[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/26 (2006.01)
H04L 29/08 (2006.01)
H02J 13/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200910184018.0

[43] 公开日 2010 年 1 月 6 日

[11] 公开号 CN 101621430A

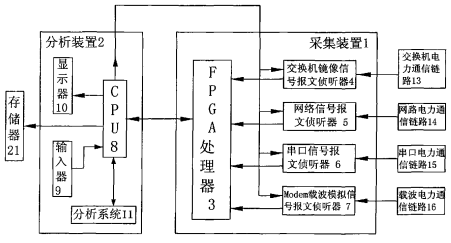
[22] 申请日 2009.7.31
[21] 申请号 200910184018.0
[71] 申请人 南京拓为电力科技发展有限公司
地址 210000 江苏省南京市玄武区后宰门佛心桥 37 号
共同申请人 绍兴电力局
绍兴电力设备成套公司
[72] 发明人 汪 彦 胡永春 程华明 朱重阳 黄飏鲲 张世平 金乃正 许伟国 王金岩 车浩军 安建锋
[74] 专利代理机构 南京苏科专利代理有限责任公司
代理人 闫 彪 何朝旭
权利要求书 6 页 说明书 18 页 附图 8 页

[54] 发明名称

便携式电力通信规约检测仪及其检测方法

[57] 摘要

本发明涉及一种便携式电力通信规约检测仪，同时涉及该检测仪的检测方法，属于电力系统通信检测技术领域。 该检测仪包括安置在一便携机箱内含有报文侦听器和并行转串行处理器的采集装置和含有 CPU、分析系统、分别与 CPU 连接的输入器和显示器的分析装置；报文侦听器输入端接入电力通信链路，其输出端并行连接于并行转串行处理器输入端；并行转串行处理器输出端串行连接于 CPU，报文侦听器和并行转串行处理器的控制端分别连接 CPU。 该检测方法在对该检测仪配置参数和系统文件后进行分析系统的初始化，然后将侦听到的电力通信链路的报文经过实时网络分析和规约分析后得出分析结果并显示。 本发明可以杜绝检测电力通信时丢失报文，从而对电力通信实现真正有效的检测。



1. 一种便携式电力通信规约检测仪,其特征在于：包括安置在一便携机箱内的采集装置和分析装置，所述采集装置含有报文侦听器和并行转串行处理器，所述分析装置含有 CPU、分析系统、分别与 CPU 连接的输入器和显示器；所述报文侦听器的输入端接入电力通信链路，其输出端并行连接于并行转串行处理器的输入端；所述并行转串行处理器的输出端串行连接于 CPU，所述报文侦听器和并行转串行处理器的控制端分别连接 CPU，所述分析系统含有用于从并行转串行处理器读取所述电力通信链路的报文的采集模块、用于对所述报文进行网络分析的网络分析模块、用于对经网络分析后的报文的应用层进行规约分析的规约分析模块和用于调度和管理所述模块的调度管理模块。

2. 根据权利要求 1 所述便携式电力通信规约检测仪，其特征在于：所述并行转串行处理器是 FPGA 处理器或多个协同工作的单片机。

3. 根据权利要求 2 所述便携式电力通信规约检测仪，其特征在于：所述报文侦听器是交换机端口镜像信号报文侦听器、网络信号报文侦听器、串口信号报文侦听器和 MODEM 载波信号报文侦听器之一，所述报文侦听器的输入端接入交换机通信链路、网络通信链路、串口电力通信链路和载波电力通信链路之一。

4. 根据权利要求 2 所述便携式电力通信规约检测仪，其特征在于：所述报文侦听器是交换机端口镜像信号报文侦听器、网络信号报文侦听器、串口信号报文侦听器和 MODEM 载波信号报文侦听器，该四个报文侦听器的各自输入端分别接入串口电力通信链路、交换机通信链路、网络通信链路和载波电力通信链路。

5. 根据权利要求 4 所述便携式电力通信规约检测仪，其特征在于：还包括存储器，所述分析系统还含有用于将采集模块读取的报文经过分析系统分析后传送至存储器存储的记录模块。

6. 根据权利要求 5 所述便携式电力通信规约检测仪，其特征在于：所述分析系统还含有用于对网络分析模块和规约分析模块产生的分析结果进行二次统计分析的统计分析模块。

7. 根据权利要求 6 所述便携式电力通信规约检测仪，其特征在于：所述 FPGA 处理器主要含有型号为 ALTERA EP3C25Q240 的芯片，该芯片通过千兆的以太网口连接 CPU；所述串口报文侦听器是分别提供 RS485、RS422 和 RS232 三种通信接口的三合一串口报文侦听器；所述 MODEM 载波信号报文侦听器含有用于侦听一路 MODEM 载波电力通信链路的二路 MODEM 载波接收接口，其二路接收接口分别并接到 MODEM 载波电力通信链路的一对收、发线上；所述 CPU 是型号为 MPC837 的嵌入式处理器。

8. 根据权利要求 7 所述便携式电力通信规约检测仪，其特征在于：所述输入器采用键盘、鼠标或触摸屏幕输入器，所述显示器是通用 CRT 或液晶显示器，所述存储器是通用 SSD 硬盘；所述报文侦听器的接口总带宽是 400Mbps；所述存储器的写盘速度为 640Mbps-800Mbps。

9. 一种根据权利要求 1 所述便携式电力通信规约检测仪的检测方法，其特征在于：包括以下步骤：

1）启动所述检测仪，通过所述输入器配置待检测电力通信链路的参数和特定规约关联指定并形成系统配置文件；

2）所述分析系统进行初始化，即所述 CPU 首先加载调度管理模块、网络分析模块和采集模块，所述调度管理模块依据所述系统配置文件再加载规约分析模块；

3）所述报文侦听器通过侦听电力通信链路的报文，并将该报文并行传送至并行转串行处理器，所述并行转串行处理器对并行接收来的报文加入时间戳，并将加入时间戳后的报文进行缓存；

4）所述采集模块从并行转串行处理器读取缓存的报文，并将该报文送入网络分析模块；

5）所述网络分析模块依据 OSI 模型各协议层语法和语义对送入网络分析模块的报文进行网络语法和语义分析直至该报文的应用层，并将应用层的报文送入规约分析模块，并将网络语法和语义分析结果送往显示界面；

6）所述规约分析模块依据规约的语法和语义对所述应用层的报文进行规约语法和语义分析，并将规约语法和语义分析结果送往显示界面。

10. 根据权利要求 9 所述便携式电力通信规约检测仪的检测方法，其特征在于：

----所述第 1）步中的特定规约关联指定是选择与待检测电力通信链路的特定规约相应的语法模型文件和语义模型文件；

----所述第 2）步中的规约分析模块是通过语法模型文件和语义模型文件形成特定规约的语法和语义环境并对该特定规约进行语法和语义分析的通用模块；加载规约分析模块是依据系统配置文件中指定的语法模型文件和语义模型文件进行初始化，即生成针对特定规约的协议层、语法分析器、会话通道管理器、语义分析器，随后将协议层组织为协议栈，接着为每个协议层配备相应的语法分析器和会话通道管理器，然后为每个会话通道管理器配置语义分析器；

----所述第 6）步中的规约语法和语义分析是，从所述协议栈的底层向上依次在每个协议层对所述应用层的报文使用语法分析器进行语法分析，并将获得的语法分析树传递给会话管理器，由会话管理器将

语法分析树分发给会话管理器接收和发送两端的语义分析器进行语义分析，语法分析器和语义分析器分别将剩余应用层的报文和语义分析结果向所述协议栈的上一层传递，由上一层再次进行上述过程，直到到达协议栈的顶端或报文结尾时，获得所述应用层报文的分析结果。

11.根据权利要求 9 所述便携式电力通信规约检测仪的检测方法，其特征在于:

----所述第 1）步中的关联指定是选择与待检测电力通信链路的特定规约相应的规约分析模块;

----所述第 2）步中的加载规约分析模块是依据系统配置文件中指定的与特定规约相应的规约分析模块；所述规约分析模块是通过程序设计形成特定规约的语法和语义环境并对特定规约进行语法与语义分析的非通用模块;

----所述第 6）步中的规约语法和语义分析是，所述应用层报文按照字节的 bit 位、字节的 bit 位组合、字节或字节组合形成单元报文结构，然后单元报文结构又组合成复合报文结构，再对所述报文结构之间的关系进行语法分析并形成语法分析结果，然后从语法分析结果中提取与上下文环境相关报文结构的值进行语义分析并形成语义分析结果，获得所述应用层报文的分析结果。

12. 根据权利要求 10 或 11 所述便携式电力通信规约检测仪的检测方法，其特征在于:

----所述第 2）步中的加载网络分析模块是，生成针对 OSI 模型的协议层、语法分析器、会话通道管理器、语义分析器，随后将协议层按照 OSI 七层模型组织为协议栈，接着为每个协议层配备相应的语法分析器和会话通道管理器，然后为每个会话通道管理器配置语义分析器;

----所述第 5）步中的网络语法和语义分析是，从所述协议栈的底层向上依次在每个协议层使用语法分析器对送入网络分析模块的报文进行语法分析，并将获得的语法分析树传递给会话管理器，由会话管理器将语法分析树分发给会话管理器接收和发送两端的语义分析器进行语义分析，语法分析器和语义分析器分别将剩余的报文和语义分析结果向所述协议栈的上一层传递，由上一层再次进行上述过程，直到到达协议栈的应用层、协议栈的顶端或报文结尾时，将应用层报文送入所述规约分析模块进行规约分析，同时获得对送入网络分析模块的报文的分析结果。

13.根据权利要求 12 所述便携式电力通信规约检测仪的检测方法，其特征在于：所述第 2）步中分析系统进行初始化时，还加载统计分析模块；还包括有第 7）步骤，所述网络分析模块和规约分析模块将分析结果送给统计分析模块进行统计分析，所述统计分析是将分析结果中的部分报文结构的值提取出来形成图表，在至少两帧报文后将提取出来的值进行运算和比较并形成统计结果，将统计结果送往显示界面。

14. 根据权利要求 13 所述便携式电力通信规约检测仪的检测方法，其特征在于：所述语法分析模型文件和语义分析模型文件是预设或现场通过输入器导入所述规约分析模块内。

15. 根据权利要求 14 所述便携式电力通信规约检测仪的检测方法，其特征在于：所述第 2）步中分析系统进行初始化时，还加载记录模块；所述步骤 4）中，所述记录模块将采集模块读取的报文经过分析系统分析后传送至存储器存储。

16. 根据权利要求 15 所述便携式电力通信规约检测仪的检测方法，其特征在于：所述调度管理模块依据所述系统配置文件对报文侦听器和并行转串行处理器的工作参数进行设置。

17. 根据权利要求 10 所述便携式电力通信规约检测仪的检测方法，其特征在于：所述通用模块是所述分析系统内部只有一个规约分析模块，不同的规约通过语法模型文件和语义模型文件来标识。

18 根据权利要求 11 所述便携式电力通信规约检测仪的检测方法，其特征在于：所述非通用模块是所述分析系统内部有多个规约分析模块，不同的规约由不同的规约分析模块来标识。

19. 根据权利要求 16 所述便携式电力通信规约检测仪的检测方法，其特征在于：当所述报文侦听器是非以太网电力通信链路报文侦听器时，首先产生一帧以太网 UDP 报文，然后将侦听的报文作为 UDP 报文的应用层。

便携式电力通信规约检测仪及其检测方法

技术领域

本发明涉及一种对电力系统通信及其过程进行实时检测的仪器，同时涉及该检测仪的检测方法，属于电力系统通信检测技术领域。

背景技术

当前电力系统已普遍采用自动化系统进行监视、控制和调度工作，如能量管理系统 EMS、变电站综合自动化系统 SCADA 等。这些系统的信息来源和控制都依赖网络通信，而且随着基于 IEC61850 通信体系的数字化变电站的实施和大面积推广，传统的通过电缆连接方式传递测控计量电流电压、断路器和隔离刀闸的控制联闭锁、继电保护跳合闸、启动、闭锁等信号，也已改为通过网络通信方式实现。因此，电力自动化系统的网络通信的正确传送就尤为重要。

通过近几年对电力自动化系统运行缺陷统计分析发现，因网络通信缺陷导致电力自动化系统运行异常呈上升趋势。这是由于：目前电力自动化系统中的各子系统往往采用多个厂家的不同产品，各厂家对通信规约的理解存在不一致，而且出于某些目的对规约进行修改和扩充的现象也非常普遍；各个厂家在通信规约的实现能力上参差不齐，导致在工程现场修改程序的现象比较平凡，使得产品缺乏足够严格的测试过程以保证通信的可靠性。据发明人所知，荷兰的 KEMA 咨询公司为国际上标准一致性测试权威机构，但其是实验室测试，无法在工程现场进行测试，也不具备系统健壮性测试，同时，其测试用例与工程现场也不完全一致，而且产品还有在工程现场修改的可能，因此，KEMA 的测试结果不足以保证通信的可靠性。

现有电力自动化系统在实际运行中的通信故障较多，这些通信故

障主要体现在以下几个方面：后台监控事故时动作事件记录不完整，保护测控装置因通信问题引起自复位，通信单元或后台监控功能异常或死机，调度和无人值班集控中心自动化系统收到的数据（报文）不全甚至全部丢失，遥测数据异常跃变，遥信数据异常变位，测控装置防误操作联闭锁故障以及计算机网络遭病毒攻击等等。由于缺乏有效的技术手段，目前维护人员往往只能对这些通信故障进行定性分析，因此不利于综合自动化系统的安全运行。

经检索发现，申请号 200610098252.8 的中国专利《通讯规约记录分析装置及其分析方法》公开了一种分体式通讯规约记录分析装置，该装置的主要技术方案是一个分布式结构，由分配在各个通信节点的通信记录仪和一个分析管理机组成，通信记录仪和分析管理机之间用单独的以太网连接；在规约记录仪中，串口接入模块、以太网接入模块、CAN 网接入模块、LONWORK 模块、GPS 模块的输出端分别与 CPU 模块的输入端连接，CPU 模块的输出端接装置异常输出模块、大容量存储模块的输入端，键盘显示模块与 CPU 模块相连接；规约记录装置的输出端接规约分析装置的输入端将记录的内容供规约分析管理机分析。该装置的分析方法主要步骤是：1）通信记录仪的通信记录模块根据通信配置文件对每个需要记录的通信端口的报文经捕捉，并每 10 分钟保存一个通信端口的原始通信报文，产生一个记录文件；2）通信记录仪的通信记录模块每产生一个记录文件后通知上行通信模块，上行通信模块将主动和分析管理机的下行通信模块通信，将该记录文件上传到分析管理机；3）分析管理机的下行通信模块在完整接收一个记录文件后依据通信配置文件对记录文件进行分类统一存储，此时并不对记录文件进行分析，而是等待用户的选择再进行分析；4）当用户选择分析某个通信端口的某个时间段的通信报文时，分析管理机在进行报文分析时利用通信配置文件取得相应的通信参数信息和规

约信息，自动调用相应的规约分析模块来分析记录文件，产生分析结果，并对分析结果经格式化显示；5）规约分析模块的分析方法是，依据规约中报文的格式从记录文件中读取原始报文，然后依据规约对原始报文按照字节和字节组合顺序进行分析，再依据规约对报文和报文之间的关系进行分析。

上述通讯规约记录分析装置及分析方法存在以下问题:

1）该装置的记录仪所述的各接入模块和存储器并行与 CPU 模块连接，众所周知，CPU 是串行工作方式，当多个接入模块同时高速传送报文到 CPU 模块时会造成报文丢失。同时 CPU 模块将多个接入模块传送来的报文传送给存储器进行报文存储，而存储器的数据吞吐量远小于接入模块的速率，又会造成存储时的报文丢失。一旦报文丢失，记录存储的报文就不完整，等出了故障后调阅这些不完整的报文进行分析时就会出错，甚至根本找不到报文产生故障的原因，从而无法进一步查找和排除相应的电网故障，进而造成较大的事故。

2）该装置中所述的某些模块（如 CAN 网接入模块、LONWORK 模块等）只有笼统的名词，没有相关的电路图和实现机制，不知道具体结构是什么，本领域技术人员无法依据专利文件进行制作。

3）该装置是分体式固定装置，需要在各输变电站综合自动化系统种布置多台，成本巨大，不便移动和携带。

4）该装置是先记录并存储各报文，等出了故障后再调阅存储的历史报文记录来分析报文故障原因，不能实时在线分析报文，难以快速及时地发现导致事故隐患的网络通信故障并找出故障原因，从而实际上对因隐藏的网络通信存在故障所导致的实时电网故障的排除和避免扩大无所作为。

5）该装置的分析管理机所述的分析方法描述模糊不清楚，该分析方法“依据规约对报文按照字节和字节组合顺序进行分析，再依据规约

对报文与报文之间的关系进行分析”，非常不全面，没有字节与字节或字节组合之间的关系、字节分支等等；没有环境关联分析、规约符合性分析等。其大部分内容为其所分析的对象和分析的结果，本领域技术人员难以按照该分析方法对记录的报文实现有效的分析。

发明内容

本发明要解决的技术问题是：提出一种真正能对现行电力自动化系统内的所有通信数据进行完整采集和分析的便携式电力通信规约检测仪及其检测方法；利用该检测仪及其检测方法应当能对电力自动化系统的所有报文进行完整采集并分析确定各报文故障的原因及报文故障的地点，从而方便维护人员及时排除与报文故障相应的电网故障和安全隐患，进而提高电力自动化系统运行的安全稳定性。

为了解决上述技术问题，本发明提出的技术方案之一是：一种便携式电力通信规约检测仪，包括安置在一便携机箱内的采集装置和分析装置，所述采集装置含有报文侦听器和并行转串行处理器，所述分析装置含有 CPU、分析系统、分别与 CPU 连接的输入器和显示器；所述报文侦听器的输入端接入电力通信链路，其输出端并行连接于并行转串行处理器的输入端；所述并行转串行处理器的输出端串行连接于 CPU，所述报文侦听器和并行转串行处理器的控制端分别连接 CPU，所述分析系统含有用于从并行转串行处理器读取所述电力通信链路的报文的采集模块、用于对所述报文进行网络分析的网络分析模块、用于对经网络分析后的报文的应用层进行规约分析的规约分析模块和用于调度和管理所述模块的调度管理模块。

实践表明，由于对电力通信规约的检测是完成对整个电力通信网络数据的侦听，故侦听网口必须工作在混杂模式下，即侦听网口要接受所有通过它的数据流，不管是什么格式，什么地址的。如果采用传统的 CPU 直接接收数据的方式进行设计，由于 CPU 对中断处理的限制，

在网络数据量较大，特别是小包大量传输的过程中，系统必然产生丢包，且数据包时标无法准确标记。而本发明的检测仪出乎意料地采用并行转串行处理器与各报文侦听器的输出端口并行连接，使得报文输入 CPU 之前得以缓冲；因此即使侦听的各通信链路报文流量很大，各报文在到达 CPU 之前也不会存在丢失的可能。同时，又由于本发明检测仪的报文是先经过规约分析模块进行实时规约分析后再存储，因此，即使存储速率较慢时丢失部分报文，也不会影响发现和分析报文故障。

为了解决上述技术问题，本发明提出的技术方案之二是：一种便携式电力通信规约检测仪的检测方法，包括以下步骤：

1）启动所述检测仪，通过所述输入器配置待检测电力通信链路的参数和特定规约关联指定并形成系统配置文件；

2）所述分析系统进行初始化，即所述 CPU 首先加载调度管理模块、网络分析模块和采集模块，所述调度管理模块依据所述系统配置文件再加载规约分析模块；

3）所述报文侦听器通过侦听电力通信链路的报文，并将该报文并行传送至并行转串行处理器，所述并行转串行处理器对并行接收来的报文加入时间戳，并将加入时间戳后的报文进行缓存；

4）所述采集模块从并行转串行处理器读取缓存的报文，并将该报文送入网络分析模块；

5）所述网络分析模块依据 OSI 模型各协议层语法和语义对送入网络分析模块的报文进行网络语法和语义分析直至该报文的应用层，并将应用层的报文送入规约分析模块，并将网络语法和语义分析结果送往显示界面；

6）所述规约分析模块依据规约的语法和语义对所述应用层的报文进行规约语法和语义分析，并将规约语法和语义分析结果送往显示

界面。

本发明的便携式电力通信规约检测仪按照上述检测方法可以在线实时检测多个待检测的电力通信链路，当发现报文故障后，可以第一时间发现通信故障原因和地点，为及时排除通信故障提供了可能，从而可以避免事故的进一步扩大，减少通信故障对电网正常运行带来的影响。

综上，本发明的便携式电力通信规约检测仪及其检测方法，不仅改变了现有通讯规约记录分析装置及其分析方法所采用的先记录后分析的状况，从而可以在线实时对各电力通信链路的报文进行分析，并及时捕捉报文故障；而且彻底解决了现有通讯规约记录分析装置存在的丢失报文的问题，从而真正实现对电力通信链路的报文进行完整有效的分析。

上述技术方案之一的改进是：所述并行转串行处理器是 FPGA 处理器或多个协同工作的单片机。

上述技术方案之一的进一步改进之一是：所述报文侦听器是交换机端口镜像信号报文侦听器、网络信号报文侦听器、串口信号报文侦听器和 MODEM 载波信号报文侦听器之一，所述报文侦听器的输入端接入交换机通信链路、网络通信链路、串口电力通信链路和载波电力通信链路之一。

上述技术方案之一的进一步改进之二是：所述报文侦听器是交换机端口镜像信号报文侦听器、网络信号报文侦听器、串口信号报文侦听器和 MODEM 载波信号报文侦听器，该四个报文侦听器的各自输入端分别接入串口电力通信链路、交换机通信链路、网络通信链路和载波电力通信链路。

上述技术方案之一的更进一步改进是：还包括存储器，所述分析系统还含有用于将采集模块读取的报文经过分析系统分析后传送至

存储器存储的记录模块。这样，在报文经过分析系统分析后对报文进行保存，以便在事故追忆和反演过程中提供宝贵的现场运行信息，可以起到举一反三的作用。

上述技术方案之一的再进一步改进是：所述分析系统还含有用于对网络分析模块和规约分析模块产生的分析结果进行二次统计分析的统计分析模块。这样，可以使分析结果更加直观化，并可以直观地观察到需要在长期监视并形成值序列后才能发现存在问题。

上述技术方案之一的又进一步改进是：所述 FPGA 处理器主要含有型号为 ALTERA EP3C25Q240 的芯片，该芯片通过千兆的以太网口连接 CPU；所述串口报文侦听器是分别提供 RS485、RS422 和 RS232 三种通信接口的三合一串口报文侦听器；所述 MODEM 载波信号报文侦听器含有用于侦听一路 MODEM 载波电力通信链路的二路 MODEM 载波接收接口，其二路接收接口分别并接到 MODEM 载波电力通信链路的一对收、发线上；所述 CPU 是型号为 MPC837 的嵌入式处理器。

上述技术方案之一的继续改进是：所述输入器采用键盘、鼠标或触摸屏幕输入器，所述显示器是通用 CRT 或液晶显示器，所述存储器是通用 SSD 硬盘；所述报文侦听器的接口总带宽是 400Mbps；所述存储器的写盘速度为 640Mbps-800Mbps。

上述技术方案之二的改进之一是：

----所述第 1）步中的特定规约关联指定是选择与待检测电力通信链路的特定规约相应的语法模型文件和语义模型文件；

----所述第 2）步中的规约分析模块是通过语法模型文件和语义模型文件形成特定规约的语法和语义环境并对该特定规约进行语法和语义分析的通用模块；加载规约分析模块是依据系统配置文件中指定的语法模型文件和语义模型文件进行初始化，即生成针对特定规约的协议层、语法分析器、会话通道管理器、语义分析器，随后将协议层组

织为协议栈，接着为每个协议层配备相应的语法分析器和会话通道管理器，然后为每个会话通道管理器配置语义分析器；

----所述第 6）步中的规约语法和语义分析是，从所述协议栈的底层向上依次在每个协议层对所述应用层的报文使用语法分析器进行语法分析，并将获得的语法分析树传递给会话管理器，由会话管理器将语法分析树分发给会话管理器接收和发送两端的语义分析器进行语义分析，语法分析器和语义分析器分别将剩余应用层的报文和语义分析结果向所述协议栈的上一层传递，由上一层再次进行上述过程，直到到达协议栈的顶端，获得所述应用层报文的分析结果。

上述技术方案之二的改进之二是：

----所述第 1）步中的关联指定是选择与待检测电力通信链路的特定规约相应的规约分析模块；

----所述第 2）步中的加载规约分析模块是依据系统配置文件中指定的与特定规约相应的规约分析模块；所述规约分析模块是通过程序设计形成特定规约的语法和语义环境并对特定规约进行语法与语义分析的非通用模块；

----所述第 6）步中的规约语法和语义分析是，所述应用层报文按照字节的 bit 位、字节的 bit 位组合、字节或字节组合形成单元报文结构，然后单元报文结构又组合成复合报文结构，再对所述报文结构之间的关系进行语法分析并形成语法分析结果，然后从语法分析结果中提取与上下文环境相关报文结构的值进行语义分析并形成语义分析结果，获得所述应用层报文的分析结果。

上述技术方案之二的进一步改进是：

----所述第 2）步中的加载网络分析模块是，生成针对 OSI 模型的协议层、语法分析器、会话通道管理器、语义分析器，随后将协议层按照 OSI 七层模型组织为协议栈，接着为每个协议层配备相应的语法分

析器和会话通道管理器，然后为每个会话通道管理器配置语义分析器；

----所述第 5）步中的网络语法和语义分析是，从所述协议栈的底层向上依次在每个协议层使用语法分析器对送入网络分析模块的报文进行语法分析，并将获得的语法分析树传递给会话管理器，由会话管理器将语法分析树分发给会话管理器接收和发送两端的语义分析器进行语义分析，语法分析器和语义分析器分别将剩余的报文和语义分析结果向所述协议栈的上一层传递，由上一层再次进行上述过程，直到到达协议栈的应用层，将应用层报文送入所述规约分析模块进行规约分析，同时获得对送入网络分析模块的报文的分析结果。

上述技术方案之二的更进一步改进是：所述第 2）步中分析系统进行初始化时，还加载统计分析模块；还包括有第 7）步骤，所述网络分析模块和规约分析模块将分析结果送给统计分析模块进行统计分析，所述统计分析是将分析结果中的部分报文结构的值提取出来形成图表，在至少两帧报文后将提取出来的值进行运算和比较并形成统计结果，将统计结果送往显示界面。这样，用户可以直观地观察到需要在长期监视并形成值序列后才能发现存在问题。

上述技术方案之二的再进一步改进是：所述语法分析模型文件和语义分析模型文件是预设或现场通过输入器导入所述规约分析模块内。

上述技术方案之二的又进一步改进是：所述第 2）步中分析系统进行初始化时，还加载记录模块；所述步骤 4）中，所述记录模块将采集模块读取的报文经过分析系统分析后传送至存储器存储。

上述技术方案之二的完善是：所述调度管理模块依据所述系统配置文件对报文侦听器和并行转串行处理器的工作参数进行设置。

附图说明

下面结合附图对本发明的便携式电力通信规约检测仪作进一步说明。

图 1 是本发明实施例便携式电力通信规约检测仪的结构框图。

图 2 是图 1 中控制系统的结构框图。

图 3 是图 1 中 FPGA 处理器的电路原理图之一。

图 4 是图 1 中 FPGA 处理器的电路原理图之二。

图 5 是图 1 中交换机端口镜像信号报文侦听器的电路原理图。

图 6 是图 1 中网络信号报文侦听器的电路原理图。

图 7 是图 1 中串口信号报文侦听器的电路原理图。

图 8 是图 1 中 MODEM 载波信号报文侦听器的电路原理图之一。

图 9 是图 1 中 MODEM 载波信号报文侦听器的电路原理图之二。

图 10 是本发明实施例便携式电力通信规约检测仪的检测方法的流程图。

具体实施方式

实施例一

本实施例的便携式电力通信规约检测仪如图 1 和图 2 所示，包括安置于一手持机箱内的采集装置 1 和分析装置 2。采集装置 1 含有报文侦听器和并行转串行处理器；其中，报文侦听器由交换机端口镜像信号报文侦听器 4、网络信号报文侦听器 5、串口信号报文侦听器 6 和 MODEM 载波信号报文侦听器 7 四个报文侦听器构成，并行转串行处理器由 FPGA 处理器 3 构成。分析装置含有 CPU8、分析系统 11、分别与 CPU8 连接的输入器 9 和显示器 10；其中，CPU8 采用嵌入式处理器（型号是 MPC8377），输入器 9 采用键盘、鼠标或触摸屏幕输入器等，显示器 10 采用通用 CRT 或液晶显示器。上述四个报文侦听器的各自输入端分别接入交换机通信链路 13、网络通信链路 14、串口电力通信链路 15 和载波电力通信链路 16，该四个报文侦听器的各自输出端

并行连接于 FPGA 处理器 3 的输入端。FPGA 处理器 3 的输出端通过千兆网口串行连接于 CPU8，上述四个报文侦听器和 FPGA 处理器 3 的各自控制端分别连接 CPU8。

由于上述四个报文侦听器的输出端分别并行连接于FPGA处理器3的输入端，四个报文侦听器的输出速率一般是十兆或百兆，FPGA 处理器 3 的千兆网口输出端速率远高于从四个报文侦听器输入的速率，加之四个报文侦听器传输的报文在 FPGA 处理器经过缓存后输出，因此可以保证四个报文侦听器所采集的所有报文能够完整传输给 CPU8 而不会丢失。

如图 2 所示，分析系统 11 含有：用于从 FPGA 处理器 3 读取电力通信链路的报文的采集模块 17、用于对采集的报文进行网络分析的网络分析模块 18、用于对经网络分析后的报文的应用层进行规约分析的规约分析模块 19 和用于负责各模块间的调度和管理的调度管理模块 20。

本实施例的便携式电力通信规约检测仪还包括连接 CPU8 的存储器 21，存储器 21 采用 SSD 硬盘（solid state disk 固态硬盘）。分析系统 11 还含有用于将采集模块 17 读取的报文经过分析系统分析后传送至存储器存储的记录模块 22、用于对网络分析模块 18 和规约分析模块 19 的分析结果进行统计分析的统计分析模块 23。

如图 3 和图 4 所示，FPGA 处理器 3 主要含有型号为 ALTERA EP3C25Q240 的芯片 U1，该芯片 U1 内将交换机端口镜像信号报文侦听器 4、网络信号报文侦听器 5、串口信号报文侦听器 6 和 MODEM 载波信号报文侦听器 7 四个报文侦听器采集到的数据在其内部进行处理后，通过千兆的以太网口传输给 CPU8，其中芯片 U1 的千兆网口是其在内部形成了一个千兆 MAC 软核。该千兆 MAC 软核再通过其 RGMII 接口（93 脚到 120 脚）先连接到芯片 U6（型号是 VSC8601）的千兆 PHY

上，在 PHY 上实现以太网物理层的转换，然后通过第一网络隔离变压器 T1 和第一双连 RJ45 接口 J1 的 A 端口（如图 5 所示）与 CPU8 相连实现物理链路上的连接。

交换机端口镜像信号报文侦听器 4 如图 5 所示，外部交换机的镜像端口（交换机通信链路 14）通过第一双连 RJ45 插座 J1 的 B 端口经第二网络隔离变压器 T2 连接到芯片 U5(型号 KS8721BL)的 100MPHY 上，在芯片 U5 上实现以太网物理层转换后将接收到的数据以标准的 RMII 口传送给 FPGA 处理器 3 进行处理。FPGA 处理器 3 在其内部的 BANK3 上实现一个 100M MAC，然后通过 RMII 口(芯片 U1 的 63-80 脚)与芯片 U5（如图 5 所示）的 PHY 对接。

网络报文侦听器如图 6 示，第二双连 RJ45 插座 J2 的 A、B 端口分别作为外部网络（网络通信链路 15）信号的输入、输出口，A、B 两端口在内部实现了物理上的直连，可以保证侦听时不对外部网络的正常通信造成破坏。外部网络的收发两路信号分别通过第三、第四网络隔离变压器 T3、T4 分别传送到两个芯片 U3 和 U4(型号 KS8721BL)的 100M PHY 上，在两个芯片 U3 和 U4 实现以太网物理层转换后，再通过 RMII 口传输给 FPGA 处理器 3 进行处理。FPGA 处理器 3 在其内部的 BANK1 和 BANK2 上实现两个 100M MAC，并分别通过 RMII 口(芯片 U1 得 4-22 脚和 38-57 脚)与两个 PHY 芯片 U3 和 U4（如图 6 示）实现对接。

如图 7 示，串口报文侦听器 6 是三合一串口报文侦听器，分别提供 RS485、RS422 和 RS232 三种通信接口，其主要功能是实现几种串行数字接口之间电平转化与驱动，并将接收到串口电力通信链路 13 的信号转化成统一 TTL 电平的 UART 信号送给 FPGA 处理器 3 进行处理。当需要侦听的串口电力通信链路 13 是 RS485 通信方式时，外部串口设备的 RS485 接口的 A（RX+）、B（RX-）分别并到芯片 U8、U9、U10

或 U14（型号 ADM485AR）的 6、7 两个引脚上。芯片 U8、U9、U10 或 U14 完成 RS485 电平到 TTL 电平转换后通过其上引脚 1 把接收到的数据输出到 FPGA 处理器 3 的串口数据接收端（芯片 U1 的 145、139、214、226 引脚上）；在 RS485 侦听模式下，串口报文侦听器 6 能同时侦听 4 路 RS485 串口。当需要侦听的串口电力通信链路 13 是 RS422 通信方式时，用两路 RS485 口去侦听一路外部目标 RS422 链路。一路 RS485 连接到外部目标 RS422 发送链路的 Y(TX+)、Z(TX-)两根线上，另一路 RS485 的连接到 RS422 接收链路的 A(RX+)、B(RX-)两根线上。当需要侦听的串口电力通信链路 13 是 RS232 通信方式时，串口报文侦听器 6 则用两路 RS232 接收来侦听一路外部目标 RS232 链路的收发两根线。外部目标 RS232 链路的接收端或者发送端并接到芯片 U11 或 U12、U13、U15（型号 SP3223EEY）的 16 引脚上，芯片 U11 或 U12、U13、U15 完成 RS232 电平到 TTL 电平转换后，通过其上 15 引脚把接收到的数据输出到 FPGA 处理器 3 的串口数据接收端（芯片 U1 的 144、142、216、230 引脚上）。

MODEM 载波信号报文侦听器 7 如图 8 和图 9 所示，MODEM 载波信号报文侦听器 7 提供二路 MODEM 载波接收接口，可用来侦听一路 MODEM 通信的目标链路（载波电力通信链路 16）。MODEM 载波信号报文侦听器 7 的两路接收接口分别并接到该目标链路的一对收、发线上。载波模拟信号通过第五、第六隔离变压器 T5、BT5 耦合输出到调制解调芯片 U16、U17（型号 MC145503）上进行解调，然后通过芯片 U18、U19（型号 74HC299）进行串并转换后，并行数据再送到单片机 U20、U21（型号 STC89c51Rc）上进行解码，解码后的数据通过单片机 U20、U21 上的各自 11 脚以 TTL 电平串行信号方式再传送给 FPGA 处理器 3 进行数据处理。

本实施例的便携式电力通信规约检测仪采用 FPGA 处理器 3 直接

在 MAC 层实现数据记录并缓存，并通过网线与 CPU8 进行数据交换，其中有三个重要的带宽指标，一是侦听接口的总带宽，二是硬盘的写盘速度，三是网线带宽。要实现完整有效检测，侦听接口的总带宽应小于硬盘写盘速度，网线带宽应大于侦听网口总带宽与硬盘写盘速度之和，并留有余度。本实施例检测仪设计的带宽指标是：每个报文侦听器的接口带宽是 100Mbps(网络风暴时)，则四个报文侦听器的接口总带宽=4 × 100Mbps=400Mbps;现在一般的 SSD 硬盘的写盘速度为 80MB/s-100MB/s，即 640Mbps-800Mbps;网线带宽是千兆带宽。由此可见，本实施例检测仪的设计带宽可以满足检测时不丢失数据的需求。

显然，上述本实施例的便携式电力通信规约检测仪可以精简和变化的方案有:1）交换机端口镜像信号报文侦听器 4、网络信号报文侦听器 5、串口信号报文侦听器 6 和 MODEM 载波信号报文侦听器 7 四个报文侦听器也可以只保留其中之一、之二或之三，或者再增加其他通信方式的报文侦听器; 2)FPGA 处理器 3 以及四个报文侦听器的具体电路构成不局限本实施例的电路结构; 3）FPGA 处理器 3 的输出端也可以通过 PCI 总线或其他连接方式与 CPU8 串行连接; 4）存储器 21 以及记录模块 22 也可以省去，本实施例的检测仪只进行实时检测分析而不记录; 5）FPGA 处理器 3 也可以由多个协同工作的单片机或其他并行转串行处理器代替。

本实施例的便携式电力通信规约检测仪的检测方法，如图 10 所示，包括以下步骤:

1）启动检测仪，通过输入器 9 配置待检测电力通信链路的参数和对特定规约进行关联指定并形成系统配置文件，

----特定关联指定是选择与待检测电力通信链路的特定规约相应的语法模型文件和语义模型文件，

----语法分析模型文件和语义分析模型文件通过预设或现场通过输

入器 9 导入检测仪内，

----调度管理模块 20 依据系统配置文件对交换机端口镜像信号报文侦听器 4、网络信号报文侦听器 5、串口信号报文侦听器 6 和 MODEM 载波信号报文侦听器 7 四个报文侦听器以及 FPGA 处理器 3 的工作参数进行设置;

2）分析系统进行初始化，即 CPU8 首先加载调度管理模块 20、网络分析模块 18 和采集模块 17、记录模块 22 和统计分析模块 23，调度管理模块 20 依据系统配置文件再加载规约分析模块 19，

----规约分析模块 19 是通过语法模型文件和语义模型文件形成特定规约的语法和语义环境并对该特定规约进行语法和语义分析的通用模块，即分析系统内部只有一个规约分析模块，不同的规约通过语法模型文件和语义模型文件来标识，

----加载网络分析模块 18 是，生成针对 OSI(Open System Interconnection 开放系统互联)模型的协议层、语法分析器、会话通道管理器、语义分析器，随后将协议层组织为协议栈，接着为每个协议层配备相应的语法分析器和会话通道管理器，然后为每个会话通道管理器配置语义分析器

----加载规约分析模块 19 是依据系统配置文件中指定的语法模型文件和语义模型文件进行初始化，即生成针对特定规约的协议层、语法分析器、会话通道管理器、语义分析器，随后将协议层组织为协议栈，接着为每个协议层配备相应的语法分析器和会话通道管理器，然后为每个会话通道管理器配置语义分析器;

3）交换机端口镜像信号报文侦听器 4、网络信号报文侦听器 5、串口信号报文侦听器 6 和 MODEM 载波信号报文侦听器 7 四个报文侦听器通过电力通信链路侦听电力通信链路的报文，其中串口信号报文侦听器 6 和 MODEM 载波信号报文侦听器 7（非以太网电力通信链路报文

侦听器）首先产生一帧以太网 UDP 报文，然后将侦听的报文作为 UDP 报文的应用层，接下来四个报文侦听器将直接侦听的以太网报文并行传送至 FPGA 处理器 3，FPGA 处理器 3 对并行接收来的报文加入时间戳，并将加入时间戳后的报文进行缓存，四个报文侦听器传送的报文分别进行缓存；

4）采集模块 17 从 FPGA 处理器 3 读取缓存的报文，并将该报文送入网络分析模块 18，采集模块 17 在该报文完成分析后将该报文送入纪录模块 22，记录模块 22 再将该报文传送至存储器 21 存储；

5）网络分析模块 18 依据 OSI 模型各协议层语法和语义对送入网络分析模块的报文进行网络语法和语义分析直至该报文的应用层，并将应用层的报文送入规约分析模块，

----网络语法和语义分析是，从协议栈的底层向上依次在每个协议层使用语法分析器对送入网络分析模块 18 的报文进行语法分析，并将获得的语法分析树传递给会话管理器，由会话管理器将语法分析树分发给会话管理器接收和发送两端的语义分析器进行语义分析，语法分析器和语义分析器分别将剩余应用层的报文和语义分析结果向协议栈的上一层传递，由上一层再次进行上述过程，直到到达协议栈的应用层、协议栈的顶端或报文结尾时）获得对送入网络分析模块 18 的报文的网络分析结果，

----将应用层报文送入规约分析模块 19 进行规约分析，将网络分析结果送入统计分析模块 23 进行统计并显示；

6）规约分析模块 19 依据规约的语法和语义对应用层的报文进行规约语法和语义分析，

----规约语法和语义分析是，从协议栈的底层向上依次在每个协议层对应用层的报文使用语法分析器进行语法分析，并将获得的语法分析树传递给会话管理器，由会话管理器将语法分析树分发给会话管理器

接收和发送两端的语义分析器进行语义分析，语法分析器和语义分析器分别将剩余应用层的报文和语义分析结果向所述协议栈的上一层传递，由上一层再次进行上述过程，直到到达协议栈的顶端或报文结尾时，获得应用层报文的规约分析结果，并将规约分析结果送往统计分析模块进行统计并显示，

7）网络分析模块 18 和规约分析模块 19 将各自的分析结果送给统计分析模块 23 进行统计分析，即将分析结果中的部分报文结构的值提取出来制成图表，在至少两帧报文后将提取出来的值进行运算和比较并形成统计结果，再将统计结果送往显示界面。

实施例二

本实施例的便携式电力通信规约检测仪与实施例一基本相同，所不同的是，FPGA 处理器 3 由多个协同工作的单片机代替。

本实施例的检测方法与实施例一稍有不同，除相同步骤以外所不同的是:

1、第 1）步中的特定关联指定是选择与待检测电力通信链路的特定规约相应的规约分析模块 19;

2、第 2）步中的规约分析模块 19 是通过程序设计形成特定规约的语法和语义环境并对特定规约进行语法与语义分析的非通用模块，即分析系统内部有多个规约分析模块，不同的规约由不同的规约分析模块来标识，

3、第 2）步中的加载规约分析模块 19 是依据系统配置文件中指定的与特定规约相应的规约分析模块;

4、第 6）步中的规约语法和语义分析是，应用层的报文按照字节的 bit 位、字节的 bit 位组合、字节或字节组合形成单元报文结构，然后单元报文结构又组合成复合报文结构，再对各报文结构之间关系进行语法分析并形成语法分析结果，然后从语法分析结果中提取与上下

文环境相关报文结构的值进行语义分析并形成语义分析结果，获得应用层报文的分析结果。

上述各实施例便携式电力通信规约检测仪的检测方法，既可以适用于在线实时分析，也可以适用于离线后的分析。当进行在线实时分析时，由于从 FPGA 处理器 3 传来的报文直接进行分析，因此可以第一时间发现并迅捷通过规约分析查找出报文故障原因和地点；同时由于报文是先经过规约分析模块 19 进行实时规约分析后再存储，因此，即使存储速率较慢时而丢失部分报文，也不会影响发现和分析报文故障。

总之，按照上述各实施例便携式电力通信规约检测仪及其检测方法，可以对现有各种电力通信链路的报文进行毫无遗漏地的检测，从而能够真正有效地检测出所有可能产生的报文故障及其原因和地点，进而为及时排除电力设施故障提供保障。

本发明的便携式电力通信规约检测仪及其检测方法不局限于上述实施例所述的具体技术方案，比如 1）规约分析模块的规约语法和语义分析也可以是将规约所有可能的报文组合以及所有可能的上下文环境进行罗列，然后将报文与所罗列的报文组合以及上下文环境进行比较来进行语法和语义分析；2）也可以将报文存储后再进行分析；3)非以太网电力通信链路报文侦听器(串口信号报文侦听器 6 和 MODEM 载波信号报文侦听器 7）的报文也可以不网络化；等等。凡采用等同替换形成的技术方案均为本发明要求的保护范围。

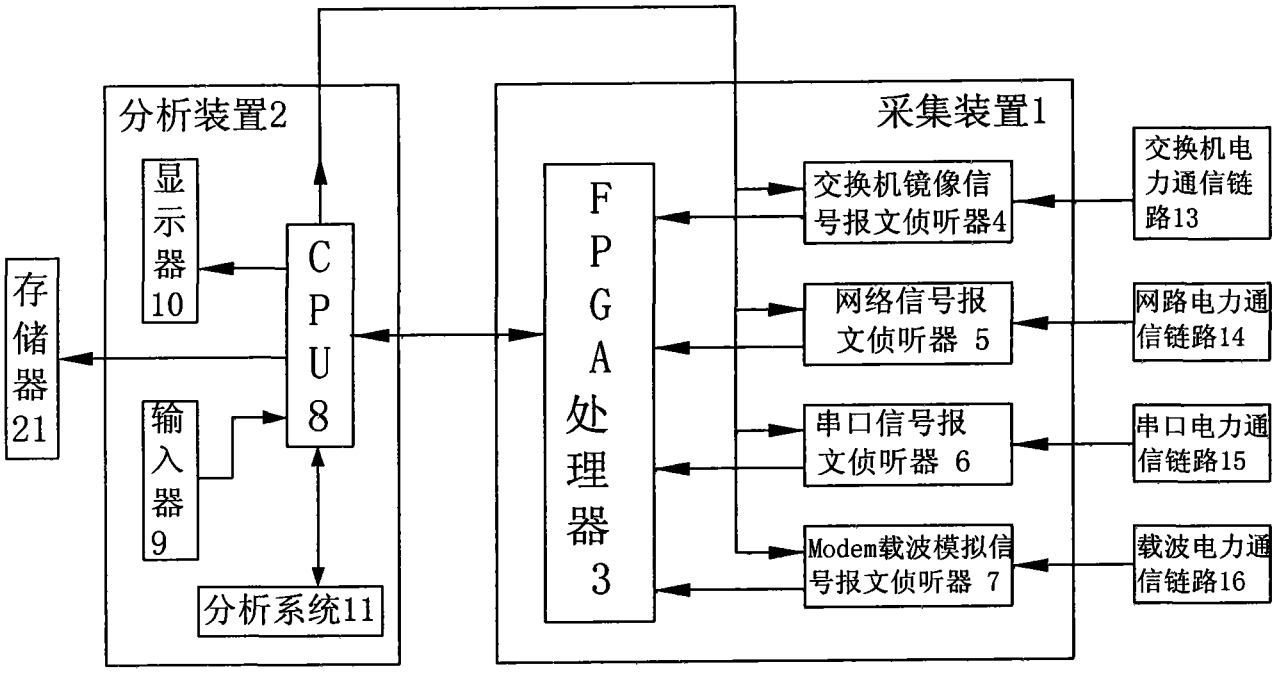

分析装置2
显示器10
CPU8
存储器21
输入器9
分析系统11
采集装置1
FPGA处理器3
交换机镜像信号报文侦听器4
网络信号报文侦听器 5
串口信号报文侦听器 6
Modem载波模拟信号报文侦听器 7
交换机电力通信链路13
网路电力通信链路14
串口电力通信链路15
载波电力通信链路16

图 1

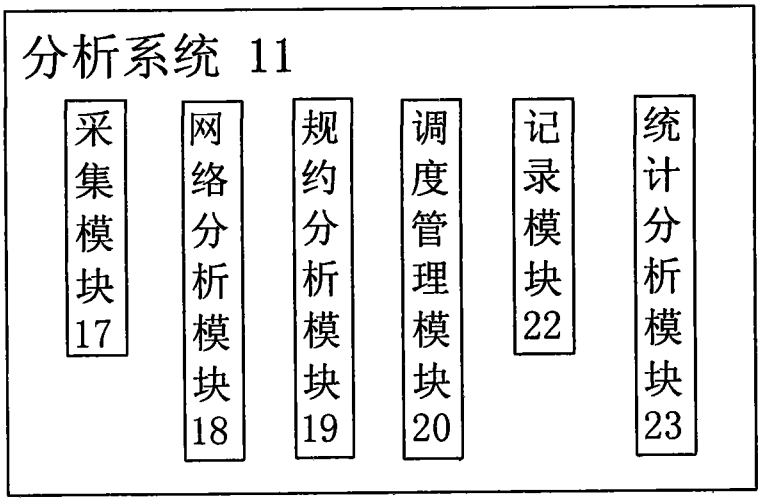

分析系统 11
采集模块17
网络分析模块18
规约分析模块19
调度管理模块20
记录模块22
统计分析模块23

图 2

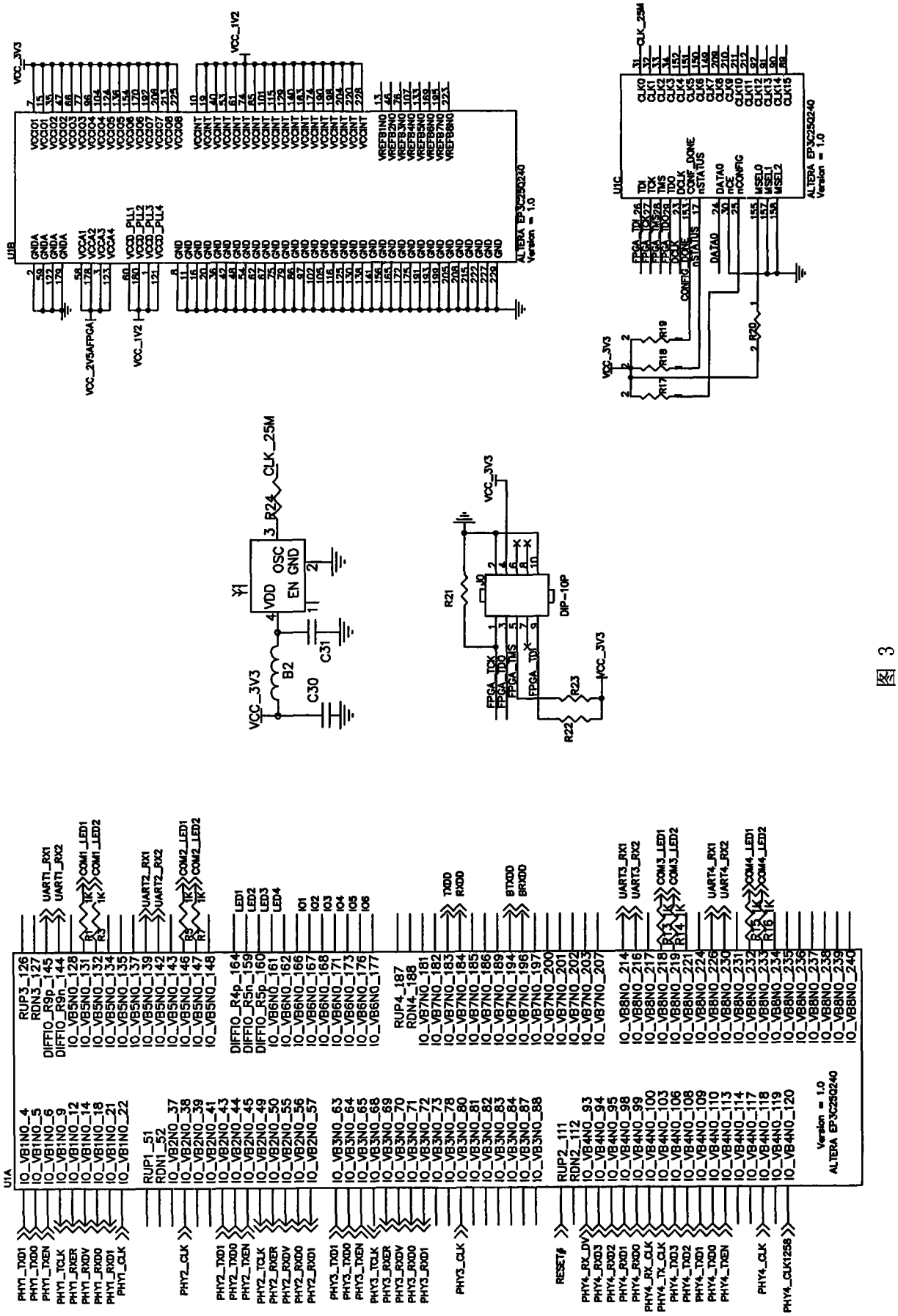


图 3

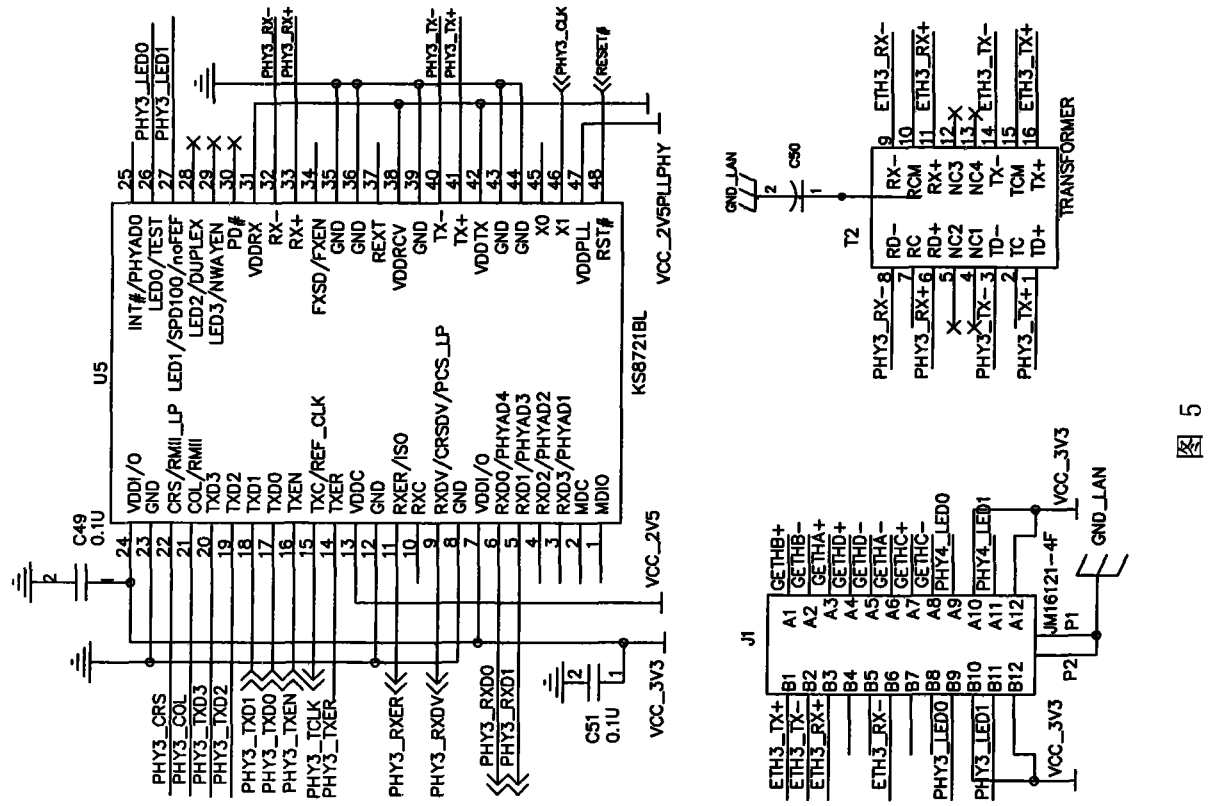

U5
KS8721BL
INT#/PHYAD0
LED0/TEST
LED1/SPD100/noFEF
LED2/DUPLEX
LED3/NWAYEN
PD#
VDDRX
RX-
RX+
FXSD/FXEN
GND
GND
REXT
VDDRCV
GND
TX-
TX+
VDDTX
GND
GND
X0
X1
VDDPLL
RST#
VDDI/O
GND
CRS/RMII_LP
COL/RMII
TXD3
TXD2
TXD1
TXD0
TXEN
TXC/REF_CLK
TXER
VDDC
GND
RXER/ISO
RXC
RXDV/CRSDV/PCS_LP
GND
VDDI/O
RXD0/PHYAD4
RXD1/PHYAD3
RXD2/PHYAD2
RXD3/PHYAD1
MDC
MDIO
PHY3_LED0
PHY3_LED1
PHY3_RX-
PHY3_RX+
PHY3_TX-
PHY3_TX+
PHY3_CLK
RESET#
VCC_2V5PLLPHY
VCC_2V5
VCC_3V3
C49
0.1U
C51
0.1U
PHY3_CRS
PHY3_COL
PHY3_TXD3
PHY3_TXD2
PHY3_TXD1
PHY3_TXD0
PHY3_TXEN
PHY3_TCLK
PHY3_TXER
PHY3_RXER
PHY3_RXDV
PHY3_RXD0
PHY3_RXD1
T2
TRANSFORMER
RD-
RC
RD+
NC2
NC1
TD-
TC
TD+
RX-
RCM
RX+
NC3
NC4
TX-
TCM
TX+
PHY3_RX-8
PHY3_RX+6
PHY3_TX-3
PHY3_TX+1
ETH3_RX-
ETH3_RX+
ETH3_TX-
ETH3_TX+
C50
GND_LAN
J1
GETHB+
GETHB-
GETHA+
GETHD+
GETHD-
GETHA-
GETHC+
GETHC-
PHY4_LED0
PHY4_LED1
VCC_3V3
GND_LAN
JM16121-4F
P1
P2
ETH3_TX+
ETH3_TX-
ETH3_RX+
ETH3_RX-
PHY3_LED0
PHY3_LED1
VCC_3V3

图 5

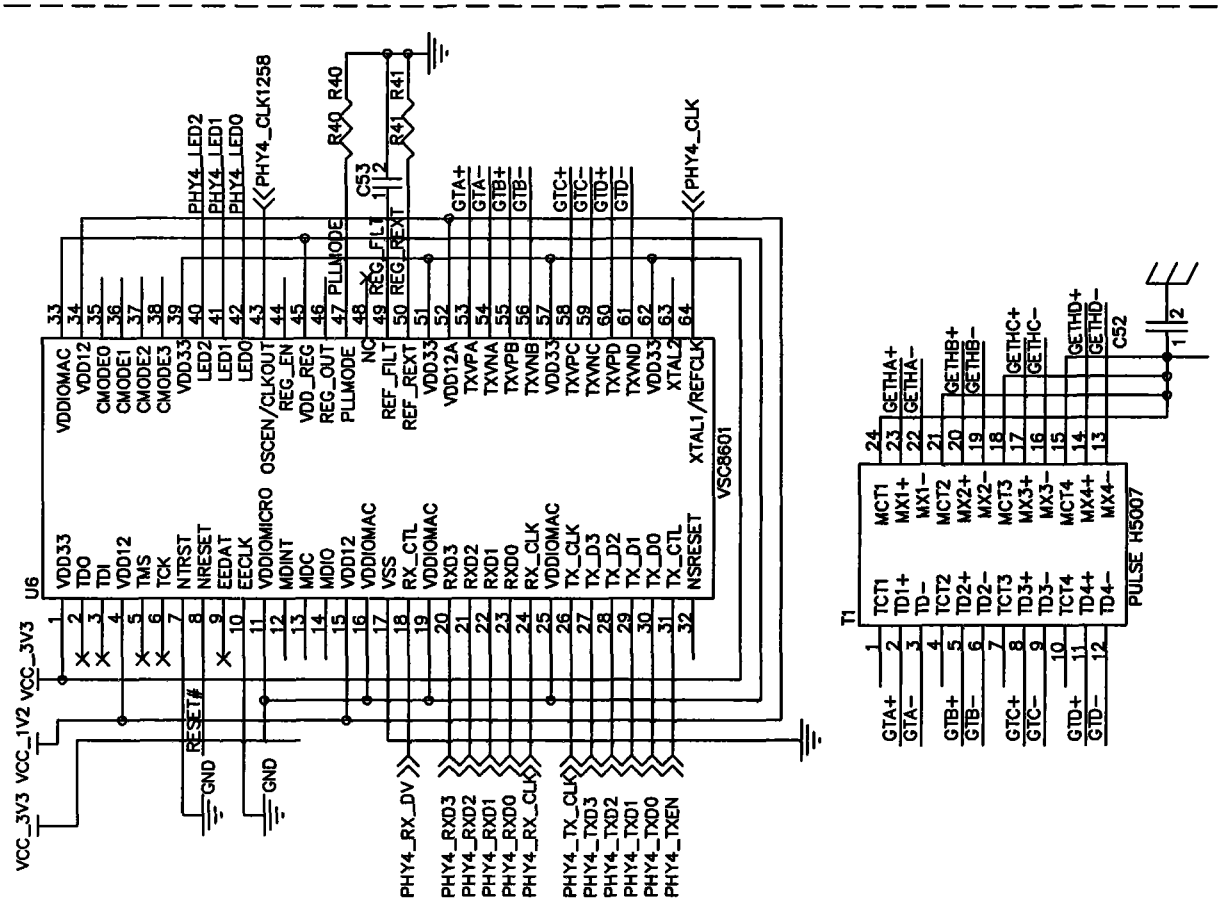

U6
VSC8601
VDDIOMAC
VDD12
CMODE0
CMODE1
CMODE2
CMODE3
VDD33
LED2
LED1
LED0
OSCEN/CLKOUT
REG_EN
VDD_REG
REG_OUT
PLLMODE
NC
REG_FILT
REF_REXT
VDD33
VDD12A
TXVPA
TXVNA
TXVPB
TXVNB
VDD33
TXVPC
TXVNC
TXVPD
TXVND
VDD33
XTAL2
XTAL1/REFCLK
VDDIOMICRO
MDINT
MDC
MDIO
VDD12
VDDIOMAC
VSS
RX_CTL
VDDIOMAC
RXD3
RXD2
RXD1
RXD0
RX_CLK
VDDIOMAC
TX_CLK
TX_D3
TX_D2
TX_D1
TX_D0
TX_CTL
NSRESET
PHY4_CLK1258
PHY4_LED2
PHY4_LED1
PHY4_LED0
R40
R41
C53
PHY4_CLK
GTA+
GTA-
GTB+
GTB-
GTC+
GTC-
GTD+
GTD-
T1
PULSE H5007
MCT1
MX1+
MX1-
MCT2
MX2+
MX2-
MCT3
MX3+
MX3-
MCT4
MX4+
MX4-
TCT1
TD1+
TD-
TCT2
TD2+
TD2-
TCT3
TD3+
TD3-
TCT4
TD4+
TD4-
GETHA+
GETHA-
GETHB+
GETHB-
GETHC+
GETHC-
GETHD+
GETHD-
C52
VCC_3V3
VCC_1V2
RESET#
GND
PHY4_RX_DV
PHY4_RXD3
PHY4_RXD2
PHY4_RXD1
PHY4_RXD0
PHY4_RX_CLK
PHY4_TX_CLK
PHY4_TXD3
PHY4_TXD2
PHY4_TXD1
PHY4_TXD0
PHY4_TXEN

图 4

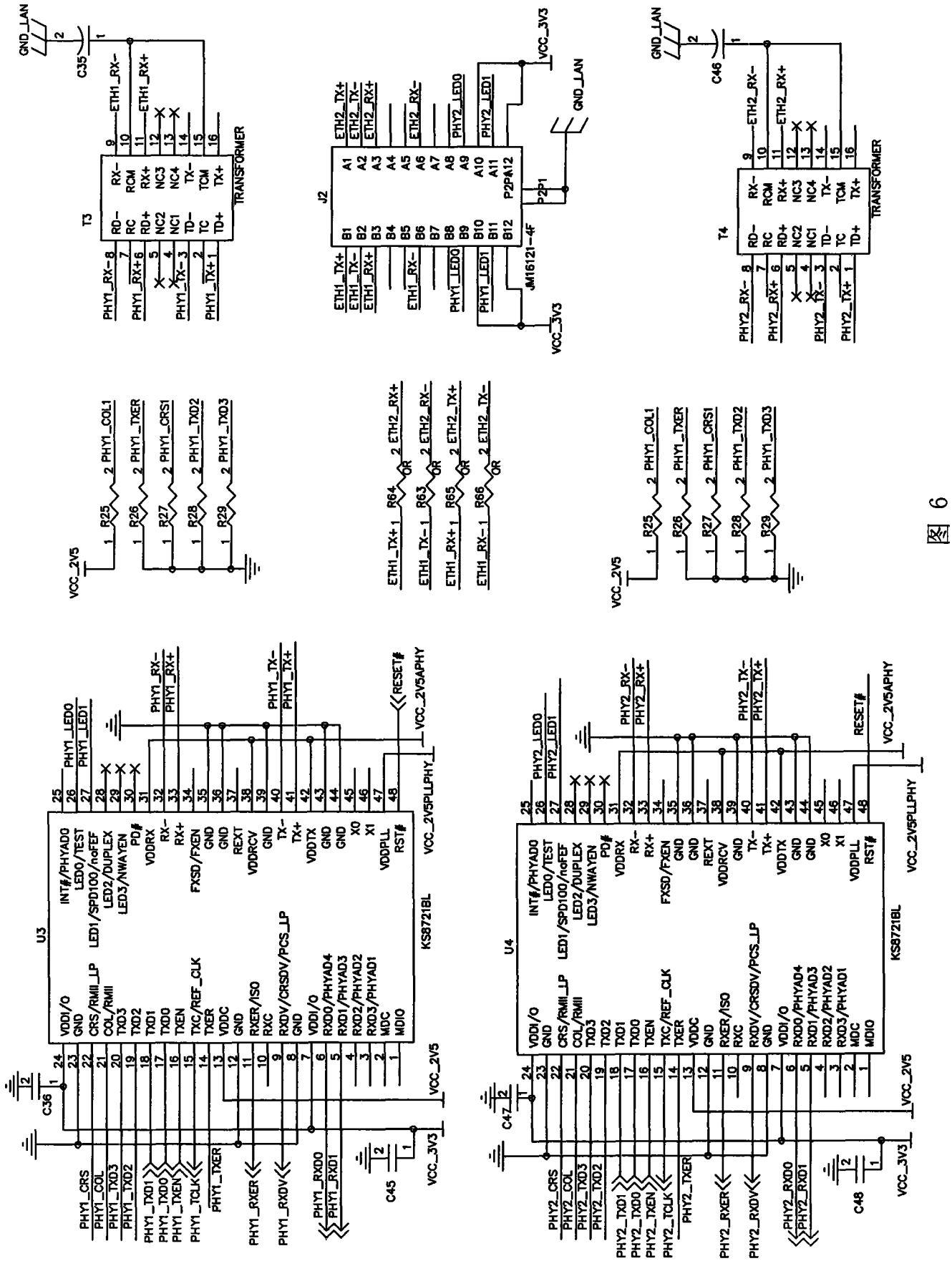

GND_LAN
C35
T3
TRANSFORMER
ETH1_RX-
ETH1_RX+
PHY1_RX-8
PHY1_RX+6
PHY1_TX-3
PHY1_TX+1
J2
JM16121-4F
P2PA12
ETH1_TX+
ETH1_TX-
ETH1_RX+
ETH1_RX-
PHY1_LED0
PHY1_LED1
VCC_3V3
GND_LAN
C46
T4
ETH2_RX-
ETH2_RX+
PHY2_RX-8
PHY2_RX+6
PHY2_TX-3
PHY2_TX+1
VCC_2V5
R25
R26
R27
R28
R29
PHY1_COL1
PHY1_TXER
PHY1_CRS1
PHY1_TXD2
PHY1_TXD3
ETH1_TX+1
ETH1_TX-1
ETH1_RX+1
ETH1_RX-1
R64
R63
R65
R66
ETH2_RX+
ETH2_RX-
ETH2_TX+
ETH2_TX-
OR
U3
KS8721BL
INT#/PHYAD0
LED0/TEST
LED1/SPD100/noFEF
LED2/DUPLEX
LED3/NWAYEN
PD#
VDDRX
RX-
RX+
FXSD/FXEN
GND
REXT
VDDRCV
TX-
TX+
VDDTX
XO
X1
VDDPLL
RST#
VDDI/O
CRS/RMII_LP
COL/RMII
TXD3
TXD2
TXD1
TXD0
TXEN
TXC/REF_CLK
TXER
VDDC
RXER/ISO
RXC
RXDV/CRSDV/PCS_LP
MDC
MDIO
RXD0/PHYAD4
RXD1/PHYAD3
RXD2/PHYAD2
RXD3/PHYAD1
VCC_2V5PLLPHY
VCC_2V5APHY
RESET#
C36
C45
PHY1_LED0
PHY1_LED1
PHY1_CRS
PHY1_COL
PHY1_TXD3
PHY1_TXD2
PHY1_TXD1
PHY1_TXD0
PHY1_TXEN
PHY1_TCLK
PHY1_TXER
PHY1_RXER
PHY1_RXDV
PHY1_RXD0
PHY1_RXD1
U4
C47
C48
PHY2_LED0
PHY2_LED1
PHY2_CRS
PHY2_COL
PHY2_TXD3
PHY2_TXD2
PHY2_TXD1
PHY2_TXD0
PHY2_TXEN
PHY2_TCLK
PHY2_TXER
PHY2_RXER
PHY2_RXDV
PHY2_RXD0
PHY2_RXD1

图 6

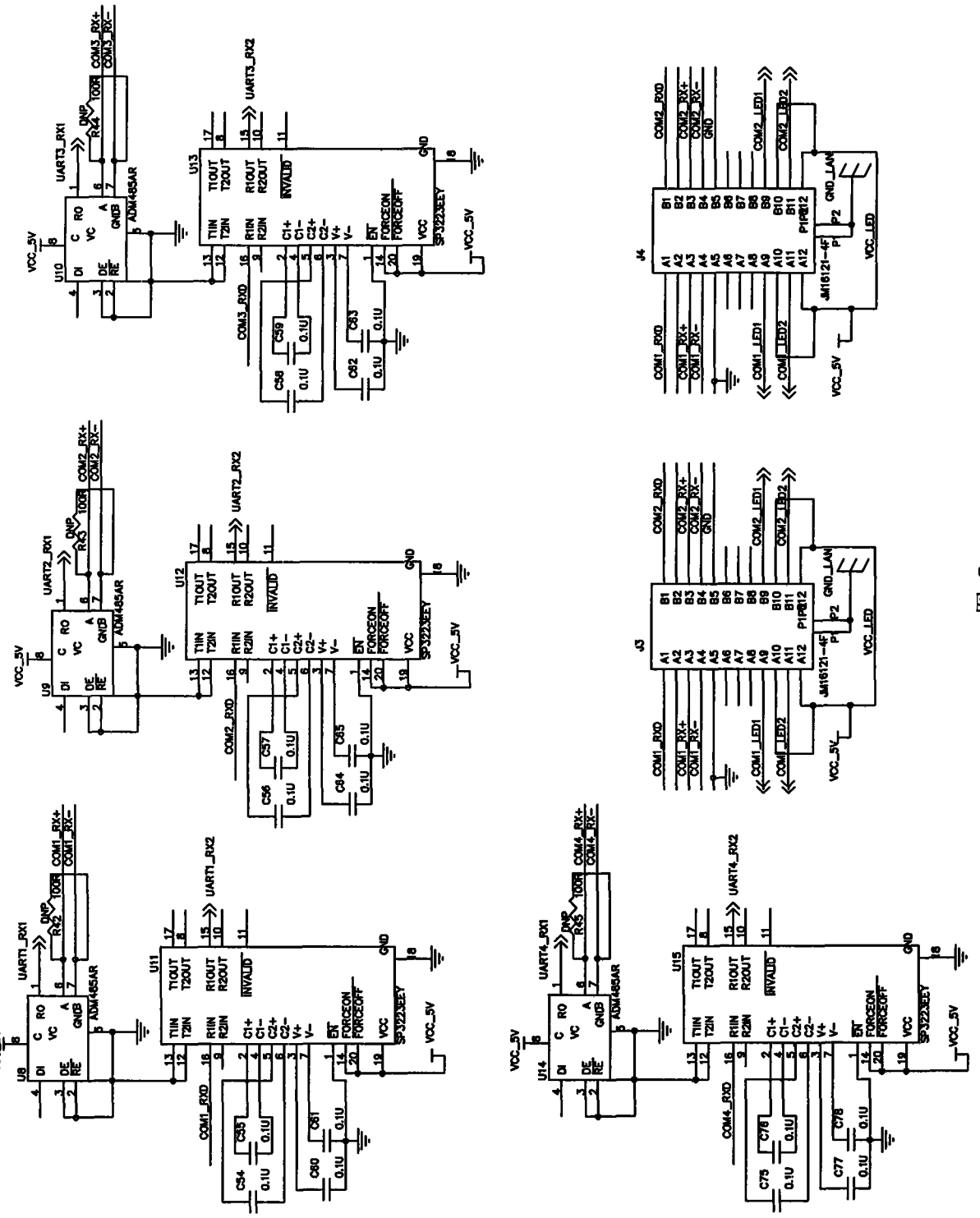


图 7

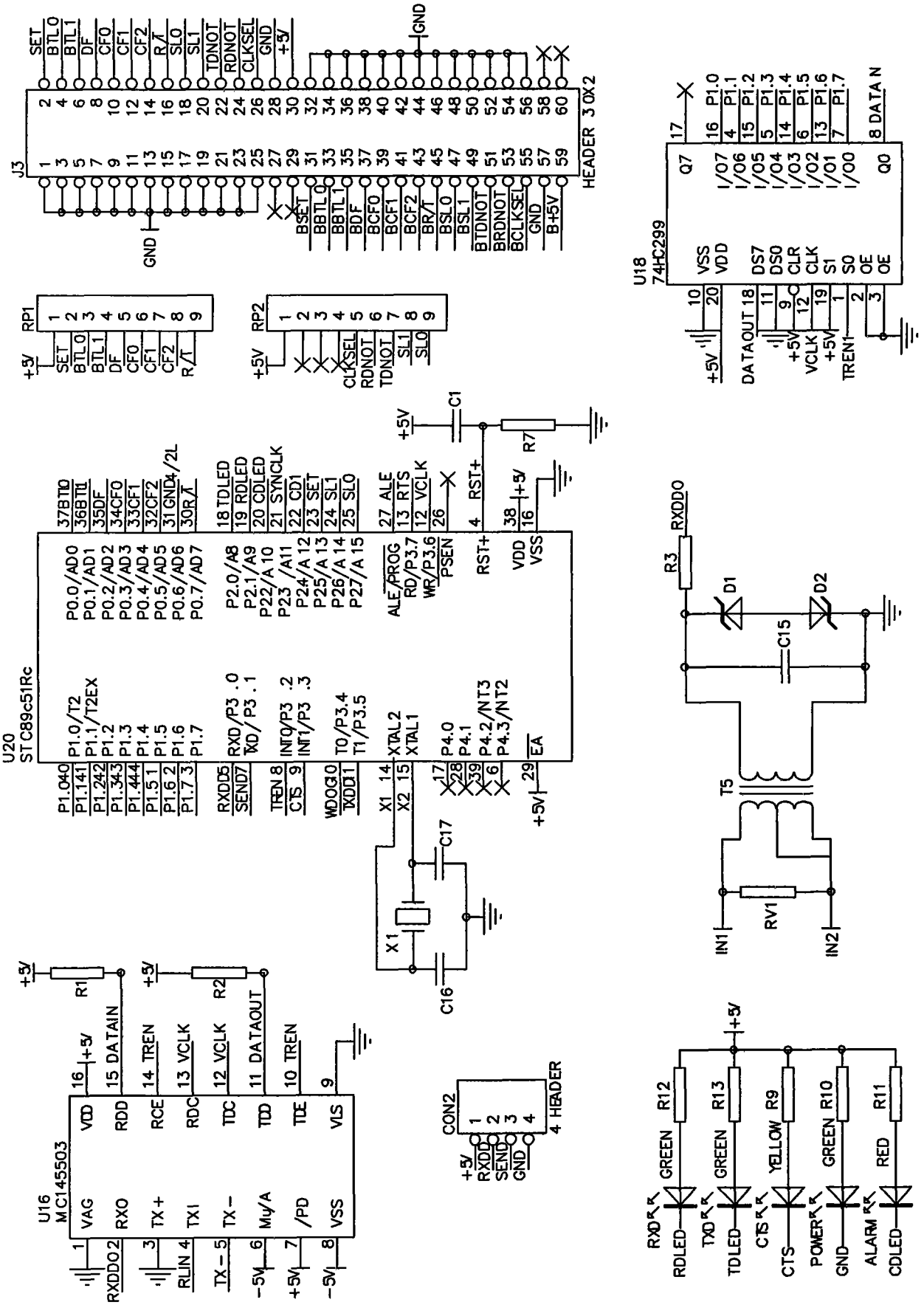


图 8

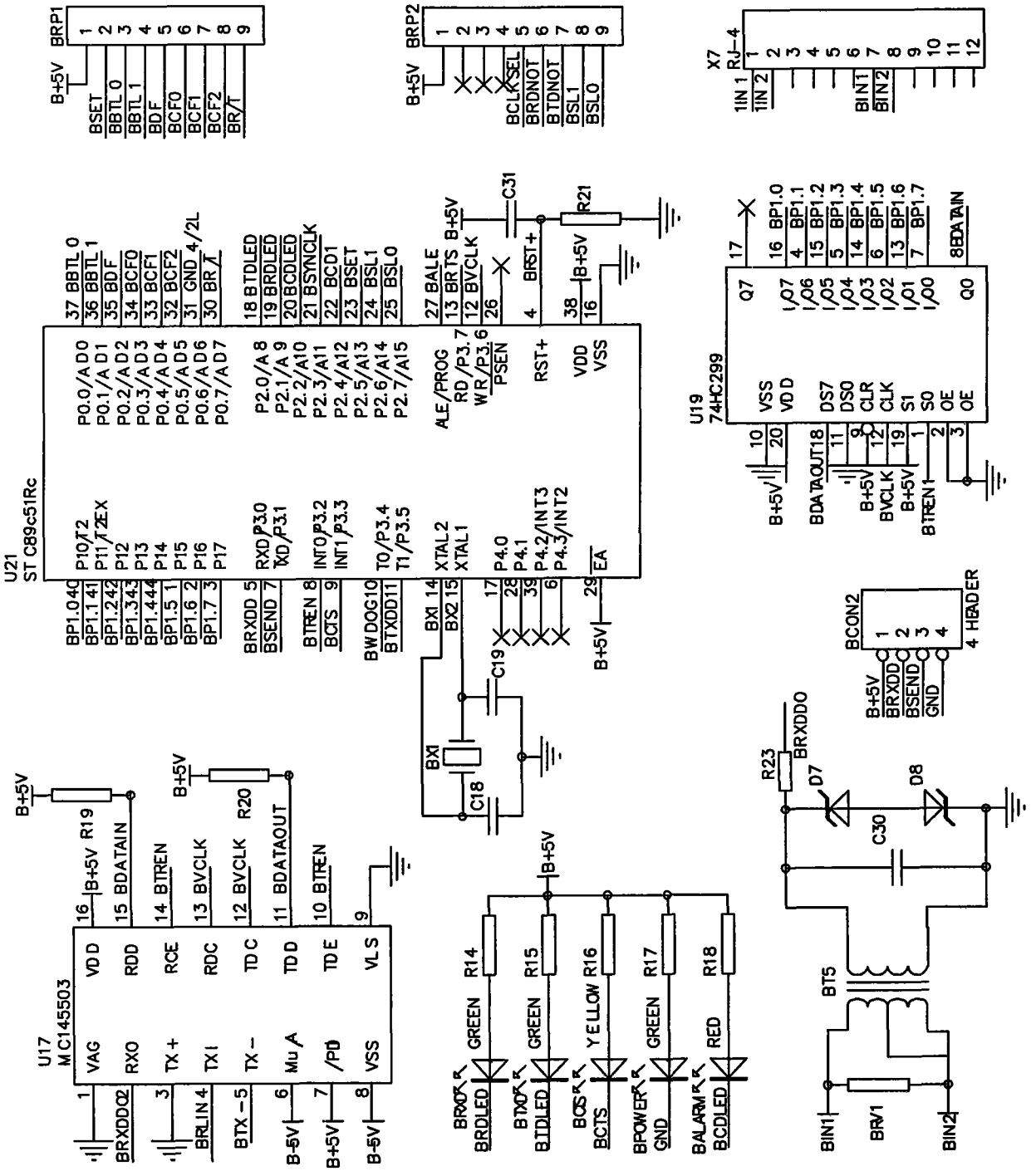


图 9

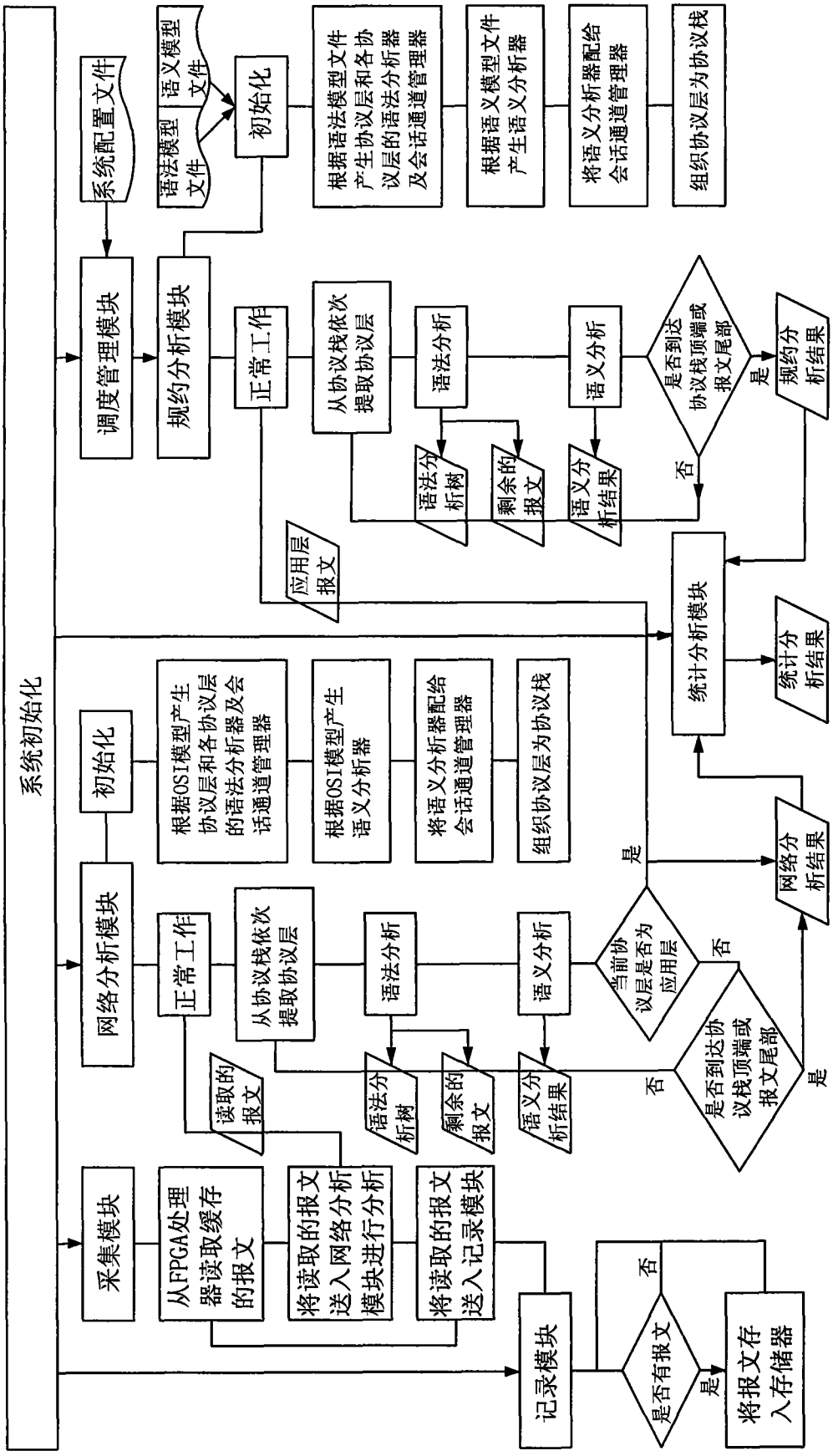

系统初始化
采集模块
网络分析模块
初始化
正常工作
从协议栈依次提取协议层
语法分析
语义分析
当前协议层是否为应用层
是
否
网络分析结果
根据OSI模型产生协议层和各协议层的语法分析器及会话通道管理器
根据OSI模型产生语义分析器
将语义分析器配给会话通道管理器
组织协议层为协议栈
读取的报文
语法分析树
剩余的报文
语义分析结果
是否到达协议栈顶端或报文尾部
否
是
从FPGA处理器读取缓存的报文
将读取的报文送入网络分析模块进行分析
将读取的报文送入记录模块
记录模块
是否有报文
否
是
将报文存入存储器
调度管理模块
规约分析模块
正常工作
从协议栈依次提取协议层
语法分析
语义分析
是否到达协议栈顶端或报文尾部
否
是
规约分析结果
应用层报文
语法分析树
剩余的报文
语义分析结果
统计分析模块
统计分析结果
系统配置文件
语法模型文件
语义模型文件
初始化
根据语法模型文件产生协议层和各协议层的语法分析器及会话通道管理器
根据语义模型文件产生语义分析器
将语义分析器配给会话通道管理器
组织协议层为协议栈

图 10