Future Skills

TEST PROJECT C2

Industry 4.0

CONTENTS

This test project proposal consists of the following documentation/files:

1.	CP-L-WSK_iDrill_20190718_V15.1.zap15_1	TIA project for drilling station
2.	CP-AM-iDrill_Siemens_v1.03_20180702.projectarchive	Original CODESYS project for the iDrilling Station
3.	Wireshark-win32-3.0.3.exe	Wireshark installation SW
4.	proneta_2_7_0_3.zip	Proneta installation SW
5.	CP Factory - CP Lab iDrilling Electrical Schematic.pdf	Electrical Schematics of the CP-Lab iDrilling Station)
6.	CP Factory - CP Lab iDrilling Manual A003.pdf	User Manual of the CP-Lab iDrilling Station
7.	67460624_PRONETA_Documentation_V2_6_en.pdf	User Manual of Proneta SW
8.	PH_SCALANCE-S615-WBM_76.pdf	User Manual of SCALANCE 615 Router
9.	PH_SCALANCE-XB-200-XC-200-XF-200BA-XP-200-XR-300WG-WBM_76.pdf	User Manual of SCALANCE 615 Router
10.	C1_S615_Start.conf	Router configuration file
11.	WSK2019_Task_A_Documentation.docx	The template file for documenting Task specific requirements

INTRODUCTION

The situation for task C2 is the same as in C1.

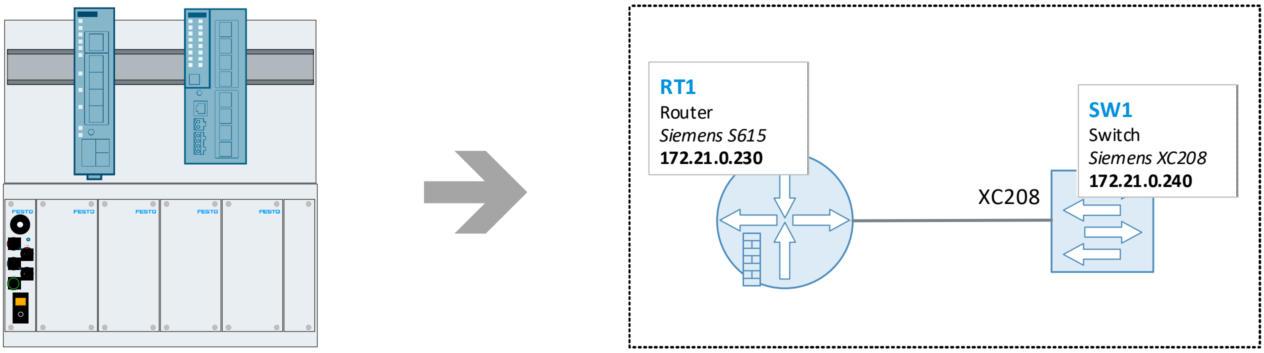
In the second stage of the block C of the contest your task is to set up the router and its firewall by yourself instead of using the prepared configuration.

Additionally, the web server access which is reachable from the plant network must be protected against unauthorized users.

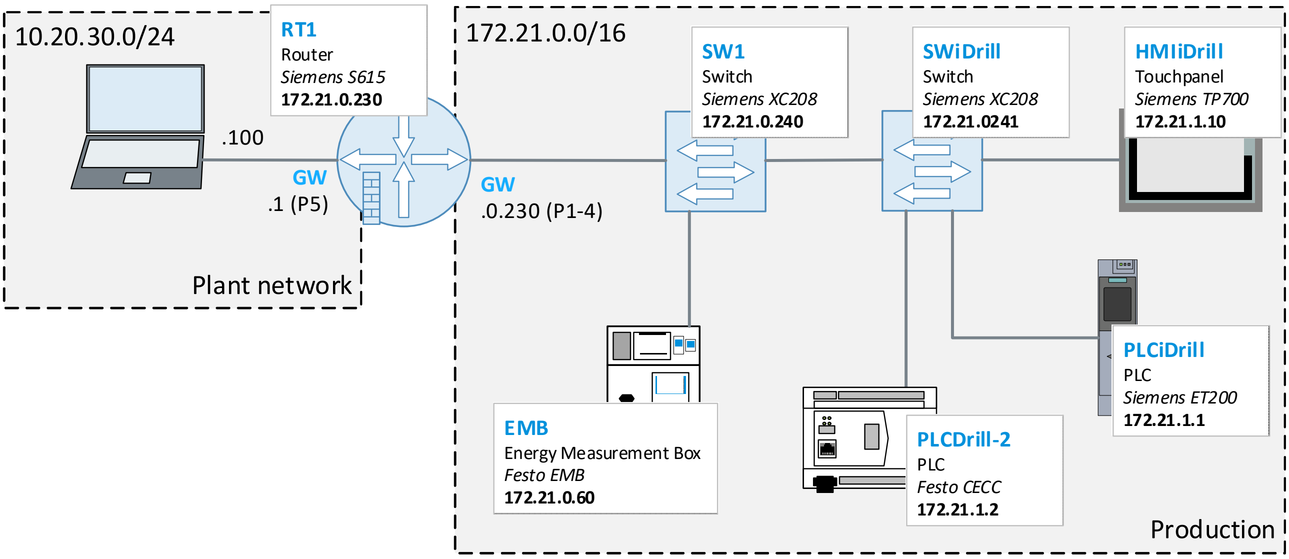
In C1 only web server access has been used. Now it shall also be possible to connect to the Siemens PLC from the plant network using TIA portal.

SCENARIO

The network components for connecting the networks are provided by the EduTrainer “Network and Security”.



The complete network scenario is presented in the drawing below:



The S615 router acts as gateway for both networks. For Profinet devices the names of the systems (first line in descriptive block) are also the Profinet names.

DESCRIPTION OF PROJECT AND TASKS

You can continue to work with the setup of C1 but the router has to be reset.

Your tasks are:

- Reset router of the EduTrainer to its factory defaults.
- Assign the correct network address to the router and login to the router’s management interface. Use the password “**Festo4.0**” when changing the default password.
- Ensure that the router answers to echo request packets on its plant network interface.
- Configure the firewall according to the requirements in section
- Capture ping answer packets (echo reply only) from all PLCs, the HMI and both switches to the notebook in the plant network using Wireshark. Save the capture file to the USB stick.
- Check the connectivity to all web servers mentioned in the section *Web access to PLCs* below.
- Change the user setup for the Siemens PLC with rights according to section
- *Access restrictions for Siemens PLC* Webserver .

Your task is completed when:

- You can demonstrate logging into the router.
- All communication from the plant network to the production network is possible like in task C1
    - Access to web servers according to the list in section *Web access to PLCs.*
    - Ping to devices according to the list in section *Connectivity check*.
- The TIA access to the Siemens PLC from the plant’s network is possible.
- No other than the allowed communication between plant network and production network is possible.
- The router's interface in the plant network answers to ping.
- The access to the Siemens PLC's webserver is protected according to the requirements in section
- *Access restrictions for Siemens PLC* Webserver .

INSTRUCTIONS TO THE COMPETITOR

ADDRESS PROVSIONING

To assign addresses and collect information about Profinet and CECC devices in your infrastructure you should use the programs Proneta and Festo Field Device Tool.

PROTECTION REQUIREMENTS FOR ACCESS TO THE SIEMENS PLC USING TIA PORTAL

The access to the Siemens PLC's project data must be multi-layer password protected. Use the following passwords for the given functional levels.

FUNCTIONALITY LEVEL	PASSWORD
Fail safe	Skills4.0
Write access	Skills3.0
Read access	Skills2.0

WEB ACCESS TO PLCS

The following URLs provide access to the web servers of the PLCs and the energy measurement box of the production system.

PLC	URL
Siemens	http://172.21.1.1
Siemens encrypted	https://172.21.1.1
iDrill CECC	http://172.21.1.2:8080/webvisu.htm
Energy measurement box	http://172.21.0.60:8080/webvisu.htm

REQUIREMENTS FOR COMMUNICATION BETWEEN NETWORKS

These are the communication scenarios that must be allowed to pass from the plant's network to the production network. The traffic shall not be limited to any IP address (all IP addresses are allowed).

SOURCE	DESTINATION	SERVICE	ACTION
Plant network	Production network	HTTPS	Accept
Plant network	Production network	HTTP	Accept
Plant network	Production network	Ping	Accept
Plant network	Production network	S7 Communication	Accept

No other traffic shall be allowed to pass through the firewall in either direction.

ACCESS RESTRICTIONS FOR SIEMENS PLC WEBSERVER

To protect the access to the web server of the Siemens PLC you must limit rights of the “Everybody” user and create a new user. The data and rights for the new user is given below:

Username: WorldSkills

Password: Skills1.0

Required access rights for user WorldSkills

- Read access to diagnostic data
- Read access to tags and to tag status
- Acknowledgement of alarms
- Identification of devices using the flashing lights feature

The unauthenticated access to the Siemens PLC using the “Everybody” user should be limited to the minimum of rights.

CONNECTIVITY CHECK

You may use the following lines to check the connectivity to your PLCs and switches:

```
ping -n 1 172.21.1.1

ping -n 1 172.21.1.2

ping -n 1 172.21.1.10

ping -n 1 172.21.0.60

ping -n 1 172.21.0.240

ping -n 1 172.21.0.241
```

EQUIPMENT, MACHINERY, INSTALLATIONS, AND MATERIALS REQUIRED

TABLE OF WIRESHARK DISPLAY FILTERS

FILTER EXPRESSION	MEANING
arp	Packets of the Address Resolution Protocol
icmp	Packets of the Internet Control Message Protocol (e.g. ping echo request and response)
arp **or** icmp	both arp and icmp packets will be shown
ip.addr ==172.21.0.90	Packets, which contain the IP address 172.21.0.90 in sender or destination
ip.src == 172.21.0.90	Packets that have been sent from the address 172.21.0.90 (src = source)
ip.ds == 172.21.0.90	Packets that have been sent to the address 172.21.0.90 (dst = destination)
dhcp	Packets of the Dynamic Host Configuration Protocol
not lldp	**Do not** show packets of the Link Layer Discovery Protocol
! lldp	**Do not** show packets of the Link Layer Discovery Protocol (alternative)
pn_dcp	Packets of the Profinet protocol Discovery and Configuration Protocol
pn_io	Packets of the Profinet protocol IO Realtime
eth.addr == 00:0e:f0:b2:53:9e	Packets with the ethernet address 00:0e:f0:b2:53:9e
opcua	Packets of the OPC UA protocol
tcp	Show packets that use the Transmission Control Protocol
udp	Show packets that use the User Datagram Protocol
tcp.port == 443	Packets being sent to the https port (TCP, port 443)
Tls	Packets with protection by Transport Layer Security (TLS)
isakmp	Packets of the Internet Security Association Key Management Protocol
esp	Packets of the encrypted IPsec protocol Encapsulating Security Payload
http.request or http.response	Show messages accessing web pages
telnet	Show unencrypted terminal access
ssh	Packets of the encrypted Secure Shell Protocol
s7comm	Siemens S7 communication protocol

PORTS AND PROTOCOLS FOR SERVICES

SERVICE	SERVICE TYPE	PROTOCOL	PORT
AMQP	IP Service	TCP	5671
DNS	IP Service	TCP UDP	53 53
HTTP	IP Service	TCP	80 or 8080
HTTPS	IP Service	TCP	443
ISAKMP	IP Service	UDP	500
MQTT	IP Service	TCP UDP	1883 1883
NTP	IP Service	TCP UDP	123 123
OPCUA	IP Service	TCP	4840
PING	ICMP Service	ICMP – Type “Echo Request”	N/A
OPCUA	IP Service	TCP	4840
S7COMM	IP Service	TCP	102
SSH	IP Service	TCP	22

MARKING SCHEME

You will receive credits for all subtasks that have been defined in the fulfilment statement:

- You can demonstrate logging into the router.
- All communication from the plant network to the production network is possible like in task C1
    - Access to web servers according to the list in section *Web access to PLCs.*
    - Ping to devices according to the list in section *Connectivity check*.
- The TIA access to the Siemens PLC from the plant's network is possible.
- No other than the allowed communication between plant network and production network is possible.
- The router's interface in the plant network answers to ping.
- The access to the Siemens PLC's webserver is protected according to the requirements in section
- *Access restrictions for Siemens PLC* Webserver .