毕业设计（论文）

题 目：面向可编程逻辑控制器的漏洞挖掘和攻击技术研究

# 摘要：工业控制系统（Industrial control system,ICS）工业控制系统 (Industrial Control System, ICS) 是对用于工业生产的控制系统和自动化控制组件的统称，包括监控与数据采集系统 (Supervisory Control and Data Acquisition, SCADA)、分布式控制系统 (DistributedControl System, DCS) 和可编程逻辑控制器 (Programmable Logic Controler, PLC)。ICS已经广泛用于工业、交通、能源、水利、安防、食品以及大型制造等行业，因此工业控制系统的网络安全与人民生命财产安全息息相关。其中PLC是ICS的核心部件，PLC控制着整个工业生产的每一个环节，并且任何环节出现失误都会造成严重的后果，对于PLC的安全研究和其固件的安全性分析具有重要意义。本文的主要内容如下：

1. 对当前所存在的PLC系统结构做简要的分析：
2. 介绍固件提取的几种技术：
3. 对M340进行固件的提取，并在上位机的角度，分析Control Expert软件和PLC的交互方式，分析M340的通信协议功能码，并尝试寻找通信协议实现过程中的漏洞，编写POC，并加以利用。

最后，对全文工作进行了总结，并指出了有待进一步研究的问题。

（**再写论文的时候一定要注意，当前的文章大标题是按照别人的写的，需要根据自己的实际情况进行补充和修改，不要简单的照搬复用**）

# 绪论

## 研究的背景及意义

当前经济社会发展迅速，各行各业信息化和智能化加速融合发展，保障涉及民生的工业领域方面的安全，对于稳定社会秩序、维护国家安全方面也是有着至关重要的作用。

1. 工业领域的信息安全事件频发

根据美国ICS-CERT收录的数据显示，自2010年震网事件以来， 全球工业领域发生的网络安全事件数量呈现逐年上升趋势。2017年5月，蠕虫病毒“WannaCry”入侵了全球150多个国家的信息系统， 多家汽车制造商被迫停产，能源与通信等重要行业损失惨重。2018年，台积电多个工厂及营运总部遭遇勒索软件攻击，导致在台湾北、中、南三处重要生产基地生产线停摆；某半导体厂商在中国大陆的生产基地遭受病毒 入侵而导致全线瘫痪；位于美国加州的Chevron石油公司网络系统和伊朗 核设施遭遇震网病毒攻击、乌克兰电厂因黑客攻击导致大面积停电。2019 年，委内瑞拉最大的电力设施古里水电站收到2次网络攻击，引发全国大面积停电；2020年，以色列供水设施突遭袭击，紧急停工更改密码；本田汽车遭受工业型勒索软件攻击，生产受阻；Model X被曝存中继攻击安全漏洞，特斯拉紧急推送修复不定等。以上事件均已说明工业领域的网络安全已成为全球课题，工业系统目标价值高，其安全系统的复杂程度远高于传统的IT网络系统，其风险来源多导致发生安全事件的后果也相当严重，安全形势十分严峻。（这一段的参考来源主要是[https://www.websaas.cn/typecho/news/usr/uploads/files/2021/06/09/[%E8%B5%9B%E8%BF%AA]%E5%B7%A5%E6%8E%A7%E5%AE%89%E5%85%A8%E5%8F%91%E5%B1%95%E7%99%BD%E7%9A%AE%E4%B9%A6%EF%BC%88202105%EF%BC%89\_563.pdf](https://www.websaas.cn/typecho/news/usr/uploads/files/2021/06/09/%5b%E8%B5%9B%E8%BF%AA%5d%E5%B7%A5%E6%8E%A7%E5%AE%89%E5%85%A8%E5%8F%91%E5%B1%95%E7%99%BD%E7%9A%AE%E4%B9%A6%EF%BC%88202105%EF%BC%89_563.pdf)）

1. 国家政策支持，工控安全市场将爆发发展

为加快推进工业互联网创新发展，加强对有关工作的统筹规划和政策协调，国家制造强国建设领导小组成立工业互联网专项工作小组，工业互 联网已上升至国家战略层面。2016年，国务院发布《关于深化制造业与互联网融合发展的指导意见》指出要强化信息技术产业支撑，充分释放“互 联网+”的力量，加快推动“中国制造”提质增效升级，实现从工业大国向工业强国迈进。2017年，国务院发布了《关于深化“互联网+先进制造业” 发展工业互联网的指导意见》，提出要加快发展工业互联网，构建网络、平台、安全三大功能体系，强化工业互联网安全保障。2018年，工信部开展工业互联网发展“323”行动，即打造网络、平台、安全三大体系，推进大型企业集成创新和中小企业应用普及两类应用，构筑产业、生态、国际化三大支撑。安全被提到了前所未有的高度，与网络、平台并列成为工业互联网的三大功能体系。工信部印发的《工业互联网发展行动计划（2018- 2020年）》中指出，以全面支撑制造强国和网络强国建设为目标，发展工业互联网平台体系，同步提升安全保障能力，初步形成有力支撑先进制造 业发展的工业互联网体系。此外，工信部还正加快编制工业信息安全标准体系建设指南，以及工业互联网安全保障技术体系方案。从政策推进上看，工业互联网已经成为未来产业的发展重点，前景非常广阔，工业互联网安全作为工业互联网发展中必不可少的安全保障，必然将随之得到快速发展。（也是上面的这个链接的直接引用部分）。

而PLC作为整个工业系统的核心，因此在保证PLC的安全性对于维护整个工控系统的安全方面有着非常重要的作用。就当前情况来看，当前PLC大多数是经过裁剪的实时操作系统，如LinuxRT、QNX、VxWorks等，这些系统也是以固件的形式存在被广泛应用到通信、军事等各个领域，由于历史和现实原因，工控设备中存在着大量的漏洞，虽然对于固件的漏洞挖掘不易，但一旦固件文件被提取、分析之后，便可以通过逆向分析获取漏洞、后门等，一旦固件漏洞被发掘并被证实可以利用后，便可能会造成工业系统的瘫痪，使得其难以修复。

本课题便基于施耐德M340 PLC展开分析，通过提取控制器中的固件和固件内容的分析，尝试挖掘PLC漏洞，为之后的固件漏洞挖掘打下必要的基础。

## 国内外的研究现状

## 当前固件分析存在的问题

在固件漏洞方面，PLC使用的操作系统存在较大安全隐患。由于工业控制现场实时性的要求, PLC采用的操作系统大多是经过裁剪的实时操作系统(RTOS), 比如 Linux RT、QNX、Lynx、VxWorks 等。嵌入式系统历来都会使用大量专有组件, 并没有与其他系统共享太多共同电路, 这意味着当发现漏洞时，由于成本或资源限制，漏洞修复难度较大。而且，PLC 的系统更新一般只能由生产厂商完成，因此其打补丁的过程就更加缓慢。这里漏洞挖掘与利用技术与传统软件漏洞挖掘利用方法并没有本质区别，所以学术界和业界的研究较为成熟。

## 本文主要工作及内容安排

本课题较为全面的梳理总结了当前针对PLC固件攻击的技术特点和一般流程，通过对于固件的提取和分析等过程，发掘M340可编程逻辑控制器的脆弱性及其利用方法，对于提升使用该设备的产业的网络安全具有直接促进作用，从个人角度来说，本课题能切实提高对PLC固件攻击技术的理解和应用能力，为以后的工作打下必要的基础。

# 当前PLC的系统结构

本节首先是从为了完成一次PLC功能的完整实现出发，自上而下将整个过程分为编程层、固件层以及硬件层三层对PLC的软硬件架构进行介绍，并对于其工作原理进行了简单的分析。接着，对于本次实验目标对象的M340 PLC的上位机编程工具Control Expert、固件层的Vxworks操作系统以及硬件层的模板分别进行介绍，以便为后续的漏洞挖掘和利用的相关工作更好的开展奠定基础。

## PLC的软硬件结构和工作过程

一款PLC设备为了能够正常的使用，需要上位机的编程工具用于编写实现特定功能的工程代码，在将项目上传到PLC之后便能够启动该项目用于控制PLC。

McMinn et al. 将PLC的运行层次分为了编程层、固件层、硬件层三层：（这里需要做出更改）

编程层主要是指编程人员进行交互的编程工具，从目前来看，各大厂商也有了自己配套的全集成编程软件，用于实现工程的编写而是先对于PLC的控制逻辑的控制。而就开发语言而言，除了C和Basic这些传统的编程语言外，还有梯形图（LD）、指令表（IL）、功能模块图（FBD）、顺序功能流程图（SFC）、及结构化文本（ST）等国际电工委员会制定PLC编程支持的语言，分别用于满足不同行业人员快速的编程和部署。

由于PLC固件本身研究的困难性，有一些针对PLC的安全性的研究便是通过编程工具入手，通过对于编程工具的分析，可以得到私有协议功能码、设备信息等，并可以通过更改工程内容实现对于设备控制流的控制，在著名的震网病毒事件中，攻击者就利用了西门子编程软件WinCC的漏洞以辅助攻击。

固件层运行在硬件之上，是整个PLC的核心，通常存储在只读存储器（ROM）上，虽然固件中非常重要的部分就是运行在PLC上的操作系统，但是固件中还包含引导程序等。在ARM、PowerPC、MIPS、Pentium等不同的架构之上，因为场景的需要，所以更多的是搭配着实时操作系统（RTOS），主要有LinuxRT、Vxworks、QNX等。在现实情况中，为了减少固件的体积，也会对固件进行压缩，常用的压缩算法有

固件层由于控制着整个设备的运行，所以该层的安全性是否很大程度上决定了整个设备的安全性，对照目前PC端的攻击手段而言，仿照传统计算机中使用Rootkit等手段实现操作系统的提权访问，实现身份的隐藏、信息的窃取，如果能够在PLC固件中也能实现这样的目的，便也能够是实现获取设备数据、篡改设备行为，以达到完全控制设备。而由于整个行业开始的时间比较早，一些设备中使用的是老旧的固件，有些甚至不能够升级，固件中必然存在着不少的漏洞，在拿到固件本身后，可以利用传统的手段对固件进行漏洞的挖掘和利用；而目前包括PLC在内的多种嵌入式设备提供在线下载升级的机制，为供应商和用户提供了便利，但同时也为攻击者提供了攻击的渠道，让可能经过篡改的固件进入到设备中从而造成安全问题。

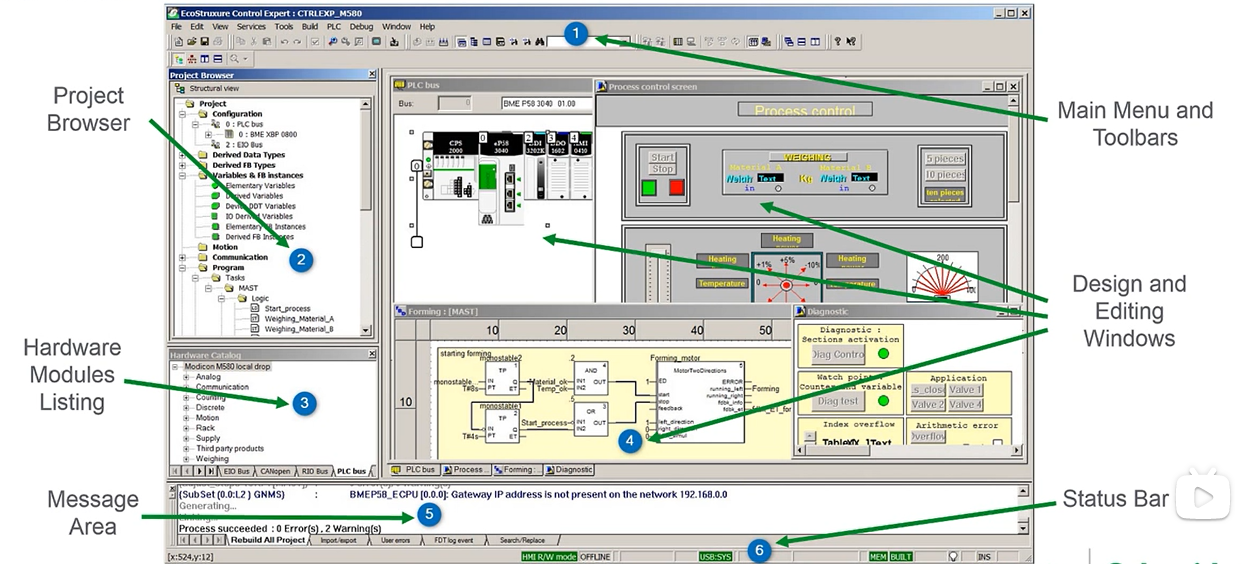
硬件层即为设备本身，就一般而言，PLC的硬件主要由中央处理器（CPU）、存储器、输入/输出单元、底板及机架模块、通信接口、扩展接口电源等部分组成。其中CPU主要功能就是执行用户程序，控制程序运行的逻辑；存储器主要存储用户程序，有的还为系统提供辅加的工作内存；输入/输出单元集成了I/O电路，并依点数及电路类型划分为不同规格的模块，主要是分为连续性和离散型两种；底板及机架模块为PLC各模块的安装提供基板，并为模块间地联系提供链路；通信接口的存在使得PLC可以与计算机或者是PLC等进行通信，还可以与其他一些控制部件组成局部网络，代表了PLC的组网能力，是PLC性能的一个重要的方面。

而对于硬件而言，常见的攻击手段主要是通过侧信道、固件篡改和供应链攻击。（这里需要补充）

## 对于M340的分析介绍

对于本次实验的研究目标施耐德M340这款设备，其是施耐德电气向全球推出的高性能中端PLC平台，以其稳定可靠的性能优势，极高的经济性等特点，适用于中小型项目、复杂机械及过程装备，在全球范围内获得了广泛成功。

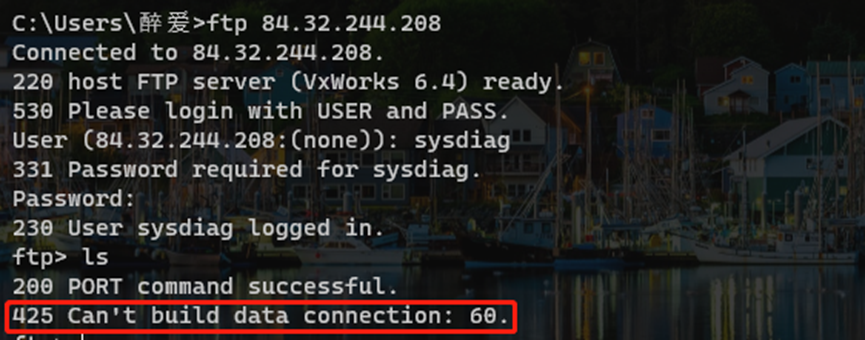
### 编程层

在编程层上来说，该设备使用的编程软件为EcoStruxure Control Expert（原名Unity Pro），是一个完整的控制和自动化系统从设计到调试、操作和维护的整个生命周期的一体化编程软件平台。

主要是具有下面的一些特点：

1. 可以使用多种编程语言进行编程，支持国际电工委员会制定PLC编程支持的全部五种语言；

### 固件层

固件通常由bootloader、内核、根文件系统及其他资源组成。在固件层面上，M340使用的是Vxworks操作系统，而这一款操作系统也是被广泛使用的一款非常成熟的RTOS，下面是对于Vxworks操作系统的介绍：

（这里需要对于个人信息隐掉）

* + - 1. Bootloader
      2. 内核
      3. 根文件系统

VxWorks是美国风河系统（WindRiver）公司于1983年设计开发的一种嵌入式实时操作系统（RTOS），是嵌入式开发环境的关键组成部分。凭借良好的持续发展能力、高性能的内核以及友好的用户开发环境，其在嵌入式实时操作系统领域占据一席之地。

VxWorks支持几乎所有现代市场上的嵌入式CPU，包括x86系列、MIPS、 LoongISA、 PowerPC、Freescale ColdFire、Intel i960、SPARC、SH-4、ARM, StrongARM以及xScale CPU。

它以其良好的可靠性和卓越的实时性被广泛地应用在通信、军事、航空、航天等高精尖技术及实时性要求极高的领域中，如卫星通讯、军事演习、弹道制导、飞机导航等。美国的F-16、F/A-18战斗机、B-2隐形轰炸机和爱国者导弹，火星探测器如1997年7月登陆的火星探测器，2008年5月登陆的凤凰号、2012年8月登陆的好奇号都使用到了VxWorks。（这一块是Wikipedia的引用）

在Vxworks的组成上，主要是分为了几大部分，

### 硬件层

在硬件层面上，M340设备使用的是供电单元为BMX CPS2000，使用的CPU为BMX P342020，其中MCU的具体型号为Atmel旗下的ARM芯片AT91AM9200-CJ-101，使用机架型号为BMX XBP0800，同时使用了四个输入输出单元，分别是BMX DDI1602(离散型输入信号)、BMX DDO1602(离散型输出信号)、BMX AMI0410(连续型输入信号)、BMX AMO0410(连续型输出信号)

## PLC芯片种类及其介绍

## Vxworks操作系统简介

VxWorks是美国风河系统（WindRiver）公司于1983年设计开发的一种嵌入式实时操作系统（RTOS），是嵌入式开发环境的关键组成部分。凭借良好的持续发展能力、高性能的内核以及友好的用户开发环境，其在嵌入式实时操作系统领域占据一席之地。

VxWorks支持几乎所有现代市场上的嵌入式CPU，包括x86系列、MIPS、 LoongISA、 PowerPC、Freescale ColdFire、Intel i960、SPARC、SH-4、ARM, StrongARM以及xScale CPU。

它以其良好的可靠性和卓越的实时性被广泛地应用在通信、军事、航空、航天等高精尖技术及实时性要求极高的领域中，如卫星通讯、军事演习、弹道制导、飞机导航等。美国的F-16、F/A-18战斗机、B-2隐形轰炸机和爱国者导弹，火星探测器如1997年7月登陆的火星探测器，2008年5月登陆的凤凰号、2012年8月登陆的好奇号都使用到了VxWorks。

# 固件提取技术和分析技术

从整个固件提取和分析的链条来看，首先需要获取到PLC的固件本身，然后对于固件进行解压缩提取，最后才是对于固件功能的分析。

## 获取固件的方式

就目前来说获取固件的方式和方法主要是由下面几种：

1. 通过官网或者是联系售后获取升级包
2. 在线升级，抓包获取下载地址并组装
3. 通过硬件电路的调试串口和固件的bootloader获取固件
4. 通过硬件调试接口获取固件
5. 通过编程器直接读取Flash芯片，读取固件内容

## JTAG调试原理

## FLASH固件提取技术

# M340固件提取和分析

# 攻击测试

## 重放攻击

## 工程文件口令获取

# 总结

# 致谢

# 参考文献

1. C. -T. Lin, S. -L. Wu and M. -L. Lee, "Cyber attack and defense on industry control systems," 2017 IEEE Conference on Dependable and Secure Computing, 2017, pp. 524-526, doi: 10.1109/DESEC.2017.8073874.