Technotalk

People and Systems Working in Harmony to Make Social Infrastructure More Resilient

Makoto Takahashi, Ph.D Professor, Management of Science & Technology Department, Graduate School of Engineering, Tohoku University
Shuji Senoo Senior Director, Advanced Security Technology Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd.
Masahiro Mimura, Ph.D. Department Manager, Enterprise Systems Research Department, Yokohama Research Laboratory, Hitachi, Ltd.
Toshihiko Nakano, Ph.D. General Manager, Control System Security Center, Omika Works, Infrastructure Systems Company, Hitachi, Ltd.
Toshiaki Arai, Ph.D. CTO, Defense Systems Company, Hitachi, Ltd.

Cyber-attacks and other threats to information security have been growing in recent years. Meanwhile, rising concerns about natural disasters and terrorism have made the provision of comprehensive countermeasures against events such as these an issue for society. Along with putting measures in place to counter growing threats, maintaining the safety of social infrastructure systems also requires appropriate measures for minimizing damage. Hitachi has built up a portfolio of security technologies in fields ranging from social infrastructure to physical security. Through total security solutions that utilize these technologies, Hitachi intends to help create a society that is safer and more secure.

Defense in Depth to Deal with the Unexpected

Arai: Along with the growth in threats to the safety and security of society, concern about the security of social infrastructure is also growing. Professor Takahashi currently heads the Tohoku Tagajo Headquarter of the Control System Security Center, of which Hitachi is a member. Can you please explain which aspects of social infrastructure security you are looking at in particular?

Takahashi: My main research topic is the security of large systems such as nuclear power plants or air traffic control systems that, if disrupted, have a major impact on society. I am looking in particular at how to improve the overall security of systems, including human factors. The idea of the "unexpected" was a key legacy of the Great East Japan Earthquake. However much you allow for various different situations, it will not prevent the unexpected from happening. Whatever capabilities you build into your systems, there will always remain some aspects where you must rely on the adaptability and flexibility of people to deal with the unexpected. My research looks at how these human factors can make

Makoto Takahashi, Ph.D

Professor, Management of Science & Technology Department, Graduate School of Engineering, Tohoku University

Graduated in 1986 with a degree in nuclear engineering from the School of Engineering, Tohoku University, and earned a doctoral degree in nuclear engineering from the Graduate School of Engineering, Tohoku University in 1991. After appointments that included assistant professor at the Graduate School of Engineering, Tohoku University in 2000, he took up his current position in 2011. He is also currently the head of the Tohoku Tagajo Headquarter of the Control System Security Center. He is a director of the Atomic Energy Society of Japan and of the Human Interface Society. He specializes in cognitive engineering, system engineering, and human error analysis.

Shuji Senoo

Senior Director, Advanced Security Technology Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd.

Joined Hitachi, Ltd. in 1984. After working as a system engineer in the public sector division of Hitachi that develops systems for local government and other government agencies, he commenced his current security-related work in 2002.

overall systems safer.

Senoo: In the case of cyber-security where new viruses and other forms of malware are continually emerging, there is no hope of being able to anticipate all risks in advance. Taking the unexpected as a given, it is important to focus on damage limitation, which means looking at how to reduce the unexpected and how to minimize damage when it does occur.

Mimura: Targeted attacks have recently become a problem for cyber-security. These are attacks that target specific devices by exploiting little-known vulnerabilities. Because the tendency in the past was to spread viruses far and wide, vulnerabilities could be identified and patched quickly. Targeted attacks on the other hand, because they are directed at a limited number of targets, are difficult to spot and are capable of doing large amounts of damage before being detected. Along with the elimination of vulnerabilities, "risk hedging" techniques that minimize damage also have an important role in dealing with this new type of threat.

Takahashi: In this sense, I also believe that a "defense in depth" approach is important. This is a fundamental concept in the military realm. Rather than erecting protective measures in duplicate or triplicate, what it means is ensuring that if one line of defense fails, other lines will continue to function. By adopting this practical approach as the basis of our planning, I believe that we can minimize the ultimate damage.

Extending Range of Regular Exercises, and Use of Information during Emergencies

Arai: Conducting command and control system training exercises is also important for reducing risks caused by human factors. Especially in the case of the emergencies that arise during a large disaster, a change in attitude is also crucial because of the different operations that are required compared to normal situations, such as working diligently through the observe, orient, decide, and act (OODA) loop.

Takahashi: In the case of large systems, simulators are used to perform exercises under near-real-world conditions. While these can include one-in-tens-of-million situations with multiple simultaneous incidents, their value depends on the details of the exercise itself. As scenario-based exercises are ineffective at delivering the unexpected, a worthwhile approach is to conduct planned exercises in which the scenario after a certain point is left undisclosed. Also, however many exercises are conducted, because the availability of information during an actual disaster can be a matter of life or death, it is also important to put measures in place for utilizing information during an emergency.

Senoo: The USA is proceeding with the adoption of a standard model for information sharing called the National Information Exchange Model (NIEM) so that preexisting infrastructure for sharing information between government, agencies, municipalities, and other participants will be available during an emergency such as a disaster or terrorist attack, and to establish the mechanisms for the smooth flow of information between the various systems involved. Japan is also looking at open data practices that encourage the availability and use of public information collected and held by government agencies. However, numerous issues still remain. Together with the use of technologies such as those for preventing tampering, I believe that making public data available in a form that facilitates secondary use is essential to conducting

Masahiro Mimura, Ph.D.

Department Manager, Enterprise Systems Research Department, Yokohama Research Laboratory, Hitachi, Ltd.

Joined Hitachi, Ltd. in 1997. After working on the research and development of financial systems and of biometric and other security technologies and systems, he commenced work in 2012 on the research and development of financial and public sector solutions together with software productivity techniques used by these solutions, and of system security technology.
Dr. Mimura is a member of the Information Processing Society of Japan (IPSJ).

Toshihiko Nakano, Ph.D.

General Manager, Control System Security Center, Omika Works, Infrastructure Systems Company, Hitachi, Ltd.

Joined Hitachi, Ltd. in 1980. He is currently engaged in the development of security for social infrastructure systems. Dr. Nakano is a member of The Institute of Electrical Engineers of Japan (IEEJ).

operations appropriately during a disaster or other emergency.

Security Risks for Control Systems

Arai: Another human consideration is that, while progress has been made on information security management systems (ISMSs) and other measures for preventing information leaks and other unauthorized tampering with corporate information systems, there is a need for rethinking attitudes to the security of control systems.

Nakano: Whereas control systems in the past were closed systems and not seen as under threat from cyber-attacks, factors such as the use of general-purpose platforms, networking, and portable storage media mean that risks are growing. I believe we have an obligation to help raise general knowledge of security and risk awareness in the control systems field.

Senoo: Security requires more than just experts with specialist knowledge. The problem is that protection functions will only work if the staff responsible for day-to-day activities have a basic understanding of security. Otherwise, their naivety will leave them prone to opening files attached to targeted e-mail attacks, for example. The challenge for businesses, I believe, is to ensure that security knowledge is spread widely, not just among system engineers (SE) and other non-technical personnel.

Mimura: The idea that security involves work and cost is also deep-rooted, I believe. Along with emphasizing the importance of security, other areas I think we should be working on include adopting countermeasures against cyber-attacks that minimize the amount of human intervention required, and the use of information technology (IT) for automation and to support administrators.

Takahashi: An important factor when an actual cyber-attack occurs is to be able to determine quickly whether it is in fact a cyber-attack rather than simply an operational problem caused by a fault in the system. While one system-based technique is to use predefined signatures to detect attacks automatically, another important approach is to have countermeasures that provide a common operational picture (COP) and other appropriate information to the people who administer the system, and to support them in situation assessment, decision making, and other related tasks.

Senoo: Because security is a new field in the case of control systems in particular, there is no way of knowing what unexpected threats may arise. Accordingly, we are focusing on ways of issuing warnings as quickly as possible and providing assistance to administrators. One example is a solution we have developed that uses decoy servers in a system to detect virus intrusion and infection at an early stage, and that alerts administrators accordingly to prevent the infection from spreading. In the social infrastructure sector, in particular, where system availability is critical, the system is being built to operate continuously over long periods.

Nakano: Compliance with the IEC 62443 international standard for security is starting to become more common in the control system sector. I believe we need to contribute to this standardization process with a view to standardizing highly reliable techniques built up over time, with the aim of ensuring security everywhere from individual components up to entire systems, operations, and society.

Toshiaki Arai, Ph.D.

CTO, Defense Systems Company, Hitachi, Ltd.

Joined Hitachi, Ltd. in 1978. Prior to taking up his current position, Dr. Arai worked on information system research and development at the then Systems Development Laboratory.

Utilizing Human Factors to Enhance Resilience

Takahashi: A recent interest of mine has been the field of resilience engineering. While resilience normally refers to a system's ability to withstand or recover from a shock, the concept is also becoming important for security. Past security measures have sought to identify the cause when an incident occurs so that measures can be adopted to prevent it from happening again. While I certainly do not want to discredit that approach, there are also cases when, rather than focusing on rare examples of failure, it is better to analyze why practices work successfully in an ever-changing environment, and to implement them accordingly. Also essential to the progress of security technology, I believe, is an approach that focuses on why practices work and establishes processes for preventing incidents by enhancing resilience through human factors, such as people's ability to make accurate predictions, to respond, and to act with flexibility.

Nakano: In the event of a major disaster or other incident of a sort that happens only once in a lifetime, there is always a potential for panic, even among people who have been through numerous training exercises. What is needed to deal with such situations, I suspect, is to study past examples of success and failure, and to have systems that can supply the best possible information in a timely manner to assist people in decision making.

Takahashi: Getting people and systems to work in harmony will be increasingly important in the future. One example might be for machines and other systems to leave decisions to people during normal situations, but also to read their state of mind from biometric or other data and provide them with assistance in situations where they appear to be reaching the limit of their capabilities, the point where they are potentially becoming unreliable. If systems like this become possible, that would be the ideal. We have embarked on research into the basic technology for such systems, which we call adaptive interfaces.

Arai: Having people and machines working harmoniously together will also be critical for physical security within Japan, which will become increasingly important as we approach the Tokyo Olympics in 2020. Hitachi has strengths in IT and is hoping to use these skills to contribute to better physical security, by combining surveillance cameras and image recognition, for example.

Senoo: There will also be uses, I believe, for biometric authentication techniques such as finger vein recognition. There have also been moves in recent times to analyze information such as people's movements ("pedestrian flow") or position information from mobile phones, and to use this for security or to improve services. If Japan as a nation can clarify its policies on privacy and information use, it will make it easier for us to develop the technologies for this use.

Mimura: Hitachi sees adaptability, readiness, and harmony as being the three key concepts needed for social infrastructure security. Adaptability means the idea of implementing security measures at all layers within a system, from the individual components up to the middleware that ties them together and the applications that run on this middleware. Meanwhile, because there is still a risk of these being compromised due to infection by a virus, the concept of readiness means being able to respond promptly to any situation. Likewise, harmony means taking steps to share information obtained about viruses or other vulnerabilities as quickly as possible with the rest of the community, including the Information-technology Promotion Agency, Japan (IPA) and the Japan Computer Emergency Response Team (JPCERT). While this already happens, I believe we should go even further and establish mechanisms for more pooling and sharing of the information needed to improve security right across society, not just for IT systems and physical security, but also for the control systems that underpin social infrastructure. I see these key concepts as also being important for security in other areas.

Arai: Hitachi supplies total security solutions based on technologies that support security in a wide range of fields, from IT and control systems to physical security. Drawing on our discussion today, I hope we can contribute to enhancing the safety and security of society. Thank you for your time today.