

DOI:10.19431/j.cnki.1673-0062.2018.04.008

一种提高工业以太网通信可靠性的方法

文 杰¹, 鄢 锋²

(1.南华大学 电气工程学院,湖南 衡阳 421001;2.长沙有色冶金设计研究院有限公司,湖南 长沙 410011)

摘 要:为了保持 PLC 与嵌入式系统之间基于工业以太网系统的稳定性,设计一种基于心跳信号的工业以太网可靠性检测算法,并将其应用于 PLC 与嵌入式装置构建的自动化工业以太网中.通过这种方法在网络节点间传递包含心跳信号的报文,判断 PLC 与嵌入式系统在通信时是否存在数据报文丢失现象,并采取相应的措施,减少两者之间的丢包率提高工业以太网间服务和通信的可用性和可靠性;同时,还有效地降低了网络中单主站多从站工作模式下 PLC 的网络负担.

关键词:PLC;心跳信号;丢包率;工业以太网;嵌入式系统

中图分类号:TP273 **文献标志码:**B **文章编号:**1673-0062(2018)04-0047-07

A Method to Improve the Communication Reliability of Industrial Ethernet

WEN Jie¹, YAN Feng²

(1.School of Electrical Engineering, University of South China, Hengyang, Hunan 421001, China;

2.Changsha Engineering & Research Institute Ltd of Nonferrous Metallurgy,
Changsha, Hunan 410011, China)

Abstract: In order to maintain the stability of industrial Ethernet system between PLC and embedded system, an industrial Ethernet reliability Detection algorithm is designed, based on heartbeat, and is applied to automatic industrial Ethernet which is built by PLC and the embedded system. In this way, it transfers message containing heartbeat between network nodes, determines whether between PLC and the embedded system has data loss in communication, and takes steps to reduce the packet losses rate between PLC and the embedded system, improve the availability and the reliability of the industrial Ethernet service, meanwhile, effectively reduce the burden of PLC in the industrial Ethernet which contains a single master and multi-slavers.

key words: PLC; heartbeat; packet losses rate; industrial Ethernet; the embedded system

收稿日期:2018-03-01

作者简介:文 杰(1983-),男,讲师,硕士,主要从事机器人控制、工业总线通信、工业人系统控制优化的研究.

E-mail:wenjie412@126.com

0 引言

随着工业自动控制的不断发展,控制系统规模不断增大,而且被控对象、测控装置等物理设备具有地域分散性,传统的工业现场总线在成本、通信的速度、实时性与开放性上已经无法满足需求.因此,以太网技术开始直接应用于工业现场,但是标准以太网协议在传输的确定性、可靠性以及应用层协议的统一性上具有较大的缺陷.针对这些问题,西门子公司基于 PROFIBUS 国际组织提出了基于以太网的工业以太网标准 PROFINET^[1-2],开发了基于该标准的 PLC 产品.该产品通过改进了传统以太网技术采用带有冲突检测的载波侦听多路访问协议(CSMA/CD)以及二进制指数退避算法保证传输的确定性和可靠性,同时在应用层定义了统一的协议.目前,已经在国内经过了广泛的应用.但是,应用层的协议开放性不够,西门子公司 ProfiNet 网络对非西门子公司设备兼容性不好,其它嵌入式设备很难通过标准的 TCP/IP 协议与 ProfiNet 网络中的 PLC 通信.为解决这个问题,可以通过使用西门子公司基于工业以太网的 S5 协议中的 Fetch 和 Write 报文,实现对 PLC 中 RAM 的直接读写.但在实际使用中,发现数据在传输中掉包明显,急需一种算法解决这些问题.

心跳信号机制^[3]是收发心跳数据包(简称心跳包)的机制,心跳包是遵循心跳信号协议定义的、周期性、循环发送的数据包,用于判断各种网络节点是否“存活”,即是否还处于联网状态.在实际运行时,首先需保证各网络节点都支持基于心跳信号的网络协议,各网络节点按照心跳信号网络协议向其它网络节点发送心跳包,用于判断对方(设备、进程或其它网元)是否正常运行,如果在指定时间段内未收到对方响应,即没有收到对方发回的心跳包,则认为与对方的连接存在问题或者有数据包丢失的可能.目前,这种方法已经广泛被用于网络通信服务、网络平台的故障检测等相关领域^[4-5].

本文将心跳信号引入工业以太网通信中,一种基于心跳信号的工业以太网丢包检测方法.通过定义工业以太网节点状态、设计基于心跳信号网络数据包协议,建立心跳模型,心跳模型考虑在工业网络最常见的结构主从模式下,通过在主站节点和从站节点之间传递包含心跳信号数据报文,主站可以通过这些报文检测对方节点状态,以便在从站数据在发送时发生丢包时,能够及时发

现并及时采取相应的措施,保证工业以太网通信能够正确的传输数据包.考虑到主站与多个从站存在通信时,主站节点的网络负担相对繁重,故在主站节点和客户端节点设计不同的心跳包处理机制,以降低主站节点的网络负担.基于心跳信号的数据包协议具有很好的扩展性,所以该方法不但可以减少网络中的丢包问题,而且,通信传输的数据量小,可靠性高,监控端和被监控端之间不会产生无效发送数据的现象.最后,在西门子 PLC 与嵌入式测控装置构建的控制系统中,应用这种丢包检测方法,结果表明基于心跳信号的丢包检测方法具有很好的可用性和有效性.

1 丢包检测方法设计

基于心跳信号的丢包方法旨在让主从模式中主站获取从站发送的各个数据报文的状态,以保证通信服务正常工作.从站按照心跳机制发送包含心跳信号的数据报文,通过判断是否接收到一个相应数据包,来判断数据通信是否正常.一般情况下,主站没有按指定顺序收到从站心跳数据包则视为从站发送数据存在丢包情况,此时从站自动重发丢失的数据报文;主站在指定时间内没有收到从站心跳包则视为从站断开,并采取相应的措施.此外,如果丢包过高超过一定比率,从站也会被视为处于断开状态.从站继续与主站通信,需要同主站重新建立连接.

1.1 站点状态设计

为完成上述功能,首先为通信网络中的主站和从站定义 4 个状态:“通信中断”,表示未建立连接链路;“通信中...”,表示正在尝试/等待建立通信连接,或心跳数据包收发不正常;“通信正常”,表示链路正常,心跳包收发正常.“通信丢包”,表示从站发送数据存在丢包情况,主站与从站状态间的转换及对应的包含心跳标识符的数据包收发状况如图 1 所示.

由图 1 可知,当程序启动后,节点仍处于“通信中断”状态.当通信连接操作成功后,主站和从站的状态转换到“通信正常”状态,只有处于该状态的心跳信号数据包可以正常收发,同时,心跳信号数据包的正常收发也表示了该站点的连接正常、通信正常;当该站点处于通信正常状态时,检测该站点发送的心跳信号数据包存在丢包,该站点将转换成通信丢包状态,并重发丢失的报文,同时,该站点会统计自身的丢包率,如果丢包率过高就会进入“通信中...”状态,反之则会回到“通信

正常”状态.此外,一旦在规定时间内无法检测到来自该站点的心跳信号数据包,则将该站点状态转换到“通信中...”,停止心跳信号数据包的收发,断开连接链路,并尝试重新建立通信连接,此

时对方站点可通过建立连接的情况,判断该站点连接是否中断,若尝试连接失败则转换到“通信中断”状态,若尝试成功则转换到“通信正常”状态,继续收发心跳信号数据包.

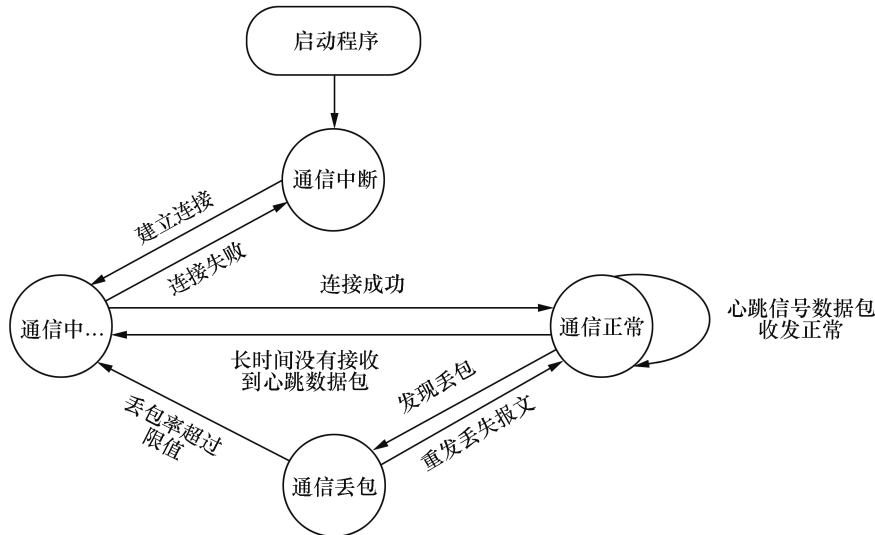


图 1 网络节点状态转换图

Fig.1 Transformation diagram of network nodes statues

1.2 基于心跳信号的丢包检测机制的设计

一般情况下,主站节点和从站节点采用相同的心跳机制,即某站点收到对方站点的心跳信号数据包后,返回一个对应的心跳信号数据包给对方站点,但现实情况中,一个控制网络往往只存在一个主站与多个从站.如按照心跳信号的传统模式,主站的心跳信号数据包发送量将是所有从站的心跳数据包发送量的总和.当从站节点过多时,主站的网络负担会十分繁重.在主站和从站设计不同的心跳信号传输机制,从而减轻主站的负担,提高网络效率.此外,心跳信号数据包的主动发包方既可以是从站,也可以是主站,但出于效率的考虑,一般由从站主动向主站发包.最后,为了能够检测从站发送到主站的包含多个测控数据的标准数据包中是否存在丢包现象,需将心跳信号直接加入标准数据包中,这样既可以帮助控制网络检测丢包问题,也减轻了控制网络的负担进一步提高效率^[6-8].

出于以上因素的考虑,可以设计心跳信号传输机制:从站主动向主站发送包含心跳信号的标准数据包,这些数据包中包含用于检测连接状态的测试数据,测试数据并不固定,每次发送心跳信号数据包时从一组数据序列循环地、顺序地选取

一位作为心跳信号;在从站的连续发送多个数据包后,主站才开始在这些接收到的心跳信号数据包中,根据心跳信号的顺序,检查是否在这些发生了丢包现象,否则,不做任何操作,继续接收下一个心跳包.当出现丢包现象时,主站将发送包含丢失报文心跳信号的报文.在这种心跳信号传输机制下,假定数据序列长度为 N ,主站收到来自客户端的 N 条心跳包后最多返回一个报文,那么主站的网络负担就减少到原有的 $1/N$.但数据序列长度过大,可能会造成丢包检测延时,影响到传输数据校验的有效性,所以数据序列的长度不宜过大.

1.3 数据包报文的设计

数据包的设计以西门子公司工业以太网协议 S5 中的 WRITE 报文和 FETCH 报文为基础,主站和从站在建立通信连接后,作为从站的嵌入式设备可以通过这两个报文用以太网直接访问作为主站的 PLC 内存块(包括 DB 块、M 模块等).这样主站就不需要编写专门的通信程序,使用方便. WRITE 报文是从站把采集到的现场数据通过以太网直接写入主站内存的报文,其主要由包头、报文长度、数据类型(DB 块、M 模块等)采样数据存放在主站内存中的起始地址和长度和采样数据区等组成.当主站接收到这种报文后返回一个报文,

用于通知从站 WRITE 报文发送成功, FETCH 报文是从站像主站询问在发送 N 个 WRITE 报文后是否存在丢包. 该报文主要包括包头、报文长度、数据类型(DB 块、M 模块等)丢包数据的心跳信号存放在主站内存中的起始地址和长度等. 当主站接收到报文后, 自动返回一个报文给从站, 从站根据返回的报文就可知是否存在丢包现象.

为满足通信实时性的要求, 数据包的大小应尽可能小, 以减少带宽的占用, 所以心跳信号直接被放入了 WRITE 报文的采样数据区中. 因此心跳信号数据包协议为:

包头	数据方向	站号	心跳信号位	包尾
----	------	----	-------	----

在该协议中: 包头、包尾均用 2 个字节; 数据方向用 1 个字节表示, 用于表示心跳信号数据包是主站发送给从站, 还是从站发送给主站; 站号多用于在从站向主站发送的心跳信号数据包中, 用

于表示从站的 ID, 这里用 2 个字节表示; 心跳信号位是用于检测连接的特定信息, 心跳信号位采用了一组序列数据, 这里采用数据序列 $0 \sim N$. 从站每次发送心跳信号数据包时, 循环地、顺序地选择序列中的一个数据作为测试位, 而主站仅在收到按顺序发送的 N 次包含特殊校验位的心跳信号数据包后, 检查发现丢包后返回一个心跳包, 其心跳信号位取值为丢失的心跳信号包所拥有的心跳信号. 该协议具有可扩展性, 可根据设计要求增减字段. 例如当需要考虑信息传输的安全性时, 可加入加密字段; 若考虑延时, 可增加时间戳字段等. 采用了以上的心跳机制后, 对于很小的延时, 仍可不定时间戳字段.

2 丢包检测流程的设计

在以上内容基础上, 基于心跳信号的丢包检测方法可按照如图 2 所示的流程实现.

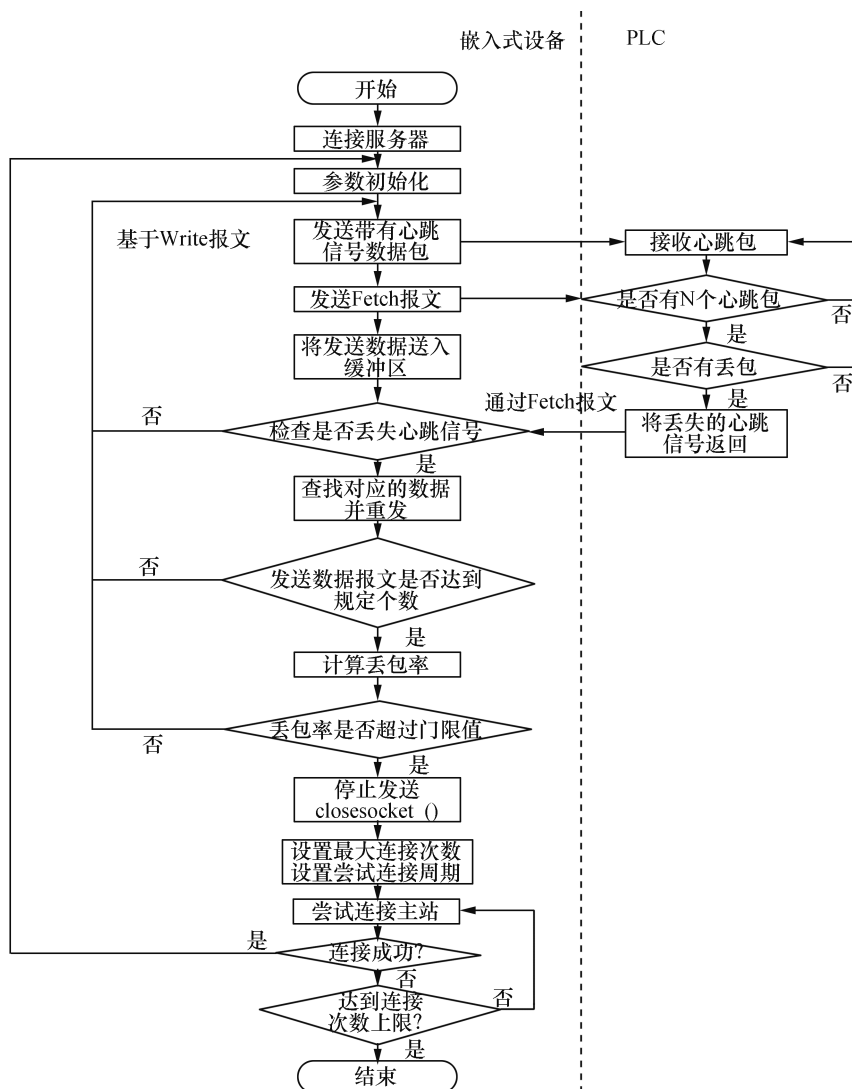


图 2 心跳模型实现流程图

Fig.2 Realization procedure of heartbeat model

首先,从站与主站建立连接后,初始化参数,主要包括以下几点:

1) 通讯连接借助于西门子公司的基于工业以太网的通讯协议 S5 完成.

2) 设置心跳信号数据包的发送周期.

3) 设置连接正常标志位.这里定义为一个 BOOL 型变量,初始值为 1,如果经校验后连接正常则置位,进行新一轮判断前,需要将其复位.

4) 设置心跳信号位数据序列.在模型的应用中采用的数据序列为 $0 \sim N$,发送心跳包时循环地、顺序地发送,当心跳信号位为 N 时,再发送的心跳信号位重新从 0 开始计数.

5) 设置重新连接主站的次数.当从站节点尝试连接服务器节点时,如果到达设定的连接次数时,仍没有成功连接主站节点,则认为连接彻底失败,服务结束.

6) 设置重新连接主站的周期.当从站节点尝试连接主站节点时,根据设置的周期值,周期性地连接主站.参数初始化完毕后,开始周期性地发送心跳信号数据包,一旦主站接收到的 N 条心跳信号数据包后,将检测是否存在丢包,如果有就返回一个校验数据包给从站,如果当从站重发的数据包,则认为连接正常;否则,认为连接出现问题,从站关闭通讯连接,并尝试重新连接主站;如果在指定的连接次数内连接成功,则继续进行数据的通

信,否则,则认为连接中断,并采取相应的应急措施,处理出现的问题.

3 丢包检测实现与测试

丢包检测方法主要应用于以西门子 PLC 作为核心构建的自动化控制网络中,具体结构如图 3 所示,如图所示,整个系统的主站有西门子的 PLC 组成,从站由多种嵌入式控制器构成.主站和从站之间通过工业以太网建立通信连接,这些嵌入式控制器是在现场进行实时控制时会产生大量的实时数据,PLC 主站可以通过工业以太网远程监测这些数据.PLC 与嵌入式控制器通信是通过基于以太网协议为基础的西门子公司的 S5 协议为基础,所以主站 PLC 需要在硬件组态时加入带有 FETCH 和 WRITE 功能的模块,同时建立 FETCH 和 WRITE 连接,其中连接类型设置成 TCP connection,同时设置好主站 IP 地址和端口号,但是不需要设置通信对方的 IP 和端口号.主站设置完成后,嵌入式控制器只需要作为传统以太网通信中的 client 与主站建立通信连接.嵌入式控制器实现以太网通信连接是借助于适用于嵌入式系统的 TCP/IP 协议栈 lwip 完成的.lwip 可以提供类似 PC 机网络通信编程使用的套接字(Socket)方式的 API,同时占用系统资源比较少,特别适合嵌入式系统的网络编程.

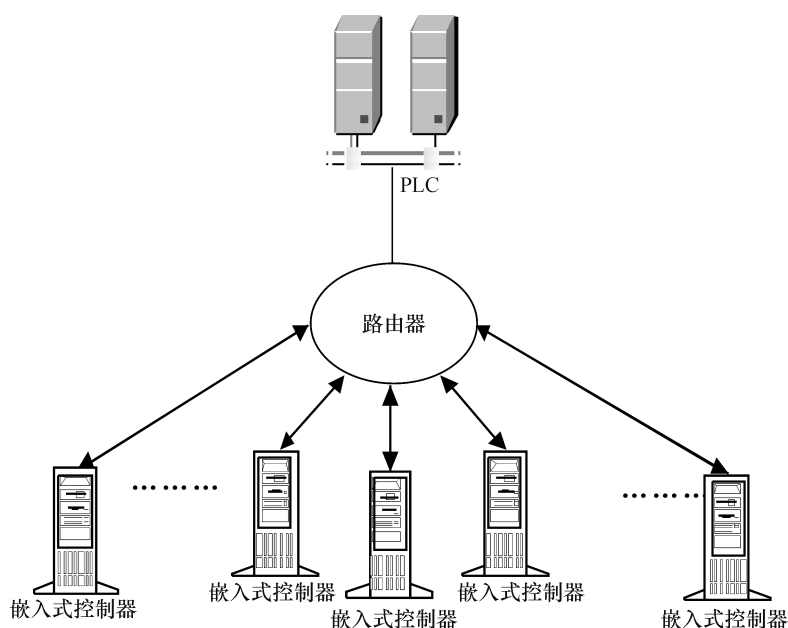


图 3 系统结构图

Fig.3 System structure diagram

通信连接建立后,嵌入式系统开始周期性地发送含有心跳信号的 Fetch 和 Write 报文给 PLC,同时将要传输给 PLC 的数据与对应的心跳信号存入预先划分好的缓冲区中,PLC 每接收到一个 Write 数据报文就将对应的心跳信号存入长度为 N 的 DB 块中,而当接收到第 N 个 Write 报文后,检查这 N 个数据对应的心跳信号是否都接收到,如果有就在 Fetch 报文的返回报文中的对应字节写入一个设定好的值表示正常,反之则把丢失的报文心跳信号写入,嵌入式系统接收到这个信号后,在缓冲区中查找到对应的数据重发给 PLC,当

完成整个数据序列的发送完,并存在丢包现象,嵌入式系统要检查丢包率,如果丢包率高于设定值,则嵌入式系统进行重连。

由于实验条件所限,为体现该方法的实际效果,用 VC 软件开发了一个测试系统模拟嵌入式设备的行为,并在 3 台 PC 应用该测试系统,自动化控制网络中作为从站的嵌入式设备由这些 pc 模拟,然后用一台西门子公司的 S7-300PLC 作为网络的主站,模拟不同网络条件,包括网络连接中、网络中断、网络丢包,并进行功能测试(如图 4 所示)。



图 4 模拟测试

Fig.4 Simulation test

测试过程表明,通过心跳包收发状态,心跳模型可以实现对网络连接状态的判断,并根据不同情况,在客户端和服务端采取相应的操作。心跳包状态、网络连接状态和采取的相应操作的对应关系如表 1 所示。测试结果表明,各状态与当前操作之间的关系符合模型的设计。

从表 1 看出,当从站节点发生丢包时,从站会从 FETCH 报文中检测到最近发送的 N 个 WRITE

报文中那个报文发送丢失,此时从站显示为通信丢包状态,如表 1 中第 5 条所示。经测试,在这种情况下,从站在重发丢失报文后,将继续正常通信,此时,从站显示状态将重新变为通信正常,如果丢包现象多次出现并超过了设定值,从站与主站以太网通信将会重连,此时,从站状态如表 1 中第 6 条所示将会回到通信中...状态。如果,重新连接不成功将会报警要求人工介入。由于连接 PLC

的工业以太网采用专用以太网络连接,经测试,作为主站的 S7-300PLC 很少出现网络连接中断的情况,所以这里认为 PLC 永远在线,一旦出现通信报文丢失过多现象,则认为工业以太网通信出现问题,PLC 将等待从站重新连接.

在完成基于心跳标识符的丢包功能测试系统的基础上,通过心跳标识符数据序列长度、最大重

连次数、尝试连接周期,以及通过启动和关闭各从站节点来模拟真实情况下的宕机和启动,对其进行连续 7×24 h 的实际使用,以测试其性能与可靠性.测试过程中,每次标识符状态的变化都会通过屏幕给予提示,结果表明,这种用于工业以太网的通信报文可靠性检测方法都能够正常的工作.

表 1 从站心跳信号状态与网络状态
Table1 Heartbeat of slave station and network status

序号	条件 1	条件 2	显示状态	当前操作
1	未建立连接		通信中断	
2	建立网络连接		通信中...	连接中
3	已建立网络连接		通信正常	
4	WRITE 报文收发正常	FETCH 报文收发正常	通信正常	发送包含心跳信号的 WRITE 报文
5	WRITE 报文发送正常	FETCH 接收报文中发现丢包	通信丢包	重发丢失报文
6	丢包次数超过限值		通信中...	开始重新连接
7	连接失败		通信中断	请求人工操作

4 结 论

基于心跳信号的丢包检测方法能够解决以西门子公司的 PLC 与嵌入式装置构建的自动化控制网络中存在的丢包问题.该方法以基于西门子工业以太网协议的 Write 报文和 Fetch 报文为基础,构建包含心跳信号的数据报文,采用的改进的包含心跳信号的报文不但能够准确的检测出从站在与主站通信时存在的丢包现象,在能够降低多从站情况下作为主站西门子 PLC 的网络负担,而且基于心跳信号模型的数据包协议具有很好的扩展性,所以该模型在工业以太网通信系统的应用中能具有很好的移植性和适用性.

参考文献:

[1] 张国栋,王有春.PROFINET 的实时性及其协议分析

[J].计算机测量与控制,2017,25(3):187-190.
[2] 李程.基于 PROFINET 协议的现场总线设备研究[D].青岛:青岛科技大学,2010.
[3] 鄢锋,桂卫华,胡志坤,等.一种网络节点通信控制的心跳模型[J].信息与控制,2008,37(5):525-528.
[4] 周奇才,张慧群,熊肖磊,等.基于 Socket 网络通信中 C#心跳包实现方法的研究田[J].机电一体化,2014,20(10):11-19.
[5] 郭兴吉,李淑珍,文永革.带心跳功能的连接池技术研究[J].现代计算机,2015(3):65-69.
[6] 文杰,阳小华,汪琳霞.心跳包在核电仪控网络安全设计中的研究[J].自动化仪表,2017,38(1):62-64.
[7] 文杰,汪琳霞,鄢锋.心跳包技术应用于高可靠工业网络中的研究[J].控制工程,2017,24(5):1048-1052.
[8] 鄢锋,桂卫华,胡志坤,等.基于 Socket 的整流装置远程监控系统[J].计算机工程.2008,34(5):243-245.
(责任编辑:扶文静)