MITSUBISHI ELECTRIC CORPORATION
PUBLIC RELATIONS DIVISION
7-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo, 100-8310 Japan

FOR IMMEDIATE RELEASE | **No. 3106**

Customer Inquiries

Information Technology R&D Center
Mitsubishi Electric Corporation
www.MitsubishiElectric.com/ssl/contact/company/rd/form.html
www.MitsubishiElectric.com/company/rd/

Media Inquiries

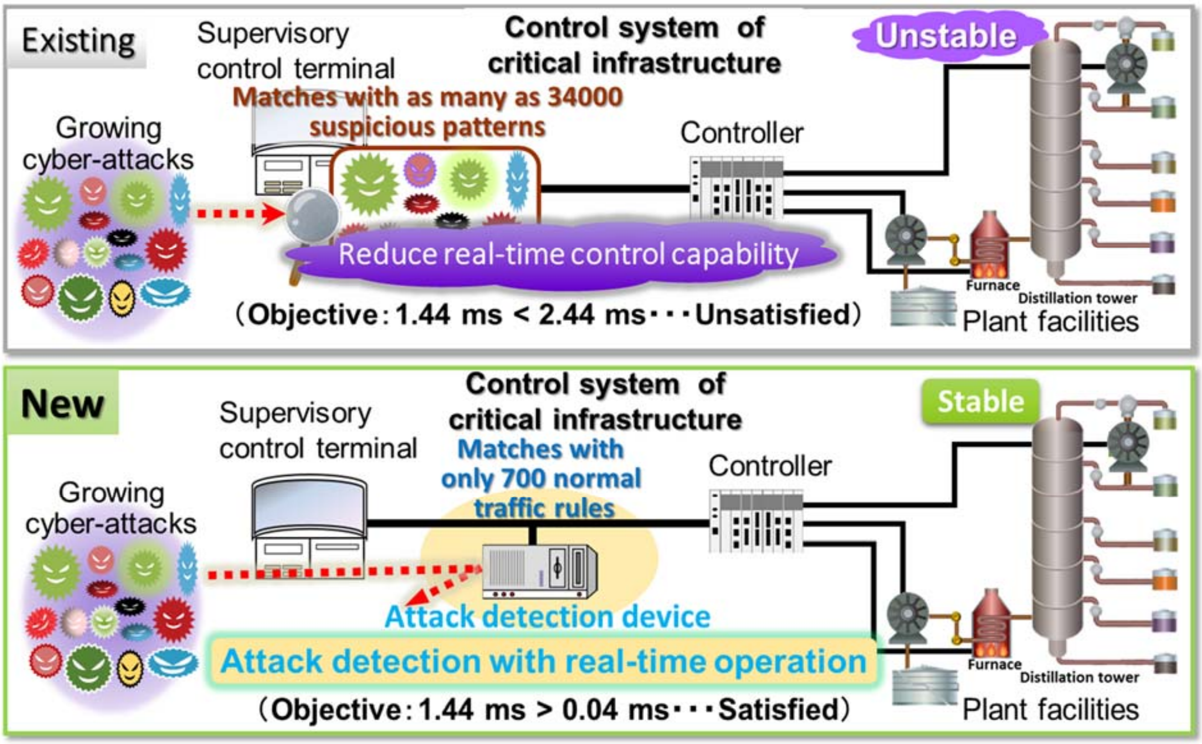
Public Relations Division
Mitsubishi Electric Corporation
prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

Mitsubishi Electric Develops Cyber-attack Detection Technology for Critical Infrastructure Systems

Real-time detection of cyber-attacks on control systems will contribute to infrastructure stability

TOKYO, May 17, 2017 – Mitsubishi Electric Corporation (TOKYO: 6503) announced today that it has developed a cyber-attack detection technology that quickly identifies network traffic that deviates from predefined normal commands in the control systems of critical infrastructure. The technology detects ingenious cyber attacks disguised as normal commands targeted on critical infrastructure for electric power, natural gas, water, chemicals and petroleum without reducing the real-time control capability, which is expected to help ensure infrastructure stability.

Commercialization for electric power infrastructure is planned from around fiscal 2018. Other applications will be developed in collaboration with the Strategic Innovation Promotion Program (SIP) challenge for the cyber security of critical infrastructure.


Existing
Supervisory control terminal
Control system of critical infrastructure
Unstable
Matches with as many as 34000 suspicious patterns
Growing cyber-attacks
Controller
Reduce real-time control capability
(Objective：1.44 ms < 2.44 ms・・・Unsatisfied)
Furnace
Distillation tower
Plant facilities
New
Supervisory control terminal
Control system of critical infrastructure
Stable
Matches with only 700 normal traffic rules
Controller
Growing cyber-attacks
Attack detection device
Attack detection with real-time operation
(Objective：1.44 ms > 0.04 ms・・・Satisfied)
Furnace
Distillation tower
Plant facilities

Realization of the new technology was partially supported by the results of "Cyber-Security for Critical Infrastructure" undertaken by the Control System Security Center (CSSC). "Cyber-Security for Critical Infrastructure" is part of the Cross-ministerial Strategic Innovation Promotion Program (SIP) promoted by the Council for Science, Technology and Innovation and has been commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

Key features

- The technology is the first in the world, as of May 17, 2017, to define the detection rules based on the normal commands for each operational state of the control system and to interpret deviations from the normal commands as attack.
- Real-time operation is ensured for the control system under our consideration when attack detection is in use because the technology does not involve a time-consuming matching process for suspicious patterns.
- The technology contributes to infrastructure stability by reducing the detection time and ensuring minimal influence on control-system processes that must finish within certain time limits.

Comparison with Existing Technologies

	Method	Real-time operation of control systems	Feasibility
New	Detects deviation from normal command rules determined by operational status	Low impact due to concise rules for normal commands	Proven effective in plant system simulations
Existing	Matches suspicious patterns with massive sets of rules	Risk of high impact due to increasing cyber attacks	Currently used in enterprise systems

Cases have occurred in which advanced cyber-attacks have penetrated control systems to issue commands that pretend to be normal and are highly indistinguishable from real commands. Existing detection methods that compare incoming traffic with known suspicious patterns can fail to detect such attacks. Comparison with the enormous volume of known suspicious patterns can take time and cause control system operations to fail.

Mitsubishi Electric observed that normal control-system traffic in critical infrastructure differs if the system is operating, not operating or under maintenance, so the new technology uses different detection rules for each operational state. With cyber-attacks continuing to increase, it takes an enormous amount of time to generate suspicious patterns and search for matches. But normal commands in control systems are limited, so the rules can be limited, which enables Mitsubishi Electric's new technology to search for matches quickly and detect attacks while preserving the real-time operation of control systems. The company evaluated the processing time of attack detection for the control system under our consideration. The evaluation revealed that the new technology only takes 0.04 ms, compared to 2.44 ms for an existing technology, while the real-time requirement is 1.44 ms.

Background

As IoT pervades the field of infrastructures, cyber security is becoming increasingly important for critical infrastructure that underpins society. Until now, the safety of infrastructure for electric power, natural gas, water, chemicals and petroleum has been ensured through physical isolation, firewalls for traffic control and stringent operational management. In recent years, however, there has been a rise, especially overseas, in advanced cyber-attacks that penetrate infrastructure control systems to send malicious commands disguised as normal for the purpose of inflicting damage, such as power blackouts and equipment destruction.

Patents

Pending patents for the technology announced in this news release number seven in Japan and seven abroad.

###

About Mitsubishi Electric Corporation

With over 90 years of experience in providing reliable, high-quality products, Mitsubishi Electric Corporation (TOKYO: 6503) is a recognized world leader in the manufacture, marketing and sales of electrical and electronic equipment used in information processing and communications, space development and satellite communications, consumer electronics, industrial technology, energy, transportation and building equipment. Embracing the spirit of its corporate statement, Changes for the Better, and its environmental statement, Eco Changes, Mitsubishi Electric endeavors to be a global, leading green company, enriching society with technology. The company recorded consolidated group sales of 4,238.6 billion yen (US$ 37.8 billion*) in the fiscal year ended March 31, 2017. For more information visit:
www.MitsubishiElectric.com

*At an exchange rate of 112 yen to the US dollar, the rate given by the Tokyo Foreign Exchange Market on March 31, 2017