Co-funded by the Erasmus+ Programme of the European Union

ISSES

ISSES – Information Security Services Education in Serbia

Supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

Critical Infrastructure Security Laboratory (CIS Lab) design

Version 1.0

Author(s)/Organisation(s):
Imre Lendak; Zorana Babić; Jelena Sekulić / UNS (P1) Viktor Varga / UT (P8) Holczer Tamas, Levente Buttyan / BME (P3)
Date of final release:
June 2021
Relevant Work Package(s):
WP3 – Lab development
Short Description:
Network security laboratory design description.
Keywords:
Critical Infrastructure Security Laboratory, lab design

Revision History:				
Revision	Date	Author(s)	Status	Description
V0.1	Jun 30, 2021	Imre Lendak, Viktor Varga, Levente Buttyan, Tamas Holczer	Working draft	Draft
V1.0	Sep 30, 2021	Imre Lendak	Working draft	First edition

CONTENTS

1 Lab equipment list

The below table lists the equipment acquired as part of the ISSES project and used within the CIS Lab.

Type of equipment	Specification	Quantity
Server	2 x 12C/24T CPU (Xeon Silver 4116, 2.1GHz), 128GB RAM, 3 x 800GB SSD, HBA 2 x 16G FC, 48 threads	3
Storage	Storage b - 8 x 16GB FC 10 x 1.2TB + 3 x 400GB flash – FC	1
Switch	L2/L3 24 x 1G + 4 x SFP/SFP+	1
Router	Virtual Router vSRX 100M	10
Uninterrupted power supply	UPS 5000VA/4500W 230V 50/60Hz ON-LINE DOUBLE CONVERSION (VFI) BUILT-IN WEB/SNMP,1xRS232 BATTERY INCLUDED, standard autonomy 8 min.	1
Rack	42U	1
Industrial controller	SIMATIC S7-1200 CPU 1212C	1
Industrial controller module	SIMATIC S7-1200 SM 1232	1

The table below lists the equipment made available by the home institution.

Type of equipment	Specification	Quantity
Laptop	Modern laptop for students in the laboratory	16
Desktop PC	Branded PC for research	4
Industrial communication	Modbus TCP Ethernet Remote IO Module (4DI+4DO+4AI+2AO)	1
Industrial communication	Necessary cables and tools to connect the cyber-physical equipment	NA

2 Lab software list

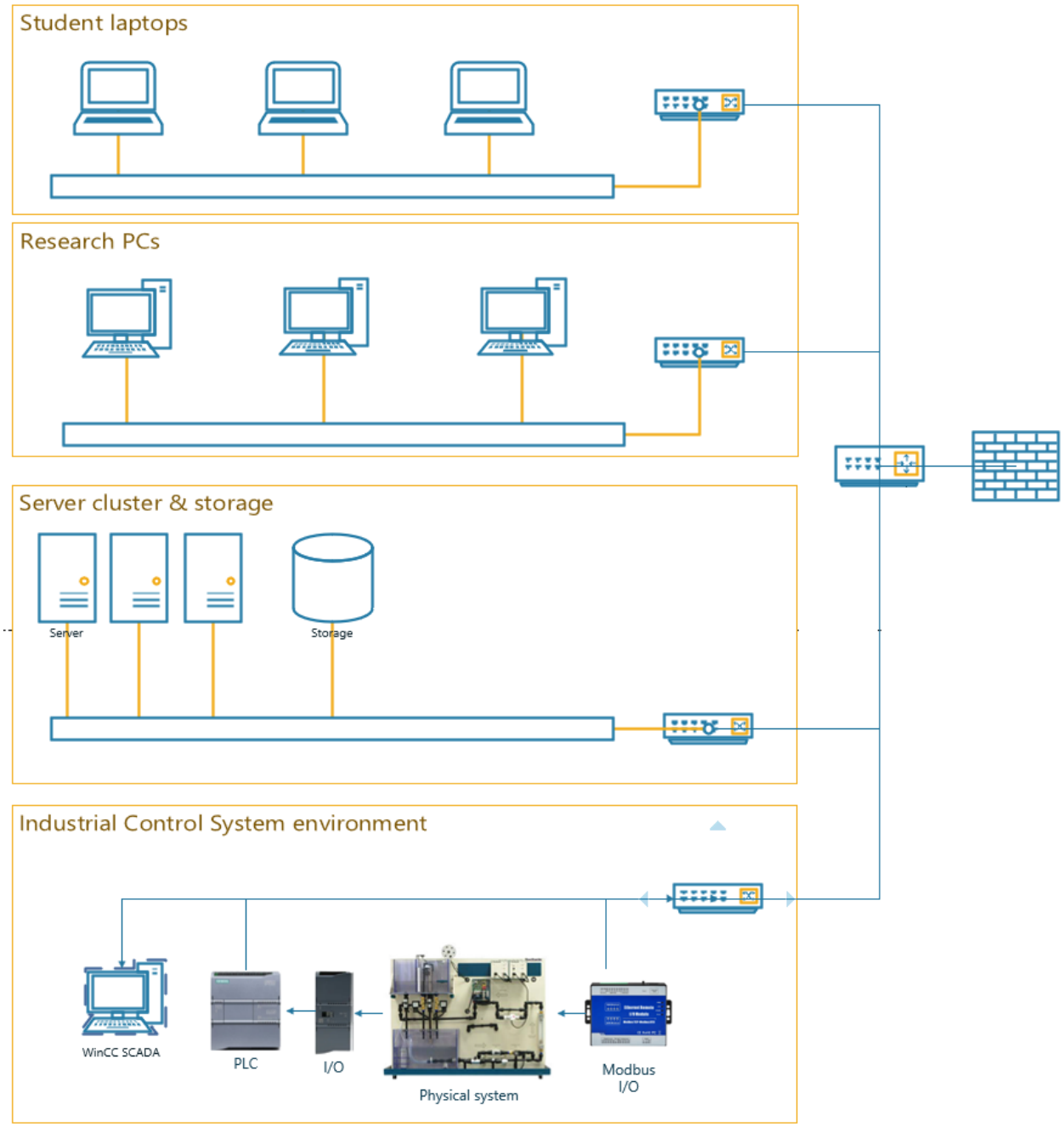
The project team planned to deploy a free-to-use virtualization platform on the acquired servers.

In the critical infrastructure context partner P1 will utilize the following pieces of relevant software either already possessed by P1 or freely available.

Type of software	**Specification**	**Source**
Virtualization	WMWare or similar	Free, online
OS	Windows 10, Kali Linux, Ubuntu	P1
E-learning	The SOVA platform based on Moodle	P1
Network security	Nmap, Wireshark, tcpdump, SHODAN	Free, online
Industrial control system	Desktop SCADA software	P1
Industrial control system	Cloud-based SCADA software	Free & limited license
Industrial control system – simulators	pyModbus or similar	Free

3 Lab deployment plan

It is planned that the acquired equipment will be deployed as shown in the detailed network diagram below.



4 Lab exercise list

The following lab exercises were included in the Course Development Plan (CDP) of the ISSES project and developed mainly for course 2.1.

Area of exercise	**Specification**
Infrastructure	Docker tutorial
PCAP analysis	MOAR Bytes PCAP analysis
ICS security	Simulators in ICS security analysis
ICS security	Industrial Testbeds: Temperature & water level control
ICS security	ICS man-in-the-middle in the OT environment
ICS security	Hijacking the SCADA Human-Machine Interface (HMI)
Infrastructure	Ransomware-as-a-service in ICS attacks

Additionally, the laboratory equipment will support the delivery of the following ISSES courses at the Faculty of Technical Sciences, University of Novi Sad (P1):

- 2.2 Secure Software Development
- 2.4 Security and privacy in the Internet of Things
- 2.5 Advanced Cryptography
- 2.6 Advanced Network Security
- 2.12 Digital Forensics Tools and Techniques
- 2.14 Security Data Science
- 2.15 Computer Security

The above courses will be mainly supported via the virtualization capabilities provided by the servers acquired as part of the ISSES project.