## (18)Title

The STAMP/STPA method of intentions and requirements description level

## Speaker, Authors

JFP, Inc. Hiroshi Nakamura

## Abstract

The working group for specifying safety in Japan Embedded Systems Technology Association is studying "Safety-guided design" as a process model of specifying safety-related requirements. The safety-guided design features to describe development intentions and system specifications, analyze those descriptions and repeat those describing according to the safety analysis, and aims at "If write intentions, safety increases". Virtual electric assist bicycle development was chosen as a trial case, and safety analysis was put into effect using the STAMP/STPA method.

When the STPA method was applied to safety analysis, a control structure was drawn as follows based on the requirements which reflect intentions about product development:

- 1) components are picked out from a System Context diagram
- 2) human-machine interactions are identified from a Use Case diagram
- 3) interactions inside the machine are identified from the intentions and requirements descriptions

I thought unsafe control actions depend on operation conditions of a bicycle, picked context variables as follows and tried to identify unsafe control actions every context :

- 1) feedback data
- 2) the data which shows outcomes of control actions

As a result, it was possible to identify several hazard scenarios, and it was possible to derive a recommendation measure which suits realization of the intentions from the identified measures. I think the STPA method is suitable for the safety-guided design and so I'd like to analyze development intentions by STPA, and to enhance safety and soundness of products.

## **Keywords**

- (1) development intention
- (2) safety analysis
- (3) electric assist bicycle
- (4) context variable