Attack demonstration took kits for Industry 4.0 using AI and cloud

The University of Tokyo

Wataru Matsuda, Mariko Fujimoto, Takuho Mitsunaga

Background

- Industry 4.0 is a new concept of automation data exchange in manufacturing, structures are significantly different from the current general ICS.
  - Autonomous judgment and execution are required.
  - Devices are supposed to connect interactively.

- It can create new attack surfaces and risks of cyber-attacks, so instructing cyber risks in Industry 4.0 is important.

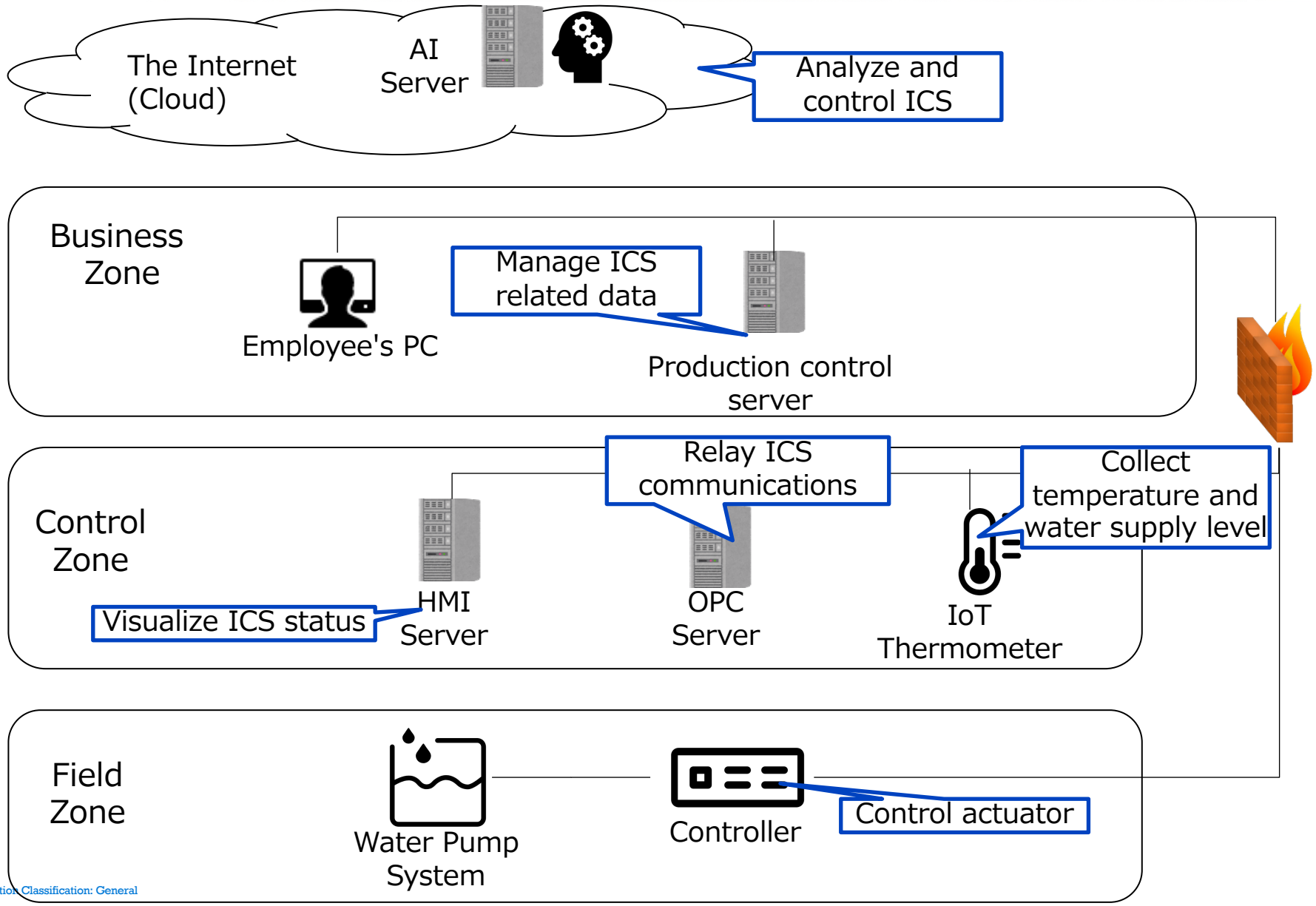
- We introduce attack demonstration took kits for Industry 4.0 using an actual machine.

Example of operation and structure in Industry 4.0

Technical components in Industry 4.0

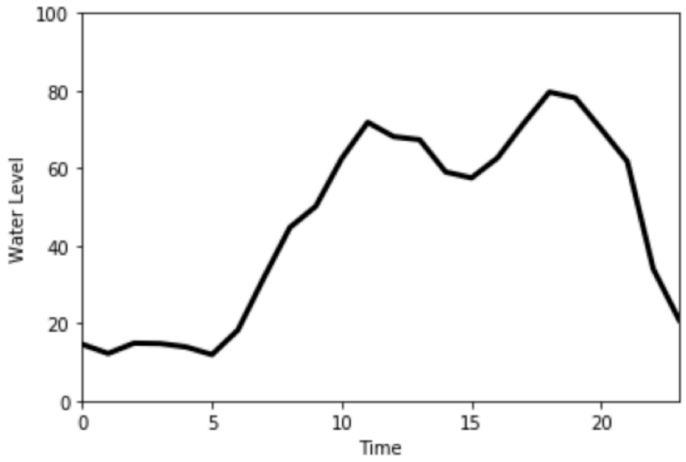
- Artificial Intelligence (AI): Judge and execute processes autonomously
- The Internet of Things (IoT): Collect and analysis of real-time data
- Cloud: Uniformly manage and monitor real-time data
- OPC Unified Architecture (OPC UA): Interoperability standard for the secure and reliable exchange of data (out of scope of the demonstration)

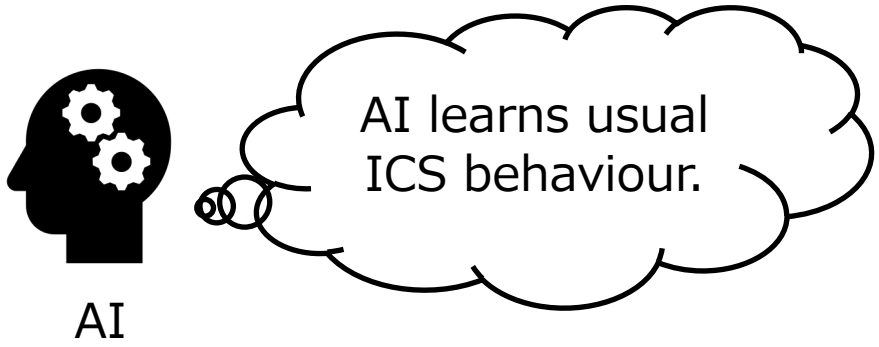
System structure of the demonstration took kits



Operational control using AI -training phase-

- The physical state (the water supply level) varies depending on the time and temperature.
- The time-series water level and temperature data obtained in the the ICS network are periodically sent to the “Production control server” in the Business zone.
- The dataset is periodically sent to the AI Server, and the AI learns appropriate water supply level corresponding time and temperature.

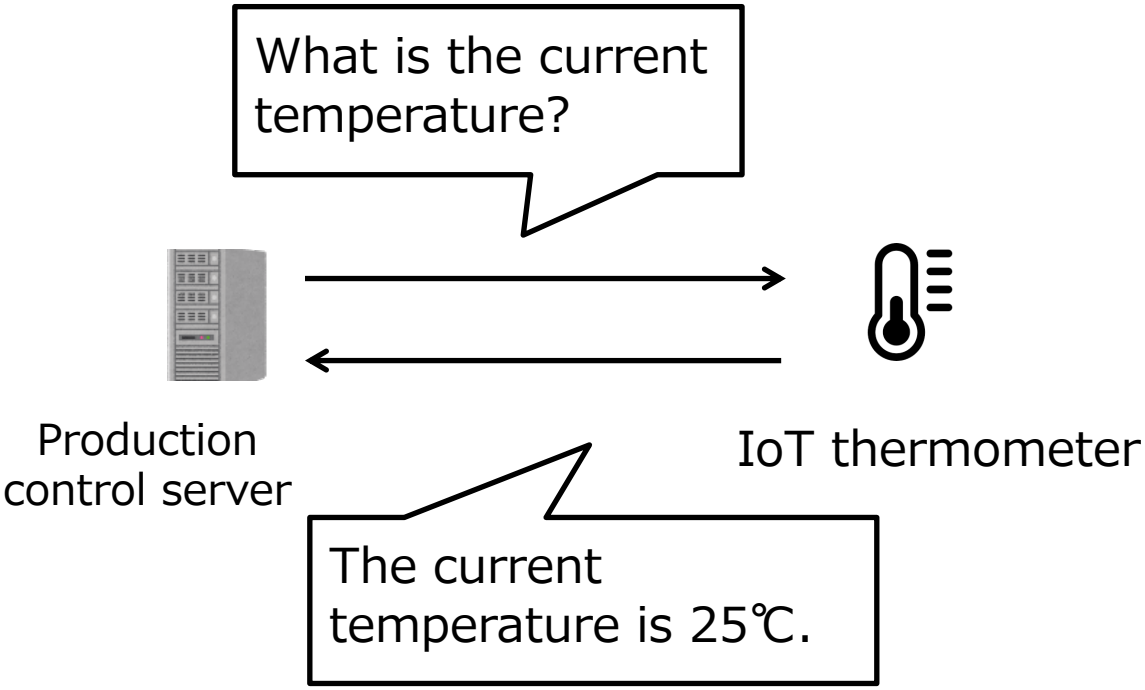




Operational control using AI -inference phase-

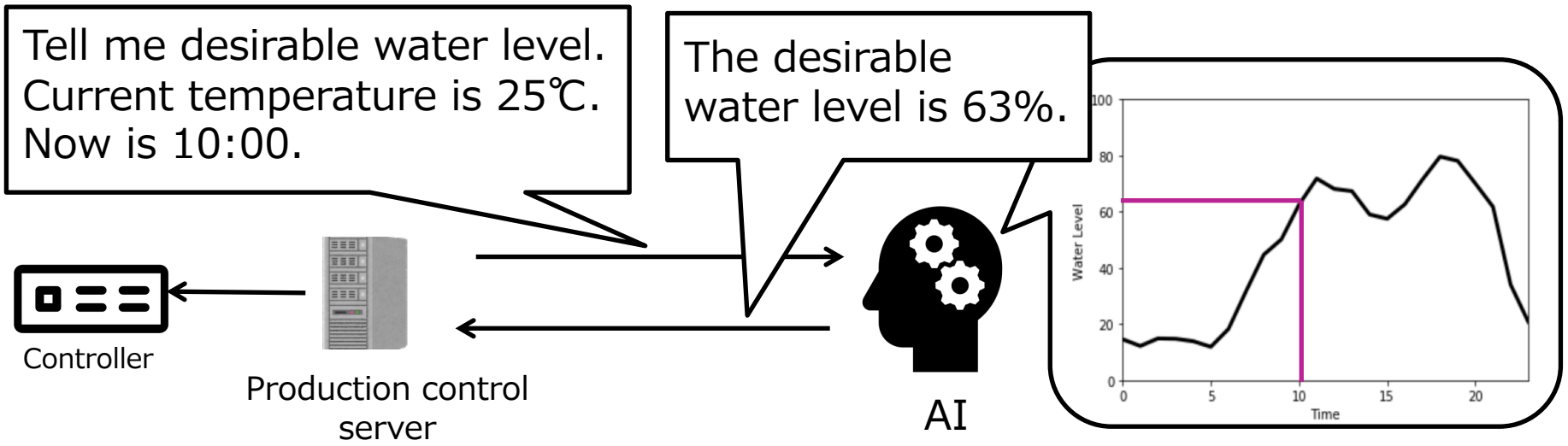
1. The Production control server periodically queries the current temperature to the IoT thermometer.

2. The IoT thermometer returns the current temperature.



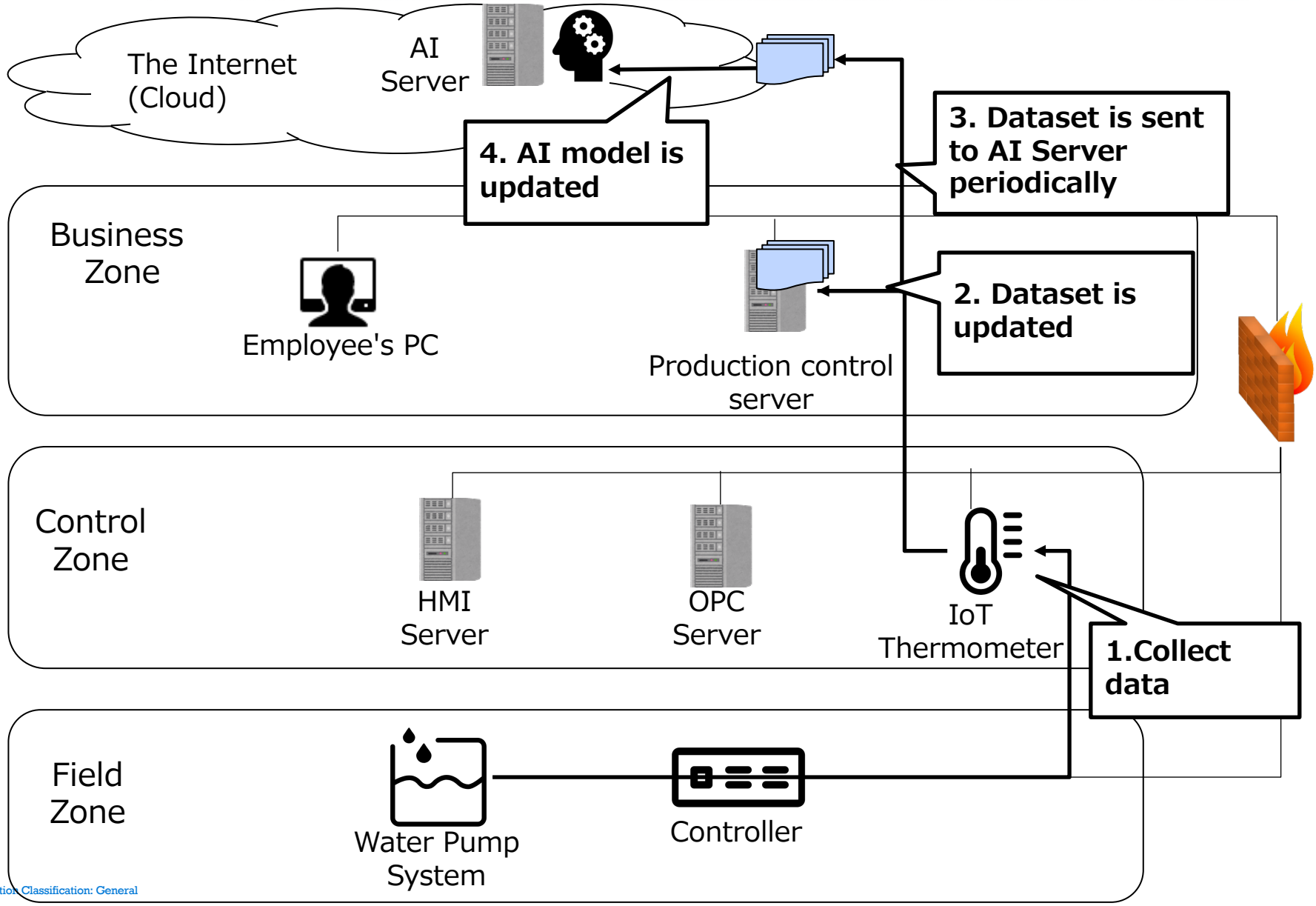
Operational control using AI -inference phase-

3. The Production control server periodically queries the desirable water supply level to the AI Server with current temperature and time.
4. The AI server conducts XGBoosting analysis, then return the desirable value.
5. The production control server receives the desired water supply level and send instruction to the OPC server.

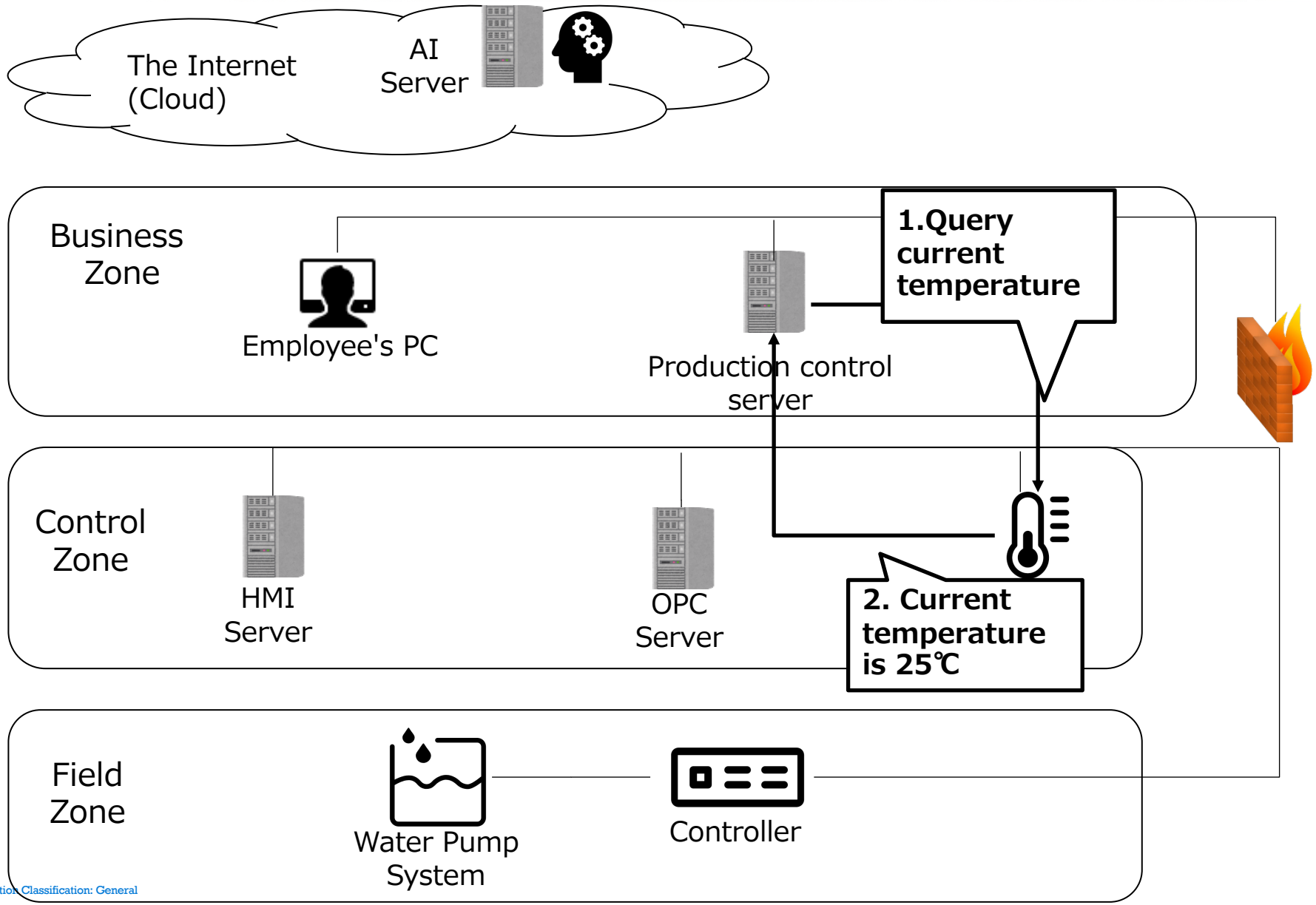


Demonstration kit

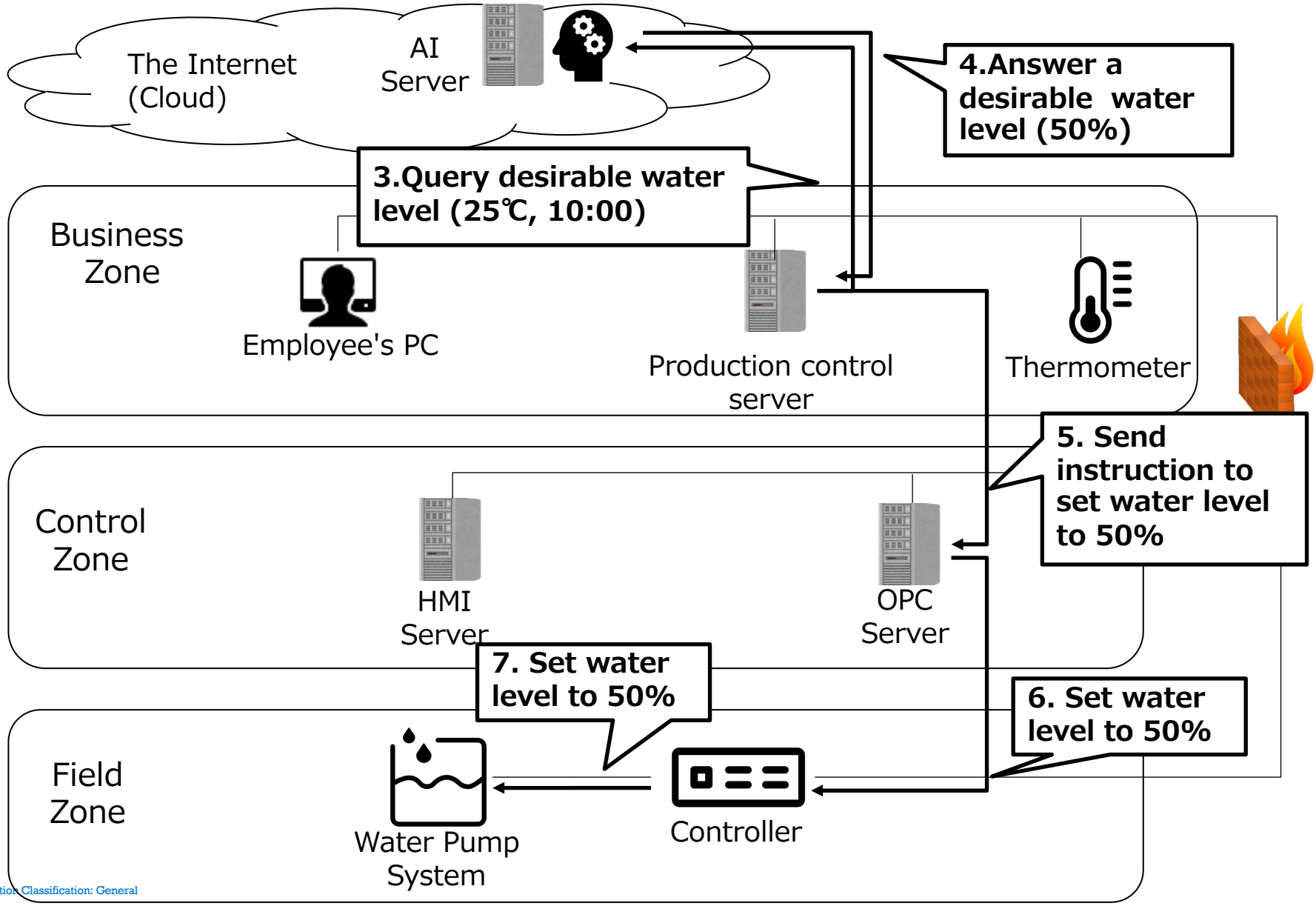
Operational control using AI -training phase-



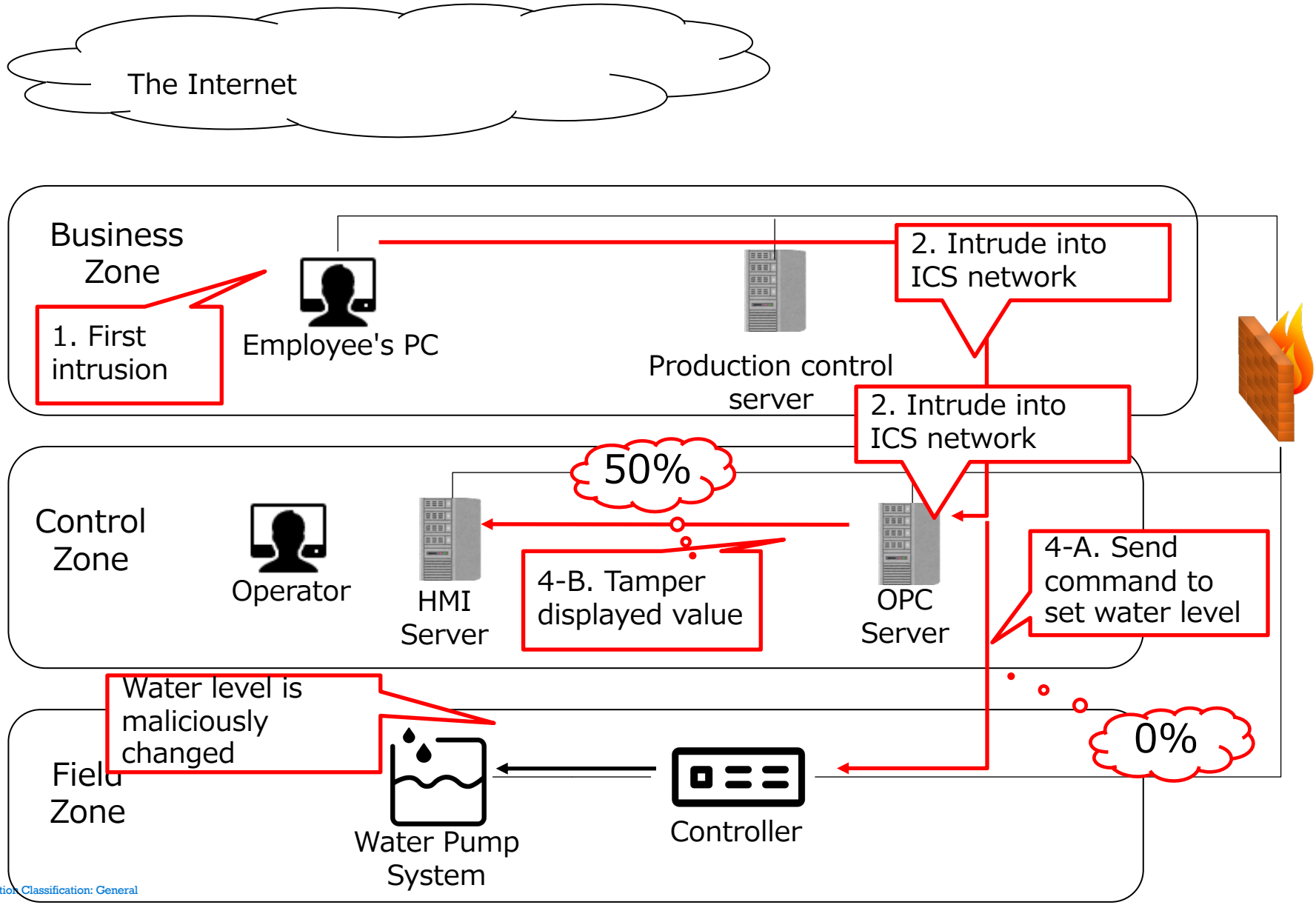
Operational control using AI -inference phase-



Operational control using AI -inference phase-



Conventional attack scenario



New attack scenario

New attack scenario

- The final goal for attackers is to impair the physical devices **without accessing the ICS network**.

- There are several possible attack scenario, in this demonstration, we will show attacks against AI.

- There are several possible attack scenarios against AI, we focus on the poisoning of the AI dataset.
  - **Direct Poisoning: attackers directly manipulate the dataset.**
  - Indirect Poisoning: attackers indirectly manipulate the dataset.

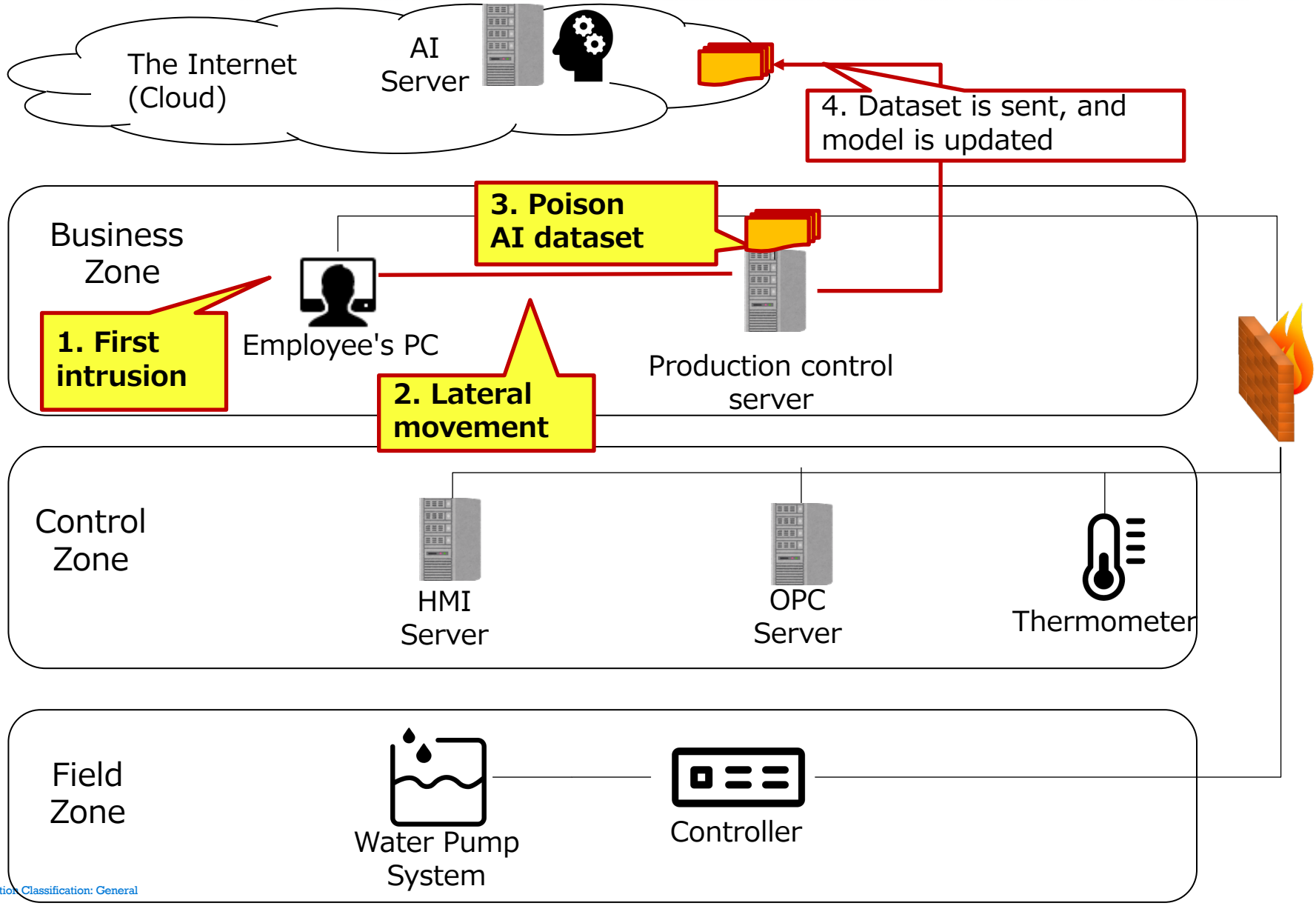
Vulnerable points

- The dataset on the Production control server is not protected (no access control, no encryption). Also no implementation for tamper detection and sanitizing.

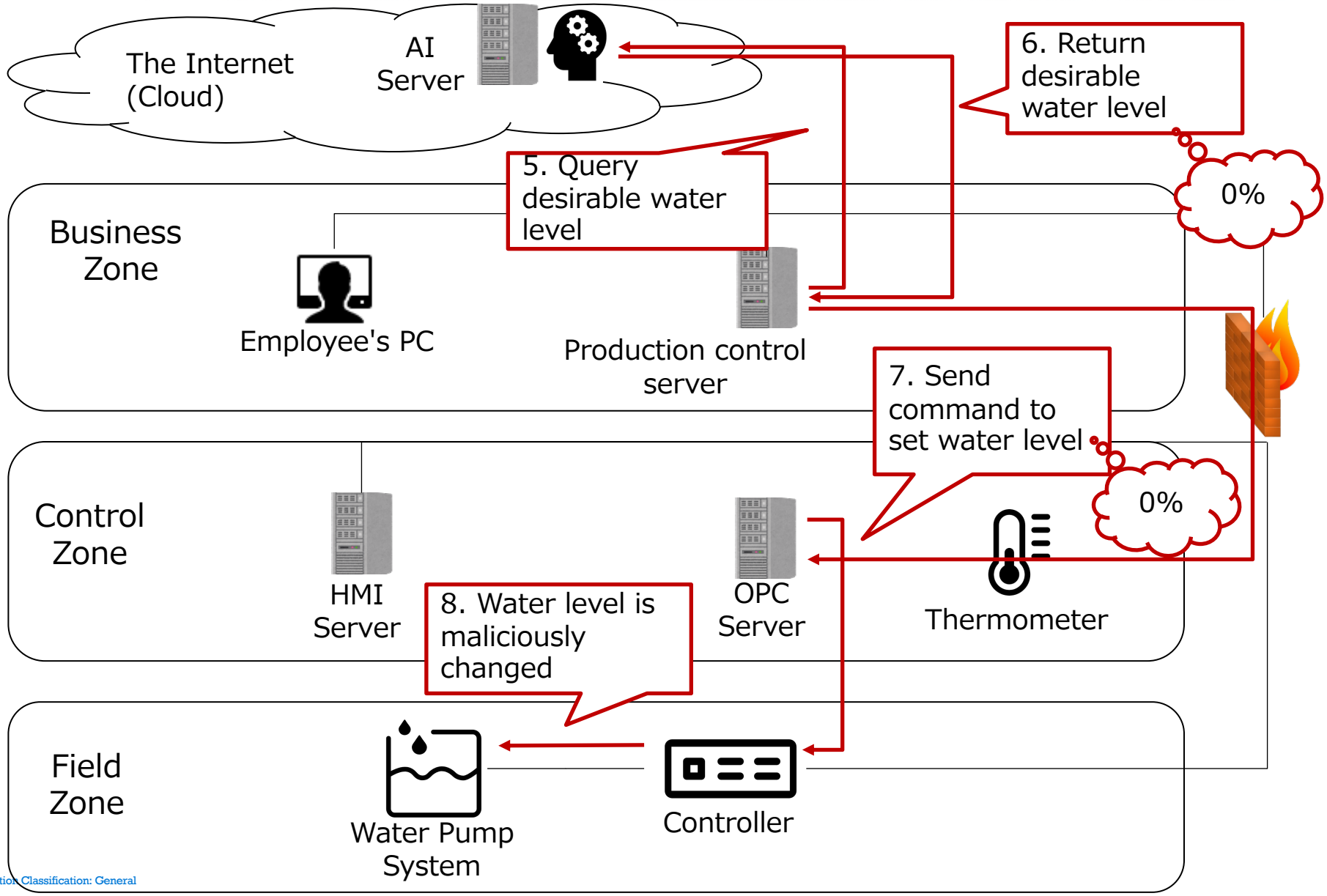
- Therefore if attackers have intruded into the Production control server, they could poison the dataset.

- In this demo, attackers change the all data regarding to water supply level to zero.

New attack scenario -training phase-



New attack scenario -inference phase-



Attack scenario detail

1. **Attackers expand infection to the Production control server from the employee's PC**
2. **Attackers poison the AI dataset on the Production control server**

Attackers' activities

3. The poisoned dataset is sent to AI Server
4. The production control server queries the desirable water supply level to the AI Server
5. AI Server returns incorrect value judged from the poisoned dataset

Normal periodic operations

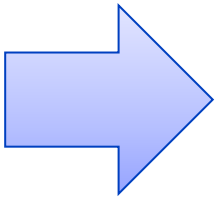
6. The production control server sends incorrect water supply level to the OPC server
7. The physical water level is maliciously changed

Result

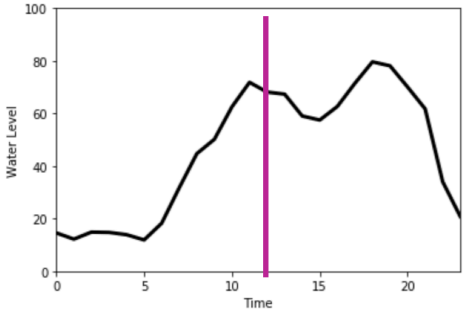
Attack result

- We conducted penetration test based on the attack scenario.
- As a result, we confirmed that we could change the physical state of the actuator without accessing control network and AI Server.

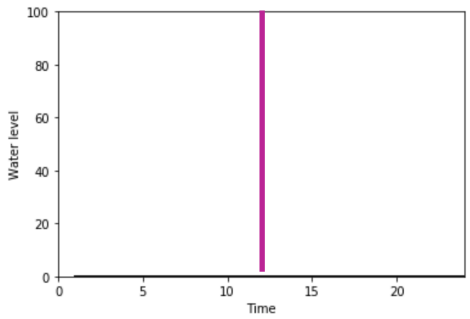
Physical water level



Water supply level provided by AI



Normal state (Almost full)



After attack (Almost empty)

Conclusion

- Industry 4.0, operations, and system structures are significantly different from the legacy ICS, thus it can create new cyber risks.
- We confirm similar attack methods are also possible in the more large-scale ICS testbed.
- Protect all related components such as AI, IoT devices, etc. in addition to the ICS.
- For future work, we will investigate the attack surface against OPC UA.

Thank you for your attention.

coe@sisoc.org

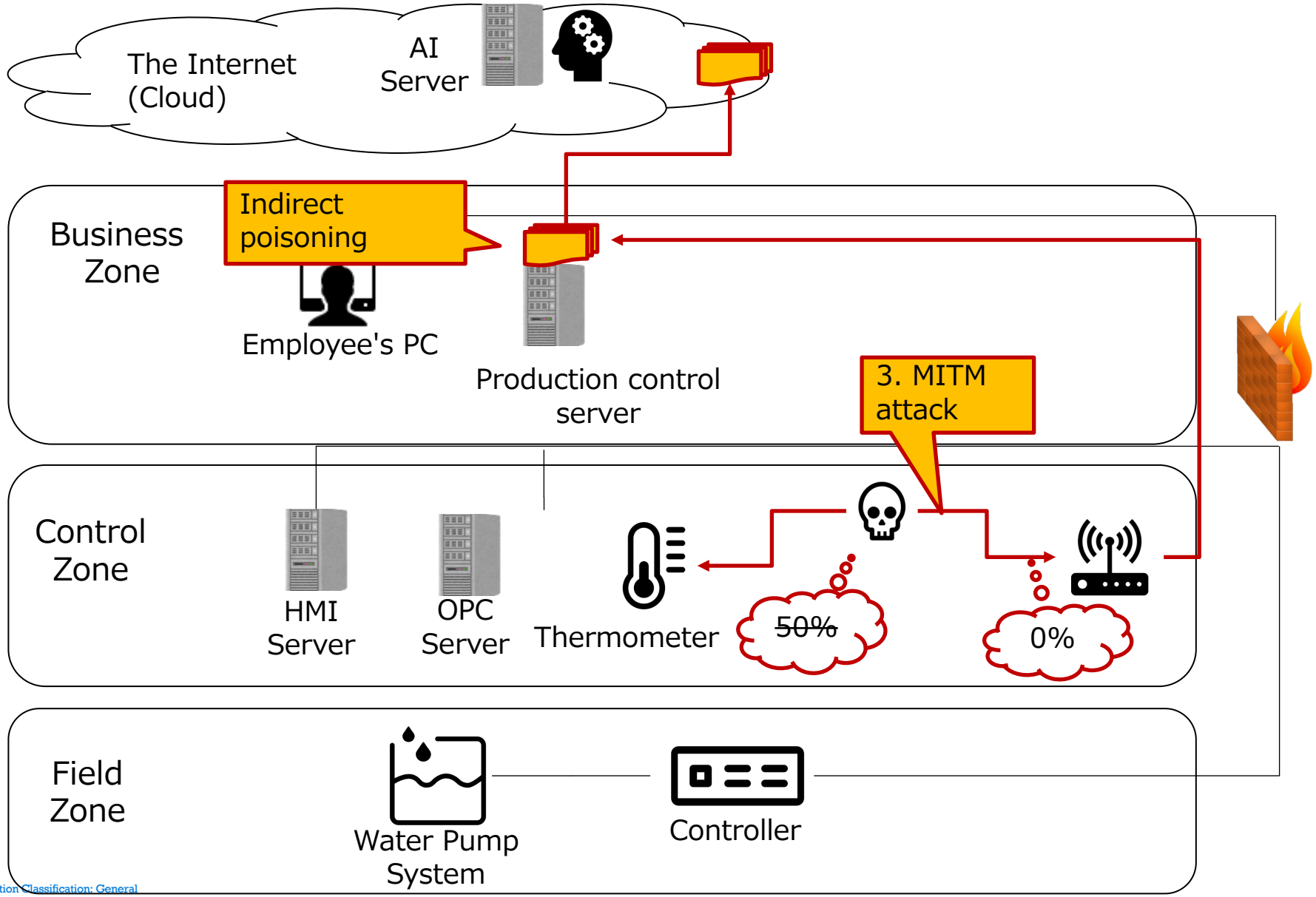
https://github.com/sisoc-tokyo/AttackDemoTookkit_Industry4

Reference

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.
Employee's PC	Windows 10	Business zone	A PC used by ICS operators.
Production control Server	WindowsServer2008 R2	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.

Attack scenario against IoT



Countermeasures

- Protect dataset from unauthorized access or manipulation using encryption, access control, etc.
- Check and evaluate dataset and AI model in suitable timing, then remove data that cause high error rates in classification from the dataset.
- Monitor ICS communization payloads and detect unusual change against the ICS.