Model Checking for Automatic Verification of Safety Instrumented System in Chemical Process Industry

김진경, 이영희, 권혁면[1], 문 일*
연세대학교; [1]산업안전관리공단
(ilmoon@yonsei.ac.kr*)

An automatic technique is proposed to verify control logics of safety instrumented system (SIS) and to validate the correctness and completeness of fault tree (FT) for safety integrity level (SIL). Model checking method is applied to find the logical errors of SIS automatically which is difficult to find manually, and to verify them. It is also useful when analyzing FT of SIS. It attempts to validate the correctness and completeness of FT for the SIS. The idea of the verification of FT is to systematically specify the system model and to prove the correctness and completeness of FT. The strength of this method is to synthesize a feasible sequence through a counter-example and to verify its correctness using computation tree logic (CTL) simultaneously. The counter-example consists of a scenario in which the model behaves in an undesired way. Thus the counter-example provides evidence that the model is faulty and needs to be revised. This paper addresses an automatic technique to provide and to modify the P&ID design and the FT of the SIS control logics in the chemical process industry, and presents how model checking approach can be used efficiently in the verification of SIS.