2000년도 대한전기학회 하계학술대회 논문집 2000.7.17-20

차세대 원전 노심보호계통 소프트웨어 요구 명세서 개발

김 동 욱
한전전력연구원 원자력연구실 (Tel: 865-5663; Fax: 865-5504; E-mail: dongwook@kepri.re.kr)

Development of Core Protection Calculator System Software Requirements Specification For Korean Next Generation Reactor (KNGR)

Dong Wook Kim
KEPRI(Korea Electric Power Research Institute)

Abstract - 차세대 신형원전에서는 디지털 기술의 적용을 기본 설계 요건으로 제시하고 있다. 차세대 원전의 노심보호계통 (Core Protection Calculator Systems; CPCS)은 원전의 안전성을 보장하기 위한 부분으로 이 부분이 올바르게 작성되고, 검증되어야 함은 분명하다. 현재 이부분은 소프트웨어로 개발 중에 있으며 개발 단계에 있어서 시작단계인 요구 명세 단계에 있다. 요구 명세 단계의 오류는 소프트웨어 개발 단계 중 소프트웨어의 품질에 가장 영향을 많이 미치는 단계로 알려져 있으므로 이 단계를 정확하게 수행하여야 한다. 안전성이 중요한 소프트웨어를 명세하는 데 있어서 우선 정의되어야 하는 것은 어떤 절차를 통해서 어떤 방법으로 할지를 결정하여 그 절차를 정하여야 한다. 기존에 소프트웨어 요구 명세에 대한 표준안이 존재하기는 하지만, 이러한 표준안들은 개념적인 언어들로 쓰여져 있기 때문에 실제 소프트웨어의 개발 과정에 사용하기 위해서는 구체적인 언어들로 다시 작성하여야 한다. 따라서, 소프트웨어 명세를 작성하기 위해서 절차와 방법에 대해서 정의하여야 한다. 본 논문에서는 개략적인 명세 절차와 명세 방법등을 기술하였다.

1. 서 론

소프트웨어 개발의 성공 여부는 소프트웨어 요구사항 (Software Requirements Specification; SRS)의 완벽한 분석과 명세에 달려있다. 소프트웨어 요구사항의 개발 단계는 소프트웨어의 요구사항을 분석하고 문서화하는 것을 목적으로 한다. 요구사항 분석은 시스템 엔지니어가 소프트웨어 기능과 성능을 명시할 수 있게 해주고, 또 다른 시스템 요소들과 소프트웨어의 인터페이스를 나타내 주고, 그리고 소프트웨어가 만족해야하는 설계 제약들을 설정해 준다. SRS는 개발되는 컴퓨터 시스템의 소프트웨어 부분에 대한 모든 요구사항을 포함한다. KNGR CPCS SRS는 CPCS 기능 설계 요건 (Functional Design Requirements; FDR)의 요구사항 중에서 소프트웨어와 관련된 요구사항과 소프트웨어가 작동할 환경으로 인해 생기는 요구사항을 포함한다. SRS는 black-box 형태로 소프트웨어의 동작을 기술함으로써 소프트웨어의 external view를 제공하며, 내부적인 설계나 구현에 관한 사항들은 포함하지 않는다.

2. 차세대 원전 CPCS 소프트웨어를 위한 명세 개요

소프트웨어 요구사항 명세서(SRS)는 요구사항 분석의 결과로 만들어진다. SRS에 기술되야하는 정보는 다음과 같다.

- 시스템 전체의 개요 및 설명
- 전체 시스템으로 들어오는 입력 변수 (monitored variable)
- 전체 시스템에서 생성되는 출력 변수 (controlled variable)
- 전체 시스템으로 들어오는 입력 변수와 소프트웨어의 입력 변수 (input varaible)와의 관계
- 전체 시스템에서 생성되는 출력 변수와 소프트웨어의 출력 변수 (output varaiblae)와의 관계
- 시스템의 행동인 monitored variable과 controlled variable간의 관계; 이 관계는 시스템의 기능을 기술한 것으로 실제 요구명세에 있어서 핵심적인 역할을 한다.
- 예상되는 오류나 fault에 대한 동작
- 시스템을 설계하는데 있어서의 제약 사항. 예를 들어, 신뢰성 (reliability), 보안성 (security), 변환 가능성 (maintainability)
- 지금까지의 내용을 참조할 수 있는 목차와 찾아보기

3. 차세대 원전 CPCS 소프트웨어 명세의 프레임

차세대 원전 CPCS 소프트웨어는 특정한 하드웨어나 공급사에 종속되지 않고 표준에 따라서 설계 중이다. IEEE(Standard No. 830-1993)은 소프트웨어 요구사항 명세에 대한 후보 형식(sample)을 제안했다. 따라서 차세대 원전 CPCS SRS는 기본적으로 IEEE에서 제안한 형식에 따라 자연어 명세가 개발되었으며, 명세의 구성은 대략적으로 다음과 같다.

1. Introduction

SRS의 목적, 범위, 구성, 표기법에 대하여 기술한다.

표 1 KNGR CPCS SRS 구성

1. **INTRODUCTION**
   - 1.1 Purpose
   - 1.2 Scope
   - 1.3 Definitions and Acronyms
   - 1.4 References
   - 1.5 Overview

2. **OVERALL DESCRIPTION**
   - 2.1 Product Perspective
   - 2.2 Product Functions
   - 2.3 User Characteristics
   - 2.4 Constraints
   - 2.5 Assumptions and Dependencies

3. **SPECIFIC REQUIREMENTS**
   - 3.1 External Interface Requirements
   - 3.2 System Functions
   - 3.3 Performance Requirements
   - 3.4 Design Constraints
   - 3.5 System Software Attributes
   - 3.6 Other Requirements

2. Overall Description

개념적 수준의 하드웨어, 소프트웨어, 그리고 휴먼 인터페이스 (Human Interface)들이 외부 시스템 요소들과 내부 소프트웨어 기능에 대해 기술한다.

3. Specific Requirements

3.1 External Interface Requirements

각각의 monitored variable과 controlled variable을 기술한다.

3.2 System Functions

CPCS의 기능적 요구사항을 기술한다.

3.3 Performance Requirements

컴퓨터 시스템의 성능 요구사항을 기술한다. 성능 요구사항은 크게 시간 요구사항 (timing requirements)과 소프트웨어 수용량 요구사항 (capacity requirements)으로 구성된다.

3.4 Design Constraints

컴퓨터 시스템의 하드웨어와 소프트웨어의 설계에 영향을 미치는 제약조건을 기술한다.

3.5 System Software Attributes

컴퓨터 시스템의 신뢰도 요구사항, 변화되기 쉬운 요구사항이나 function, 소프트웨어에 관련된 모든 안전성 요구사항, 소프트웨어의 갑작스런 변경을 막기위한 요구사항을 기술한다.

3.6 Other Requirements

금까지 언급되지 않은 기타 요구사항을 기술한다.

4. SRS의 기본 모델(Basic Model)

SRS의 functional requirements는 가장 핵심적인 부분이다. 이것은 monitored variable에 의해 정의 되는 controlled variable의 값을 정의한다. SRS에서 기본적으로 가정하고 있는 모델은 discrete time 상에서 각 variable들의 값으로 정의되는 finite state machine이다. 즉, 시간의 각 점은 z = 0, 1, 2, ... 의 값을 가지게 되며 z의 초기값은 0이다. 각 연속적인 시간의 값 z 간의 간격은 시스템에서 지정된 임의의 시간 T 초 이다. C(z)는 시간 z에서의 controlled variable의 값을 표시하며, 초기화가 된 후 z*T 초 이후의 controlled variable의 값을 의미한다. 이때 T는 실제 프로그램 혹은 센서의 주기이다. 또한 M(z)는 시간 z에서의 monitored variable의 값을 표시한다. 시스템 function이 monitored variable로 부터 controlled variable로의 함수 OUTPUT으로 기술될 때에는 C(z) = OUTPUT(M(z))로 기술할 수 있다. 한편 기술된 시스템 내부에 state variable과 관련이 있는 부분이 있을 경우에는 함수 C(z) = OUTPUT(S(z),M(z)) 로 기술할 수 있다. 이때, state variable의 함수또한 S(z) = NEXTSTATE(S(z-1), M(z)) 로 정의된다. 단 이경우 z >= 1를 만족해야 하고, S(0)는 별도로 정의되어야 한다.

4.1 표기법 (Notation)

monitored variable로 부터 controlled variable로의 함수로서 시스템의 기능을 기술한다고 하였다. 이때의 표기법을 정의해 주어야 한다. 예를 들어 monitored variable의 경우에 접두사로 ''m_"을 사용하고, controlled variable의 경우에 접두사로 ''c_" 을 사용하는 것과 같은 표기법을 정의하여야 한다. 이러한 변수의 이름에 대한 표기법 외에도 각 부분에 대해서 어떻게 기술할 것인가에 대해서도 정의하여야 한다. 이부분에 대해서는 차후에 정밀하게 정의하도록 한다.

4.2 State Transition Diagrams

STD의 경우는 메모리가 필요한 함수로 기술하기 위해 이것은 계층 구조와 병행 수행을 위한 AND component가 제공되지 않는 기본적인 state transition diagram과 동일하다. 차후 시스템의 분석을 간단하게 하도록 이런 간단한 constructor 만을 제공하도록 정의하였다. 이것은 원전 명세에 있어서 어떤 조건을 만족했을때 바로 신호를 보내주지 않고 잠시 유지하고 있는 히스테리시스(hysteresis)를 기술하는 경우에 주로 사용된다. 또한 STATEMATE와 같은 계층 구조와 병행수행을 지원하는 언어에서는 상호 병행적으로 수행되어지는 부분끼리 무한히 event를 주고 받는 문제가 발생함으로써 전체 시스템의 동작을 결정적으로 정의하고

분석하기가 어려운 경우가 있다. STD로 기술된 함수의 동작은 discrete 한 시간에 동작하는 시스템의 기본 모델하에서 정의되어지는데, 각 상태정보를 출력으로 내놓으며, 각 상태간의 이동은 상태간에 연결된 천이에 기술된 조건문을 만족할 때 이동하게 정의한다. 이때 천이에 기술된 조건문은 SDT가 기술되는 AND-OR 테이블의 형식과 비슷하게 기술되어 지며, STD에 기록된 transition 이름과 일치하게 된다.

4.3 평가

차세대 원전의 CPCS에 있어서 기능의 주된 부분은 계산 부분이다. 즉 센서로 부터 주기적으로 읽어 들인 값을 평가하고 비교하여 적당한 출력을 내어 주는 부분이라고 할 수 있다. 따라서 이러한 부분을 기술하는데에는 데이타의 흐름을 중심으로 하여 시스템을 기술하는 것이 자연스럽다고 할 수 있다. 따라서 본 논문에서 제안된 명세 방법이 적합하다고 판단된다. 또한 이 명세 방법에서는 상태정보가 필요한 경우를 자연스럽게 표현하기 위하여 State transition diagram을 도입하였다.

5. 결론

개발된 차세대 원전 노심보호계통 SRS는 현재 IEEE 표준에 따른 자연어 명세를 기준으로 작성되어 있다. 그러나 원전 안전성 관련 소프트웨어이므로 자연어 명세외에 정형 명세 방법인 State Transition Diagrams법을 적용하여 개발중에 있다. CPCS SRS에 자연어 명세와 정형 명세를 결합함으로써 원자력 분야에 적합한 SRS가 될 수 있다고 본다.

[참고문헌]

[1] IEEE Standards 830-1993, "Software requir Specifications"

[2] 김동욱, "CPCS Software Requirements Specifi for KNGR", 1999. 9

[3] Karl E. Wiegers, "Software Requirements", Microsoft Press

[4] KAIST, "월성 2,3,4호기 원자로 정지계통의 필수 프트웨어의 건전성 평가 보고서", 1995. 12