The 3rd STAMP Workshop in Japan

Title

An Application of STAMP to Safety and Cyber Security for ICS

Speaker, Authors

Nagoya Institute of Technology   Shun KONDO, Souta SATO, Takashi HAMAGUCHI, Yoshihiro HASHIMOTO

Abstract

In recent years, cyber-attacks against industrial control systems (ICS) have become a real possibility, and the damage caused by cyber-attacks has become serious. Unlike cyber-attacks against information system, cyber-attacks against ICS can directly influence the physical space, and there is a risk of accidents and disasters affecting human life. There is an incredible amount of ways for cyber-attacks and it is impossible to assume every detail situations. Therefore, it is necessary to strength countermeasures from the viewpoint of the occurrence of cyber incidents so that abnormality does not lead to accidents, and to strengthen resilience so as to promptly recover and secure business and manufacturing continuity.

Safety design based on the Independent Protection Layer (IPL) is being promoted for important ICS from the viewpoint of preventing abnormalities and accidents beforehand or suppressing equipment damage and loss of human life. However, cyber-attacks can occur simultaneously. Even if the safety instrumentation system (SIS) installed independently of the basic process control system for safety countermeasure, the cyber-attacker may change the program of SIS and it may not work at the time of occurrence of an abnormality. In addition, if the information on monitoring console such as process variables is tampered and manipulated, the operator may not be able to take appropriate incident response. That is, since the multiplicity of the IPL is in danger of being invalidated under the cyber-attacks, in addition to the conventional viewpoint, it became necessary to design countermeasures from the viewpoint that "safety measures against cyber-attacks can maintain multiplicity."

To consider and evaluate both safety and cyber security for ICS, we propose a method by combining a diagram expressing function-linked structure in multiple countermeasures installed by STAMP model and network configuration information of ICS. The proposed design method can be the first step to discuss "design of safety countermeasures that can maintain multiplicity against cyber-attacks" and "selection of effective countermeasures at cyber incident."

Keywords

(1)   Safety

(2)   Cyber Security

(3)   Incident Response

(4)   Design of Multiple Protection