*启用前绝密

2022 年 CIMC“西门子杯”中国智能制造挑战赛

智能制造工程设计与应用类赛项-信息化网络化方向

初赛 任务二：工业网络现场实施赛题

2022 年 9 月

说明：该题目用后需要回收并重复使用，请保持页面干净整洁。

一、工厂网络描述

工厂网络拓扑结构如图 1 所示。工厂包含两个工艺单元，工艺单元 A 与工艺单元 B 中各有一个 PLC 用于控制工艺单元内部生产加工操作。工艺单元 A 中 PLC 通过交换机接入生产主干环网。工艺单元 B 中考虑 PLC 信息安全，将 PLC 的 IP 地址进行转换后，经无线模块接入主干环网。控制中心的工程师站能够对工艺单元 A 中的 PLC 的变量进行在线监视。远程维护主机能够在 WEB 界面中使用 IP 地址+端口号方式访问工艺单元 B 中的 PLC。

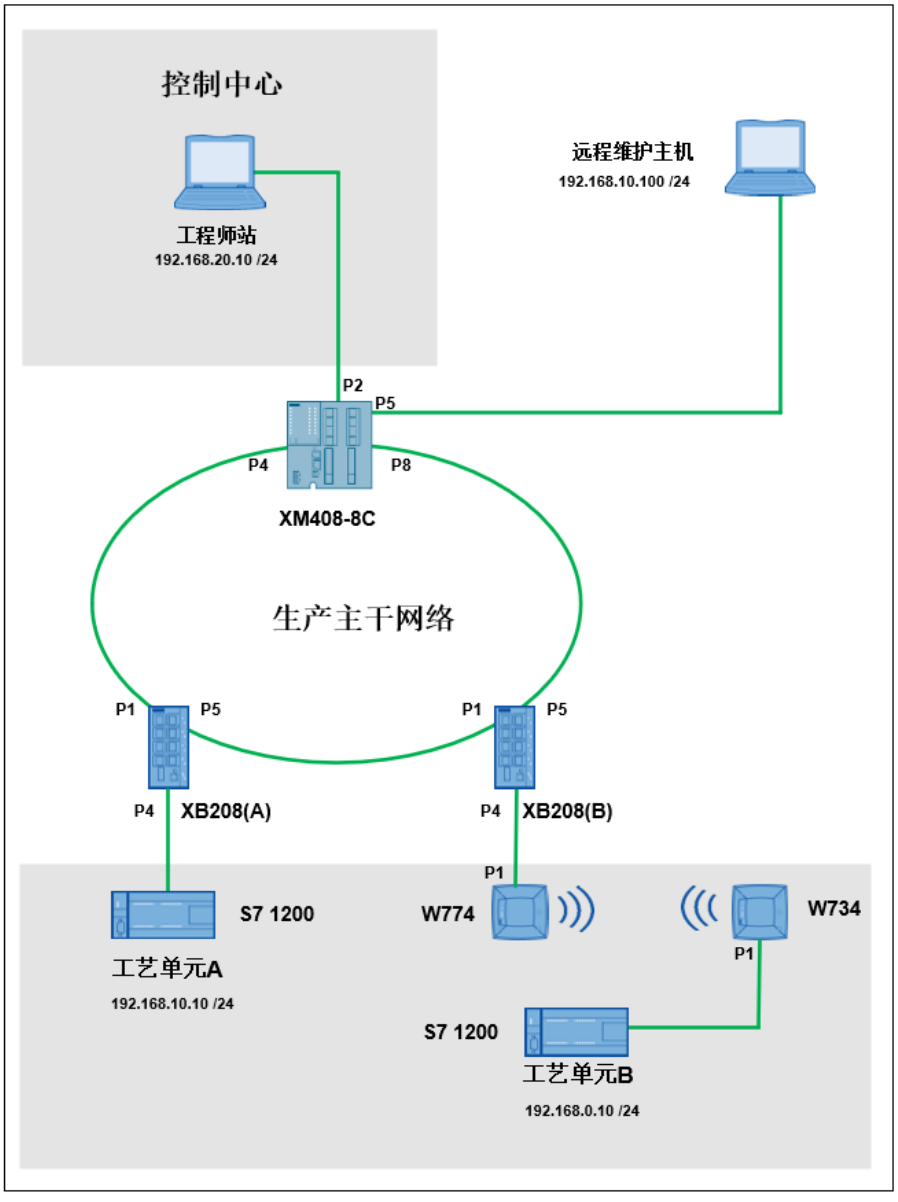

图 1 网络拓扑结构图

二、任务要求

1、工艺单元任务

（1） 将工艺单元 A S7 1200 的 IP 地址设置为 192.168.10.10/24。

（2） 将工艺单元 B S7 1200 的 IP 地址设置为 192.168.0.10/24。

（3） 工艺单元 A 与工艺单元 B 都属于 VLAN10。

（4） 在工艺单元 A S7 1200 的“默认变量”表中添加 1 个变量，说明如下：

名称	数据类型	地址	与“工艺单元”的操作面板对应关系	说明
加工	Bool	%I0.*	对应 DI *开关 (操作面板 A 正常工作开关)	拨动开关，“加工”变量取值为 TRUE 时，代表开始加工；取值为 FALSE 时，代表停止加工。
☆☆☆：I0.* 对应设备中操作面板 A 中 DI *开关（请根据《竞赛设备清单》选择设备操作面板 A 中能中正常工作的开关）				

（5） 在工艺单元 B S7 1200 的“默认变量”表中添加 1 个变量，说明如下：

名称	数据类型	地址	与“工艺单元”的操作面板对应关系	说明
加工指示灯	Bool	%Q0.*	对应 DQ *指示灯 (操作面板 B 正常工作指示灯)	该变量值来自于工艺单元 A 中的“加工”变量，取值为 True，指示灯亮，代表收到“加工”的消息；取值为 False，指示灯灭，代表没有收到此消息。
☆☆☆：Q0.* 对应设备中操作面板 B 中 DIQ*指示灯（请根据《竞赛设备清单》选择设备操作面板 B 中能正常工作的指示灯）				

（6） 两个工艺单元之间可以相互交互。

2、配置工业无线网络

配置工艺单元到生产主干环网的无线网络：配置 SCALANCE W774 和 W734，SCALANCE W774 作为无线接入点，SCALANCE W734 作为无线客户端。

为确保 PLC 信息安全，需使用 NAT 技术将工艺单元 B 中 S7 1200 的 IP 地址转换为 192.168.10.11。

使用 NAPT 技术允许远程维护主机**使用 IP 地址+端口号**的方式访问工艺单元 B S71200 的 WEB 界面，实现对工艺单元 B S7 1200 的状态监控。

3、构建生产主干网络

配置交换机 SCALANCE XM408-8C 和两个 SCALANCE XB208，使得三个交换机能够形成环形冗余网络，其中 SCALANCE XM408-8C 交换机作为冗余管理器，P4 (web 配置界面 1.4)和 P8 (web 配置界面

1.8)端口作为冗余端口；两个 SCALANCE XB208 的 P1 和 P5 端口作为冗余端口。

4、控制中心功能配置

（1）工程师站 IP 地址为 192.168.20.10/24。

（2）配置控制中心的 SCALANCE XM408-8C 交换机。

VLAN 功能：P2 (web 配置界面 1.2)端口属于 VLAN 20，P5 (web 配置界面 1.5)端口属于 VLAN 10。其余端口自定义。VLAN 10 属于 192.168.10.0/24 网络， VLAN 20 属于 192.168.20.0/24 网络。

路由功能：配置路由功能，使得 VLAN 10、VLAN 20 之间可以通讯。

ACL 功能：

仅允许 IP 地址为 192.168.20.10 的工程师站接入 XM408-8C 的 P2 (web 配置界面 1.2)端口访问远程维护主机和工艺单元 A 中 S7 1200。

仅允许 IP 地址为 192.168.10.100 的远程维护主机接入 XM408-8C 的 P5 (web 配置界面 1.5)端口访问工艺单元 A 中 S7 1200。

仅允许 IP 地址为 192.168.10.100 的远程维护主机接入 XM408-8C 的 P5 (web 配置界面 1.5)端口使用 **IP 地址：端口号**访问工艺单元 B 中的 S7 1200。

5、远程维护主机功能

（1）远程维护主机 IP 地址为 192.168.10.100/24。

（2）远程维护主机可以使用 **IP 地址：端口号**的方式访问工艺单元 B 中的 S71200 的 WEB 界面。

任务三：数据抓包分析（共 20 分，**请在任务二搭建的网络架构上完成任务三**）

请在边裁提供的“数据抓包分析”word 文档中作答，答题结束，将**word 文档及导出的数据包文件（数据包保存格式. pcapng）**提交裁判； 提交时 word 文档命名：**任务三数据抓包分析_X 组 X 号_队伍编号，数据包文件命名：任务三数据抓包分析_X 组 X 号_队伍编号**

序号	评分项	具体描述	所占分值
1	抓包工具使用	（截图张贴区）	2
		使用抓包工具抓取**工艺单元 A 与工艺单元 B S7 1200 间通讯数据包**，并将整个抓取到数据包的工具窗口截图，粘贴在上方的**“截图张贴区”**	
2	工艺单元 A 发送给工艺单元 B 数据包分析	（截图张贴区）	2
		从抓取的数据包中筛选出由**工艺单元 A 发送给工艺单元 B** 的数据包，并打开数据包，找到源 IP 地址与目的 IP 地址区域，截图并粘贴在上方的**“截图张贴区”**并将源 IP 地址与目的 IP 地址填在下方： **（若上图“截图张贴区”截图不得分，则此项也不得分）** **源 IP：　　目的 IP：**	1

序号	评分项	具体描述	所占分值
2	工艺单元 A 发送给工艺单元 B 数据包分析	（截图张贴区）	2
		从抓取的数据包中筛选出由**工艺单元 A 发送给工艺单元 B** 的数据包，并打开数据包，找到源 MAC 地址与目的 MAC 地址区域，截图并粘贴在上方的**“截图张贴区”**并将源 MAC 地址与目的 MAC 地址填在下方： **（若上图“截图张贴区”截图不得分，则此项也不得分）** **源 MAC：　　目的 MAC：**	1
3	工艺单元 B 发送给工艺单元 A 数据包分析	（截图张贴区）	2
		从抓取的数据包中筛选出由**工艺单元 B 发送给工艺单元 A** 的数据包，并打开数据包，找到源 IP 地址与目的 IP 地址区域，截图并粘贴在上方的**“截图张贴区”**并将源 IP 地址与目的 IP 地址填在下方： **（若上图“截图张贴区”截图不得分，则此项也不得分）** **源 IP：　　目的 IP：**	1

附录——竞赛设备说明

1、 如图 2 所示:

模块下方的“控制中心”、“工艺单元”和“主干环网”标签分别代表该模块属于“控制中心网络”、“工艺单元网络”和“主干环网”。

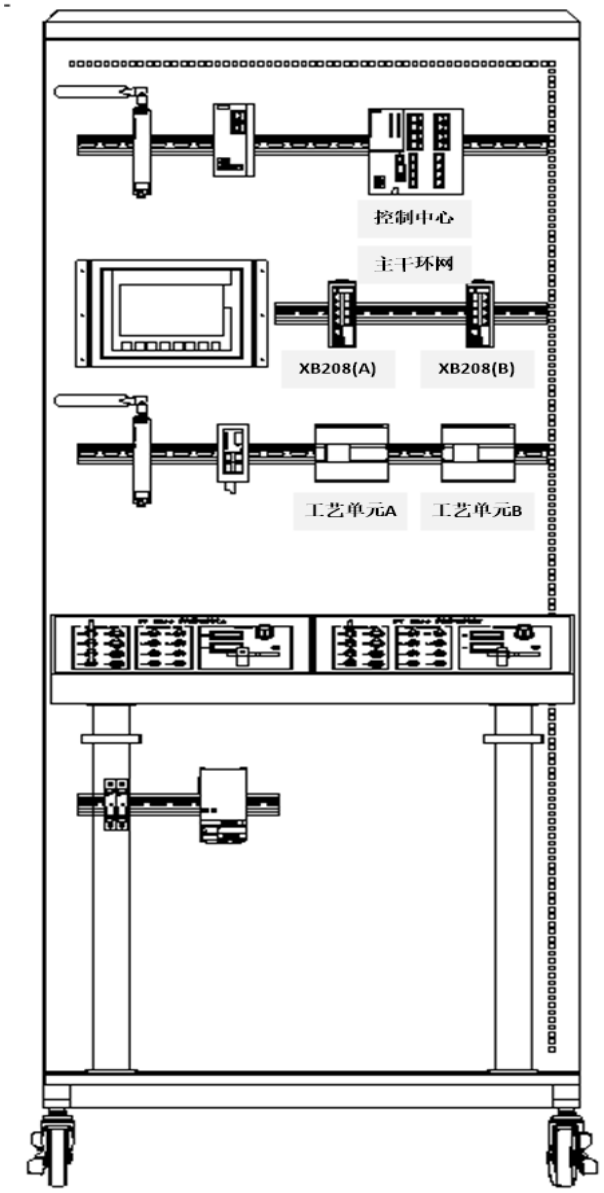

图 2 模块所属网络分配

2、配置 S7 1200PLC 时，请务必使用 TIA portal V15.1 版本

3、无线模块的天线型号：ANT795-4MA

4、**所有网络模块设定的密码必须为 A_123456**