

A practice of software Quality Assurance of the Computerized Procedure System - Engineering System using requirement traceability matrix

Dae-Seung Park, No-Kyu Seong, Yeonsub Jung

Instrumentation & Power Engineering Laboratory
Korea Hydro & Nuclear Power Company

ABSTRACT

Objective: The purpose of this study is to verify the safety and accuracy of the computerized procedure(CP) which is installed in the ShinKori Unit 3&4 that is the reference plant for APR1400. It is necessary to check the CP about how the CP is created because the safety and accuracy of the CP will guarantee the safety of the nuclear power plant. **Background:** Traditional nuclear power plants have used the paper based procedure to operate the nuclear power plant. Recently, digital MMIS(Man Machine Interface system) is applied in Nuclear Power Plants(NPPs). The beneficial of using the computerized procedure system(CPS) rather than the paper based procedure is that the computerized procedure is information resources for the operators. And it will give operators a safe and accurate environment to operate because the procedures will check operators' decision once again. The items must double checked for CP editing software are eliminate the possible problems in the CP, follow the right schema for the Procedure eXecution System(PXS), give the writers the right framework for what the procedure writer wants, and etc.. These items must be guaranteed because if the quality of the CP editing software is not assured then the installed CP will cause the problems. **Method:** The quality of the CP editing software which is called the Engineering System(ES) have to be verified that all the functions to work correctly and checked the design objectives identified in the design requirements so that the nuclear power plants safety are promised. In this study, we uses the vertical and horizontal requirement traceability matrix the followings: the design requirements(45 items), the system requirements(33 items), the technical design(22 items), implementation(4626 classes from source code), and test(29 items). **Conclusion:** We have identified and related the requirements to the design, to the source code, and to the test by using the vertical and horizontal requirement traceability matrix. For designing the software and system designs, using the vertical and horizontal requirement traceability matrix methods may apply to the fields which are concerned of safety and accuracy(ex: aviation field, traffic management, chemical plant industry, and etc.).

Keywords: Computerized Procedure System, CPS, Engineering System, ES, 전산화절차서설계지원시스템, 전산화절차서

1. Introduction

신고리 3,4호기의 주 제어실은 컴퓨터기반 절차서를 이용하는 전산화절차서 시스템(Computerized Procedure System)이 처음 적용되었다[1,2]. 추후 선형호기인 신고리 3,4호기를 기반으로 신울진 1,2 그리고 UAE에 컴퓨터기반의 주 제어실이 설치될 예정이다. 절차서수행시스템(Procedure

Execution System, PXS)은 주 제어실(Main Control Room)과 원격정지실(Remote Shutdown Room)에서 절차서를 수행하는 시스템으로 전산화절차서(Computerized Procedure, CP)가 PXS에 설치 및 실행된다. 전산화절차서 설계지원시스템(Engineering System : 이하 ES)은 PXS(Procedure Execution System) 상에서 실행되는 전산화절차서를 디자인하고 작성하기 위한 저작 도구이다.

컴퓨터기반의 주 제어실이 추후 계속적으로 설치되는 이

유는 전산화절차서가 인적 오류 예방 및 운전지원 기능을 제공하고 운전원들의 판단을 수월하게 하기 위해 그래프와 같은 미리 계산된 값을 제공하여 운전원의 직무부하를 저감시키기 때문이다[3].

본 논문에서는 ES의 지정된 기능들이 정확한 수행 하는가, 설계목적에 부합되도록 만들어지고 동작하는가를 검증 및 확인하여 전산화절차서(CP)를 활용하는 원자력 발전소의 정확성 및 안전성을 확고히 하는 데에 있다. 이를 정확히 확인하는 데에 소프트웨어 설계시 생성된 45개의 설계 요구사항과, 33개의 시스템요구사항, 22개의 설계사항, 그리고 4626개의 구현사항을 수직적 양방향 요구사항의 추적성이 보장됨을 확인하여 소프트웨어의 정확성 및 안전성을 확인하였다.

2. Software Verification and Validation Process

ES의 주요 기능은 현장(신고리 3,4호기) 운전원들이 원자력 발전소의 운전시 지침이 되는 “중이절차서”를 전산화하고 이를 관리하기 위한 시스템이다.

이와 같은 ES의 소프트웨어 구성특성을 신고리 3,4 및 신울진 1,2 SPM(Software Program Manual)과 IEEE 1012:2004를 참고하여 적절한 개발생명주기의 개발단계별 검증 및 확인방안을 수립하였다.

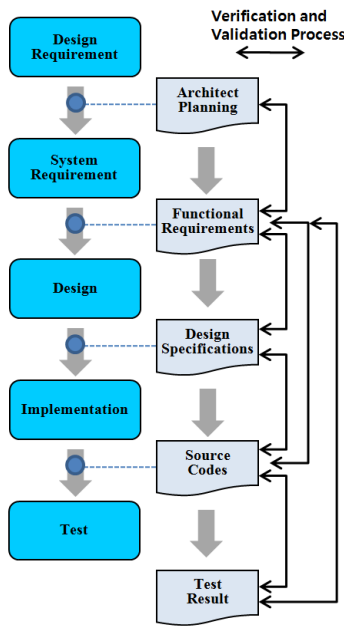


Figure 1. Verification and Validation Process

ES의 개발단계는 설계요구사항, 시스템요구사항, 설계단계, 구현단계, 시험단계로 구성되며 전체 개발의 각 단계별 산출되는 개발문서 간의 요구사항이 빠짐없이 모두 반영되었는가를 각 요구사항 및 개발사항의 식별자(ID)를 주어 이와 관련한 양방향 추적성 분석을 통해 검증 및 확인하였다.

3. Software Development Steps

2.1 설계요구사항

설계요구사항은 신고리 3&4 및 신울진 1&2의 전산화절차서시스템 설계이전과 이후에 나온 ES의 설계요구들을 종합하였다. 그 이유는 전산화절차서가 사용될 발전소의 공급자와 개발자가 다르므로써 생기는 차이, 버그 수정, 그리고 개선사항들을 모두 요건에 넣었기 때문이다.

식별된 설계요구사항을 개발 관점에서 기능적 요구사항을 도출하였으며 ES의 기능요구사항은 절차서 프로젝트관리, 절차서 개정이력 관리, 절차서 확인, 절차서 시험, PWG/PWT관리 그리고 기존 ES의 기능에 추가되는 기능으로 분류되어 기술되었다.

ID	상세내용	설계요건 확인사항
FR_01	신고리 3&4 전산화 절차서 시스템의 계통설계 개정 사항 반영	확인
FR_02	신울진 1&2 전산화 절차서 시스템의 계통설계 개정 사항 반영	확인
FR_03	신고리 3&4 사업진행에 따른 웨스팅하우스(WEC)의 기기설계사항 및 절차서 XML Schema를 반영	확인
FR_04	WEC의 전산화 절차서 시스템 개발환경인 QT4.6을 개발에 적용	확인
FR_05	WEC의 편집기와 연계개발을 위한 Plug-in 지원 라이브러리(ES_Plugin)를 개발에 적용	확인
FR_06	신울진 1,2에 전산화 절차서 편집기에 제공되는 두산중공업 개발 CPS와 연계 개발환경(미정)을 적용	확인
FR_07_01	로그인기능 - 응용프로그램 접근 제어를 위한 사용자 입력 및 Password 관리 기능	확인
FR_07_02	로그인기능 - 로그인 사용자별 권한설정 및 협업을 위한 기능	확인
FR_07_03	CPP Manager(Create CPP)- 화면에서 입력되는 PNS No, Project Name, Project ver 등이 WEC 절차서 생성에 필요한 부족 정보와 자동 입력 버그 수정	확인
FR_07_04	CPP Manager(Revise CPP)-절차서 로그인, 열기, 저장 등의 통제 관점에서 조회 개선	확인
FR_07_05	CPP Manager(Revise CPP)-기호에 대한 종이인쇄 및 Excel 저장 기능개선	확인
FR_07_06	CPP Manager(Show Reports)-Revise CPP 선택 시 Project Name이 정상적으로 표시 문제 개선	확인
FR_07_07	CPP Manager(Show Revision)-Revision History에 대한 종이 인쇄나 Excel 저장기능 추가	확인
FR_07_08	CPP Manager(Show Revision)-Change History에 대한 종이 인쇄나 Excel 저장기능 추가	확인
FR_07_09	CPP Manager(Trace Change)-Trace Change 결과 대한 종이인쇄나 Excel 저장기능 추가	확인
FR_07_10	CPP Manager(Edit ES Property)-ES Properties에 대한 추가 요구 사항을 반영하도록 개선(초기 PWG에 대한 직무 분석을 반영할지 여부 등)	확인
FR_07_11	CPP Manager(Edit ES Property)-Logic 관해서 현재는 NETEC PB 기준으로 사용자가 로직을 직접 입력하는 형태로 되어 있으나 WEC PB에서 작성한 로직을 테스트 및 설정 가능한 형태로 개선, picklist 등과 연계되어 변수 값에 대해서도 반영	확인
FR_07_12	Verification(Check Verification)-Verification에 따른 Comment추가 입력 기능 반영	확인
FR_07_13	Verification(Check Verification)-Comment추가에 따른 Report기능개선, Success, Fail, Not Tested 목록 갱신 이상 수정	확인

Figure 2. Design Requirements

2.2 시스템요구사항

시스템요구사항은 ES가 생성, 개정, 추적, 관리, 활용 등의 기능들의 조건들을 모아놓은 것으로 기존의 기능들과 추가되는 기능으로 구분된다. 시스템요구사항을 통해 불필요한 시스템 기능들을 구분하고 시스템요구사항을 정리하여 꼭 필요한 기능들만이 설계에 반영되도록 조건을 정리하였다.

2.3 설계

설계 단계에서는 모든 기능구현이 가능하도록 정의되어야 하고, 각 입력변수의 전체구간 중 각 클래스 단위의 동작들을 지정하여 클래스별 기능이 원활하게 수행되도록 설계한다. 이를 위해 기능 요구사항명세서에서 예상된 상황의 동작들을 지정하여 방정식, 알고리즘, 제어논리 등이 기술하였으며, 시스템의 구성 및 특성과 소프트웨어 구현을 위한 변수 및 흐름도를 소프트웨어 설계 명세서에 명시하였다.

2.4 구현

구현 단계에서는 설계단계에서 명시된 기능 요구사항명세서에서 예상된 상황에서의 동작들, 방정식, 알고리즘, 제어논리, 시스템의 구성 및 특성과 소프트웨어 구현을 위한 변수 및 흐름도 등을 바탕으로 소스코드를 작성한다. 설계사항을 바탕으로 구현단계에서는 4626개의 구현사항(코드파일)이 구축되었으며, 식별된 모든 설계사항에 대한 코딩이 완료됨이 확인되었다.

2.5 통합시험

ES의 시험은 수립된 시험절차에 따라 수행되었으며, 시험결과는 시험명(Test case ID 포함), 시험대상 기능요구사항, 시험절차, 시험담당자, 판정기준, 그리고 결과와 관련된 설계요구사항이 포함된 Test Report에 따라 문서화 하였다. ES 통합시험을 통해 설계사항을 만족하는지, ES 건전성이 상시 유지되는지를 확인하였다.

3. Verification and Validation Results

모든 45개 설계요구사항과 33개 시스템요구사항의 수직적 양방향 요구사항 추적성이 보장됨을 확인하였다. 고객 요구사항 중 FR_12는 기능적 구현을 위한 요구사항이 아닌

개발수행관리를 위해 정의된 비기능적 요구사항으로 시스템의 기능개발을 위한 설계, 구현, 시험항목에 직접적 관련이 없는 것으로 확인되었다. 33개 시스템요구사항과 22개 설계사항의 수직적 양방향 요구사항 추적성이 보장됨을 확인하였고 22개 설계사항과 4626개 구현사항의 수직적 양방향 요구사항 추적성이 보장됨을 확인하였다. 마지막으로 4626개 구현사항과 29개 시험사례 및 결과(Test case & Results)가 수직적 양방향 요구사항 추적성이 보장됨을 확인하였다.

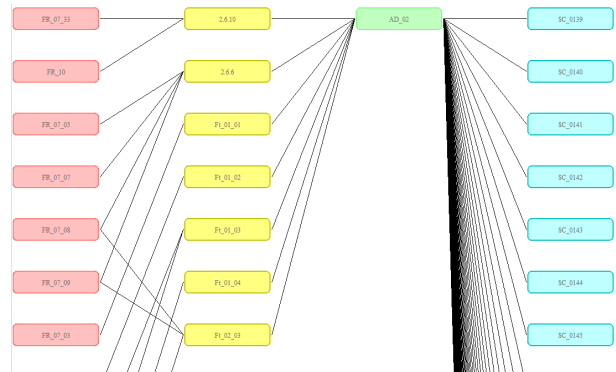


Figure 3. Traceability Diagram

4. Conclusion

본 논문에서는 신고리 3.4 원자력발전소에 최초 적용되는 전산화절차서 시스템의 작성기인 ES 안전성 및 정확성을 보증하기 위한 연구이다. 발전소의 안전을 보증하기 위해 전산화 절차서 시스템에 설치되는 전산화 절차서(Computerized Procedure)가 운영상의 문제가 생길 수 있는 부분을 미리 제거하고, 작성자가 원하는 방향으로 올바르게 작성되어 설치 이후에도 전산화 절차서 실행기(Procedure eXecution System)의 규칙에 맞게 작성된 절차서가 설치됨을 보증해야 하므로 전산화 절차서 편집기의 품질확보가 무엇보다 중요하다.

본 연구에서는 ES 소프트웨어 설계시 고려한 설계요구사항(45개), 시스템요구사항(33개), 그리고 설계사항(22개)와 개발시 고려한 구현사항(소스코드의 클래스 파일 4626개), 그리고 통합시험(29개)의 수직적 양방향 요구사항의 추적성을 확인하여 소프트웨어가 설계대로 잘 만들어졌음을 확인하였다.

이와 같은 소프트웨어 또는 시스템과 같은 설계를 올바른 방향으로 설계하는 방법을 제시하여 발전분야, 화학 플랜트 산업분야, 항공, 교통관계분야 등 안전성 및 효율성이 요구되는 대형의 산업분야에서도 적용될 수 있을 것이라 판단된다.

References

- [1] Sungjin Lee, Yungoo Kim, Hyunnam Kim, "Implementation of Concurrent State-based Procedure Execution Using the Hierarchical State Machine and the Active Object", Transactions of the Korean Nuclear Society Autumn Meeting Jeju, Korea, October 21-22, 2010
- [2] No Kyu Seong, Yun Goo Kim, Yeong Cheol Shin, "The design of engineering system for verification and validation of computerized procedure" proceedings of the Korea Intelligent Information System Society Spring Conference, 2011
- [3] Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance, NUREG/CR-6634.
- [4] No Kyu Seong, Yeong Cheol Shin, "The Application of Logic Based Computerized Evaluation in Determining Procedure Flow in APR1400 CPS", The Korean Society of Safety Autumn Meeting, 2012.

Author listings

Dae-Seung Park: thepark@khnp.co.kr

Highest degree: M.S, Information and Communication Technology Management, University of Science and Technology

Position title: Researcher, Central Research Institute, Korea Hydro and Nuclear Power Co.,(KHNP)

Areas of interest: Human Factors Engineering, MMI, Power System

No Kyu Seong : nkseong@khnp.co.kr

Highest degree: M.S., Department of Electrical, Electronic & Computer Engineering, Sung Kyun Kwan Univ.

Position title: Researcher, Central Research Institute, Korea Hydro and Nuclear Power co.,(KHNP)

Areas of interest: I&C, MMI & Power System

Yeon-Sub Jung: ysjung@khnp.co.kr

Highest degree: M.S, Department of Chemistry, Seoul National University

Position title: Group Leader, Central Research Institute, Korea Hydro and Nuclear Power Co.,(KHNP)

Areas of interest: Human Factors Engineering, Operator Experience, MMI, Power System, Process Optimization