# 工业控制网络的研究现状及发展趋势

胡 毅[1,2] 于 东[2] 刘明烈[2]
(中国科学院研究生院 北京 100039)[1]
(中国科学院沈阳计算技术研究所高档数控国家工程研究中心 沈阳 110171)[2]

**摘 要** 工业控制网络在工业通信及先进制造领域起到关键性作用。回顾了工业控制网络的发展历程,重点分析了工业以太网的实时通信技术,针对通信实时性的强弱性质将目前主流工业以太网进行了分类研究,将其划分为软实时、硬实时以及同步硬实时3类,重点探讨了各自的实时通信机制。同时阐述了正在进入工业控制领域的实时异构网络及无线网络,最后讨论了工业控制网络研究的技术难题,并提出了新的发展方向。

**关键词** 工业控制网络,工业以太网,软实时,硬实时,同步硬实时
**中图法分类号** TP393 **文献标识码** A

## Present Research and Developing Trends on Industrial Control Network

HU Yi[1,2] YU Dong[2] LIU Ming-lie[2]
(Graduate University of Chinese Academy of Sciences, Beijing 100039, China)[1]
(National Engineering Research Center for High-End CNC, Shenyang Institute of Computing Technology, CAS, Shenyang 110171, China)[2]

**Abstract** Industrial control network is needed for industrial communication and advanced manufacture. An overview on the evolution process was given, and the real-time technology of industrial ethernet was summarized. By analyzing the real-time behavior of industrial ethernet, this paper divided it into soft real-time, hard real-time and isochronous real-time classes, and expatiated the real-time research methods of each class in detail. The architecture of real-time heterogeneous networks was described, and the researches of wireless industrial network were proposed. Finally, the prospects and the further research direction were pointed out.

**Keywords** Industrial control network, Industrial ethernet, Soft real-time, Hard real-time, Isochronous real-time

## 1 引言

工业控制网络在提高生产速度、管理生产过程、合理高效加工以及保证安全生产等工业控制及先进制造领域起到越来越关键的作用[1]。工业控制网络从最初的计算机集成控制系统CCS到集散控制系统DCS,发展到现场总线控制系统[2]。近年来,以太网进入工业控制领域,出现了大量基于以太网的工业控制网络[3,4]。同时,随着无线技术的发展,基于无线的工业控制网络的研究也已开展[5]。图1总结了工业控制网络的4大主要类型:传统控制网络、现场总线、工业以太网以及无线网络。传统控制网络现在已经很少使用,目前广泛应用的是现场总线与工业以太网,而工业以太网关键技术的研究是目前工业控制网络研究的热点。

本文对目前广泛采用的现场总线、工业以太网以及无线网络的现状及发展趋势进行了探讨,重点在于工业以太网关键技术的研究。工业通信的核心问题是通信实时性,本文基于实时性这一关键问题将工业以太网划分为软实时、硬实时以及同步硬实时工业以太网3类展开研究。

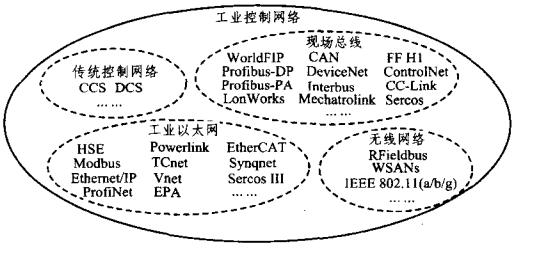


图1 工业控制网络的主要分类

## 2 现场总线

现场总线广泛应用于连接现场设备,如控制器、传感器与执行器等,采用全数字通信,结构简单,节约线缆。与传统DCS相比,现场总线安装成本降低了约50%[1]。现场总线实现信息处理的现场化,在传输控制信息的同时,可从现场获取更多诊断、维护等非控制信息。

目前现场总线技术已得到广泛应用,其定义、规格、实现和市场等方面都比较成熟[6,7]。国际标准IEC 61158中包含了TS61158, Profibus, P-NET, WorldFIP, Interbus, FF H1, Sercos以及CC_Link等10余种主要类型的现场总线[8,27]。

到稿日期:2009-03-04 返修日期:2009-05-06 本文受科技部国家科技支撑计划重点项目(2007BAP20B01),中科院东北振兴重点项目资助。
胡 毅(1982-),男,博士研究生,主要研究方向为开放式数控系统、数控总线、工业控制网络等,E-mail:huyi@sict.ac.cn;于 东(1966-),男,博士,研究员,博士生导师,主要研究方向为数控技术、数控总线等;刘明烈(1938-),男,研究员,主要研究方向为数控技术、工业控制网络等。

引领世界的主要有 Profibus 总线以及 Interbus 总线[9]。同时，也有一些应用广泛但还没有纳入 IEC 标准的现场总线，如 DeviceNet 总线以及 CAN 总线等[10]。

对比研究发现，各种现场总线在传输率、支持节点数以及传输距离等方面各不相同。目前现场总线产品主要是低速总线，传输速率为 31.25kbps，从应用状况看，低速总线如 FF 和 Profibus 等能良好实现速率要求较低的过程控制。而高速总线最高传输速率为 16Mbps，且种类较少，主要用于控制网内部互连，如连接控制器、PLC 等智能程度较高、处理速度较快的设备。

随着应用需求的提高，现场总线的高成本、低速率、难于选择以及难于互连、互通、互操作等问题逐渐显露。工业控制网络发展的基本趋势是逐渐趋向于开放性以及透明的通讯协议。现场总线出现的问题的根本原因在于总线的开放性是有条件且不彻底的。同时，以太网具有传输速度高、易于安装和兼容性好等优势，因此基于以太网的工业控制网络是发展的趋势。

## 3 工业以太网

将以太网应用于工业控制领域，构成工业以太网，已成为目前研究的热点[10,11]。典型的工业以太网结构如图 2 所示，由现场设备层、控制层以及管理层构成。各层都有其本质需要和不同类型的信息交换，网络大小、支持设备数量、网络速度、反馈时间和负载大小等方面的不同导致各层所采用的网络技术也不同[12]。考虑到工业以太网对实时性能的需求，实时性主要依赖于传输消息的类型，在现场设备层，要求进行实时通信，有严格受限的硬件及通信资源，而在管理层则可允许进行非实时通信[3,13]。

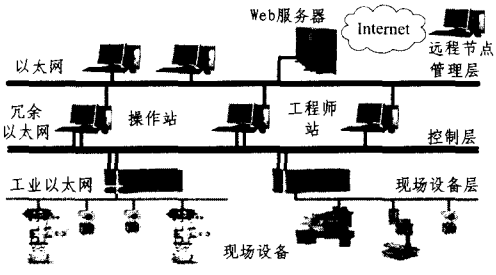


图 2 典型工业以太网基本结构

### 3.1 工业以太网实时技术研究

目前，工业以太网研究的关键技术包括通信实时性、网络互操作性、总线供电、安全性与可靠性等方面[9,12]，本文重点研究通信实时性。

传统共享式以太网采用总线式的拓扑结构和多路存取载波侦听/碰撞检验 CSMA/CD 通信方式[14]，集线器被动接收输入端口信息并以广播方式发送到所有输出端口。冲突的存在使得共享式以太网具有不确定性，会导致某些节点数据帧的丢失[15]。共享式以太网通信延时定义如下：

$$T_E = T_{ETE} + T_C \tag{1}$$

其中，$T_{ETE}$ 表示网络上端到端节点的通信延时；$T_C$ 表示数据帧在源节点的等待延迟，定义如下：

$$T_C = \sum_{k=1}^{N_C} (T_{CDT} + T_{JAM} + T_{BOK}) \tag{2}$$

其中，$N_c$ 为最大碰撞次数，$T_{CDT}$ 为碰撞检测时间，$T_{JAM}$ 为碰撞发生后发送阻塞信号所需的时间。$T_{BOK}$ 为 BEB 算法退避时间，定义如下，其中 $T_S$ 是缝隙时间。

$$T_{BOK} = (uniform[1, 2^{\min(k,10)}] - 1) \cdot T_S \tag{3}$$

文献[4]以 10BASE-T 以太网为例对共享式以太网的最大通信延时进行了计算。1bit 数据传输时间 $T_b = 1/10 \times 10^6 \text{bps} = 0.1\mu s$，传输速度 $T_V = 0.65 \times 2.0 \times 10^8 \text{m/s}$。电缆长度为 100m，传输一个 177Bytes 数据帧，共享式以太网最大通信延时 $T_E = 418.8\text{ms}$，这不能满足工业通信实时性的要求[4]。

为解决共享式以太网在通信实时性方面存在的问题，近年来的研究主要集中在交换式以太网技术及全双工通信技术等领域[16-18]。交换式以太网的特点是使用交换机代替集线器，交换机主动识别接收信息的目的端口并将数据帧通过目的端口传递，从而有效避免了碰撞，另外采用全双工方式提高了传输效率[19,20]。交换式以太网通信延时定义如下：

$$T_E = T_{ETE} + T_Q \tag{4}$$

其中，$T_Q$ 为端口排队延时，在没有端口排队的情况下，该延时与传统以太网中无碰撞时延时相同，均为 $T_{ETE}$。假设端口缓冲区有 $N_q$ 个帧排队，$T_Q$ 定义如下：

$$T_Q = \sum_{k=1}^{N_q} (T_{IF} + T_{TK}) \tag{5}$$

其中，$T_{IF}$ 是两帧传输之间的等待时间，$T_{Tk}$ 为第 $k$ 个数据帧加上前导码的最大比特数。以上述例子为例[4]，交换式以太网可计算得出最大通信延时 $T_E = 741.57\mu s$。

由此可见，交换式以太网采用交换机代替集线器，使交换设备各端口之间可以同时形成多个数据通道以降低网络流量，端口之间的报文不受 CSMA/CD 影响。同时采用全双工通信技术，使端口之间的线路同时接收和发送报文帧。交换式以太网的最大传输延时比共享式以太网要小很多，能较好地保证工业控制网络的实时性能，是目前工业以太网实时性能研究的方向。

### 3.2 工业以太网的分类

目前工业以太网种类较多，国际标准 IEC 61784 包含有 Modbus，Ethernet/IP，ProfiNet，Tcnet，Vnet/IP，Powerlink，EtherCAT 以及 Sercos III 等[21,22]。通过对这些网络协议的深入分析，本文从实时调度的角度对工业以太网进行了分类研究。一类工业以太网数据传输的调度在 TCP(UDP)/IP 之上，主要采用交换式以太网技术调度实时和非实时数据。这类方式对实时和非实时优先级的设置严格。另一类数据传输的调度则在以太网 MAC 上，研究重点是运动控制中同步数据传输的实时机制以及实时与非实时之间的调度机制。因此，按照通信的实时性，现有工业以太网可划分为以下几类进行研究：

(1)软实时工业以太网。数据传输的实时调度在 TCP(UDP)/IP 之上，响应时间为几十毫秒，主要用于工厂控制领域。典型的有 Modbus，Ethernet/IP 等。

(2)硬实时工业以太网。数据传输的实时调度在 MAC 之上，响应时间为 1ms～10ms，主要用于过程控制领域。典型的有 ProfiNet IO，Tcnet，Vnet 等。

(3)同步硬实时工业以太网。带精确的时钟同步，响应时间为 250μs 到 1ms，抖动小于 1μs，主要用于运动控制领域。典型的有 Powerlink，EtherCAT，Sercos III，基于等时特性的

ProfiNet IO 及基于时间同步的 Ethernet/IP 等。

(4)非实时工业以太网。主要用于诊断、维护、测试等方面,不在本文研究之列。

由于不同类型数据具有不同的传输需求,需要不同的传输机制,因此工业以太网采用了不同的应用模型。典型应用模式包括客户/服务器 C/S 通信模型和发布者/订阅者 P/S 通信模型[23,24]。

表 1 按通信实时性对 IEC 61784 中主要工业以太网进行了分类,从传输率、传输距离、实时和非实时调度方式以及应用模式等方面进行了对比。

表 1 基于实时性分类的工业以太网

| 类型 | 实时类型 | 最大传输率 | 最长距离 | 实时调度 | 非实时调度 | 模型 |
|---|---|---|---|---|---|---|
| Modbus-RTPS | 软实时 | 100Mbps | 100m/seg | TCP/IP之上 | TCP/IP之上 | P/S |
| Ethernet/IP | 软实时 | 1Gbps | IEEE 802.3 | TCP/IP之上 | TCP/IP之上 | P/S |
| ProfiNet | 软实时 | 100Mbps | 100m/seg | UDP/IP之上 | UDP/IP之上 | P/S |
| TCnet | 硬实时 | 100Mbps | 100m/seg | MAC之上 | TCP/IP之上 | P/S |
| Vnet/IP | 硬实时 | 1Gbps | IEEE 802.3 | MAC之上 | UDP/IP之上 | C/S |
| Powerlink | 同步硬实时 | 100Mbps | 100m/seg | MAC之上 | UDP/IP之上 | C/S |
| EtherCAT | 同步硬实时 | 100Mbps | 100m/seg | MAC之上 | UDP/IP之上 | C/S |

### 3.2.1 软实时工业以太网

软实时工业以太网主要采取了交换式以太网技术与 TCP(UDP)/IP 机制,其实时调度在 TCP(UDP)/IP 之上,但所使用的对象模型和应用过程机制各不相同。软实时工业以太网提供了几十毫秒范围内响应时间,其实时行为是不可决定的。工业应用有 Modbus-RTPS, Ethernet/IP, FF HSE 以及 ProfiNet 等。

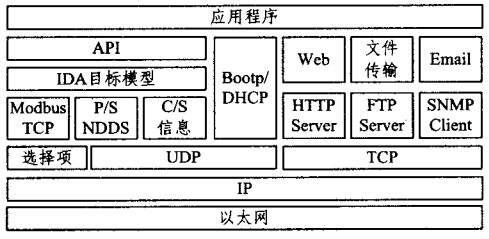


图 3 Modbus-RTPS 的通信协议模型

• Modbus-RTPS[25]

Modbus-RTPS 是 2005 年由 Modbus 组织和德国 IDA 集团联合开发的基于 Ethernet TCP/IP 的实时以太网。Modbus-RTPS 的实时扩展在于建立一个新的实时通信应用层,采用一种新的通信协议 RTPS(Real Time Publisher/Subscriber),其模型如图 3 所示。该模型建立在面向对象的基础上,这些对象可通过 API 被应用层调用。通信协议同时提供实时服务和非实时服务。实时通信服务建立在 RTPS 实时 P/S 模式和 TCP/IP 协议之上。非实时通信服务则基于 TCP/IP 协议,充分利用 IT 领域成熟技术,如 HTTP, FTP, SNMP, SMTP 等。

• Ethernet/IP[26]

Ethernet/IP 基于以太网 TCP(UDP)/IP 协议,支持周期和非周期的数据传输。采用 TCP 技术支持非周期的数据传输,对有时间要求和周期性要求的实时数据传输由 UDP 处理。Ethernet/IP 采用了交换式以太网技术,实时扩展基于 TCP/IP 之上附加的通用信息协议 CIP。CIP 针对 Ethernet/IP, ControlNet 以及 DeviceNet 等进行设计,网间通过 CIP 路由器传输数据包。CIP 工作在 TCP/IP 之上,目的在于提高设备间的互操作性,其控制部分用来实现实时 I/O 数据报文通信,信息部分用来实现非实时的信息交换。

• ProfiNet[28]

ProfiNet 在满足实时通信要求的同时还满足 Profibus 的标准通信,支持从现场层到工厂管理层通信的连续性。ProfiNet 通信协议提供了一个标准通信通道和两个实时通信通道。标准通信通道使用 TCP/IP 协议的非实时通信通道,响应时间在 100ms 左右,主要用于设备参数化、组态和读取诊断数据等,IT 标准服务如 HTTP, HTML, SNMP, DHCP 等均可使用。实时通道 RT 用于响应时间要求严格的高性能数据传输,RT 极大地减少了数据在通信栈中的处理时间,响应时间为 5ms~10ms。同步实时通道 IRT 用于对实时性要求更高的现场级通信中,以满足同步数据的高性能传输。ProfiNet 支持开放的、面向对象的通信,以对象的形式表示的 ProfiNet 组件根据对象协议交换数据。

### 3.2.2 硬实时工业以太网

软实时工业控制网络由于在 TCP(UDP)/IP 上进行实时调度,因此 TCP(UDP)/IP 本身特点会导致实时行为受限。硬实时工业控制网络直接在 MAC 层上使用中间件技术实现实时调度。其强调实时行为可决定性,但不强调同步性。工业应用有 ProfiNet IO, TCnet 以及 Vnet 等。

• ProfiNet IO[15,28]

基于以太网的 ProfiNet IO 用于分散式现场设备数据的输入和输出,其模型与 Profibus-DP 模型类似。图 4 描述了 ProfiNet IO 的通信方式,左边部分显示了使用面向连接 RPC 的 ProfiNet/CBA 的连接建立,右边部分显示了使用无连接 RPC 的 ProfiNet IO 的连接建立,中心部分显示了使用实时调度的周期和非周期的数据交换,通常是周期性数据交换。ProfiNet IO 含 3 种设备类型:IO 设备、IO 控制器以及 IO 监视器。与 ProfiNet 相同,在通信进行中,循环用户数据和事件触发中断通过实时通道传输,参数分配、组态或读取诊断信息通过基于 UDP/IP 的标准通道实现。

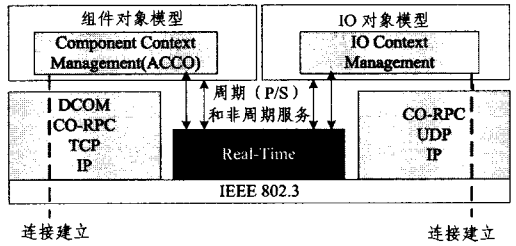


图 4 ProfiNet IO 通信方式

ProfiNet IO 提供了一种合理的实时和非实时数据传输机制,如图 5 所示,数据传输帧按周期发送,每个周期大小通过 $T_{Sendclock}$ 配置,周期范围一般在 31.25μs~4ms 之间,通常使用 1ms。数据传输顺序按如下优先级进行:周期实时数据 cRT,非周期实时数据 aRT,非实时数据 non RT。在传输周期开始时,首先发送用于 ProfiNet IO 应用服务实体的周期实

时数据 cRT，cRT 数据传输时间不超过周期带宽的 50%。接着，发送用于 IO 警告的非周期实时数据 aRT，aRT 数据传输不超过 10%。最后，发送用于 UDP/TCP 的非实时数据 non RT，占用了剩余 40%的带宽。ProfiNet IO 的这种实时传输机制可满足实时应用需求。

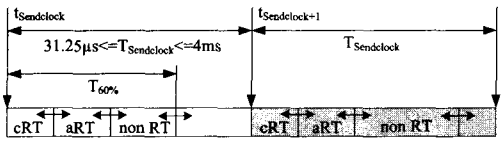


图 5　ProfiNet IO 数据帧传输机制

• TCnet[29]

TCnet 由东芝公司开发，其在 MAC 层上进行了实时扩展，也开发了标准通信通道和实时通信通道。TCnet 在应用层针对时间严格的应用定义了通用存储，在数据链路层扩展了调度功能。应用层包含了 3 种协议机：现场总线应用层服务协议机 FSPM、应用关系协议机 ARPM 以及数据链路映射协议机 DMPM。数据链路层的调度采用令牌传输机制，目标节点循环时间依赖于周期时间。在一个同步帧以后，广播所有节点，每个节点可在预设的时间内发送数据。

• Vnet[30]

Vnet 由横河公司开发，可支持最多 254 个子网，每个子网最多可由 254 个节点组成。该协议的实时扩展是实时可靠数据报协议，在传输层采用 UDP 协议，在 IP 层进行了优化以实现冗余网络连接。Vnet 的应用层也包含了 3 种类型的协议机：FSPM，ARPM 以及 DMPM。实时和非实时的调度在 MAC 上进行，数据链路层还进行时钟同步维护。

3.2.3　同步硬实时工业以太网

同步硬实时工业以太网为满足运动控制的要求设计了精确的时钟同步，其响应时间更短，为 250μs～1ms，抖动也更小，小于 1μs。其实时行为既强调可决定性，也强调同步性。工业应用有 EtherCAT，Powerlink 以及 SERCOS III 等。

• EtherCAT[31]

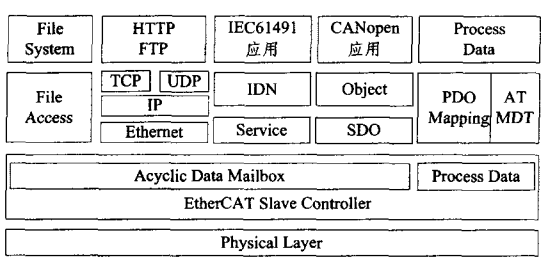


图 6　EtherCat 通信协议模型

EtherCAT 由德国 Backhoff 公司开发，用于现场级的超高速网络，使用了标准的以太网物理层和常规以太网卡。EtherCAT 采用基于 IEEE 1588 的时间同步机制以支持运动控制中的实时应用。EtherCAT 的通信协议模型如图 6 所示，定义了直接模式和开放模式。借助直接模式，在 EtherCAT 主站与 EtherCAT 网段之间使用了标准的以太网端口。使用开放模式，一个或多个 EtherCAT 网段可通过交换设备连接到一个或多个主站设备。EtherCAT 的应用层遵循 CANopen 模式，使用对象字典处理服务数据与过程数据。整个协议通过 EtherCAT 的状态机维护，EtherCAT 通过协议内部的优先权机制区别传输数据的优先权，使实时以太网数据比其他数据具有更高的优先级。非实时数据在实时数据传输的间隙通过专用的服务通道进行传输。

• Powerlink[32]

Powerlink 由奥地利 B&R 公司开发，目的是基于以太网建立现场总线系统，以满足运动控制中苛刻的实时要求。Powerlink 通信协议对 TCP(UDP)/IP 栈进行了实时扩展，增加了基于 TCP/IP 的异步中间件 Async 用于异步数据传输以及等时中间件 ISOchron 用于快速、周期的同步数据传输。Powerlink 在以太网网段上采用槽隙通信网络管理 SCNM 中间件，控制网络上的数据流量。SCNM 采用主从调度方式，每个站只有在收到主站请求的情况下才能发送实时数据。因此，在一个特定的时间，只有一个站能够访问，所以没有冲突，从而确保了通信的实时性。同时，Powerlink 采用 IEEE 1588 的时间同步。Powerlink 实时数据传输周期最小达 200μs，抖动小于 1μs。

• SERCOS III[33]

SERCOS III 是 SERCOS 接口的最新版本，使用了以太网作为传输机制，将现有的 SERCOS 接口连接到了以太网的高速带宽上，在精确时间模式下依据循环数据转化原则连续作业。SERCOS III 使标准 IP 报文在非实时的时隙内传输，与运动控制所要求的实时数据传送并行移动，将确定的实时机制和诊断能力与在以太网中可利用的通用通信能力相结合，以满足运动控制的高实时特性。

### 3.3　实时异构网络

上述研究的工业以太网都基于局域网技术，而广域网在工业控制领域的使用也已展开了研究，类似于局域网中交换式以太网技术在广域网中亦可应用[16]。局域网和广域网在工业通信领域的应用，会导致工业通信中异构网络的产生。异构网络中存在运行在不同操作平台和通信协议下的不同制造商的产品和系统[17]。由于被控对象、测控装置等物理设备的地域分散性，以及控制与监控等任务对实时性的要求，工业控制内在需要一种分布式实时控制系统，以实现异构网络中的信息实时传输与控制。实时异构网络是将来的发展趋势，具有不同层次的实时行为。自动化领域最重要的需求是保证数据包的响应时间，研究的重点是针对数据包传输的响应行为如何保证其服务质量 QoS 等。

## 4　无线网络

无线通信技术逐渐进入工业控制网络领域，为工业控制带来了诸如降低安装复杂度以及减少线缆等好处，同时其配置灵活，使用方便[5]。目前，无线通信在工业自动化领域的研究主要有以下几类：无线总线 RFieldbus、无线传感器与执行器网络 WSAN、基于 IEEE 802.11 的无线局域网 WLAN 以及基于 IEEE 802.15 的无线个域网 WPAN 等[12,34]。较流行的是欧洲 RFieldbus(RadioFieldbus)计划。RFieldbus 需要额外的协议机制来支持工业通信中实时和非实时传输的调度。基于 RFieldbus 计划的无线总线主要有无线 Profibus、无线 FF、无线 HART 以及无线 I/O 等。用于工业控制的无线网

络的发展趋势是，在无线技术本身发展的同时考虑工业通信的特点以满足每个个体工作站的实时需求，未来研究领域包括无线网络的安全性、可靠性以及实时传输的效率等。

## 5 未来发展方向

工业控制网络的发展历经了从传统控制网络到现场总线，再到目前广泛研究的工业以太网以及无线网络的过程。以太网的广泛使用为工业控制的发展提供了良好的基础结构，但如何保证工业通信的实时性是研究的关键。本文综述了目前广泛研究的工业通信网络，并对工业以太网的实时性进行了深入研究。笔者就工业控制网络未来发展的一些技术难题及相关解决方法进行了总结，主要包括：

(1)提高通信的实时性

提高操作系统和交换技术以支持实时通信。操作系统基于优先级策略对非实时和实时传输提供多队列排队方式。交换技术支持高优先级的数据包接入到高优先级的端口，以便高优先级的数据包能够快速进入到传输队列。此外，可改善拓扑结构以提高实时性。其他研究方向还包括怎样提高在MAC层上的数据传输的调度方法等。

(2)提高通信的安全性

安全性意味着能预防危险，如系统故障、电磁干扰、高温辐射以及恶意攻击等因素所带来的威胁。IEC 61508针对安全通信提出了黑通道机制并制定了安全完整性等级SIL。提高工业通信的安全性，以满足SIL高级别的要求，是工业控制网络安全性发展的趋势。目前一些总线研究机构基于黑通道原理针对数据破坏、丢失、时延以及非法访问等错误采用了数据编号、密码授权以及CRC安全校验等安全保护措施，如Interbus Safety，Profisafe以及EtherCAT Safety等，这可作为工业控制网络安全性研究的参考。

(3)提高通信可靠性

工业控制网络基于不同的网络交换技术，需进行不同类型网络站点之间的通信，因此通信的可靠性显得尤为重要。研究方向之一在于设计虚拟自动化网络，以构筑深层防御系统。虚拟自动化网络中包含有不同的抽象层和可靠区域，可靠区域包括远程接入区域、局部生产操作区域以及自动设备区域等，重点在于可靠区域的设计。

(4)多总线集成

多总线并存且相互竞争的局面由来已久，在未来相当长的时间内这种局面还将继续。多总线集成协同完成工业控制任务，是未来发展的趋势。研究方向之一是通过使用代理机制，将单一总线系统中的设备映射到基于工业以太网的工业控制网络中。

(5)实时异构网络

无线通信进入工业控制领域的趋势无可置疑。通过有线网络与无线网络融合、广域网与局域网集成来构建实时异构网络，是未来发展的趋势。

## 参 考 文 献


[1] 凌志浩. 现场总线与工业以太网[M]. 北京：机械工业出版社，2006

[2] 王浩，吴中福，王平. 工业控制网络安全模型研究[J]. 计算机科学，2007，34(5)：96-98

[3] 冯冬芹，廖智军，金建祥，等. 基于以太网的工业控制网络实时通信模型研究[J]. 仪器仪表学报，2005，26(9)：891-894

[4] 沈青，桂卫华，杨铁军. 基于工业以太网的实时控制性能分析[J]. 计算机工程，2007，33(1)：233-235

[5] 于海斌，曾鹏，王忠锋，等. 分布式无线传感器网络通信协议研究[J]. 通信学报，2004，25(10)：102-110

[6] 潘月斗，许镇琳，杨堂勇，等. 一种基于CAN总线的机床数控系统接口设计研究[J]. 中国机械工程，2007，18(2)：178-182

[7] 胡毅，于东，李培楠，等. 基于现场总线的开放式数控系统的设计与实现[J]. 小型微型计算机系统，2008，29(9)：1745-1749

[8] Yu D, Hu Y, Xu X W, et al. An Open CNC System Based on Component Technology[J]. IEEE Transactions on Automation Science and Engineering, 2009, 6(2): 302-310

[9] Jonathan L. Process Automation Handbook: A Guide to Theory and Practice[M]. Springer Verlag, 2007

[10] Pantoni R P, Mossin E A, Donaires O S, et al. Configuration Management for Fieldbus Automation Systems[C]// IEEE International Symposium on Industrial Electronics. 2007: 1844-1848

[11] Valdés M D, Domínguez M á, Moure M J, et al. A Reconfigurable Communication Processor Compatible with Different Industrial Fieldbuses[C]// Lecture Notes in Computer Science. 2004, 3203: 1011-1016

[12] Neumann P. Communication in industrial automation - What is going on[J]. Control Engineering Practice, 2007, 15: 1332-1347

[13] Valckenaers P. Challenges of Next Generation Manufacturing Systems[R]. SoftSpez Final Report. 2004: 23-28

[14] Cuong D M, Kim M K. Real-time Communications on an Integrated Fieldbus Network Based on a Switched Ethernet in Industrial Environment[C]// 3th International Conference on Embedded Software and Systems. 2007: 498-509

[15] Jämsä-Jounela S L. Future trends in process automation[C]// Annual Reviews in Control. 2007, 31: 211-220

[16] Plesowicz P, Metzger M. Experimental Testing of TCP/IP/Ethernet Communication for Automatic Control[C]// International Federation for Information Processing. 2007: 260-275

[17] Loeser J, Haertig H. Low-latency hard real-time communication over switched Ethernet[C]// 16th EURI MICRO Conference on Real-time Systems. 2004: 13-22

[18] Song Y, Koubaa A, Simonot F. Switched Ethernet for real-time industrial communication: Modelling and message buffering delay evaluation[C]// 4th IEEE International Workshop on Factory Communication Systems. 2002: 27-35

[19] Hung M H, Tsai J, Cheng F T, et al. Development of an Ethernet-based equipment integration framework for factory automation[J]. Robotics and Computer-Integrated Manufacturing, 2004, 20: 369-383

[20] Hashim H, Haron Z A. A Study on Industrial Communication Networking: Ethernet Based Implementation[C]// International Conference on Intelligent and Advanced Systems. 2007: 1111-1114

[21] Decotignie J D. Ethernet-based Real-time and Industrial Communications[J]. Proceedings of the IEEE, 2005, 93(6): 1102-1117


(下转第46页)

抗原；2）当前的安全技术无法处理日益复杂的计算机威胁。人们希望从生物获取灵感的方法，如 AIS，以满足这些挑战。

本研究针对存储元数据，提出一种新颖的免疫存储异常检测方案来监控存储访问行为。经过分析和类比，AIS 模型能成功地适用于存储异常检测，其检测系统能识别合法的访问行为和各种异常行为。仿真结果揭示，本方案能达到较高的检测率和较低的误警率。开销测试表明 SADS 造成的性能损耗是可接受的。因此，存储异常检测将有助于增强存储系统的预警能力并提高存储系统的安全性。

## 参 考 文 献


[1] 舒继武. 网络存储安全[J]. 中国教育网络，2007(11)

[2] 莫宏伟. 人工免疫系统原理与应用[M]. 哈尔滨：哈尔滨工业大学出版社，2002

[3] Pennington A G, Strunk J D, Griffin J L, et al. Storage-based Intrusion Detection: Watching storage activity for suspicious behavior[C]// Proceedings of the 12th USENIX Security Symposium. 2003:137-151

[4] Gopal R K, Meher S K. A Rule-based Approach for Anomaly Detection in Subscriber Usage Patter[J]. Int. J. of Mathematical, Physical and Engineering Sciences, 2007, 1(3):171-174

[5] Qayyum A, Islam M H, Jamil M. Taxonomy of Statistical-based Anomaly Detection Techniques for Intrusion Detection[C]// Proceedings of the IEEE Conference on Emerging Technologies (ICET'05). 2005:270-276

[6] Durgin N A, Zhang P C. Profile-based Adaptive Anomaly Detection for Network Security[R]. SAND2005-7293. 2005

[7] Sekar R, Gupta A, et al. Specification-based anomaly detection: a new approach for detecting network intrusions[C]// 9th ACM Conference on Computer and Comm. Security. 2002:265-274

[8] Du Y, Wang H Q, Pang Y G. A Hidden Markov models-based Anomaly Intrusion Detection Method[C]// Proceeding of WICA'04. 2004:4348-4351

[9] De Castro L N, Von Zuben F J. Artificial Immune Systems: Part I-Basic Theory and Applications[R]. RT DCA 01/99. 1999:1-95

[10] Forrest S, Perelson A S, Allen L, et al. Self-nonself Discrimination in a Computer[C]// Proceedings of the 1994 IEEE Symposium on Security and Privacy. Los Alamitos, CA, 1994:202-212

[11] Kim J, Bentley P J. Towards an Artificial Immune System for Network Intrusion Detection: An Investigation of Dynamic Clonal Selection[C]// Proceeding of Congress on Evolutionary Computation. 2002:1015-1020

[12] Oda T, White T. Immunity from spam: An analysis of an Artificial Immune System for Junk Email Detection[C]// Proceeding of the 4th International Conference on Artificial Immune Systems (ICARIS'05). 2005:276-289

[13] Gonzalez F A. A study of artificial immune systems applied to anomaly detection[D]. the University of Memphis, 2003

[14] Huang J Z, Xie C S, Zhang C F, et al. Security Framework for Networked Storage System based on Artificial Immune System [C]// Proceeding of 5th MIPPR. Proc. SPIE. Vol. 6790, 2007

[15] Zadok E, Nieh J. FiST: A Language for Stackable File Systems [C]// Proceedings of the Annual USENIX Technical Conference. San Diego, CA, June 2000:55-70

[16] Balthrop J, Esponda F, Forrrest S, et al. Coverage and Generalization in an Artificial Immune System[C]// Proceedings of the Genetic and Evolutionary Computation Conference (GECCO'02). 2002:3-10

[17] Ji Z, Dasgupta D. Augmented negative selection algorithm with variable-coverage detectors[C]// Proceedings of 2004 Congress on Evolutionary Computation (CEC'04). 2004:1081-1088

[18] Ji Z, Dasgupta D. Applicability Issues of the Real-valued Negative Selection Algorithms[C]// Proceeding of Genetic and Evolutionary Computation Conference (GECCO'06). ACM Press, 2006:111-118


(上接第 27 页)


[22] Bello L L, Mirabella O, Raucea A. Design and Implementation of an Educational Testbed for Experiencing with Industrial Communication Networks[J]. IEEE Transactions on Industrial Electronics, 2007, 54(6):3122-3133

[23] Krommenacker N, Lecuire V. Building Industrial Communication Systems Based on IEEE 802.11g wireless technology[C]// IEEE Conference on Emerging Technologies and Factory Automation. 2005:71-78

[24] Haertig H, Loeser J. Using switched Ethernet for hard real-time communication[C]// International Conference on Parallel Computing in Electrical Engineering. 2004:349-353

[25] IEC 2004b. IEC65C/341/NP. Real - time Ethernet : Modbus - RTPS[S]. 2004

[26] IEC 2004c. IEC65C/361/NP. Real - time Ethernet: EtherNet / IP with time synchronization[S]. 2004

[27] Pantoni R P, Brandão D. Developing and implementing an open and non-proprietary device description for foundation fieldbus based on software standards[J]. Computer Standards & Interfaces, 2009, 31:504-514

[28] IEC 2004a. IEC65C/359/NP. Real - time Ethernet : ProfiNet IO [S]. 2004

[29] IEC 2004h. IEC65C/353/NP. Real - time Ethernet : TCnet [S]. 2004

[30] IEC 2004i. IEC65C/352/NP. Real-time Ethernet: Vnet/IP[S]. 2004

[31] IEC 2004g. IEC65C/355/NP. Real-time Ethernet: Ethercat[S]. 2004

[32] IEC 2004f. IEC65C/356/NP. Real - time Ethernet : Powerlink [S]. 2004

[33] IEC 2004e. IEC65C/358/NP. Real-time Ethernet: Sercos III[S]. 2004

[34] Miorandi D, Pitturi S. Hybridwired/wireless implementations of Profibus DP: A feasibility study based on Ethernet and Bluetooth[J]. Computer Communications, 2008, 27(10):946-960