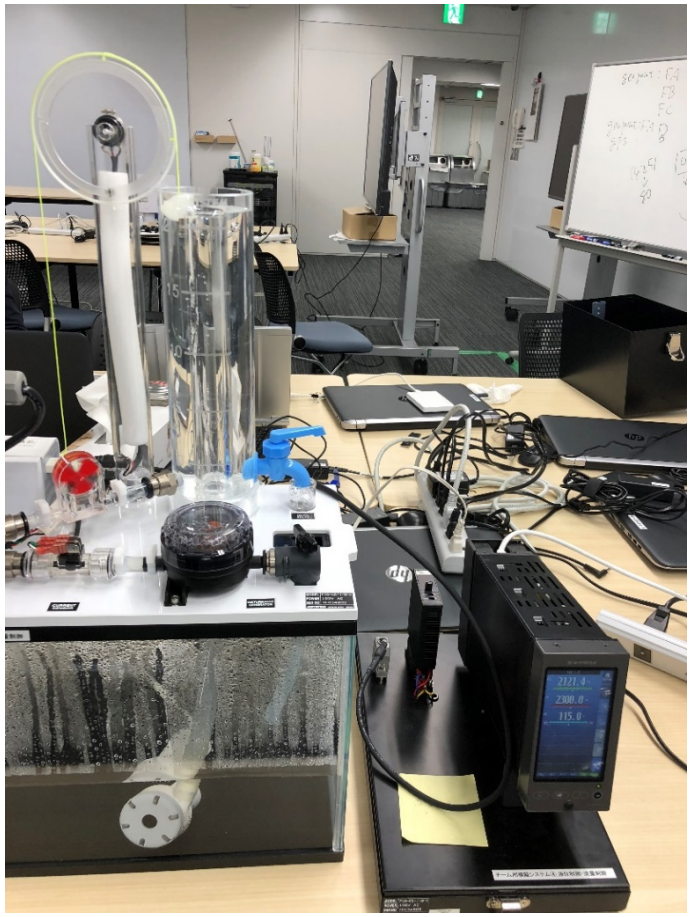
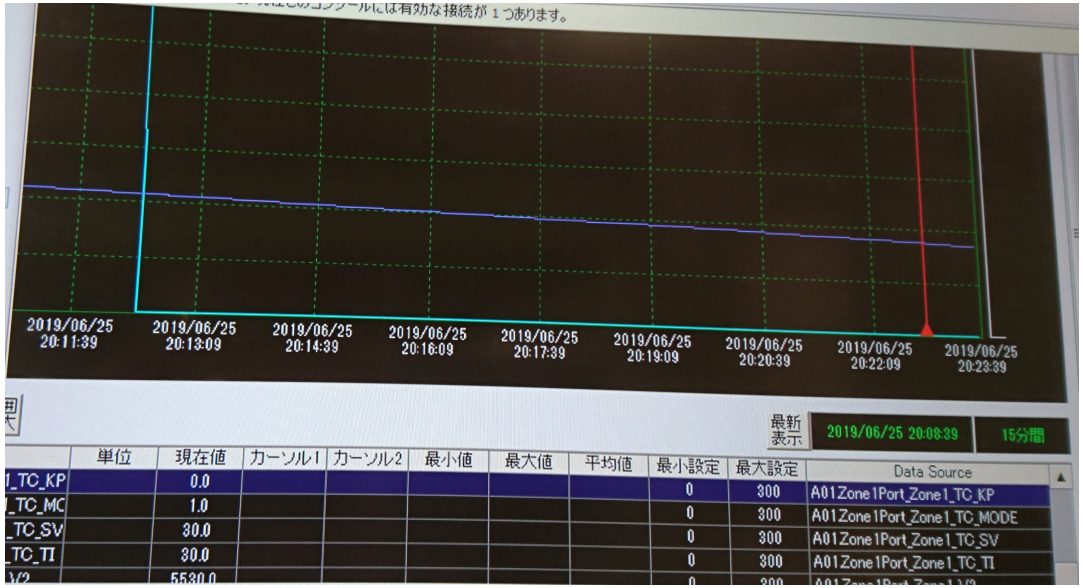
Attack demonstration took kits for Industry 4.0 using AI and cloud

The University of Tokyo
Wataru Matsuda,
Mariko Fujimoto,
Takuho Mitsunaga

ICS testbed environment



Water pump system

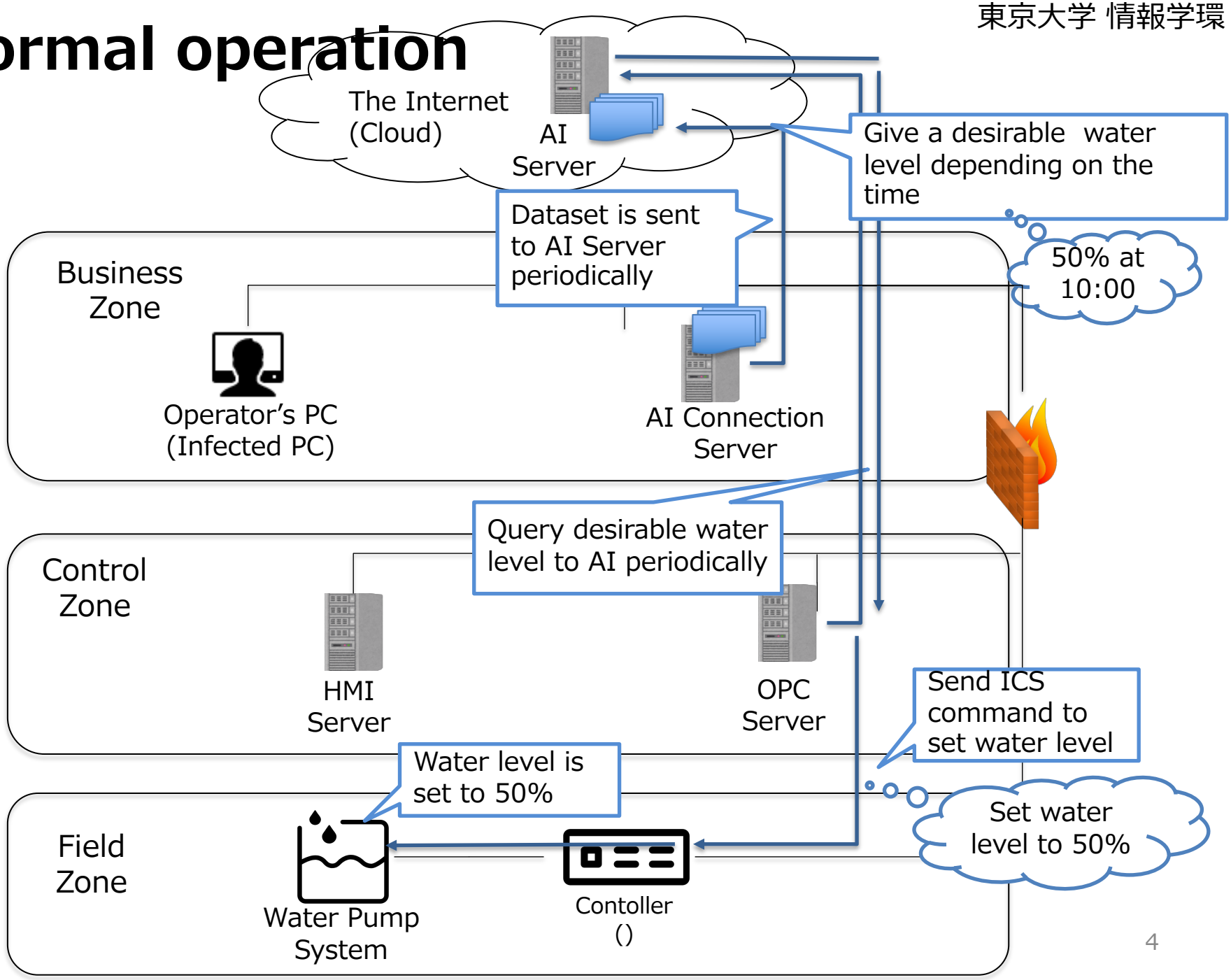


HMI

ICS testbed environment

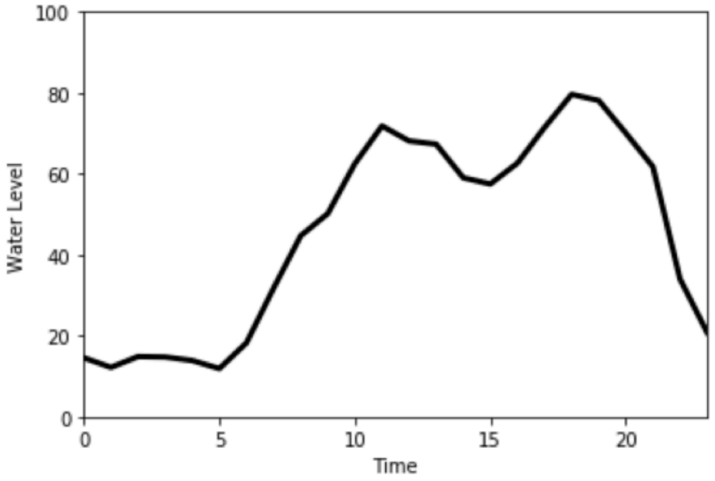
Device	OS	Network segment	Summary
Water pump	-	filed zone	Provides water for consumers.
Controller	SC2000 (M-Systems)	filed zone	Controls the water level of the cylinder.
OPC Server	WindowsServer2008 R2	control zone	Relays communications among controller and HMIs using Modbus and OPC-DA.
HMI	WindowsServer2008 R2	control zone	Gets Process Value from the OPC Server and visualize them using graphs.
Operator's PC	Windows 10	Business zone	A PC used by ICS operators.
AI Connection server	Windows 7	Business zone	Stores the time series dataset of the water level.
AI server	Cent OS 7	Cloud (The Internet)	Analyze desirable water level and temperature depending on the time using machine leaning.

Normal operation



Normal operation(creation of the AI dataset)

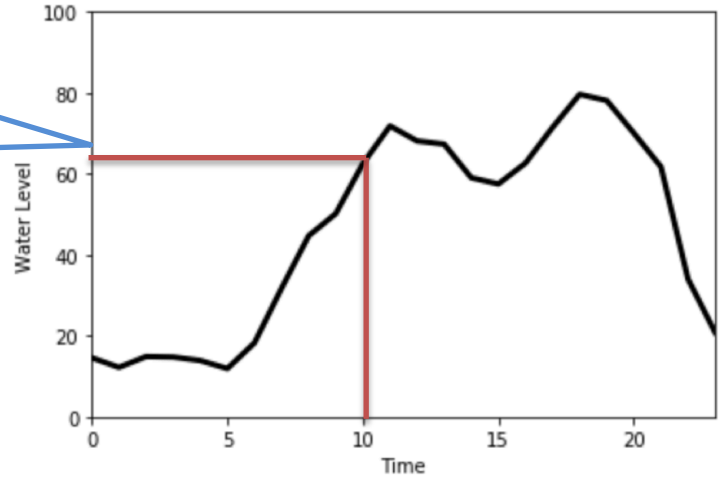
- Precondition
  - The water level and water temperature vary depending on the time.
  - The time series water level and temperature data are periodically sent to the AI connection Server, and dataset is created.
  - The dataset is periodically sent to the AI Server, and model for AI is updated.



Normal operation(controlling SetPoint using AI)

- The OPC Server periodically queries desirable values (SetPoint) to the AI Server via the AI Connection Server using the Web API.
- The AI server conducts XGBoosting analysis against the desirable water rate and temperature using the model created by the dataset sent from the AI Connection Server. Then return the desirable values.
- The OPC Server receives the desirable values and controls the controller.

The desirable water level at 10:00 is 63%.



Vulnerable points

- The dataset on the AI Connection Server is not protected (no access control, no encryption). Also no implementation for tamper detection.
- Therefore attackers who can intruded into the AI Connection Server could change the dataset.
- Since the AI Connection Server is located in the business network, attackers who compromised a PC on the business network could conduct lateral movement to the AI Connection Server.

Attacker's purpose

- In this demonstration, the purpose of attackers is to **impair physical devices without accessing the ICS network**.

- In such a situation, attackers try to attack AI which controls ICS.

- There are several possible attack scenarios against AI, but we focus on the contamination of the AI dataset.

Attack scenario

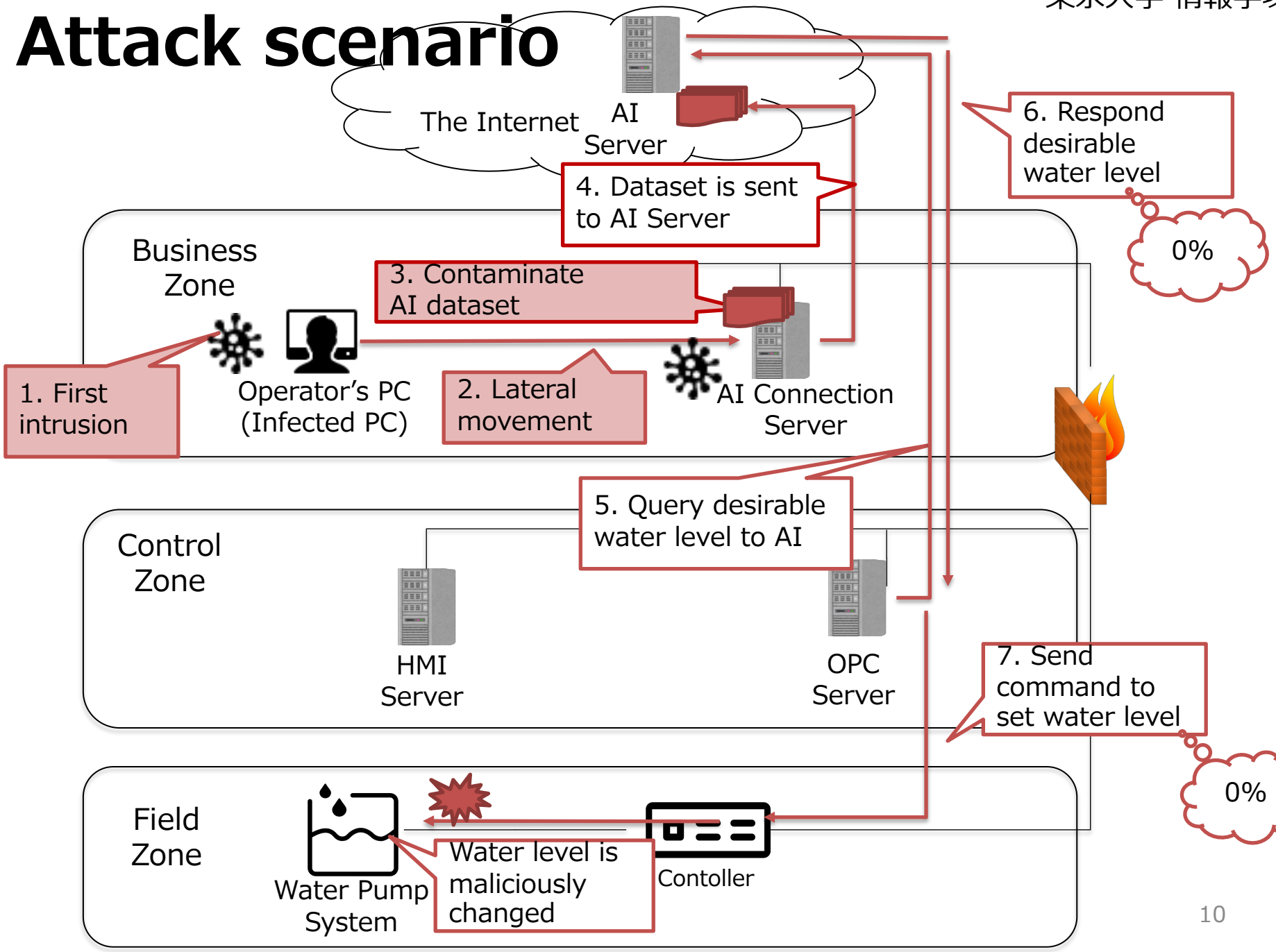
1. **Infects a operator's PC in the Business zone**
2. **A lateral movement to the AI Connection Server**
3. **Contaminate the AI dataset on the AI Connection Server**

Attacker's activities

4. The contaminated dataset is sent to AI Server
5. OPC Server queries the desirable SetPoint to the AI Server
6. AI Server returns incorrect value judged from the contaminated dataset
7. OPC Server sends incorrect SetPoint to the Contoller
8. The physical statue of the water pump is maliciously changed

Normal operations

Attack scenario

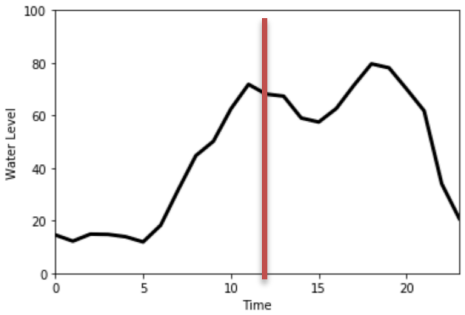


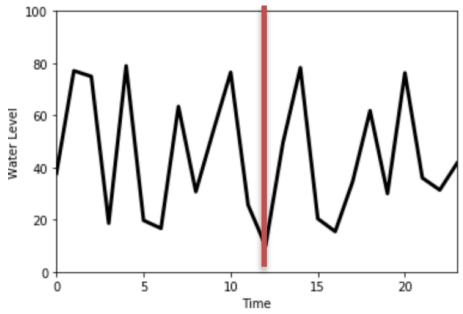
Attack result

- We conduct preterition test based on the attack scenario.
- As the result, we successfully changed the physical state of the actuator without accessing Control network and AI Server.

Pump system

Setpoint provided by AI





Normal state (Almost full)

After attack (Almost empty)