

文章编号:1001-9081(2008)05-1123-02

用测试的方法确定计算机自动控制网络的结构

刘晓秋

(湖南涉外经济学院 计算机科学与技术学部,长沙 410205)
(lxq561025@163.com)

摘要:计算机自动控制网络的建立不同于互联网和局域网,在计算机自动控制网络的结构中,底层设备可能是计算机,也可能是智能模块。如何使这些设备在这种网络工程中构成一个整体尤为关键,唯一正确的方法是网络施工前经过有效的网络测试,在测试中保证主要部件和通信的一致性是这种方法的关键。

关键词:异地模式;本地模式;网络测试

中图分类号: TP39 **文献标志码:**A

Determination of computer automatic control network structure with test method

LIU Xiao-qiu

(Computer Science and Technical Department, Hunan International Economics University, Changsha Hunan 410205, China)

Abstract: The establishment of computer automatic control network is different with the Internet and the local area network. In the computer automatic control network structure, the lower level equipment might be the computer or the intelligent module. How to enable these equipments to constitute a whole in this kind of network project? The network test of process effective before the network construction is the only correct method, in which the congruence of the major components and the communication is the key.

Key words: different area pattern; local pattern; network test

0 引言

随着计算机的发展,在自动控制网络工程中利用计算机实施异地模式(本企业或本集团之外)、本地模式(本企业或本集团之内)控制是一个发展方向,在这样的网络工程中一般有自己独特的通信线路、网络通信协议、系统控制命令等。网络工程在实施中每个部分必须经过网络测试,在各种网络的测试中一般使用已有的专用测试设备与专用测试软件,但是在网络工程联调时常出现一些想不到的、非常难查的问题,有时还会出现使部分系统功能失效的事件,其产生的原因应该从系统的软件和硬件上进行考虑。

已有的专用网络测试设备和专用测试软件不等于实际中的网络设备和运行的实际网络控制软件,具体在软件上存在的差异主要表现在网络时序处理、控制、理解用户需求和网络功能上;在硬件上存在的差异主要表现在硬件的配合上、系统综合时间、系统结构上;另外还要注意网络层次、网络连线、网络节点对底层设备的影响等。

如何提高构网成功率、减少构网成本,经过多次研究和实际操作总结出一个较简单的方法。在经过专用的网络测试设备与网络测试软件操作后,一定要用自己独特的设备和方法对网络进行最后的测试。在构造网络的前期,这种再次测试是要加大人力、物力的投入,但对整个计算机自动控制网络工程来讲提高了可靠性,最终可以从计算机自动控制网络的经济效益中得到回报。

1 采取最后测试的要求

最后测试的原则是按将要构成的计算机控制网络进行通信,重要器件与在将要构成的计算机控制网络中使用设备的主

件完全一样。

方法是在理论上按图 1 的形式建立测试平台,手动操作,网络运行数据不用保存,但出现错误的状态操作等情况用手工形式进行详细记录。

由于计算机自动控制网络往往不能互换、通用,因此最后进行测试的设备、器件往往只能对应一个具体的计算机自动控制网络。要提高这种设备的通用性,必须加大资金的投入;增加设备自动处理功能,彻底改变人为因素的影响。

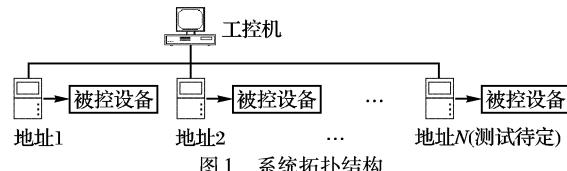


图 1 系统拓扑结构

下面以电信局动力、环境监控系统为例总结说明最后进行测试的优点与不足。

这是一个大工程,根据合同要求电信局提供监控点和监控任务并保证监控中心到监控点之间的专用光缆布线和联通,任务完成后通知施工方进行确认。

施工方按图 2 形式建立平台,测试人员由双方技术人员组成。首先测试光缆的状态是通或不通,其次测试通信数据是否正确无误,最后根据实测监控点使用环境确定被测点的设备配置。在正常情况下,线路的状态,设备的配置在测试现场就能确定。如果通信出现错误时现场就可分析错误产生的原因,错误方自己确定自己的纠错工作,因此没有必要将通信错误数据长期保存的必要,而是由此进入下一步工作。

这种测试方法很受用户与施工方欢迎,因为用户避免了盲目配置的问题,施工方避免盲目工程投入的情况,双方努力合作后如果没有一个满意的结果,将会有个强烈的行为出

收稿日期:2007-11-30;修回日期:2007-12-31。

作者简介:刘晓秋(1956-),男,湖南长沙人,工程师,主要研究方向:计算机应用及自控网络信息处理。

现。这也是为何要进行最后测试的原因。

测试现场最大的问题是操作不规范,人为影响因素较多。



图 2 实例测试框图

2 智能模块的设计

图 2 中测试设备可以是一台计算机,也可是一块智能模块,测试的成败在很大程度上由智能模块决定,因此智能模块的设计是前期测试工作的重心。由于计算机自动控制网络特点,智能模块的设计没有一个标准的设计方法和步骤,工程合同与用户的要求是智能模块的设计依据。

1) 智能模块的基本功能

微处理器和可编程器件以及外围硬件构成了智能模块(保证与实际网络中使用设备的主件一样),该智能模块中程序可使用符合要求的计算机语言编制,在测试中智能模块能接收计算机的命令并受控于上行计算机,智能模块响应计算机的命令后将完成相应工作,同时向上行计算机发送相应结果。

2) 智能模块的基本结构

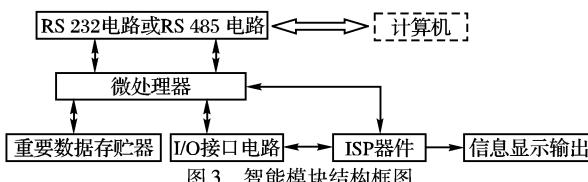


图 3 智能模块结构框图

3) 通信数据和命令的定义

命令类:所有命令均由计算机发出。被计算机访问的智能模块接收到命令经判别后向计算机发送判别信息(Ok 或 Error),智能模块在判断正确的情况下要完成相应的功能动作。计算机继续工作的条件是接收到 Error 或 OK 信息后。

命令分为工作命令和功能命令,具体定义如表 1。

表 1 命令定义表

命令名	属性	功 能	传 送 方 向	响 应 信 息
EA	工作命令	进入握手通	计算机	
		信工作状态	至智能模块	Ok 或 Error
EB	工作命令	进入拨号通	计算机	
		信工作状态	至智能模块	Ok 或 Error
EC	功能命令	定时	计算机	
		发送功能	至智能模块	Ok 或 Error
ED	功能命令	键盘输入	计算机	
		发送功能	至智能模块	Ok 或 Error

数据传输类:按数据流向分上行数据和下行数据。上行定义为智能模块向计算机发送数据,计算机处于接收状态;下行定义为计算机向智能模块发送数据,计算机处于发送状态。

如:下行时数据结构为 AL9N0102030405C,则可定义:A 为下行开始符;L10 为数据长度;N0102030405 为传送数据;C 为结束符。

如:上行时数据结构为 B0L9N987654321C,则可定义:B 为上行开始符;0 为定时中断数据发送计数器初值;L9 为数据长度;N987654321 为传送数据;C 为结束符。

地址码:智能模块的地址码由三位组成。第一位为 0,第二、三位按实际使用的智能模块数量用十进制顺次编排。在实际联机中,智能模块地址码可为:000~020。

3 应用程序的设计

1) 工程项目的建立

计算机上运行的应用程序控制智能模块,本例中应用程序使用 VC++6.0 中的单文档形式建立,对话框设计如图 4 所示,对话框标题设计人员可根据具体功能确定,本例为:模块通信测试程序。

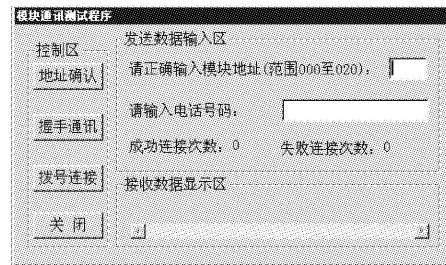


图 4 计算机通信对话框

2) 对通信控件 CMSComm 的主要属性设置如表 2:

表 2 CMSComm 常用属性设置

属性	值
InputLen	0(全部读取缓冲区数据)
InputMode	1(以二进制类型接收数据)
RThreshold	1(每接收一个字符就触发 OnComm 事件)
SThreshold	0(发送数据时不触发 OnComm 事件)

缓冲区 InBufferSize 和 OutBufferSize 的大小设置则根据现场使用情况来确定,其他可采用缺省值。

3) 控件对应的重要函数如表 3。

表 3 控件对应的变量和响应函数

变 量	函 数
IDC_BUTBH(拨号通信按键)	OnButbh()
IDC_BUTHAND(握手通信按键)	OnButhand()
IDC_SEND(地址确定按键)	OnButsend()

4 测试平台

计算机和智能模块间建立的联系是通过智能模块的地址码来实现,因此,智能模块核定地址码是其工作的关键,同时也是系统工作的基础。校验地址码可分为硬件校验和软件校验,本例的系统中采用软件校验的方法。

1) 不同的地点则有不同的结构

(1)本地模式:计算机与智能模块利用 RS485 专用网线组网,网络最远传输距离不大于 1 200 m。智能模块的地址码,设计人员根据现场实际使用智能模块的数量顺次编排并固化在微处理器中,以上无误后按图 5 连接。

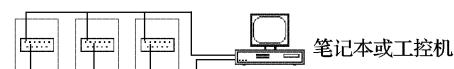


图 5 智能模块 485 端口与计算机连接图

(2)异地模式:计算机要访问一个智能模块,是通过“专线通信光缆方式”或“集团内部通信线路方式”访问智能模块(如图 2)。使用专线通信光缆方式时,直接在光缆两端的光电设备上取信号;使用集团内部通信线路方式时,通过内部交换机完成拨号访问。在“拨号方式”时与计算机连接的 Modem 设为开始端,与智能模块连接的 Modem 设为应答端。在测试时采用人工输入电话号码软件拨号,这样有利于统计

(下转第 1127 页)

以推出,这个消息 $\{MPARx_r\}K_{PA}$ 发生在申请者串 S_{peer} 的最后一个点上且 $C - height(S_{peer}) = 7$ 。

3.2 申请者认证

定理6 假定 C 是 IEEE 802.11i 串空间 Σ 中的一个丛; $P \neq R$; 且 $K_{SA}, K_{PA} \notin K_{pen}$ 。若 $s \in Peer[P, M, R, A, c_i, q_j, x_k, K_{PA}]$ 且 $C - height(S_{peer})$ 至少为7,则 C 中必然存在正常串:

1) $S_{auth} \in Auth[P, M, R, A, c_i, q_j, x_k, K_{PA}, K_{RA}]$ 且 $C - height(S_{auth})$ 至少为10。

2) $S_{radius} \in Radius[P, M, R, A, c_i, x_k, K_{RA}]$ 且 $C - height(S_{radius}) = 4$ 。

证明 串 $S_{peer} \in Peer[P, M, R, A, c_i, q_j, x_k, K_{PA}]$ 的迹表示为如下: $\langle + \{MAP\}, - \{MPAq_1\}K_{PA}, + \{MPAx_1\}K_{PA}, - \{MPARc_1\}K_{PA}, + \{MPARx_2\}K_{PA}, - \{MPARc_2\}K_{PA}, + \{MPARx_r\}K_{PA} \rangle$ 。

可以选取节点 $\{MPARc_r\}K_{PA}$ 与 $\{MPARc_r\}K_{RA}$,类似于定理3的证明,可以证明定理6成立。但是此处不能保证申请者最后发送的消息一定被认证者收到,因为攻击者,可以把信息窃取掉,所以我们这里假设申请者串的高度至少为6,而不是申请者串 S_{peer} 的实际高度7。

3.3 服务器认证

定理7 假定 C 是 IEEE 802.11i 串空间 Σ 中的一个丛; $P \neq R$; 且 $K_{RA}, K_{PA} \notin K_{pen}$ 。若 $s \in Radius[P, M, R, A, c_i, x_k, K_{RA}]$ 且 $C - height(S_{radius})$ 至少为3,则 C 中必然存在正常串:

1) $S_{peer} \in Peer[P, M, R, A, c_i, q_j, x_k, K_{PA}]$ 且 $C - height(S_{peer})$ 至少为5。

2) $S_{auth} \in Auth[P, M, R, A, c_i, q_j, x_k, K_{PA}, K_{RA}]$ 且 $C - height(S_{auth})$ 至少为8。

证明 串 $S_{radius} \in Radius[P, M, R, A, c_i, x_k, K_{RA}]$ 的迹表示为如下: $\langle - \{MPARx_1\}K_{RA}, + \{MPARc_1\}K_{RA}, - \{MPARx_2\}K_{RA}, + \{MPARc_r\}K_{RA} \rangle$ 。

选取节点 $\{MPARx_2\}K_{PA}$ 与 $\{MPARx_2\}K_{RA}$,类似定理3的证明,可以证明定理7成立。虽然此处,我们只能保证申请者的高度至少为5,但是从协议的执行过程,可以知道申请者在第五个节点正好发送完服务器挑战的响应信息,所以申请者串 S_{peer} 的

(上接第1124页)

通信时信号的中断率。拨号的方式现在使用的环境不多,但作为一种测试工具还是应该具有这样的功能。

2) 测试和测试结果最后决定网络结构

在双方人员共同参加的条件下完成的测试,现场即可直接决定网络的最后结构、智能模块的器件和网络其他硬件设备的选型,达成双方可接收的方案后现场的测试数据也失去保存的意义,而网络工程则进入下一个工作周期。在网络设计时,自控网络在具体现场的工作只能通过现场测试获得保证,决不能通过设计来确定。

3) 数据块的测试:

在智能模块的存储器中连续存入一定量的数据,目的是验证智能模块在不受计算机的控制下,向计算机发送数据块的能力。

如现有数据 BON: Hello! I'm very happy that you can work with us. Please check the input numbers carefully! Now the computer is in the condition of input and the intelligent modules of lower level equipment is output. Ok;

智能模块用循环的形式连续向计算机发送,测试人员对数据是已知的,计算机在接收到这个数据后不加任何处理就

高度至少为5,不会影响到服务器对申请者的认证。

4 结语

本文在文献[1]的基础上,对 IEEE802.11i 的串空间模块进行了修改,并从保密性与认证性两方面进行了分析。结果证明,在目前的攻击者模型中,IEEE 802.11i 协议是安全的。

参考文献:

- [1] FURQAN Z, MUHAMMAD S, GUHA R K. Formal verification of IEEE 802.11i using strand space formalism[C]// Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06). Washington, DC: IEEE Computer Society Press, 2006: 140–140.
- [2] THAYER F J, HERZOG J C, GUTTMAN J D. Strand spaces: why is a security protocol correct[C]// Proceedings of the 1998 IEEE Symposium on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1998: 160–171.
- [3] FABREGA F J T, HERZOG J C, GUTTMAN J D. Honest ideals on strand spaces[C]// Proceedings of the 11th IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 1998: 66–77.
- [4] CHEN J C, JIANG M C, LIU Y W. Wireless LAN security and IEEE 802.11i[J]. IEEE Wireless Communications, 2005, 12(1): 27–36.
- [5] SITHIRASENAN E, ZAFAR S, MUTHUKUMARASAMY V. Formal verification of the IEEE 802.11i WLAN security protocol[C]// Proceedings of the Australian Software Engineering Conference (ASWEC'06). Washington, DC: IEEE Computer Society Press, 2006: 181–190.
- [6] 刘璟,祝世雄,周明天. Yahalom 协议的串空间模型及分析[J]. 小型微型计算机系统,2006,27(5): 788–792.
- [7] MISHRA A, ARBAUGH W A. An initial security analysis of the IEEE 802.1x standard[EB/OL]. [2007-11-12]. http://www.ieee802.org/1/files/public/docs2000/ieee_plenary.pdf.
- [8] 卜凡金,邢育红. RSA-CEMD协议的分析及基于串空间模型的形式化证明[J]. 计算机工程与科学,2007,27(2): 12–15.

直接将其显示出来,这个数据块中只要有一个地方出错,测试人员即可知道。

5 结语

计算机通信对话框与部分程序在具体的自动控制网络中要根据情况进行符合要求的修改,用这种方法对网络进行测试确实可提高计算机自动控制网络在运行中的可靠性,减少构网成本。如何使智能模块具有好的通用性,是网络集成工程技术人员努力的方向。

参考文献:

- [1] 阮家栋. 计算机通讯技术[M]. 北京:电子工业出版社,2000.
- [2] 房小翠. 单片机实用系统设计技术[M]. 北京:国防工业出版社,1999.6.
- [3] 京辉热点工作室. 路设计实用指南[M]. 北京:人民邮电出版社,2000.
- [4] 龚荣武. 汇编语言程序设计[M]. 北京:科学出版社,2004.
- [5] 刘昌华. 层次化设计方法在数字电路设计中的应用[J]. 武汉工业学院学报,2004,23(4): 41–44.
- [6] 祖志华. 利用可编程器件实现点阵式 LED 显示[J]. 无线电工程,2006,36(8): 58–60.