IPA Better Life with IT

ICSCoE REPORT

Industrial Cyber Security Center of Excellence

3.25.2021

vol. 07

The ICSCoE Report is a public relations newsletter on ICSCoE's activities.

The 4th Core Human Resource Development Program has started

In July 2020, the Industrial Cyber Security Center of Excellence (ICSCoE) held the opening ceremony for the fourth Core Human Resource Development Program, welcoming 47 trainees expected to play a leading role in cybersecurity for Japan's future social infrastructure.

For the current program year, we organized the opening ceremony amid coronavirus (COVID-19) pandemic by taking necessary infectious disease control measures, such as requiring all participants to wear a face mask, ensuring a sufficient distance between seats, and installing an acrylic panel on the podium.

Dr. ENDO, Director General of ICSCoE, encouraging trainees

Dr. TOMITA, Chairman of Information-Technology Promotion Agency, Japan (IPA), strongly encouraged every trainee to be aware of his/her missions, set goals, and proactively work on them in order to enrich a year even under the COVID-19 pandemic.

Dr. ENDO, Director General of ICSCoE, mentioned growing importance of security in handling data as our society has been shifting from “Information Society” to “Data Society”. He also inspired the new trainees to "aim for a top-class leader with a strong will, who could direct the entire company, industry, and even country", throughout a year.

Introducing trainees

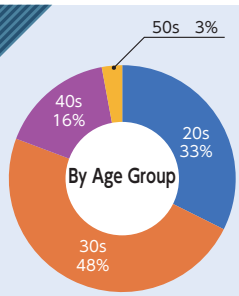
Mr. NISHIYAMA Keita, then-Director-General of Commerce and Information Policy Bureau of the Ministry of Economy, Trade, and Industry (METI), gave his speech to encourage the trainees to not only acquire new knowledge but also deconstruct the ideas that they developed throughout their career, and newly reconstruct those ideas through meeting new colleagues in this program.

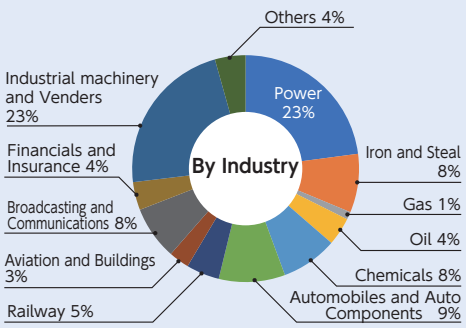
After the ceremony, trainees were introduced to lecturers and introduced themselves to each other to start the year-long learning process.

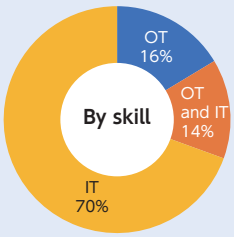
Core Human Resource Development Program

FACT & DATA

Profile of 1st to 4th cohorts







The 3rd Core Human Resource Development Program was completed

The 3rd Core Human Resource Development Program Completion Ceremony (June 2020)

The completion ceremony for the third Core Human Resource Development Program was held in June 2020. At the ceremony, the 3rd cohorts received a video message from Mr. KAJIYAMA, Minister of Economy, Trade and Industry. In this video, the minister encouraged the 3rd cohorts, “I would expect you to play an active role in various fields of society as core personnel responsible for the security for the Japanese society at large”. On behalf of all 3rd cohorts, Mr. ANDO Satoshi (Central Japan Railway Company) looked back over the year-long program and addressed his new determination.

Address by Mr. ANDO Satoshi, Central Japan Railway Company

Mr. ANDO representing 3rd Cohort

As the representative of the 3rd cohort, I have three things to talk about.

Firstly, I feel grateful for making us possible to face a day to complete this program. After the Japanese government had declared a state of emergency due to the spread of COVID-19, all classes were conducted remotely, and we were worried whether we could complete the program. We would not be here today to celebrate our completion ceremony if everyone involved in this program had not made exertions to continue this program. I genuinely express my gratitude to them.

Secondly, I would like to look back on the past year. When I think of the opening ceremony held a year ago, I remember being very nervous. The program expected us to become an expert, who could protect Japan’s critical infrastructures from the aspect of cybersecurity, but I was worried whether it could be possible for me to become such personnel. When I looked around, everyone had a nervous expression that made me more anxious. A year past since then. All of us here achieved excellent results from our final projects and proved our abilities to play an active role as core human resources.

Now that I think of the program, first, we had well-thought-out curricula; thus, even inexperienced trainees could learn security systems step by step. We worked hard on practical exercises and “hands on practices” in an environment similar to the actual sites. We also learned soft skills required as core human resources, who could serve as a bridge between upper management and field staff. Furthermore, we realized that we had narrow and inward views and focused only on Japan through the overseas deployment exercises.

The instructors enthusiastically responded to our desires to learn. They organized the special lectures by external experts for the trainees, who were eager to deepen their knowledge, and guided us after-lecture hours when we needed I saw their attitudes of thoroughly facing each one of the trainees and felt they were dependable.

Building relationships among the trainees was the most beneficial aspect of this program. Sixty-nine trainees with great individuality got together from various industries. We carried out discussions and tried to improve by leaning from others within our curricula during the daytime, and each of us cultivated friendships with others by playing futsal and other activities after work. We kept communicating among the trainees even when working remotely; thus, we could complete our final projects. I was truly blessed to spend a year surrounded by a group of people who could learn from, inspire each other, and were reliable.

Thirdly and finally, I would like to express our resolution for the future. We can say that very harsh conditions will await us on our return. However, we, the third cohort, have 69 colleagues. Besides, we have cultivated relationships with over 150 senior colleagues from the 1st and 2nd cohorts, as well as instructors and other experts. We believe that we will be able to strive with any difficulties with these colleagues. We will continue to work on operations, with a sense of mission, in order to support Japan’s critical infrastructures from cybersecurity perspectives once we return to our company. I must thank you most sincerely.

A video message from Mr. KAJIYAMA, Minister of Economy, Trade and Industry

The 3rd cohort Efforts from the final project

We introduce four of our 25 projects.

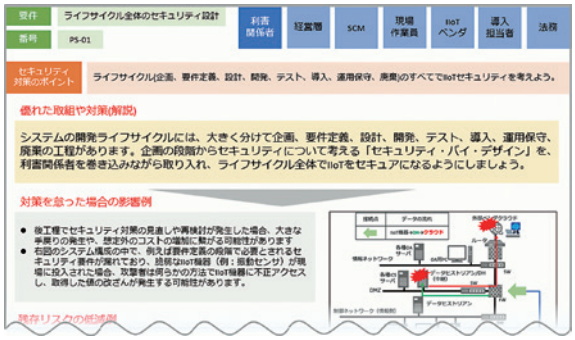
1 Security for IIoT Implementation

As a part of DX (Digital Transformation) initiatives in the manufacturing industry, it is expected to implement and use IoT for industrial applications (IIoT: Industrial Internet of Things) in factories. However, some in-house systems are designed under the assumption of not connecting to external networks; therefore, considering its security becomes a critical issue when implementing IIoT.

For that reason, in this project, we focused on security considerations of implementing IIoT and developed a workflow and manual of security measure guidelines for implementing new systems.

Some IIoT devices, operated by wireless communications or batteries, can be installed without extensive construction works and might be overlooked when considering their security. Thus, the team organized the workflows that the person responsible for implementations could consult with security personnel at an early stage.

The manual also provides clear and concise explanations of security measures mentioned in “Good Practices for Security of Internet of Things in the Context of Smart Manufacturing” published by ENISA. Furthermore, in our manual, the team illustrated the stakeholders with whom we need to collaborate and the possible impacts resulting from neglecting countermeasures in order to consider risks specifically and advance our measures.



Comments from Team

This project started with recognizing our issues and agendas: “we could not proceed with risk analysis just by reading IIoT security guidelines”, “there are multiple guidelines with different perspectives so that it was difficult for us to read them all at one time”, and “we wanted to put together these guidelines into a foundation for implementing to our own company”.

We would like to contribute to safe factory operations as security personnel by taking advantage of the lessons learned at ICSCoE and tailoring the developed manuals suitable to our own company’s business styles.

2 Optimization of asset management in control systems

As the spread of IoT and the advancement of DX, the opportunities for connecting control systems at manufacturing sites to information networks in order to improve productivity have been increasing.To minimize cybersecurity risks in such manufacturing environments, “Establishing the Context” defined in ISO 31000 - asset management stated in risk management (identification of protected assets), becomes essential.However, there are challenges in control system asset management: an absence of guidelines on specific methods and issues, countless manual procedures, a lack of cybersecurity perspectives, etc.

In this project, the team aimed to contribute to improving the cybersecurity for the organization, formulate the guidelines presenting the necessities and directions of asset management on control systems and guidebooks and checklists encouraging specific activities. The team also developed a tool enabling us to recognize and visualize devices connected to the network and verified the effectiveness of automated asset management.

To learn more about the deliverables of this project, “Asset Management Guidelines for Control Systems”, “Asset Management Checklists for Control Systems”, and “Asset Management for Control Systems Handbooks”, please check the ICSCoE website. You can also find the above-mentioned tools on external websites.

〈Introduction page for the final project〉
https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project.html

Comments from Team

We hope that the guidelines and tools developed in this project will help you realize the importance of asset management on control systems or motivate you to practice asset management.

We used our simulated plant environment to verify the effectiveness of the tools we developed. The ability to conduct such verification works is a unique learning experience at ICSCoE.

3 Cloud Security Guidelines

Regarding cloud services, the core technology of DX, various security guidelines have been released in Japan and overseas, and the number of companies promoting to apply these guidelines has been increasing. However, we see some issues necessary to be addressed, such as “each guideline has different principles and target audiences” and “we have not prepared or sufficiently disseminated uniform guidelines for our internal security policies.”

In consequence, the team mapped the contents of “Guideline of Effectively Managing Security Service in the Cloud” (issued by Cloud Security Alliance Japan) and the auditing rules of commercial cloud services such as AWS and Azure and developed a “Guideline Summary Sheet” based on “Information Security Management Guidelines for the use of Cloud Computing Services” (issued by Ministry of Economy, Trade and Industry in 2013). This sheet enables us to select and consolidate the contents, which can determine quantitatively from user’s perspective, and to check the contents and rules of each guideline simultaneously. In addition, the team created a “Website Deployment Template”, which would enable us to build a secure website for each cloud service automatically, and an “Auditing Rules Template” which uses the auditing functions of each cloud service and would set the rules following the guidelines automatically. These templates are available for both completed and current trainees and companies dispatching them; thus, we expect that these companies will improve the security level of their cloud environment.

Comments from Team

In this project, we not only consolidated the guidelines but also developed the templates available for AWS and Azure, and we believe that we did contribute to laying the foundation for using a secure cloud environment. Each cloud service keeps evolving; thus, the idea of "you have done this much so you will have no problem" no longer applies. We realized the necessity of adapting to changes as a user.

4 OT ATTACK

The team started this project to respond to the desires of security personnel: “I want to perform advanced penetration tests on in-house products or implemented products” and “I want to acquire skills in making concrete proposals on how to protect our plants”.

To fulfill their desires, the team first organized the DoS testing methods for security and network products and then developed a penetration testing tool. Additionally, the trainees evaluated the developed tool, performed penetration tests on actual products, and confirmed its effectiveness. They also explored the strategies to avoid and reduce risks. We expect that they will utilize the combination of the developed tool and the acquired skills and evaluate the robustness of in-house products or implemented products and promote countermeasures once returning to each dispatched company.

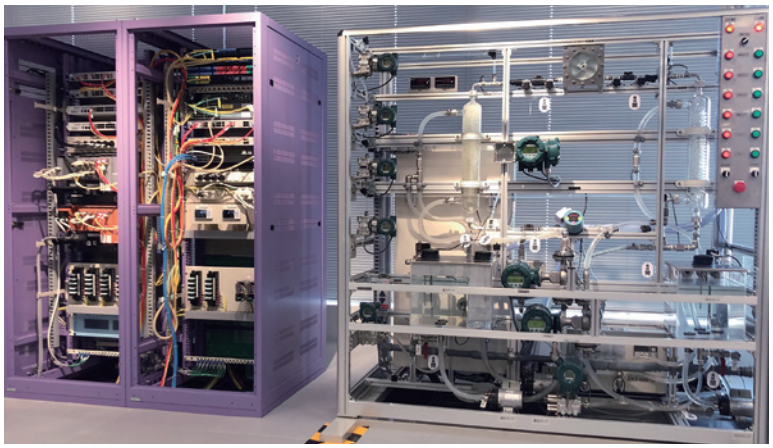
With the simulated plants as a topic for the project, the trainees identified the possible threats per plant and developed their attack scenarios accordingly. They arranged and implemented the defense methods from the scenarios and examined the countermeasure automation based on the fundamentals of SOAR. We expect they will contribute to improving plant security by utilizing the skills in promoting defense methods acquired through these activities and the basic concepts of countermeasure automation.

Comments from Team

As we learned the advanced penetration testing methods at ICSCoE, we started thinking of the necessity to conduct these tests on the products we have developed and may implement in our plants. We believe we will be able to conduct in-house tests on products by utilizing the tools developed in this project and take countermeasures based on test results. We also believe that we may contribute to further improvement in our product robustness through these activities.

ICSCoE built a new plant “Thermal Resource Distributed Control System”

ICSCoE built a PA (Process Automation) plant in Akihabara UDX as the new training facility, which centrally controls fluids: such as liquids and gases. The new plant named “Thermal Resource Distributed Control System” is basically controlled by DCS (Distributed Control System) in which each element making up the system is controlled while providing feedbacks. This system will broaden the scope of future training. The following is an overview of the new plant and its significance in Q&A format.



Thermal Energy Conversion Plant

Q1 Why chose “Thermal Resource Distributed Control System”?

We have been considering introducing a PA plant since ICSCoE was established. However, it is not possible to install a chemical plant using dangerous chemicals in an office building. When we thought of a system installable and allowing us to practice PA control, the answer we reached was the “Thermal Resource Distributed Control System”, which controls “heating, cooling and agitating water”.

Q2 What kind of system is it?

Thermal Resource Distributed Control System consists of two plants, each of which has different functions and a system integrally controlling them.

The first plant is the “Thermal Energy Conversion Plant”. This plant evaporates a substance with a lower boiling point than water into gas using the heat of hot water, and this vaporized gas spins a turbine to generate electricity. It also returns the vaporized substance back to liquid by cooling with cold water and then uses that liquid again to generate electricity. The second plant is the “Thermal Resource Circulation Plant”. This plant circulates hot water at specified water quality and temperature. The plant system measures the turbidity, pH, and chlorine concentration of the hot water, and it comprehensively controls water quality by mixing and agitating the chemicals in accordance with the water quality. The plant also controls the water temperature to keep the specified level by operating the heater and injecting cooling water or hot water into the system whenever required.

In addition, the “Thermal Resource Distribution Control System” continuously and automatically controls the entire system by connecting the two plants and circulating hot water (thermal resource) between them.

Thermal Resource Circulation Plant

Q3 Does it expand the scope of exercises at ICSCoE?

Indeed, it enables comprehensive control and prevention exercises using DCS in various fields such as electric power, gas, oil, and chemicals. In particular, the trainees will be able to perform control and prevention exercises dealing with fluids not as desktop experiments but physical devices.

Q4 What is the significance of exercises utilizing our new plants?

DCS is used in various industry fields; however, it poses a substantial risk of causing serious damages once it is targeted by cyber attacks. We believe that enabling the trainees to learn countermeasures through exercises utilizing these new plants is highly meaningful for Japan's social and industrial infrastructures to strengthen their protection capabilities.

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

Bunkyo Green Court Center Office,
2-28-8 Honkomagome, Bunkyo-ku, Tokyo, 113-6591
TEL 03-5978-7554 FAX 03-5978-7513