The 3rd STAMP Workshop in Japan

Title

Proposal and application of risk analysis / countermeasure selection method using STPA

Speaker, Authors

Tokyo Denki University　Takuo Hayakawa

Abstract

The number of IoT (Internet of Things) devices is increasing. IoT devices are used in everything from appliances to medical devices. These devices were originally assumed to operate in a standalone environment. Therefore there are problems with connection to the Internet in that devices are exposed to unexpected security threats, such as cyber-attacks and malware. There is also a possibility that safety threats, such as malfunctions and stoppages, may occur due to security threats. Therefore, manufacturers must apply Secure by Design practices, which take functional safety into account from the design stage.

Risk communication is indispensable for achieving Secure by Design devices. By establishing a consensus among stakeholders on the risk to the system beforehand at the design stage, countermeasures against risk can be selected. Normally, risk communication includes risk analysis procedures such as tree analysis. Conventionally, fault tree analysis and attack tree analysis have been used for risk analysis. As a result, consensus formation based on the value of risk and the selection of measures can be selected. On the other hand, at present, there are divergences between the fields of safety and security, which are discussed as separate areas. Such a situation can be said to be inappropriate for the IoT because functional safety and Secure by Design interactions cannot be taken into account without integrating security and safety. In addition, the IoT is an unfamiliar system that includes many components and controls. Therefore, it is desirable to analyze not only the conven-tional tree structure but also the system model.

In this research, we propose a new risk analysis / countermeasure selection method to realize integrated risk communication of IoT safety and security. This method includes a safety analysis method STPA and a risk analysis procedure by EFT (Extended Fault Tree) which is one of tree analysis methods, and a selection procedure by a defense tree. The overall of the proposed method is shown in Figure 1 below and the procedure of proposed method is shown in Table 1 below. In addition, we show an example in which the proposed method is actually applied to an insulin pump, which is an IoT device for diabetic patients.

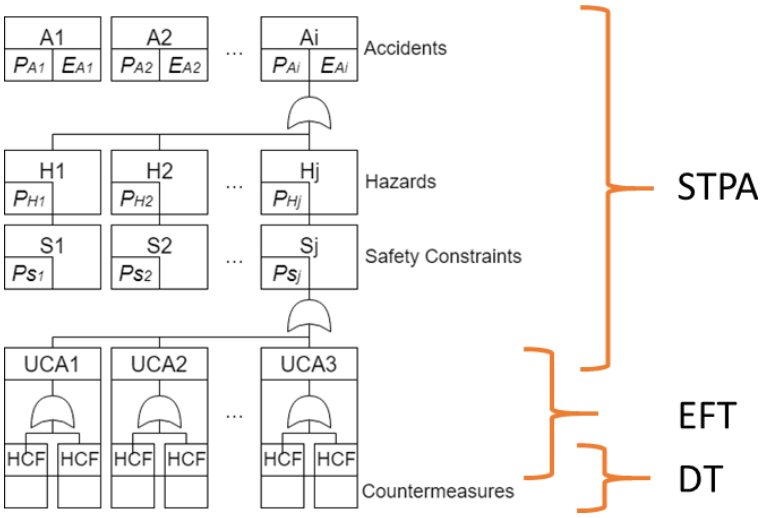

Figure 1. Overall of the proposed method

Step	Explains
1	Identify accidents, hazards, and safety constraints
2	Construct a Control Structure
3	Identify UCAs
4	Identify hazard causal factors
5	Probability analysis of accidents
6	Selection of countermeasure

Table 1. Procedure of proposed method

Keywords

(1) Risk analysis

(2) Countermeasure selection

(3) Tree analysis

(4) Security by Design