DOI:10.19651/j.cnki.emt.1802353

# 一种工业以太网状态安全监视器的设计*

韩丹涛 赵艳领 公彦杰
(机械工业仪器仪表综合技术经济研究所 北京 100055)

**摘 要**：针对工业控制网络信息安全以及病毒防护，以广泛应用的 ModbusTCP 为研究对象，采用 ModbusTCP 通信协议深度解析检测与网络层防火墙功能相结合，设计了 Modbus TCP 的专用工业网络状态安全监视器。根据配置策略实现未授权设备的非法访问、网络状态、异常报文的识别，采用边界法实现 Modbus 关键数据的监测，提出并实现了基于工艺关系的安全监视策略。实验结果表明，该工具在不影响正常网络通信的情况下，针对要保护的关键设备，可从网络层、数据流量、设备关键数据以及工艺关系等多层次进行保护，当有非法入侵访问时实时显示具体报警信息，对当前的工业网络安全具有重要意义。

**关键词**：工业控制网络；Modbus TCP；工艺关系；安全监视器
**中图分类号**：TP39；TN91 **文献标识码**：A **国家标准学科分类代码**：510.1040

# Design of industrial ethernet security monitor

Han Dantao Zhao Yanling Gong Yanjie
(Instrumentation Technology & Economy Institute, Beijing 100055, China)

**Abstract**: For the industrial network security and virus protection, A special industrial Ethernet security monitor with industrial network layer firewall and depth detection on Modbus TCP is designded for protecting industrial control network. According to the configuration of safety strategy, the monitor can detect unauthorized access, network status and abnormal message, and the critical data of Modbus by using the boundary method, a security monitoring strategy based on process relation is proposed and implemented. Display alarm information and give Suggestions for processing. After testing, the results show that the tools has no influence on the normal industrial control network, the key device can be protected from multiple levels, such as network layer, data flow, key equipment data and process relations.and can effectively detect the exception of industrial control network based on the configuration strategy.

**Keywords**: industrial control network; Modbus TCP; process relation; security monitor

## 0 引 言

工业控制系统现场设备通信正逐步由封闭的现场总线向开放的工业以太网过渡，同时系统高效和标准化集成也成为工业控制系统的重要方向[1]。Modbus TCP 作为典型的工业以太网得到了越来越多的广泛应用。因此针对支持该类协议接口的设备的信息安全攻击有可能导致工业控制系统的瘫痪，继而影响生产安全。工业以太网通用防火墙可以实现管理网络与工业控制网络的防护，但是针对工控系统的国家级的网络病毒，在工业控制网内部也需要针对性的防护。目前国内外基于 Modbus TCP 安全的研究较多，大部分的研究只针对协议在工业控制系统中的安全性以及脆弱性进行了分析[2-8]，并提出了解决方案，但是方案偏向于互联网的安全技术，针对入侵检测，有部分研究采用基于参数或者状态的异常监测方法，准确性存在误报问题。本文在以上研究的基础上，设计了 Modbus TCP 的专用工业网络安全监视器，采用 Modbus TCP 通信协议深度解析检测与网络层防火墙功能相结合的方式，可准确实时监控工业控制系统中的关键设备，并显示非法入侵时的异常报警信息。

## 1 系统原理

Modbus 是 OSI 模型第 7 层上的应用层报文传输协议，在工业领域是一种通用的标准。目前常用的方式是基于串行链路的实现(Modbus RTU)和基于以太网上 TCP/IP 技术的实现(Modbus TCP/IP，简称 Modbus TCP)。

收稿日期：2018-11-30
* 基金项目：工信部 2016 年智能制造综合标准化与新模式应用专项“电子信息产品智能工厂/数字化车间物流综合标准化及试验验证”项目资助

Modbus 协议应用广泛,但是 Modbus 协议应用层设计存在缺陷,主要是缺乏认证、授权和加密等安全机制,由于报文使用明文传输,容易进行捕获并解析。参考目前 Modbus TCP 安全有效的研究[9-12],一种是根据已知攻击特征匹配网络中的通信流量,这种方式具有误报率较低的特性,但由于工控系统攻击行为特征库不可能包含所有的攻击行为,因此容易产生漏报的情况。另一种是建立在工业控制系统本身通信流量具有简单固定的通信模式的基础之上,通过建立系统正常行为的轮廓模型识别出异常的流量,这种方式能够探测出未知特征的攻击行为甚至操作人员的误操作,缺点是容易出现误警现象。目前比较流行的是基于 Modbus 协议深度解析方法和通讯安全规则模型,但是缺少工艺关系的监测,并且对工业控制系统的通信的实时性和可靠性造成影响。在实际的工业控制系统中,数字量一般代表线圈和保持寄存器,篡改某一个线圈的数值会使得本来应该处于闭合状态开关打开,这样会对工业控制系统将会造成很严重的后果。此外,某些工艺要求两个阀门同时打开或者一个打开另一个必须关闭,如果只对一个阀门操作,也会造成严重的工业事故。

根据以上研究基础,针对工控系统中网络攻击的特征,以及在大多数现场环境不能新增装置的情况,采取从交换机的镜像端口获取网络报文,通过配置策略对数据进行检测,采用网络防火墙原理,对控制网络和现场设备的未授权访问进行报警,并在此基础上,根据 Modbus 协议报文的应用层数据包进行协议分析以及深度检测,通过配置策略采用边界法对关键 Modbus 数据进行监测。实现了基于工艺关系的安全监视策略,识别其中的危险报文,产生相对应的报警信息。安全监视器原理如图 1 所示。

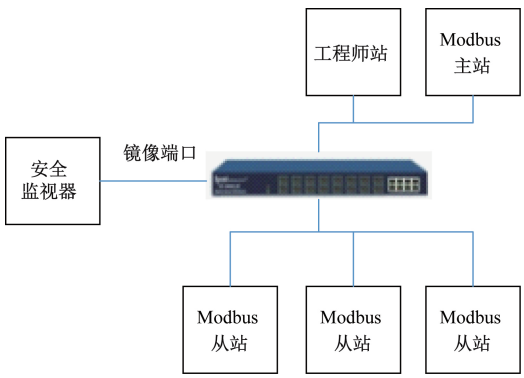


图 1 安全监视器原理

## 2 功能设计

根据网络攻击的行为以及安全防护的原理将安全监视器划分为如下 4 个模块[13]:安全策略配置模块、网络层解析模块、Modbus 模块和报警模块。

1)安全策略配置模块

安全策略配置模块是安全监视器的核心模块,此模块关系到整个系统进行安全监视的成败,用户根据实际情况通过配置安全策略,对关键系统进行监视。此模块可以保存配置的安全策略,并在系统运行中解析更新安全策略。

2)网络层解析模块

网络层解析模块是前端预处理模块,基于对 IP 封包初步解析,基于配置的安全策略,当监测到非法报文以及异常报文时实时进行报警处理。

3)Modbus TCP 模块

Modbus TCP 模块也是安全监视器的核心模块,针对 Modbus TCP 协议进行深度解析[14-15],识别其中的功能码以及关键数据,基于边界算法对关键数据进行处理,对超出边界的数据进行报警;基于工艺关系的配置策略对数据进行处理,对不符合工艺要求的命令进行报警。Modbus TCP 报文结构如图 2 所示,由 MBAP(Modbus 应用协议)和 PDU(协议数据单元)构成。MBAP 报文结构如表 1 所示。

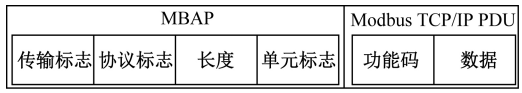


图 2 ModbusTCP 报文结构

**表 1 MBAP 报文结构表示**

| 区域 | 长度/Byte | 描述 | 客户端与服务器 |
|---|---|---|---|
| 传输标志 | 2 | 请求和响应传输过程中序列号 | 客户端生成,服务器应答时复制该值 |
| 协议标志 | 2 | Modbus 协议默认为 0 | 客户端生成,服务器应答时复制该值 |
| 长度 | 2 | 剩余部分的长度 | 客户端请求时生成,服务器应答时生成 |
| 单元标志 | 1 | 从机标志(从机地址) | 客户端生成,服务器应答时复制该值 |

4)报警模块

报警处理模块主要功能实时显示报警信息,并给出处理建议,报警模块主要由报警时间、报警设备、报警级别、报警内容以及处理建议构成。系统整体架构如图 3 所示。

## 3 系统实现

### 3.1 安全策略配置

安全策略主要功能是将配置信息保存到文件系统,当系统运行时将配置策略读取到内存,系统根据此配置策略进行相应的处理。配置策略主要分为 4 部分:第 1 部分是设备基本信息,包括设备 MAC 地址、IP、端口号,通过这些信息确定被保护的设备;第 2 部分是网络流量信息,由单位时间内通过报文个数和单位时间内报文流量构成;第 3 部分是网络层信息,主要包括 IP 白名单、MAC 地址白名单以

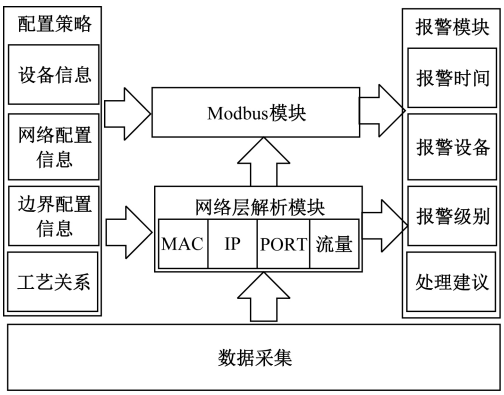


图 3　系统架构

及 IP 与 MAC 绑定；第 4 部分是 Modbus 安全策略，主要是数据超限以及工艺关系配置策略。

### 3.2　网络层解析模块

网络层解析模块基于安全策略对 IP 封包进行解析，首先解析目的 MAC 地址，如果目的地址在安全策略表，加载对应的安全策略，根据安全策略对 MAC 地址、IP 地址以及协议类型进行检验，对不符合安全策略的报文以及校验失败的异常报文进行报警，通过报警模块上传报警信息。

### 3.3　Modbus TCP 模块

Modbus TCP 模块主要由以下 3 个模块构成：

1）Modbus TCP 报文解析：识别 Modbus TCP 报文，并深入解析识别具体类型 Modbus TCP 报文；

2）Modbus 数据监视：根据配置策略，对设备的关键数据采用边界法进行监视，超出范围进行报警处理；

3）Modbus 工艺关系监视：根据配置策略，对关键数据进行监测，当操作不符合工艺关系时进行报警。

### 3.4　报警功能

报警功能主要是根据配置策略，将其他模块产生的报警进行显示，根据功能划分，报警内容如表 2 所示。系统防护策略流程如图 4 所示。

**表 2　报警内容**

| 报警模块 | 内容 |
|---|---|
| 网络层解析模块 | 非法访问，XX 不在 MAC 名单 |
| | 非法访问，XX 不在 IP 名单 |
| | 非法访问，IP 与 MAC 绑定不符 |
| | 流量异常，限定流量为：XX，当前流量： |
| | 畸形报文 |
| Modbus 模块 | 非法操作，数据超限，数据范围：当前： |
| | 非法操作，工艺关系错误，限定关系：，当前： |

## 4　工具仿真验证

根据安全监视器的功能，采用 Modbus 仿真软件进行

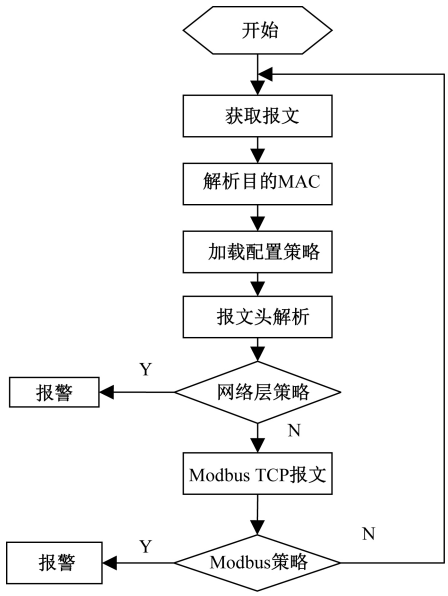


图 4　系统防护策略流程

功能验证。选两台测试主机，一台模拟主站，一台模拟从站，分别安装主流的 Modbus 仿真软件，主站采用 Modbus Poll V6.3.1，从站采用 Modbus Slave V6.2.0，交换机采用带有镜像端口功能的西门子工业交换机 Scalance X204IRT，网络拓扑图如 5 所示。

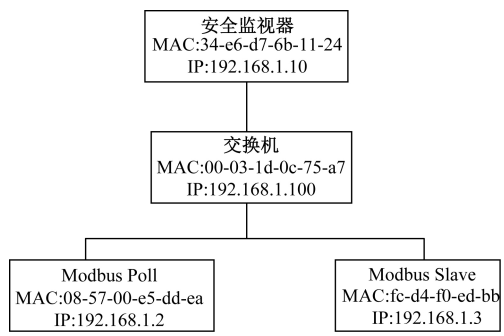


图 5　测试网络结构

实验验证主要分为两部分进行，每个测试项都进行 100 次测试，并统计报警结果。第 1 部分是网络正常测试，首先配置主站 Modbus Poll 与从站 Modbus Slave 通信，主站可正常读取从站数据。将 Modbus Slave 作为监视设备，增加到安全监视器中，并将主站 Modbus Poll 的相关信息如 IP、MAC 等添加到安全监视器的白名单中，启动安全监视器，此时，主站可正常读写从站数据，安全监视器无报警信息。第 2 部分是异常防护测试，首先进行网络层防护报警，将主站信息在安全监视器的白名单中移除，当主站读取从站数据时，安全监视器发出相应的报警信息。然后进行 Modbus 数据边界测试，配置 Modbus 数据边界，寄存器支持的数据类型如表 3 所示。

**表 3 支持的数据类型**

| 编号 | 数据类型 |
|---|---|
| 1 | Uint8 |
| 2 | Int8 |
| 3 | Uint16 |
| 4 | Int16 |
| 5 | Uint32 |
| 7 | Int32 |
| 8 | Float |

主站发起写寄存器指令,当数据访问超限,安全监视器发出相应的报警信息。最后是 Modbus 工艺关系测试,首先配置 Modbus 线圈对应关系,如线圈地址 1 与地址 5 必须同时写入值 1,主站发起写线圈指令,当只写单个线圈或者多个线圈时,由于不符合工艺关系,安全监视器发出相应报警信息。测试内容及结果如表 4 所示。

**表 4 测试内容及结果**

| 编号 | 测试项 | 报警内容示例 | 成功率/% |
|---|---|---|---|
| 1 | MAC 白名单 | 非法访问,MAC-085700E5DDEA 不在 MAC 名单 | 100 |
| 2 | IP 白名单 | 非法访问,IP-192.168.1.2 不在 IP 名单 | 100 |
| 3 | IP 与 MAC 绑定 | 非法访问,IP-192.168.1.2 与 MAC-085700E5DDEA 绑定不符 | 100 |
| 4 | 网络流量报文个数 | 流量异常,限定流量:10 个/s,当前流量:11 个/s | 100 |
| 5 | 网络流量负载 | 流量异常,限定流量为:1 Mbps,当前超限 | 100 |
| 7 | Modbus 数据边界 | 非法操作,数据超限,配置数据范围:10～20,当前值:30 | 100 |
| 8 | Modbus 工艺关系 | 非法操作,工艺关系错误,地址 1～5,限定关系为:相同,当前写入值相反 | 100 |

通过以上的测试实验结果分析,安全监视器对正常的工业网络通信无影响,网络可正常通信;通过配置安全策略,当有设备非法访问时,可以实时监测并给出具体非法设备信息,当现场工程师更改设备数据时,如果未在合理区域内修改或者不符合工艺流程,安全监视器将会实时给出报警警示,以防止造成不必要的损失或者严重事故。安全监视器可实时产生报警信息,没有误报信息产生,对关键的数据及工艺流程进行了合理监控,达到了预期效果。系统报警界面如图 6 所示。

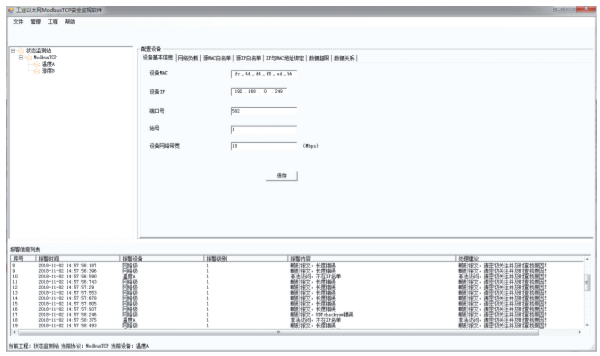

图 6 系统报警界面

## 5 结 论

工业以太网 ModbusTCP 安全监视器实现了网络层以及应用层的安全监视,可针对目前主流的病毒攻击进行安全报警,并深入 Modbus 应用层,提出并应用了基于工艺关系的安全防护,该系统配置简洁清晰,安全监视切入实际场景,仿真实验验证了改方案的有效性。但是防护策略需要依赖于现场的工程人员根据实际场景配置,不了解工艺的人员配置时容易产生误报警,后续需要进一步进行安全防护测试以及网络系统的稳定性测试,对工业控制系统网络安全具有重要意义。

## 参考文献


[1] 谢素芬,刘丹.工业控制网络通用技术要求[J].中国仪器仪表,2017(4):19-22.

[2] 尚文利,安攀峰,万明,等.工业控制系统入侵检测技术的研究及发展综述[J].计算机应用研究,2017,34(2):328-333,342.

[3] 李小强,陈涤新.工业控制网络系统安全防护的思考[J].制造业自动化,2017,39(6):140-144.

[4] 蒋宁,林浒,尹震宇,等.工业控制网络的信息安全及纵深防御体系结构研究[J].小型微型计算机系统,2017,38(4):830-833.

[5] 冯涛,鲁晔,方君丽.工业以太网协议脆弱性与安全防护技术综述[J].通信学报,2017,38(S2):185-196.

[6] 张建伟.企业局域网的网络安全问题解析[J].电子测量技术,2018,41(7):69-74.

[7] 徐丽娟,许静,唐刚.工业控制系统网络安全隐患分析方法研究[J].电子科学技术,2015,02(6):679-684.

[8] 朱建军,安攀峰,万明.工控网络异常行为的 RST-SVM 入侵检测方法[J].电子测量与仪器学报,2018,32(7):8-14.

[9] 周兵,李娜.基于 MODBUS/TCP 协议桥梁监测系统的电力监控设计[J].电子测量技术,2010,33(9):126-129.

[10] 万明,尚文利,曾鹏,等.基于功能码深度检测的

Modbus/TCP 通信访问控制方法[J].信息与控制,2016,45(2):248-256.

[11] 伊胜伟,张翀斌,谢丰,等.基于 Peach 的工业控制网络协议安全分析[J].清华大学学报(自然科学版),2017,57(1):50-54.

[12] 张盛山,尚文利,万明,等.基于区域/边界规则的 Modbus TCP 通讯安全防御模型[J].计算机工程与设计,2014,35(11):3701-3707.

[13] 韩丹涛,赵艳领,闫晓风.工业以太网 PROFINET 安全隔离器的设计[J].自动化仪表,2017,38(7):46-49,53.

[14] 全国工业过程测量和控制标准化技术委员会第四分技术委员会.基于 Modbus 协议的工业自动化网络规范第 1 部分:modbus 应用协议:GB/T 19582.1-2008[S].北京:中国标准出版社,2008.

[15] 全国工业过程测量和控制标准化技术委员会第四分技术委员会.基于 Modbus 协议的工业自动化网络规范第 3 部分:modbus 协议在 TCP/IP 上的实现指南:GB/T 19582.3-2008[S].北京:中国标准出版社,2008.

## 作者简介

**韩丹涛**,硕士、工程师,主要研究方向为工业网络控制与集成。

E-mail:handantao@tc124.com