한국철도학회논문집
제10권 제6호 2007년 | pp. 730-734

철도신호 내장형제어기 안전성 향상을 위한 워치독타이머 설계 및 평가

Design and Assessment of a Watch Dog Timer for Safety Improvement of an Embedded Railway Signal Controller

신덕호† · 이강미* · 이재호** · 김용규**
Ducko SHIN · Kang-Mi LEE · Jae-Ho LEE · Yong-Kyu KIM

Abstract In this paper, we suggest the criticality of Hidden Failure with regard to the design of watch dog timer, used to detect HALT on railway signaling embedded controller, via FMEA and FTA. Hidden Failure means reliability and safety degradation of the system due to any failure occurred on elements added for fault tolerance. In this paper, therefore, we design vital watch dog timer to prevent the system from operating in low SIL conditions and assess the safety of circuit on failure occurrence to demonstrate that safety degradation problems owing to existing design are supplemented.

Keywords : Embedded Controller, Watch-Dog Timer, Vital, Safety, SIL (Safety Integrity Level)

요 지 본 논문은 철도신호 내장형제어기의 정지결함검출을 위해 적용되는 워치독타이머 설계와 관련하여 FMEA와 FTA를 통해 타이머 결함발생을 시스템이 인식하지 못하는 은폐고장(Hidden Failure)의 심각성을 제시한다. 은폐고장은 결함허용을 목적으로 추가된 소자의 결함발생으로 인한 시스템의 신뢰성 및 안전성의 저하이다. 이러한 은폐고장으로 인해 안전무결성레벨이 저하된 상태로 시스템이 운용되는 것을 방지하기 위해 본 논문에서는 바이탈워치독타이머를 설계하고, 결함발생에 대한 회로의 안전성을 평가하여 기존 설계로 인한 안전성저하 문제가 보완되었음을 입증한다.

주 요 어 : 내장형제어기, 워치독타이머, 바이탈, 안전성, 안전무결성레벨

1. 서 론

내장형제어기를 사용하여 열차의 진로와 간격을 제어하는 철도신호시스템은 우발고장(Random Failure)패턴을 갖는 내장형제어기의 신뢰성 및 안전성향상을 위해 결함허용(Fault Tolerance)구조를 사용한다. 결함허용구조는 여분(Redundancy)을 사용하여 발생된 결함이 오류 또는 고장으로 확산되지 않도록 결함을 검출, 차단, 재구성하여 허용한다[1].

내장형제어기의 주요 구성요소는 프로세서, 메모리, 직렬입출력회로, 병렬입출력회로, 버스제어기, 타이머, 리셋회로, 소자선택신호의 생성을 위한 어드레스 디코더 등이 있다. 따라서 내장형제어기의 결함허용을 위해서는 위와 같은 주요 구성요소의 결함을 실시간으로 검출하여 억제 또는 재구성을 통해 허용해야 한다.

내장형제어기의 능동결함허용을 위해서는 자기검사회로 또는 비교회로를 사용하여 동일입력에 대한 출력신호의 불일치를 결함발생으로 판단하는 원리가 사용된다[2].

워치독타이머는 내장형제어기의 마이크로프로세서 또는 마이크로컨트롤러의 정지(Halt)고장을 검출하기 위해 널리 사용되는 설계기법으로써, 본 논문에서는 기존에 사용되던 일반적인 구조의 워치독타이머를 제시하고, 마이크로프로세서 정지고장에 대한 위험측고장의 발생빈도를 고장모드영향분석(FMEA, Failure Mode Effect Analysis)과 결함트리분석(FTA, Fault Tree Analysis)을 사용하여 정량적으로 평가한다.

시간당발생빈도로 평가되는 위험측고장은 안전무결성레벨(SIL, Safety Integrity Level)로 평가할 수 있으며, 제어기가 사용되는 응용분야의 SIL요구사항보다 위험측고장률이 높은 발생빈도로 평가되면 안전이 확보되지 않은 것으로 판

† 책임저자 : 회원, 한국철도기술연구원, 전기신호연구본부 선임연구원
E-mail : ducko@krri.re.kr
TEL : (031)460-5442 FAX : (031)460-5449
* 회원, 한국철도기술연구원, 전기신호연구본부 주임연구원
** 회원, 한국철도기술연구원, 전기신호연구본부 책임연구원

단하여 추가적인 안전대책을 적용하여 발생빈도를 완화시킨다[3]. 예를 들어 철도신호의 대표적 안전설비인 전자연동장치의 내장형제어기는 역구내 궤도별 궤도계전기 상태를 입력받아 열차위치에 따른 진로쇄정 및 해정취급을 하며, 선로전환기 및 신호기를 제어하여 열차의 진로를 제어한다[4]. 따라서 연동장치의 위험측고장은 열차의 충돌 및 탈선을 발생시킬 수 있다.

본 논문에서는 이러한 안전필수(Safety Critical)분야 제어기의 정지결함검출을 위한 워치독타이머의 안전성평가를 통해 위험원을 도출하고 안전확보를 위한 대책을 제시한다.

2. 일반적인 워치독타이머 제시

워치독타이머는 마이크로프로세서의 구동클럭과 독립된 클럭생성기인 오실레이터 또는 크리스탈을 사용하여 그림 1과 같이 구성한다.

워치독타이머를 이용한 마이크로프로세서 정지결함검출의 원리는 다음과 같다. 마이크로컨트롤러가 워치독카운터의 값을 초기값으로 설정하면 워치독타이머의 클럭발생기에 의해 카운터값은 자동으로 증가하여 최대값에 도달하면 워치독신호를 발생한다.

따라서 마이크로컨트롤러는 워치독카운터가 최대값에 도달하기 전에 타이머값을 주기적으로 초기화시켜 워치독신호가 발생하지 않도록 억제한다. 워치독카운터가 최대값에 도달하여 워치독신호가 발생하면 마이크로컨트롤러는 정지상태고장이 발생한 것이므로 이때 워치독신호를 사용하여 마이크로컨트롤러의 가용성 향상을 위해 재시작 시키거나 안전성 확보를 위해 결함이 발생한 모듈을 차단하고 대기계로 제어권을 절체시킨다[5].

워치독카운터의 값이 자동으로 상승하도록 구현하는 위와 같은 설계가 업카운트(Up-count) 워치독타이머이며, 카운터 값이 자동으로 감소하도록 구현하는 반대의 개념이 다운카운트(Down-count) 워치독타이머로써 모두 동일한 동작원리를 갖는다.

그림 1의 워치독타이머를 포함한 제어기능에서 제시한

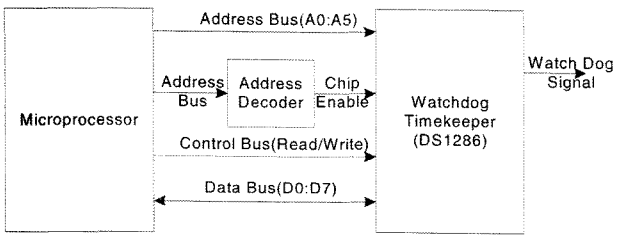

Fig. 1. General Structure of Watch-Dog Timer

DS1286 Watchdog Timekeeper는 코레일 차상신호(ATP)시스템인 Bombardier Transportation의 Ebicab시리즈와 한국형 고속철도 차상ATC 및 분산형전자연동장치에 사용하는 코어인 모터롤라 CISC(Complex instruction set computer)칩과 주로 호환된다.

본 논문에서 예로 제시한 DS1286은 4비트의 데이터를 설정레지스터에 따라 1초, 1/10초, 1/100초, 1/1000초 단위로 다운카운트하는 워치독타이머이다[5]. 그림 2에서 워치독내부의 클럭(Watch Dog Clock)의 발진에 의해 워치독내부 타이머레지스터(Watch Dog Internal Register)의 값은 감소한다. 예를 들어 1/10초의 다운카운트 워치독으로 DS1286의 내부레지스터를 설정하면, 그림 2에서 DS1286의 선택신호(/CE)와 쓰기신호(R/~W)가 활성화 되는 순간에 마이크로프로세서가 데이터버스에 데이터(0x04)를 쓰면, DS1286은 0.1초 간격으로 내부워치독 레지스터의 값을 1씩 감소시킨다.

워치독 내부카운터의 값이 0x00이 되면 워치독신호가 발생하므로 그림 1과 같이 설계하는 경우에는 워치독 내부카운터를 0x04로 설정한 후 0.4초 이전에 다시 워치독 내부카운터에 0x04를 써주어야만 워치독카운터는 워치독신호를 발생하지 않는다. 이러한 원리에 의해 프로세서에서 정지결함이 발생하면 그림 1의 DS1286 워치독신호가 발생하여 프로세서를 차단시키는 신호원으로 사용하게 된다.

3. 워치독타이머 안전성평가 및 바이탈워치독 설계

3.1 워치독타이머의 안전성평가

철도신호의 내장형제어기를 설계하는 경우 워치독타이머를 기본으로 설계에 포함시킨다. 하지만 워치독타이머 사용의 결정은 내장형제어기의 임무실패의 전체적인 확률인 신뢰성과 제어기 위험측고장에 대한 확률인 안전성의 요구사항을 분석하여 포함여부를 판단하는 것이 적절하다[6].

안전성의 평가를 위해서는 제어기의 임무에 대한 가정이 필요하다. 본 논문에서는 제어기의 위험측고장으로 인한 사

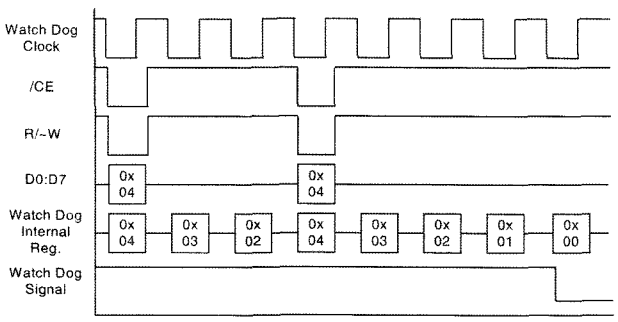

Fig. 2. Timing Chart for Watch-Dog Timer

고가 열차충돌에 해당하는 응용분야인 전자연동장치의 위험원중 하나인 "열차점유궤도의 비점유판단"을 제어기의 위험원으로 가정한다.

우리나라 철도사고 중 중대사고에 해당하는 열차충돌의 결과는 3인 이상의 사망에 해당하므로 해당 위험원의 위험도(Risk)를 구성하는 심각도는 치명적(Catastrophic)에 해당한다[7]. 따라서 이러한 위험원을 안전하게 제어하기 위해서는 안전대책이 포함된 제어기의 위험측고장발생빈도를 최고수준으로 억제한 SIL4를 적용한다[6].

표 1의 궤도회로입력기능에 대한 FMEA결과 "열차위치의 위험측인식" 위험원의 발생빈도는 안전대책 적용 후를 기준으로 그림 3과 같이 FTA를 통해 평가된다. 그림 3의 각 이벤트 고장발생빈도는 통상적인 가정치를 적용하였다. 단 위험원의 원인 중 "마이크로프로세서 연산오류"의 안전대책은 소프트웨어의 정량적고장률평가가 어려우므로 IEC 62279에서 적용하는 SWSIL4의[8] 체계를 준수한 것으로 가정하여 고장률을 "0"으로 할당하여 그림 3의 FTA에서 제외하였다.

그림 3에서 워치독타이머가 없다면 "Gate 101"의 고장률은 10^{-6}/hour가 되고, "Top Event 100"의 고장률도 10^{-6}/hour가 되어 SIL4의 기준인 10^{-8}/hour 미만을 만족하지 못하게 된다. 따라서 해당 위험원을 안전하게 제어하기 위해서는 워치독타이머를 사용하지 않는 경우에 마이크로프로세서의 고장률이 0.9×10^{-8}/hour미만이어야 한다.

하지만 현재 철도신호에 적용되고 있는 마이크로프로세서는 국방기준의 제품이라도 위의 기준을 만족하기 어려우므로 워치독타이머를 추가하여 안전성을 확보하고 있다.

그림 1과 같은 일반설계에서 워치독타이머는 프로세서의 정지결함을 검출하기 위한 결함검출회로이며, 그림 3과 같이 워치독타이머의 정상동작을 가정하여 위험측고장률의 발생빈도를 SIL4로 확보하였다.

하지만 그림 1과 같은 일반설계에서 워치독타이머의 고장은 프로세서가 인지할 수 없다. 이러한 현상은 결함검출을 목적으로 설계하는 회로에서 흔히 발생되는 설계상의 문제점으로 검출대상의 결함만을 고려하여 검출회로의 결함에 의한 영향을 누락시킨 결과이다.

만약 워치독타이머 DS1286의 내부 클럭결함으로 인해 클럭이 발생하지 않으면 그림 4와 같이 워치독타이머는 주기적인 프로세서의 워치독레지스터의 갱신이 없어도 워치독신호를 발생하지 않는다. 이러한 워치독타이머의 결함은 그림 1과 같은 일반구조에서는 마이크로프로세서가 결함을 인지하지 못하여 그림 3의 Top-Event의 발생빈도가 10^{-6}/hour인 상태로 유지된다.

그림 4는 워치독타이머 내부결함이 발생한 상태에서 마이크로프로세서의 정지결함이 발생하면 정지결함의 검출이 되지 않는 경우의 타이밍도이며 이러한 정지결함의 검출실패로 인해 사고의 원인이 되는 위험원의 발생빈도가 높아진다. 그림 5는 워치독타이머 내부결함이 발생한 후 제어기는 인식하지 못하지만 이때의 위험원 발생빈도가 SIL4를 만족하지 못하는 상황을 표현한 그림이다.

따라서 워치독타이머의 결함이 제어기로 보고되지 않는 설계가 차상제어장치 또는 전자연동장치에 적용되면 열차충돌

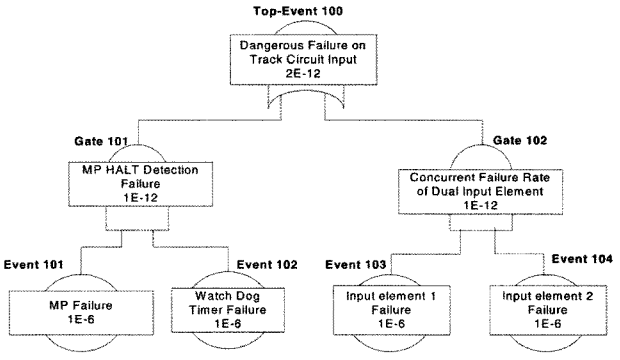

Fig. 3. Dangerous Failure Frequency FTA for Track Circuit Input

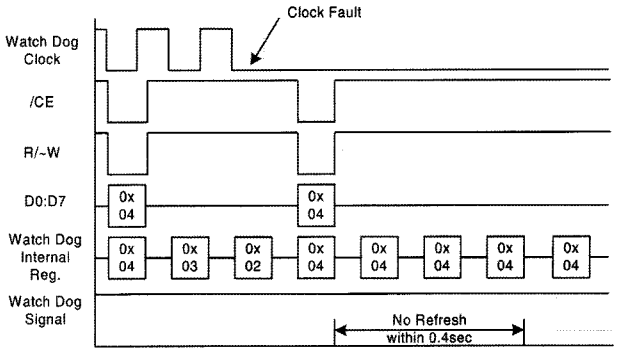

Fig. 4. Timing Chart for Fault Detected Watch-Dog Timer

Table 1. FMEA for the track circuit input

Function	Failure Mode	Cause	Safety Measure	Frequency	Results
Track Circuit Input	Dangerous Identification (Identify occupied state as unoccupied)	1.Track Relay Input Element Failure 2.MP Operation Error 3.MP HALT	1.Duplicate Input Element 2.S/W Verification (Applying SWSIL4) 3.HALT Detection Using Watch Dog Timer	10^{-12} /hour	Controller Fail-Safe Operation

및 탈선에 대한 위험측발생빈도가 안전의 허용수준을 만족하지 못하게 되었음에도 아무 조치 없이 장치를 운영하게 되어 이때 위험측고장이 발생하면 아무 대책 없이 사고가 발생하게 된다.

3.2 바이탈워치독 타이머 설계

본 논문에서 분석한 워치독타이머 클럭결함에 대한 위험측 고장 발생빈도 저하문제는 다양한 방법으로 해결이 가능하다. 가장 쉬운 방법은 마이크로프로세서가 그림 6과 같이 워치독 타이머의 레지스터를 세팅한 후에 그 값이 변화하는지를 주기적으로 점검하는 소프트웨어적인 해결방법이 있다.

그림 6에서와 같이 마이크로프로세서의 소프트웨어에 워치독타이머의 주기적 레지스터 세팅을 0x04로 한 후 0.2sec 후에 그림 6의 명암처리된 0x02와 같이 타이머값의 변화를 모니터링 하는 방법이다. 하지만 이러한 소프트웨어 결함검출은 다음과 같은 단점이 있다.

- 추가된 워치독타이머 감시프로시저에 의해 프로그램 처리성능이 저하된다.
- 소프트웨어에 의한 감시프로시저는 정량적인 실패율 계산이 불가능하다.

따라서 본 논문에서는 그림 7과 같은 하드웨어방식의 워치독타이머 결함검출회로를 제안한다.

그림 7은 그림 1에 DS1286의 타이머클럭 출력신호인 "Square Wave Output"신호를 이용하여 워치독타이머의 클럭결함을 검출한다. 만약 워치독타이머 클럭결함이 발생하면 DS1232 "Micro Monitor Chip"에서 클럭결함검출신호가 발생하여 기존의 워치독신호의 발생과 조합하여 제어기를 차단하도록 구성하였다. 그림 8은 바이탈워치독타이머의 동작타이밍도이다.

바이탈워치독타이머는 워치독타이머 내부클럭이 정지하면 DS1232가 "Clock Fault Signal"을 발생하여 "Vital Watch Dog Signal"을 발생한다. 워치독타이머 내부클럭이 정상일 경우에 마이크로프로세서 정지결함이 발생하면 DS1286의 "Watch Dog Signal"이 발생하여 "Vital Watch Dog Signal"을 발생시킨다.

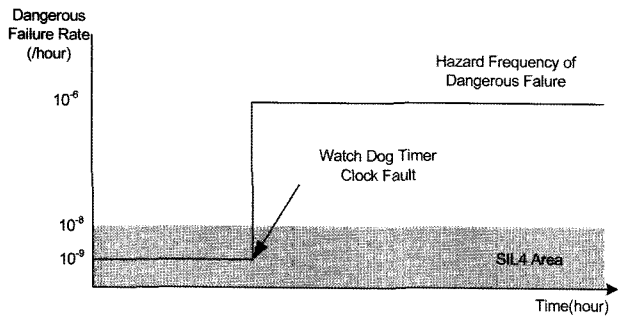

Fig. 5. Timing Chart for Fault Detected Watch-Dog Timer

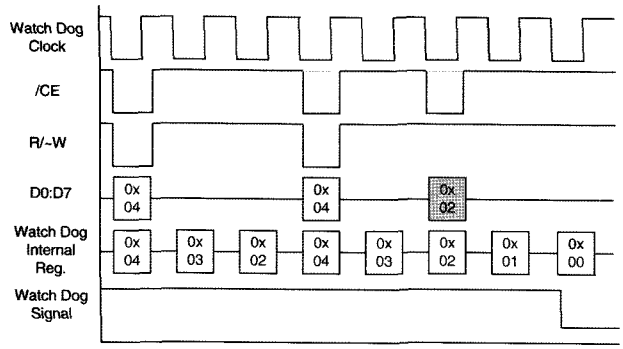

Fig. 6. Watch-Dog Timer Inspection Timing Chart via S/W

3.3 바이탈워치독타이머를 포함한 제어기의 안전성평가

워치독타이머의 클럭결함을 검출하여 제어기를 안전측으로 차단시키는 바이탈워치독타이머의 안전성은 제어기와 워치독타이머가 모두 정상인 상태에서는 그림 3의 FTA결과와 동일하게 SIL4를 만족하며, 워치독타이머 내부결함이 보고되지 않아 제어기가 안전하지 않은 상태에서 동작하는 그림 5와 같은 상태는 그림 9와 같이 결함발생즉시 검출 및 제어기의 차단이 실행되어 안전성을 확보할 수 있다.

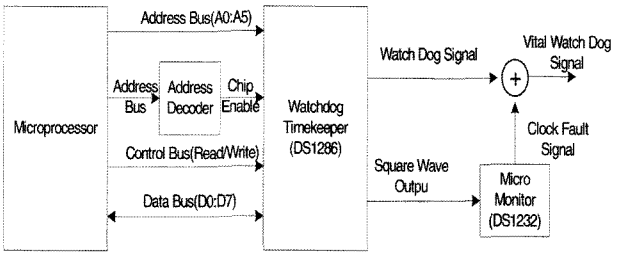

Fig. 7. Vital Watch-Dog Timer Composition Chart

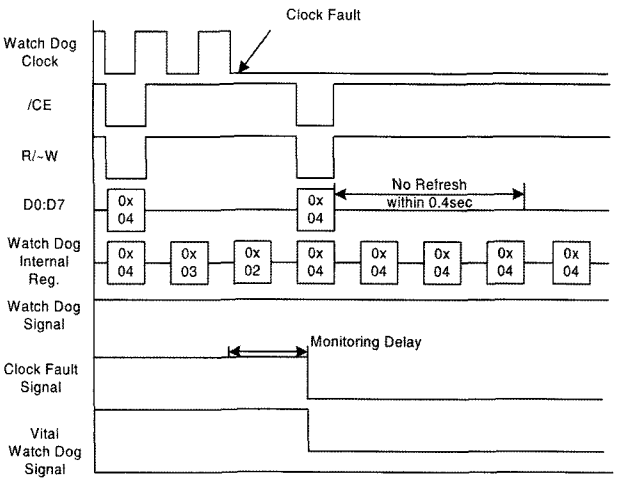

Fig. 8. Movement Timing Chart for Vital Watch-Dog Timer

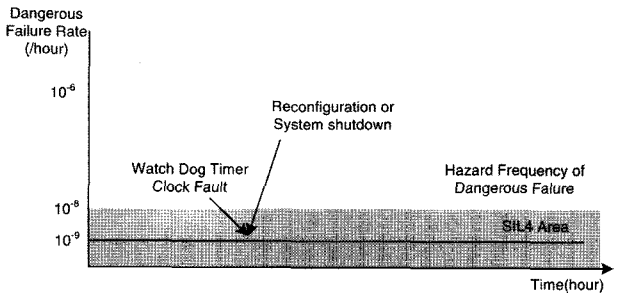

Fig. 9. Timing Chart for Fault Detected Vital Watch-Dog Timer

4. 결 론

본 논문은 내장형제어기의 정지결함을 검출하기 위한 기존의 워치독타이머 회로를 제시하고 FMEA와 FTA를 통해 워치독타이머 회로가 내장된 제어기의 정지결함 검지불능과 관련된 위험원을 정량적으로 평가하여 SIL4를 만족함을 보였다. 또한 이러한 기존구성이 갖는 위험원인 워치독타이머 클럭결함 발생에 대한 제어기의 결함검출 실패를 도출하여 안전이 확보되지 않은 상태로 시스템이 운용될 수 있음을 입증하였다.

이러한 워치독타이머의 클럭결함 검출을 위해 별도의 회로를 추가하여 결함발생시 제어기를 안전측으로 차단하는 바이탈워치독타이머 회로를 제안하고, 제안된 회로의 워치독타이머 클럭결함에 대한 타이밍분석을 통해 제어기 또는 워치독타이머의 결함 발생시에도 제어기가 SIL4로 유지됨을 입증하였다.

위와 같은 문제의 심각성은 시스템의 안전성을 고려하는 모든 분야에서 이슈가 되고 있으며, RCM II의 경우에는 이러한 결함검출, 회피, 억제 등을 목적으로 추가된 회로의 결함을 Hidden Failure로 정의하여 추가회로의 정상동작을 보증하기 위한 유지보수활동의 임무를 별도로 할당하고 있다[9]. 따라서 본 논문에서와 같이 제어기의 결함뿐만 아니라 결함허용을 위해 추가된 기능과 관련 없는 회로의 결함도 안전성활동에 반드시 반영되어야 한다.

참 고 문 헌

1. Dhiraj K. Pradhan (1996), "Fault-Tolerant computer system Design", Prentice Hall. pp.6-10.
2. Barry W. Johnson (1989), "Design and Analysis of Fault-Tolerant Digital Systems". pp.62-69.
3. IEC 61508 (1998), "Functional Safety of electrical/electronic/programmable electronic safety-related systems, Part1: General requirements", pp.65.
4. 김영태(2006), "철도신호제어시스템(개정4판)", pp.362-379.
5. Dallas Semiconductor(1997), "DS1286 Watchdog Timekeeper", pp.5-6.
6. 신덕호 외, 한국철도학회(2006), "열차제어시스템의 안전입증에 관한 연구", 제9권 제4호, pp.412-418.
7. 대통령령 제18933호(2005), "철도안전법 시행령, 제57조(건설교통부장관에게 즉시 보고하여야 하는 철도사고 등)".
8. IEC 62279 (2002), "Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems", pp.102-121.
9. John Moubray (1997), "Reliability Centerd Maintenance II", pp.111-128.

(2007년 9월 20일 논문접수, 2007년 11월 20일 심사완료)