안전- 필수 소프트웨어에 관한 안전성분석 체계구성에 대한 연구

A Study of Software Safety Analysis System for Safety-Critical Software

장훈선, 신현국, 장영우, 정재천, 김재학, 한희환
한국전력기술주식회사

손한성
한국원자력연구소

요약

소프트웨어 수명주기에 걸쳐 안전성 분석이 수행되는 안전-필수 소프트웨어에 대하여 안전성 관련 중요 인자 및 요건을 추적하고, 단계별로 안전성 분석을 수행하는 절차 방법론에 대해 기술하였다. 개념단계에서는 안전성분석 체계를 구축하기 위한 계획, 조직 등의 점검사항 및 시스템 관련 고장모드 및 영향분석(Failure Modes and Effects Analysis)을 수행하였다. 요건단계에서는 HAZOP(Hazard and Operability) 기법을 이용하여 안전성에 관련한 파라미터 및 구현하여야 할 소프트웨어 항목 도출 및 체크리스트 작성에 의한 워크스루(Walk-Through)를 통하여 타당성 평가 및 수행여부를 점검하였다. 설계단계에서는 시스템을 안전하게 구동하도록 설계된 소프트웨어 모듈의 알고리즘을 안전성 측면에서 고장수목(FTA: Fault Tree Analysis) 기법을 이용하여 위험요소 등을 분석하였다. 적용 사례연구는 원자력발전소 계측제어 소프트웨어 중 원자로보호계통의 가압기 저압력 트립 알고리즘을 대상으로 실시하였다. 시험단계에서는 개념단계의 고장모드 및 영향분석(FMEA)을 기반으로 제공된 시험항목에 대한 시험 수행여부를 점검하였다. 소프트웨어 수명주기 동안에 수행되는 안전성 관련 업무에 대하여 체계적인 표준을 작성하여 업무를 수행함으로써 중요 안전요인을 집중적으로 확인할 수 있었으며, 아울러 요건추적 기반의 CASE 도구를 사용하여 개념단계부터 시험단계까지의 안전성 관련 중요 항목들을 추적함으로써 효율성을 높일 수 있었다.