Delights and Debts of Computerization

Seiichi Shin
Graduate School of Informatics and Engineering,
the University of Electro-Communications

The year 1972, when I was a high-school student, saw the advent of micro-computers, which were the result of the confluence of the computer revolution and the silicon revolution. While I continued my studying to improve my level in many subjects in college and graduate school, micro-computers were being increasingly introduced into various instruments such as measurement and control devices, home appliances, and automobiles. Thanks to micro-computers, today's society has become very convenient (although we had imagined the 21st century would be more futuristic). Take a smartphone as an example. The smartphone, which almost everyone in Japan from children to the elderly carries about, with micro-computers installed in it can direct you to anywhere you want while giving you information about the destination, and enable you to pay your fare with it. On your way, you can also get food and drinks with it. Of course, this gadget can be used for various other purposes including text and image messaging, web browsing, and playing games to kill time.

Until the end of the last century, people made every effort to computerize various instruments by mounting micro-computers in them. Starting from highly technical instruments for measurement and control, computerization has expanded to cover consumer products. After this movement subsided around 2000, the age of networking started, in which people can enjoy advanced benefits by connecting multiple micro-computers not just a single unit.

In recent years, micro-computerizing and networking are being perfected. Automobiles, in each of which nearly 100 micro-computers are installed, are making use of various services via a mobile phone network and vehicle information communication system (VICS) network. Home appliances such as televisions, video devices, interphones, air-conditioners, refrigerators, washing machines, microwave ovens, and electronic rice cookers with micro-computers installed in them are also connected via a power line communication (PLC) network and wireless LAN network. In addition, as represented by the word "V2H (Vehicle to Home)," both are working together not only via information system networks but also in terms of energy.

Not only such consumer products but also critical infrastructure for electricity, gas, water supply and wastewater treatment, transportation networks, and communication networks are being micro-computerized and networked. Of course, they are deepening their cooperation with home appliances and automobiles. The expression "Internet of Things (IoT)", the expression that puts all these 'things' together, and "big data" are attracting attention.

When I was young, I realized the huge potential in micro-computer chips and since then I have been deeply involved in the process of improving them and disseminating them throughout the world. As an engineer, I am delighted about this. However, if I am asked whether I am satisfied, I answer "No." In fact, I have two "debts." Without settling these "debts," I will never be satisfied with the situation.

The first "debt" is the "black box" - a side effect of micro-computerizing. Micro-computers in an automobile contain hundreds of thousands of lines of software, while in a smartphone tens of millions of lines. In a PC, one hundred million lines of software are installed. Usually, one page paper contains a little less than 40 lines, and 100 pages can constitute a book. To make calculations easy, let the lines contained in a book be 5,000. The software in an automobile is equivalent to several books; the software in a smartphone is 1,000 books; and the software in a PC is 10,000 books. You can stock 100 books on your bookshelf, but 1,000 books need a vault, and 10,000 volumes require the space of a library. This amount of information is beyond your comprehension.

People in general can use smartphones for daily purposes. However, they do not know how it works inside and what it is communicating with. In fact, even professionals do not understand everything. Specialists are also human; their understanding is limited to about ten books at a time. The information equivalent to books on a bookshelf is beyond human capacity, to say nothing of those in a vault or library.

This is only about software. Mechanical parts and electronic parts are working with it. People are surrounded by micro-computerized products that neither makers nor users can understand. This is modern life today, and it is a big problem.

To solve this problem, a framework that systematically deals with mechanical, electronic and software parts is indispensable.

With the help of Yokogawa Electric Corporation, since 2006, our university has been providing a training course for graduates to develop advanced IT specialists. In this course, practical education is given to graduates, in which they proceed with designs while graphically simulating cooperation among parts using a CAD system for control system design. In addition, our university helps people in general to understand the essence of micro-computerizing and networking through open labs and visiting lectures at high schools.

The other "debt" is a cyber-security issue. There is no utopia where all people are good. Even if it exists, such a place is full of vulnerability. A group of the naive is easy prey for the evil.

We must admit that some people are good and others are not. Networking is convenient but vulnerable. Security software is supposed to be used for PCs. For information systems, firewalls are indispensable. Similarly, at present, appropriate security measures are needed for control systems that are networked.

In 2010, when such measures were not common, a uranium enriching plant in Natanz, Iran was exposed to cyber-attacks. In the Great East Japan Earthquake on March 11, 2011, critical infrastructure was destroyed. The supply of electricity, gas, and water, which most people think are available at any time, was disrupted. Trains that should arrive on time were destroyed, and mobile phones that should get through suddenly became useless. The aftermath was not limited to the stricken area. A tsunami caused the nuclear disaster at the Fukushima Daiichi Nuclear Power Plant, and the resulting power shortage forced the rolling blackouts within other areas covered by Tokyo Electric Power Corporation. People all over Japan are still affected by power shortages caused by the shutdown of nuclear power plants and the resulting surge in energy prices.

Followed by these two incidents, the Control System Security Center (CSSC) was set up in March 2012 as a technology research association approved by the Ministry of Economy, Trade and Industry (METI) in Japan. Yokogawa, an initial member of CSSC, had been involved in developing cyber-security measures for control systems long before such problems occurred. The Society of Instrument and Control Engineers had tackled cyber-security problems at its industrial application division since 2004, and worked with the Japan Electric Measuring Instruments Manufacturers' Association (JEMIMA) and the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) to publicize the importance of this issue and disseminate security measures. Such advanced activities by those organizations have facilitated the quick setting-up of CSSC.

In May 2013, CSSC set up the Tohoku Tagajo Headquarters in the Miyagi Reconstruction Park, constructed on a vacant lot previously used as the site for a Sony plant before the earthquake, in Tagajo-shi, Miyagi Prefecture, an area stricken by the Great East Japan Earthquake, and opened seven simulation plants for education and research on cyber-security measures.

Control systems differ in the power, gas, water supply, and other industries and it is difficult to perform research and development (R&D) in facilities in operation, so simulation plants are indispensable for R&D of these systems. Actually, there are no other sites that are equipped with as many as seven simulation plants covering various critical infrastructures. Owing to this distinctive feature, many VIPs both from in and outside Japan who are interested in cyber security visited the headquarters after the opening.

A noteworthy fact in 2013 was the start of two certification services with the help of METI. One is the embedded device security assessment (EDSA) certification. In July 2014, CSSC certified Yokogawa's CENTUM VP production control system and Hitachi's HISEC 04/R900E controller. Meanwhile, Yokogawa acquired a similar certification from the ISA Security Compliance Institute (ISCI) in the US for its ProSafe-RS safety instrumented system in January 2014. The knowledge obtained through acquiring this certification is made good use of for CSSC's certification service, and CSSC is also working with ISCI to expand the service.

Another certification service is for the cyber security management system (CSMS), which is promoted by the Japan Information Processing Development Center (JIPDEC). This management system is based on the information security management system (ISMS), for which more than 4,000 companies are certified in Japan. In the CSMS, security management is expanded to cover control systems including sensors and actuators. In April 2014, CSSC gave the world's first preliminary certification to Yokogawa Solution Service and Mitsubishi Chemical Engineering. The CSMS certification service is also offered by CSSC.

These days, third-party certification is highly evaluated. You can promote the merits of your products. This is self-certification and only self-satisfaction. Second-party certification is widely performed, in which customers inspect products on acceptance. However, standards differ for each customer. Third-party certification is performed by outside independent organizations applying a unified standard. This secures the independency of certification and suppliers can deliver their products to many customers with a single certification. In addition, customers can purchase products based on a unified standard from a wide variety of suppliers.

The 20th century was the age of mass production. Because of the shortage of goods, it was necessary to manufacture products in large quantities at low cost. In the mature society of the 21st century, however, safety, security, and differentiation are required. Third-party certification secures the former two conditions. The products and production systems can quickly satisfy individual requirements presuming the provided platform of safety and security are expected. CSSC is supposed to develop such platform to provide safety and security to people both in and outside Japan. In addition, each company in the association is supposed to achieve further convenience.

My life as a researcher and engineer was full of excitement. Settling the two "debts" is my remaining task. The late Hisashi Inoue, a Japanese famous playwright, said "Make the difficult easy, the easy profound, and the profound interesting." With these words in mind, I will educate people about the mechanisms of micro-computerized devices, and will proceed with the development of cyber-security measures.