소프트웨어 FMEA 의 전력 전자 사례 연구

정승호*, 이봉기*, 조주현*
*LS 산전 전력전자연구소
e-mail : shjeongb@lsis.com, bklee@lsis.com, joohyunc@lsis.com

A Case study on Software FMEA for Power Electronics Domain

Seungho Jeong*, Bong-ki Lee*, Joo-hyun Cho*
*LS IS Co., Ltd.

요 약

본 논문은 기능 안전에 대한 관심이 고조되고 있는 전력 전자 응용 분야에서 소프트웨어 FMEA 로 안전성 분석을 수행한 사례 연구를 설명한다. 우선, 기존 연구들이 제안한 소프트웨어 FMEA 의 방법론을 고찰하여 전력 전자 응용에 적합하게 다시 모델링을 한다. 전력 전자 소프트웨어의 안전 필수 컴포넌트를 선정하여 소프트웨어 FMEA 를 수행하고, 본 연구에서 사용한 워크시트를 소개한다. 마지막으로 소프트웨어 FMEA 를 전체 소프트웨어로 확대 적용하기 위한 방법을 고찰한다.

1. 서론

오늘날 컴퓨터, 전기, 전자 부품 또는 장치들이 복합적으로 다양한 시스템에 포함되면서, 대부분의 안전 필수 시스템(Safety-Critical System)에서도 소프트웨어가 탑재된 경우를 쉽게 찾을 수 있게 되었다. 때문에 시스템의 고장(Failure)이 치명적인 재난의 원인이 되는 장치에서 안전성을 평가하기 위한 결함 분석 기법을 소프트웨어에도 적용하려는 노력이 이루어지고 있다. 특히, 전력 전자 분야의 응용 시스템은 안전 필수 시스템인 경우가 많기 때문에 소프트웨어의 안전성을 증명하거나, 발견된 결함을 제거하는 기술에 관하여 보다 심도 있는 연구가 필요하다고 판단된다.

본 논문에서는 소프트웨어 안전성 분석 기법 중 하나인 소프트웨어 FMEA (Failure Mode & Effects Analysis)를 실제 전력 전자 제품에 대해서 수행한 사례 연구를 설명한다. 우선, 다양한 기존 연구들을 소개하고 각 연구들의 특징을 분석한다. 그리고 전력 전자 소프트웨어의 특이 사항을 설명하고, 전력 전자 분야의 소프트웨어에 기존 연구들의 소프트웨어 FMEA 방법론을 적용하면서 각 특징들이 가져올 효과를 고찰한다. 그리고 전력 전자 분야에 적합하게 다시 모델링한 방법론을 설명하고 그 결과를 보인다.

2. 소프트웨어 FMEA 연구 사례

소프트웨어 FMEA 는 1983 년에 소개됐으며, 각 컴포넌트의 잠재적인 고장을 분석하여 전체적인 시스템에 미치는 영향을 예측하는 하나의 프로세스로 연구되어 왔다. Godderd 등은 소프트웨어 FMEA 가 다양한 시스템 설계에 적용될 수 있으며, 설계의 잠재적인 취약점을 발견하고 이에 대한 개선을 권고함으로써 시스템과 소프트웨어 설계에 기여한다고 밝히고 있다[1].

ISO26262 가 표준화되면서 기능 안전에 대한 요구가 많은 자동차 전기/전자 시스템에서 김형호 등이 설명한 소프트웨어 FMEA 사례[3]는 분석의 최소 단위가 되는 소프트웨어 컴포넌트 정의 방안과 Failure Mode 의 주요 원인, 그리고 효율적 안전 메커니즘 설계 방안을 제시하고 있다. 또한 김효영 등은 소프트웨어 FMEA 를 제품 개발 프로세스에 접목하여, 제품 결함뿐 아니라, 개발 과정 중 발생할 수 있는 fault 를 줄일 수 있는 결함 예방 모델을 제안했다[2]. 또다른 연구로 결함트리 분석(FTA)과 FMEA 를 결합한 시스템 결함 분석 방법을 제안하고 이를 유비쿼터스 헬스케어 시스템에 이용한 사례연구가 있다[4].

본 논문에서는 소프트웨어 컴포넌트의 정의 방안을 제시한 김형호 등의 연구[3]를 차용하여, 본 논문에서는 전력 전자 소프트웨어에서 보편적으로 쓰이는 PID 제어 기능 컴포넌트와 PWM 컴포넌트, 그리고 센싱 컴포넌트를 정의한다. 그리고 소스 코드로 기 구현된 컴포넌트를 식별하여 이를 FMEA 를 위한 최소 단위로 도출한다. MATLAB Simulink 와 시각적 모델링 언어 또한 많이 사용되는 구현 방식이므로 해당 논문에서 설명한 식별 방안은 모두 사용이 가능하다. 또한 김명희 등의 연구[4]를 참고하여 각 컴포넌트의 고장 유형들을 정리하고 SW-FMEA 기반의 결함 예방 모델 연구[2]에서 제시한 Pre SW-FMEA 를 기 구현된 소프트웨어 컴포넌트에 수행하여 그 결과를 보인다. 하지만 유비쿼터스 헬스케어 시스템과는 달리 전력 전자 분야에서는 데이터베이스와 통신과 관련된 고장보다 제어 기능 고장이 안전성에 미치는 영향이 훨씬 치명적이기 때문에 고장 유형들에 대한 새로운 정의가 필

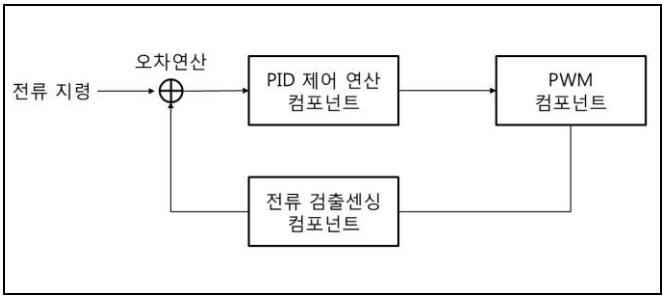
요하다.

3. 소프트웨어 FMEA 적용

전력 전자 분야에서는 디지털 제어, 보호 동작, 진단, 통신 등의 기능에 소프트웨어를 널리 사용해왔다. 특히 디지털 제어 기능은 실질적으로 하드웨어 소자들을 제어해서 필요한 전류와 전압을 제어하는 기능으로 안전과도 매우 밀접한 관련이 있다. 때문에 본 연구에서는 디지털 제어기능에 주목하여, 실제로 모터를 제어하는 소프트웨어에 FMEA 를 실행하였다.

(그림 1)은 저전압 드라이브(Low-voltage Drive, Inverter)의 디지털 제어 기능을 도식화 한 것이다. 디지털 제어기능은 크게 세 가지 컴포넌트로 이루어지며 각 컴포넌트의 기능은 다음과 같다.

- PID 제어 연산 컴포넌트: PID 제어 연산을 수행하는 소프트웨어 컴포넌트이다.
- PWM 컴포넌트: 스위치 소자에 연결된 PWM 출력기능을 구현한 소프트웨어 컴포넌트이다.
- 전류 검출센싱 컴포넌트: 제어 대상 전류의 양을 검출하는 소프트웨어 컴포넌트이다. 검출된 전류의 양은 피드백(Feedback)되어 PID 제어 연산에 사용된다.



(그림 1) 디지털 제어 기능

고장 유형과 영향 분석을 위해서는 워크시트를 결정하고 이 워크시트를 바탕으로 각 컴포넌트와 시스템에 소프트웨어 FMEA 를 수행해야 한다. 표 1 은 고장 유형과 영향분석을 위한 워크시트의 표본이다. 워크시트는 기존 연구들 [2, 4]을 참고하고, 소프트웨어 컴포넌트의 I/O 가 중요한 분석 요소임을 고려하여 이를 반영하였다. 워크시트에는 각 함수에서 I/O 를 목적으로 사용하는 전역 변수들을 명세하고 각 변수들의 고장 유형과 영향 분석 결과를 정리하였다. 이를 통해 각 컴포넌트의 I/O 의 분석 결과를 더욱 쉽게 파악할 수 있으며, 소프트웨어 FMEA 가 컴포넌트 간 I/O 에 주목하면서 수행되기 때문에 더욱 효과적인 결과를 보였다.

소프트웨어 FMEA 를 수행한 결과, 설계상의 안전 결함을 찾아내는 데에 효과가 있었으나 분석에 많은 인력과 시간이 필요하여 이를 연구 개발 중인 모든 소프트웨어에 적용하기에는 부담이 크다. 때문에 본 연구에서는 소프트웨어 컴포넌트 간의 I/O 에 주목하여 FMEA 를 수행했으나, 김효영 등의 연구[2]에서 제안한 Pre SW-FMEA 를 접목하여 데이터베이스를 구축하면 더욱 효과적인 FMEA 가 가능할 것으로 기대되며, 효율적인 SW-FMEA 연구를 계획하고 있다.

4. 결론

본 논문에서는 기존 연구들[2, 3, 4]을 참고하여 전력 전자 응용 소프트웨어에 소프트웨어 FMEA 를 수행한 방법과 결과를 소개했다. 전력 전자 분야의 소프트웨어에서 가장 중요한 기능일 뿐 아니라 안전성에도 큰 영향을 주는 소프트웨어 컴포넌트들을 선정하여 이들 컴포넌트의 I/O 를 중심으로 소프트웨어 FMEA 를 수행했다. 그 결과 안전성의 취약점을 알 수 있었으며, 추후 연구 개발 할 소프트웨어에 반영할 계획이다. 마지막으로 소프트웨어 FMEA 에 투입되는 인력과 시간을 줄이기 위한 방법을 고안 할 계획이며, 이를 통해 안전 관리 연구 분야에 기여를 할 수 있을 것으로 기대된다

참고문헌

[1] Peter L. Goddard, Raytheon, Troy, “Software FMEA techniques,” *Pro. annual Reliability and Maintainability symposium*, IEEE, pp.119-123, 2000.

[2] 김효영, 한혁수. “SW-FMEA 기반의 결함 예방 모델”, 정보과학회논문지 : 소프트웨어 및 응용 33(7), pp. 605-614, 2006.7.

[3] 김형호, 이남희. “기능 안전의 효율적 향상을 위한 소프트웨어 FMEA 사례 연구” 한국자동차공학회 학술대회 및 전시회, pp. 1303-1308, 2012.11.

[4] 김명희, 박만곤. “소프트웨어 안전성 평가를 위한 소프트웨어 고장 유형과 영향 분석에 관한 연구” 멀티미디어학회논문지 15(1), pp. 115-130, 2012.1.

<표 1> 고장 유형과 영향분석을 위한 워크시트

Sl No.	Variable Name	Variable Scope	Function Details	Functions								
			Module Name /Function Name	Func1()	Func2()	Func3()	Func4()	Func5()	Func6()	Func7()	Func8()	Func9()
1	Variable1	Global-Static		OO	II	-	-	-	-	-	-	-
2	Variable2	Global-Static		OO	II	-	-	-	-	-	-	-

										After implementation of recommendations		
Sl No.	Variable Name	Data Type range	Actual Values range	Failure Modes		Software Module / Function Name	Effects		Potential Severity	Recommendations	Severity	Remarks
				Expected	Actual		Local Effect	System Effect				