(16)Title

Safety requirement analysis of level crossing control system using STAMP/STPA method

Speaker, Authors

East Japan Railway Company . Takashi KUNIFUJI

Abstract

In recent years, with the development of the information communication technology on which the railway signalling system is based, advancement and complication of both hardware and software are progressing. Coupled with its expertise in the railway signalling system, there are special circumstances such as high safety requirements, large order-made elements, ambiguous responsibility boundaries between operators and suppliers, and these exist in railway signalling systems making it even more complicated. Under such circumstances, as one of the technological development leading to the reduction of the development cost of the railway signalling system and the improvement of the safety, we are working on verifying validity through the safety analysis of software and control logic itself.

In this research, we tried to apply the STAMP / STPA method to the risk analysis carried out in the upstream process of development, with the theme of the level crossing control system in the station yard made in the past. In this trial, it was possible to efficiently extract general safety requirements for level crossing control, and confirmed that the STAMP / STPA method is effective for a railway signalling system which is one of event driven system. On the other hand, it was also found that there is still a problem that securing comprehensiveness of risk analysis has a large dependence on experiences of the target system owned by the analyst. Based on these, we also present future prospects for more effective use of the STAMP method.

Keywords

(3) Level crossing
(4) Railway signalling system
(5) Safety
(6) STAMP/STPA
(7) STAMP/CAST