3-1 R&D on How to Check the Conformance for Promoting Social Implementation of R&D Technologies

Social implementation technologies

Consideration of the framework for conformance checking with which social implementation can be achieved more effectively and rapidly than ever before

Features

I. Comparison of multiple security regulations is made possible using natural language processing technologies to streamline and quantify the conformance checking.

II. The conformance checking is securely achieved through the development of *security by design* and the use of templates for goal-oriented analysis.

Related technology fields: requirement analysis, security and safety analysis
Linked industry type: critical infrastructure related companies

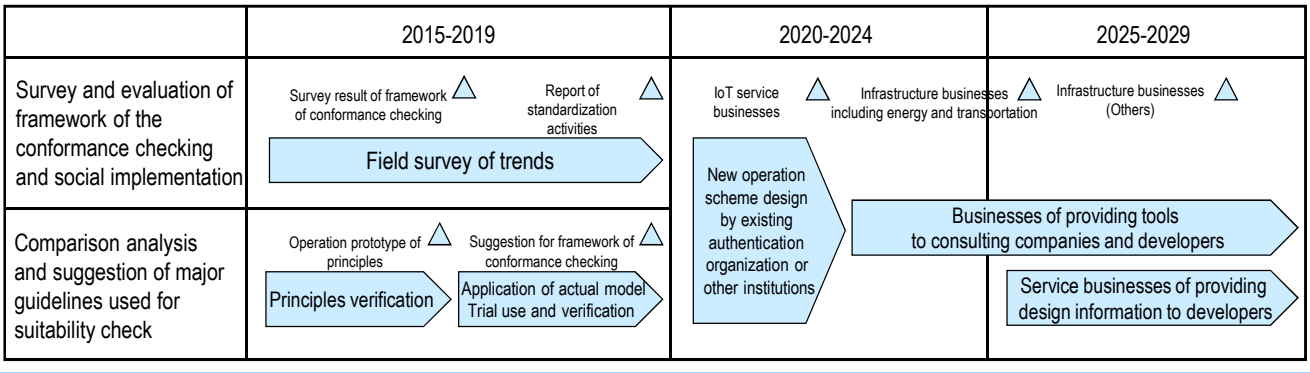
Aim of Research

Based on basic data obtained through surveys on the introduction of energy infrastructures of smart grid systems or other mission-critical systems of countries that are ahead of the other countries, we have promoted the implementation of a security evaluation system while considering the environment and risks concerning critical infrastructure companies and systems in Japan. Through these research studies, with regard to the achievement of cybersecurity in critical infrastructure and other high-risk environments, we investigate and evaluate the framework whose social implementation is feasible more effectively and rapidly than ever before.

Research Details

1. We have surveyed the trends and actual situation in Europe and the U.S. concerning the technologies for achieving cybersecurity in critical infrastructure and other high-risk environments, and analyzed the corresponding relationship between the authenticity determination technology (a1) and SP800-53 and provided the analysis result.
2. Comparison and analysis of the major guidelines used for the conformance checking has been greatly streamlined and quantified by using natural language processing technologies. This method is available when a product that is already conformed to a certain regulation needs to be conformed to another regulation. Comparison of the regulations of Europe and the U.S. with those of Japan has led to item 3 below.
3. Based on the results of 1 and 2, a case study has been conducted taking the operation monitoring/analysis technology (a2) as the topic. This study has concluded that recovery actions should be required to monitor products/services, and such requirements should be included in the uniform government standards.
4. We have considered international standardization activities for establishing requirements for recovery actions for the monitoring products/services mentioned in 3. We have concluded that while making requirements specific to infrastructures to be standardized in the standardization committee of applicable critical infrastructure sectors, technologies common to critical infrastructures should be standardized by a committee for security.
5. For secure conformance, we have built and verified basic principles of the requirements analysis process support tool in accordance with the development method of *security by design* and the goal-oriented analysis method.
6. For conformance checking, we have established basic principles for analyzing mutual influences between the security and safety functions and then produced and evaluated a prototype.

Schedule



(1) Method of Analyzing Multiple Security Regulations Using Natural Language Processing Technologies

With the use of IT, analysis has been greatly streamlined and quantified, which was manually performed before. This method is available when a product that already conforms to a certain regulation needs to conform to another regulation. In addition, the results of comparison and analysis of regulations can also be referenced by not only developers of critical infrastructure but by those who formulate regulations as well.

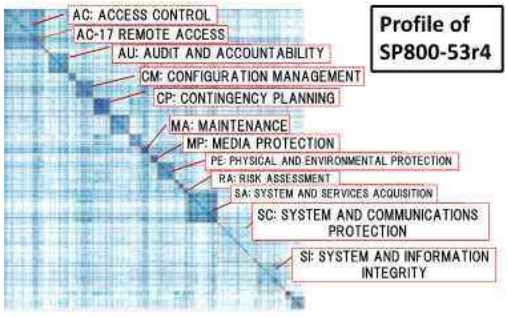


Figure Autocorrelation analysis of P800-53

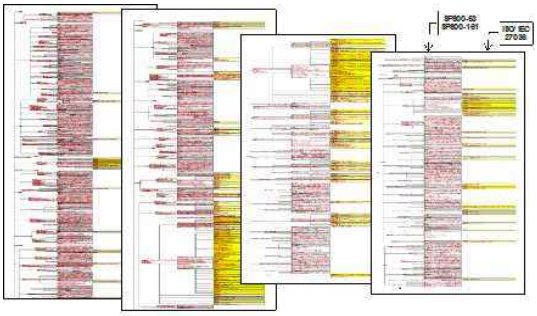
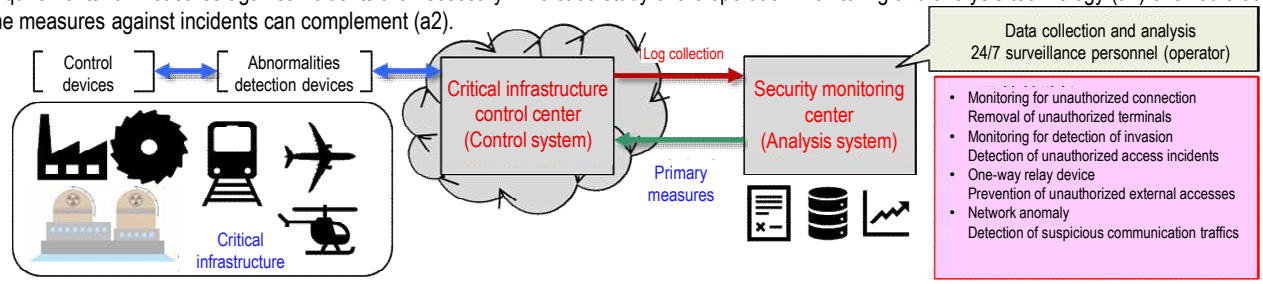


Figure Cross-check analysis between SP800-161 and SIO/IEC27046

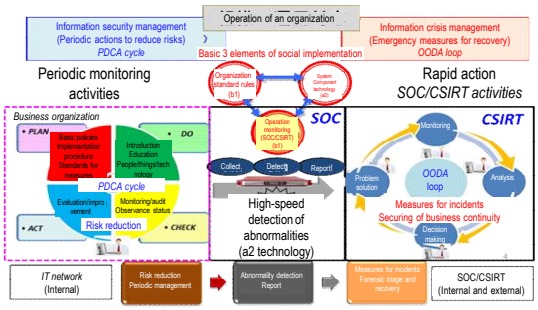
(2) Use of (1) and Case Study

As a result of analysis of the uniform government standards and SP 800-53 using (1), we found that for uniform government standards, requirements for measures against incidents are necessary. The case study of the operation monitoring and analysis technology (a2) showed that the measures against incidents can complement (a2).



Basis functions of A2 technology
NIST SP800-53 management measures
(i) IR-5: Incident monitoring and automatic data collection/analysis/…
(ii) IR-6: Incident report and automatic report/…

Features and innovativeness of A2 technology
・Self-learning of abnormal system statuses
・Automatic detection of abnormal statuses without prior registration
・Use of defense-in-depth detection algorithm
(reconnaissance, malware spread, IT/OT attacks)
・While the detection response is slow with the conventional detection by the total of risk scores,
Detection response is fast with the method the a2 type, which detects individual fine change.



(3) How to Check Conformance to Regulations Concerning Security

We developed a method that can determine whether products or others conform to the regulations or others by developing products with using the development method of *security by design* according to the regulations or others, generating evidence that the development processes conform, and comparing the evidence against a template representing the structure of requirements based on the goal-oriented analysis. This method can be used for any specific product within a company to check if the product conforms to the regulations or others.