

## **(22)Title**

Verification of Cyber-Physical Systems Using STAMP / STPA

## **Speaker, Authors**

Nihon Unisys, Ltd. Yoshitaka Aoki, Shinshu University. Shinpei Ogata, Osaka University. Hiroyuki Nakagawa

## **Abstract**

CPS (Cyber Physical System) is used in various fields. Many systems will include CPS in the future. CPS connects cyber world and physical world. Therefore, it is influenced by the fluctuation of the external environment. Thus, CPS has uncertainty in the behavior of system and it is difficult to verify the safety.

STAMP / STPA is a method of safety analysis of complex systems. STAMP/STPA is based on Systems-Theoretic Accident model. Hazard analysis is performed by finding unsafe interactions among components. STAMP / STPA can also include a dynamic external environment in the accident model. Therefore, it is suitable for analysis of CPS system which is greatly affected by external environment. However, since CPS operates competingly for multiple devices, it is assumed that the control structure becomes complicated and analysis becomes difficult.

In this presentation, we propose a method of arranging complicated control structures and a method of verifying the stable state of the control loop using model checking. In this paper, we analyze the safety of traffic control system using Vehicle-to-Device (V2D) system as case study. The combination of STAMP / STPA and this proposal is useful for verifying the safety of a CPS system which is difficult to predict behavior.

## **Keywords**

- (1) STAMP/STPA
- (2) Cyber-Physical Systems
- (3) Model Checking