# 교훈: 목표지향 제어봉제어계통 독립 소프트웨어 확인 및 검증

이자영**, 손광영**, 이상석**, 이준구*, 박근옥*
*한국원자력연구원 MMIS
**㈜한국신뢰성기술 원자력엔지니어링
e-mail : kysohn@korts.co.kr

# Lesson learned: Target-based independent S/W verification and validation for CEDMCS

jayoung Lee**, kwangyoung Sohn**, sangseok Lee**, junku Lee*, geunok Park*
*MMIS, Korea Atomic Energy Research Institute (KAERI)
**Nuclear Engineering, Korea Reliability Technology and System (KoRTS)

**요 약**

단순 부품부터 계통까지 기존의 아날로그 제품들이 최근 들어 펌 웨어(Firmware)와 고수준의 컴퓨터 언어로 구현된 응용 소프트웨어를 포함하는 디지털 설비로 바뀌고 있다. 따라서 어느 때 보다 소프트웨어의 확인 및 검증의 중요성이 대두되고 있으며, 이를 위해 학계뿐만 아니라 국제표준 기관에서 확인 및 검증을 위한 지침을 제시하고 있는 실정이다. 본 논문은 원자력발전소 출력을 제어하는 제어봉제어계통의 업그레이드와 관련하여 IEEE 1012 에 따라 수행된 독립 확인 및 검증 업무를 요약하고, 이를 통해 얻은 교훈을 기술한다.

## 1. 서론

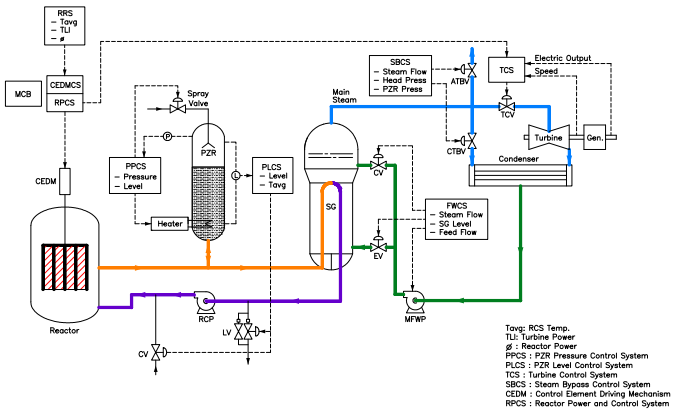
최근 영광 3,4 호기 원자력발전소의 제어봉제어계통이 기기단종 및 노후화로 인하여 업그레이드되었다. 과제 계획단계에서 제시된 IEEE 1012 를 기준으로 관련 소프트웨어의 확인 및 검증이 이루어 졌다. 다음은 소프트웨어 확인 및 검증을 위한 전략, 발행된 불일치 보고서의 처리 메커니즘을 기술하고, 최종적으로 본 업무를 통해 얻어진 교훈과 쟁점들을 기술한다.

## 2. 영광 3,4 제어봉제어계통

영광 3,4 호기 발전소는 한국형표준원전으로 제어봉제어계통의 기기의 단종 및 노후화로 업그레이드를 실행하였다. 관련하여 상위 기술사양서에 준하는 소프트웨어의 확인 및 검증 활동을 수행하였다.

제어봉제어계통(그림 1 참조)은 원자력발전소의 출력을 제어하기 위해 제어봉(Control Rod)의 삽입과 인출을 통하여 출력을 제어하게 된다. 제어봉 제어를 위한 운전모드는 자동, 수동 및 기타 연동논리를 포함한다. 또한 운전과 관련되어 운전원과의 연계를 위하여 유지보수 및 시험 패널(Maintenance and Test Panel : MTP)이 제공된다.

제어봉 제어를 위하여 Waterfall Model 로 수행된 설계 Track 과 달리, 제어논리의 확인 및 검증은 IEEE 1012 에서 제공하는 SDLC (Software Development Life Cycle) 에 따른 V-shape 의 확인 및 검증 절차를 따라 수행되었다. 확인 및 검증 수행결과는 보고서, 요건추적 매트릭스 (Requirement Traceability Matrix : RTM), 불일치 보고서 (Anomaly Report : AR)를 그 결과물로 제공하였다.
또한 제공된 확인 및 검증 결과물은 AR 관리를 위하여 설계부서와의 검토회의를 통하여 타당성을 확인하고 설계반영여부를 결정하였다.




(그림 1) 제어봉제어계통 개요

## 3. 영광 3,4 제어봉제어계통 확인 및 검증

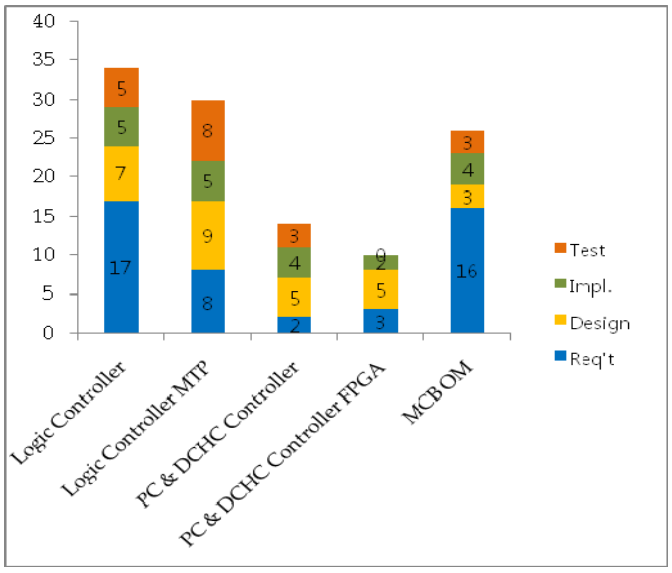
제어봉제어계통의 확인 및 검증 결과는 표 1 에 나타

나 있고 이를 도표화 한 다이어그램은 그림 2 에 도시되어 있다. 확인 및 검증의 결과 발생된 불일치보고서는 대부분 설계 초기단계인 요건단계(Requirement phase)에서 확인되었다.

(표 1) SDLC 별 불일치보고서 수량

| | Req't | Design | Impl. | Test |
|---|---|---|---|---|
| Logic Controller | 17 | 7 | 5 | 5 |
| Logic Controller MTP | 8 | 9 | 5 | 8 |
| PC and DCHC Controller | 2 | 5 | 4 | 3 |
| PC and DCHC Controller FPGA | 3 | 5 | 2 | 0 |
| MCB OM | 16 | 3 | 4 | 3 |
| Total | 46 | 29 | 20 | 19 |

확인 및 검증은 IEEE 1012 에서 이야기 하는 설계의 정확성(Correctness), 완전성(Completeness), 일관성(Consistency), 시험성 (Testability), 가독성 (Readability), 가용성 (Availability) 등의 대 분류를 목적으로 수행되었다. <표 1>에서 알 수 있듯이 제어봉제어계통을 구성하는 하부계통의 경우 SDLC 의 초기단계인 요건단계에서 많은 부분의 Design Inconsistency 가 발견되었다. 이는 계획, 개념단계에서의 상위설계, 사용자 요구사항 등이 기대했던 것 만큼 완벽하지 않았던 것으로 판단되고 있다. <그림 2>는 표 1 의 수량을 도표화 한 것이다.




(그림 2) 단계별 AR 수량 도표

## 4. 결론

IEEE 1012 에서 기술하는 지침을 기반으로 확인 및 검증을 수행한 결과, 지침이 제공하는 Criteria 를 이용하여 기술적인 Fault 를 발견하는데 한계가 있음을 확인하였다. 즉 지침자체가 SDLC 단계의 설계 행위들이 적절하게 수행되었는지 확인하는 단순 역무로 오해받을 수 있는 요지가 있었다. 따라서 SDLC 단계의 Monitoring 이 아닌 기술적인 오류의 발견을 위해서는 확인 및 검증 수행자가 설계 Track 의 자료를 바탕으로 다음과 같은 제어봉 제어계통 고유의 검토를 위한 요건들을 별도로 준비하는 것이 타당한 것으로 판단된다. 즉, Target 시스템의 특성에 종속적인 검토기준이 재 생성되어야 한다는 것이다.

1. 제어봉제어계통의 필수 기능특성의 파악
2. 통신 또는 통시주기와 같은 내외부 서브계통 간의 연계특성 확인
3. 제어봉제어계통의 필수 성능특성 확인
4. SDLC 전 주기 별 기능의 결합도 및 응집도에 대한 기준 및 확인
5. 기능 및 성능의 신뢰성 확인기준
6. 예외사항 및 초기조건(가정)에 대한 확인
7. Test coverage 에 대한 확인
8. 고유기능, 성능과 관련된 HMI 적합성 판단기준

물론 상기에 기술된 대 분류 기준보다 구체화하면 보다 많은 Target 시스템 종속적인 확인 및 검증 기준이 도출될 것이다. 단지 위와 같은 기준을 재 생성한 것은 SDLC 별로 개념적인, 반복적인 검토기준이 Target 계통의 기술적 오류를 발견하기 힘들며, SDLC 단계의 설계 Activity 를 감시하는 수준에 머무는 것을 방지하기 위한 것이었다.

Acknowledgements
이 논문은 2013 년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (SMART 안전성 향상을 위한 MMIS 연구. No. 2013024421)

## 참고문헌

[1] IEEE Std 1012™, "IEEE Standard for Software Verification and Validation", 2004
[2] Roger S. Pressman, Ph. D, ISBN 0073655783, "Software Engineering, A Practitioner's Approach", Fifth Edition, McGraw-Hill Higher Education.
[3] IEEE 829, "IEEE Standard for Software and System Test Documentation", 2008