The 3rd STAMP Workshop in Japan

Title

Practice of process model deriving method based on Extending STPA

Speaker, Authors

Nihon Unisys Ltd.　Yuko Fukushima

Abstract

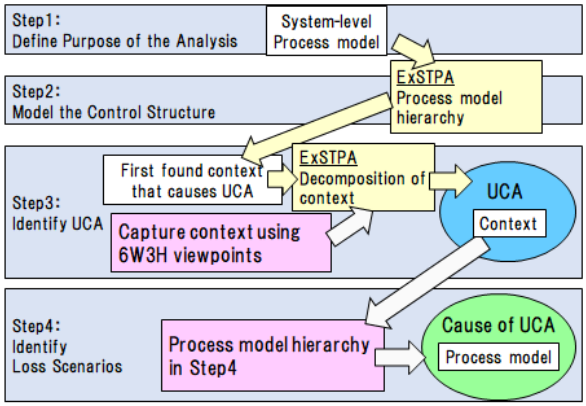
In STAMP / STPA, one of the common causes of accidents is that the "unsafe control action" (UCA) is executed when the process model does not match the system. While the process model is important, the method by which to derive the process model is not presented. Therefore, analysts should derive it ad hoc.

To solve this issue, Dr. Thomas of MIT introduced a technique called Extending STPA. In this method, analysts can take high-level context from a hazard and understand the refined process models. Then, identify the UCA by combining the process models.

Although Extending STPA is an effective method, the process models may be overlooked while refining the hazard context in process model hierarchy. Therefore, we can apply the viewpoints of 6W3H while UCA identification broadly captures the context.

We applied the viewpoints while applying STAMP/STPA and Extending STPA to the real system and confirmed the effect.

The presentation will explain the issue of STAMP/STPA, outline Extending STPA and its issue, and explore the results of applying 6W3H to identify the context.



Keywords

(1) STAMP/STPA
(2) Extending STPA
(3) Context
(4) Process Model
(5) 6W3H