

The 3rd STAMP Workshop in Japan

Title

Cybersecurity Assessment with STAMP/STPA

Speaker, Authors

Tokyo Denki Univ. Cyber security Lab Takahashi, Yuji / Hayashi, Hiroshi

Abstract

Risk communication is one of the most important portion for cybersecurity process.

Both of the Cybersecurity and the Safety are usually discussed at once for cybersecurity measurement of IoT devices which are rapidly drawing recently, and the importance of Risk Communication is increasing and going more difficult.

We identified that the STAMP/STPA is one of the most effective tool to assess the IoT devices with both of cybersecurity and safety and developed “MRC-IoT”, the Risk communication tool using STAMP/STPA. The output from IPA STAMP/STPA Workbench will be utilized for semi-quantitative assessment.

With this tool, we can utilize the result of STAMP/STPA includes huge amount of items of Cyber risk scenarios and Hazards to make common understanding and decision among stakeholders.

Risk Communication is one of the most important process to make decision and execute cybersecurity preparation and countermeasures.

Recently the importance and assessments of both of cybersecurity and safety is discussed at once and mixed.

We are thinking that the importance of STAMP/STPA with which we can consider safety and security at one is very effective method to discuss IOT devices and developed MRC-IOT. IPA STAP/STPA Workbench is used for the pre-process of MRC-IOT.

On this workshop we would like to report our new method and example analysis using MRC-IOT with IPA STAMP/STPA workbench.

Keywords

- (1) Risk Communication
- (2) IoT
- (3) MRC-IoT
- (4) Cyber Security
- (5) IPA STAMP/STPA Workbench