WANGLUO XINXI

ANQUAN SHIXUN

网络信息安全实训

孙建国 编 著

北京邮电大学出版社
www.buptpress.com

网络信息安全实训

孙建国　编著

北京邮电大学出版社
www. buptpress. com

内 容 提 要

本书基于网络与信息安全创新实践训练，选择在大学生网络信息安全竞赛、大学生电子设计竞赛信息安全专题邀请赛获奖的作品，在基本的网络与信息安全实用技术和理论基础上，按照设计意义、关键技术、系统架构等环节，系统介绍网络与信息安全实际作品实际作品设计的完整流程。本书不仅介绍信息安全的基本理论和方法。通过作品设计意图、技术方案设计、实验验证等实际训练，学生可以系统掌握网络与信息安全创新训练的全部环节，掌握网络与信息安全的理论知识和理论结合实践的创新能力、实战能力。

本书取材新颖，采用完整案例教学的组织形式，内容由浅入深，循序渐进。书中给出了多个设计实例及技术方案，不仅可以作为教学内容进行学习，而且极具工程实践价值。本书可作为高等院校计算机类、电子类等有关专业的教材和参考书。

图书在版编目(CIP)数据

网络信息安全实训 / 孙建国编著. -- 北京：北京邮电大学出版社，2016.4
ISBN 978-7-5635-4731-9

Ⅰ.①网… Ⅱ.①孙… Ⅲ.①计算机网络—信息安全—安全技术—高等学校—教学参考资料 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2016)第 071966 号

书　　名：网络信息安全实训
著作责任者：孙建国　编著
责 任 编 辑：艾莉莎
出 版 发 行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京九州迅驰传媒文化有限公司印刷
开　　本：720 mm×1 000 mm　1/16
印　　张：9.75
字　　数：197 千字
版　　次：2016 年 4 月第 1 版　2016 年 4 月第 1 次印刷

ISBN 978-7-5635-4731-9　　定价：20.00 元

序

1. 写作背景

目前，关于我国高等教育的信息安全学科和专业方向设置问题受到非常大的关注。对于信息安全专业的本科生教育而言，其基本的培养方案、课程设置和教学大纲都需要根据新的形势发生变革，保密与信息安全专业方向也在积极地进行准备。

在新形势下，对于信息安全专业人才的培养标准是：具有宽厚的理工基础，掌握信息科学和管理科学专业基础知识，系统地掌握信息安全与保密专业知识，具有良好的学习能力、分析与解决问题能力、实践与创新能力。特别是在能力方面，要求专业学生能够做到：具有设计和开发信息安全与防范系统的基本能力，具有获取信息和运用知识解决实际问题的能力，具有良好的专业实践能力和基本的科研能力。

本教材的编写思路是：从网络与信息安全竞赛题目中，遴选出重点的课题内容，针对课题背景、关键技术、设计流程以及方案进行细致阐述，既满足于日常的实验教学活动，又能够促进学生创新实践能力的培养和提高。

这些实际竞赛题目不仅起到加深学生理论课所学知识的作用，还有助于培养学生建立理论与实践联系并在解决实际问题的能力。对于实现当前的高等教育改革目标，提高毕业生综合素质具有重要的意义。网络信息安全实训内容，是对计算机网络、现代密码学、信息系统安全、网络安全、软件安全、信息安全管理等专业核心课程的有效支撑。

2. 本书特点

本书兼顾高等学校理论教学需要与培养学生实践能力的需求，借鉴国外名校在信息安全专业课程设置及相关课程内容安排，组织本教程的相关理论知识及实验用例设计，力争理论详尽、用例科学、指导到位。配合高等学校的计算机网络、现代密码学、信息系统安全、网络安全、软件安全、信息安全管理等课程的实践教学环节，突出实用性，可操作性强，与实践结合紧密。

本书可作为信息安全专业及相关专业“计算机网络”、“现代密码学”、“信息系统安全”、“网络安全”、“信息安全管理”等课程的实践教材，书中的全部示例都经

过精心的设计和调试，可以放心使用。

3. 内容安排

本书的内容安排如下。

第1章介绍了一个无线数据通信安全防护系统，该作品荣获信息安全类比赛国家级二等奖。

第2章介绍了移动动态安防系统，该作品荣获软件类、信息安全类比赛国家级二等奖。

第3章介绍了文件实时监控销毁系统，该作品荣获了嵌入式类、信息安全类国家比赛二等奖。

第4章介绍了地理信息安全保障系统，该作品荣获了软件类、嵌入式类、信息安全类国家比赛多项大奖。

第5章介绍了视觉交互的ATM取款系统，该作品荣获了信息安全类国家比赛二等奖。

4. 致谢

首先感谢哈尔滨工程大学计算机科学与技术学院计算机实验教学中心的各位老师和研究生，感谢他们的大力支持和热情帮助。以下同学参与了本书实验示例代码的编写和调试以及原始资料的翻译和整理工作：董国忠、李丽、王亚卓、陈明涛、李玲、郝钟翁、周沫等，感谢他们付出的辛勤劳动。感谢张国印老师的热情帮助，作为本教材的主审。

感谢评阅专家对本书提出的宝贵修改意见，对于完善和提高全书质量起到了关键的作用。

编者虽然从事信息安全实践教学多年，但是由于水平所限，书中难免存在缺点和错误，诚恳地感谢各位读者提出宝贵意见，编者的联系方式为：sunjianguo@hrbeu.edu.cn。

作　者

目　录

第 1 章　ZigBee 通信安全防护系统

1.1　概　　述

随着社会信息产业的高速发展，网络通信、数据采集、无线通信、无线控制等技术受到了广泛的关注和应用。信息获取是信息技术应用的重要环节，同信息传输、处理和应用之间密不可分，具有标志性的作用。其中，传感器技术是信息获取的最重要和最基本的手段之一。特别地，ZigBee 无线传感器网络的应用使信息的获取变得更方便、快捷和准确。

ZigBee 是一种新兴的短距离、低速率无线网络技术，它拥有自己的无线电标准，得到了广泛的应用。无线传感器网络是基于 IEEE 802.15.4 技术标准和 ZigBee 网络协议而设计的无线数据传输网络，目前 ZigBee 无线传感器网络的应用主要集中于以下几个领域。

(1) 军事应用，通过布置于战场敏感区域的无线传感节点回传的信息，作战人员用手持式 PDA 等工具接收信息，就可以实时了解战场上的各种情况，真正做到运筹帷幄。

(2) 环境科学，传感器网络为野外随机的研究数据采集提供了方便。

(3) 医疗应用，在住院病人身上安装特殊用途的传感器节点，如心率和血压监测设备，利用传感器网络，医生就可以随时了解被监护病人的病情，及时进行处理。

(4) 商业应用，工业监控、楼宇自动化、流量过程控制、热能数据采集等。

无线传感网络在进行数据采集、融合和传输时，为了保证采集点的机密和数据传输的安全，与其他无线网络一样需要安全机制。由于节点单元能力的受限，以及无线传感网络节点的协作特性，必然要权衡安全强度的问题。无线传感器网络的中心节点网关收集的信息一般都是通过有线网络方式传输至控制中心，但在这过程中信息的传输存在很大的安全隐患，很容易被人窃取和篡改，因此，对这个有线传输网络的安全性保障就显得尤为重要，同时也必须对传输网络采取有效的安全检测。

加密是一种很好的信息安全解决方案，目前成熟的加密算法有 AES 加密算

法、混沌加密算法、RSA 加密算法等。AES 加密算法作为最新一代的加密标准，是一种数据块长度和密钥长度均可变的分组迭代加密算法，其数据块的长度和密钥长度可以分别是 128 位、192 位或 256 位。AES 加密算法具有安全、性能好、效率高、实用、灵活等特点，因此在信息安全领域具有广泛的应用。加密算法可以用软件和硬件实现，软件实现较为简单和灵活，但用硬件是实现能够提供更快的加解密速度和更好的安全性能。加密算法的硬件实现就是应用硬件描述语言对加密算法进行系统级设计及编码。

对网络的安全机制保障措施也较多，包括物理隔离、用户授权、防火墙技术等。目前的措施一般都是比较单一，基本的安全性能够得到保障。

针对信息通信过程中存在的信息泄露和安全隐患，结合 ZigBee 技术的应用领域，本书提出了可移动基于 FPGA 平台的高可靠通信系统的理论及模型，并对该系统进行了实现。本书的内容安排如下。

第 1 章：绪论，主要介绍系统的背景，目的及意义；第 2 章：系统的总体方案设计，介绍系统需求分析及相关支撑技术，详细介绍了系统总体设计过程；第 3 章：系统原理及实现，主要介绍系统中各部分的实现原理，重点介绍了 AES 加解密算法，详细介绍了具体实现技术及过程等；第 4 章：系统测试及分析，主要进行了 AES 加解密测试，网络安全监测和报警测试及相应的分析；第 5 章：总结及前景展望。

1.2 系统结构设计

1.2.1 问题的提出

在工业控制领域，利用 ZigBee 和传感器网络，使得数据的自动采集、分析和处理变得更加容易，作为决策辅助系统的重要组成部分，ZigBee 无线传感器网络在无线数据采集及监控等领域得到了广泛应用。这种网络主要是中短距离无线系统的连接，提供通用传感器的接入，能够满足各种传感器网络的数据输出和输入控制及信息需求，使系统网络化，无线化。无线传感器网络系统具有快速配置，自动识别及组网等显著特点。无线传感器数据采集都需通过网关传输至控制中心，在这个过程中信息传输的安全性逐渐成为人们关注的焦点。因此，设计一种安全可靠的通信解决方案显得尤为重要。

信息安全的解决方案目前主要集中于采取单一的措施来保证信息的安全性，针对各种攻击手段，防范措施主要集中于信息加密技术、安全交换机技术、防火墙技术、认证技术、入侵检测技术等，这些技术从不同的方面对安全性提供了较好的保障，但各有缺点和不足，这将成为网络防护的软肋，因此，本文也尝试性地提出了

一种集数据加密技术和访问控制策略于一体的信息安全解决方案。

1.2.2　AES 加密算法分析

AES 加密算法作为新一代的分组迭代加密算法，其采取对称密钥，数据块的分组长度和密钥长度分别可选择 128 位、192 位、256 位。AES 加密算法具有安全性，灵活性等特点。

RSA 算法是第一个能同时用于加密和数字签名的算法，也易于理解和操作。但 RSA 加密算法的缺点主要有：(1)密钥的产生烦琐，受到素数产生技术的限制，因而难以做到一次一密；(2)分组长度太大，为保证安全性，n 至少也要 600 bit 以上，使运算代价很高，尤其是速度较慢，与对称密码算法相差多个数量级；且随着大数分解技术的发展，这个长度还在增加，不利于数据格式的标准化。

混沌加密算法一般作为数字语音信息等的加密，在实际加密应用过程中其精度和保密性方面都存在着缺陷，因此，不适宜于该系统的加解密算法选择。

1.2.3　支撑硬件选择

鉴于 AES 加密算法的特点以及算法的抗攻击性能，因此，本文选用其作为加密应用技术。

加密算法可以通过软硬件实现，由于算法本身的灵活性，效率高，用软件实现比较简单、方便，但同时也带来一些问题，使算法的速度、安全性等都在某种程度上受到了影响。AES 算法的硬件实现不仅具有快的速度，而且占用的资源也将减少。因此，AES 加密算法硬件实现能够提供更快的速度和安全性。

采用 Spartan 系列 FPGA 作为 AES 加密算法实现的硬件载体。Spartan-3e 开发平台采用 50 万门的 XC3S500E-4FG320C 芯片，提供了 DDR SDRAM、Flash 和常用的扩展接口 10M 的网口、两个 RS232 串口、PS2 键盘接口、通用扩展接口等，能够支持 32 位的软核 MicroBlaze 的运用。因此，基于 Spartan-3e 平台能够很好地构建一个 SOC 系统。

1.3　系统总体设计

1.3.1　无线传感器网络

ZigBee 无线传感器网络是基于 IEEE 802.15.4 技术标准和 ZigBee 网络协议的无线数据传输网络，根据信息采集的需要，该系统采用星形网络结构。Chipcon 公司的 CC2430 是一颗真正基于 ZigBee 技术的 SOC CMOS 解决方案，它能够满

足以 ZigBee 为基础的 2.4 GHz ISM 波段的低成本和低功耗的无线传感器网络要求。因此，本文选择自行设计基于 CC2430 芯片的传感器采集终端。

ZigBee 无线传感器网络支持 ZigBee 网络协议，数据传输采用多层次握手方式，保证数据传输的准确可靠；无线传感器网络支持自动组网技术，最多可以支持多达 6 万多个无线采集节点，因此，根据具体的需要可以方便加入新的节点。在该系统中构建一个星型无线传感器网络，各个终端节点采集的信息通过中心节点网关上传至服务器端的 Spartan-3e 平台进行处理。

1.3.2 系统服务器端

服务器端采用 XILINX 公司的 Spartan-3e 开发平台，根据 XILINX 公司提供的设计开发工具，构建以 MicroBlaze 软核为处理器、Xilkernel 3.0 为操作系统的 FPGA 嵌入式平台。

MicroBlaze 软核处理器拥有 RISC 架构和哈佛结构的 32 位指令和数据总线，可以全速执行存储在片上存储器和外部存储器中的程序，并和其他外设 IP 核一起完成可编程系统芯片(SOPC)的设计。其内核结构如图 1-1 所示。

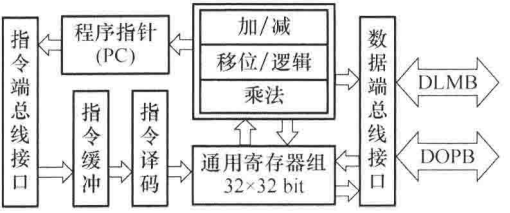

图 1-1 MicroBlaze 内核结构图

将服务器端作为 ZigBee 无线传感器星型网络的数据上传网关，Spartan-3e 开发平台的通用扩展接口外接 CC2430 无线模块，通过定制无线接口模块 IP，实现无线传感器网络和服务器端的信息交互。AES 加密算法具有灵活、效率高等特点，因此，AES 的硬件实现能够得到更快的速度和安全性，通过编写 VHDL 代码，从算法级实现 AES 加解密算法，并且根据输入自动选择加密还是解密操作。服务器端结构如图 1-2 所示。

1.3.3 系统客户端

客户端设计与服务器端相似，客户端作为该系统的主控中心，根据用户需要发送信息指令，指令包括自身唯一的 ID 和控制信息，指令经过 AES 加密后经网络传输至远程的服务器端。为了方便用户输入信息，该系统通过 PS2 口外接键盘，输入内容通过 LCD 液晶显示，为用户提供了很好的人机接口。其设计框图如图 1-3

所示。由于与服务器端理论基础相似，有关问题不在此赘述。

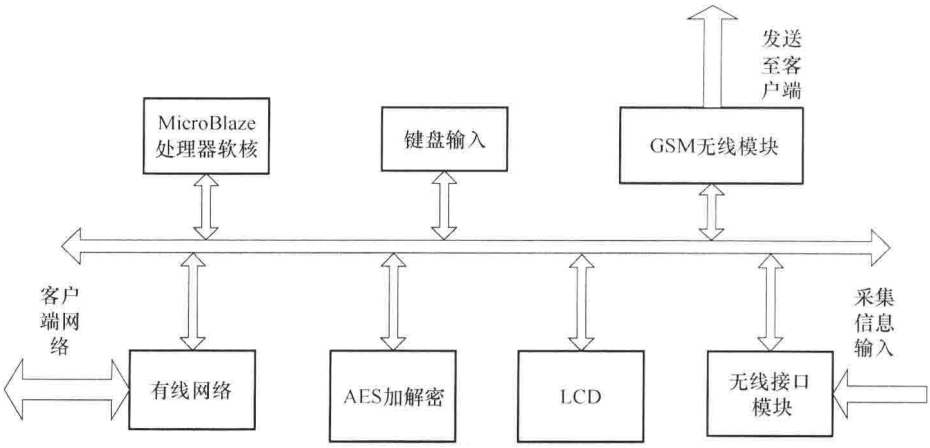

图 1-2　服务器端设计框图

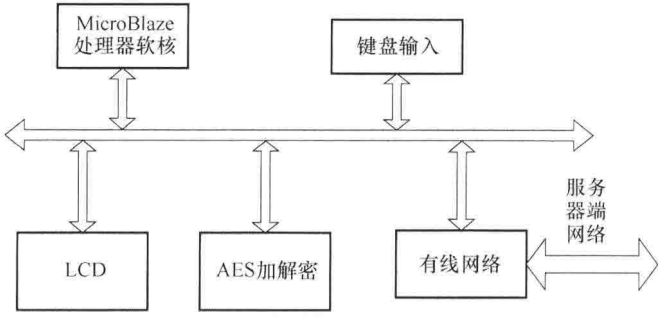

图 1-3　客户端设计框图

1.3.4　系统整体流程

本系统主要的目标在于“针对 ZigBee 无线传感器网络中，端到端控制过程中存在的安全隐患和信息邪路问题，自主设计了一套基于 FPGA 平台的高可靠通信系统”。该系统主要由 3 部分组成：ZigBee 无线传感器网络、服务器端、客户端。系统总体设计框图如图 1-4 所示。

服务器端采用 XILINX 公司的 Spartan-3e 开发平台，在该平台上构建基于 MicrBlaze 处理器和 Xilkernel 操作系统的嵌入式系统。当服务器端收到经过 AES 加密的请求 IP 数据包时，在服务器端，信息需要经过 AES 解密处理，根据解密后信息分析并提取请求方的 ID 信息和 IP 信息，客户端的 ID 信息是唯一的授权证号。

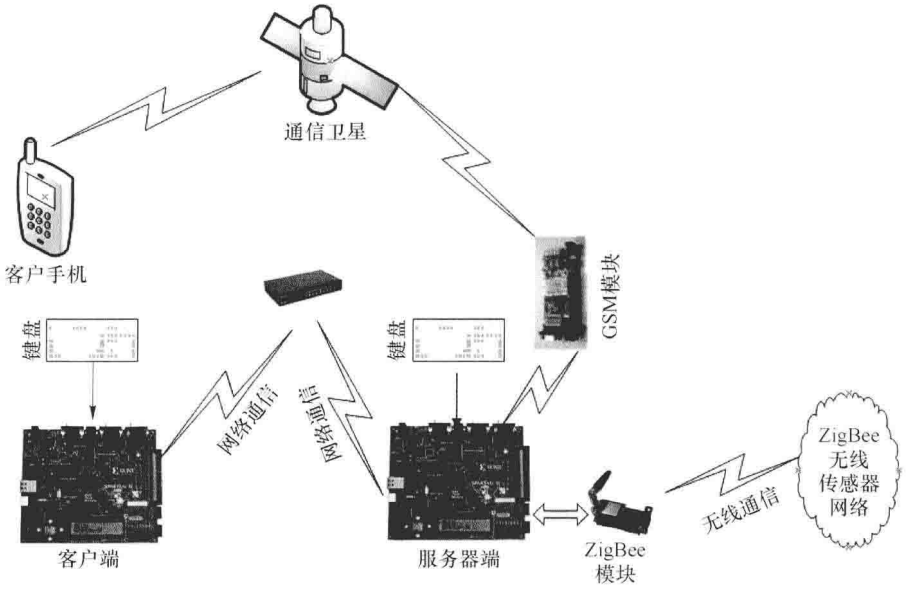

图 1-4　系统总体设计框图

客户端同样采用 XILINX 公司的 Spartan-3e 开发平台，但该系统中只需要定制 AES 加解密 IP、键盘 IP、LCD IP 并添加 EDK 中自带的网络控制器 IP。客户端作为整个系统的控制中心，当需要采集信息时，客户端通过键盘把自己的授权 ID 信息经 MD5 加密后形成自己的加密 ID，指令信息和加密 ID 信息经过 AES 加密后发送至服务器端，当服务器端响应其请求后，视其身份权限作出相应处理。

1.4　系统具体实现

1.4.1　ZigBee 无线传感器网络的实现

ZigBee 无线传感器基于 IEEE802.15.4 技术标准和 ZigBee 网络协议而设计的无线数据传输网路，该网络由若干个 ZigBee 终端节点和一个中心节点构成一个星型网络，终端节点主要负责各个传感器模块的信息采集和传送。中心节点主要用于接收各个终端节点的上传数据，并对其进行压缩处理后通过扩展接口传送至服务器端。如图 1-5，图 1-6 所示。

传感器模块采用 51 单片机控制，通过扩展串口与采集模块相连，其主要负责接收和处理采集数据。该系统中传感器采用的是数字温度传感器 DS18b20，该传感器的精度高，使用方便，传感器的采集数据经串口 ZigBee 模块发送。由于扩展

了 2 个串口，可以根据实际需要方便、快捷地扩展其他类型的传感器模块。

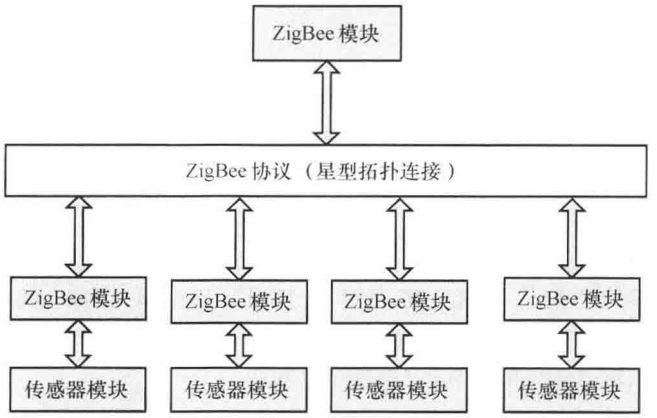

图 1-5　ZigBee 无线传感器网络拓扑结构图

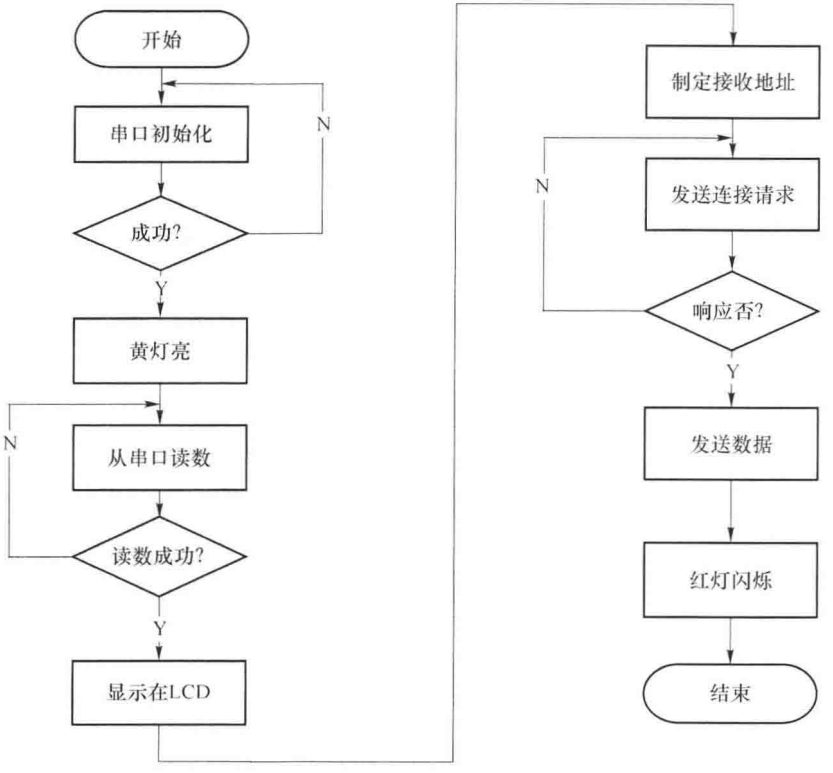

图 1-6　无线传感器网络终端节点软件流程图

1.4.2 系统服务器端实现

1. 接口模块

服务器端采用 Spartan-3e 平台扩展了 PS2 接口、16X2 的 LCD 液晶显示，3 个 6 针的通用扩展接口，这些接口方便了外设的连接和扩展。键盘在该系统中实现了单向通信。

LCD 液晶显示模块的控制器包括 3 个子模块：初始化模块、状态机模块、LCD 实现模块。LCD_RW 赋值为低电平，其余信号按照 LCD 时序进行设计。

无线接口模块通过平台通用扩展接口 J1、J2、J3 与 CC2430 模块进行信息交互，该模块作为无线传感器网络的中心网关节点，存储各终端节点的设备信息，负责终端节点的入网控制，终端节点信息的接收。

各个接口模块通过 EDK 添加自定义 IP 的方式添加到 OPB 总线中，其中键盘、LCD、串口 DTE 使用中断。驱动程序在自动生成的驱动程序模板基础上完成各个模块的驱动程序。

2. 监测及报警实现

服务器端通过添加 EDK 中网络控制器 IP 核，移植 LwIP 网络协议栈，实现基于 SOCKET 的网络通信。服务器端收到客户端请求时，对接收到的 IP 数据包进行解密，对请求的 IP 数据包进行分析，提取对应的 ID 信息和 IP 信息，由于该 ID 信息是经过 MD5 加密算法加密的，因此该 ID 作为授权客户的唯一 ID，根据 ID 信息与授权的 ID 列表进行比较，若为授权 ID，则根据客户请求把相应的信息加密处理后发送至客户端；若为非授权 ID，则说明该网络已存在非授权 ID 用户，此网络已经存在不安全性，则把提取的 IP 信息通过 GSM 网络发送至指定接收端手机，达到网络的实时检测和报警功能。网络安全监测及报警的软件设计流程图如图 1-7 所示。

3. 服务器端软件

服务器端构建基于 MicroBlaze 处理器和 Xilkernel 操作系统的嵌入式系统，通过扩展 PS2 键盘，LCD 液晶显示屏等设备，实现具有良好的人机交互接口的系统。Xilkernel 操作系统支持多线程操作，通过配置一些参数就可以灵活应用。虽然其没有网络系统，但可以通过移植 LwIP 协议栈就可以实现基于 socket 的网络通信。

当系统运行时，液晶显示相关信息，当出现等待键盘输入密钥时，输入 16 个字符密钥，同时对密钥进行密钥确认。系统调用 socket()函数创建 socket，调用 listen()函数开始监听。

一旦接收到用户请求时就创建 socket_process_thread 线程。在 socket_process_thread 线程中，提取 IP 数据包的相关信息，首先检查客户端发送的 ID 是否在授权 ID 列表之内，如果 ID 无误，将从无线模块接收到的数据进行 AES 加密，发送加密过后的数据给客户端。如果 ID 有错误，提取其收到 IP 数据包中的 IP，并启用 GSM 模块，将提得的 IP 通过短信发送给指定接收端。