**Virtual Industrial Control System for Education of Cybersecurit**y

A. Harada a, S. Yamada b and J. Sato \*,c

a NIT, Yonago College, Dept. of Electric and Electronic Engineering, Yonago, Japan

b NIT, Ishikawa College, Dept. of Electric and Electronic Engineering, Tubata, Japan

c NIT, Tsuruoka College, Dept. of Creative Engineering, Tsuruoka, Japan

\* jun@tsuruoka-nct.ac.jp

**Abstract**

**This research aims to realize an industrial control education environment using digital twin technology that can actually be used in student experiments and practical training, as well as the climate suitable for cybersecurity education in Industrial Control Systems (such as Plants, Manufacturing Lines, etc.), to develop human resources who can respond to the paradigm shift.**

**Keywords:** *Cyber Security, Security Education, Operational Technology, Industrial Control System, Digital Twin*

**Introduction**

The manufacturing industry is undergoing a rapid trend toward digitalization. As a result, information and manufacturing systems are integrated into today's industrial systems. In this context, damage caused by cyber-attacks has become apparent, and cyber-attacks on factories are on the rise domestically and internationally. As a result, there is an increasing need for cybersecurity measures and education in the manufacturing industry and factories.

The industrial automation industry has begun to develop designs with virtual commissioning based on digital twin models, and all of these development tasks are increasingly conducted in virtual space. However, no security education materials based on these technologies utilize cyber-physical space (CPS), which is free from time and space.

Therefore, in this study, we create a model that moves in a virtual space similar to that of the actual experimental equipment. These models can be configured as a simple digital twin of the experimental equipment that also exists in real space and can be linked to experiments and practical training using actual equipment as before. An environment will be created in which these models can be operated and exercised in a virtual space.

The models can control pressure and water level at the same time with control exercise equipment at NIT KOSEN Yonago College. The entire plant, including the pressure and water tank, will be modeled on a process simulator (Siemens SIMIT), and the controller (PLC) will be virtualized.

When experiments and practical training are conducted in a distance education environment using digital twin technology, the same educational effects can be expected as with conventional investigations and practical training using actual equipment. In addition, by combining experiments and practical training using existing equipment with extensive use of modelling and the distance education environment, it is possible to expand into large-scale, complex, and diverse fields that were previously unfeasible due to many constraints (space, cost, human resources, etc.), and to safely conduct practical cyber security exercises The new system also allows for safe and practical cyber security exercises to be undertaken.

**Digital Twin and Process Automation**

Digital twin technology plays a significant role in enhancing process automation by providing a virtual representation of physical assets, systems, or processes. Here are some key points highlighting the relationship between digital twin and process automation:

1. Virtual Representation: A digital twin is a virtual replica or model of a physical asset or system, such as a manufacturing plant, a production line, or a specific piece of equipment. In the context of process automation, digital twins represent the automation systems and associated processes in a virtual environment.
2. Real-time Monitoring and Control: Digital twins enable real-time monitoring and control of process automation systems. By connecting the digital twin to the actual automation systems, data can be collected from sensors, equipment, and other sources in real time. This data can then be used to monitor the performance, status, and conditions of the automation processes.
3. Predictive Analysis and Optimization: Digital twins facilitate predictive analysis and optimization of process automation systems. By integrating historical data, real-time data, and advanced analytics techniques, digital twins can provide insights into system behavior, identify potential issues or anomalies, and optimize process parameters for improved efficiency, quality, and productivity.
4. Testing and Simulation: Digital twins enable testing, simulation, and what-if scenarios for process automation systems. Before implementing changes or new automation strategies in the physical environment, the digital twin can be used to simulate and validate the impact of these changes. This reduces risks, optimizes decision-making, and minimizes downtime during implementation.
5. Remote Monitoring and Troubleshooting: Digital twins allow for remote monitoring and troubleshooting of process automation systems. By accessing the digital twin remotely, operators and maintenance personnel can analyze system performance, diagnose issues, and remotely implement corrective actions, reducing the need for physical presence on-site.
6. Lifecycle Management: Digital twins support the entire lifecycle of process automation systems, from design and development to operation and maintenance. They provide a unified platform for collaboration, data integration, and knowledge sharing among different stakeholders involved in the automation lifecycle.

By leveraging digital twin technology, process automation systems can be optimized, monitored, and controlled more effectively. Digital twins enable better decision-making, reduce downtime, and improve overall system performance, ultimately leading to enhanced productivity and operational efficiency in industrial processes.

Digital twins can play a crucial role in enhancing the security of process automation systems. Here are some key reasons why digital twins are important for security:

1. Risk Assessment and Vulnerability Testing: Digital twins provide a safe and controlled environment for conducting risk assessments and vulnerability testing. Security professionals can simulate potential cyber threats and attacks on the digital twin without impacting the actual process automation system. This helps in identifying vulnerabilities, weaknesses, and potential attack vectors that need to be addressed.
2. Real-time Monitoring and Anomaly Detection: Digital twins enable real-time monitoring of process automation systems and facilitate the detection of anomalies or suspicious behavior. By comparing the behavior of the digital twin with the actual system, security teams can quickly identify deviations or abnormal activities that may indicate a security breach or unauthorized access.
3. Incident Response and Recovery: In the event of a security incident or breach, digital twins provide a valuable resource for incident response and recovery efforts. By analyzing the state of the digital twin prior to the incident, security teams can better understand the impact, identify the root cause, and develop appropriate remediation strategies to mitigate the effects of the incident on the actual system.
4. Testing Security Controls and Countermeasures: Digital twins allow security controls and countermeasures to be tested and validated in a controlled environment. By implementing security measures within the digital twin, such as access controls, encryption, or intrusion detection systems, their effectiveness and impact on the overall system can be evaluated before implementation in the live process automation environment.
5. Training and Education: Digital twins serve as valuable tools for training and educating personnel on security best practices and response procedures. Security teams, operators, and maintenance personnel can undergo simulated training exercises within the digital twin environment to enhance their understanding of security threats, incident response protocols, and proper security practices.
6. Continuous Improvement: Digital twins facilitate continuous improvement of security measures in process automation systems. By monitoring the performance and behavior of the digital twin, security teams can identify areas for improvement, implement security updates or patches, and ensure that the system remains resilient to evolving cyber threats.

By leveraging digital twins for security purposes, organizations can proactively assess risks, detect anomalies, respond effectively to security incidents, and continuously enhance the security posture of their process automation systems. Digital twins provide a valuable tool for testing, monitoring, and improving security controls while minimizing the potential impact on the live production environment.

**Digital Twin System Configuration**

First, we will introduce the water plant exercise equipment at Yonago KOSEN, which is the subject of Digital Twin. The exercise apparatus has a water level control unit and a pressure control unit. Figure 1 shows a photograph of the device, Figure 2 shows a photograph of each control unit, Figure 3 shows a front view drawing, and Figure 4 shows a P&I diagram of the plant.



Figure 1 Overview of Plant

屋内, グリーン, 座る, テーブル が含まれている画像

自動的に生成された説明屋内, グリーン, 座る, 金属 が含まれている画像

自動的に生成された説明

1. Water Level Control (b) Pressure Control

Figure 2 Control Units

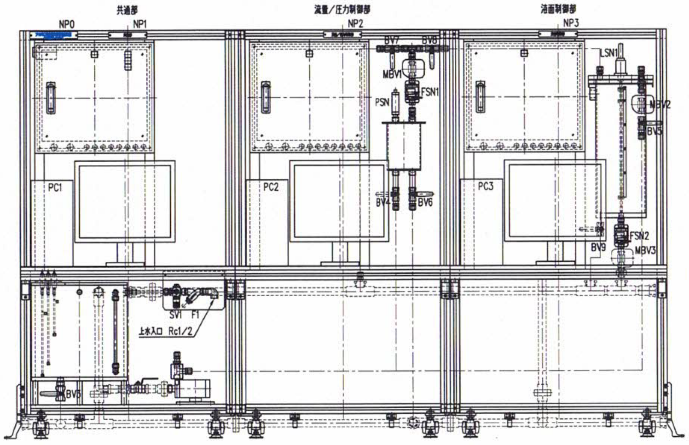
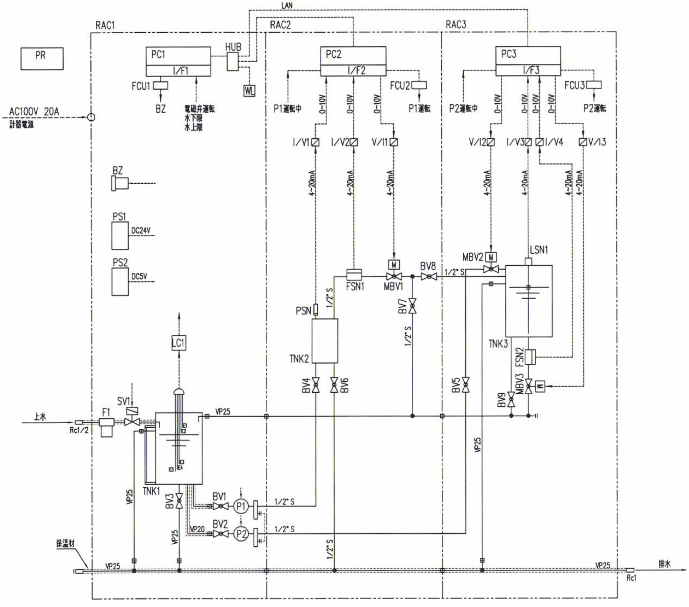


Figure 3 Front View



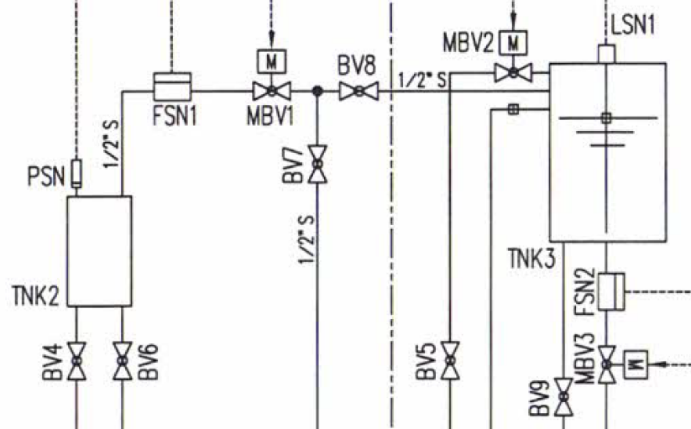


Figure 4 P&I Diagram

Next, the actual machine is modeled and the control code for this model is created. Figures 5 and 6 show part of the model created by Siemens SIMIT.

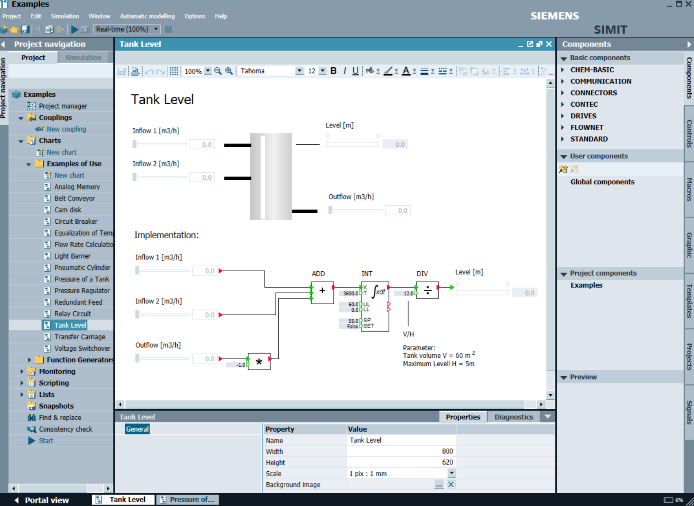


Figure 5 Behaviour Model by SIMIT (Level Control)

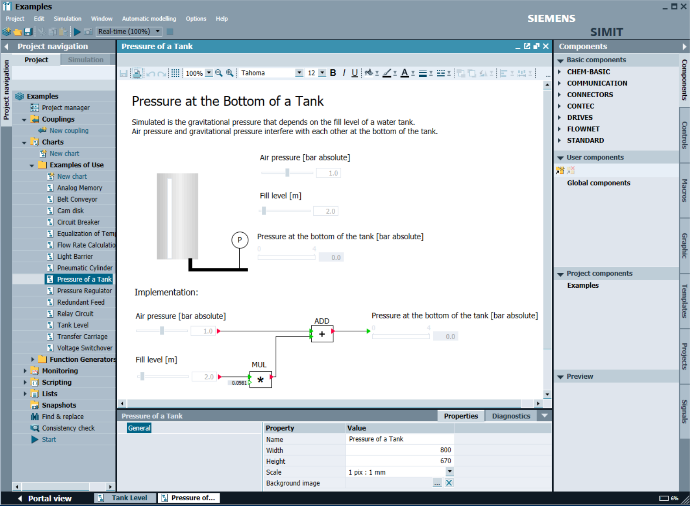


Figure 6 Behaviour Model by SIMIT (Pressure Control)

In this case, the actual machine and virtual machine can be used as controllers. Siemens S7-1200 was used as the real PLC and Siemens PLCSim Advanced (Figure 7) as the virtual PLC.

グラフィカル ユーザー インターフェイス, アプリケーション

自動的に生成された説明

Figure 7 Virtual PLC (Siemens PLCSim Advanced)

The control code used the usual PLC development tools and Siemens PCS7, a process system development environment. Figure 8 shows the control code in CFC (Continuous Flow Chart) format.

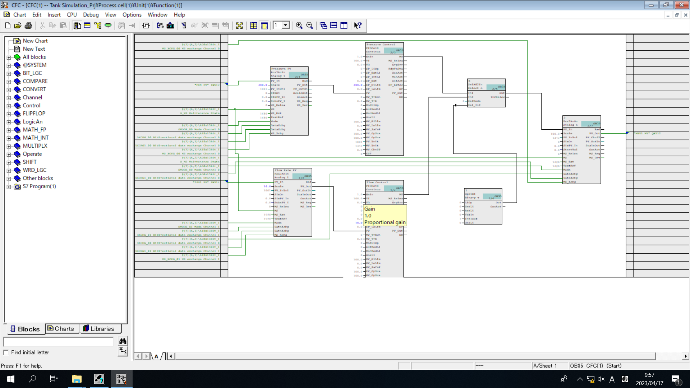


Figure 8 CFC (Continuous Flow Chart)

The operational status of the entire system is checked by the HMI (Human Machine Interface) shown in Figure 9, which was created in Siemens WinCC. The behavior of the virtual plant can be checked on SIMIT as shown in Figure 10.

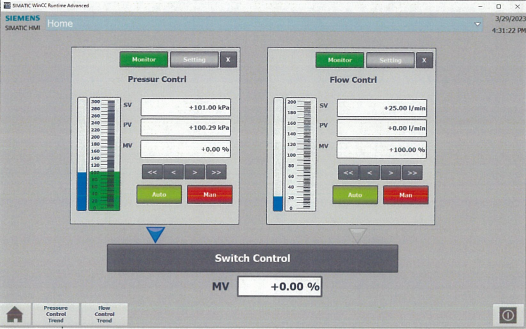


Figure 9 HMI (Human Machine Interface) Panel View

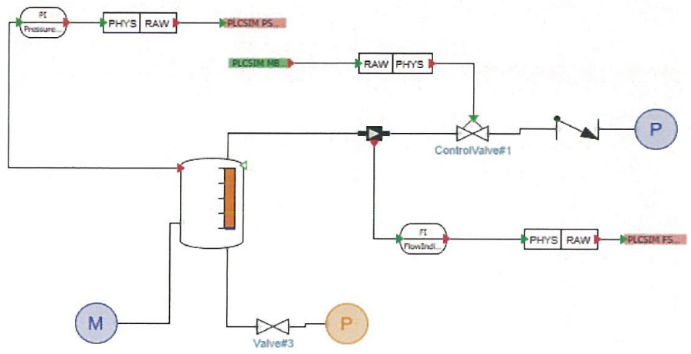


Figure 10 View of Pressure Tank in SIMIT

**Conclusions**

Using the process control system development environment, a virtual plant system was constructed, which was combined with actual equipment to realize a Digital Twin environment. This environment is effective for the development of plant control education, and also provides an environment where security exercises for plants can be conducted safely.

**References**

Sube Singh, Ankit Barde, Biswajit Mahanty, M.K. Tiwari (2019) Digital Twin Driven Inclusive Manufacturing Using Emerging Technologies, IFAC-PapersOnLine, Volume 52, Issue 13, Pages 2225-2230

H. P. Lin, et al. (2020) Digital Twin-Enabled Predictive Maintenance Framework for Industrial Automation Systems, 2020 International Conference on High Performance Computing & Simulation

Adrien Bécue, et al. (2021) A New Concept of Digital Twin Supporting Optimization and Resilience of Factories of the Future, Appl. Sci. 2020, 10(13), 4482

ISA/IEC 62443: The ISA/IEC 62443 series of standards

NIST SP 800-82: The National Institute of Standards and Technology (NIST)

IEC 61511: The IEC 61511 standard

ISO/IEC 27001

IEC 62443-3-3

DHS ICS-CERT: The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)