ISSN 1975-8359(Print) / ISSN 2287-4364(Online)
The Transactions of the Korean Institute of Electrical Engineers Vol. 63, No. 12, pp. 1637~1639, 2014
http://dx.doi.org/10.5370/KIEE.2014.63.12.1637

원자력발전소 안전등급 계통 적용을 위한 디지털 상용기기 품질검증

Commercial Grade Item Dedication of Digital Devices for Safety-related System in Nuclear Power Plant

홍 영 희* · 배 병 환* · 박 재 현†
(Young Hee Hong · Byung Hwan Bae · Jaehyun Park)

Abstract - In the past, the analog protection relays have been widely used for the safety-related systems in the nuclear power plants due to their stability and reliability. Meanwhile, as the high performance digital system has been developed, the digital systems have been adopted in the non-safety systems. However, since the digital systems currently used in the non-safety systems were not developed according to Q-class standard, Commercial Grade Item Dedication (CGID) procedure should be performed in order to apply them to the safety-related system.
The purpose of this paper is to describe the CGID procedure including the analysis of the hardware architecture as well as the software embedded in protective relay to apply to the emergency diesel generator in the nuclear power plant. The entire CGID procedure was performed strictly according to the international standard and regulations.

Key Words : Commercial grade item dedication(CGID), Nuclear power plant, Safety protection system,

1. 서 론

원자력발전소 전력계통 고장파급 방지와 기기 보호를 위한 아날로그 방식과 고정배선방식(Static) 방식의 제어시스템이 널리 사용되어 왔으나 아날로그 제품의 단종과 최신 설비로의 개선 수요로 인하여 신뢰성과 성능이 입증된 디지털 제품으로의 교체 필요성이 대두되었다. 그러나 원자력발전소 안전등급 계통에 적용되기 위해서 요구되는 안전등급기기에 대한 엄격한 요건에 비하여 상대적으로 협소한 시장규모로 인하여 원자력발전소 전력계통 보호에 특화된 디지털기기의 개발은 매우 제한적으로 이루어지고 있는 반면 원자력발전소 비안전등급 제어계통에는 다양한 기능을 가진 고성능 디지털기기가 널리 채택되어 활용되고 있다. 그러나 이들 디지털기기는 원자력품질보증계획에 따라 설계·제작·성능검증절차를 거쳐 개발된 기기가 아니므로, 이들 디지털기기를 원자력발전소 안전등급 계통에 적용하기 위해서는 일반규격품 품질검증(Commercial Grade Item Dedication; CGID)절차를 통하여 안전성과 신뢰성에 대한 평가와 검증이 선행되어야 한다.

일반규격품에 대한 품질검증 절차에 관한 규정과 표준은 미국 원자력 규제기관인 EPRI 가이드라인 NP-5652에 근거가 마련되어있다[1]. 그러나 NP-5652는 모든 부품에 적용될 수 있는 일반적인 절차를 규정하고 있어, 전통적인 기계·전기·계측 부품에는 적용이 용이하나, 최신 디지털기기 특히 소프트웨어가 탑재된 지능형 디지털기기에 적용하기 위해서는 별도의 세부적인 절차가 요구된다. 따라서 디지털기기에 대한 인증 절차와 요건은 IEEE 7-4.3.2 표준[2]과 별도의 EPRI 가이드라인 TR-106439[3]에 규정되어 있다.

국내 원자력발전소에서 일반규격 디지털기기의 품질검증 사례는 많지 않으나, 동유럽과 중국 등 비교적 최근에 원자력발전소를 새로 건설하거나 대규모 설비개선 작업을 진행한 외국에서는 디지털기기에 대한 일반규격품 품질검증 사례를 발견할 수 있다[4]. 또한 이들 일반규격품 품질검증 절차를 학술적으로 접근한 연구 결과도 제시되고 있다[5,6].

국내에는 이미 23기의 원자력발전소가 상업운전을 하고 있으며, 현재 건설중인 원자력발전소도 6기에 달하는 등 원자력발전 관련 디지털기기의 수요는 매우 높은 편이다. 이들 원자력발전소 안전등급 계통에 소요되는 부품 중 기계적 부품, 케이블과 같은 수동형 부품과 지시계와 같은 비교적 단순한 디지털기기에 대해서는 꾸준히 일반규격품 품질검증 절차가 진행되고 있으나, 소프트웨어가 탑재된 지능형 디지털기기에 대해서는 일반규격품 품질검증 사례가 없었다.

본 논문은 디지털 일반규격기기를 고도의 안정성과 신뢰성이 요구되는 원자력발전소 안전등급 전력계통에 적용함에 있어 필수적인 절차인 일반규격품 품질검증 절차를 설명하고 국내 가동중인 원자력 발전소에 적용된 디지털보호계전기에 대한 일반규격품 품질검증 사례를 기술한다.

2. 일반규격기기의 품질검증 절차

원자력발전소 안전계통에 일반규격기기를 적용하기 위한 인증 평가방법은 EPRI NP-5652 가이드라인에 규정되어 있는데 일반규격기기의 안전기능 분석과 필수특성 수립 등의 기술평가를 표 1의 4가지 평가방법을 활용하여 수행하여야

† Corresponding Author : Dept. of Information and Communication Engineering, Inha Univeristy, Korea
E-mail:jhyun@inha.ac.kr
* Central Research Institute, Korea Hydro and Nuclear Power Company., Korea .
Received : September 01, 2014; Accepted : November 18, 2014

한다. 다만, 이들 평가방법 중, 방법 2와 4는 단독으로 사용될 수 없으며 반드시 방법 1과 3을 포함할 경우 보조적으로 사용할 수 있는 평가 방법이다.

표 1 일반규격기기 인증 평가 방법[1]
Table 1 Assessment Method for CGID[1]

방법	평가 방법
1	Special test and inspection
2	Commercial grade survey of supplier
3	Source verification
4	Acceptable supplier/item performance record

NP-5652 가이드라인과 더불어 디지털기기에 대한 일반규격품 품질검증 절차는 EPRI TR-106439를 따르도록 하고 있다. TR-106439에 따르면 기기평가 항목을 필수특성(Critical characteristics)에 따라 평가하도록 규정하고 있는데, 대표적인 필수특성으로 물리적 특성(Physical characteristics), 성능특성(Performance characteristics), 신뢰성 특성(Dependability characteristic)의 세 가지 특성을 제시하고 있다. 제시된 세 가지 특성 중, 안전등급 계통에 사용되는 디지털기기의 성능특성의 경우 IEEE에서 정한 표준에 준거하여 설계되어야 하는데 이때 적용되는 표준이 IEEE 7-4.3.2 표준이다. 표준에 따르면 보호계통에 사용되는 디지털기기의 경우, 독립성, 단일고장배제원칙 등이 제시되고 있으며, 이와 같은 성능특성이 만족되는지를 품질검증과정에서 확인하여야 한다. 또한 신뢰성 특성 관점에서는 소프트웨어가 탑재된 디지털기기의 경우 하드웨어와 더불어 탑재된 소프트웨어의 신뢰성 검증이 반드시 수반되어야 한다. 소프트웨어의 신뢰성을 검증하는 방법은 ISO 또는 IEEE 표준에 준거하여 수행되는데 IEEE Std. 1012와 IEEE Std. 1074 표준이 적용될 수 있다[7,8]. 이와 더불어 미국 원자력위원회의 가이드라인인 NUREG-CR6421의 적용에 가능하다[9].

소프트웨어 평가는 개발과정뿐 아니라 제품 기획에서부터 폐기까지 전체 생명주기에 대한 검증이 이루어져야 하는데 이는 원자력발전소의 수명이 40년 이상으로 사용기간이 타 산업분야에 비하여 매우 장기간이며, 수명기간동안 발생할 수 있는 다양한 오류에 대한 적절한 보완과 성능개선 과정을 평가하기 위함이다.

3. 국내 디지털 일반규격기기 품질검증

본 논문에서는 2013년도에 수행한 원자력발전소용 디지털 보호계전기에 대한 일반규격기기 품질검증 사례를 제시한다. 품질검증 대상 디지털보호계전기는 원자력발전소 안전운전과 정지에 필요한 전원상실 시 원자로 보호와 제어계통에 필수전원을 공급하는 비상디젤발전기용 보호계전기이다. 디지털 보호계전기는 비상디젤발전기에서 발생한 전기적 고장의 파급방지와 발전기 보호기능을 수행한다.

본 품질검증 절차를 수행하기 위하여 EPRI TR-106439에서 제안하는 필수특성을 표 2와 같이 도출하고 각 특성에 대하여 EPRI NP-5652에 규정된 1, 2, 3, 4 방법 모두를 적용 평가하였다. 특히 물리적 특성과 성능 특성은 주로 방법

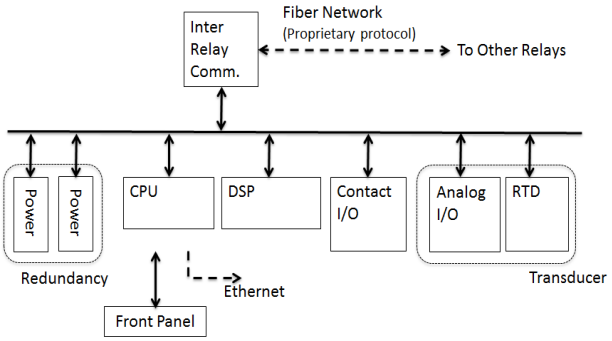

그림 1 검증대상 보호계전기 블록도
Fig. 1 Block diagram of Digital Protection Relay

1을 적용하여 국내기관에서 수행하였으며, IEEE 7-4.3.2에 준거한 설계 성능특성, 하드웨어와 소프트웨어 신뢰성 특성은 방법 2, 3을 적용하여 품질보증계획, 제품의 기획·설계·제조·공장검사 등 전 과정에 대한 검사와 평가를 제작사 방문을 통해서 수행하였다.

3.1 물리적 특성 평가

물리적 특성평가는 주로 하드웨어 특성을 평가하는 것으로 보호계전기의 정격확인, 내구성 및 전기적 특성을 평가하게 된다. 물리적 특성에 대한 평가는 NP-5652에 정의된 평가방법 1에 따라 국내기관에서 진행하였으며 이는 일반 기계부품과 수동기기에 대한 평가와 동일한 평가방법과 절차에 따라 하드웨어의 내환경특성을 포함한 모든 동작특성 및 이상상황에서의 안정적 동작 여부를 평가하였다.

3.2 성능 특성 평가

성능 특성은 대상 기기의 안전기능 수행에 필요한 기능 필수특성과 제품의 고유 설계 필수특성으로 나누어지며, 이는 원자력기기로서의 설계기준과 성능검증 요건을 만족하는지 여부를 평가하였다. 기능 필수특성은 물리특성과 마찬가지로 방법 1에 따라 국내기관에서 검사하였으며, 설계 필수특성 평가는 방법 2를 이용하여 제작사를 방문하여 설계문서 열람과 설계자의 인터뷰를 통하여 평가하였다.

설계 필수특성 평가 시 가장 중요하게 평가되는 항목은 IEEE 7-4.3.2 표준에 부합여부를 평가하는 것으로 단일고장에 대한 영향, 독립성, 고장수목평가, 정시성(결정론적 수행시간 준수 여부) 등이다. 특히 기기내부에 탑재된 운영체제의 정시성과 안정성에 대한 집중적인 평가가 수행되었다. 평가대상인 디지털보호계전기의 경우 그림 1에 보이는 블록도와 같이 전제 시스템을 관장하는 메인프로세서와 계전기 보호 알고리즘이 수행되는 보조프로세서가 존재하는 다중 프로세서 구조이므로 각각의 프로세서에서 수행되는 소프트웨어의 성능 평가 및 상호 연동에 따른 영향, 특히 보호알고리즘의 결정론적 수행 능력에 대한 평가가 진행되었다.

3.3 신뢰성 특성 평가

일반규격기기 품질검증 절차에 따른 디지털기기의 신뢰성 특성평가는 기기 자체의 신뢰성에 대한 평가와 탑재된 소프트웨어의 신뢰성 평가로 나누어 진행되었다. 기기 자체에 대한 신뢰성 평가는 기기의 운용이력(Operating history)를

표 2 필수 특성
Table 2 Critical Characteristics

	필수특성	판정기준	검증방법
물리 특성	제품의 정격	구매사양에 부합여부	방법 1
	인터페이스	지시, 조작 적합성	방법 1
성능 특성	계전기 보호기능	구매규격과 일치여부	방법 1,2
	실시간 보호기능	제작사 사양서	방법 1,2,3
	비정상상태 작동	제작사 사양서	방법 1,2,3
신뢰성 특성	설계품질	SW 설계와 V&V	방법 2,3,4
	고장관리	SW 오류개선 절차	방법 2,3,4
	형상관리	SW 업그레이드 절차	방법 2,3
	신뢰도와 가용성	기기 신뢰도 등 만족	방법 2,3,4

통한 평균고장시간(MTBF) 조사와, 고장발생 시 제작사의 대처방안, 타 산업영역에 적용 사례와 평가 등을 NP-5652에 규정된 방법 2, 3, 4 에 따라 제작사를 방문하여 관련 서류 검토와 담당임원의 면담을 통하여 검증하였다.

탑재된 소프트웨어의 신뢰성 평가는 NP-5652 방법 3에 따라 제작사를 방문하여 IEEE Std. 1012에 규정된 소프트웨어 검증절차(Verification and Validation; V&V)에 의거하여 평가되었다. 평가 시 주안점은 소프트웨어 생애전주기(Life cycle time)에 거쳐 표준에 준거한 관리가 이루어지고 있는지 여부와, 소프트웨어 V&V 수행 조직의 독립성 여부, 소프트웨어 형상관리의 완결성 등이다. 이와는 별도로 최근 대두되고 있는 사이버보안의 준수 여부의 확인을 통하여 탑재 소프트웨어의 위변조 가능성을 확인하였다.

4. 결 론

본 논문은 디지털기기의 일반규격기기의 국내 원자력발전소 안전계통에 적용을 위한 품질검증 절차를 소개하고 이를 운전중인 원자력발전소의 비상발전기용 디지털 보호계전기를 대상 적용한 실례를 제시 하였다. 본 논문에서 제시한 일반규격기기 품질검증 절차는 관련 국제 규정인 EPRI NP-5652, NP-106439, IEEE-7-4.3.2 등에서 규정된 절차와 부합하며, 특히 디지털기기의 특성을 고려하여 탑재된 소프트웨어에 대한 V&V 절차와 결과물을 확인하는 절차가 강조되었다. 본 논문에서 소개한 일반규격 디지털기기 품질검증 사례는 국내에서 원자력발전소 안전계통에 사용되는 지능형 디지털기기의 일반규격품 품질검증(CGID) 사례로는 최초의 사례라는 의미가 있으며, 향후 원자력발전소에서 사용되는 다양한 종류의 디지털기기의 일반규격품 품질인증에 적용될 수 있을 것이다.

References

[1] EPRI NP-5652 : Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications.

[2] IEEE Std. 7-4.3.2 : IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.

[3] EPRI TR-106439 : Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications

[4] Damir Mandic, "Usage of Commercial Grade Programmable Digital Systems in Safety Related Applications," Proceedings of International conference on Nuclear Option in Countries with Small and Medium Electricity Grids, pp.26-27, Dubrovnik, May 21-25, 2006.

[5] Fink, R.T.; Betlack, J.O.; Torok, R.C., "Application of guidelines on digital I&C upgrades," IEEE Conference on Nuclear Science Symposium and Medical Imaging Conference, vol. 3, pp.1063-1067, Oct. 30 - Nov. 5, 1994.

[6] Das, R.K.; Hajos, L.G., "Commercial grade item (CGI) dedication of generators for nuclear safety related applications," IEEE Transactions on Energy Conversion, vol.8, no.1, pp.138-144, Mar. 1993.

[7] IEEE Std. 1012 : IEEE Standard for Software Verification and Validation

[8] IEEEStd. 1074 : IEEE Standard for Developing Software Life Cycle Processes

[9] NUREG/CR6421 : A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications

저 자 소 개

홍 영 희(Young Hee Hong)

1993년 조선대학교 전기공학과 학사. 2009년 충남대학교 전기공학과 석사. 1993년~현재 한국수력원자력(주) 중앙연구원 근무. 관심분야는 원전기기 성능검증과 전력설비 설계·정비

배 병 환(Byung Hwan Bae)

1983년 KAIST 핵공학과 석사, 1983년~현재 한국수력원자력(주) 중앙연구원 근무. 관심분야는 원전기기 성능검증과 신형원전 개발

박 재 현(Jaehyun Park)

1986년 서울대학교 제어계측공학과 학사, 1988년 동 대학원 석사, 1994년 동 대학원 박사, 1995년~현재 인하대학교 정보통신공학과 교수, 관심분야는 임베디드시스템, 고신뢰성 컴퓨터시스템