

안전필수 소프트웨어의 확인 및 검증 Safety Critical Software Verification and Validation

김희철, 백영우, 윤청
충남대학교
김복렬
한국원자력안전기술원

요약

원자력 산업계에서 컴퓨터 기술의 적용은 다른 응용 분야와 마찬가지로 요구되는 시대적 변화라 할 수 있다. 그러나 현재까지 원자력 분야에 컴퓨터 적용이 용이하지 않았던 주된 요인은 시스템 제어가 소프트웨어로 이루어지는 경우 하드웨어를 사용하는 것보다 오류를 발견하기 어려워 안전 필수 시스템의 경우 소프트웨어를 사용하는 것에 많은 저항이 있어 왔다. 이러한 안전성 및 신뢰성을 확보하는 문제가 디지털 계측제어 시스템의 경우 중요한 쟁점으로 떠오르고 있다. 이러한 문제를 해결하기 위해 원자력 발전소 계측제어 소프트웨어에 요구되는 품질보증 활동에 대한 연구가 수행되어 왔다. 소프트웨어의 품질을 보증하는 중요한 수단으로서 확인 및 검증은 소프트웨어 시스템 개발 과정 중 모델링과 분석결과에 대하여 잠재적인 위험이 발생될 확률과 심각성을 판단할 수 있으며, 오류를 제거하고 위험을 제거할 수 있다. 본 연구는 안전필수 소프트웨어의 생명주기 전반에 걸쳐 이루어지는 확인 및 검증의 계획 및 절차에 대하여 설명하고자 한다.

원전 소프트웨어 개발의 소프트웨어 공학 기법 적용 Appliance of Software Engineering in Development of Nuclear Power Plant

백영우, 김희철, 윤 청
충남대학교
김복렬
한국원자력안전기술원

요약

원자력 산업계에서 컴퓨터 기술의 적용은 다른 응용 분야와 마찬가지로 요구되는 시대적 변화라 할 수 있다. 그러나 현재까지 원자력 분야에 컴퓨터 적용이 용이하지 않았던 주된 요인은 이러한 기술의 적용이 원자력 분야의 안전성에 미치는 잠재적인 영향 때문이라고 해도 과언이 아니다. 그리고 가동중인 원자력 발전소의 노후화된 계측제어 설비를 교체하는 디지털 개선사업과 차세대 원자력 발전의 디지털 계측제어 시스템에 대한 안전성, 신뢰성을 얻고 품질보증을 평가할 수 있는 지침의 설정 및 규제 기술을 개발하는 것이 시급한 과제가 되고 있다. 따라서 소프트웨어 개발과 운영에 있어 기술적인 한계를 극복하고 품질을 보증할 수 있는 방안들이 마련되어 일관된 틀과 방향이 제시되어야 한다. 본 논문에서는 기존의 폭포수 모델과 원전 소프트웨어 개발에 필요한 소프트웨어 생명주기의 차이점을 살펴보고 원자력발전소의 계측제어 시스템 개발에 필요한 일관된 틀을 제시하고자 한다.