**控制系统信息安全防护模块总体方案**

**电子科技大学自动化工程学院自动化研究所**

**2016年 月 日**

目录

[1引言 3](#_Toc441325195)

[2 需求分析 3](#_Toc441325196)

[2.1总体目标 3](#_Toc441325197)

[2.2 基本功能 3](#_Toc441325198)

[3 系统设计 4](#_Toc441325199)

[3.1 系统结构 4](#_Toc441325200)

[3.2 软件设计 5](#_Toc441325201)

[3.2.1 软件平台需求 5](#_Toc441325202)

[3.2.2 软件平台选型 5](#_Toc441325203)

[3.2.3 软件架构 7](#_Toc441325204)

[3.3 硬件设计 11](#_Toc441325205)

[3.3.1硬件平台需求 11](#_Toc441325206)

[3.3.2 硬件平台选型 11](#_Toc441325207)

[3.3.3硬件开发技术路线 13](#_Toc441325208)

[4测试环境 15](#_Toc441325209)

[4.1信息安全测试平台搭建 15](#_Toc441325210)

[4.2 攻击与防护测试过程 16](#_Toc441325211)

[5结束语 17](#_Toc441325212)

## 1引言

随着信息化与工业化的深度融合，越来越多的工业控制系统产品（如SCADA、DCS等）采用通用协议、通用硬件和通用软件，以各种方式与MIS网络、因特网等公共网络连接，但是由于工业控制系统与传统的IT系统之间有着很大的区别，工业控制系统方面还存着很多不足，而由于防护不足会造成很多严重的问题，其中包括核心数据被窃取、关键工控流程被破坏、对工业系统功能未经授权的访问甚至造成工厂停产等，所以增加工业控制系统的防护功能有非常重要的意义。

## 2 需求分析

### 2.1总体目标

开发与DCS(分布式控制系统)集成的控制系统信息安全防护模块，如图2-1所示，以保障工业控制系统在公共以太网中的信息安全。

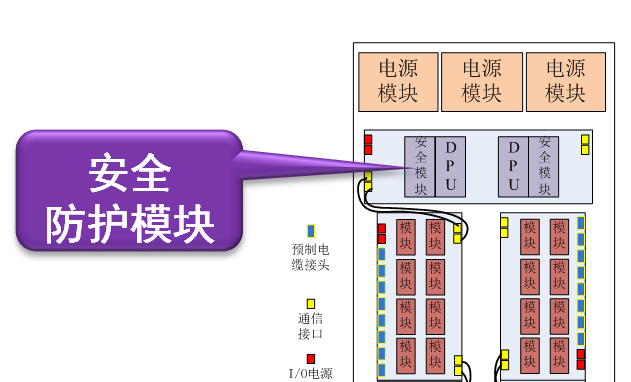


图2-1 控制系统信息安全防护模块

### 2.2 基本功能

该安全防护模块具体应包含如下功能：

1. 透明模式

安全防护模块采用无IP工作模式，不需要对其设置IP地址。

(2)抗攻击防护功能

对工业控制系统的通讯环境需求和DCS系统的特点与传统IT网络攻击进行对比分析，可得到针对本模块的主要攻击有SYN Flood、ICMP Flood和Ping of Death攻击等，进而采取具体有效的抗攻击方法，实现抗攻击防护的功能。

(3)访问控制和深度包检测功能

访问控制是网络安全防范和保护的主要策略，其目的保证安全防护模块的网络资源不被非法访问和使用。深度包检测的任务就是把当前数据包中应用层载荷的特定内容与协议标准定义的期望值进行比较，检查其是否符合协议标准的规定，从而确定应用层协议的种类以及应用的内容，实现用于载荷的分析与过滤。

(4)防火墙管理配置功能

防火墙管理配置软件采用web配置客户端和软件配置客户端，用于验证用户管理权限，实现网络拓扑组态和安全规则组态(包括自定义安全规则和安全规则自学习)，还包括网络设备识别、实时报警和查询分析等功能。

(5)报警日志管理功能

日志管理服务器为异常和报警提供日志服务，对日志进行统计、查询、分析、备份等，并将日志存储本地，同时也将日志通过syslog形式传输到远程的服务器进行存储。

(6)支持多种工业协议

该模块需要支持Modbus TCP、OPC和DNP3.0等大多数基于以太网的通讯协议。

## 3 系统设计

### 3.1 系统结构

控制系统信息安全防护模块是基于内置工业通讯协议的隔离防护平台，而工业通讯协议通常是基于常规TCP/IP协议在应用层的高级开发，所以该安全防护模块不仅是在端口上的防护，更重要的是基于应用层上数据包深度检查，属于新一代工业通讯协议防火墙，为工业通讯提供独特的、工业级的专业隔离防护解决方案。当数据包到达防火墙，会对其进行深度包检测检测，检验合格让其通过，不合格直接丢弃。

信息安全防护模块系统整体架构如图3-1所示：



图3-1 系统整体架构

### 3.2 软件设计

#### 3.2.1 软件平台需求

工业控制信息安全防护模块需要时刻防护来自DCS系统外部的攻击，并且需要实时、稳定和准确地确保DCS系统安全地运行。因此，安全防护模块的软件平台需要满足如下要求：

⮚ 安全性高

⮚ 稳定性高

⮚ 实时性强

⮚ 拥有良好的网络性能

#### 3.2.2 软件平台选型

Linux系统因其稳定性、安全可靠性、灵活性以及可制定性使其在信息安全防护行业非常受欢迎，目前国内90%以上安全防护产品都是基于Linux内核开发的。Linux操作系统不仅本身拥有安全的系统结构，而且拥有许多支持信息安全防护的环境和工具。

Linux的安全结构主要由根用户的自主访问控制、网络访问控制、加密和日志几部分组成。在信息安全防护方面，Linux的netfilter框架能够将安全模块对数据包的处理引入IP层中。Netfilter框架位于Linux网络层和安全防护内核功能模块之间，通过Netfilter结构将防火墙对数据包的处理引入IP层中，从而构成不同的模块，使得整个系统在结构生很清晰，有利于扩展。Linux的Netfilter/Iptables框架能够很好的支持信息安全防护的数据包处理功能，Linux系统本身具有的高安全性，也使得Linux系统在信息安全防护方面能够防护许多对系统的攻击。

为了提高普通Linux系统的实时性能，实时Linux改进了普通Linux系统，使得实时Linux不仅具有普通Linux系统的网络特性，还具有较高的实时性能。该安全防护模块需要选择稳定性和网络性能较高的实时操作系统，可供选择的实时Linux主要有Monta Vista和RT-Linux，它们都拥有良好的实时性能和强大的开发工具。表3-1为两种系统的比较。

表3-1实时Linux比较

|  |  |  |
| --- | --- | --- |
| 操作系统 | Monta Vista | RT-Linux |
| 版权费用 | 商用收费 | 商用收费 |
| 实时性能 | 为Linux系统开发了一种抢占式内核 | 实现了一个微内核的实时操作系统，而将普通Linux作为一个该系统中的一个低优先级的任务 |
| 内核版本 | Linux 3.10 | Linux .4.28 |
| 支持标准 | LSB4.1、ATCA、CGL | POSIX.1B、ATCA、CGL |
| 开发工具 | Monta Vista DevRocket  Eclipse-based IDE | Wind River Workbench 3.0 |
| 技术支持 | Monta Vista | WindRiver |
| 支持硬件 | X86架构处理器 | X86架构处理器 |

Monta Vista符合LSB 4.1标准（Linux Standard Base 4.1）和ATCA标准（Advanced Telecom Computing Architecture）。相对于RT-Linux系统，Monta Vista拥有很高的实时性能，安全性高，稳定性好，具有良好的网络特性，同时又有完善的开发环境和更好的技术支持。Monta Vista提供DevRocket Eclipse-based IDE开发环境，并且提供GNU工具链，包括gcc编译器、gdb调试工具等。此外，一些第三方工具也很大支持了Monta Vista的应用开发。

结合以上优点，Monta Vista更加适合工业控制信息安全防护模块的开发。

#### 3.2.3 软件架构

安全防护模块系统软件架构分为软件平台、基础层、解析层和应用层，如图3-2所示。



图3-2 软件架构

⑴ 应用层:

应用层包括web配置客户端和软件配置客户端，主要对安全防护模块进行配置，包括透明模式配置、报警日志管理、安全防护规则以及深度包检测协议配置。Web/软件客户端结构图如图3-3所示。



图3-3 web/软件客户端结构图

⑵ 解析层:

解析层主要对web配置客户端以及软件配置客户端的配置信息进行解析，通过配置基础层相关软件实现用户所需功能。

⑶ 基础层:

基础层主要包括Syslog服务器、Bridge-utils、iptables、DPI和Snort，其中：

⮚ **Syslog服务器**

Syslog服务器提供报警日志服务，可以统一收集并实时监控安全防护模块的通讯日志，将日志存储在本地或传输到远程服务器，达到日志的完整、安全、长时间存储的目的，报警日志简示图如图3-4所示。



图3-4 报警日志简示图

同时，本日志方案还支持对报警进行组态，将产生的报警信息归类到不同的组别中。方便查看、记录和区别。报警组态示意图如图3-5所示。

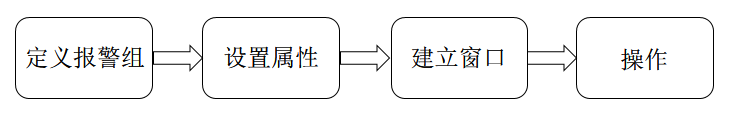


图3-5 报警组态示意图

⮚ **Bridge-utils**

Bridge-utils为网桥管理器，可将安全防护模块设置为工作在透明模式下，即采用无IP工作方式，在使用时不必重新设定或修改路由，可以直接放置到网络中使用，即增加了网络的安全性，又降低了管理的复杂程度。

⮚ **Iptables**

iptables是与最新的 3.5 版本 Linux [内核](http://baike.baidu.com/view/1366.htm)集成的 IP 信息包过滤系统，用来设置、维护和检查Linux内核的IP包过滤规则，可以根据需求来设置特定规则，有利于在 Linux 系统上更好地控制 IP 信息包过滤和防火墙配置。基础层中iptables主要通过检测数据包的头部信息，包括源地址、目的地址、端口等，实现访问控制功能以及抗攻击防护功能，访问控制流程如图3-6所示。



图3-6访问控制流程

⮚ **DPI**

DPI技术（即深度包检测技术）是一种基于应用层的流量检测和控制技术，当IP数据包、TCP或UDP数据流通过基于DPI技术的带宽管理系统时，该系统通过深入读取IP包载荷的内容来对OSI七层协议中的应用层信息进行重组，从而得到整个应用程序的内容，然后按照系统定义的管理策略对流量进行整形操作。 在基础层中通过深度包检测数据包能否通过，DPI流程如图3-7所示。

图3-7 DPI流程

⮚ **Snort**

Snort是一个具有跨平台(Multi-Platform)、实时(Real-Time)流量分析、网络IP数据包(Pocket)记录等特性的强大的网络入侵检测/防御系统，能够对网络上的数据包进行抓包分析，并根据所定义的规则进行响应及处理。Snort通过对获取的数据包，进行各规则的分析后，根据规则链，可采取Activation（报警并启动另外一个动态规则链）、Dynamic（由其它的规则包调用）、Alert（报警），Pass（忽略），Log（不报警但记录网络流量）五种响应的机制。Snort的有三种模式的运行方式：嗅探器模式，包记录器模式，和网络入侵检测系统模式。其中最重要的用途是作为网络入侵检测检测系统（NIDS），入侵检测模式能对数据包进行分析、按规则进行检测并出响应。

Snort入侵检测系统的部署非常灵活，能够适应多种平台，源代码开放且使用免费。Snort的体系结构如图3-8所示。



图3-8 Snort体系结构

⑷ 操作系统层:

操作系统层主要包含Linux内核、文件系统、Netfilter、Bridge模块、TCP/IP协议栈等，其中：

⮚ **Netfilter**

Netfilter组件是由Rusty Russell提出的Linux 2.4内核防火墙框架，该组件也称为内核空间（kernel space），是Linux内核的一部分，由一些信息包过滤表组成，这些表包含内核用来控制信息包过滤处理的规则集，可实现安全策略应用中的许多功能，如数据包过滤、数据包处理、地址伪装、透明代理、动态网络地址转换（NAT），以及基于用户及媒体访问控制地址的过滤和基于状态的过滤、包速率限制等。Netfilter组件和Iptables组件共同构成了IP信息包过滤系统。

数据包通过Netfilter系统的过程如图3-9所示：



图3-9 Netfilter功能框架

### 3.3 硬件设计

#### 3.3.1硬件平台需求

工业控制信息安全防护模块的硬件平台需要满足以下条件：

⮚ 拥有高效的处理性能

⮚ 低功耗，外形尺寸小、无风扇结构

⮚ 产品生命周期长、稳定性高、可扩展性强

⮚ 包含多个千兆以太网口

⮚ 支持IPv4/IPv6协议和Bypass功能

#### 3.3.2 硬件平台选型

x86是英特尔首先开发制造的一种微处理器体系结构的泛称，具有很高的处理性能，在设计过程中着重考虑了向前兼容性，保证了硬件平台能继续运行以往开发的各类应用程序。许多处理器厂商都推出了x86架构下的低功耗处理器家族，例如Intel的Atom处理器、AMD的G系列处理器。因此，基于x86的硬件平台在拥有高效处理性能的条件下，不仅功耗低，还具有开发灵活性高、可扩展性强的特点。

当前，有多家公司设计、生产并售卖x86处理器，其中主要包括英特尔（Intel）、AMD、威盛电子（VIA）、美国国家半导体公司等。在这些公司生产的x86处理器中，Intel的Atom系列处理器、AMD的G系列处理器、VIA的Nano系列处理器，都具有较高的处理性能和较低的功耗，表3-2为这三款处理器的对比：

表3-2 三款低功耗x86处理器比较

|  |  |  |  |
| --- | --- | --- | --- |
| 处理器型号 | Intel Atom系列 | AMD G系列 | VIA Nano系列 |
| 主频 | 600MHz~1.91GHz | 615MHz~1.65GHz | 1GHz~1.8GHz |
| 功耗 | （2~13）W | （4.5~18）W | （5~25）W |
| 内核数量 | 1~4 | 1~2 | 2 |
| PCI总线 | PCI-Express2.0  (5Gb/s) | PCI-Express2.0  (5Gb/s) | PCI-Express1.0  (2.5Gb/s) |
| 支持最大内存 | 2GB~8GB | 1GB | 2GB |
| 硬件安全特性 | AES-NI、可信执行技术和执行禁用位 | 不支持 | AES、RNG和SHA-1 |
| 生命周期 | 7年 | 至少5年 | 7年 |

在作为安全防护模块时，x86平台通常使用一颗或多颗主CPU来处理业务数据，网卡芯片和CPU通过PCI总线来传输数据。Nano系列处理器只支持PCI-Express 1.0，PCI-Express 1.0的数据传输速率为2.5Gbps。Atom系列处理器支持的PCI-Express 2.0在数据传输速率上作出了重大升级，从2.5Gbps翻倍至5.0Gbps。由于每条线路的速度能达到2.5Gbps，PCI-Express 2.0非常适用于多块网卡作为输入输出扩展模块的场合。在作为安全防护模块方面，由于Atom系列处理器支持PCI-Express 2.0，拥有更高的数据传输速率。

在硬件安全特性方面，英特尔还拥有数据保护技术和平台保护技术。Atom系列处理器具有AES数据保护技术，以及可信执行技术和执行禁用位两种平台保护技术。英特尔Trusted Execution Technology（可信执行技术） 是一组针对英特尔处理器和芯片组的通用硬件扩展，可增强数字办公平台的安全性（如测量启动与保护执行）。此项技术实现这样一种环境：应用可以在其各自的空间中运行，而不受系统中所有其它软件的影响。执行禁用位是一项基于硬件的安全特性，它能减少受病毒和恶意代码攻击的机会，并防止有害软件在服务器或网络上执行和扩散。

相对与AMD G系列处理器和VIA Nano系列处理器，Intel的Atom系列处理器不仅具有更高的处理性能，还拥有更低的功耗，因此该安全防护模块的硬件平台选用基于x86架构设计的Intel Atom处理器。

#### 3.3.3硬件开发技术路线

基于工控机开发和自主设计开发两种方式同时进行，即在工控机上完成基本的软件开发，同时自主完成模块主板和机箱的设计，最后将工控机上的软件系统移植到自主研发的硬件平台上。

1. 基于工控机开发

基于工控机开发有两种机型可供选择：

⮚ **其阳华夏科技SCB-6010**

该工控机最高支持3.2版本的Linux内核，其产品特性如表3-3所示:

表3-3其阳华夏科技SCB-6010工控机参数

|  |  |
| --- | --- |
| CPU和内存 | Intel Atom Bay Trail（1.46GHz）,2GB DDR3内存 |
| 接口 | 1xVGA，3xUSB2.0, 6 x以太网口，1xConsole |
| 散热设计 | 无风扇设计 |
| 尺寸 | 170x140x60mm |

⮚ **华北工控BIS-7870**

该工控机能支持较新版本的Linux内核，其产品特性如表3-4所示：

表3-4 华北工控机参数

|  |  |
| --- | --- |
| CPU和内存 | Intel Atom D525, 1GB DDR2内存 |
| 接口 | 1xVGA，2xUSB2.0, 6 x以太网口，1xConsole |
| 散热设计 | 无风扇设计,采用“冰翅”散热系统传导散热 |
| 尺寸 | 300x194x50mm |

1. 自主设计开发

⮚ **Bypass功能设计**

Bypass有三种触发方式：通过电源触发、GPIO控制和Watchdog控制，如图3-10所示：

图3-10 Bypass功能设计

⮚ **主板设计**

模块主板基于Intel Pineview-M/D+ICH8M芯片组，搭载Intel Atom处理器，1条SO-DIMM最大支持4GB DDR3内存，内置1个VGA接口，2个USB2.0接口，1个Console接口及6个千兆以太网接口，支持两组Bypass功能。主板设计如图3-11所示：

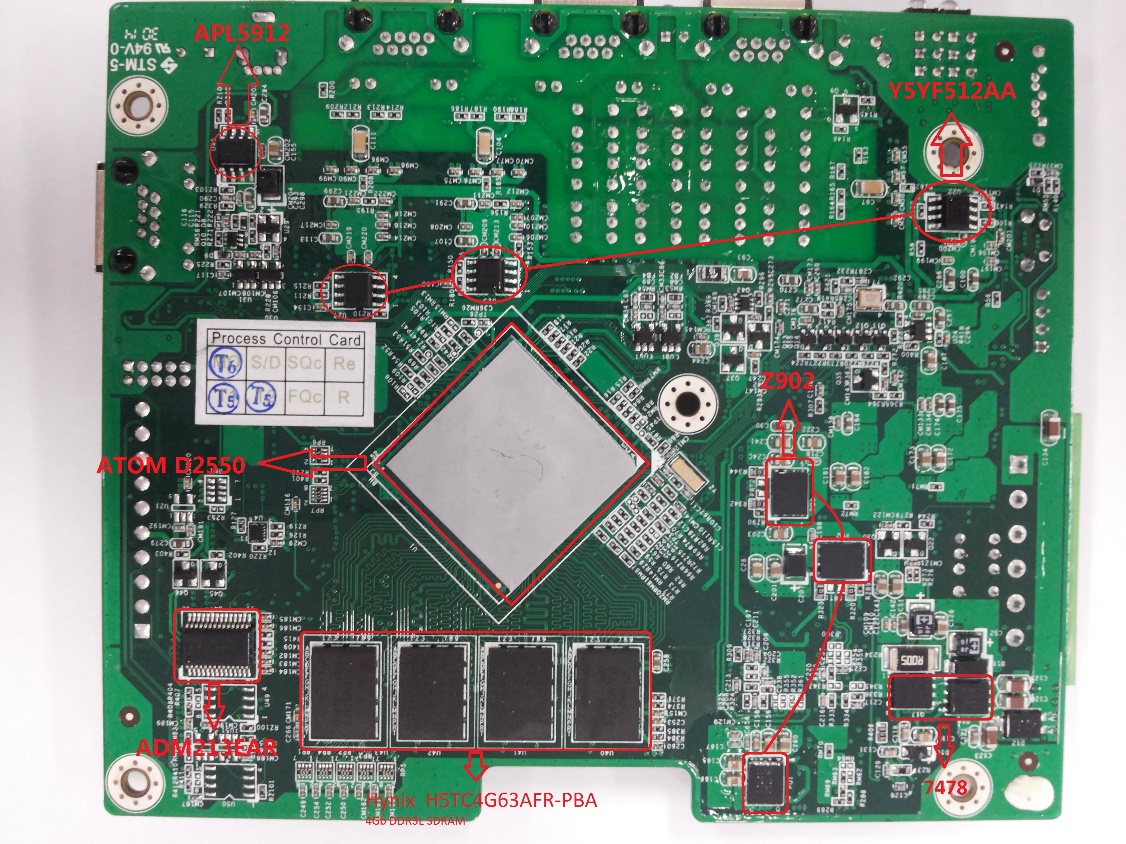


图3-11 模块主板

⮚ **机箱设计**

模块机箱采用无风扇设计，如图3-12所示。

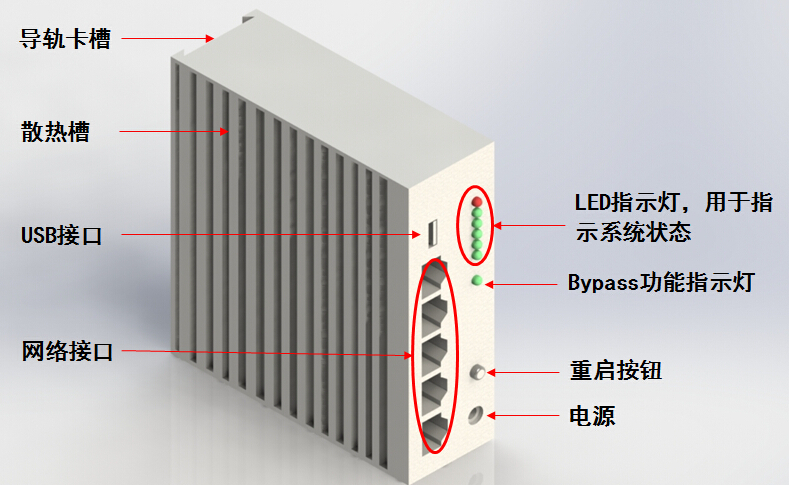


图3-12 防护模块机箱设计图

## 4测试环境

### 4.1信息安全测试平台搭建

工业控制系统信息安全测试平台的硬件部分由PLC控制器实验台，安全防护模块，PLC控制器监控端，防护模块规则配置管理端以及模拟外部攻击端组成。PLC控制器实验台是一个内部网络，被防护模块隔离保护，其拓扑结构如图4-1所示。



图4-1 工业控制信息安全防护模块测试平台拓扑结构

⮚ **PLC监控端**

PLC监控端既可以在屏幕上显示信号的变化，也可以对PLC直接发出操作命令，在该上位机应用与GE PLC配套的iFIX组态软件可以实现实时监视控制PLC的运转状态，从而控制相关设备和驱动装置。

⮚ **防护模块配置端**

该规则配置端可以根据不同的工业环境，远程配置防护模块的相关过滤规则。例如，该实验太如果选择基于modbus TCP协议的通信模块，那么可以选择modbusTCP协议配置界面，进行规则的配置。

⮚ **攻击端**

通过相应的攻击软件可以模拟出相应的攻击，该实验可以通过拒绝服务攻击（DOS）PLC控制器，或者通过伪造、发送不合理的数据包的方式攻击PLC控制器。

### 4.2 攻击与防护测试过程

该测试平台通过模拟DOS攻击和伪造数据包攻击来对安全防护模块进行测试：

⮚ **DOS攻击及防护过程**

DOS主要通过对PLC控制器发送大量不合法的请求连接数据包占用连接资源，造成PLC控制器故障甚至于断开网络，使监控端无法收到控制器返回的信号，也无法对控制器进行控制，造成无法预知的后果。由图4-1可知，所有的数据包必须通过防护模块才能到达PLC控制端。若防护模块没有开启，则默认通过所有数据包，当大量的请求连接数据包到达PLC控制器，PLC会出现故障，并断开网络连接，负责监控PLC工作状态的PLC监控端无法获取PLC控制器的运行状态；若防护模块开启，并通过配置端进行数据包过滤规则配置。配置完成后，该防护模块就能进行数据包过滤，实现严格的防护功能，当不合法的数据包到达防护模块，就会被它直接丢弃，拒绝不合法的请求数据包，合法的数据包才能通过。

⮚ **伪造数据包攻击及防护过程**

通过伪造并发送不合理的控制命令包的方式攻击PLC控制器，使PLC控制器出现故障，有可能停止运转或者不按正常方式运转，对PLC及其被控对象造成不可预知的破坏。由图4-1中拓扑结构可知，所有的数据包必须通过防护模块才能到达PLC控制端。若防护模块没有开启，则默认通过所有数据包，当伪造的数据包到达PLC控制器，PLC会出现故障，负责监控PLC工作状态的PLC监控端也会出现相应的提示；若防护模块开启，并通过配置端进行数据包过滤规则配置。配置完成后，该防护模块就能进行数据包过滤，实现严格的防护功能，当含有攻击的数据包到达防护模块，防护模块会对数据包进行深度检测，就会被它直接丢弃，拒绝危险数据包的通过。只有满足协议规则并且合理的数据包才能让其通过。

## 5结束语

基于深度包解析的信息安全防护模块有利于提高工业控制系统的安全性，具有很强的实际价值，开发流程也对以后的研究有一定的借鉴意义。