원자력발전소 디지털 제어기기를 위한 정형기법 기반의 소프트웨어 개발 방법론

(A Formal Methods based Software Development Method for Digital Controllers in Nuclear Power Plants)

유 준 범*
(Junbeom Yoo)

Abstract : Software safety is an important issue for real-time embedded control systems such as PLCs(Programmable Logic Controllers) in nuclear power plants. Use of formal method to formally specify and verify software is strongly recommended by the most safety experts and government authorities. This paper introduces our experience in developing KNICS consortium's RPS(Reactor Protection System) software with support of formal methods in comparison with existing development methods.

Keywords : Software development method, formal methods, PLC, RPS, nuclear power plant

Ⅰ. 서 론

최근 원자력발전소의 제어시스템은 기존의 RLL(Relay Ladder Logic) 기반의 아날로그 시스템에서 PLC(Programmable Logic Controller) 기반의 디지털 시스템으로 교체되고 있다. PLC 기반의 제어시스템의 기능은 IEC 61131-3 (Function Block Diagram)와 LD(Ladder Diagram)[1] 등의 프로그래밍언어를 이용하여 소프트웨어로 구현되므로, PLC와 이들 프로그래밍언어의 특성이 잘 반영되어 있는 개발방법론을 사용하여 소프트웨어를 개발해야 한다. 또한, 원자력발전소와 같은 안전 최우선 시스템들은 정형기법(Formal Methods)과 같은 수학에 기반한 개발 및 검증 기법을 이용하여 소프트웨어의 안전성[2]을 보장하도록 권고되고 있다. 따라서 본 논문에서는 원자력발전소에서 사용되는 PLC 기반의 디지털 제어기기용 소프트웨어를 개발하기 위한 정형기법 기반의 개발 방법론을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 지난 10 여 년 동안 사용되어 오던 기존의 PLC 소프트웨어 개발 방법론을 소개한다. 3장에서는 기존의 개발 방법론이 지닌 문제점들을 보안하기 위하여 제안된 정형기법 기반의 개발 방법론을 소개하며, 4장에서 논문을 마무리한다.

* 유준범 : 건국대학교 컴퓨터공학부

Ⅱ. 기존의 개발 방법론

기존의 원자력발전소 제어시스템은 아래의 그림 1 에서 소개된 개발방법론을 이용하여 개발되었다. 물론 국가나 기관에 따라 약간의 편차는 있으나 그림 1과 유사한 절차에 의거해 개발되었다. 원자력발전소 제어시스템은 안전성이 매우 중시되는 시스템이므로 항상 개발 프로세스와 함께 검증 및 안전성 분석 프로세스가 병행되어 수행된다. 먼저, 개발 프로세스에서는 Waterfall Model에 의거하여, 요구사항 분석 단계에서 자연어(한국어, 영어)로 쓰인 요구사항명세서를 작성한다. 디자인 단계에서는 요구사항명세서를 기반으로 FBD 프로그램을 작성한다. 이 단계에서는 소프트웨어 엔지니어가 자연어로 명세된 요구사항을 이해한 후, 이를 FBD 프로그램으로서 변환하는 작업으로서, 오류가 많이 발생하는 단계이다.

완성된 FBD 프로그램은 지멘스나 포스콘과 같

은 PLC 제조사들이 제공하는 Engineering Tool (Compiler)에 의해서 해당 PLC를 위한 실행 가능한 기계어로 자동 변환된다. 따라서 FBD 소프트웨어와 PLC 시스템에 대한 테스트 작업만 추가적으로 완료된다면, FBD 프로그램이 완성되는 디자인 단계에서 실질적인 PLC 기반의 소프트웨어 개발이 완료되는 것으로 간주할 수 있다.

검증 프로세스에서는 각 개발 단계의 산출물들에 대한 검증 작업을 수행한다. 주로 Inspection 기법을 사용하여 요구사항명세와 FBD 프로그램에 대한 검증을 수행한다.

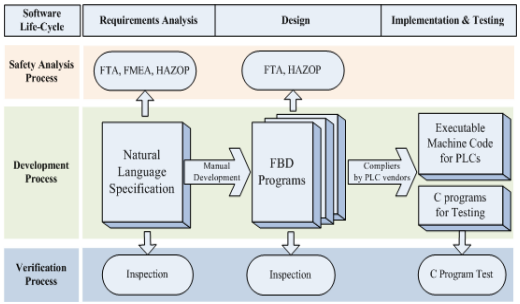

그림 1. 기존의 개발 방법론

안전성 분석 프로세스에서는 검증 프로세스와 마찬가지로 각 개발 단계의 산출물에 대해서 안전성 분석을 수행한다. 적용되는 안전성 분석 기법으로는 FTA(Fault Tree Analysis), FMEA(Failure Mode and Effect Analysis), HAZOP(Hazard and Operability)가 있다.

이와 같이 세 종류의 프로세스를 동시에 진행함으로써 원자력발전소 제어시스템은 안전성을 확보해 왔다. 반면에 이러한 개발 방법론은 여러 문제점을 안고 있는데, 우선 요구사항명세서가 자연어로 작성되므로 해석과 이해에 대한 여러 가지 문제가 발생하게 된다. 기존의 RLL 기반 아날로그 시스템에 비해 최근의 PLC 기반 디지털 시스템들은 그 복잡도가 크게 증가되었고, 소프트웨어가 사용되므로, 이러한 자연어 기반의 개발 기법은 개발된 제품을 안전성을 보장하는 데 어려움을 겪게 되었다. 따라서 한국원자력안전기술원과 같은 규제 기관에서는 정형명세 및 정형검증 등의 정형기법을 사용하여 제어시스템 소프트웨어의 안전성을 보장할 것을 요구하고 있다.

Ⅲ. 정형기법 기반의 개발 방법론

다음의 그림 2 는 본 연구에서 제안하는 정형기법 기반의 원자력발전소 개발 방법론을 소개하고 있다. 기존의 방법론과는 달리, 붉은 색의 테두리는 정형기법임을 의미하며, 파란 색 테두리의 화살표는 자동생성 및 자동수행, 녹색 테두리는 수동으로 수행되는 기법을 지원하는 기법을 의미한다. 먼저 개발 프로세스에서는 여러 문제점들을 야기했던 자연어로 써진 요구사항명세가 아닌 정형명세기법인 NuSCR[3]을 사용하였다. NuSCR은 원자력발전소의 RPS 시스템을 효과적으로 명세하기 위하여 개발된 정형명세 언어이다. NuSCR로 작성된 정형 요구사항명세서는 기존의 자연어 명세에서 발생되었던 inconsistency, incompleteness, ambiguity 등의 문제를 해결 할 수 있을 뿐만 아니라, 추가적으로 요구사항명세에 대한 수학적인 정형검증을 가능하게 해준다.

NuSCR 정형명세가 작성되면, 이와 동일한 행위를 가지는 FBD 프로그램을 자동적으로 생성할 수 있다[4]. 물론, 개발자가 고심하여 작성한 FBD 프로그램보다는 약 2.54 배 정도 사이즈가 크지만, FBD 프로그래밍을 위한 시작점으로서 유용하게 사용될 수 있다.

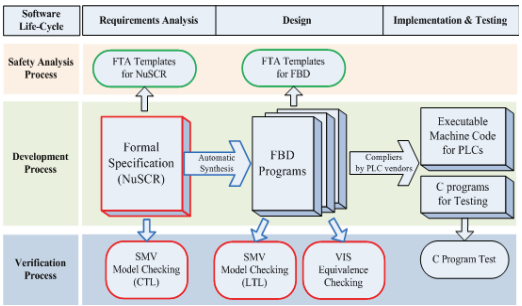

그림 2. 정형기법 기반의 개발 방법론

검증 단계에서는 기존의 Inspection 외에 다양한 정형검증 기법을 적용할 수 있다. 우선 NuSCR로 작성된 정형 요구사항명세에 대해서는 Cadence SMV model checker를 이용하여 모델 체킹을 수행할 수 있다[5]. 또한, FBD 프로그램에 대해서도 기존의 Inspection 외에 정형검증을 수행할 수 있는데, 이를 위하여 FBD 프로그램을 동일 행위를 가지는 Verilog 프로그램으로 변환하여 SMV model

checker와 VIS verification system를 이용한 정형 검증을 수행하였다 [6,7]. SMV model checker는 해당 FBD 프로그램이 특정 특성과 요구사항을 만족하는가를 수학적으로 검사할 수 있으며, VIS는 서로 다른 수정된 두 FBD 프로그램이 같이 행위를 보이는 가를 검사할 수 있다. 이러한 두 정형검증 기법은 디자인 단계의 FBD 프로그램을 검증하는 데 유용하게 사용되었다.

안전성 분석은 분석을 수행하는 전문가의 능력과 경험에 의해서 그 결과의 많은 부분이 좌우되는 분야이다. 따라서 안전성 분석은 검증 프로세스와 같이 자동화 할 수 있는 작업은 아니다. 본 연구에서는 안전성 분석 전문가가 안전성 분석을 수행하는 데 도움을 주기 위하여, NuSCR 정형요구사항명세와 FBD 프로그램을 위한 FTA 템플릿을 제공하고 있다[8,9].

이와 같이, 본 연구에서 제안하는 개발 방법론은 원자력발전소의 제어 소프트웨어의 안전성을 보장하기 위하여 정형기법을 다양한 개발 단계에서 효과적으로 이용하고 있다. 또한, 참고문헌에 제시된 바와 같이 실제 원자력발전소 제어 소프트웨어 개발에 광범위하게 사용됨으로써 그 효과를 인정받고 있다.

IV. 결 론

본 연구에서 제안하는 정형기법 기반의 원자력발전소 제어 소프트웨어 개발 방법론은 기존의 자연어 기반의 개발 방법론에 비해 소프트웨어의 안전성을 크게 증대 및 확보할 수 있다. 따라서 향후 원자력발전소 신규 개발에 널리 사용될 수 있도록, 지원 CASE 도구들을 확충하고, 도구들의 안전성을 확보해야 할 것이다. 또한, 아직 부족한 연구 즉, 추적성과 테스트 관련 연구들에 집중함으로써 제안하는 개발 방법론이 보다 넓은 범위를 지원할 수 있도록 할 계획이다.

참고문헌

[1] IEC(International Electrotechnical Commission). International standard for programmable controllers: Programming languages, part 3, 1993.

[2] N.G. Leveson. SAFEWARE, System Safety and Computers. Addison Wesley, 1995.

[3] Junbeom Yoo, Taihyo Kim, Sungdeok Cha, Jang-Su Lee, Han Seong Son, "A Formal Software Requirements Specification Method for Digital Nuclear Plants Protection Systems," Journal of Systems and Software, Vol.74, No.1, pp73-83, 2005.

[4] Junbeom Yoo, Sungdeok Cha, Chang Hwoi Kim, Duck Yong Song, "Synthesis of FBD-based PLC Design from NuSCR Formal Specification," Reliability Engineering and System Safety, Vol.87, No.2, pp287-294, 2005.

[5] Jaemyung Cho, Junbeom Yoo, Sungdeok Cha, "NuEditor - A Tool Suite for Specification and Verification of NuSCR," In proceeding of Second ACIS International Conference on Software Engineering Research, Management and Applications(SERA2004), pp298-304, LA, USA, May5-7, 2004.

[6] Junbeom Yoo, Sungdeok Cha, and Eunkyoung Jee, "A Verification Framework for FBD based Software in Nuclear Power Plants," In the proceeding of 15th Asia Pacific Software Engineering Conference(APSEC), Beijing, China, Dec. 3~5, 2008.

[7] Junbeom Yoo, Sungdeok Cha, and Eunkyoung Jee, "Verification of PLC Programs written in FBD with VIS," Nuclear Engineering and Technology,Accepted.

[8] Younju Oh, Junbeom Yoo, Sungdeok Cha, Han Seong Son, "Software Safety Analysis of Function Block Diagrams using Fault Trees," Reliability Engineering and System Safety, Vol.88, No.3, pp215-228, 2005.

[9] Taeho Kim, Junbeom Yoo, Sungdeok Cha, "A Synthesis Method of Software Fault Tree from NuSCR Formal Specification using Templates," Journal of Korea Institute of Information Scientists and Engineers, SE Vol.32, No.12, 2005.

저 자 소 개

유 준 범(Junbeom Yoo)

1999년 2월 : 홍익대학교 컴퓨터공학과 학사
2001년 2월 : 한국과학기술원 전산학전공 석사
2005년 8월 : 한국과학기술원 전산학전공 박사
2008년~현재 : 건국대학교 컴퓨터공학부 조교수

관심분야 : 소프트웨어공학, 정형기법, 안전성분석
Email : jbyoo@konkuk.ac.kr