物联网安全课程实验报告

实验一

实验名称：“工控网络安全移动实验箱”安全需求分析

姓名：_____郭裕彬_____

小组：_____

学号：_____2114052_____

专业：_____物联网工程_____

提交日期：_____2023.09.16_____

一、实验目的

通过工控实验箱了解工控系统基本工作原理，并对其进行安全需求分析。

二、实验要求及要点

根据对这套工控系统的了解及所学知识，单独撰写实验报告。

1. 基于实验箱，总结工控系统工作基本原理

通过实验，借助试验箱可以将工控系统划分为数据采集、数据处理、设备控制等方面。以储水罐工业系统为例，有物理按键和触屏按钮两种设备控制方式，用于控制储水罐上方入水口和下方排水口的开闭；储水罐中安装有传感器以检测罐中的水量，通过显示屏以直观刻度和数值表示两种方式显示；对于传感器获取到的数据，通过自定义函数的方式对其进行处理，在数值高于高报警限制或低于低报警限值时控制显示屏做出报警的显示。

2. 针对此试验箱模拟的工业控制环境，进行安全需求与风险分析

以储水罐工业系统为例，受到监控和控制的设备主要包括水量传感器、水口阀门和中控系统，要求传感器获取到的数据是真实准确的、阀门能够正常响应开关操作、中控系统报警逻辑的设置是正确的。传感器受到攻击，导致传出的测量数据遭到恶意修改、阀门由于物理或控制线路的异常而不能正常开闭、中控系统程序被恶意控制等情况的出现都是储水罐工业系统存在的风险。

抽象而言，对于工业控制环境的安全需求和风险分析，要从环境中存在的组件、设备和实现的功能入手，结合实际章程制度、行业规范、法律法规等的具体要求，明确系统必须满足的安全需求。要识别系统中所有可能的危险源，对其进行风险模拟和评估，从而制定相应的风险控制措施，提升系统的可靠性和安全性。

三、实验内容

了解工控系统的一般使用过程

1. 阅读纸质实验教程（HMI 类）P1-P12，了解 HMI 及其配置过程
2. 阅读纸质实验教程（PLC 类）P1-P18，了解 PLC 及其编程过程

3. 根据实验教程配置 HMI（一般默认已经配置好，无需更改）

4. 储水罐功能演示

a) 在 HMI 屏幕上点击“储水罐”

b) 按 SH1 按钮，观察储水罐蓄水流程

c) 按 SH2 按钮，观察储水罐停止蓄水流程

d) 使用触屏重复上述操作

e) 触屏点击“打开”/“关闭”，阀门开启/关闭排水

f) 观察储水罐报警功能，SH3 为指示灯

工控系统开发过程

1. 下载安装 STEP 7-MicroWIN SMART 软件，

2. 用网线连接电脑与试验箱

3. 配置电脑的 IP 地址，使其能与 PLC 通信

a) 配置 IP:“网络和 Internet 设置”——更改适配器选项——右键点击对应的网络接口——属性——IPV4

b) 电脑 IP 地址设置为 192.168.1.127，子网掩码 255.255.255.0，网关 192.168.1.1。

c) 使用命令行 ping PLC 地址 192.168.1.3 以确保联通。

4. 将对应的储水罐程序重新下载至 PLC 中运行

a) 打开 PLC.smart 文件

b) 点击窗口上面的“下载”

c) 选择相应的通信接口（网卡），自动查找 PLC

d) 在弹出的窗口点击“下载”

e) 结合阅读的实验教程手册，理解该系统开发过程

实验结果

按下 SH1 或点击显示屏上的启动按钮，储水罐开始进水，水位和水量数值的显示开始上升；按下 SH2 或点击显示屏上的停止按钮，储水罐停止进水，水位和水量数值停止变化。点击显示屏上的打开按钮，储水罐开始出水，水位和水量数值开始下降；点击显示屏上的关闭按钮，储水罐停止出水，水位和水量数值停止变化。修改了储水罐的高报警限值从 0.8 至 0.7，当储水罐水量超过高报警限值或低于低报警限值时，显示屏显示对应的报警信息，同时 SH3 指示灯亮。

使用 STEP 7-MicroWIN SMART 软件进行工控系统开发，连接 PLC 后下载已编好的 smart 文件，停止运行 CPU 后，实验箱对物理按键不能做出反应，显示屏能够切换模拟的不同程序，但也不能对程序中的触屏操作做出反应，实验箱下方的 PLC 物理件左侧指示灯全黄，CPU 指示灯全灭；重新运行 CPU 后，系统恢复正常。

遇到的问题

1. 计算机使用 STEP 7-MicroWIN SMART 时无法通过选择通信接口来自动识别到 PLC 的 CPU：

在正确的通信接口下选择手动添加 CPU，设置 IP 地址为 192.168.1.3，子网掩码 255.255.255.确定后即可正常连接。

2. 计算机使用扩展网口时无法正确识别接口：

确定是由于扩展网口套娃插入在前一个扩展坞导致的，将扩展网口直接接入到笔记本 USB 或 Type-C 接口即可。

四、回答问题

1. （模拟）储水罐工业控制系统具有什么报警功能？

具有检测储水罐储水量超出或低于某阈值时进行报警的功能。

2. 为什么实验箱设计了触屏操作和物理按键两种控制储水功能的操作方式？

分别针对不同的实际使用场景，物理按键可以设置在设备所处环境中，适应厂房中的较恶劣环境，以安全性和稳定性来保证紧急情况下的操作成功；触屏操作可以集成在系统总控室等远程控制环境中，用于集成度和用户友好性要求高的日常使用环境中。此外，两种控制方式的存在也可以保证在其中一种方式异常时另一种方式能正常控制系统。

五、收获感悟

认识了工业控制系统在实际生产过程中的各个部分，基本了解了实验箱的操作方式有。通过阅读实验文档，接触到了 HMI 和 PLC 的相关理论，对于新的编程语言有了形式上的认知。工控系统由于其环节的繁杂和涉及设备的多样性，要全面保障系统安全较为困难，需要对系统的各个方面进行立体的安全分析和风险检测。