Bahria University
Discovering Knowledge

Fall 2024
Department of Computer Science
Bahria University, Karachi Campus

ASSIGNMENT No. 3
Complex Computing Problem

Course Title: Information Security
Course Code: CSC-407
Class: BS (CS)-8A/8B Submission deadline: **20-Dec-24**
Course Instructor: Dr. Taha Jilani Marks: 10

Instructions

1. Copied assignments will be marked zero.
2. Submit your assignment in soft and hard copies both. Make a single pdf file and upload on LMS.
3. Solution must be designed by applying the following characteristics.

Characteristics	**Problem Solving description**
Depth of analysis required	Has no obvious solution, and requires conceptual thinking and innovative analysis to formulate suitable abstract models
Depth of knowledge required	A solution requires the use of in-depth knowledge of IS provided in class.

1. Problem [CLO 3, PLO 8, C6]

A critical-infrastructure, such as water-treatment plant employ various treatment methods to ensure safe drinking water for the locality. Consider a computerized water-treatment plant that follows a sequence of treatment steps, including coagulation, flocculation, sedimentation, filtration, and disinfection (Figure 1). A Cyber-Physical System (CPS)-based water treatment plant called SWaT operates as a 6-stage facility, producing treated water at a rate of 5 gallons per minute. The plant's six sub-processes, each corresponding to one treatment stage, are illustrated in Figure 2. Each sub-process is managed by a controller (PLC), with sensors measuring its state and actuators enabling control. For instance:

- At SWaT, the sensor LIT101 measures the water level in tank T101
- Similarly, a motorized valve MV101 controls the flow of water into T101

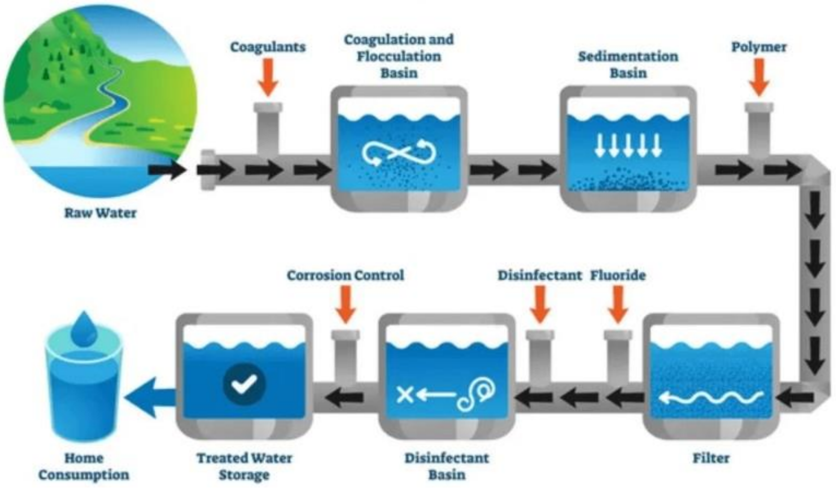

Fig-1 – Multiple stages at Water Treatment Plant

Each sub-process is managed by a controller, with its state monitored by sensors and control executed through actuators. The plant includes a variety of sensors and actuators, some of which are standbys intended for use only if a primary actuator fails. In total, there are 68 sensors and actuators in the plant, though not all are depicted in Figure 2. For example, pump P102 remains in standby mode and activates only if pump P101 fails.

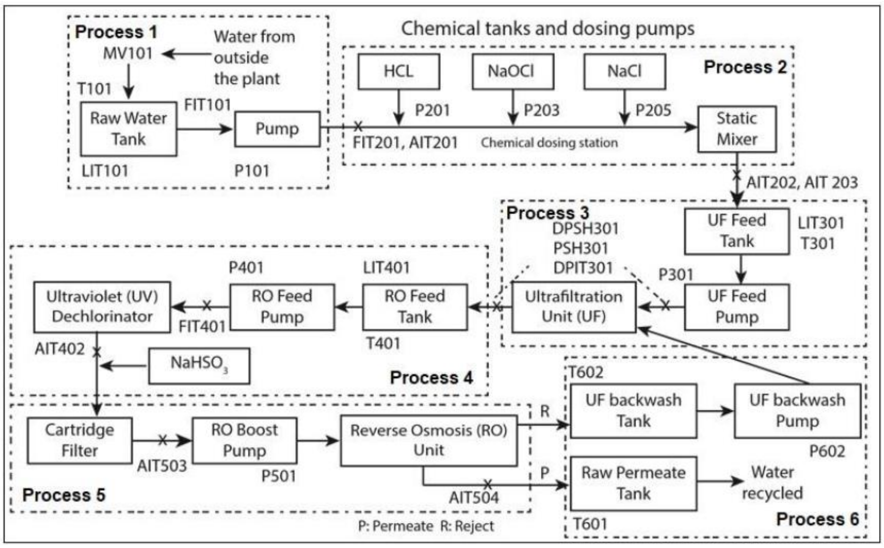

Fig 2 – The six-processes at SWaT

As it can be seen from Figure-3, various distribution pumps are controlled by an operator using an HMI based interface. However, there are chances that a cyber-attack can interrupt the whole process, and the preset settings of the various operations at water treatment plant can be manipulated, thus security can be compromised. A multi-layer network enables communications across all components of plant. The ring network at each stage at level 0 enables PLCs to communicate with sensors and actuators at the corresponding stage. A star network at level 1 enables communications across PLCs, SCADA, HMI and the historian. Therefore, to prevent from cyber-attack on this water-treatment plant, and it is required to design and develop an anomaly-based intrusion detection system, so that novel-attacks can be detected and prevented.

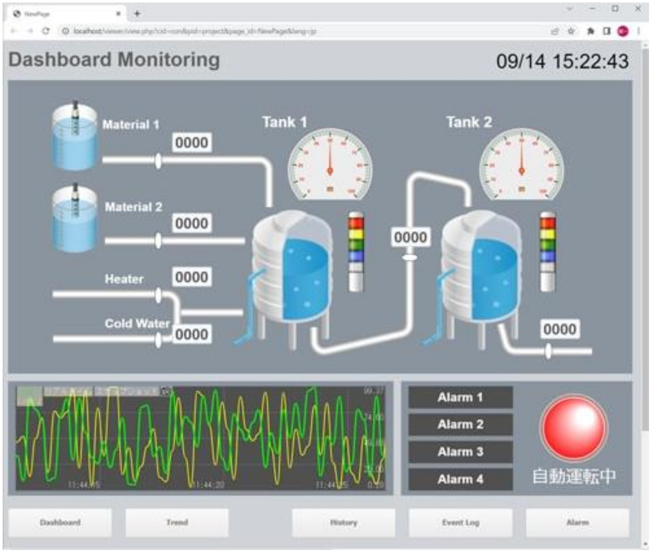

Fig-3 – Plant with HMI, PLC and SCADA control

2. Assumptions

a) <u>Operation:</u>

Operation of SWaT is initiated and controlled by an operator at the SCADA workstation. State information can be viewed at the workstation and at the HMI, and is recorded in the historian. Process anomaly detectors, i.e. monitors, developed by using design centric approach have been installed in SWaT. Detectors generate visual alerts and send messages to the operator. SWaT can be attacked by compromising its communications network at all levels as well as directly by accessing the PLCs, the SCADA workstation, and the HMI.

b) <u>Communications</u>

A multi-layer network enables communications across all components of SWaT. The ring network at each stage at level 0 enables PLCs to communicate with sensors and actuators at the corresponding stage. A star network at level 1 enables communications across PLCs, SCADA, HMI and the historian.

c) <u>Cyber Attack:</u>

A cyber-attack has been performed on this testbed and the same data is collected from it. This can be used to detect any anomaly in the IDS.

Dataset is available at: https://sites.google.com/view/muhammadtaha/is *<CCP Folder>*

3. Deliverable

You are supposed to **develop** a controller for the anomaly-based IDS that utilizes a best ML/DL approach to detect anomalies. You are expecting to detect the attacks, while mainly focusing the False Positive for detected-attacks, confusion-matrix and design approach. Finally, you will provide a comprehensive security mechanism in the form of report incorporating all secure-design aspects, the best ML/DL approach supporting with all analysis and its performance parameters. The report should contain the recommendations that how overall security can be deployed for the above stated CPS system.

4. Evaluation Criteria

Complete System Design and Development	--	50%
Data & Results Interpretation	--	30%
Viva-voce	--	20%