构的支持。

9 设备描述语言

9.1 背景

工厂和过程自动化在过去几年的快速发展中形成了一个无疑的基本概念:工程师和技术员必须得到基于计算机工具的支持。这一点特别适用于分布式控制系统。现场总线在控制器和传感器/执行器

之间以及在工程师站和所有设备之间传送数据。在工程过程的所有不同阶段,运行于 PC、工作站或终端上的一个或多个工具需要知道它们所连接的设备类型。包括供应商的信息、硬件和固件的版本、交换的数据格式、响应时间以及物理单位等。在多数情况下,位于工程师站的现场总线控制器还需要知道关于响应时间、支持的波特率等通信能力。随着可远程访问的设备的发展,大多数设备特性被集中在设备描述中。设备描述和设备一起被交付。使用了电子设备描述这个术语,因为它不仅是一种语言,而且实际上是一种如何在所有 DCS 生命周期中集成设备的技术。

9.2 基本要求

为了得出一般的用户需求,首先要定义用户(user)这个术语的含义。可以区别两种类型的用户:

- 工厂或机器的操作员或终端用户;
- 系统集成商。

尽管它们工作在同一分布式系统中,它们对电子设备描述的要求不同吗?下面的段落将分析这个问题。

对于分布式控制系统的终端用户而言,最重要的是设备描述的透明性。终端用户仅希望看到 SCADA-软件中的图形用户界面或其他的人机界面(HMI)。因此,电子设备描述需要按照即插即用的概念来构建。另外,要求在中交换设备不会导致巨大的工程任务,而是要求由技术员简单且安全地完成。设备描述必须支持这一点。

和终端用户相比,完成工程、安装和编档的系统集成商需要达到不同的目的。他的目标是减少解决互操作问题的工程时间,同时提高设计最优应用的工程工作,并关心所生产的过程控制系统产品的质量。他的工作,包括工厂/机器生命周期的预生产阶段,效果直接取决于他必须处理的、机器可读的设备描述的定义良好性、标准性和完整性。

这种分析所得的结论是,必须主要从系统集成商的角度去看待用户的需求,因为他必须直接地去处理电子设备描述。因为计算机工具,以过程控制系统闻名,是系统集成商使用的最新型的工具,这些工具的需要将产生电子设备描述的要求,以最好地支持工程过程。

控制过程系统提供了对生产过程的控制和监督。它们连接人(如操作员)和机器。它们由输入/输出设备、数据处理单元、人机界面和通信系统组成。

传统地,从运行时的角度(功能、设备和系统)来看待 PCS。由于渐增的复杂性和所牵涉的费用,工程方面变得更加重要。复杂性是由影响工程过程的几个因素导致的,如不同的设备成分(输入/输出、数据处理、HMI、通信)、处理物理过程(机械的、电气的等)、生命周期阶段和设备供应商。现在,这些不同领域的集成一般通过创建硬件和软件接口来实现,并执行昂贵的基于试错法的试运行过程。在所有权原则的真实成本下,这种集成是不可能的。为了避免数据丢失和不一致,要求集成工具来支持整个工程过程。没有公共的传输语法和标准化的数据模型,使用纸质文档不能充分地解决集成问题,即使使用电子方法也不能。

现场总线提出了一些使用电子方式交换数据的方法,包括设备描述语言(DDL)和设备数据库(GSD)(HART、FF 和 PROFIBUS)。

电子设备描述(EDD)的要求,包括相应的语言,可以概括如下:

- a) 要求 EDD(以文件的形式)由设备供应商连同设备一起交付。
- b) EDD 应用于分布式控制系统的工程过程、支持计划、试运行、运行、诊断和维护。
- c) EDD 在已决定的结构模型的关系内使用,并由带有标准接口的软件工具(编辑器、记号赋予器(tokenizer)和解释器)相应链支持。
- d) 要求两种不同的 EDD 表示:
 - 1) 源(人可读并且计算机可解释);
 - 2) b- optional: 二进制(由记号赋予器(tokenizer)创建,由解释器解释)。
- e) 要求 EDD 存储在磁盘上并且要求存储在设备内(通过现场总线传输)。

- f) 要求 EDD 独立于基本的现场总线系统。
- g) 要求 EDD 描述辨识每一项以及定义它们之间的关系(层次型、关系型)的信息。
- h) 要求 EDD 至少描述 FB 模型。
- i) 要求 EDD 为在 HMI 内的表示和通信访问提供语言元素。
- j) 要求 EDD 包括面向对象的特性。
- k) 要求 EDD 为时间考虑提供语言元素。
- l) 另外,作以下假设:
 - 1) 不考虑 EDD 集成到设备开发自身;
 - 2) 要求 EDD 文件代表静态的描述,如设备的说明部分,因此,只需要描述设备的外部接口/特性(对内部的代码没有兴趣)。

9.3 一般要求

如果有一个现场设备的完整的 FB 模型,只需要从它导出描述语言的需求。下面是和语言性质有关的关键的概念。

- a) 为了达到一致,要求非冗余地指定 EDD 参考模型的层次结构。
一般化/特殊化技术(Gen/Spec):这个概念首先用于面向对象分析和保证某种应用领域的清晰观察。对于未来所选择的层次结构的扩展,这个概念是非常重要的。
- b) 为了保证同未来 IFD(智能现场设备)-EDD 规范的互操作性和版本控制,要求为每个规范定义一致的类。
容器类原理:同上,这个概念自然地由现代面向对象方法支持。
- c) 为了达到一定的标准化水平并且同时为提供商或用户提供附加的空间以便引入专有特性(也可以替代下面的服务),服务有 3 种不同的分类子集:
 - 1) 基本的或强制的服务:要求实施;
 - 2) 可选的服务:完全指定,并不设想需要实施;
 - 3) 供应商服务:未指定,供应商选择实施。
- d) 接口技术:像面向对象世界中提出的一样,接口概念允许一组相关的方法或功能的逻辑表示。
注:例如,CORBA 或过程控制用 OLE(OPC)规范所使用的技术。
- e) PRIAM 模型在较高的抽象层次定义,所要求的通道通过所使用的现场设备的使用来实施,若必要,带有附加软件。根据 PRIAM 的推荐,较低层次的抽象可以帮助在 FB 模型上映射:在这种层次下,设备数据和功能可以组合为所谓的设备功能单元,设备功能单元代表了典型的硬件或软件成分。这就要求用功能分解模型来描述现场设备,在该模型中,数据流同样是可见的。

功能分解技术:通常,这种推荐可能导致使用对象建模的方法来描述应用。这种模型一旦设计好,将要求支持分布式过程控制系统的整个生命周期。这种总的模型超出了本部分的范围。

这种总的概念需要使用一些面向对象技术的概念。要求支持数据库概念。标准化描述工具以避免开发一种全新计算机语言的支出,必须审查已存在的正式标准和工具。

附 录 A

(资料性附录)

系统生命周期

A.1 FB 的由来及实现

A.1.1 得到 FRD 的步骤

A.1.1.1 标题

A.1.1.1.1 控制功能

有不同类型的控制功能：

- a) 直接地或间接地传送过程测量的测量控制功能。
- b) 控制功能：
 - 控制开/关(on/off)执行器的开环控制功能；
 - 控制调节执行器的单个或级联的闭环控制功能；
 - 协调下层控制功能的顺序控制功能。

A.1.1.1.2 控制层次图(CHD)

过程控制应用的控制功能层次的图形图表和结构化表示。最底层由与变送器和执行器相互作用的控制功能组成。上层由协调下层控制功能的控制功能组成。

通过 CHD,过程工程师可以通过将控制功能分配到 Folio 来定义 FRD 的文档结构。

A.1.1.1.3 Folio

FRD 被结构化为一组 Folio。Folio 是分配到该 Folio 的控制功能需求的详细描述。使用图形化的 FB 语言来将控制功能的特性描述为 EFB 和应用 FB 的网络。

A.1.1.1.4 FB

EFB:它是一种可用于不同类型的过程控制应用(化工、石化、能源等)的简单的逻辑数学操作。EFB 独立于任何提供商的程序设计语言。IEC SC 65C 正在考虑一个标准的 EFB 的库。

AB:它是一种复杂的逻辑数学应用,应用由一个公司或为一个公司定义和确认。AB 取决于过程控制应用(化工、石化、能源等)的类型。AB 独立于任何提供商的程序设计语言。

注：有必要规定 AB 的行为,以实现互操作。这种规范应该定义如何连接 AB、在库中的分组、在资源中使用时的标识、版本控制等。

A.1.1.1.5 功能需求图(FRD)

由过程工程师使用中性的 FB 语言来描述的控制功能的详细需求。该语言由使用标准构造规则建立的标准 EFB 和 AB 组成。

A.1.1.1.6 过程流程图(PFD)

它是过程某部分的图表和图形表示。PFD 代表了主要的机械单元、这些单元间的管道、远程变送器和执行器。过程工程师定义过程环路图到过程基本操作的划分。

A.1.1.1.7 扩展的管道和仪表图(P&ID)

常规的 P&ID 中只表示了控制环路。扩展的 P&ID 中表示了所有的控制功能。

A.1.1.1.8 过程基本操作

过程基本操作是 PFD 的一部分,表示物质和能量的一种典型变换。将 PFD 分解为过程基本操作,以强调受控物质和能量的主要变换。

A. 1. 1. 2 从过程到 FRD

A. 1. 1. 2. 1 概述

本条的目的是为了说明 FB 的用途。FB 的需求被描述为工程公司规定控制的关键元件。

FRD 是控制过程的控制功能的规范。FRD 可以通过不同的方法获得,这取决于工业领域。

这些研究应该被归纳在以下的生命周期中。由于 FRD 完全取决于控制的过程,必须被控制的过程基本操作必须首先标识在 PFD 中。在 P&ID 中,必须定义过程和过程基本操作的控制功能(要控制的过程基本操作的网络)。在 CHD 中,控制功能的文档是一组 Folio 的结构。在每个 Folio 中,控制功能被详细地描述为 FB 网络,以获得 FRD。这个生命周期被归纳在图 A. 1 中。

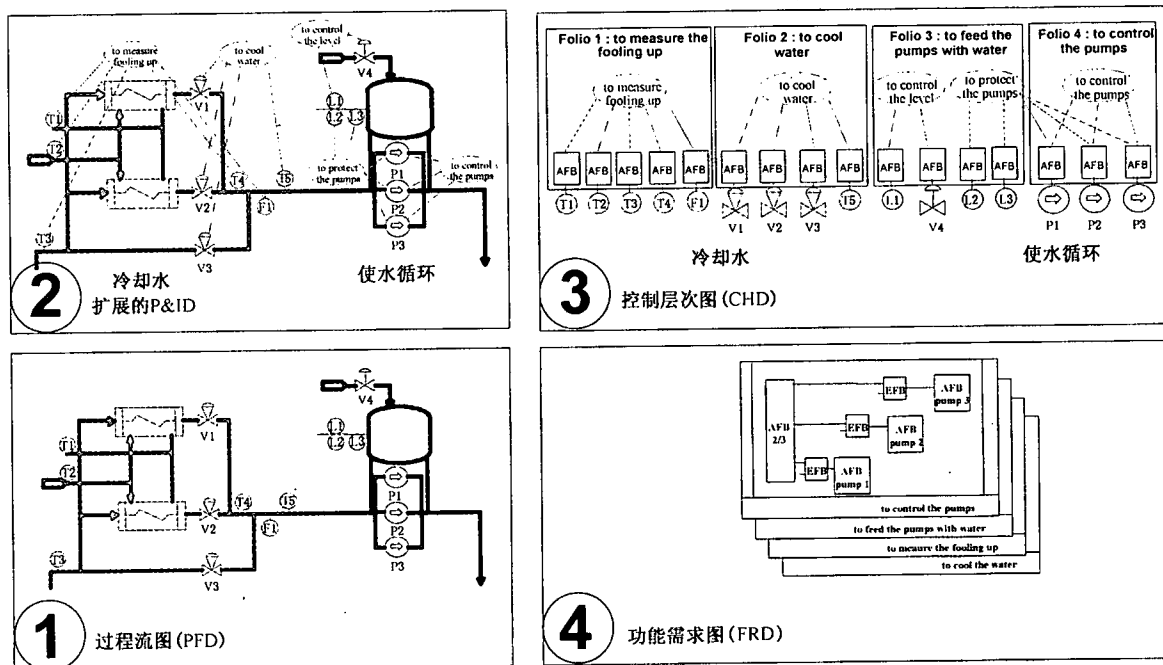


图 A. 1 从过程回路到 FRD 的生命周期

A. 1. 1. 2. 2 PFD 的使用

PFD 是被控过程的示意性表示。图 A. 1 只给出了理解过程操作所必须的过程信息。在 PFD 中,任何过程工程师都可以将过程视为支持主要过程基本操作的装置的网络。

在 PFD 中,图形符号应该与机械符号标准一致。不幸的是,没有统一的标准。在化工和石化工业领域中的符号标准主要来自 ISA。也还有 IEC 图形符号标准和一些重要的公司标准。这些标准是不同类的。

A. 1. 1. 2. 2. 1 要控制的过程基本操作的标识

由于控制功能完全取决于过程的类型,所以必须标识要控制的过程基本操作。过程装置单元支持基本操作。基本操作对物质和能量进行转换,其目的如:

- 冷却水;
- 使水循环;
- 抽水。

图 A. 2 给出了包括两个过程基本操作的 PFD 的例子,两个操作用来冷却水和使水循环。

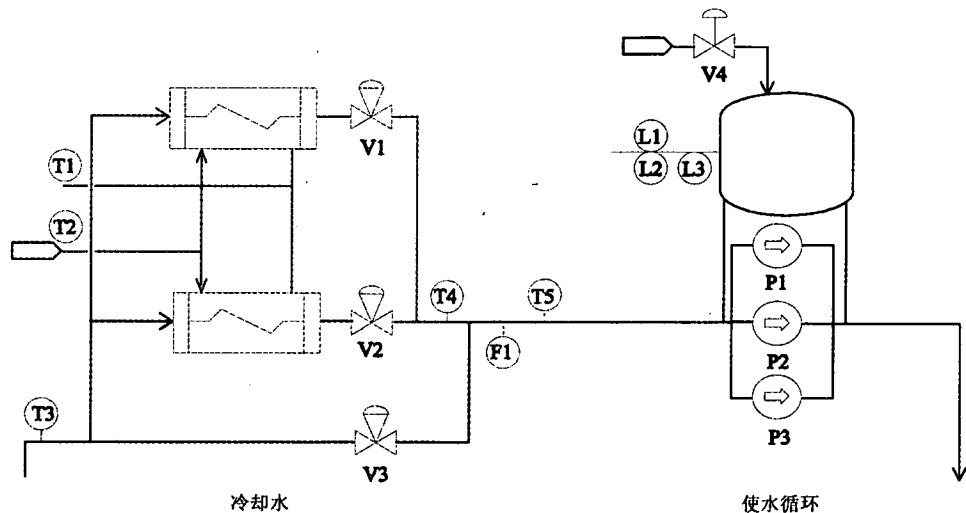


图 A.2 包含两个过程基本操作的 PFD

通过 PFD,任何过程工程师都可以明白这个过程是两个基本过程操作的连接。第二个基本过程操作可以分解为两个子操作,如装载泵和抽水。基本过程操作的定义取决于公司。

通过 PFD,过程工程师定义控制功能来控制这两个过程基本操作以及包含这两个过程基本操作的过程。

A.1.1.2.3 扩展的 P&ID

为了说明控制功能和过程的关系,采用了在化工和石化工业中通常使用的所谓的 P&ID 的扩展。在传统的 P&ID 上,主要表示了远程变送器、远程执行器和控制器。

除远程变送器和执行器之外,扩展的 P&ID 表示了所有的控制功能。过程工程师可区别不同类型的控制功能:

- 测量控制功能:对来自于一个或多个变送器的测量的加工;
- 开环控制功能:控制关于一个或多个测量的和/或关于来自于操作员或一个序列的命令的开/关(on/off)执行器;
- 闭环控制功能:控制关于一个或多个测量和一个设定值的被调执行器;
- 顺序控制功能:控制开/关(on/off)执行器、顺序的开环和闭环控制功能以及其他的序列。

除闭环控制功能的控制器外,在过程控制图中,也描述其他类型的控制功能,如测量控制功能、开环控制功能和顺序控制功能等。

扩展的 P&ID 中,在表示输入、控制处理和输出的符号之间,一个控制功能应该被表示为一个图。在内部控制功能的标签内,控制处理是一个单独的图形符号。控制功能的输入应该是来自于其他控制功能的测量和/或数据。它们被表示为控制处理符号和远程变送器符号和/或其他控制功能符号之间的连接。控制功能的输出应该是到受控制的执行器的命令和/或其他控制功能的数据。它们被表示为控制处理符号和远程执行器符号和/或其他控制功能符号之间的连接。为了说明的方便,通过增加一个符号和标签来标识控制功能。以表示控制功能的处理、用一条线来表示控制功能处理与变送器、执行器以及其他控制功能之间的连接。

图 A.3 是在前面图 A.2 中描述的过程的扩展的 P&ID 的一个例子。

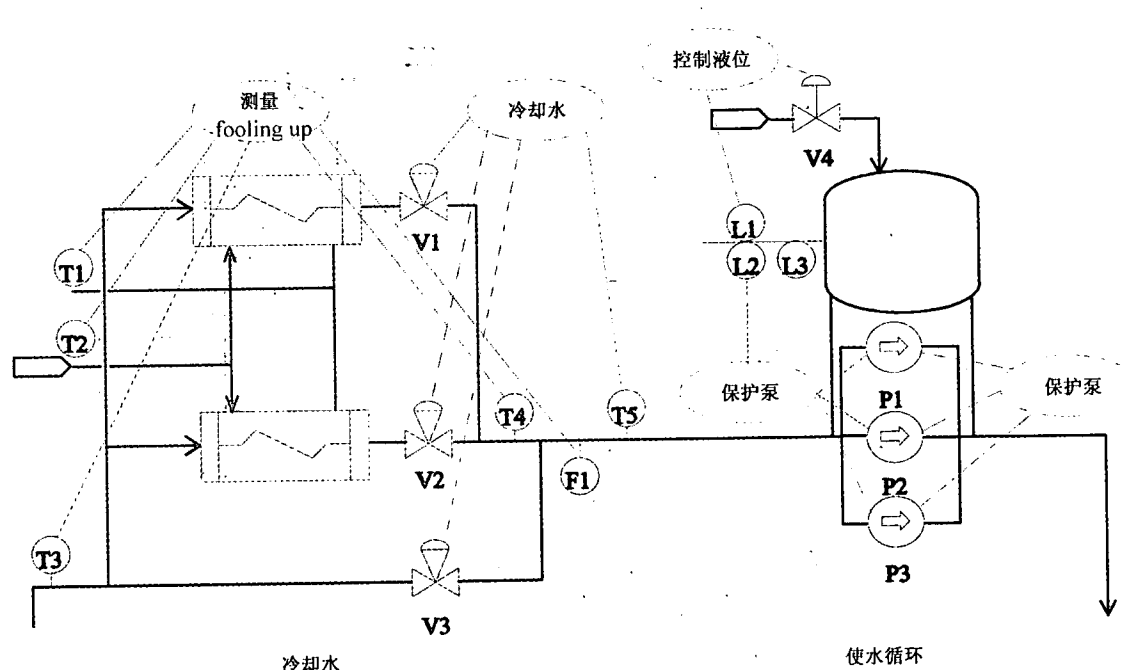


图 A.3 控制功能在扩展 P&ID 上的明确表示

在扩展的 P&ID 中,对于每一个控制功能,观察(来自于变送器和其他控制功能)和命令(到执行器和其他控制功能)之间的因果关系是清晰可见的。

为了控制第一个过程基本操作“冷却水”,过程工程师定义了两个控制功能。第一个过程功能是闭环控制功能“冷却水”,控制来自远程变送器 T5 的水温并启动调节阀 V1、V2 和 V3。第二个控制功能是测量功能以“测量 fooling up”,计算来自远程温度变送器 T1、T2、T3、T4 和远程流量变送器 F1 的交换器的 fooling up。该测量功能控制当前换热器在正常范围内操作,如果出现故障,将发送一个信号给操作员。

为了控制第二个过程基本操作“使水循环”,过程工程师定义了三个过程功能。第一个过程功能是闭环控制功能“控制液位”,通过控制阀 V4 的值来控制来自于远程液位阈值 L1 的容器的液位,并维持容器的液位。第二个控制功能是开环控制功能“保护泵”,控制来自于两个远程阈值 L2 和 L3 的容器的液位,当容器的液位太低时,关闭泵 P1、P2 和 P3。第三个控制功能是开环控制功能“控制泵”,允许泵 P1、P2 和 P3 间的两两操作,以确保水的循环。

扩展的 P&ID 适用于过程工程师和 I&C 工程师,并且它有助于两者的通信。一旦控制功能被标识并加以标签,就应该组织描述控制功能的文档框架。

A.1.1.2.4 控制层次图(CHD)

A.1.1.2.4.1 概述

控制层次图(CHD)的目的是结构化控制功能的文档。CHD 首先是从扩展的 P&ID 的控制功能中提取出来的。其次是控制功能的,特别是 AB 的,需求定义。再次是 FRD 的结构化文档。

A.1.1.2.4.2 从扩展的 P&ID 提取的 CHD

CHD 专注于控制,因此不再需要关于过程的数据。如果需要这种数据,则应该使用 PFD 或扩展的 P&ID。CHD 首先通过从扩展的 P&ID 的控制功能的提取而获得。在下面的图 A.4 中,有一个来自图 A.3 中扩展的 P&ID 的控制功能的提取。

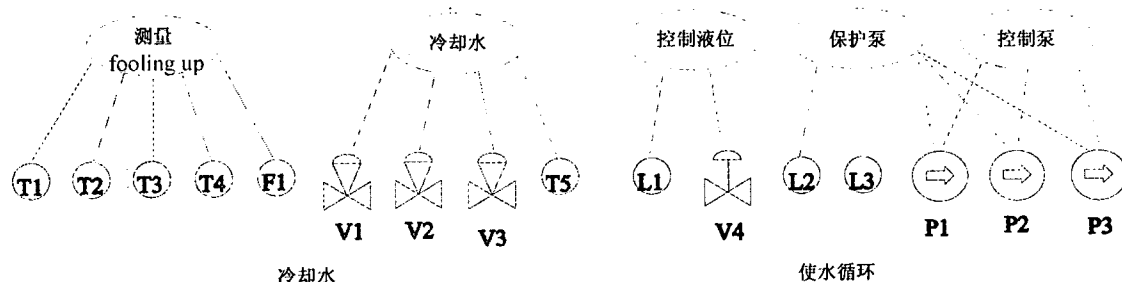


图 A.4 来自扩展 P&ID 的控制功能的提取

在上图的例子中,控制功能的层次是水平的,仅有控制功能的一个层次。因为这个过程容易控制并且这个控制应用的自动化级别低。对于复杂的过程或级别的自动化应用,就要用到高于控制功能第一层的控制功能。

A.1.1.2.4.3 控制功能的需求和标准化 AB 的需求

CHD 是控制功能的层次化表示,明确地描述了控制功能和过程接口、变送器和执行器之间的关系。在 CHD 中,过程工程师将指定控制功能和 AB 的需求。

AB 是私有应用库的标准块。标准块重用的目的是降低成本并提高控制应用的质量。对于每个控制功能,过程工程师选择并指定适合于控制功能和被控过程的 AB 的需求。

例如,对于控制功能“测量 fooling up”,过程工程师从 AB 库中选择适合于不同类型变送器 T1、T2、T3、T4 和 F1 的 AB,并设置每个 AB 关于变送器类型和过程约束的需求。为其他控制功能“冷却水”、“控制液位”、“保护泵”和“控制泵”填充 AB 需求。

图 A.5 是前面图 A.4 的改进。在控制层次图 CHD 中,可以看出为每个控制功能选择的应用功能块。

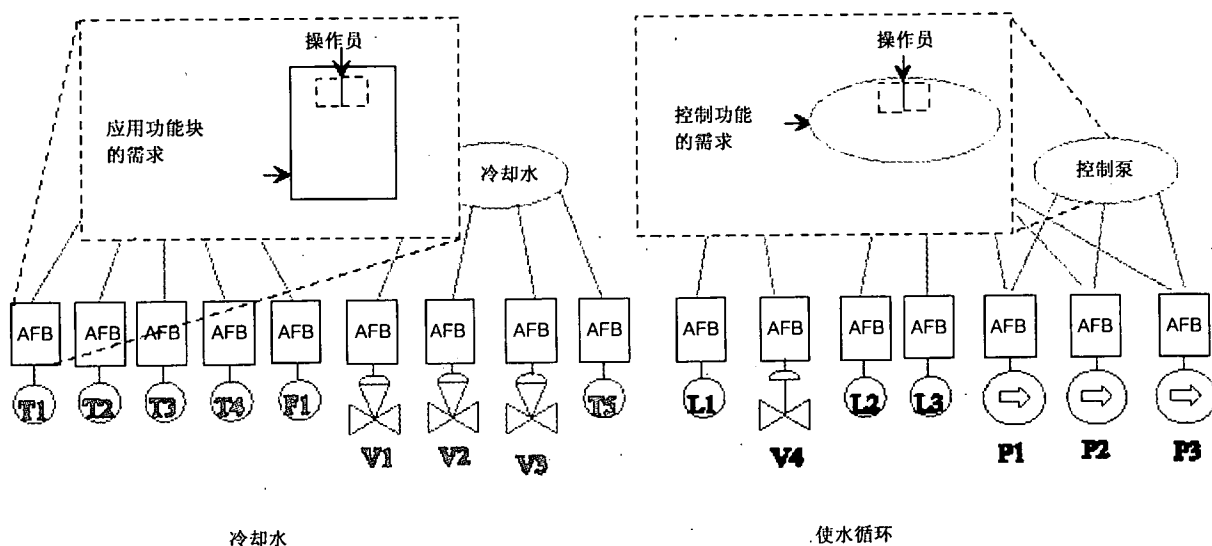


图 A.5 控制功能和 AB 的需求

注:点线表明是 AB 的基本需求,操作员接口从 AB 得到。

控制工程师选择并填充不同类型应用 FB,如测量、执行、切换等的需求。应用 FB 的需求是受限制的,例如精确性、采样时间、处于哪个状态的操作员接口数目、操作员命令和执行器操作之间的响应时间、接口有效性、安全及其他。

也需要完成控制功能的需求,例如控制环的采样时间、报警检测和保护操作之间的响应时间。AB 和控制功能的需求都是功能性的:在这一阶段,并不知道控制功能会在哪一个 I&C 系统中实现,但是有

足够的信息可以估计任何 I&C 的大小并准备投标要求。

A. 1. 1. 2. 4. 4 功能需求图文档的结构化

图 A. 6 给出了 FRD 的文档组织结构。FRD 是一组 Folio, 在这些 Folio 上使用 FB 详细描述了控制功能。结构化 FRD 的文档意味着分配控制功能到 Folio 中。

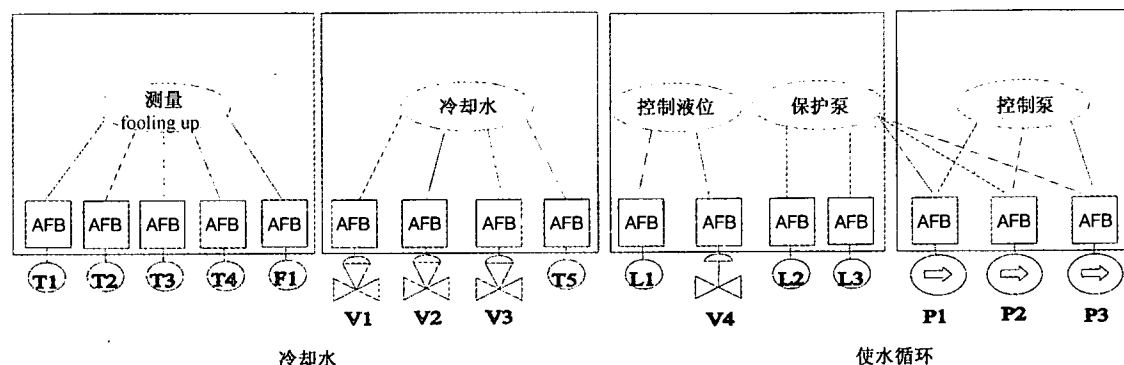


图 A. 6 控制功能需求的结构化文档

一个 Folio 可以支持一个或多个控制功能, 这由过程工程师来决定。图 A. 6 是一个例子, 过程工程师指派控制功能“测量 fooling up”到 Folio 1, “冷却水”到 Folio 2, “控制液位”和“保护泵”到 Folio 3, “控制泵”到 Folio 4。一旦完成了控制功能和 AB 的需求, 并分配到 Folio 中, 就可获得未来控制系统的清晰、明确的需求文档。

A. 1. 1. 2. 5 FRD 的使用

A. 1. 1. 2. 5. 1 Folio: FRD 文档结构的关键

FRD 是控制功能的详细需求。这些详细需求在 Folio 中被描述为 Folio 的 EFB 和 AB 的网络。在 CHD 中选择这些 Folio。

FRD 中 Folio 完整的描述需要填充 Folio 的四部分。左边部分描述了输入信号, 右边部分描述了输出信号, Folio 的中间部分是根据 FB 网络描述的信号处理, 低下部分描述的是 Folio 的标题。Folio 的四部分如图 A. 7 所示。

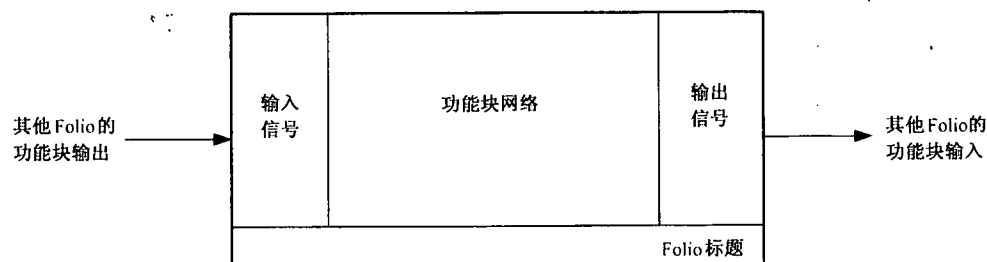


图 A. 7 Folio 的四部分

Folio 的输入信号来自其他 Folio 的输出。Folio 的输入信号用作 Folio 中某些 FB 的输入。

Folio 的输出信号用作其他 Folio 的输入数据。Folio 的输出信号来自 Folio 中某些 FB 的输出。

A. 1. 1. 2. 5. 2 控制功能详细需求的 Folio

在 CHD 中, 过程工程师分配控制功能到 Folio 中(一个 Folio 可以支持一个或多个控制功能), 例如, 测量和执行选择不同类型的 AB。为了详述控制功能的需求, 过程工程师使用 Folio。

考虑 Folio, 除了先前在 CHD 中选择的 AB 以外, 过程工程师只有一个空的 Folio。详述 Folio 中的控制功能的需求意味着构造 EFB 和 AB 的网络。为了使用 EFB 组成 AB 网络, 过程工程师将选择 AB 的输入和输出。下面的图 A. 8 简述了考虑 Folio 并选择 AB 的输入输出。

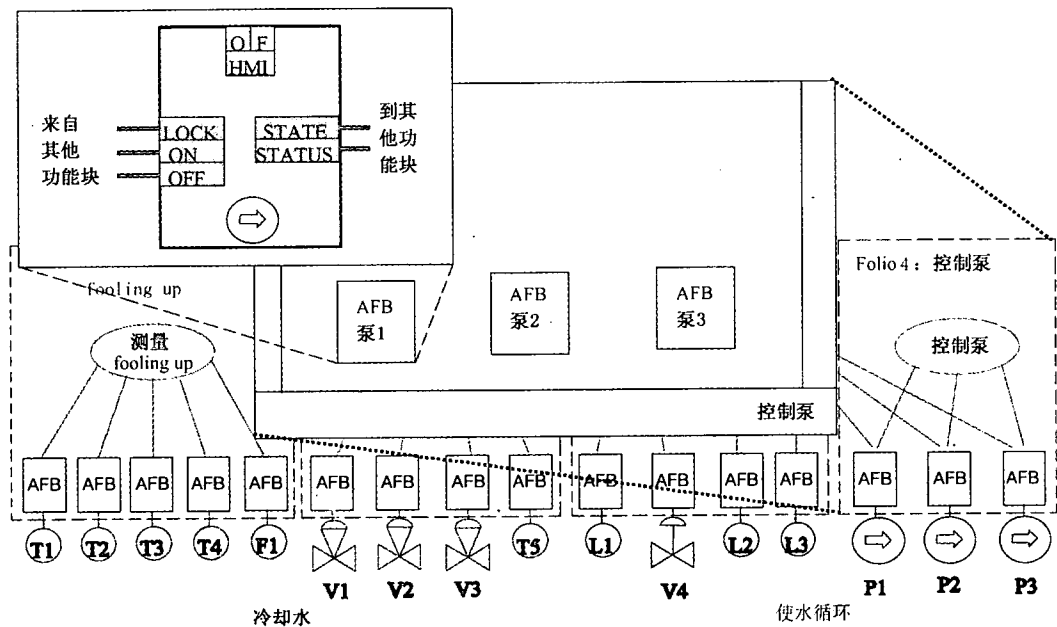


图 A.8 从控制层次图中选择 Folio

A.1.1.2.5.3 完成支持控制功能的 Folio

为了完成 Folio 中控制功能的详细需求,过程工程师需要填充 Folio 的四部分。
Folio 的输入信号必须与来自其他 Folio 的信号一致。Folio 的输出信号必须与其他 Folio 中使用的信号一致。例如,参考图 A.6,在控制功能“保护泵”和控制功能“控制泵”间有一个连接,这是一个保护信号,当容器的液位太低时关闭泵。因为控制功能“保护泵”在 Folio3 中详细描述,控制功能“控制泵”在 Folio4 中详细描述,所以这个连接代表 Folio3 的输出信号和 Folio4 的输入信号。在 Folio4 中,这个信号输入将连接到泵的 AB。

为了描述控制功能的特性,过程工程师根据控制功能的需求和目的,将 EFB 和 AB 组成网络。
图 A.9 是控制功能“控制泵”已完成的 Folio 的例子。该图是一个真实的例子,控制功能的特性是 EFB 和 AB 详细的网络(三个泵执行 AB 和一个三取二切换 AB)。

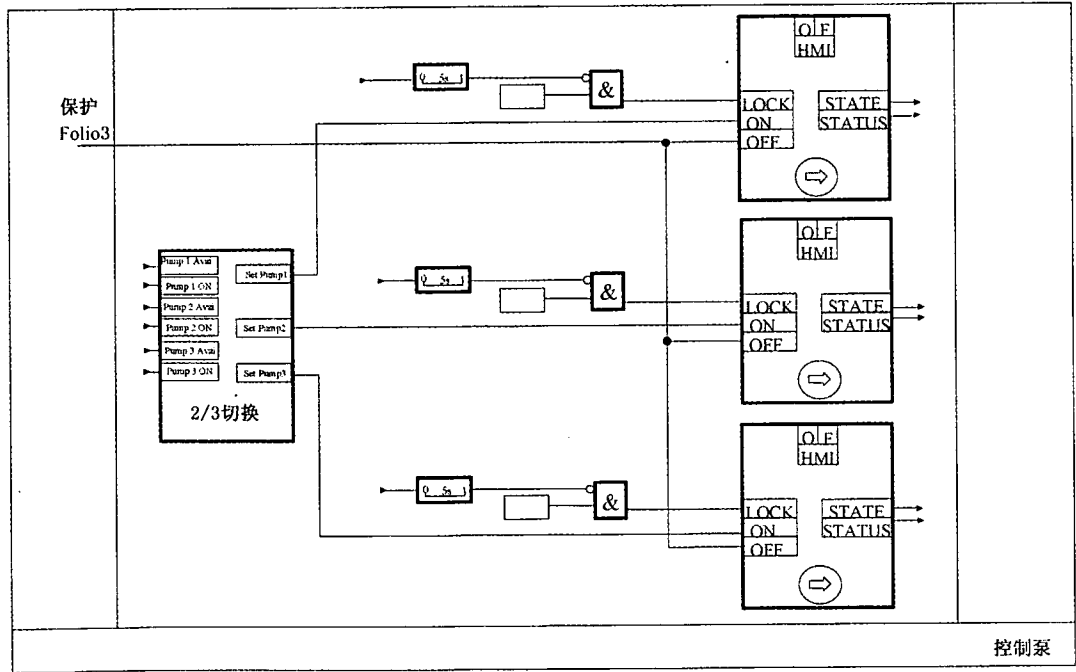


图 A.9 控制功能“控制泵”详细需求的 Folio

A. 1. 1. 2. 5. 4 作为 Folio 集合的 FRD

过程工程师将详述所有分配到 Folio 的控制功能。对于每个 Folio,他们会填充它的四个部分。对于每个控制功能的特性,他们会添加 EFB 和 AB 的合适网络,如图 A. 10。一旦完成了 Folio 的描述,FRD 就准备好了。

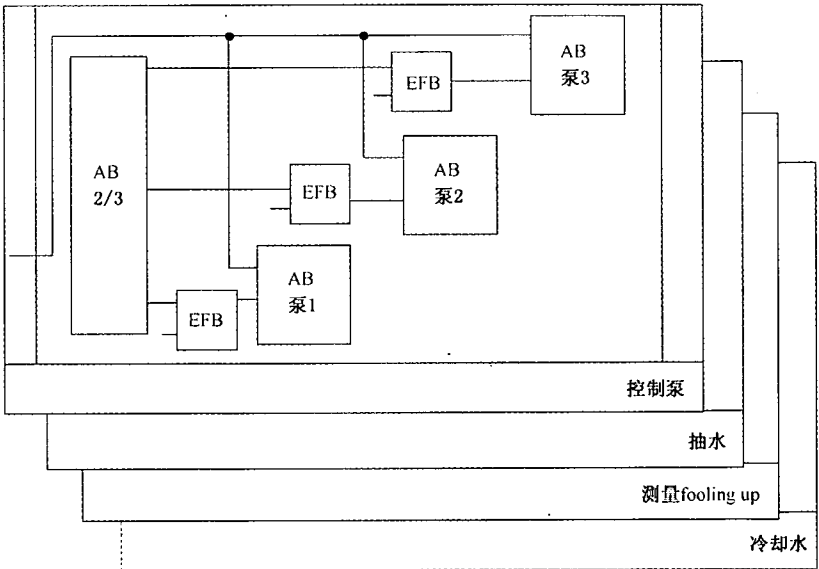


图 A. 10 FRD 的示例

图 A. 10 中,FRD 的四个 Folio 描述了控制功能的详细需求,这些控制功能是在先前的 CHD 中分配到这些 Folio 中的。控制功能“控制泵”的图形表示是被简化了的。

过程工程师还定义附加到 EFB 和 AB 上的约束,如安全性、可用性和时间约束。(例如,功能块处理顺序、EFB 和 AB 的实现约束;某些 EFB 和 AB 必须在同一 I&C 设备中一起实现,其他某些 EFB 和 AB 不能在同一 I&C 设备一起实现)。

FRD 应该被视为控制过程的控制功能的规范。FRD 不是程序设计方案。FRD 描述了控制功能(EFB 和 AB 的网络)、未来实现 FRD 的 I&C 系统的性能和约束(可用性,安全性)。

图 A. 11 描述了独立于 I&C 系统实现的 FRD。

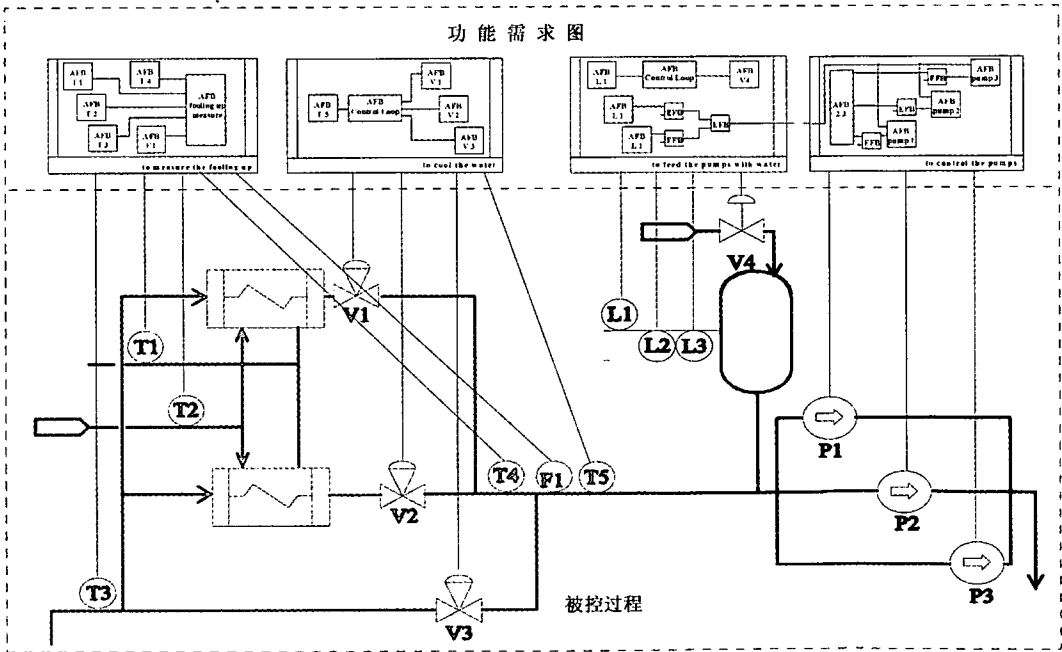


图 A. 11 独立于 I&C 系统实现的功能需求图

A.1.1.2.6 标准 FB 语言的需求

A.1.1.2.6.1 概述

在前面的章节中,已经为每个控制应用建立了功能需求图。工程公司需要工程 FB 语言来描述 FRD。I&C 提供商需要编程 FB 语言以便在 I&C 系统中实现这些 FRD。

工程 FB 语言要与编程 FB 语言兼容,如图 A.12。这意味着需要标准的 FB 语言作为核心来定义工程 FB 语言或编程 FB 语言。

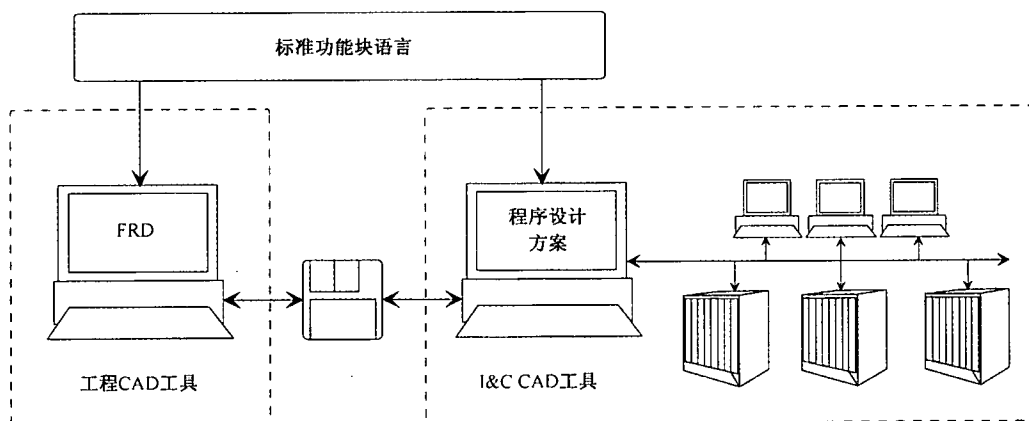


图 A.12 标准功能块语言的需要

标准 FB 语言的要求是:

- 它应该是创建工程 FB 语言和编程 FB 语言的核心。
- 它应该建立在标准的基础之上,特别是:
 - 它应该建立在标准的 EFB 之上;
 - 它应该建立在标准的构造规则之上,以定义可在 I&C 系统中实现的专用 AB(能源、制造、化工等)。

工程公司应该使用这种标准 FB 语言来定义自己的工程 FB 语言,以允许过程工程师描述控制应用的 FRD。

使用工程 FB 语言来描述 FRD,并不是意味着不考虑市场上可获得的 I&C 设备的性能。而是指定义的可在任何 I&C 系统中实现的 FRD 与这个标准兼容。

这也意味着 FRD 可在当前的可扩展的 I&C 系统和可升级的 I&C 系统中实现,通过 A.1.1.1.4 FB,可以在将来与这个标准兼容。

为了使用可通过任何编程语言实现的任何工程语言来描述 FRD,IEC 标准 FB 语言要提供:

- 一个 EFB 的库;
- 创建 AB 的规则。

A.1.1.2.6.2 可用于 FRD 的 EFB 的需求

一个 EFB 是一个重复的数理逻辑处理,它嵌入在一个块中。EFB 是过程控制域内的特定处理模块。EFB 是不能被分割的。

EFB 的库应该是标准的。这个 EFB 的库应该满足不同类型工业(化工、能源、食品等)的需要(见图 A.13)。这个库应该是一个标准化的 EFB 核心库。这个库对于不同类型的工业和专用于某工业类型(如化工、能源、食品等)的库是通用的。

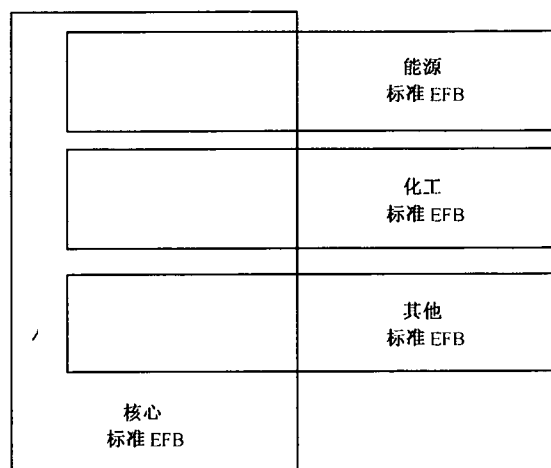


图 A.13 标准 EFB 库

EFB 应该是标准化的。每个块都需要标准的外部图形表示和其正规的内部特性描述。

FRD 和程序设计方案都要使用外部图形表示。

特性的正规内部描述应该使用 IEC 建议的正规语言。需要指出,GB/T 15969 建议的 ST 语言是不完全的。

因为 EFB 将在数字的 I&C 系统中实现,所以内部描述要包括块的正常特性和块的异常特性。需要指出,GB/T 15969 没有标准化块的异常特性。对于过程控制,特别是对于安全限制,在技术支持的一般故障影响某些块特性(如初始化、热启动、冷启动)的情况下,或特别故障影响某些块(如来自变送器的输入信号错误、同输入块冲突的 I&C 输入卡错误、同计算块冲突的上溢和下溢)的情况下,块的异常特性的定义是必须的。

A.1.1.2.6.3 用于 FRD 的 AB 的需求

一个 AB 是依赖于过程控制应用类型的一个可重用控制部分。

对于 EFB,AB 的外部 and 内部的表示是必要的。

因为 EFB 应该独立地实现,所以在 EFB 中,只使用 AB 的外部图形表示。AB(如测量和执行 AB)的内部特性完全取决于支持测量和执行的技术类型,所以一旦选择了支持 AB 的技术,AB 的内部特性将在程序设计方案中使用程序功能块语言来描述。

A.1.2 从 FRD 到实现

本条的目的是完成控制应用的 FB 的需求。工程公司需要 EFB 和 AB,使用工程 FB 语言来指定 FRD。这些 EFB 和 AB 通过程序设计方案,应该可实现于与本部分兼容的任何 I&C 系统和设备。

一旦定义并确认了 FRD 后,I&C 工程师必须通过 FRD 设计程序设计方案,并将这个程序设计方案实施于 I&C 系统和设备中,如图 A.14。

FRD 是独立于 I&C 系统的,这就意味着 FRD 是任何控制应用的长期规范,FRD 应该可实现于任何新应用的可升级的 I&C 系统和设备中。对于现有的 I&C 系统和设备,它也意味着,为了维护和更新现有 I&C 系统(部分或全部),FRD 应该可实现于升级后的新 I&C 系统和设备中。

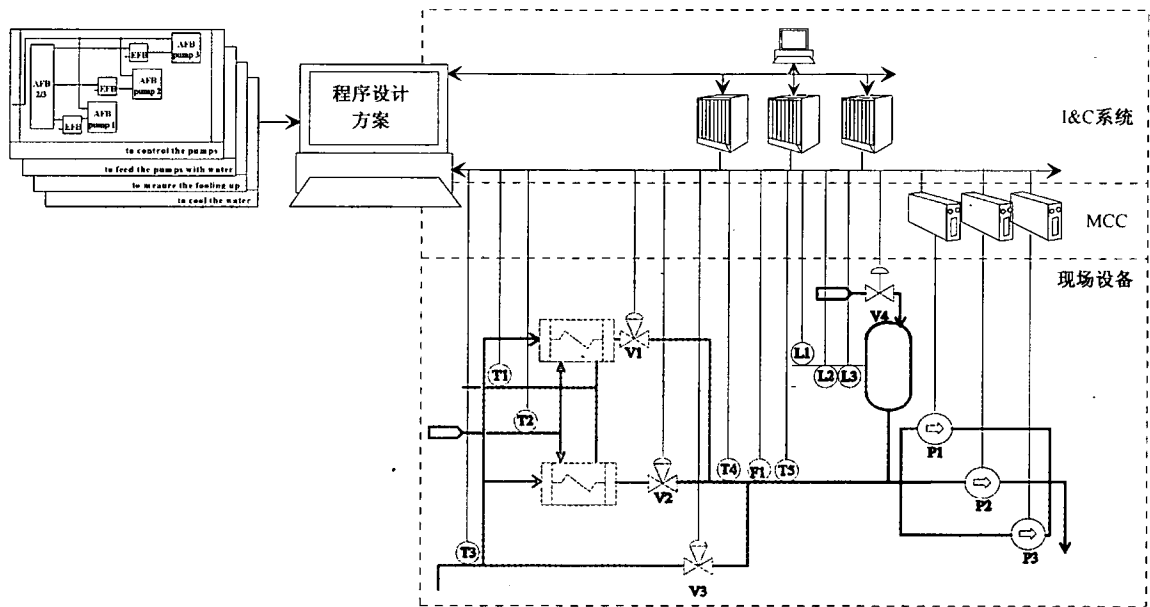


图 A.14 从功能需求图到 I&C 系统和设备

A.1.2.1 AB 的设计

A.1.2.1.1 概述

为了从 FRD 得到程序设计方案,应该设计 AB 的内部特性。

AB 应该由不同供应商交付的不同内部块组成。这些内部块应该被分配并实现于不同的 I&C 设备中。AB 可以分割为不同的内部块。

AB 可以具有过程接口(带有变送器和执行器)和人机界面。AB 可以没有过程接口或 HMI 接口。下面将给出两个例子。

A.1.2.1.2 执行 AB 的详细设计

图 A.15 表示了执行 AB 的一个执行及其内部块。这个例子关注于控制,执行应该典型地由不同提供商交付的不同设备组成。例如,提供商交付的智能执行器、提供商交付的智能电机控制中心 (MCC) 和实现于提供商交付的 I&C 系统的设备中的处理块。

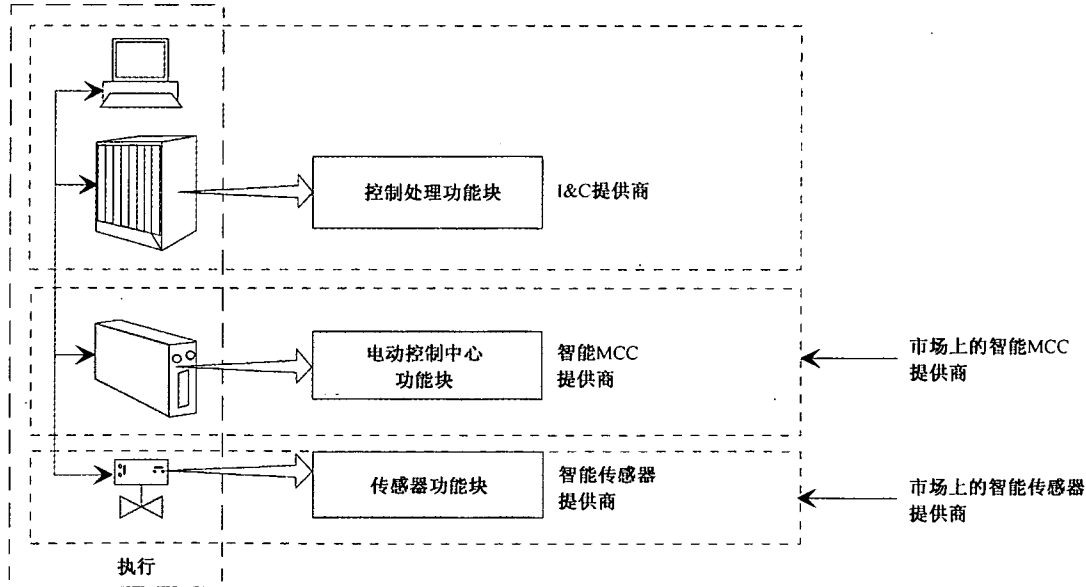


图 A.15 一个执行的设计及其来自现货供应的执行设备的 AB

这是不同类型执行的典型情况。不同的提供商为每一种执行交付执行设备。I&C 工程师选择符合过程工程师指定的需求的、现货供应的执行设备。无论选择什么样的设备,它们都会被集成在一起并且共同操作,以实现过程工程师所要求的执行。为实现互操作,创建的执行设备的内部块应该符合 IEC 标准。本部分允许执行设备提供商创建内部块。为了获得一致性的执行,内部块实现于执行设备中,它们通过硬连接的点对点数据连接或通过总线连接在一起并且相互操作。

图 A. 16 表明,在每个 FRD 中,过程工程师描述每个 AB 的需求和性能,实现是独立的,因为过程工程师不知道 AB 会在哪个 I&C 设备中实现。

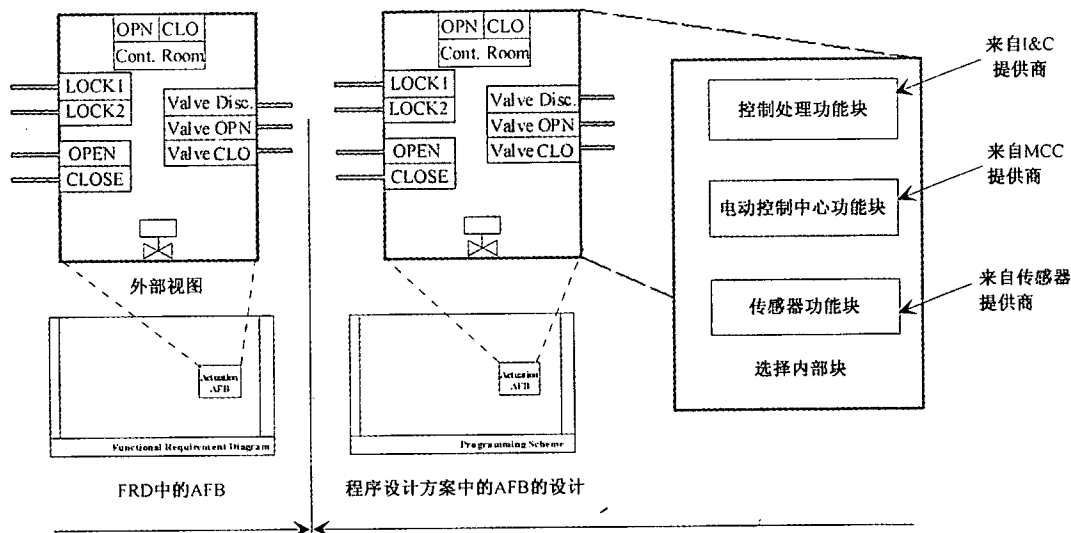


图 A. 16 来自现货供应执行设备的执行 AB 的内部特性设计

对于每个执行 AB 的设计, I&C 工程师应该从提供商那里选择符合过程工程师指定需求和性能的、现货供应的执行设备。I&C 工程师选择执行设备和执行 AB 的内部块。

一旦选定内部块后, I&C 工程师必须确保内部块的输入和输出是兼容的,然后将不同的内部块连接在一起并确保这些内部块的互操作与所要求的执行 AB 是一致的。

在某些情况下,现有的内部块可能不能满足需求, I&C 工程师应该增加扩展或创建内部块,例如在 I&C 设备中。

如图 A. 17, I&C 工程师还必须将这些执行 AB 与控制功能的 EFB 和 AB 连接成网络。执行 AB 的输入来自上游 EFB 和 AB 的输出,执行 AB 的输出连接到下游 EFB 和 AB 的输入。执行 AB 的输入连接到内部块的输入,输出连接到内部块的输出。

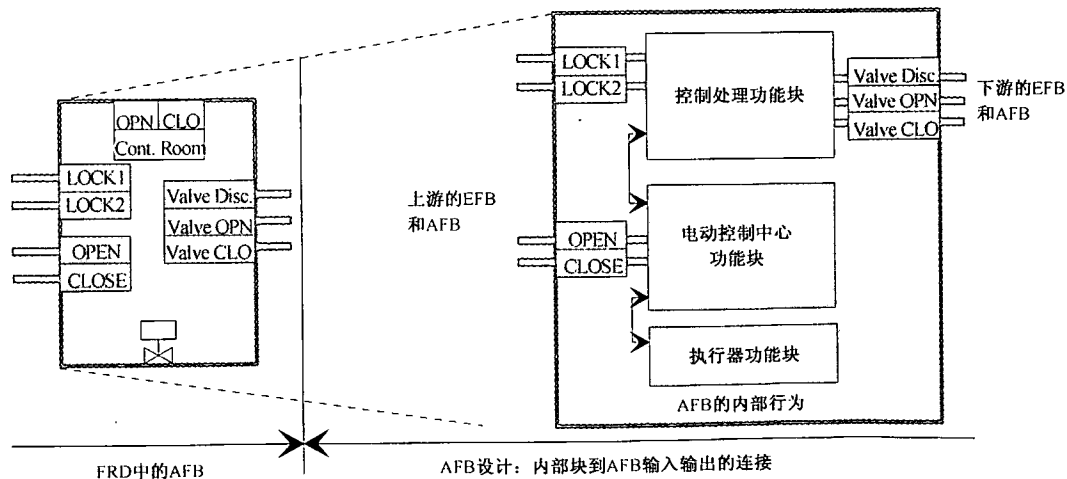


图 A. 17 AB 的内部块与控制功能的上游和下游 EFB 和 AB 的网络

在本例中,执行 AB 应该由三个内部块组成。控制处理内部块应该嵌入到 I&C 设备中,这个块应该支持人机界面、不同类型的命令(自动、手动、命令序列)、控制数据(例如执行的状态)和电机控制中心的命令。电机控制中心内部块应该嵌入在电机控制中心中,这个块应该支持命令优先级和控制数据(电机控制中心的状态)。执行内部块应该嵌入在智能执行器中,这个块应该支持控制数据(智能执行器的状态)。

这个执行 AB 有两种类型的接口,一个操作员接口,一个执行器接口,见图 A. 18。

在 FRD 和程序设计方案中,操作员接口应该使用标签(一个标签描述操作接口的类型,另一个标签描述来自操作员接口的命令的类型),在执行 AB 图形符号的上部清晰地描述。

对于执行器接口,现在,在执行 AB 的图形符号上没有清晰描述执行器接口的信息。执行器内部块应该连接到执行器的仪表(扭矩和位置),这种数据连接不应该在 FRD 和程序设计方案内的执行 AB 图标上清晰地描述。

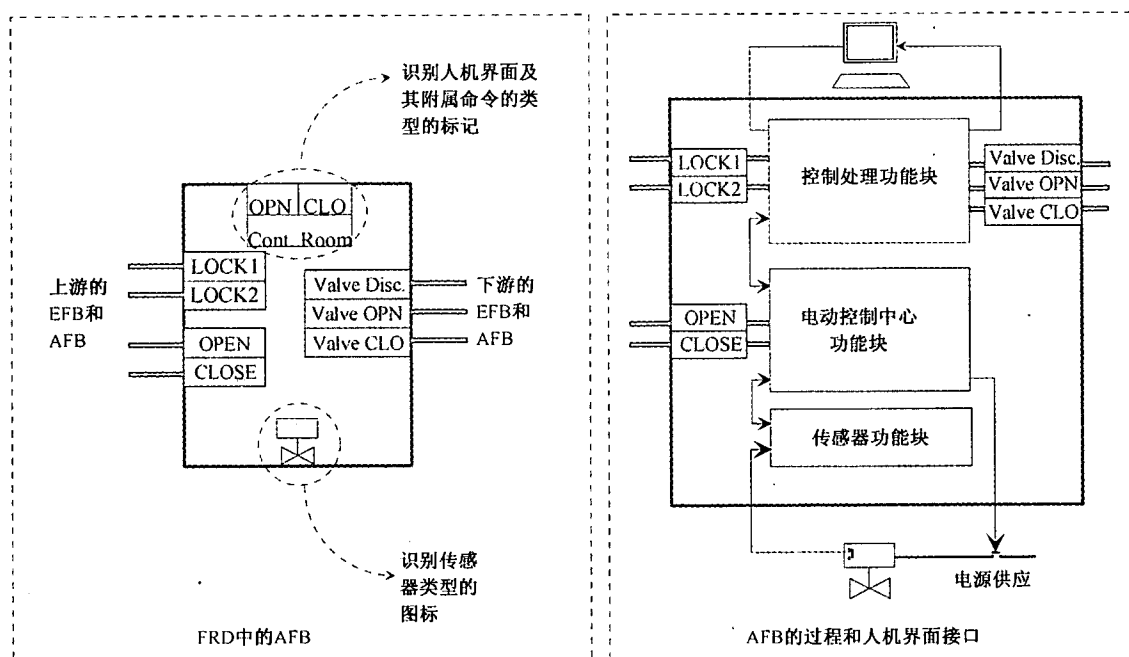


图 A. 18 执行 AB 的图形符号和不清晰的内部描述

图 A. 19 是使用 GB/T 19769.1—2005 系统模型的内部块分布到 I&C 设备中的执行 AB 的图示。

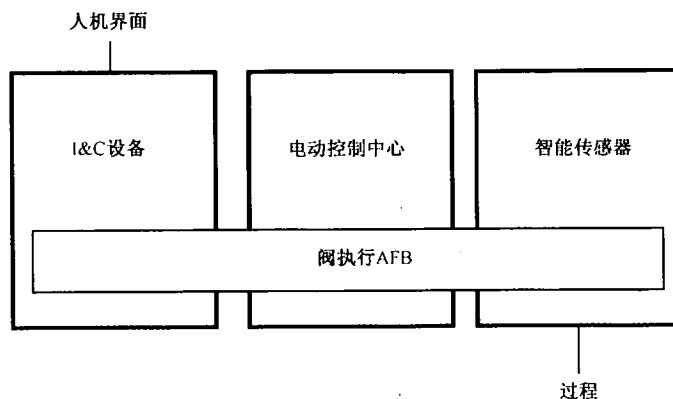


图 A. 19 使用 GB/T 19769.1—2005 系统模型的开/关(OFF/ON)阀执行 AB

图 A.20 是使用 GB/T 19769.1—2005 系统模型的执行 AB 内部块的图示。

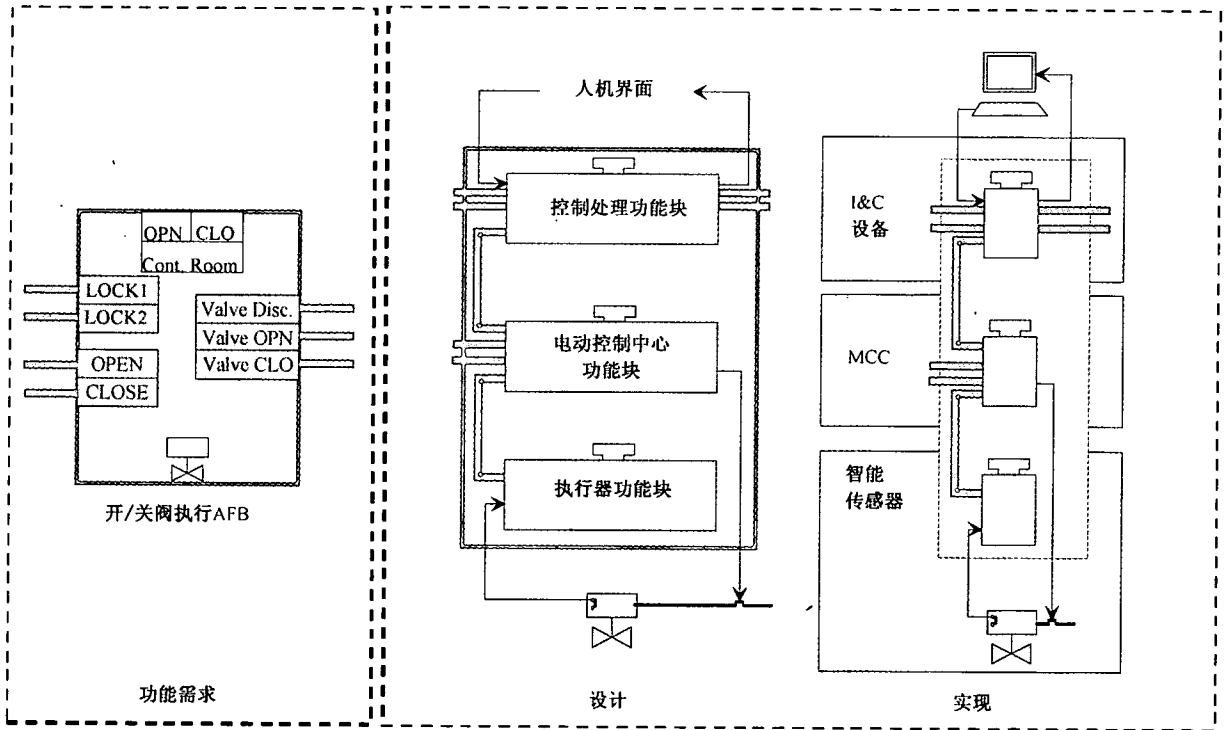


图 A.20 使用 GB/T 19769.1—2005 系统模型的 OFF/ON 执行 AB

A.1.2.1.3 三取二安全切换 AB 的详细设计

图 A.21 给出了一个没有过程接口也没有人机界面的 AB 的示例，即三取二安全切换。在标准的三取二切换功能作为 EFB 的情况下，这个 EFB 应该在单个的可编程控制器中实现。

为了安全的应用，三取二安全切换必须在几个 PLC 中实现，以避免公共的故障。这种情况下，安全切换应建立在三取二 AB 之上，这个三取二切换 AB 由三个内部块组成。这三个内部块应该实现于三个 PLC 中。

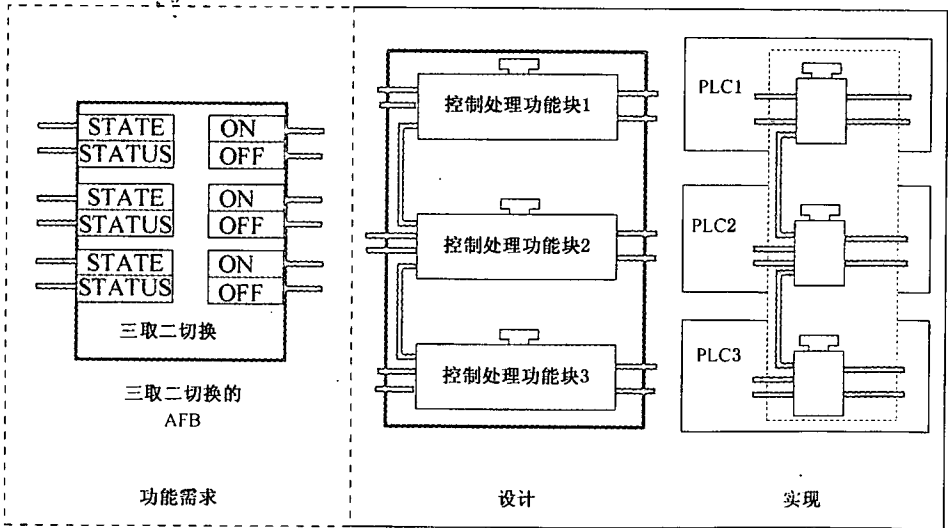


图 A.21 三取二安全切换 AB 的示例

图 A.22 给出了使用 GB/T 19769.1—2005 系统模型的执行 AB 的图示。

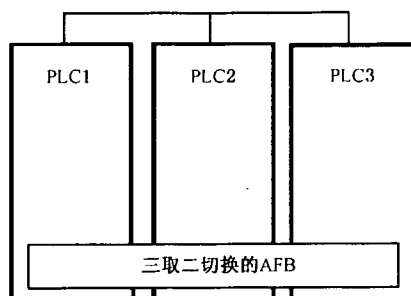


图 A.22 使用 GB/T 19769.1—2005 系统模型的三取二切换 AB

A.1.2.2 控制功能在 I&C 设备中的实现

A.1.2.2.1 概述

I&C 系统的结构是分布到不同层的设备的集合：

- 第 2 层：人机界面；
- 第 1 层：处理；
- 第 0 层：电源接口和现场设备。

随着市场上智能设备的出现，这些 I&C 层也会发展。新兴的技术使当前的控制孤岛易于集成、易于维护和管理（技术上的和经济上）。

第 2 层支持人机界面的控制、维护和管理。第 1 层支持处理的控制、维护和管理。第 0 层支持智能电源接口和现场设备。

下面的条款关注于控制功能，同时维护和管理被看作是同一原则的扩展。

A.1.2.2.2 从 FRD 到完整的控制功能的设计

作为一个例子，Folio 4 专注于单个的控制功能“控制泵”。图 A.23 给出了 FRD。控制功能“控制泵”被描述为 EFB 和 AB 的网络。

AB 的设计应该由 I&C 工程师在选定 I&C 结构和不同类型设备后完成。从 FRD 到程序设计方案，I&C 工程师按照需求和控制系统的结构，使用泵执行器现有的设备和 I&C 系统中三取二安全切换的现有的库来设计 AB。

为了控制功能的完整设计，必须设计四个 AB。泵 AB 的内部块应嵌入到泵执行器的不同设备中。三取二切换 AB 的内部块应该包含在 I&C 提供商的库中。图 A.23 给出了一个控制功能完整设计的示例。

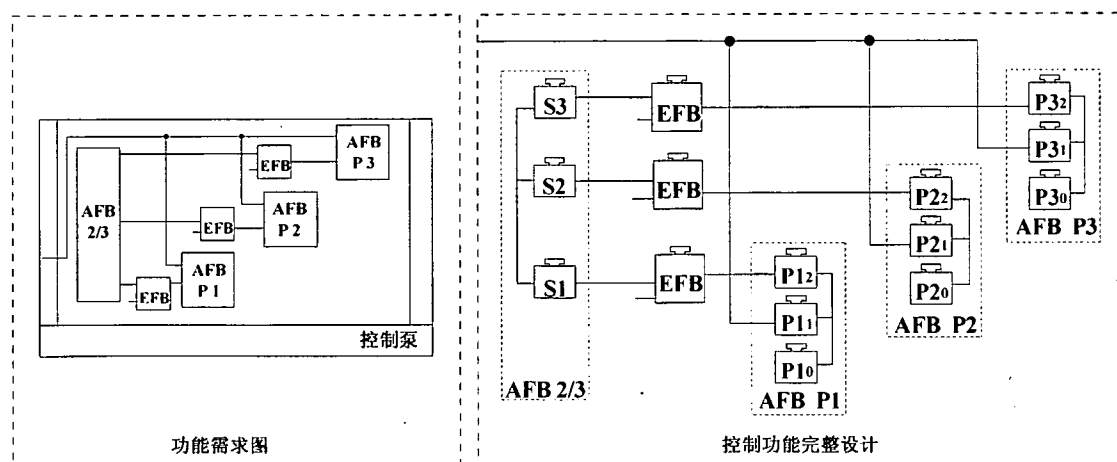


图 A.23 使用 GB/T 19769.1—2005 系统模型的从 FRD 到程序设计方案

对于每个泵执行 AB，三个内部块应该分布到 I&C 系统的三个层中。例如，分配第 0 层到电动控制

中心(MCC), 分配第 1 层到 PLC, 分配第 2 层到人机界面(HMI), 见图 A. 24。

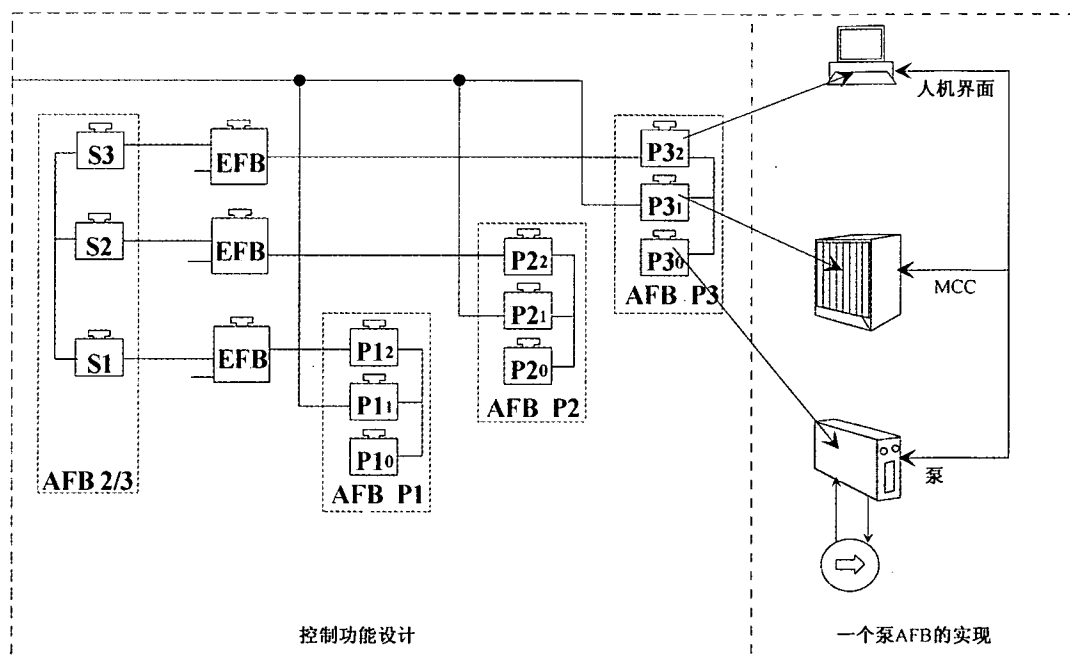


图 A. 24 泵 AB 的内部块分布

A. 1. 2. 2. 3 从完整设计到将控制功能的内部块分布到 I&C 结构

一旦完成了 AB 的设计, EFB 和 AB 中的内部块将被分配到 I&C 系统结构中。

I&C 工程师, 考虑 FRD 所要求的安全性、可用性和性能限制, 将块分配到 I&C 设备中。

在图 A. 16 中, 因为安全性限制, 三取二切换 AB 必须分配到三个不同的 PLC 中, 并且泵执行 AB 应该实现于单独的设备中, 以避免公共的故障。

对于泵 1 执行 AB, 内部块 P10 被分配到第 0 层的 MCC1 中, 内部块 P11 被分配到第 1 层的 PLC1 中, 内部块 P12 被分配到第 2 层的 HMI 中。

对于泵 2 执行 AB, 内部块 P20 被分配到第 0 层的 MCC2 中, 内部块 P21 被分配到第 1 层的 PLC2 中, 内部块 P22 被分配到第 2 层的 HMI 中。

对于泵 3 执行 AB, 内部块 P30 被分配到第 0 层的 MCC3 中, 内部块 P31 被分配到第 1 层的 PLC3 中, 内部块 P32 被分配到第 2 层的 HMI 中。

对于三取二切换 AB, 内部块 S1 被分配到第 1 层的 PLC1 中, 内部块 S2 被分配到第 1 层的 PLC2 中, 内部块 S3 被分配到第 1 层的 PLC3 中。

EFB 被分配到第 1 层的 PLC 中, 见图 A. 25。每个 EFB 都会在同一的 PLC 中作为上游和下游内部块实现。例如, 在三取二切换 AB 的 S1 内部块与泵 1 执行 AB 的 P12 内部块之间的 EFB 将在 PLC1 中实现。

在分配 EFB 和 AB 的内部块到 I&C 设备中期间, 需要 I&C 设备之间的通信。在这一阶段, I&C 工程师要清楚地知道不同 I&C 设备之间的交换数据的类型和数量。基于这一点, I&C 工程师应该按照通信的需要, 能够确认 I&C 设备中可获得的通信带宽。

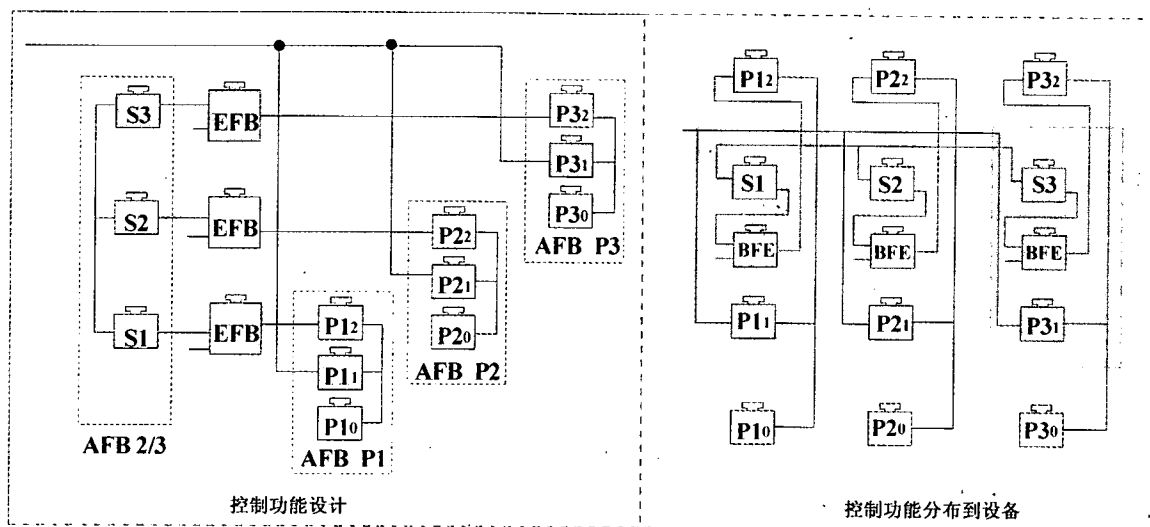


图 A.25 分布 EFB 和控制功能“控制泵”的 AB 到 I&C 结构

A.1.2.2.4 从分配到控制功能在 I&C 设备中的实现

一旦 I&C 工程师完成了 EFB 和 AB 的内部块的分配,控制功能将被分配到 I&C 结构的设备中。控制功能可以在 I&C 系统设备中实现,见图 A.27。

对于第 2 层,有一个专用的设备作为人机界面来多路转换三个泵执行 AB 的三个内部块 P12、P22 和 P32。

对于第 1 层,PLC1 用来多路转换泵 1 执行 AB 的内部块 P11、三取二切换 AB 的内部块 S1 以及这两个块间的 EFB。PLC2 用来多路转换泵 2 执行 AB 的内部块 P21、三取二切换 AB 的内部块 S2 以及这两个块间的 EFB。PLC3 用来多路转换泵 3 执行 AB 的内部块 P31、三取二切换 AB 的内部块 S3 以及这两个块间的 EFB。

对于第 0 层,MCC1 专用于泵 1 执行 AB 的内部块 P10,MCC2 专用于泵 2 执行 AB 的内部块 P20,MCC3 专用于泵 3 执行 AB 的内部块 P30。

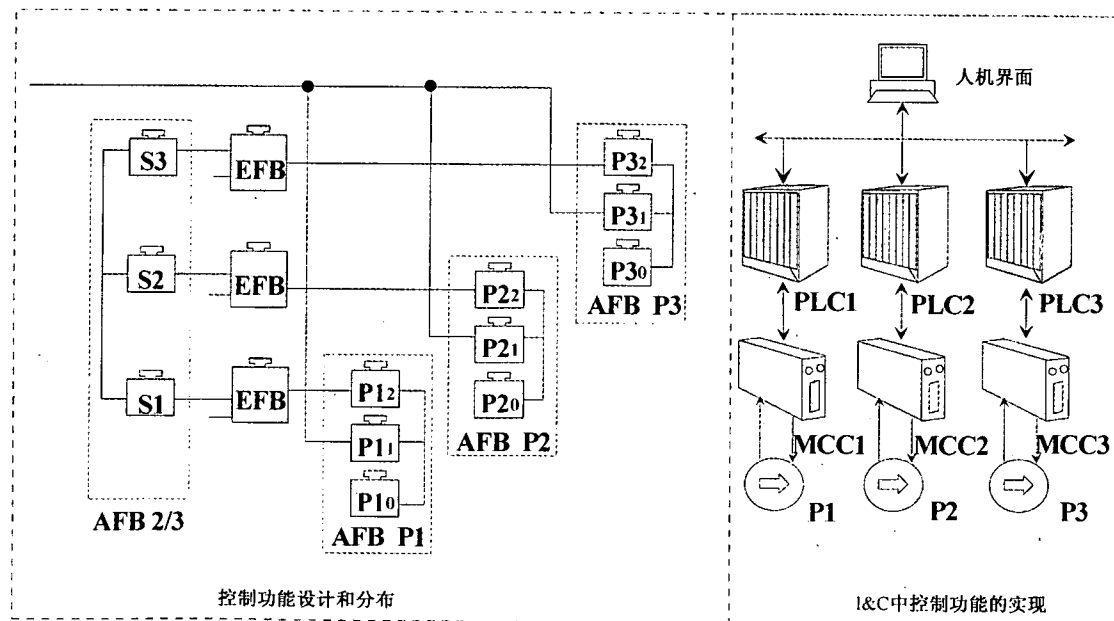


图 A.26 控制功能在 I&C 设备中的实现

图 A.26 是控制功能“控制泵”在 I&C 系统设备中的实现的示例。图 A.27 使用了

GB/T 19769.1—2005系统模型来描述控制系统。

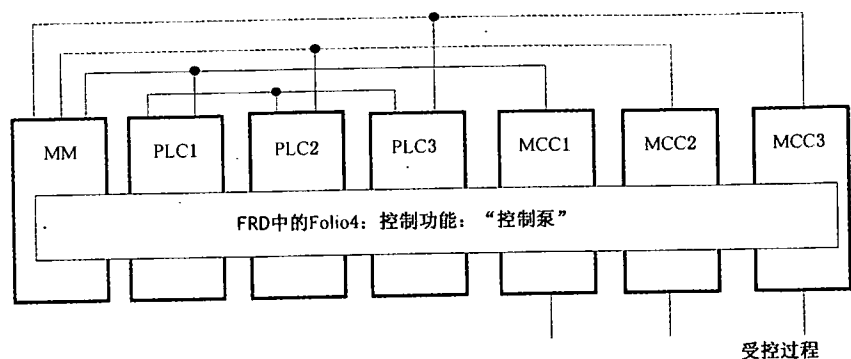


图 A.27 使用 GB/T 19769.1—2005 的控制功能“控制泵”的分布

A.1.2.2.5 从 FRD 到控制应用在 I&C 设备中实现

I&C 工程师应该为 FRD 的每个控制功能设计 AB。按照需求,考虑可现货供应的 I&C 设备的性能,选择 AB 的内部块。I&C 工程师应该为某些 AB 定义内部块。一旦完成了 AB 的设计,就可获得实现于 I&C 设备中的程序设计方案,见图 A.28。

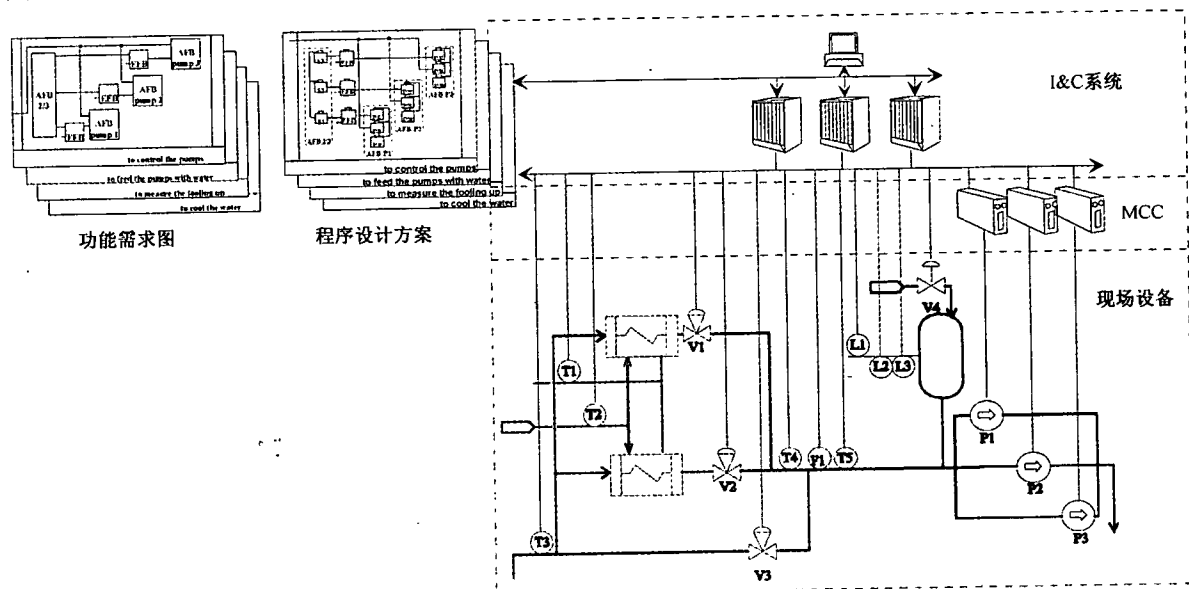


图 A.28 从 FRD 到程序设计方案

A.1.2.3 控制功能设计和实现的需求

EFB 和 AB 的内部行为应该用统一的标准的形式化语言来描述。应该指出,GB/T 15969 不能满足这种需求。未来的 IEC 标准应该提出构造规则和语言(语法和语义)来描述 EFB 和 AB 内部块的内部行为。通过这种标准的语言,应该能够建立 AB,存储这些 AB 到私有的库中,将这些 AB 用于应用中,在符合这个标准的不同技术支持下分布和实现这些 AB。这个标准应该是完整的并且考虑技术支持的正常和异常操作、处理和通信支持。

这个标准应该考虑 AB 中分布式、同步内部块的分布和协作的所有技术方面。

- 允许 I&C 工程师描述 EFB 和内部块的正常及异常行为(如变量类型、声明、语法、语义、形式证明等)的形式化语言。
- EFB 的标准集合,包括正常和异常操作。
- 创建内部块的正常和异常操作的规则。
- 支持这些块的设备的异常操作的 EFB 和内部块的标准行为。如:

- 初始化、热启动、冷启动；
- 输入输出硬件故障、组件故障；
- 计算错误、上溢、下溢(特别注意舍入错误和舍入的传播)。
 - 在一个设备内和分布在多个设备中的 EFB 和 AB 的同步和排序规则。
 - EFB 和 AB 的内部数据的管理规则。
 - 在 EFB、AB 和 AB 内部块之间的数据共享规则。
 - 在一个设备内和分布在多个设备中的 EFB 和 AB 之间的数据交换规则。
 - 在一个设备内和分布在多个设备中的 AB 的内部块的同步和排序规则。
 - 在一个设备内和分布在多个设备中的 AB 的内部块的数据交换规则。
 - 与其他 EFB 和 AB 的数据交换规则。

附 录 B
(资料性附录)
FB 功能性需求:用户视图

B.1 概述

模型化系统是一件巨大的任务。单个的模型不能获取描述一个系统所需的所有信息。GB/T 19769.1—2005为工业测量和控制系统(IPMCS)的分布式功能块应用制定了通用的标准。GB/T 19769.1—2005包括以下模型:

- 应用模型;
- 设备模型;
- 资源模型;
- FB 模型;
- 系统模型。

GB/T 21099.2 中采用的识别功能需求的详细方法考虑了描述用户期望的系统用户视图模型。

这种视图提供了系统用法(要求的功能性)的通用描述。这种视图是中心的。系统的最终目的是提供通过这种视图来描述的功能性以及一些非功能性属性。因此,这种视图将影响所有其他方面。

也建议将这种视图用于 FB 规范和用户期望之间的一致性测试(问:“用户定义的哪个功能单元被这个功能块规范所覆盖?”以及“这个功能单元被 FB 规范覆盖的程度?”)。

本附录收集了关于系统用户视图模型的所有概念,因为在需求规范中将考虑它们。

B.2 定义

B.2.1 概述

为了该附录使用方便,以下的定义补充了 GB/T 19769.1—2005 给出的定义。

B.2.2 规范术语列表

B.2.2.1

智能执行和测量 Intelligent Actuation and Measurement; IAM

CMM 系统所需的所有执行和测量的所有需求的总和。

注:这里的智能指提供用户所需的所有功能。

B.2.2.2

访问权限管理功能 access right management function

该功能提供了 IAM 不同组成部分和 IAM 用户之间所需的“握手”。作为系统需求的结果,对于每个 IAM 操作模式,一些 IAM 功能是活动的,另一些是非活动的。

IAM 的实际操作模式和其组成成分受到自动化系统管理功能的影响。这个功能也负责协调从实际操作模式到其他模式的转换。

代理和 IAM(或其部分)之间所有的交互都由与操作模式的关系来调节,以允许这些功能的仅被授权的交互起作用,如系统需求的规定,这些功能可以在每一操作模式中是活动的。因此,对于 IAM(或其部分)的每一操作模式:

- 一组 IAM 功能被激活;
- 只能完成指定的交互,其他的(不允许的)交互无效。

建议标准化一个矩阵,它的行列出潜在的操作模式,列列出与 IAM(或其部分)潜在的交互。基于每个用户的需求来决定(通过标记对应行和列的交叉点)交互的授权(例如,当参数化系统的时候)。

B.2.2.3

代理 agent

使用 IAM 的任何人(如操作员)或任何事物(如设备)。沿着 IAM 生命周期的特定阶段,每一个代理与 IAM 进行交互。

B.2.2.4

校正维护 corrective maintenance

故障发生后执行的维护,目的在于使某项恢复到可以执行所要求功能的某个状态。

B.2.2.5

功能校验 functional validation; F. VAL

- 对于测量

F. VAL 是校验受检查的测量和来自受控过程的其他测量集合之间的一致性的功能。使用受控过程一个合适的模型来检查这种测量之间的联系。

- 对于执行

F. VAL 是校验阀的状态和测量(来自过程上游和下游阀)之间的一致性的功能,它定义了阀状态的实际效果。

B.2.2.6

维护 maintenance

所有的技术和相应管理活动的组合,其目的在于使某项保持或恢复到可以执行所要求功能的某个状态。

注 1: 更详细的维护的定义参见“预防维护”和“校正维护”。

注 2: 所要求的功能可以被定义为一个确定的条件。

注 3: 这里的维护关注 IA/IM-通道及其所有部分。

B.2.2.7

操作校验 operational validation; O. VAL

- 对于测量

O. VAL 是检查一个可信测量和来自多个冗余转换器(或一个转换器的冗余部分)的其他冗余测量(两个或更多)之间的一致性的功能。

注 1: 这是一个自底向上的过程。

- 对于执行

O. VAL 是校验执行器的任何状态或变量与操作员或反射处理设备发出的命令之间的一致性的功能。

O. VAL 也提供对阀-定位回路的性能是否偏离设计范围的检查。

注: 这是一个自顶向下的过程。

B.2.2.8

预防维护 preventive maintenance

根据预定义的标准(知识库)执行的维护,以降低设备故障和服务质量下降的可能性。

- 定期维护(时间或活动驱动):按预定义计划或使用次数(如启动次数)进行的预防维护。

- 基于状态的维护(条件或状态驱动):以设备性能降低的记录(如:自动诊断、磨损测量的结果)为基础执行的预防维护。它基于渐进的、部分的和间歇的故障的可见性。

B.2.2.9

系统(或设备)属性 system (or device) properties

为了方便设备的评估,如图 B.1,将属性分为了几个组。

注: 包含在 IEC 61069-1 和 61069-5 中。

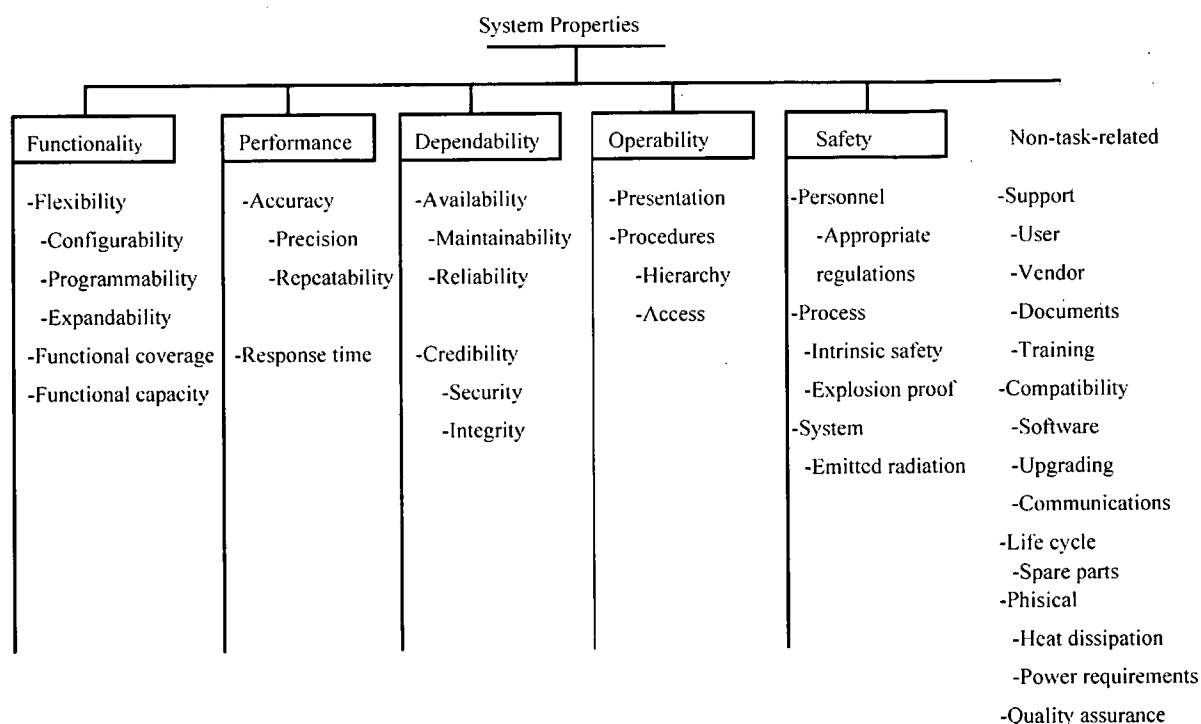


图 B.1 系统属性

注：IAM 系统的属性是为整个自动化系统而定义的。因此，IAM 系统的属性取决于每个 IAM 通道的每个单独部分的属性以及这些部分合作以执行通道功能的方法。当然，对于其每一功能，通道的属性可能不同。

B.2.2.10

技术校验 technological validation; T. VAL

a) 对于测量

——T. VAL 是提供电子、电源以及伴随变送器的感应变量的状态检查的功能，以确保相关参数在正常条件内；

——T. VAL 保证变送器已经产生了测量，该传感器工作在变送器状态报告所记载的检测条件下。

b) 对于执行

——T. VAL 是提供电子、电源和伴随执行器每一部分的感应变量的连续状态检测的功能。执行器包括：

- 处理能力；
- 电源接口；
- 电动机；
- 阀。

——T. VAL 保证执行器在已查明到的条件下操作，通过专用仪表来对状态进行执行和报告。

B.2.2.11

校验 validation

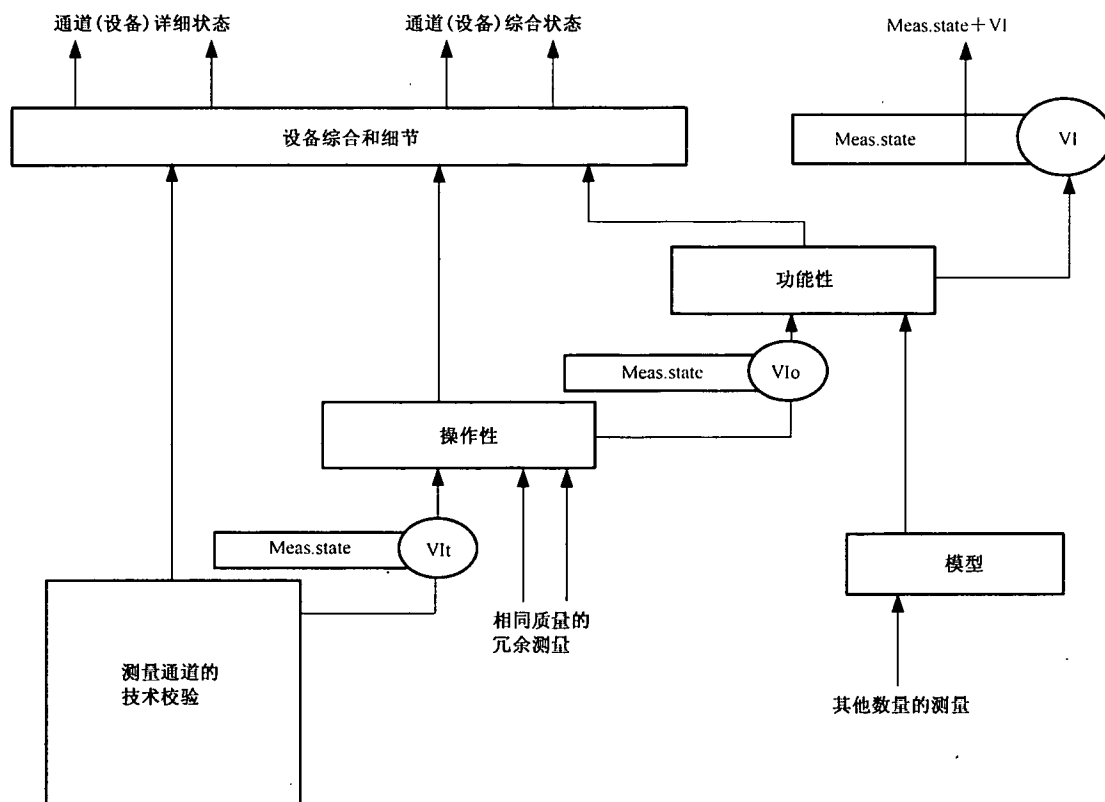
a) IA/IM-通道校验

校验是一种功能，是 IAM 宏功能的一部分 (state f., status f., 等.)。它的目的是检查每一完

整测量通道和执行通道的产品质量(状况:数据、活动等)和行为(状态)。检验只是执行器和变送器自身执行的一部分。

行为的一个重要的例子是及时地产生测量(或执行)。这里的及时定义为在同一时刻(在规定的抖动内)产生不同数量的测量(或执行)或者是在一个给定的采样周期下(在规定的抖动内)产生一个测量(或执行)的准时程度。

对于每个 IA/IM 通道,校验产生叫做“通道状态”的信息,见图 B. 2。



VI. t: 技术校验后的 VI

VI. o: 操作(+技术)校验后的 VI

VI: 有效性指数 (Validity Index)

图 B. 2 IA/IM-通道校验

对于 IA/IM 通道的结果(执行值、测量值等),校验决定了这些结果的质量,通过它们的 VI 表示(见测量不确定度, VI)。

IA/IM 通道校验可以被视为处于本字典定义三个层次中,见图 B. 2:

- 技术校验;
- 操作校验;
- 功能校验。

注 1: 划分是在进化的(如操作校验可以视为技术校验的一部分)。

注 2: 在实现层次上,校验分布于现场设备和通道的剩余部分中。

b) 现场设备校验

现场设备校验是 IA/IM 通道复杂功能的一部分,它同时检查它们的特性和结果(数据、活动

等)的质量。对于每个现场设备,校验产生叫做“设备状态”的信息。对于现场设备的结果,每一结果都伴随自身部分的 VI。这是现场设备中处理的部分校验的结果。

B.3 过程控制应用的功能视图

B.3.1 概述

数字现场通信(如现场总线)、智能现场设备(如转换器、执行器、开关设备等)、控制器的嵌入式软件等技术正有力地推动自动化的发展。它们实际上可以使制造商能转移部分功能到现场设备中,即使是部分地并且不太有效,传统地这部分位于集中式计算机中。这是很好的市场机会,可为用户需求提供更好的支持,假定终端用户制定了更明确和完整的需求并且需求对于实施是易于理解的。

B.3.2 功能需求和 FB 规范之间的关系

B.3.2.1 概述

在本部分中表示的功能需求列表定义在一个确定的抽象级别,该抽象级别的定义应该使得终端用户和提供商都容易理解。

该抽象级别不同于 FB 抽象级别。FB 抽象级别直接由提供商和系统集成商使用。

本部分定义的在一个较高抽象级别提供的“功能需求”与 GB/T 21099.2 定义的在一个较低抽象级别提供的“FB”之间没有必要一一对应。这两个抽象级别间的对应关系可以是一对一、一对多或多对一。

功能需求被视为是分布式应用需要达到的目标。

在每一 FB 的定义中,声明与此处描述的功能性要求的清晰关系是强制性的。

在需求期间的分布是处于现场仪表级别的,因为已经(至少部分)实现了。期望不久后,相同的逻辑方法在控制块级别也有效会成为现实。

将来需要描述用户视图模型,它被用作功能需求描述的基础。

B.3.3 智能执行和测量(IAM)与控制维护管理(CMM)

B.3.3.1 概念

用户视图模型的关键概念包括:

- CMM 概念:描述关于工厂操作控制、故障查找维护和技术管理的综合用户需要。
- IA 通道/IM 通道概念:描述关于 CMM 应用所指定的每个执行或测量的综合用户需要;通道的概念对应于系统(控制器)中带有附加功能的现场设备的恰当集成,能够回答用户的需要。

自动化可以辅助人类组织实现定义的目标。因此,用户需求辨识开始于对各种支持的逻辑总和的分析,该支持是与自动化系统相互作用的所有人类组织所需要的。分布式自动控制系统的参考功能结构是用户视图模型,见图 B.3。给出的系统作为人类组织的一个合适的合作者。建议将人类组织的活动使用 7 种任务来描述;具有相同名字的 7 个宏-功能(访问权限、标识、配置、参数化、按需测试、测量/执行、诊断),代表了系统提供的相应功能支持。

这同样适用于执行子系统和测量子系统以及 IA 通道和 IM 通道的所有组成子系统。

一旦通道作为一个整体来描述,所需要的功能支持表明了需要实现的目标,该目标由通过累加系统集成者用于创建通道所使用的所有组成部分的功能来计算。

系统生命周期所有阶段的人类组织

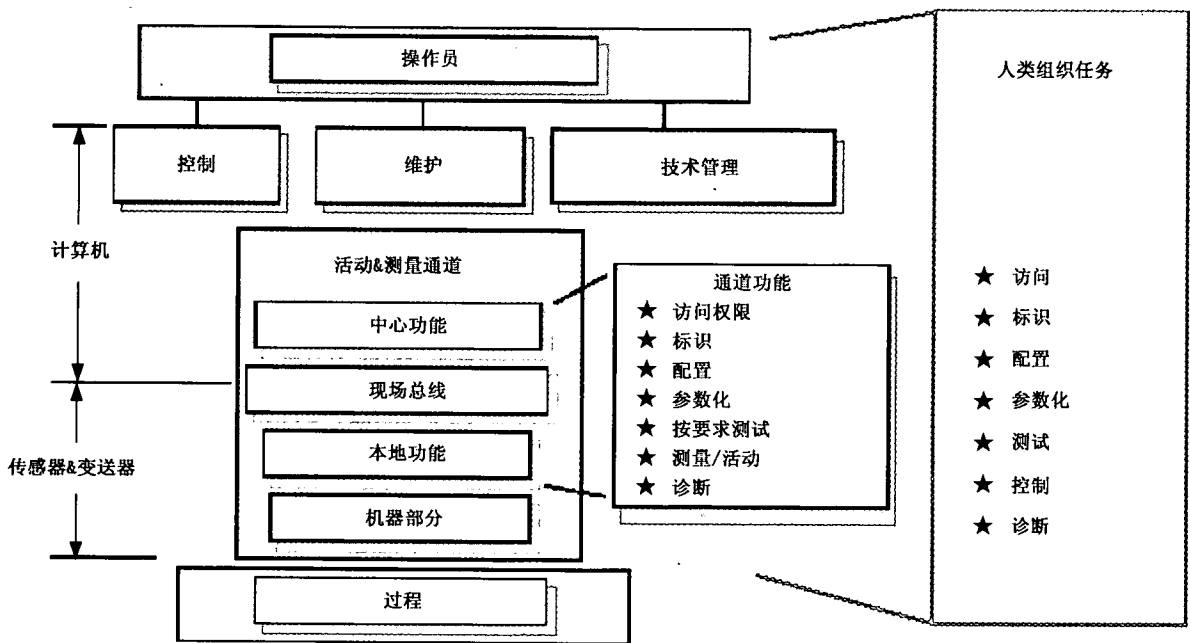


图 B.3 分布式自动控制系统的参考功能结构

参考功能结构是标识可能的功能需求列表的基础。它同样用于指导用户从完整列表中选择一部分，以标识自己的功能需求。

该指导不仅适用于终端用户，也适用于所有“使用”每个沿生命周期集成到相应 IA/IM 通道的设备的其他用户：制造商（厂内测试）、系统集成者、承包者（试运行测试）等。

B.3.3.2 CMM

最重要的 CMM 功能需求将在以下描述。这个需求表示了通过 IA/IM 通道的适当帮助所要达到的最终目标。

a) 控制需求

通过包含现场仪表异常情况的自动处理扩展了控制需求。这个自动处理相当于当前由控制操作员根据维护操作员的调查结果所做的处理。其好处来自于，例如，及时的自动化动作。为了包括系统的现场部分，对传统自动化系统的管理方法和异常处理规则的使用进行了扩展。一般地说，用户可以根据满足应用需求的通道的相应特性，为应用定义通道性能下降的一个或多个级别。

b) 现场仪表的维护

每一通道的每一可替换部分的实际状态的直接并且及时的可见性是有帮助的。对于每一可替换部分，预定义的级别是可以被辨认和记录的。这样，预防维护可以被组织为基于条件的维护。仅实际需要时才计划进行维护干预。附加信息的条文有助于这些干预。另外，有助于加快可替换部分修复的信息可以在用户与修理者之间的维护合同中定义并达成一致。

c) 技术管理

这特别涉及到设备中特定项目的性能和可靠性的评价。例如，来自不同厂商的两个阀在发生

故障前所达到的循环次数的比较,以及在相同操作环境下执行相同功能的比较。收集每一通道的每一可替换部分的使用历史和“健康”(条件)历史是基本的需求。目前,这种数据是非常有限的。因此,就很难进行工厂设备更改的管理决策所要求的详细及有效的统计分析。

B.3.3.3 IA/IM 通道

每一通道都必须提供参考功能结构中给出的功能支持。

图 B.4 给出了标识用户需求所不可缺少的最小粒度。这种级别的粒度主要在指定功能需求期间使用。有时使用更小的粒度。

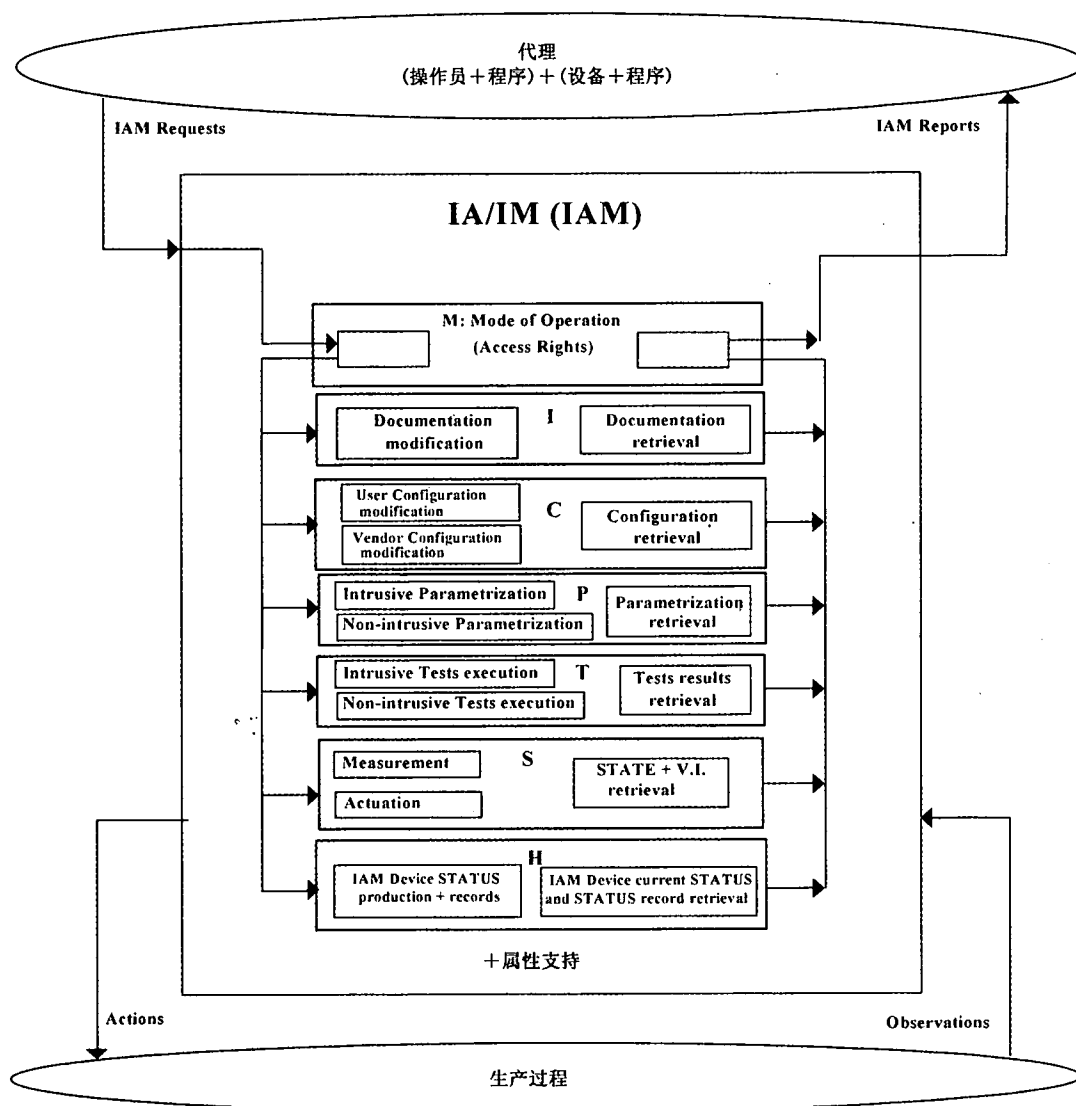


图 B.4 每个 IAM 功能的主要功能成分的用户视图

注: M=MACRO-FUNCTION 宏-功能操作模式

为了支持 IAM 系统及其在整体系统管理控制下的部分的操作模式的协调管理。基本上,这个功能管理每一代理对以上列出的任何 IAM 功能的预定义访问。作为用户需求的一部分,用户定义这种访问。

I=MACRO-FUNCTION 宏-功能标识

为了支持描述 IAM 系统的信息的存储和检索。

C=MACRO-FUNCTION 宏-功能配置

为了支持 IAM 系统功能配置的建立、修改或可视化。被视为系统(通道或设备)配置。

P=MACRO-FUNCTION 宏-功能参数化

为了支持 IAM 系统功能参数化的建立、修改或可视化。被视为系统(通道或设备)参数化。

T=MACRO-FUNCTION 宏-功能按需测试

为了支持自动化或半自动化 IAM 测试的执行和报告结果。

S=MACRO-FUNCTION 宏-功能声明

为了支持测量或活动的确认和伴随预定义 VI 的测量或活动的结果报告的完成。

注：这个功能由所有的用于支持指定 VI 和相关质量标准的诊断和校验补充。

H=MACRO-FUNCTION 宏-功能状态的状况和历史

为了产生系统(或设备)状态中定义的记录 IAM 状态的信息。这个功能由所有的用于支持 IAM 特性可视化的诊断和确认补充。

注：这些宏-功能的解释活动,是绑定 IAM 设备详细规范和 IAM 用户需求定义的关键。强制进行密切的合作，以保证在用户期望与 IAM 设备中执行的支持功能和属性之间的关系有清晰的定义。

IAM 的功能被聚类为 7 种宏-功能,它们可以被视为“目的”(或用户期望)和“行动”(制造商解释)。在图 B. 5 中,用一个黑盒子代表一个 IAM 通道,它明确地列出了与 CMM 和操作员相交换的信息。IA 通道用相似的方法来表示,主要是将“测量+VI”用“执行+VI”来代替。如前所述,整个通道的功能视图就是提供许多通道成分的合适集成。

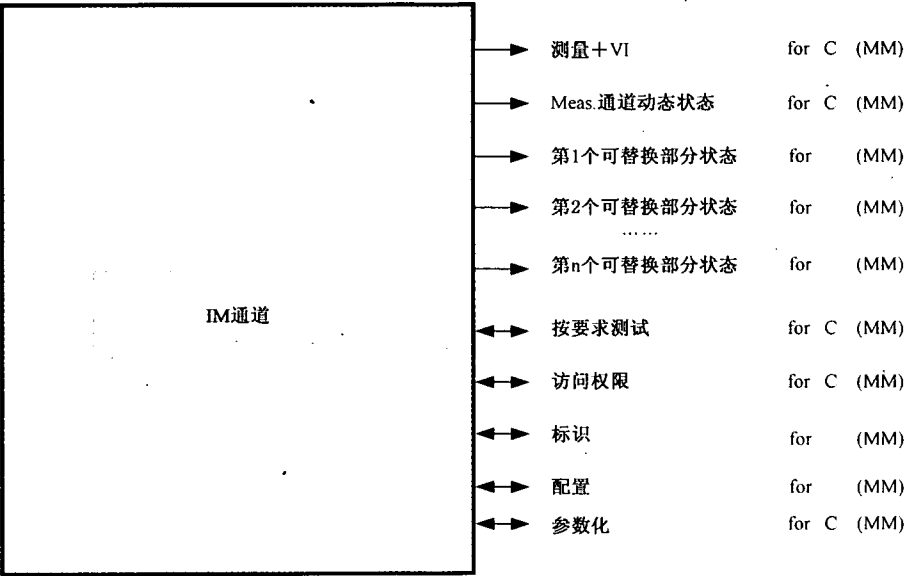


图 B. 5 IM 通道/CMM 交互:用户视图

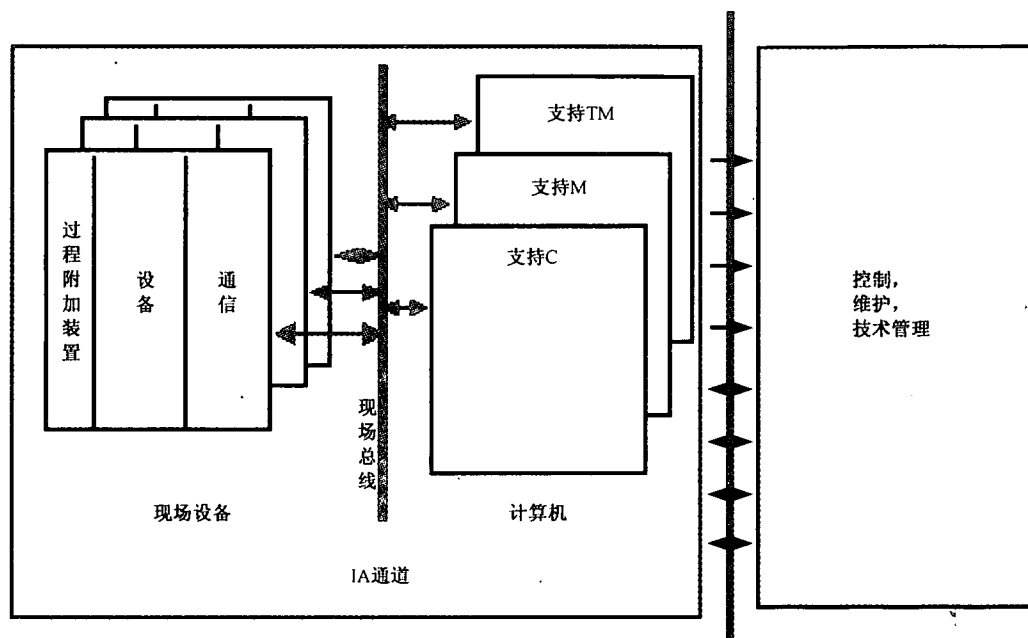


图 B.6 使用现场总线的分布式平台:物理组成

执行 CMM 应用所指定的每一测量所必需的每一 IM 渠道的技术成分是(见图 B.6):

a) 现场部分:

- 过程附属装置(管道等);
- 传感器;
- 变送器;
- 网络(如现场总线)。

b) 补充部分:

- 支持控制阀门、电动机和传感器设备的补充处理;
- 支持维护的补充处理;
- 支持技术管理的补充处理;
- IA 通道具有相似的成分,主要区别在于现场部分,如阀门。

B.3.4 通道和现场设备功能单元

如图 B.4 所示,现场设备用于构造相关的通道。

图 B.5 给出了一个变送器的现场设备功能单元参考模型,执行器模型具有相似的成分,主要区别在于现场部分,如阀、电机和执行器设备。

变送器和执行器中的各种数据和功能被组合到功能单元中。这些功能单元以一个中等的抽象级别表明了特定的硬件或软件成分。这个中等的抽象级别介于图 B.3、图 B.4 所示的用户视图的较高抽象级别与功能块的较低抽象级别之间。

功能需求的描述是映射通道模型到设备参考模型所有功能单元的结果。这有利于功能需求到 FB 规范的映射。

当然,现场设备功能参考模型被视为是覆盖了通道和现场通信计算机部分的相应模型的补充。后面的模型给出了所有通道部分的补充功能单元和管理协作,这种协作是系统级别的协作。

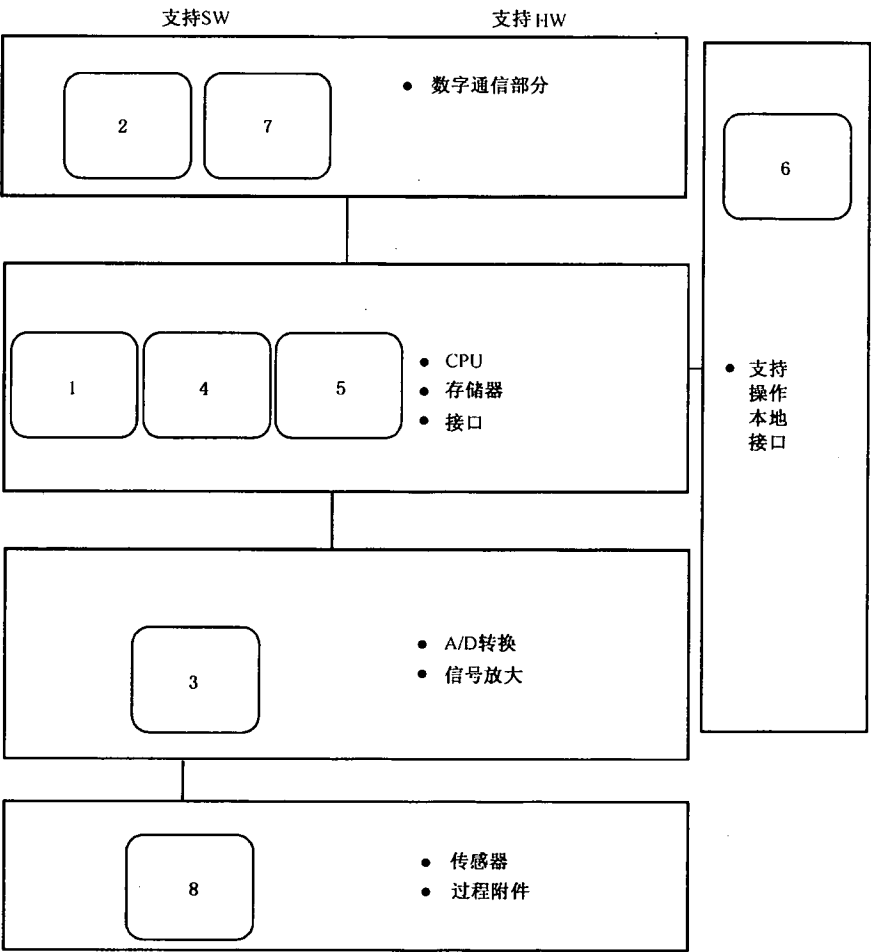
B.3.5 现场设备功能需求列表

直到这里的描述为止,B.3.2 和 B.3.3 中的功能需求都是通过逻辑方法来标识的。它们与现场设备有关。

每一功能单元都使用一个段来描述,仅有“设备管理”功能单元例外。如果补充进本附录给出的背

景,这种描述应该可以充分地阐明用户需求的具体含义。

技术的进步可使设备制造商能转移更多的功能到现场设备中,见图 B.7。



图例：

- | | |
|-----------|-------------|
| 1——设备管理 | 5——诊断和测试支持 |
| 2——网络管理 | 6——本地操作接口附件 |
| 3——信号处理 | 7——现场设备通信功能 |
| 4——测量信息处理 | 8——测量转化 |

图 B.7 智能传感器参考模型

对于“设备管理”功能单元,由于需求的复杂性,需要彻底说明所需的功能分解。定义了以下的几个方面:

- 标识管理;
- 配置管理;
- 参数化管理;
- 测量管理;
- 时间管理;
- 及时控制管理;
- 故障管理;
- 操作模式管理;
- 访问权限管理。

B.3.6 系统级别功能需求列表

注 1: 技术的进步可使设备制造商能转移更多的功能到现场设备中。为帮助这种进步,参见下面的附加需求。

注 2: 在某些情况下,存在相同的设备需求描述;当然,这里是从系统级别来看的。

在 IAM 通道层次来看,下面的需求是一个整体。

每一通道都必须提供所有被要求的功能,分布在组成通道的几个部分中,同时还要提供分布式功能组合的协调执行(通过数字通信)。

所有的需求被归为两大类:

a) 控制,以及与控制部分进行的交互,当可操作时,都:

——在工厂中;

——在车间中。

b) 维护和技术管理,以及所有其他的交互,都:

——在工厂中;

——在车间中。

B.3.7 控制的系统需求

B.3.7.1 介绍

对于分布式控制应用的需求,需要分析为 IAM 通道选择的一些主要的用户需求,如管理访问权限(与负责控制的进行商议)、控制算法状态的访问和综合设备状态信息的访问,也列出了应用于 IAM 通道的系统属性的需求(如可靠性等)。

这些需求覆盖了所有的设备生命周期,因此它们部分涉及到用户、制造商和系统集成者。

无论选择什么样的通信标准,关键问题是必须保证分布式应用之间的同一实时交互。需要扩展这种描述了应用交互的需求,以覆盖在时间同步方面的内容。

B.3.7.2 测量/执行处理

B.3.7.2.1 概述

宏-功能按照处理复杂度高或低来定义。此后将列出主要的成分功能。

注:直接和间接的测量要求相同的基本机制。

B.3.7.2.2 测量验证

有三种级别的验证:

- 第一级验证:在设备层使用诊断信息来验证原始测量信息。
- 第二级验证:比较由冗余变送器及时(数据的时间连贯性)产生的同步信息和测量的速度。
- 第三级验证:比较由前一级别验证后的测量和来自过程模型的测量信息。

注:对于每种测量,用户必须指定需要完整模型的那一部分。需要的部分必须记录在通道配置文档中。

B.3.7.2.3 验证过的测量的趋势

数据文件记录已定义的现象(见 6.8.6)。

B.3.7.2.4 事件通知(起点)

事件通知是由现象检测算法异步产生的。它可以通过已定义的及时性需求来表征。一般地,它不能丢失。换句话说,必须确认能正确收到。

B.3.7.3 测量管理

B.3.7.3.1 一次发生应用触发

一次发生应用触发用于触发应用功能的执行控制,它开始于触发的收到,然后结束。需要一种机制来保证,在信号产生时间后的预定义时间间隔内,如果应用可以获得一次发生触发信号,则完成时带有肯定的及时(timeliness)信息,反之,完成时带有否定的及时(timeliness)信息。

注:应该根据应用的需求来(由用户/系统集成者)规定时间间隔。

B.3.7.3.2 循环应用触发

该服务可用于以较低频率(例如每周期为 5 s)来重新同步一个高频率脉冲序列发生器(例如每周期

为 100、10、1 ms)。该脉冲序列可用于,例如,功能的执行控制,这些功能需要在同步的时间间隔内在不同的设备中执行。一个典型的例子是从不同设备中获取冗余的测量。

B.3.7.3.3 数据的时间连贯性(及时)

在系统级别,要求不同设备产生的数据(在生产、传播和接收中)带有一个及时符号,它可以表明数据的有效时间。例子有测量或命令的接收。

B.3.7.3.4 分布式的“绝对时间”(年、月、日、小时等)

它由两部分组成:

- “绝对时间”参考数据的分布。
- 设备同步的计数由两种机制获得:
 - 分布式同步时钟的使用(见前面脉冲序列的例子);
 - 重复以低频率同步设置绝对时间值。

B.3.7.3.5 分布式“相对时间”

与前面的“绝对时间”类似(如系统开始于一个零点时间)。

B.3.7.3.6 应用的分布式调度

系统的需求是,分布式应用执行必须的整个时间由所选择的分布策略决定。

必须确认是否必须考虑一些中间的同步,例如重新启动整个应用。

B.3.7.4 可靠性

B.3.7.4.1 冗余的支持

要求对冗余的支持具有两个级别:

- 功能级别,在应用级别上;
- 在资源级别上的冗余。

B.3.7.5 支持访问权限管理功能

B.3.7.5.1 操作管理功能的模式(为访问权限管理做的扩展)

这是一个系统管理功能,目的是管理几个操作模型间的转换。特别地,它管理在不同的人或自动控制操作员之间的访问权限的转换程序。用于支持现场设备中的干预程序,以实现人类组织之间达成一致的干预计划。因此,为了实现这个目标,设备管理应该与系统管理相互合作。

B.3.7.5.2 访问权限管理功能(对每个设备功能的访问进行资格审查)

在每种操作模式下,设备本身允许操作员在其上执行某些预定义的活动。

很明显,例如,当测量处理功能必须为活动时(如在控制操作模式中),禁止对设备的配置、参数化、按需测试的写权限是非常重要的。

B.3.8 维护和技术管理的系统需求

B.3.8.1 概述

对于分布式维护和技术管理应用的需求,需要为 IAM 通道分析主要的用户需求,包括:检查和修改应用参数、管理访问权限、读取设备标识、检查所提供的方案的功能配置、检查/修改应用参数、检查设备状态和支持按需测试。

这些需求覆盖了所有的设备生命周期,因此,它们部分涉及到终端用户、制造商和系统集成者。

B.3.8.2 设备标识

用于支持维护活动的设备标识信息已经在本部分的正文部分描述了。

B.3.8.3 配置

维护操作员或试运行操作员必须检查或修改设备的功能配置。他们还需要确认,特别是在替换了设备后,通道功能配置是一致的。这是一个系统级别的功能,目的是检查组成通道的设备中执行的所有功能都被适当地配置了。例如,如果通道需要滤波功能,该功能要么在现场设备中执行,要么在外部设备中执行,但不是同在两者中,也不是不在两者之一中。

要求下列功能:

- 配置修改
 - 与用户相关的设备/通道配置修改;
 - 与制造商相关的设备/通道配置修改。
- 配置检索
 - 与用户相关的设备/通道配置修改;
 - 与制造商相关的设备/通道配置修改。

B.3.8.4 参数化

在试运行或维护干预期间,该功能检查/修改应用参数。

在设备参数的每一改变之后,在系统级别上要求获得该功能,以为维护/试运行操作员提供帮助。操作员必须确认功能参数在组成通道的设备之间是一致的(例如,通常较高层次设备所期望的工程单位或低通滤波器频率要真正匹配于现场设备中所使用的)。

设备/通道参数分为以下两类:

- 介入参数:这些参数的修改将干扰干预设备/通道的正常操作;
- 非介入参数:这些参数的修改不干扰干预设备/通道的正常操作。

所要求的功能如下:

- 参数修改
 - 介入设备/通道参数修改;
 - 非介入设备/通道参数修改。
- 参数检索
 - 设备/通道参数检索。

B.3.8.5 监控设备状态

在系统级别上,每个用户根据自己的要求需要具有一个设备的健康视图。

因为“基于条件的维护”的需要,终端用户需要知道必须替换哪一个可替换的部分,而且,他还需要制造商要求用于更快速、适当地修复设备的信息。

维修人员可能还需要更多的详细信息来执行他的干预。

所要求的功能如下:

- 设备/通道详细状态检索
 - 设备/通道详细状态信息检索。

B.3.8.6 支持按需测试

执行和测量远程或本地测试(如校准)所需的支持被分为两类:

- 介入测试:这些测试的执行将干扰设备/通道的正常操作;
- 非介入测试:这些测试的执行不干扰设备/通道的正常操作。

对于所要求的测试,需要必须的许可,并且设备/通道必须被置为相应的操作模式。

所要求的功能如下:

- 测试执行
 - 介入设备/通道测试执行;
 - 非介入相关设备/通道测试执行。
- 测试结果检索
 - 设备/通道测试结果检索。

B.3.8.7 支持访问权限管理功能

这是一个系统管理功能,参见控制需求的描述。

B.3.9 网络管理

以下的功能必须支持 IAM 通道的设备和系统管理的协作活动:

- 网络试运行测试(如网络配置/参数化确认等);
- 网络管理操作支持;
- 通信监控(错误和统计);
- 通信故障管理(带或不带冗余);
- 及时(timeliness)控制支持。

B.3.10 功能块功能需求一致测试

必须进行某些类型的一致性测试,以保证哪部分功能需求被功能块规范及其扩展所覆盖。这个测试很重要,因为它的结果使得在功能需求和使用标准功能块的市场方案之间的一致性测试更容易。

附录 C

(资料性附录)

GB/T 21099 和 GB/T 19769.1—2005 间的关系

C.1 本附录范围

GB/T 19769.1—2005 为工业测量和控制系统(IPMCS)的分布式功能块应用制定了通用标准。下列是 GB/T 19769.1—2005 中的模型:

- 应用模型;
- 设备模型;
- 资源模型;
- FB 模型;
- 系统模型。

GB/T 21099 关于设备和 FB 模型的详细方法在下面的章条中描述。这里简要地概述了共同的规范和差异。本附录通过 GB/T 19769.1—2005 来描述 GB/T 21099 高级 FB 的一个示例作为结束。

本附录收集了所有关于 GB/T 19769.1—2005 与 GB/T 21099 之间的关系,是在需求规范期间获得的。

C.2 与 GB/T 19769.1—2005 功能块模型的关系

C.2.1 概述

本条给出了 GB/T 19769.1—2005 FB 模型的用法或差别。GB/T 19769.1—2005 模型的细节没有描述。关于 GB/T 19769 更详细的介绍见 GB/T 19769.1—2005 和 GB/T 19769.2—2005。

C.2.2 一般特性

GB/T 19769.1—2005 定义了 FB 模型,图 C.1 给出了它的图形表示。它由 FB 头部和 FB 主体组成。FB 主体包含了数据流(数据输入和输出、运算法则、内部数据,附加于 GB/T 19769.1—2005 的所谓的内含数据。内含数据不包含在数据流中,但会调整算法)和事件流的头部(事件输入、事件输出和执行控制图)。

这些成分大体上刻画了 GB/T 21099 功能块的特性。

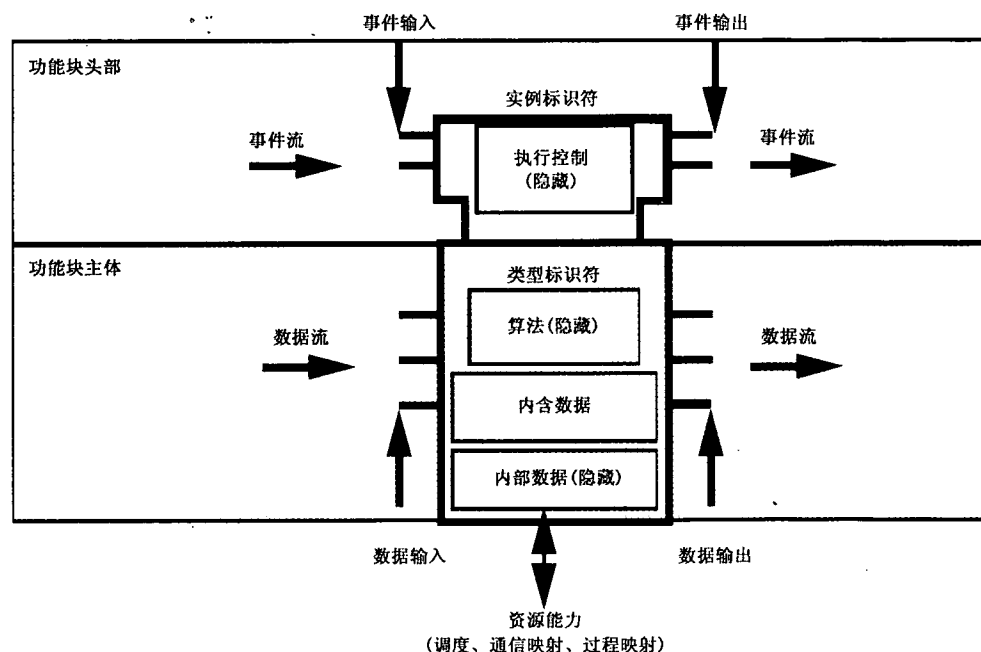


图 C.1 GB/T 19769.1—2005 功能块结构

GB/T 21099 的 FB 类型的特性由定义好的有名事件输入和事件输出、有名数据输入和数据输出、内含数据、执行控制的一个确定集合和细节、算法的一个确定集合和细节来刻画,如图 C.2 所示。类型是 FB 接口的描述,在有名数据(即算法)后带有某些行为。无论怎样,带有一个事件输入和事件输出和一个算法的 FB 仍然在 GB/T 21099 范围内。

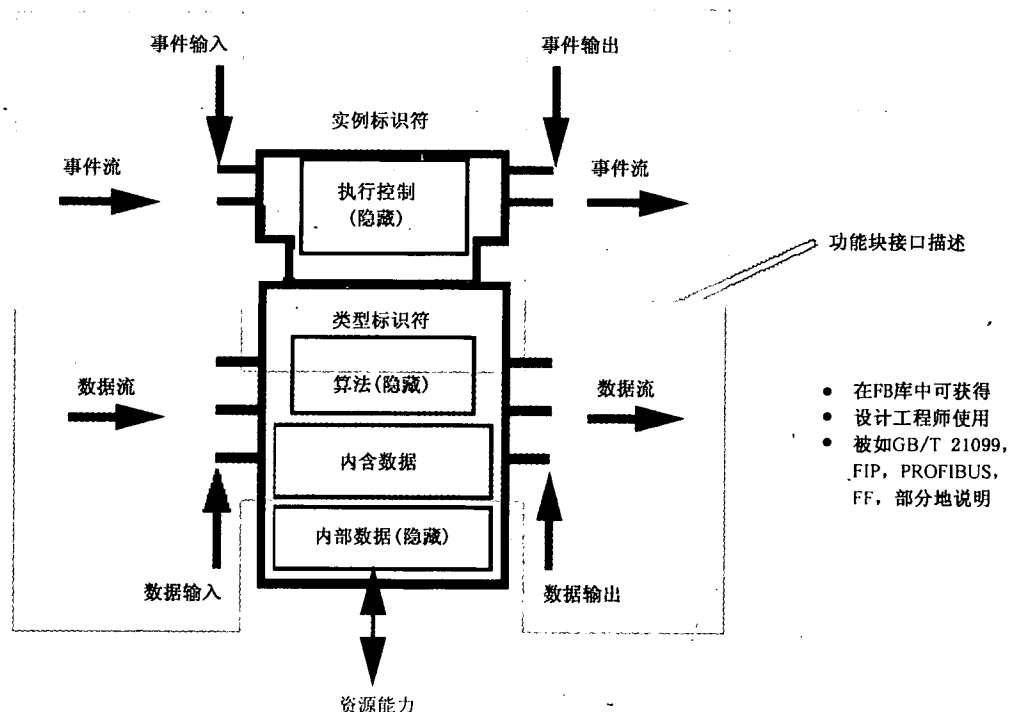


图 C.2 GB/T 19769.1—2005 功能块的类型细节

内部数据、算法和执行控制的细节超出了 GB/T 21099.2 的范围。这些方面是实现的细节,在 FB 的外部视图被隐藏了(见图 C.3)。

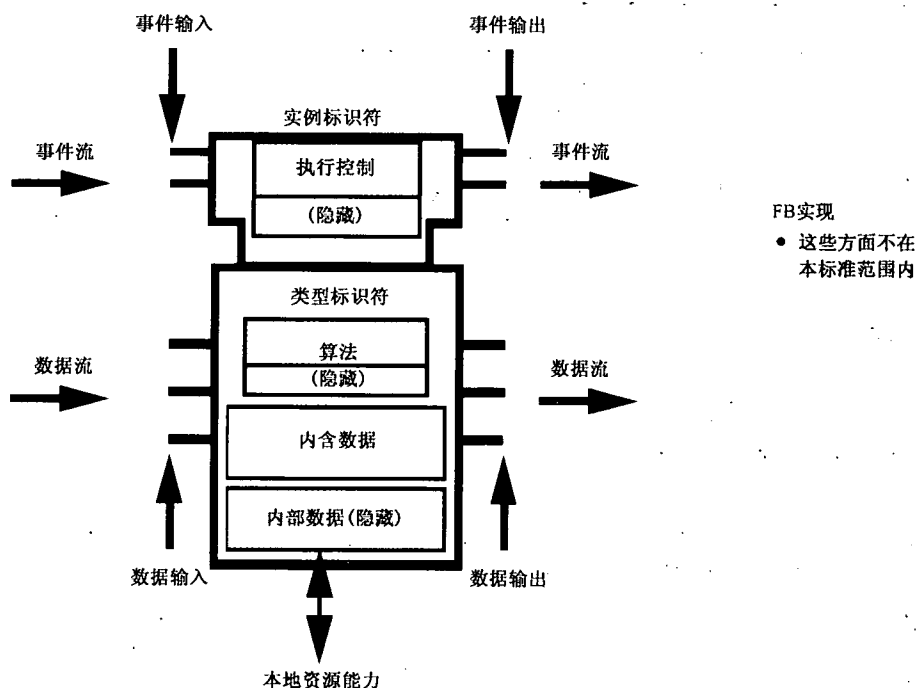


图 C.3 实施细节方面

在集中式程序中,FB 的执行顺序由资源文件中调用 FB 的顺序决定,或由一个资源的任务系统调度(见图 C.4)。在 GB/T 19769.1—2005 的分布式环境中,FB 的执行顺序由 FB 头部的事件流决定。FB 执行控制头部和被视为调度功能的本地操作系统之间具有事件连接。FB 头部是分布式操作系统的可配置部分。换句话说,分布式操作系统由每个资源的本地操作系统以及 FB 执行控制头部之间的连接组成。

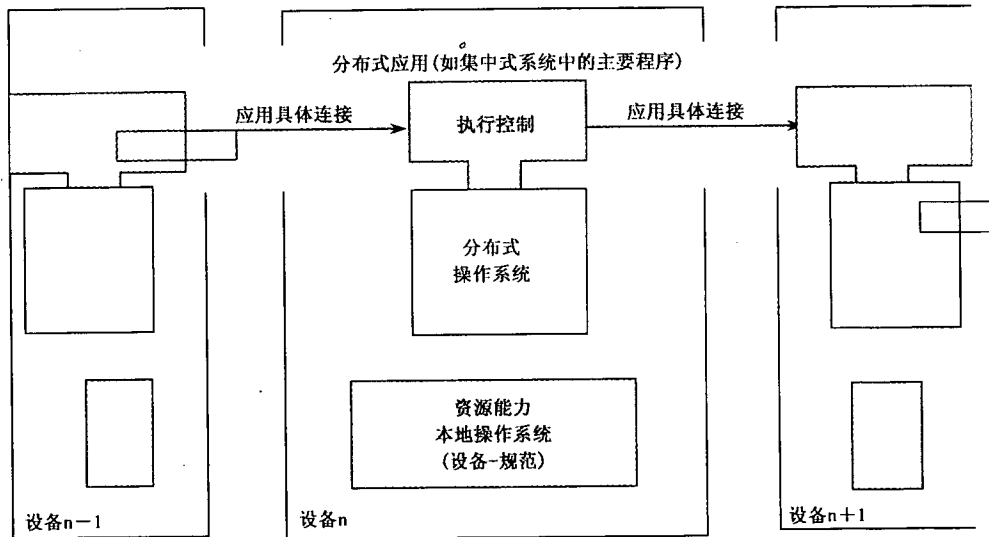


图 C.4 分布式应用和分布式操作系统

作为 GB/T 19769 的使用摘要,表 C.1 着眼于来自 GB/T 19769.1—2005 的标准,将从特定的应用设计来定义类型和应用。

表 C.1 GB/T 19769.1—2005 功能块特征概述

	GB/T 19769.1—2005 特性	类型规范特性	应用规范特性
头部	事件流(边缘)	执行控制 事件输入/输出	事件间的连接
本体	数据流	数据输入/输出 含有数据的算法的一部分	数据间的连接 (数据连接)

C.2.3 FB 类型规范

过程 FB 包括:

- 标准化的数据结构;
- 标准化的语义;
- 与标准数据相关的一般行为;
- 基本输入、输出、事件输入、事件输出和控制功能的标准定义;

C.2.4 FB 实例特性

对于过程工业,FB 实例名被定义为块标签。在一个工厂站点的系统范围内,标签是无歧义的。

C.2.5 GB/T 19769.1—2005 功能块元件映射到 GB/T 21099

用在过程工业中的功能块可以解释下列定义在 GB/T 19769.1—2005 中的特性(见图 C.5):

- 事件用于触发 FB 主体中的不同算法,例如初始化、正常操作的执行、异常操作的执行(见 C.2.6)。
- FB 之间的数据流由包含变量值及其状态的变量记录执行,即使用数据流中的变量和远程非 FB

设备中的变量是不同的。

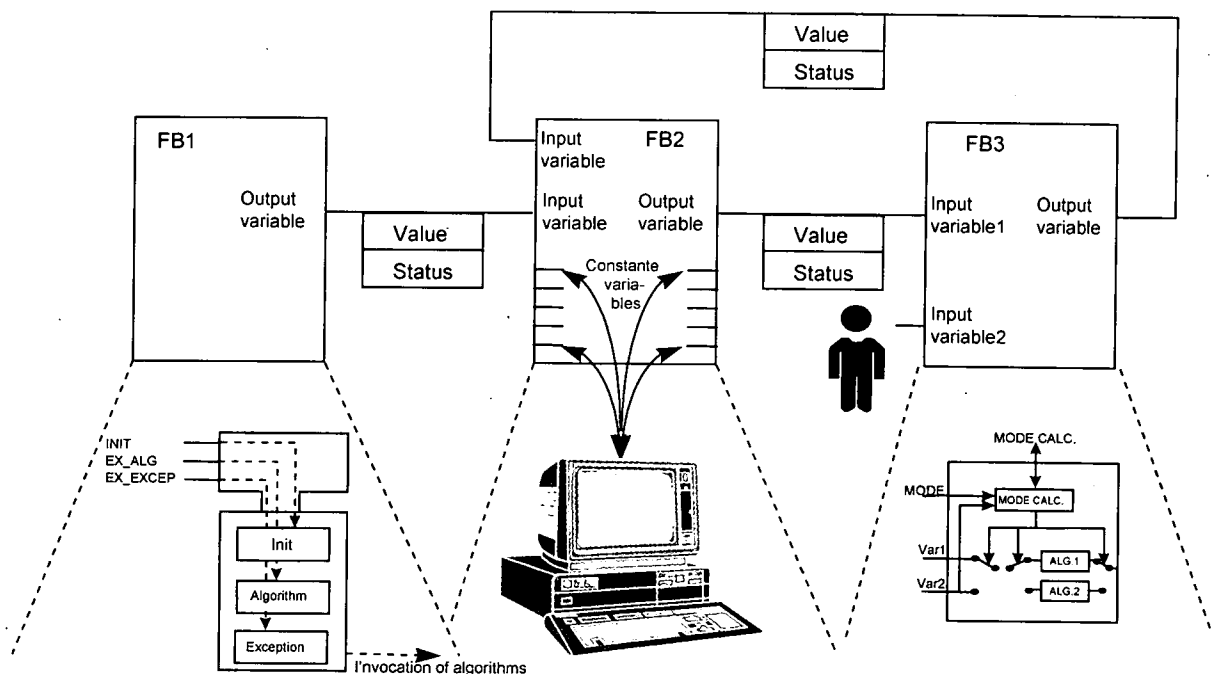


图 C.5 过程控制功能块的基本概念

- 内含数据的一个附加集合,可以被映射到相应的内含变量,以便与维护、HMI、监测和其他应用进行交互。

内含变量是一种变量,它的值由操作员、高级别的设备配置或由计算而得到的。它不能连接到其他FB输入或输出,因此不包含状态。基于块的类,可以支持风格一致的附加变量。

- 每个中都有一个特殊的FB算法,它控制FB其他算法中的信息计算。这个算法就是“操作模式”。
- 在FB中定义了变量的数目、名字、数据类型和顺序。

C.2.6 FB 算法

FB由数据输入、数据输出和负责正常操作(即在FRD中可见的操作(见附录A))的算法组成。这些算法有,如,带有相关变量和参数的PID、线性化或数学方程式。FB的正常操作由处于肯定条件的,在稳定操作期间的(操作点)过程和自动化设备执行。初始化、报警或冷启动,以及更多的高级操作,如进入安全模式,是过程控制FB的附加功能。这些操作是FB的固定部分,默认连接到相关事件。这些操作就是异常操作或异常处理。

过程工程师在FRD方案中设计正常的操作,而I&C工程师增加异常操作以完成完整的功能块配置方案(见附录A)。

功能块算法结构见图C.6。

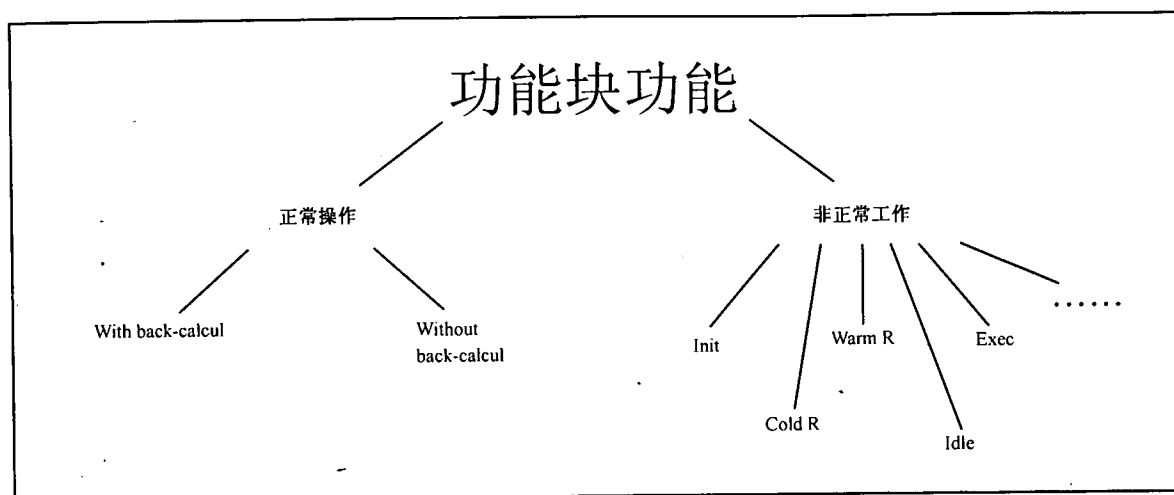


图 C.6 过程控制 FB 中的功能成分

FB 包含执行正常操作的主要算法(一个或多个)和异常操作的算法。活动的事件选择执行哪一个算法。在正常操作的大多数时间中,都执行主要的算法。在试运行、维护或鉴定过程阶段,执行异常操作算法。GB/T 19769.1—2005 图形表示给出了一个例子(见图 C.7)。

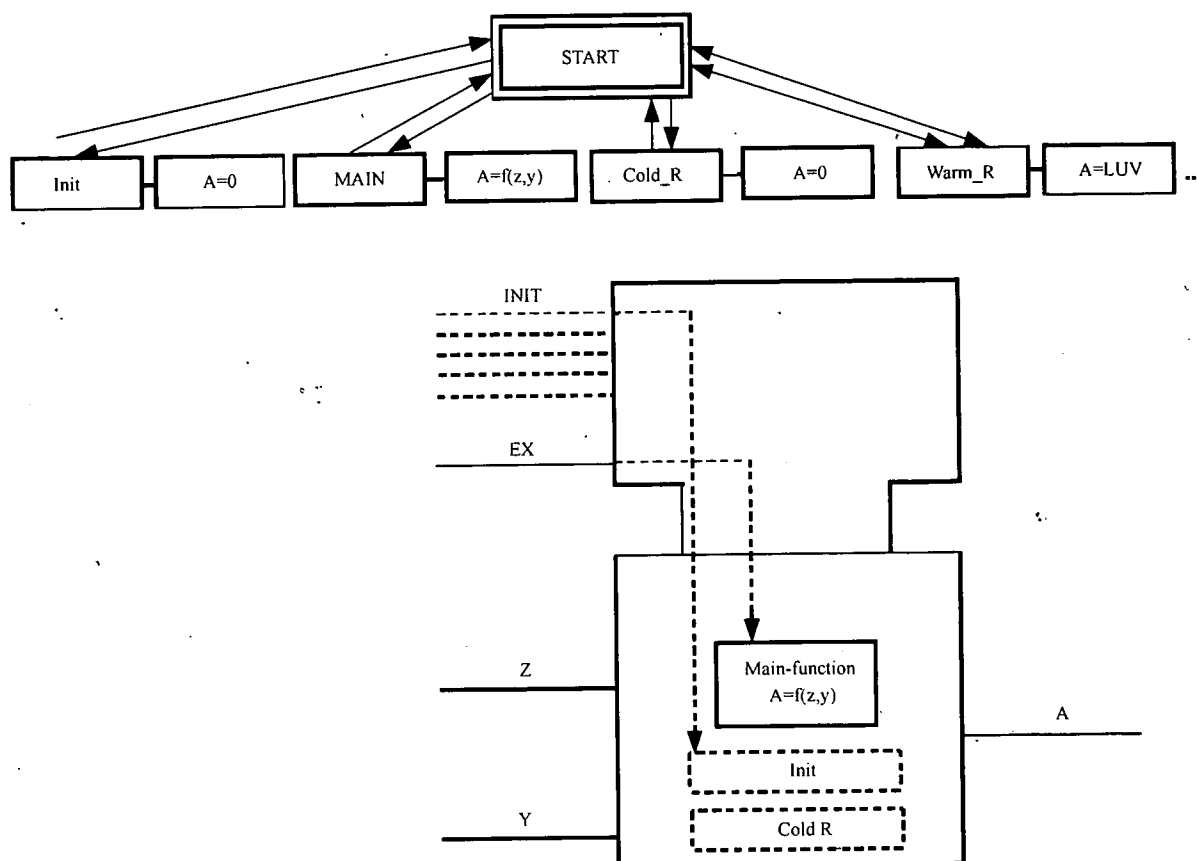


图 C.7 一个过程控制 FB 的 GB/T 19769.1—2005 图形表示

图 C.7 给出了由相关事件触发的正常和异常操作算法。AB 和 EFB 正常与异常操作的结合是合法的。当然,异常操作的实现的程度取决于应用领域。因此,必须定义一致的类。

FB 应该包括为每个块的初始化和重启定义的标准功能。应该为下列的操作环境定义行为:

- 新设备;

- 冷启动(扩展电源故障);
- 热启动(短电源故障);
- 从设备故障-安全返回。

图 C. 8 给出了 EFB 的完整结构。

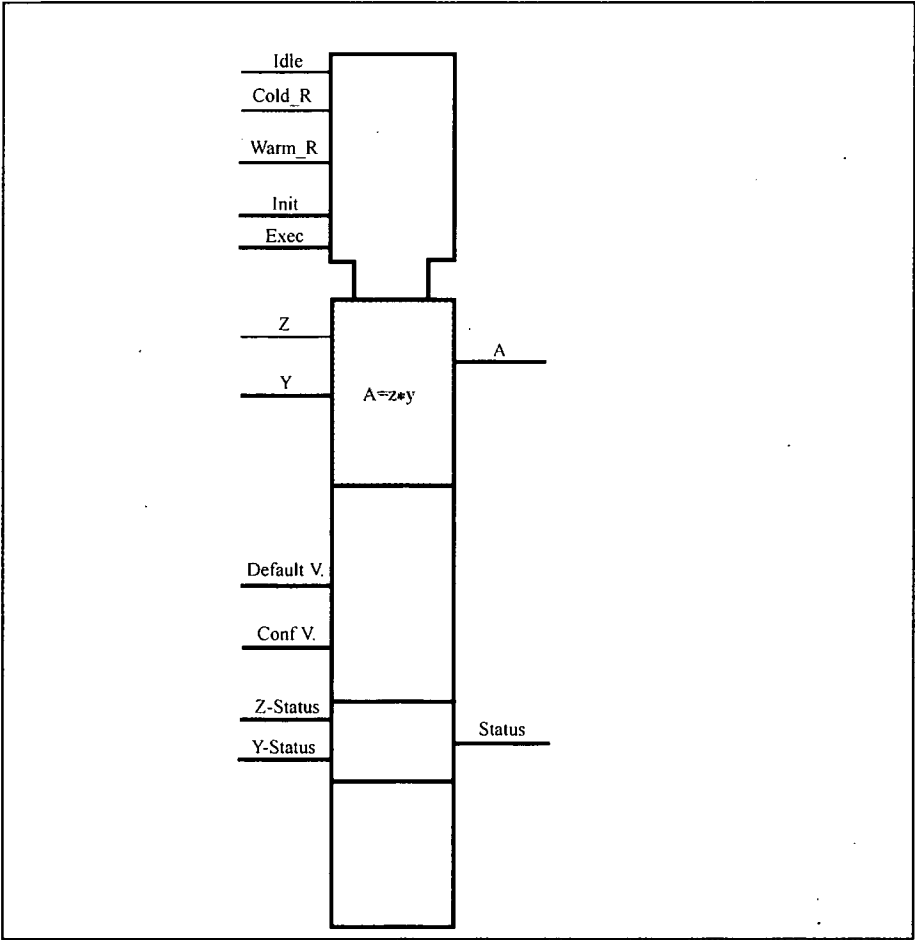


图 C. 8 EFB 的完整结构(示例)

C. 2. 7 GB/T 19769. 1—2005、GB/T 21099 以及其他标准活动的关系

FB 的目的因应用而异。FB 分类的目的是结构化为层次结构。在本规范中,应该只沿着一条路径来继承已定义的功能。应该使用面向对象的方法来分类。分类反映了几种观点,如应用外围(通信、过程、操作系统或无)接口的存在、数据流或事件流或两者的操作、过程的功能目的。就规范而言,层次的每个元素是一个实体。根据属性来指定实体的属性。具有一条关于规范的连接关系,从没有特殊变量和属性的 GB/T 19769. 1—2005 类型规范和具有某些属性集合的多重目的 FB 到具有专用变量和属性集合的特定专用 FB 的规范(见图 C. 9)。

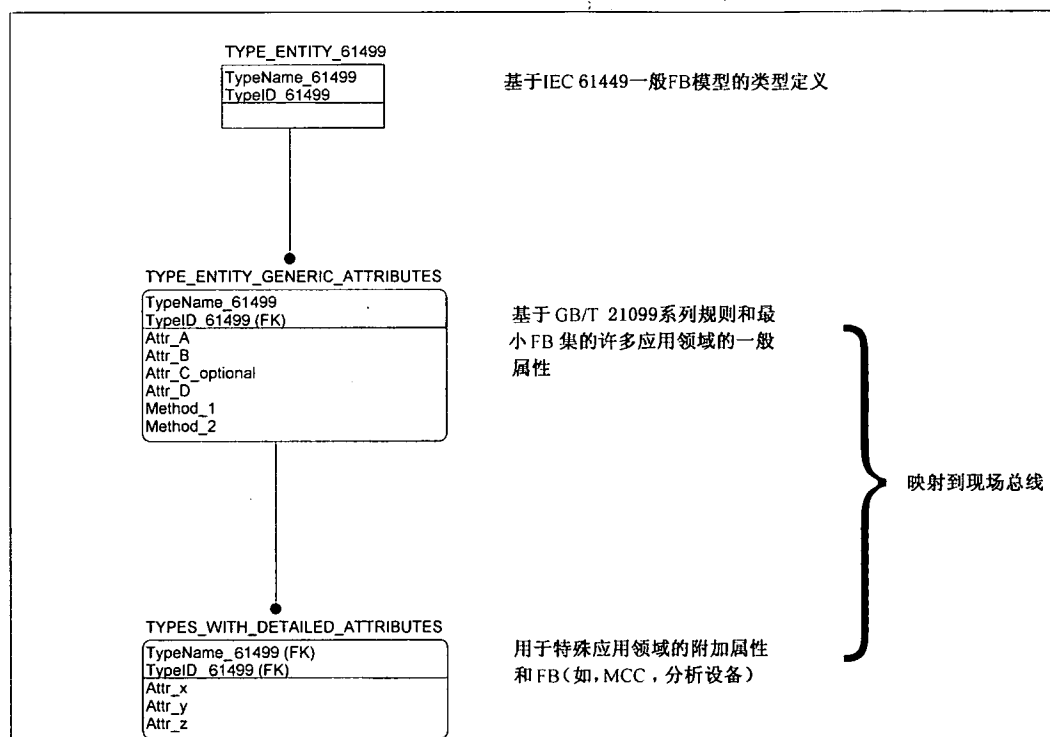


图 C.9 GB/T 19769.1—2005、GB/T 21099 以及其他标准化活动的关系

C.3 GB/T 19769.1—2005 设备和资源模型映射到 GB/T 21099

C.3.1 概述

下面的条款描述 GB/T 21099 设备模型为需求规范的结果。本章与两个规范的设备模型之间的参考概述密切相关。

C.3.2 GB/T 21099 设备模型组成成分概述

在一个实际的设备和资源中,仅有数据和功能(程序)代码以及通信、过程和 HMI 的接口。通过通信系统,通过配置或设计工具,这些数据和程序代码被视为 FB、管理代理或数据连接。设备模型的规范是设备执行的外部视图。设备模型描述了整个系统体系结构的细节。设备模型是实际设备的抽象。

执行 FB 应用的设备的基本组成部分有(见图 C.5):

由数据和事件输入输出、内部数据、内含数据和运算法则组成的 FB 应该具有以下的一般需求:

——FB 环境

FB 嵌入到作为 FB 环境给出的操作环境中。FB 环境执行特殊的过程控制功能,如趋势,这些功能是没有经过任何程序设计活动的即可获得的应用部分。FB 环境功能由独立于 FB 应用的外部应用使用,即并行。

——应用管理实体(AME)

从功能性观点看,许多过程控制设备需要采用已使用的硬件配置。例如,模块化设备中可用的 FB 必须被配置,或者为了测量补偿带有或不带的附加输入的模式版本。这导致增加或删除功能块。这些功能由所谓的 AME 发起,即,设备中的附加功能修改它们的应用软件。本部分没有定义 AME,它在 IEC 61158 框架中定义。

——通信

FB 之间的数据传输、FB/FB 环境和维护间的交互、HMI 监控和 FB 环境/AME 与配置功能间的交互,都需要通信服务和协议的支持。FB 和 FB 环境的规范独立于通信系统。FB 环境和

通信系统间的子层映射可以适应应用和通信。

在 FB 应用进程、系统和网络管理应用进程中的参数、块、对象和功能需要有效地映射到所使用的通信协议和服务。FB 应用进程、系统和网络管理应用进程使用的通信协议和服务应该被特别设计,以用于分布式应用进程,并且应该提供这些应用所要求的服务。

有三种不同类型的通信需求:

- 时间严格通信

FB 应用进程使用的通信协议和服务应该支持时间严格通信的统一需求,包括:

- 1) 可靠传输;
- 2) 空间连贯性传输;
- 3) 时间连贯性传输。

- 命令通信

FB 应用进程使用的通信协议和服务应该支持时间-有效通信的统一需求,包括大数据块的分段传输。FB 应用进程使用的通信协议和服务还应该支持“异常报告”通信的统一需求。

- 事件通信

FB 应用进程使用的通信协议和服务应该支持通信事件的统一需求,并被特别设计,以:

- 1) 最小化静止周期内的装载;
- 2) 防止高速活动周期内的过载。

——资源

资源被认为是设备中的软件(可能是硬件)结构的逻辑划分。资源独立地控制自己的操作。可以修改资源的定义,而不影响设备中其他的资源。一个资源接收和处理来自过程和/或通信接口的数据和/或事件,并返回数据和/或事件到过程和/或通信接口,这由使用资源的应用规定。应用的互操作网络视图通过设备资源来提供。每个资源指定一个或多个本地应用(或分布式应用的一部分)的网络可见部分。

C.3.3 FB 分类

C.3.3.1 概述

以下描述了 FB 应用结构的组成部分,它可以通过相关资源来访问(见图 C.6)。它们是:

- a) 块

- 资源块;
- 转换块;
- FB。

- b) 报警块;

- c) 趋势块;

- d) 视图块。

C.3.3.2 资源块

与资源相关的物理子成分的特性可由一个包含变量的资源块集合描述。资源块也可以包含与 FB 和转换块相同的变量,如置故障-安全。这些变量在资源块中定义。

C.3.3.3 转换块

转换块封装特定的 I/O 设备,如传感器、执行器和开关。转换块通过为 FB 使用而定义的独立于设备的接口来控制对 I/O 设备的访问。转换块也执行功能,如 I/O 数据的校准和线性化,以将其转换为独立于设备的表示。它们到 FB 的接口被定义为一个或多个独立于 I/O 通道的执行。

C.3.3.4 FB

FB 是在 FB 应用中定义监测和控制的主要方法。FB 代表了由应用执行的基本自动化功能,该应用尽可能独立于具体的 I/O 设备和网络。每个 FB 根据特定算法和内含变量的内部集来处理输入变量

和转换块输入。它们产生输出变量并向转换块输出。

基于处理的算法,可以提供期望的监测、计算和控制功能。来自 FB 执行的结果可能表现在操作或诊断信息的内含变量中。此外,处理结果还可能表现在对转换块的输出或一个或多个可能与其他 FB 连接的输出变量。

C.3.3.5 视图块

FB 环境包括了定义来允许对相关的块参数进行成组访问的数据结构,称为视图块。在浏览功能块数据时,视图块提供方便快速的显示响应。

对于每个 FB 类型,为下列块参数组定义视图块:

- 操作动态参数;
- 操作静态参数;
- 所有动态参数;
- 其他静态参数。

C.3.3.6 趋势块

FB 应该包括数据结构定义,以允许成组地访问单个块参数的带有时间戳的多个采样,被称为趋势块。趋势块消除了为了形成趋势而快速扫描参数所需的通信和系统处理器开销。

趋势对象定义应该包括标准采样类型及其相关采样功能(如点采样,整体平均,最小值,最大值等)的定义。

C.3.3.7 报警块

FB 环境应该包括数据结构定义和相关资源及 FB 功能,以允许在系统内受控地传输报警和事件信息,被称为报警块。在系统内,报警块将报警和事件预测性地并且有效地路由到选定的目的地。

报警块定义包括:标准交换协议的定义,这些协议用于初始化、发送和确任报警对象报告;确认报警;解释标准的和自定义原因的代码;以及配置报警功能,如报警关键字、报警优先级、报警自动确认等。

当检测到报警时,资源块、转换块和 FB 使用报警来传递通知信息。报警是对一个块离开某个特殊状态以及何时返回该状态的检测。报警状态的检测时间作为一个时间戳包含在报警信息中。同样,也包含优先权,以表示该警报是建议性的还是关键性的。

C.4 GB/T 19769.1—2005 管理功能块的映射

管理属于在 IEC 61158 的范围,本部分不涉及。

C.5 GB/T 19769.1—2005 文本语言

GB/T 19769.1—2005 文本语言用于描述 GB/T 21099FB 的示例,以阐述 FB 的定义。

C.6 GB/T 19769.1—2005 和 GB/T 21099 间的模型构件参考

表 C.2 概述了 GB/T 19769.1—2005 和 GB/T 21099 间的模型构件参考。这个参考不是正式的,它们应该表现两个概念的共同规范和区别。

表 C.2 GB/T 19769.1—2005 和 GB/T 21099 间的模型构件参考

GB/T 19769.1—2005	GB/T 21099	注释
系统模型	系统概述	GB/T 21099 系统概述,见第一部分图 1,有非 FB 应用和 FB 应用的交互。GB/T 19769.1—2005 仅涉及 FB 应用
应用模型	FB 应用	GB/T 21099FB 应用,见第一部分图 1,有非 FB 应用和 FB 应用的交互。GB/T 19769.1—2005 仅知道 FB 应用
设备模型	设备	没有差别
资源模型	资源	没有差别

表 C.2(续)

GB/T 19769.1—2005	GB/T 21099	注释
调度功能(部分)	FB 环境	现在可以隐含地得到 IPMCS 过程控制通用功能,如报警处理、通信系统特定服务质量(QoS)的使用、访问权限管理及其他。在 GB/T 21099.2 中,需要决定这些功能的哪些是明确的(如变为 FB),哪些仍然是隐含的 GB/T 19769.1—2005 指定的都是明确的
FB 模型	FB	没有差别,作为应用设计的明确部分的事件连接并不是强制的
—	资源块	GB/T 19769.1—2005 没有涉及
过程的服务接口 FB	转换块	没有差别
为通信服务接口 FB 提供输入的特殊的 FB 集合	视图块	GB/T 21099 有到通信的隐含映射
为通信服务接口 FB 提供输入的特殊的 FB 集合	报警块	GB/T 21099 有到通信的隐含映射
为通信服务接口 FB 提供输入的特殊的 FB 集合	趋势块	GB/T 21099 有到通信的隐含映射
管理 FB	—	这是 IEC 61158 系统管理的一部分

附录 D

(资料性附录)

模拟输入 FB 到 GB/T 19769 的映射

D.1 概述

作为一个示例,本附录给出了模拟输入块到 GB/T 19769.1—2005 模型的映射。

D.2 介绍

D.2.1 一般

映射使用了部分 GB/T 19769.1—2005 模型来描述由 ISP、PROFIBUS 和 FF 规定的过程控制 FB。特别地,下面的例子是由 PROFIBUS-PA 规定的模拟输入 FB(AI FB)。

GB/T 19769.1—2005 包含了附录 B 中的模型的文本语法,它用于,除了图形表示外的,AI FB 描述。使用 GB/T 19769.1—2005 为出发点的原因如下:

- 应用 GB/T 19769 到过程控制 FB 系统,即获得 GB/T 19769 模型应用的经验;
- 为过程控制验证 GB/T 19769 模型(测试适合性);
- 找出文本表示的问题;
- 提出本部分需求给 IEC TC65 WG6 或其他用户;
- 调查 GB/T 19769 文本表示是否适合 GB/T 21099 输出的形式化描述;
- 帮助澄清 GB/T 21099 与 IEC TC65 间的误解。

D.2.2 映射版本的修正:1.1

版本 1.1(时间:1999 年 7 月 7 日)列出了下列修正:

- a) 修正:更新和添加映射到 GB/T 19769 的版本,使用独立的事件来控制 MODE 算法;
- b) 修正:仅使用带有模式事件、修改输入和输出变量及事件的 AI FB 映射;
- c) 参数描述的集成。

D.3 模拟输入块

D.3.1 模拟输入块概述

模拟输入块代表变送器,其参数见图 D.1。

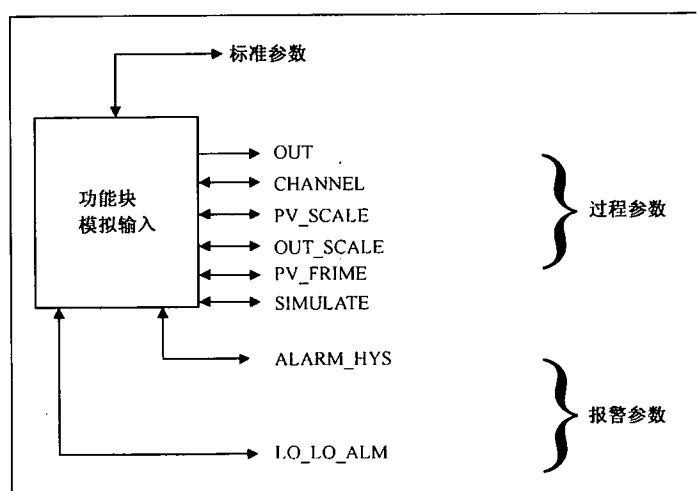


图 D.1 模拟输入块的参数概要

图 D.2 给出了带有仿真、模式和状态的模拟输入的结构。

图 D.3 归纳了模式和状态产生的输入和输出。

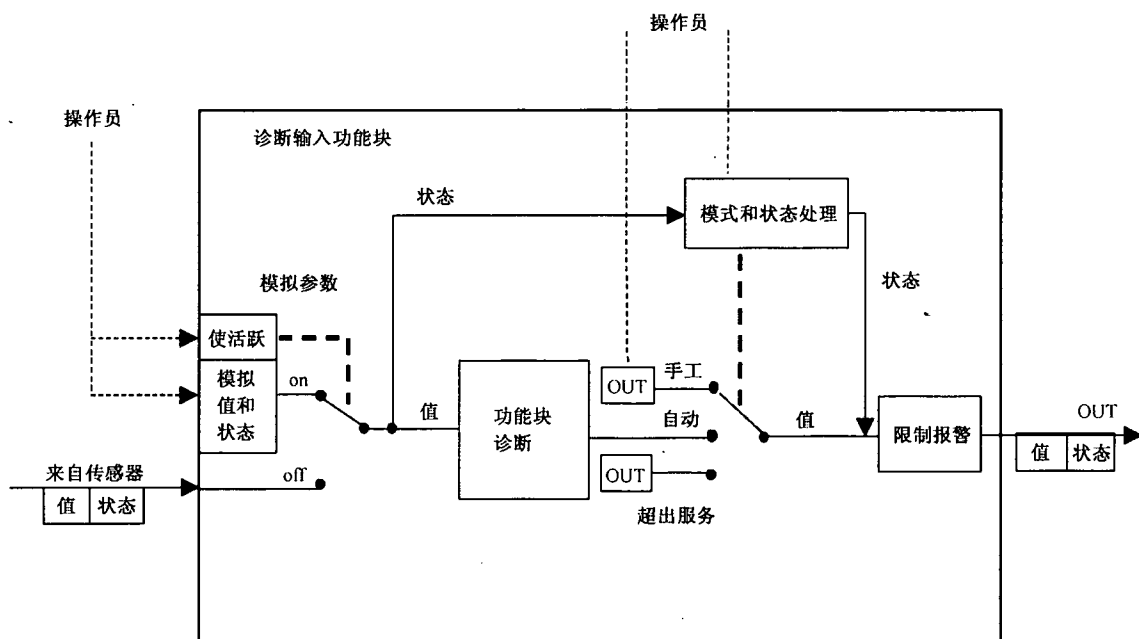


图 D.2 模拟输入块的仿真、模式和状态图

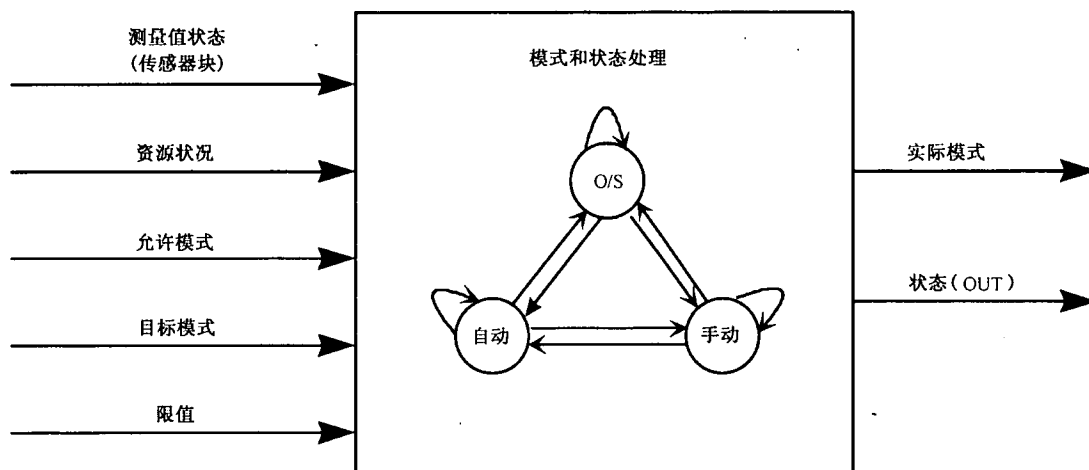


图 D.3 模式和状态产生条件

由转换器块通过通道传给功能块的测量值/状态是模式计算的一个输入。一般地说,描述设备健康状况的资源状态在本规范中没有明确定义,即这是设备细节,并没有作为参数给出,但资源状况至少能够区别好和不好。允许实际的和正常的模式作为 MODE_BLK 的功能块参数。目标模式由操作员设置,允许的模式来自于块设计者。关于输出值的高低限制值(HI_LIM, HI_HI_LIM, LO_LIM, LO_LO_LIM)将影响输出的状态。

实际模式是 MODE_BLK 功能块参数的属性和模式计算的结果。状态(输出)要加上块的输出参数(DS 33)。

D.3.2 AI 状态机

AI 的允许的模式有不可用(O/S)、Man(手动)和 Auto(自动)。

可能的转换见图 D.4。

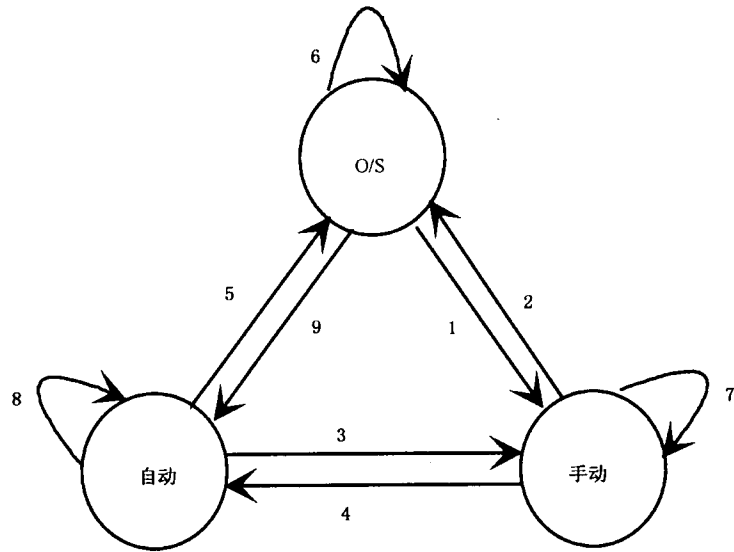


图 D.4 模拟输入块的状态机

D.3.3 计算实际模式及改变目标模式的条件

下面的表格在左边部分包含了所有的条件,从实际模式(最近执行)转换到 AI-FB 的新的、实际的目标模式。计算的结果列在右边部分。

在表 D.1 中,第一列是状态机的转换的编号,一般的条件是,允许的模式为 O/S (一个设备或块配置错误后的状态)、Man(操作员提供 OUT 值)或 Auto(设备提供 OUT 值)。

表 D.1 实际模式计算的条件和结果

条件					结果	
转换	目标模式 (操作员)	实际模式 (前期执行)	资源状态	状态 (传感器输入)	目标模式 (计算后)	实际模式 (计算后)
T2,T5,T6	*	*	<>OK	*	O/S	O/S
T2,T5,T6	O/S	*	*	*	O/S	O/S
T1	Man	O/S	OK	*	Unchanged	Man
T1	Auto	O/S	OK	*	Unchanged	Man
T4	Auto	Man	OK	Good (NC)	Unchanged	Auto
T7	Auto	Man	OK	<>Good (NC)	Unchanged	Man
T3	Auto	Auto	OK	<>Good (NC)	Unchanged	Man
* 没有影响。						

D.3.4 产生输出状态的条件

表 D.2 给出了哪些条件将影响输出参数的状态。条件列在左边部分,计算结果列在右边部分。

表 D.2 计算输出参数的状态的条件和结果

条件				结果状态 (输出)
实际模式	模拟	输出限制	状态(传感器输入)	
O/S	*	*	*	Bad-out of service
Man	*	*	*	Uncertain - ok, high limit, low limit

表 D. 2(续)

条件				结果状态 (输出)
实际模式	模拟	输出限制	状态(传感器输入)	
Auto	Inactive	*	Good (NC)	Good (NC) - ok
Auto	Inactive	*	High limit	High limit
Auto	Inactive	*	Low limit	Low limit
Auto	Active	*	*	From simulate parameter
*	*	High	*	High limit
*	*	Low	*	Low limit
* 没有影响。				

表 D. 3 归纳了模拟输入块所有附加的参数及其属性。

表 D. 3 模拟输入块参数属性

	参数名	对象类型	数据类型	存储	大小	访问	参数使用/ 传输类型	默认值	强制选择 (Class A,B)
标准参数									
模拟输入块附加参数									
10	OUT	Record	DS-33	D	5	r	O/cyc	变量、状态的测量	m (A,B)
11	PV_SCALE	Record	DS-36	S	11	r/w	C/a	—	m (A,B)
12	OUT_SCALE	Record	DS-36	S	11	r/w	C/a	—	m (B)
14	CHANNEL	Simple	Unsigned16	S	2	r,w	C/a	—	m (B)
16	PV_FTIME	Simple	Float	N	4	r,w	C/a	0	m (A,B)
19	ALARM_HYS	Simple	Float	S	4	r,w	C/a	0.5% of range	m (A,B)
21	HI_HI_LIM	Simple	Float	S	4	r,w	C/a	Max. value	m (A,B)
23	HI_LIM	Simple	Float	S	4	r,w	C/a	Max. value	m (A,B)
25	LO_LIM	Simple	Float	S	4	r,w	C/a	Min. value	m (A,B)
27	LO_LO_LIM	Simple	Float	S	4	r,w	C/a	Min. value	m (A,B)
30	HI_HI_ALM	Record	DS-39	D	14	r	C/a	0	m (A,B)
31	HI_ALM	Record	DS-39	D	14	r	C/a	0	m (A,B)
32	LO_ALM	Record	DS-39	D	14	r	C/a	0	m (A,B)
33	LO_LO_ALM	Record	DS-39	D	14	r	C/a	0	m (A,B)
34	SIMULATE	Record	DS-39	N	6	r,w	C/a	Disable	m (B)

D. 3.5 模拟输入块参数描述

表 D. 4 和表 D. 5 包含表 D. 3 中的参数的非形式化描述。图 D. 5 描述了限制检查参数之间的关系。

表 D.4 过程参数描述

参数	描述
CHANNEL	参考给 FB 提供测量值的活动转换块,编号和设备管理目录中的 Composite_Directory_Entry 中的转换块相同
OUT	过程变量 按照提供商特定的或已配置好的工程单位,FB 的参数 OUT 包含当前过程变量的值及其状况
PV_SCALE	过程变量到百分比的转化,使用高和低精确度值、工程单位代码和小数点右边的位数
OUT_SCALE	过程变量的范围 FB 的参数 OUT_SCALE 包含低限制和高限制有效范围的值、过程变量工程单位的代码和小数点右边的位数
PV_FTIME	过程变量滤波时间 FB 的参数 PV_FTIME 包含,从输入跳变开始,FB 输出上升到 63.21% 的上升时间的时间常数。参数的工程单位为秒

表 D.5 报警参数描述

参数	描述
ALARM_HYS	延迟 PROFIBUS-PA 规范的变送器,具有监测限制可调的限制违反(离开限制条件)的功能。 一个过程变量的值可能和一个限值相同,也可能围绕限制上下波动,这将导致产生很多的限制违反,触发很多消息。因此,必须在等待一个可调的延迟之后再触发消息。警报消息触发的灵敏度是可以调整的。延迟的值固定在 ALARM_HYS 中,对于 HI_HI_LIM、HI_LIM、LO_LIM 和 LO_LO_LIM 而言是相同的。延迟是小于限值和大于或等于限值之间的一个区间值,其工程单位为 xx_LIM
HI_ALM	警告上限状况 这个参数包含警告的上限状况和相关时间戳。时间戳表明了被测变量等于或高于警告上限的时间。没有时钟的设备使用 PROFIBUS-PA 的开始时间(1992 年 1 月 1 日)作为时间戳*
HI_HI_ALM	报警上限状况 这个参数包含报警的上限状况和相关时间戳。时间戳表明了被测变量等于或高于报警上限的时间。没有时钟的设备使用 PROFIBUS-PA 的开始时间(1992 年 1 月 1 日)作为时间戳*
HI_HI_LIM	报警上限值 带工程单位的报警上限值。如果被测变量等于或高于报警上限值,那么,OUT 的状况字节的状况位置 1,FB 的 ALARM_SUM 参数的状况位置 1
HI_LIM	警告上限值 带工程单位的警告上限值。如果被测变量等于或高于警告上限值,那么,OUT 的状况字节的状况位置 1,FB 的 ALARM_SUM 参数的状况位置 1
LO_ALM	警告下限状况 这个参数包含一个警告的下限状况和相关时间戳。时间戳表明了被测变量等于或高于警告下限的时间。没有时钟的设备使用 PROFIBUS-PA 的开始时间(1992 年 1 月 1 日)作为时间戳*

表 D.5(续)

参数	描述
LO_LIM	警告下限值 带有工程单位的警告下限值。如果被测变量等于或低于下限值,那么,OUT 的状况字节的状况位置 1,FB 的 ALARM_SUM 参数的状况位置 1
LO_LO_ALM	报警下限状况 这个参数包含一个报警的下限状况和相关时间戳。时间戳表明了被测变量等于或高于报警下限的时间。没有时钟的设备使用 PROFIBUS-PA 的开始时间(1992 年 1 月 1 日)作为时间戳 ^a
LO_LO_LIM	报警下限值 带有工程单位的报警下限值。如果被测变量等于或低于下限值,那么,OUT 的状况字节的状况位置 1,FB 的 ALARM_SUM 参数的状况位置 1
^a 见 ALARM_FLOAT_STRUCTURE。	

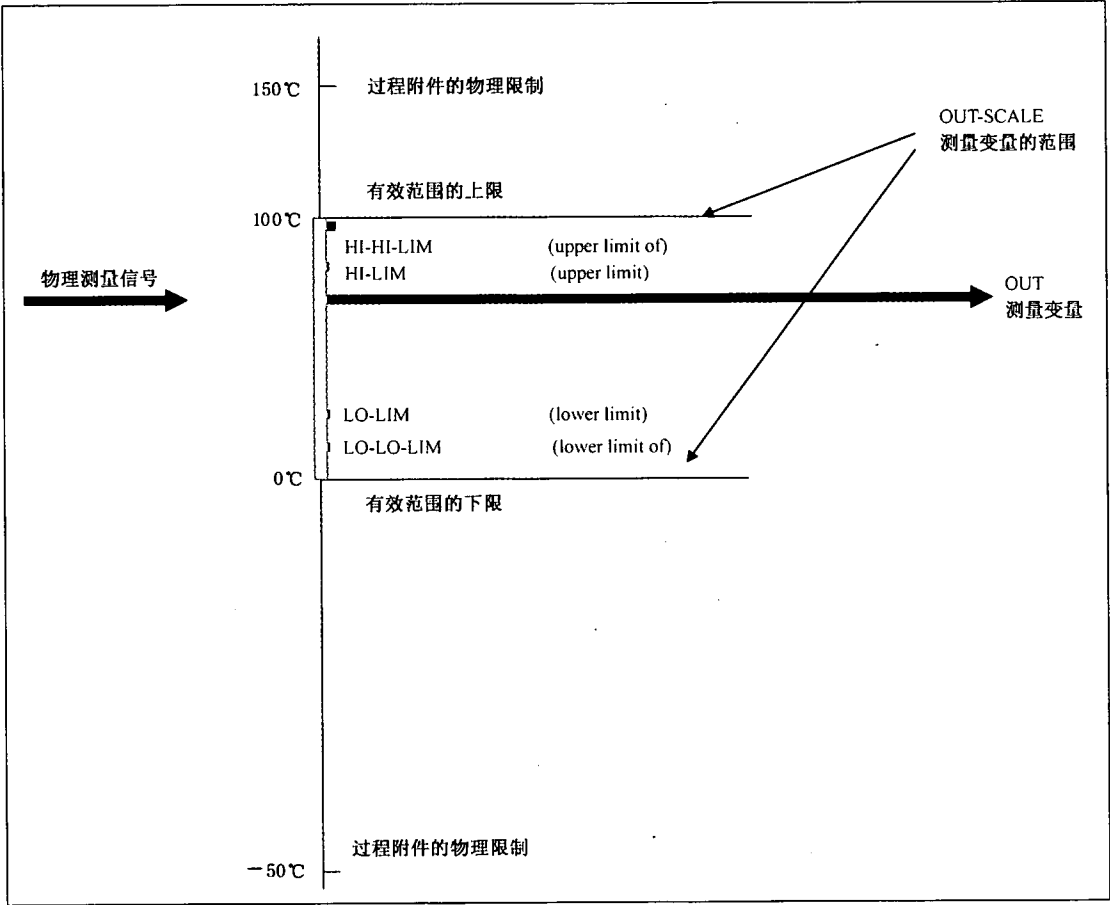


图 D.5 模拟输入块实例

表 D.6 仿真

参数	描述
SIMULATE	为了试运行和测试,可以改变模拟输入块 AI-FB 中来自转换块的输入值,这就意味着断开转换块和 AI-FB

D.4 映射

D.4.1 按照 GB/T 19769 图形表示的带有模式-事件的模拟输入块规范

在图 D.6 的图形表示中,很明显,FB 所谓的内含参数仅作为 INPUT 使用。功能块没有改变任何包含参数,因此,在输出事件产生之前这些参数不会被更新。AI_RESET_I 并没有强制功能块更新来自外部数据连接的 INPUT 变量。AI_RESET 功能是重置到默认值。

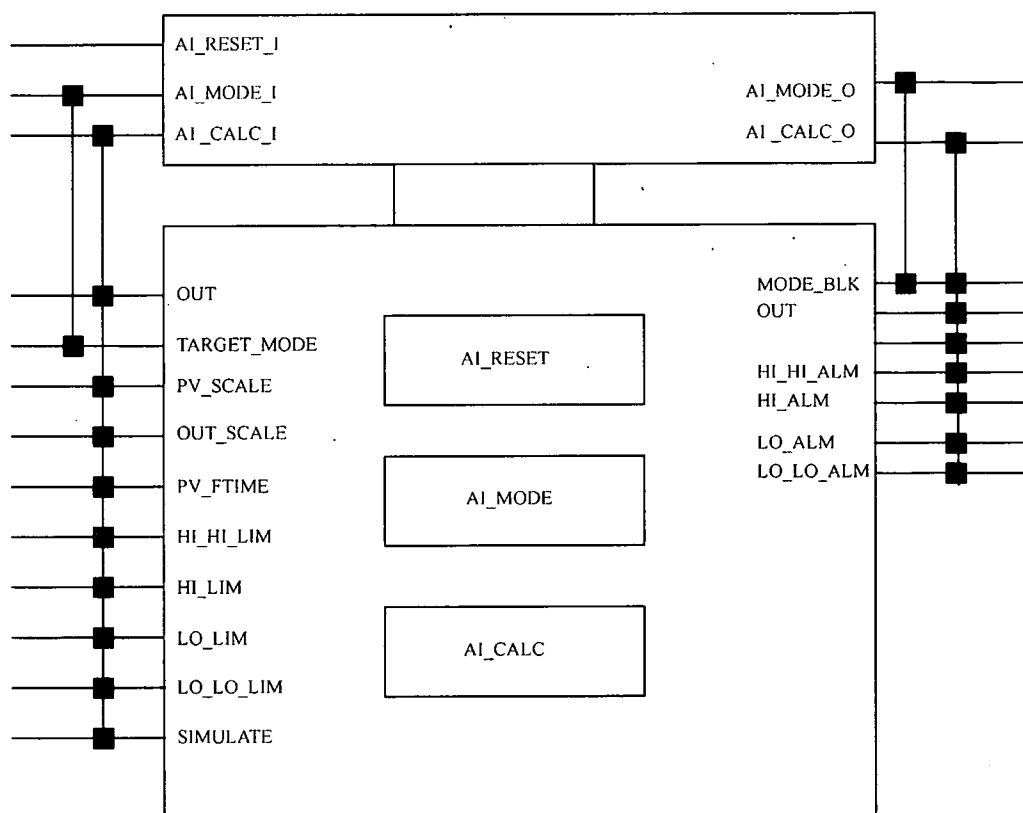


图 D.6 AI-FB 图形表示

D.4.2 根据 GB/T 19769 的模拟输入块的 ECC 规范

AI FB 有四个状态: START、RESET、MODE 和 MAIN, 见图 D.7。空闲状态是 START。当一个事件发生后, 转换到相关状态, 执行所连接的算法。算法执行完后产生输出事件。然后在没有其他事件的情况下返回到 START 状态(TRUE 转换)。

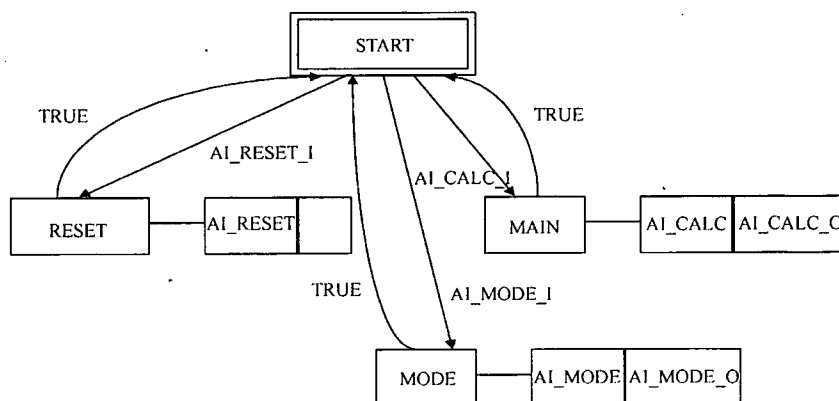


图 D.7 AI-FB ECC

D.4.3 根据 GB/T 19769 文本表示的模拟输入块规范

(* # 定义 STATUS 常量, 例如 BAD_OUT_OF_SERVICE, NC_GOOD, ... *)
 (* # 定义 MODE 常量, 例如 OUT_OF_SERVICE, MAN, AUTO *)
 (* 声明数据结构 DS_33, DS_37, *)

FUNCTION_BLOCK ANALOGUE_INPUT

EVENT_INPUT

AI_RESET_I;
 AI_MODE_I WITH TARGET_MODE;
 AI_CALC_I WITH OUT
 PV_SCALE,
 OUT_SCALE,
 PV_FTIME,
 HI_HI_LIM,
 HI_LIM,
 LO_LIM,
 LO_LO_LIM,
 SIMULATE;

END_EVENT

EVENT_OUTPUT

AI_MODE_O WITH MODE_BLK,
 AI_CALC_O WITH MODE_BLK,
 OUT,
 HI_HI_ALM,
 HI_ALM,
 LO_ALM,
 LO_LO_ALM,

END_EVENT

EC_STATES

START

RESET : AI_RESET;
 MODE : AI_MODE; AI_MODE -> AI_MODE_O;
 MAIN : AI_MODE, AI_CALC -> AI_CALC_O;
 (* Is it necessary that every ec_action generate an output event? *)

END_STATES

EC_TRANSITION

START TO RESET := AI_RESET_I;
 START TO MAIN := AI_CALC_I;
 START TO MODE := AI_MODE_I;

```

    RESET TO START      := TRUE;
    MODE TO START       := TRUE;
    MAIN TO START       := TRUE;
END_TRANSITION

```

(* ----- *)

VAR_OUTPUT

```

    MODE_BLK :          DS_37;
    OUT :              DS_33;
    HI_HI_ALM :        DS_39;
    HI_ALM :           DS_39;
    LO_ALM :           DS_39;
    LO_LO_ALM :        DS_39;
END_VAR

```

VAR_IN

(* INPUT variables are read/write *)

```

    TARGET_MODE      Unsigned8;
    OUT :            DS_33;
    PV_SCALE :       DS_36;
    OUT_SCALE :      DS_36;
    PV_FTIME :       FLOAT;
    HI_HI_LIM :      FLOAT;
    HI_LIM :         FLOAT;
    LO_LIM :         FLOAT;
    LO_LO_LIM :      FLOAT;
    SIMULATION :     DS_50;

```

(* for MANUAL MODE *)

END_VAR

VAR

```

    TB_MEASURED_VALUE : DS_33;
    PV : DS_33;
    TEMP : FLOAT;

```

(* input value from the transducer FB *)

END_VAR

(* ----- *)

(* 注：内部算法使用 GB/T 15969.3 的结构化文本语言来描述。 *)

ALGORITHM AI_RESET

```

    OUT := 0;
    PV_SCALE.EU0 := 0;
    PV_SCALE.EU100 := 100;
    PV_SCALE.EU := 35;

```

(* code for ... *)

```

PV_SCALE.DP := 2;                                (* valid decimal point *)
OUT_SCALE.EU0 := 0;
OUT_SCALE.EU100 := 100;
OUT_SCALE.EU := 35;                                (* code for ... *)
OUT_SCALE.DP := 2;                                (* valid decimal point *)
PV_FTIME := 1;
HI_HI_LIM := OUT_SCALE.EU100;
HI_LIM := OUT_SCALE.EU100;
LO_LIM := OUT_SCALE.EU0;
LO_LO_LIM := OUT_SCALE.EU0;
END_ALGORITHM

(* ----- *)

```

ALGORITHM AI_MODE

(* 实际 MODE 值的计算 *)

```

IF RESOURCE_STATE <> OK
    THEN MODE_BLK.ACTUAL = OUT_OF_SERVICE;
END_IF
IF TARGET_MODE = OUT_OF_SERVICE
    THEN MODE_BLK.ACTUAL = OUT_OF_SERVICE;
END_IF
IF TARGET_MODE = MAN & MODE_BLK.ACTUAL = OUT_OF_SERVICE
    & RESOURCE_STATE = OK
    THEN MODE_BLK.ACTUAL = MAN;
END_IF
IF TARGET_MODE = AUTO & MODE_BLK.ACTUAL = OUT_OF_SERVICE
    & RESOURCE_STATE = OK
    THEN MODE_BLK.ACTUAL = MAN;
END_IF
IF TARGET_MODE = AUTO & MODE_BLK.ACTUAL = MAN
    & RESOURCE_STATE = OK
    & TB_MEASURED_VALUE.STATUS = NC_GOOD
    THEN MODE_BLK.ACTUAL = AUTO;
END_IF
(* TB_MEASURED_VALUE is a call by reference in the PROFIBUS/FF FB model *)
IF TARGET_MODE = AUTO & MODE_BLK.ACTUAL = MAN
    & RESOURCE_STATE = OK
    & TB_MEASURED_VALUE.STATUS <> NC_GOOD
    THEN MODE_BLK.ACTUAL = MAN;
END_IF
IF TARGET_MODE = AUTO & MODE_BLK.ACTUAL = AUTO
    & RESOURCE_STATE = OK

```

```

                                & TB_MEASURED_VALUE.STATUS (>) NC_GOOD
      THEN MODE_BLK.ACTUAL = MAN;
    END_IF
  (* calculation of the OUT status *)
    IF MODE_BLK.ACTUAL = OUT_OF_SERVICE
      THEN OUT.STATUS := BAD_OUT_OF_SERVICE;
    END_IF
    IF MODE_BLK.ACTUAL = MAN
      THEN OUT.STATUS := UNCERTAIN_NON_SPECIFIC;
    END_IF
    IF MODE_BLK.ACTUAL = AUTO
      & TB_MEASURED_VALUE.STATUS = NC_GOOD
      & SIMULATE.ENABLE = FALSE
      THEN OUT.STATUS := NC_GOOD_NON_SPECIFIC;
    END_IF
    IF MODE_BLK.ACTUAL = AUTO
      & TB_MEASURED_VALUE.STATUS = HIGH_LIMIT
      & SIMULATE.ENABLE = FALSE
      THEN OUT.STATUS := HIGH_LIMIT;
    END_IF
    IF MODE_BLK.ACTUAL = AUTO
      & TB_MEASURED_VALUE.STATUS = LO_LIMIT
      & SIMULATE.ENABLE = FALSE
      THEN OUT.STATUS := LO_LIMIT;
    END_IF
  END_ALGORITHM

```

(* ----- *)

ALGORITHM AI_CALC

VAR FIELD_VALUE : FLOAT; END_VAR

(* FB simulation *)

```

    IF SIMULATION.ENABLE = TRUE
      THEN TB_MEASURED_VALUE.STATUS := SIMULATION.STATUS;
      TB_MEASURED_VALUE.VALUE := SIMULATION.VALUE;
    END_IF;

```

(* calculation of MEAS_VALUE in % *)

```

    FIELD_VALUE := (TB_MEASURED_VALUE.VALUE - PV_SCALE-EU0) /
                  (PV_SCALE-EU100 - PV_SCALE-EU0)

```

```

    PV.VALUE := FIELD_VALUE * (OUT_SCALE-EU100 - OUT_SCALE-EU0)
                + OUT_SCALE.EU0

```

(* calculation of OUT in Engineering Unit *)

```

    IF MODE_BLK.ACTUAL = AUTO

```

```

OUT.VALUE := PV.VALUE
END_IF
(* limit check and Alarm generation *)
IF OUT.VALUE > HI_LIM THEN

END_IF;
IF OUT.VALUE > HI_HI_LIM THEN

END_IF;
IF OUT.VALUE < LO_LIM THEN

END_IF;
IF OUT.VALUE < LO_LO_LIM THEN

END_IF;
END_ALGORITHM
END_FUNCTION_BLOCK

```

```

OUT.STATUS := HIGH_LIMIT;
HI_ALM.VALUE := OUT.VALUE;
HI_ALM.ALARM_STATE := 1; (*... *)
HI_ALM.SUBCODE := 1; (*... *)

OUT.STATUS := HIGH_LIMIT;
HI_HI_ALM.VALUE := OUT.VALUE;
HI_ALM.ALARM_STATE := 1; (*... *)
HI_ALM.SUBCODE := 1; (*... *)

OUT.STATUS := LO_LIMIT;
LO_ALM.VALUE := OUT.VALUE;
HI_ALM.ALARM_STATE := 1; (*... *)
HI_ALM.SUBCODE := 1; (*... *)

OUT.STATUS := LO_LO_LIMIT;
LO_LO_ALM.VALUE := OUT.VALUE;
HI_ALM.ALARM_STATE := 1; (*... *)
HI_ALM.SUBCODE := 1; (*... *)

```


附 录 E
(资料性附录)
AME 需求

E.1 概述

系统和网络管理的规范超出了本部分的范围。本部分以下应用的信息不是标准化的。然而,本附录中描述的 AME 需求是本部分和 GB/T 21099.2 中描述的分布式功能块系统的预期的实际实现。

E.2 系统管理需求

E.2.1 标签

一个设备至少需要一个唯一的标识符,可由下面的四个资源参数实现:

- a) 制造商名字;
- b) 类型或模型编号;
- c) 修正号;
- d) 序列号。

这些参数由制造商固定在设备中。

- 在正常操作下,一个设备由单个的叫做物理标签的唯一设备参数来命名。物理标记用于在正常设备操作期间同设备的通信。当设备从系统中移去或失电又恢复时,要求物理标签一直保持在设备中(即非易失性)。
- 要求系统和网络管理有能力确定一个设备没有分配物理标签(即为缺省值或空标签)的功能,以便通过制造商/型号/序列号识别该设备,并给它分配一个物理标签。要求这些功能的操作不妨碍系统中其他设备之间的通信。
- 要求系统和网络管理有能力确定一个标签(物理标签或块标签)在系统中是唯一的(即,在物理标签和块标签中都是唯一的)。只要分配了一个新标签、改变了一个标签或系统中加入了带有预配置标签的新设备时,系统和网络管理都要执行这些功能。要求这些功能的操作不妨碍系统中其他设备之间的通信。
- 在含有单个 FB 和 FB 资源的设备中,要求物理标签、资源块标签和 FB 标签是同一个标签。
- 在含有单个 FB 资源的设备中,要求物理标签和资源块标签是同一个标签。

E.3 网络寻址

- a) 要求系统和网络管理具有从系统中增加和移除设备的功能,而不妨碍系统中的其他设备的网络寻址或运行。
- b) 要求系统和网络管理支持三种类型设备的寻址:
 - 1) 临时设备;
 - 2) 新设备(不带有系统分配的地址);
 - 3) 系统设备(带有系统分配的地址)。
- c) 要求系统和网络管理支持三种地址分配方法:
 - 1) 预分配;
 - 2) 系统固定分配;
 - 3) 系统动态分配。
- d) 通过硬件跳线或开关将预分配节点地址固定到设备中。当设备从系统中移去或失电又恢复时,系统固定分配节点地址一直保持在设备中(即非易失性)。当设备从系统中移去或失电时,系统动态分配节点地址不保持在设备中(即易失性)。
- e) 要求系统和网络管理具有允许系统确定设备所支持的节点地址分配方法的功能。

- f) 要求支持系统指定节点地址分配的设备同时支持固定的和动态的分配方法。要求无论是固定的还是动态的系统分配节点地址方法都是在设备中通过硬件跳线或开关由用户配置的。
 - g) 设备的物理标签和节点地址一一对应。在系统分配节点地址给设备前,要求支持系统分配节点地址的设备具有一个已分配的物理标签。在使用预分配节点地址在系统中正常操作前,要求带有预分配节点地址的设备具有一个已分配的物理标签(即带预分配节点地址的但没有物理标签的设备仅允许做系统管理操作)。
 - h) 要求系统和网络管理具有允许系统来确定那些保持在新设备中的节点地址(预定义的或固定的)在系统中是唯一的。新设备加入系统中时,要求系统和网络管理执行该功能。要求该功能的操作不妨碍系统中其他设备的节点寻址和操作。
 - i) 在系统中一些设备含有预定义的节点地址,而其他设备含有系统分配的节点地址,要求系统和网络管理防止系统中出现节点地址的重复。同样地,在系统中一些设备含有系统分配的固定的节点地址,而其他设备含有系统分配的动态的节点地址,要求系统和网络管理防止系统中出现节点地址的重复。
- 注:这意味着,要求带有预定义或固定节点地址的设备,支持与带有动态节点地址的设备相同的系统和网络管理节点地址分配协议。
- j) 要求系统和网络管理防止某些设备的引入,这些设备含有的标签与系统中已经操作的标签重复。要求阻止这种新设备的运行,如果新设备支持预分配节点地址;并且不要为这种新设备分配节点地址,如果这种新设备支持系统指定节点地址(固定的或动态的)。

E. 4 数据对象命名约定

DFBAP 中的参数的寻址/命名具有不同的视图,FB 应用视图、通信配置视图、设备标识视图和其他可能的视图。标识符在系统指定部分的范围内是不同的,即标识符在定义的区域是唯一的。这要求在标准中明确的定义。

图 E. 1 给出了一个可能的方法。

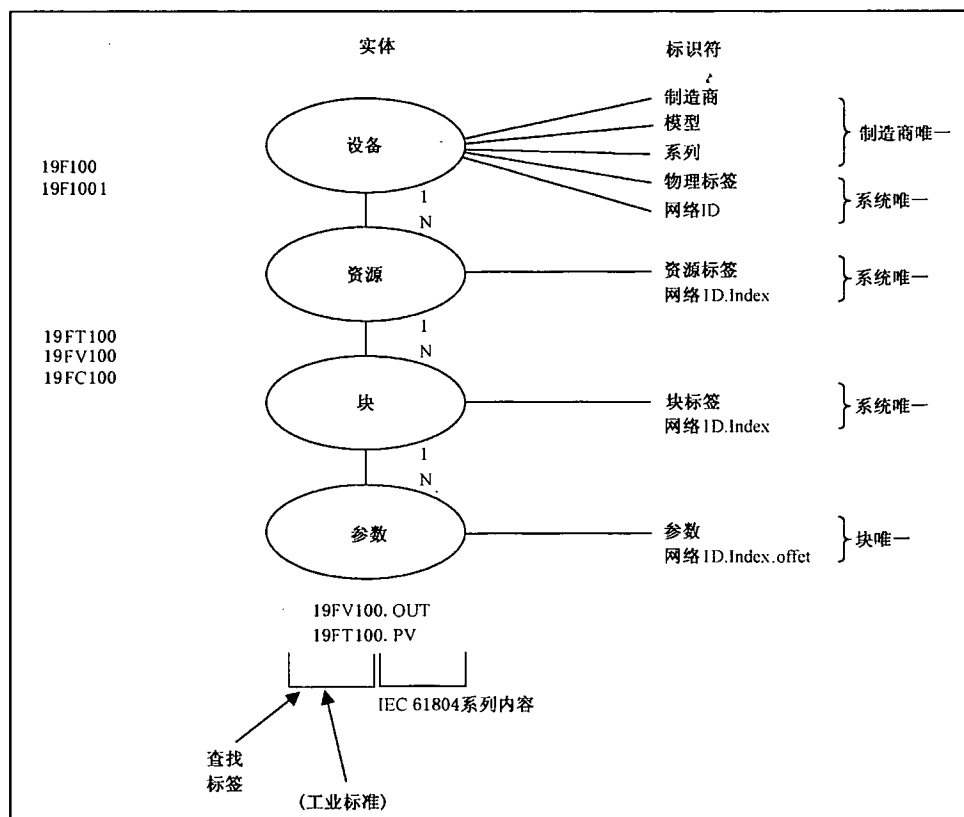


图 E. 1 命名和寻址方法

E.5 设备通信关系

- a) 要求系统和网络管理具有建立和终止不同设备功能中的块间通信关系的功能。要求这些功能的运行不妨碍现有的通信关系或系统中其他设备和功能的运行。
- b) 要求不同设备功能之间的通信关系通过参考“标签参数”确定。要求系统和网络管理具有确定设备中的“节点地址和索引”参考的功能、授予“标签参数”参考,反之亦然,以支持功能块环境中通信关系的配置。
- c) 当失电又恢复时,要求保持已确定的不同设备功能之间的通信关系。

E.6 时间同步

E.6.1 时间对象

要求系统和网络管理包括数据结构定义和相关功能,以使 FB 环境时间和数据链路时间相关联,称为时间对象。要求事件对象支持数据通信和 FB 执行之间的协调。

E.6.2 时间发布者

- a) 要求系统和网络管理包括数据结构定义功能和协议,以发送应用时间同步到分布式 FB 环境,称为时间发布者。要求时间发布者支持分布式应用中数据时间戳和功能执行之间的协调。
- b) 要求系统和网络管理包括支持多余冗余时间发布者(主要的和多个次要的)的功能和协议。

E.6.3 时间订阅者

要求系统和网络管理包括数据结构定义和相关功能,以便分布式 FB 环境接收应用时间同步,称为时间订阅者。要求时间订阅者与时间发布者结合进行操作。

E.6.4 本地时间

要求系统和网络管理时间分配方法支持本地的和世界时间的分配。

E.6.5 网络(链路)时间

- a) 要求系统和网络管理包括用于同步各总线段的网络(链路)时间的功能和协议。要求网络(链路)时间支持多段间的时间严格通信的同步。
- b) 系统和网络管理需要包括用于同步总线网段和更高层系统(如 DCS 或 PLC 控制器)间的网络(链路)时间的功能和协议。要求网络(链路)时间支持总线段和高层次系统间的时间严格通信的同步(即在网段设备和更高层系统设备之间的串级结构中同步 FB 执行和通信)。

E.7 冗余系统组成部分

- a) 要求系统和网络管理包括用于管理多余(N-redundant)系统组成部分的功能和协议,包括:
 - 1) 媒体;
 - 2) 物理层;
 - 3) 设备(包括网关、路由器、网桥、中继器和终端设备);
 - 4) 设备中的应用过程。
- b) 要求系统和网络管理包括用于管理单工-双工(simplex-to-duplex)网桥和路由器的数据、功能和协议。
- c) 要求系统和网络管理包括用于管理单个设备中的双工(duplex)媒体和物理层的数据、功能和协议。
- d) 要求系统和网络管理包括用于支持设备、段和网络的通道选择的数据、功能和协议。
- e) 要求系统和网络管理包括用于支持某些应用过程的冗余方面的数据、功能和协议。如:
 - 1) 路由器和网关应用过程;
 - 2) 投票应用过程;
 - 3) 包含冗余应用实体(即,冗余 FB)的应用过程。

E.8 诊断

- a) 要求系统和网络管理包括用于管理系统组成部分性能的数据结构、功能和协议,包括:
 - 1) 执行预防维护;
 - 2) 诊断中断错误;
 - 3) 通报和定位错误;
 - 4) 初发错误和故障的警告;
 - 5) 从错误和故障中恢复。
- b) 要求系统和网络管理用于诊断的数据结构、功能和协议服务于:
 - 1) 媒体;
 - 2) 设备;
 - 3) 应用;
- c) 要求系统和网络管理用于诊断的数据结构、功能和协议至少包含下面的诊断计数器:
 - 1) 到或来自 FB 资源的通信消息的总数;
 - 2) 到或来自 FB 资源的 CRC 错误的总数;
 - 3) 到或来自 FB 资源的帧错误的总数;
 - 4) 到或来自 FB 资源的“参数不支持”错误的总数;
 - 5) 到 FB 资源的接收缓冲区满错误的总数;
 - 6) 到 FB 资源的报警缓冲区满错误的总数;
 - 7) 到或来自 FB 资源的 FB 服务忙错误的总数;
 - 8) 来自 FB 资源的发送缓冲区非空错误的总数;
 - 9) 到或来自 FB 资源的其他通信错误(上面未列出的)的总数。
- d) 要求这些计数器初始化为零,且要求由系统和网络管理提供服务来重新初始化它们。如果发生了延期,要求系统和网络管理就发出一个 FB 环境延期警告消息。这个消息包含发生延期的时间和计数器的标识。
- e) 要求系统和网络管理用于诊断的数据结构、功能和协议包括一个诊断计数器重置参数,这个参数包含(本地)时间。
- f) 要求系统和网络管理用于诊断的数据结构、功能和协议包括一个错误率参数,定义为每个通信周期内 CRC 错误数和成帧误差数的总和。
- g) 要求系统和网络管理用于诊断的数据结构、功能和协议包括一个可配置的错误率限值参数。如果错误率超过了这个错误率限值,要求系统和网络管理就发出一个 FB 环境错误率限制报警消息。这个消息包含时间和当前错误率。
- h) 要求系统和网络管理用于诊断的数据结构、功能和协议为支持环回测试的设备包括控制和执行物理层环回测试的功能。要求系统中一个终端设备的环回测试不妨碍系统中其他终端设备的时间严格通信。

E.9 通信管理

要求系统和网络管理服务包括用于建立和维护所有设备中所有协议层的通信配置(即管理所有设备中所有层管理实体)的数据结构、功能和协议。

E.10 系统和网络管理服务

要求提供下面的系统和网络管理服务:

- a) 设置物理标签(带或不带有已分配的节点地址);

- b) 设置地址(仅带物理标签);
- c) 清除地址(仅带物理标签);
- d) 标识设备(物理标签和节点地址);
- e) 查找标签(物理或块);
- f) FB 启动(带有块标签);
- g) 管理信息基本权限(读和写);
- h) 发布时间(应用和连接)。

E.11 设备模型的综合管理

设备模型中需要一个明确的管理模型的规范。这是规定 AME 和 FB 环境之间的接口的先决条件。

参 考 文 献

[1] GB/T 18272.1—2000 工业过程测量和控制 系统评估中系统特性的评定 第1部分:总则和方法学 (IEC 1069-1:1991, IDT)

[2] GB/T 18272.5—2000 工业过程测量和控制 系统评估中系统特性的评定 第5部分:系统可信性评估 (IEC 1069-5:1994, IDT)

[3] PRIAM:1995, Prenormative Requirements for Intelligent Actuation and Measurement (Esprit Project, 1992-1995)

[4] VDI/VDE 3696:1995, Herstellerneutrale Konfigurierung von Prozeßleitsystemen

[5] EOQ (European Organisation for Quality): Glossary of terms used in the management of quality Afnor NFX 60-010—Maintenance—Concepts and definitions of Maintenance activities

[6] IEC 60870-6-503:1997, Telecontrol equipment and systems—Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations—Section 503: TASE.2 Services and protocol

[7] IEC 60870-6-702:1998, Telecontrol equipment and systems—Part 6-702: Telecontrol protocols compatible with ISO standards and ITU-T recommendations—Functional profile for providing the TASE.2 application services in end systems

[8] IEC 61158:2001, Digital data communication for measurement and control—Fieldbus for use in industrial control systems3: Part 1 : Introduction to IEC 61158 series, Part 5 : Application Layer service definition. Part 6 : Application Layer protocol specification

[9] ISO 15745-1, Industrial automation systems and integration—Open systems application integration frameworks—Part 1: Generic Reference Description3

[10] ISA-TR50.02, Part 9—2000, Fieldbus Standard for Use in Industrial Control Systems: User Layer Technical Report.

[11] BSI 7986:2001 Specification for Data Quality Metrics for Industrial Measurement and Control Systems.

中 华 人 民 共 和 国
国 家 标 准

过程控制用功能块

第 1 部分：系统方面的总论

GB/T 21099.1—2007/IEC/CDV 61804-1:2003

*

中国标准出版社出版发行
北京复兴门外三里河北街16号

邮政编码：100045

网址 www.spc.net.cn

电话：68523946 68517548

中国标准出版社秦皇岛印刷厂印刷

各地新华书店经销

*

开本 880×1230 1/16 印张 6.5 字数 193 千字

2008年1月第一版 2008年1月第一次印刷

*

书号：155066·1-30435 定价 50.00 元

如有印装差错 由本社发行中心调换

版权专有 侵权必究

举报电话：(010)68533533



GB/T 21099.1-2007