요건추적매트릭스의 국제핵융합실험로 AC/DC 컨버터 Plant Interlock System(PIS) 적용연구

신현국, 오종석, 최정완, 서재학, 이락상*, 이의재**
국가핵융합연구소, 다원시스*, 모비스**

Application Study of Requirement Traceability Matrix (RTM) to ITER AC/DC Converter Plant Interlock System (PIS)

Hyun Kook Shin, Jong Seok Oh, Jungwan Choi, Jae Hak Suh
Rack sang Lee*, Ei Jae Lee **
National Fusion Research Institute, Dawonsys*, Mobiis**

ABSTRACT

ITER 한국사업단은 AC/DC Converter 최종설계검토(FDR)를 2014년 4월에 끝내고, 제작에 관련된 준비사항 점검인 MRR (Manufacturing Readiness Review)를 2014년 10월에 수행하였다. 1차 제작공정인 CCU/L 컨버터와 관련 I&C System은 2014년 11월부터 제작에 착수하여 곧 FAT(Factory Acceptance Test)를 앞두고 있다. 이 시점에서 중요한 것은 FAT를 앞둔 제작된 기기가 ITER의 설계요건을 충분히 만족하는지에 대한 검증을 하는 것이다. 본 논문은 초전도자석 및 컨버터의 이상상태 또는 고장 시에 장치를 보호하는 중요한 Plant Interlock System(PIS)이 ITER의 설계요건을 충실히 반영하였는지 확인하기 위한 요건추적매트릭스(RTM) 기법을 소개하고, Interlock System의 중요기능인 사고 시 초전도 코일에 충전된 에너지를 급속 방전하기 위한 장치인 DLIB와의 연계기능에 적용한 예를 보이고자 한다.

1. 서 론

요건추적매트릭스(RTM)는 설계단계의 계통요건(System Requirement)이 하드웨어 및 소프트웨어에 잘 반영되었는지 확인하는데 많이 사용되고 있다.[1] 최근에는 컴퓨터에 기반을 둔 확인검증(V&V) 툴이 많이 사용되고 있으며, 개념설계단계부터 설계단계, 구현단계, 시험단계까지의 전 과정에 요건추적매트릭스가 사용되고 있다.

그러나 검증 소프트웨어 툴은 많은 장점에도 불구하고 요건추적에 어려움이 있다. 즉 소프트웨어 툴에 기초하여 모든 문서를 개념단계에서 제작 및 소프트웨어 개발까지 일관성 있게 사용되어야 하는데, 개발 현실은 그렇지 못하다. 소프트웨어 툴을 사용하기 위해 모든 설계입력을 정형화된 형식에 맞추어야 하고, 컴퓨터가 인식할 수 있게 약속된 단어 및 문장을 사용해야 하는 어려운 제약이 따른다.

특히 ITER Project와 같이 ITER 국제기구가 개념설계를 한 후에 여러 참가국전담기관 및 공급자가 설계 및 제작을 각각 진행한 경우, 검증 소프트웨어 툴을 사용하여 요건을 추적하기가 어렵다. 따라서 이런 경우에는 계통설계를 이해하는 사람이 요건추적매트릭스 테이블을 작성하고 ITER에서 요구하는 계통요건을 설계단계, 제작단계 그리고 시험단계의 문서를 확인하여 적용하는 수작업 방식이 바람직하다. 따라서 본 논문에서는 계통설계 관점에서 요건추적매트릭스 기법을 사용하여 요건추적의 적합성을 검토하였다.

2. ITER Plant Interlock System 구조 및 기능

ITER의 Interlock system은 Central Interlock System(CIS)과 Plant Interlock System(PIS) 두개 층으로 구성되어 있다. CIS는 다수의 PIS를 조율하여 피해를 줄 수 있는 사건/사고로부터 초전도체와 컨버터들을 보호하는 기능을 제공한다. PIS는 해당 Plant system의 설비를 보호하는 역할을 담당한다.[2]

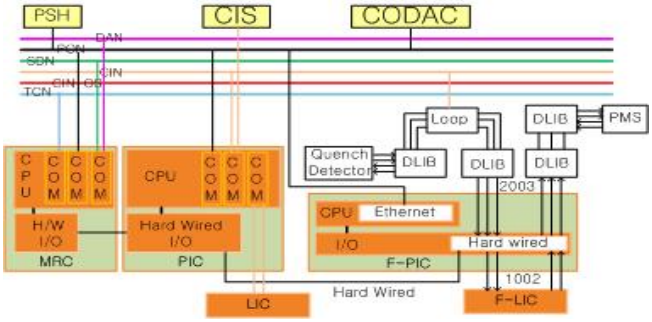

그림1. ITER Plant Interlock System (CC Plant) 구성도

Interlock System의 주 기능은 Powering permit과 Powering failure이다. 전자는 CIS에서 PIS로 내려가는 명령이고, 후자는 Plant system에서 사건/사고가 발생한 경우 PIS에서 상위 CIS에 전달하는 것이다. Central Interlock 신호가 발생하면, PIS는 Powering permit 신호를 제거하며, 이 명령은 LIC (Local Interlock Controller)에 다시 전달된다. 그리고 인터록과 관련된 데이터인 Non critical interlock data는 LIC로부터 직접 또는 Fast PIC로부터 PIC(Plant Interlock Controller)를 거쳐 PSH (Plant System Host)에 전달된다.

그림1의 Fast PIC(F PIC)은 Hardwired logic인 DLIB (Discharge loop Interface Box)와 직접 연결되어 있으며, 코일 상태를 감지하고 이상 시에 PMS (Protective Make Switch)를 작동시킨다. F PIC은 신호의 고속처리를 위하여 FPGA (Field Programmable Gate Array)가 내장된 CompactRIO를 이용하며, slow PIC과 LIC은 Siemens PLC를 사용한다.

3. PIS의 요건추적매트릭스 적용 및 검토

3.1 PIS의 요건추적매트릭스(RTM) 적용

ITER PIS의 설계요건은 PCDH(Plant Control Design Handbook) 6절 Interlock I&C Specification에 잘 기술되어 있다. Interlock 설계요건을 기준으로 FDR(Final Design Review), MRR 및 최종시험(FAT) 단계별로 생산된 문서를 검토하여 요건에 부합한 내용을 매트릭스에 정리하였다. PIS의 요건은 45개로 정리되었다. 단계별로 생산된 문서 중 사용된 문서는 아래 표1과 같다.

요건추적매트릭스 기법으로 작성한 sample이 표 2에 제시되어 있다. 요건추적매트릭스에 작성된 내용을 검토하면, PIS의 설계 및 제작이 대부분 요건을 만족하였다. 매트릭스 표2에 있는 빈칸들은 단계별 생산된 문서에서 찾아내기가 어려웠던 부

분이다.

표1. 요건추적에 사용된 문서목록

	FDR 문서	MRR 문서	FAT 문서
1	DEF-02 RAMI analysis and spare parts	M D D - 1 6 Manufacturing and Inspection Plan for MCS	FAT Procedure for MCS of CCPS
2	DEF-07 Local I&C System for CC AC/DC Converter	Incoming Inspection Procedure for MCS	DJF-13 FAT for MCS CCPS
3	DEF-11 SDDD for MCS	D1B - CCPS I&C Functional Analysis	MDD-19 Software Test Plan for MCS of PIC
4	DEF-12 Functions of MCS	D1C - CCPS Plant System I&C Architecture	CCPS MCS softwre test plan
5	DEF-13 Design of MCS	D31 - Functinonal Specification of MCS	
6	RQF-04 Interface of MCS	D32 - Software Documents and files	

예를 들면, 표2의 R216 “PCDH에 따라 PIS가 정의되고, 특성화되고, 구분된 각 기능은 충실히 수행되어야 한다.”는 요건은 관련문구나 문장을 FAT 절차서나 Test plan에서 찾을 수 없었지만, FDR 단계나 MRR 단계의 문서에서는 찾을 수 있었다. 이와 같이 구체적인 것이 관련 단계에 없어도 다른 단계에 있다면 추적성을 만족한다고 판단하였다. 특히 표2에서 R243, R333, R335을 보면 요건이 구체적일수록 모든 단계의 문서에서 추적성이 잘 관찰되었다.

표 2. PIS Requirement Traceability Matrix Table

번호	요건내용	FDR 단계 문서	MRR 단계 문서	FAT 단계 문서
R 216	Each function carried out by a plant system interlock I&C shall be defined, characterized and classified according to the guidelines given in this chapter or by an equivalent method.	DEF-12 (46P) : PIS 구조는 Local인지, Central 인지 기능분석과 Integrity level, safety time, allocation rule에 따라 특성이 정해진다.	D1B (48P) : PIC은 컨버터 간의 인터록사건을 조율하고, 컨버터를 운전하기 위해 CIS로부터 인터록 요청을 받는다. 등 PIC 기능에 대한 서술 있음.	
R 217	Each function shall be described with at least the following fields: Protection/function name: define a name or unique identifier		D31 (34P): 4.3 Function Breakdown of the Plant Interlock Controller (PIC): 그림 4-3에 PIC의 구조와 기능에 대한 기술하였음.	
R 243	Plant Interlock System Controllers shall comply with the assigned SIL level.	DEF13(119P): PIC implements the 3IL-2 interlock functions, enables a response time in the order of 100ms and interfaces with other controllers.	Incoming Inspection Procedure for MCS (7P) :4.3 To be inspected components PLC S7-400, UR2 Rack, 9 Slots.	MDD-19 (12/13P) : Test Environment The MCS PIC is based on the 3IL-2 as it is based on the Siemens S7-400FH.
R 333	The slow architecture is based on COTS industrial components Programmable Logic Controllers, (PLC).	DEF13(119P) : PIC is an interlock controller based on the slow architecture, where Siemens Simatic S7- 400FH PLC.	Incoming Inspection Procedure for MCS (7P) : 4.3 To be inspected components PLC S7-400, UR2 Rack, 9 Slots	MDD-19 (12/13P) : Test Environment The MCS PIC is based on the 3IL-2 as it is based on the Siemens S7-400FH.
R 335	The Interlocks may be maskable or bypassable independently from the ITER Global Operation States (GOS)	DEF-13 (147P) : 11.4.1 State Machine of PIC The Table 11-4 describes each state of PIC in more detail.	D31(37P) : Machine/converter operator: Central Interlock event 발생 시에, PIC는 차tth 부터 Interlock action 명령을 받는다. 이때 sub-CVOS change도 요구한다.	FAT Procedure for MCS (54P): On State Machine make a request to change the COS of MAG as Ready by clicking the Ready button indicated as a red block in the figure.

RTM 표의 모든 단계에서 추적성을 만족시키지 못한 요건은 R223, R227, R233 3개 이며, 이들의 추적성이 낮은 이유는 크게는 요건이 추상적이며, 애매한 경우다. 이들 요건에 대한 사유를 분석하면 표3과 같이 추정할 수 있다.

표3. 추적성이 낮은 요건의 사유분석

	설계요건	사유분석
R223	The complexity of the I&C shall be restricted to the minimum required.	복잡성의 최소화 기준을 세우기가 어려움
R227	Inviolability implies that everything should be implemented to restrict the risks of errors during: periodic test operations, corrective maintenance operations, modifications of the installation	모든 설비가 보수유지 중 실수에 의해 고장을 일으키지 않도록 설계하는 것은 암묵적으로 반영된 것으로 판단됨
R233	Incoherencies in behaviour (control or measurements conflicts) between redundant equipment shall be reported to the operators.	측정과 제어 간에 모순이 발생하면, 운전자는 제어콘솔에 표시된 정보로 쉽게 판단이 가능함

3.2 F-PIC 연계시험을 통한 요건적용 확인

요건추적이 어려웠던 R223의 설계반영 여부를 확인하기 위해 마그넷코일에 quenching이 발생한 경우 Fast Action을 위해 복잡한 로직의 소프트웨어로 구동되는 PLC보다 반응속도가 빠른 하드웨어로 구성된 DLIB 설계를 검토하였다. 보호계통에서는 어떤 경우에도 동작하는 하드웨어를 선호한다. 소프트웨어로 구동되는 PLC를 제외하고 하드웨어를 사용한 것은 인터록 기능의 단순성 및 신뢰성을 높인 것으로 판단된다.

그림 2는 F PIC과 DLIB 간의 연계를 확인하는 시험으로 Test Board의 스위치를 이용하여 연계 및 2oo3 voting logic의 정확성을 체크하였다. 특히 wire로 연결된 F PIC의 Controller의 고장에도 DLIB의 구동에는 영향을 주지 않아 인터록 기능의 신뢰성이 매우 높은 것으로 판명되었다. DLIB 설계는 복잡성을 최소화하면서 기능의 신뢰도를 높인 사례로 판단된다.

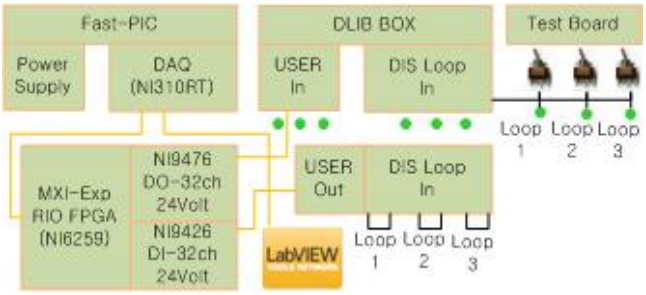

그림 2. DLIB Interface 작동시험

4. 결 론

요건추적매트릭스 기법을 ITER PIS 문서의 요건 추적에 적용하였다. ITER 전원장치 PIS설계 경우, RTM 소프트웨어의 툴에 의해 작성되지 않았지만, 대부분 요건을 만족하고 있었다. 일부 추적이 어려운 요건은 정성적 분석과 장치의 간단한 시험을 통하여 만족여부를 판단하였다. ITER와 같이 규모가 크고, 여러나라가 장치 및 설비를 공급하는 Project에는 RTM 소프트웨어 툴을 도입하여 사용하는 것이 설계관리 및 설계의 정확성을 높일 수 있다고 판단된다.

이 논문은 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 국책연구사업임 (No. 2007 -2006995)

참 고 문 헌

[1] 정천수, 김승렬, “정보시스템개발 프로젝트에서 효과적인 요구사항추적 관리방안연구”, Journal of The Society of Computer and Information, V0l 17 No. 5, May 2012.

[2] Luigi Scibile, Jean Yves Journeaux, Izuru Yonekawa, 외2인, “An Overview of the ITER Interlock and Safety Systems”, Proceedings of ICALEPCS 2009, Kobe, Japan.