한국철도학회논문집
제14권 제5호(2011년 10월) | pp. 416-424

열차제어를 위한 USN Gateway 신뢰성, 안전성 평가 및 향상에 관한 연구

A Study on the Reliability/Safety assessment and improvement of USN Gateway for Train Control

신덕호† · 조현정[1] · 신경호[1] · 송용수[2]
Ducko Sin · Hyunjeong Jo · Kyengho Shin · Yongsoo Song

Abstract The recent development of USN (Ubiquitous Sensor Network) technology has broadened its applications to many fields of industry. The USN technology enables the system to monitor and control the status of distributed sensor nodes based on the low-powered communications. Applying the USN in the train control domain, the operational efficiency can be enhanced, where the reliability and the safety of the system are the key challenges. This paper suggests the system design for evaluating and improving the reliability and safety of the gateway, which is a USN component that manages the radio network among the sensors and collects the information from them. For this purpose, the reliability and the level of safety integrity of a general gateway have been predicted quantitatively and the supplementary design has been proposed for the selected week points. The verification on the reliability and the safety of the improved gateway according to the related standards has been followed. With the results of the study, the applicability of USN gateway for train control systems has been reviewed.

Keywords : USN, Gateway, Reliability, Safety, SIL, FMEA, FTA

초 록 본 논문에서는 소출력 무선통신기술을 기반으로 분산 배치된 센서노드의 상태를 감시하고 제어를 수행하는 USN(Ubiquitous Sensor Network)시스템을 철도의 열차제어에 활용하기 위한 신뢰도 모델링결과를 제시한다. 일반적인 USN시스템은 센서노드, 게이트웨이, 서버로 구분할 수 있으며, 본 논문에서는 USN의 구성요소 중 다수의 센서노드간 무선망을 관리하고 정보를 취합하는 게이트웨이를 대상으로 신뢰성 및 안전성을 평가하고 향상시키기 위한 설계방안을 연구하였다. 이를 위해 일반적으로 사용되는 게이트웨이의 신뢰도와 안전무결성수준을 정량적으로 예측하고, 취약부분을 선별한 후 보완설계를 실시하여 향상된 게이트웨이의 신뢰성 및 안전성을 관련 규격에 따라 입증함으로써 열차제어에 대한 USN 게이트웨이 적용 가능성을 검토하였다.

주요어 : USN, 게이트웨이, 신뢰성, 안전성, 안전무결성레벨, 고장모드영향분석, 결함트리분석

1. 서 론

국내 IT기술의 발달로 인해 유비쿼터스 센서 네트워크(USN, Ubiquitous Sensor Network)기술은 사회전반에 적용이 확산되고 있다. 소출력 무선통신기반의 USN시스템을 이용하여 고속의 정보수집 및 분석에 의한 제어가 가능해짐에 따라 철도를 포함한 교통전반에도 과거 인력에 의존하던 많은 업무들이 USN시스템 도입을 통해 운영효율 향상을 추구하고 있다.

하지만 철도, 원자력발전소, 국방, 항공우주, 화학플랜트와 같이 제어기의 위험측고장(Dangerous Failure)으로 인한 사고결과가 인명 및 대규모 재산손실의 원인이 되는 안전필수(Safety Critical)분야에 USN시스템을 적용하기 위해서는 제어기의 신뢰성 및 안전성이 정량적으로 평가되어 운영조건에 따라 결정된 허용위험도 수준 이하로 모든 위험원의 위험도가 저감되어야 한다[1]. 하지만 현재 철도분야에서는 신뢰성 및 안전성 정량화에 대한 개발기관의 경험부족으로 인해 USN시스템이 단순 진단 및 유지보수업무 지원 등의 안전무관(Safety Not Related) 분야에서만 우선 적용되고 있다.

따라서 본 논문에서는 Fig. 1과 같이 센서노드, 게이트웨이, 서버로 구성되는 USN시스템의 구성요소 중 센서노드의 무선통신망을 관리하고, 센서노드로부터 수집된 정보를 상위 서버로 전송하며, 서버로부터의 제어명령을 센서노드로 전송하는 USN 게이트웨이를 대상으로 신뢰성 및 안전성의 정량화적 평가와 이를 향상시키기 위한 방안을 연구한다.

이러한 연구를 통해 최근 도시철도의 운영효율 향상 및 일반철도와 고속철도의 유지보수비용 절감을 목적으로 도입 중이거나, 연구개발이 진행되고 있는 무선기반 열차제어에 적용 가능한 게이트웨이를 설계하고 정량적 신뢰성 및 안전성

†교신저자 : 한국철도기술연구원 지능형도시철도제어연구실
E-mail : ducko@krri.re.kr
[1]한국철도기술연구원 지능형도시철도제어연구실
[2]한국철도기술연구원 무선통신열차제어연구단

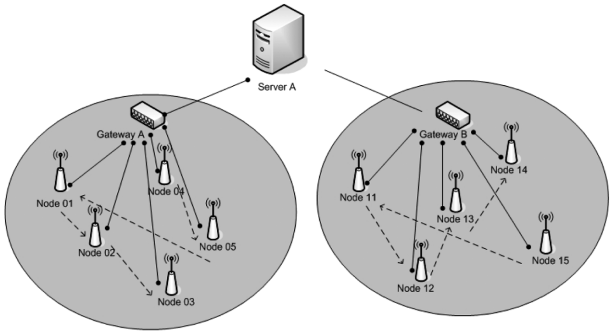

Fig. 1 Concept Diagram of Ubiquitous Sensor Network

평가를 통해 관련국제표준인 IEC 61508의 요건만족을 입증하였다.

2. 본 론

2.1 열차제어를 위한 USN Gateway의 요건분석

2.1.1 신뢰성 및 안전성의 정량화

신뢰성은 주어진 시간 동안 기대된 기능을 수행할 확률이며, 안전성은 모든 위험원(Hazard)의 위험도(Risk)가 허용할 수 있는 수준으로 제어된 상태를 의미한다[2]. 따라서 철도, 원자력, 산업플랜트와 같이 제어기 기능의 안전확보가 요구되는 분야에서는 이러한 정성적 특성의 만족여부를 확인하기 위해 신뢰성과 안전성을 정량화하여 목표를 수립하고, 만족여부를 입증하도록 강제하고 있으며, 이러한 절차를 국제표준 IEC 61508(전기/전자/프로그래머블제어기의 기능안전)에 명시하고 있다. 특히 안전성에 대해서는 사고의 원인이 되는 위험측고장에 대하여 사양의 오류, 개발자실수 등의 시스템적고장(Systemically Failure)과 전자부품 고유의 우발고장(Random Hardware Failure)으로 구분하고 있으며, 시스템적고장 평가 및 억제를 위한 조직구성, 문서화기준, 입증자료의 평가 등에 대한 요건을 규격에 명시하고 있다[3]. 또한 우발고장에 대해서는 고장영향 분석 및 평가를 통해 위험원을 도출하고, 각각의 위험도를 평가하여 안전성을 확보하기 위한 절차가 규격에 제시된다[4].

2.1.2 정량적 신뢰성 및 안전성목표 제시

안전필수분야에서는 신뢰성과 안전성목표의 정량화가 필수요건이다. 신뢰성에 대해서는 평균고장시간(MTBF, Mean Time Between Failure) 및 평균서비스고장시간(MTBSF, Mean Time Between Service Failure)을 사용하여 장치의 수명에 대한 기대수준을 요구한다. MTBF는 장치의 약 67%가 생존하는 평균시간이며, 안전필수분야에서는 MTBF를 장치의 교체주기 결정에 활용하고 있다. 마찬가지로 MTBSF는 서비스불능상태를 일으키는 장치고장에 대한 평균시간으로써, MTBF와 MTBSF는 고장 및 서비스고장의 정의에 따라 구분된다.

현재 철도분야 특히 열차제어에 적용되는 고장은 기능요구사항에 제시된 기능유지의 실패로 정의하며, 서비스고장은 코레일 운전규정의 여객열차 운행지연의 정의를 적용하여 10분이상의 열차운행에 지장을 발생시키는 고장으로 적용하고 있다[5].

안전성목표는 위험도의 허용수준을 매트릭스 형태로 제시하여 모든 위험원의 위험도가 허용수준으로 제어됨을 입증하는 위험도매트릭스(Risk Matrix)방식과 안전대책의 도입 및 유지에 소요되는 비용과 그로 인한 위험도 억제효과의 편익(Benefit)을 계산하는 합리적수준의 위험도제어(ALARP, As Low As Reasonably Practicable) 방식이 사용되고 있다. 하지만 위험도매트릭스와 ALARP방식을 적용하기 위해서는 위험원의 발생빈도와 별도로 발생된 위험원으로 인한 심각도(피해정도)의 정량화가 필요함으로, 운영시나리오의 정의가 선행되어야 한다. 따라서 운영시나리오가 결정되지 않은 범용 장치에 대해서는 안전무결성레벨(SIL, Safety Integrity Level)을 적용하고 있다[6,7].

4등급으로 구분되는 SIL의 평가체계는 IEC 61508에 정의되며 각각의 SIL목표에 따라 Table 1의 요건을 모두 만족하도록 강제하고 있다.

하드웨어 우발고장에 대한 SIL별 허용기준은 SIL평가 기능의 사용빈도가 1회/1년을 기준으로 이하인 경우 저빈도운영모드(Low demand mode of operation)를 적용하고, 초과인 경우 고빈도운영모드(High demand or continuous mode of operation)으로 구분한다. 저빈도운영모드의 경우 SIL별 기능요구에 대한 실패율을 횟수 단위로 제시하며, 고빈도운영모드의 경우 단위시간당 위험측고장의 발생빈도를 SIL별로 제시하고 있다[8].

따라서 본 논문에서는 USN 게이트웨이에 대한 신뢰성과

Table 1 SIL requirement of IEC 61508

No	Requirement	Contents of Requirement
1	Management of Functional Safety	- Random Hardware Failure - Software Functional Safety(IEC 61508 Part3) - Hardware Architectural Constraints
2	Technical Requirements	- Functional Test - Environment Test - Operating Test
3	Competence of Persons	- Personal Information - Evidence of Competence
4	Functional Safety Assessment(FSA)	- Functional Safety Review - Evidence of Independence

Table 2 Reliability and safety target of the USN gateway

Category	Quantitative Requirement	Define of Failure
Reliability	MTBF 60,000 over	Failure of required function
Safety	SIL2($\geq 10^{-7}$/h to $< 10^{-6}$/h)	Probability of dangerous failure per hour

안전성의 목표를 Table 2와 같이 가정하여 목표달성을 위한 신뢰성과 안전성설계를 수행하였다. 또한 신뢰성과 안전성의 평가를 위해 필요한 고장 및 위험측고장의 정의는 각각 USN 게이트웨이에 기대된 기능실패와 예측할 수 없는 결과의 발생으로 정의하였다.

2.2 USN Gateway의 신뢰성 및 안전성 향상

Table 2에서 설정된 신뢰성과 안전성의 정량적 목표를 만족하기 위하여 일반 USN시스템 응용분야에 사용되고 있는 게이트웨이의 고장률을 예측하고 안전필수분야인 열차제어에 대한 적용가능성을 평가하였다.

USN 게이트웨이의 열차제어분야 적용을 위해서는 정량적인 신뢰성과 안전성의 평가가 요구된다. 따라서 본 논문에서는 게이트웨이의 MTBF와 SIL을 평가하여 열차제어분야 적용을 전제로 가정한 Table 2의 정량적 목표 만족여부를 평가하였으며, 목표만족을 위한 설계보완 및 재평가를 통해 안전필수분야에 활용이 가능한 USN 게이트웨이를 설계하였다.

2.2.1 USN 게이트웨이의 신뢰성 정량화

신뢰성의 정량화는 예측(Prediction)과 입증(Demonstration)으로 구분할 수 있다. 예측은 관련표준을 근거로 산출하며, 입증은 적용환경에서 발생된 고장의 원인을 고장보고분석 및 정정시스템(FRACAS, Failure Report, Analysis and Corrective Action System)과 같이 정형화된 방법을 사용하여 신뢰성을 정량화 한다. 적용환경이 고정된 경우 입증치가 실제 장치의 고장률을 정확하게 평가할 수 있는 방법이지만, 이를 위해서는 장시간의 시스템고장정보 수집과 분석이 필요하므로, 개발과정에서는 관련 표준에 의한 예측을 통해 신뢰성을 정량적으로 평가하고 있다[9].

본 논문에서는 미국방지침인 MIL-HDBK-217FN2를 적용하여 상온의 지상설치환경에서의 기존 USN 게이트웨이 신뢰도를 예측하였다. 이를 위해서는 Table 3과 같이 USN 게이트웨이를 구성하는 부품의 고장정보(종류, 수량, 용량, 적용부하, 온도 등)를 사용하여 부품단위로 고장률을 산출하여, Fig. 2와 같이 하부 기능블럭 및 장치전체에 대한 신뢰도를 신뢰도블럭다이어그램(RBD, Reliability Block Diagram)을 통해 제시한다.

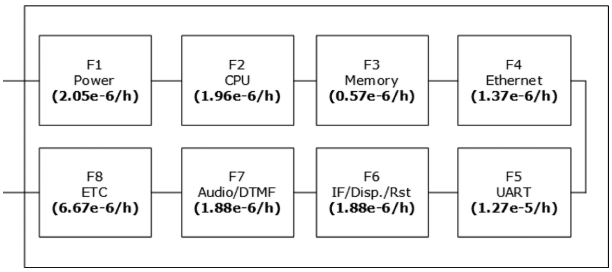

Fig. 2 RBC of the existing USN Gateway

8개의 기능블럭이 총 149개의 부품으로 구성된 기존 USN 게이트웨이의 고장률은 Fig. 2와 같이 2.91e-5/h로써 고장률의 역수로 근사되는 MTBF는 34,387시간(약 3.92년)으로 평가되었다. Fig. 2의 신뢰도블럭다이어그램(RBD, Reliability Block Diagram)은 USN 게이트웨이의 기능모듈단위 고장률을 해당 부품고장률의 합으로 표현하여, 게이트웨이 전체 고장률에서 차지하는 기능별 고장률의 비율을 표기함으로써, 게이트웨이 고장률 억제를 위해 기능별로 수행되어야 할 향상대책 수립을 용이하게 하기 위함이다.

즉, 기존 USN 게이트웨이의 MTBF 34,387시간은 Table 2에서 수립한 신뢰도목표인 60,000시간에 미달되는 수준이다. 예측신뢰도가 신뢰성목표에 미달되는 경우 부품의 고장률을 낮추어 목표를 만족하도록 설계를 개선해야 한다. 신뢰도 향상을 위한 가장 단순한 방법은 설계의 간소화, 부품의 품질향상(예를 들어 산업용 및 군용부품으로 대체) 등의 방법이 있으며, 하드웨어 다중화에 의한 신뢰도향상 방법도 적용이 가능하다. 본 논문에서는 MIL-HDBK-217FN2를 기준으로 입력된 부품별 스트레스 팩터에 의한 부품단위, 기능단위, 장치단위 정량적 고장예측을 위해 상용도구인 Relex를 사용하였다.

Table 3 Example of the components list of the existing USN gateway

No	Design No.	Component Name	Type	Quantity [EA]	Description
1	BT100	BATTERY		1	CR2032_BS-1
2	C702,C705,C706,C707,C708	Tantal Capacitor	Tantal"A"	5	0.1uF/33V
3	C709,C701	Tantal Capacitor	Can Tpye	1	220uF/6.3V
4	C100,C101,C103,C104,C105	Chip Capacitor	2012	5	4.7uF(2012)/25V
5	C102,C802,C804	Chip Capacitor	1608	3	1nF/50V
6	C106	Chip Capacitor	3216	1	33uF(3216)
8	C108,C114,C500,C605,C617, C623,C628,C629,C630, C700, C704,C710,C712,C803,C916	Chip Capacitor	2012	15	10uF/16V
9	C110	Chip Capacitor	1608	1	6pF/50V
10	C111	Chip Capacitor	1608	1	480pF/50V
11	C112,C113,C203,C204,C624, C625,C908,C911,C936,C937	Chip Capacitor	1608	10	18pF/50V

2.2.2 게이트웨이의 안전성 정량화

안전성정량화를 위해서는 본 논문의 2.1에서 언급한 바와 같이 USN 게이트웨이의 위험측고장을 발생시키는 고장모드를 FMEA를 통해 도출하여, 고장모드별 발생빈도를 신뢰성 평가를 통해 산출된 예측고장률을 바탕으로 평가한 후, 위험측고장률의 발생빈도를 결함트리분석(FTA, Fault Tree Analysis)을 사용하여 목표 SIL과 비교한다.

FMEA는 2.1에서 정의한 위험측고장 정의인 “예측할 수 없는 결과출력”을 대상으로 Table 4와 같이 8개 기능블럭 13개 세부기능별로 고장모드를 도출하였으며, 위험측고장의 원인이 되는 고장모드의 발생빈도를 정량적으로 평가하였다. 이때 고장모드별 고장률 정량화는 기능블럭의 고장률을 고장모드 원인부품의 고장률에 따라 비율로 나누어 가중치(Weight)를 할당하여 산출한다.

Table 4의 위험측고장관련 고장모드를 Fig. 3과 같이 FTA를 수행하면 USN 게이트웨이의 위험측고장 발생빈도가 산출된다. Fig. 3의 FTA는 Table 4의 결과가 위험측고장(Dangerous Failure)을 발생시키는 기능을 이벤트로 설정하여, 각각의 이벤트발생률에 따른 게이트웨이의 위험측고장 발생빈도를 산출하였다. FTA수행과 관련하여 Table 4의 고장모드별 발생률은 단위가 /h인 단위시간 기반의 고장률이며, Fig. 3의 FTA 이벤트는 불신뢰도(Q, Unreliability)인 단위가 없는 확률이다. 본 논문에서는 식(1)의 지수모델에 고장률과 동일하게 단위시간($t = 1$)을 적용하여 고장률과 불신뢰도간 변환을 사용하였다.

$$1 - Q = R = e^{-\lambda t} \tag{1}$$

FTA결과 USN 게이트웨이의 위험측고장발생빈도는 8.48e-6/h로써, SIL1으로 평가되었으며, Table 2에서 제시한 열차제어분야 적용을 위한 안전목표인 SIL2에 만족하지 못하는 것으로 평가되었다. 따라서 열차제어에 USN 게이트웨이를 도입하기 위해서는 향상설계가 수행되어야 한다.

USN 게이트웨이의 안전성 향상설계는 목표만족에 장애가 되는 설계요인을 파악하여 대책을 수립 및 적용해야 하며, 향상 설계가 반영된 게이트웨이의 신뢰성 및 안전성 재평가를 통해 목표 도달이 입증될 때까지 보완과 평가를 반복하여 수행한다.

Table 4 FMEA of the existing USN gateway

Function Block (Failure Rate[/h])	Function	FMCA Code	Failure Mode	Consequence (Gateway Level)	Weight (A)	Frequency[/h] (A X λ_{LRU})
Power 2.05e-6	Power Supplying	GW001	Inability to power supply	Failure with safe sate	0.2	4.10e-7
		GW002	Overvoltage supply	Dangerous Failure (Unpredictable)	0.1	**2.05e-7**
		GW003	Inadequate current supply	Dangerous Failure (Unpredictable)	0.2	**4.10e-7**
		GW004	Output short-circuit	Dangerous Failure (Unpredictable)	0.2	**4.10e-7**
		GW005	Input short-circuit	Dangerous Failure (Unpredictable)	0.3	**6.15e-7**
CPU 1.96e-6	Data Processing	GW006	Inability to transmit data	Failure with safe sate	0.4	7.84e-7
		GW007	Transmission of erroneous data (corrupted information, unwanted transmission, transmission of incomplete telegrams)	Dangerous Failure (Unpredictable)	0.2	**3.92e-7**
	Self Diagnostic	GW008	Diagnosis of failure information and failure handling thereof	Dangerous Failure (Unpredictable)	0.2	**3.92e-7**
		GW009	Handle erroneous failures under normal operation	Failure with safe sate	0.2	3.92e-07
Memory 5.71e-7	Storage of data processing	GW010	Inability to store information	Dangerous Failure (Unpredictable)	0.5	**2.86e-7**
		GW011	Errors of information storage (corruption of stored information, reading/writing incomplete data	Dangerous Failure (Unpredictable)	0.5	**2.86e-7**

Table 4 Continued

Function Block (Failure Rate[/h])	Function	FMCA Code	Failure Mode	Consequence (Gateway Level)	Weight (A)	Frequency[/h] (A X λ_{LRU})
Ethernet 1.37e-6	Receiving event/ command from high level	GW012	Inability to collect and transmit information	Failure with safe sate	0.5	6.85e-7
	Transmitting event/ command to high level	GW013	To collect and transmit erroneous data (corruption occurred when collecting and transmitting data, unwanted transmission, transmission of incomplete telegrams)	Dangerous Failure (Unpredictable)	0.5	**6.85e-7**
UART 1.27e-5	Providing debug port & Auxiliary interface	GW014	Inability to link with external devices	Unaffectedness	0.4	5.08e-6
		GW015	Transmission of erroneous data to external devices	Unaffectedness	0.5	6.35e-6
		GW016	Gateway Reset occurred due to the electrical defects in linking	Dangerous Failure (Unpredictable)	0.1	**1.27e-6**
IF/Display & Reset 1.88e-6	Interface with external device	GW017	Inability to link with external devices	Unaffectedness	0.3	5.64e-7
		GW018	Transmission of erroneous data to external devices	Unaffectedness	0.1	1.88e-7
		GW019	Gateway Reset occurred due to the electrical defects in linking	Dangerous Failure (Unpredictable)	0.1	**1.88e-7**
	Display	GW020	Inability to display operating conditions	Failure with safe sate	0.2	3.76e-7
		GW021	Display the errors of operating conditions	Failure with safe sate	0.1	1.88e-7
	Reset	GW022	Fail to reset, if required	Failure with safe sate	0.1	1.88e-7
		GW023	Unnecessary reset occurred	Failure with safe sate	0.1	1.88e-7
Audio/DTMF 1.88e-6	Audio	GW024	Unable to output audio signals	Unaffectedness	0.5	9.40e-7
		GW025	Unaware of keystrokes	Unaffectedness	0.5	9.40e-7
ETC 6.67e-6	Power Supplying (AC220V to 5V)	GW026	Inability to power supply	Failure with safe sate	0.1	6.67e-7
		GW027	Overvoltage Supply	Dangerous Failure (Unpredictable)	0.02	**1.33e-7**
		GW028	Inadequate current supply	Dangerous Failure (Unpredictable)	0.02	**1.33e-7**
		GW029	Output short-circuit	Dangerous Failure (Unpredictable)	0.03	**2.00e-7**
		GW030	Input short-circuit	Dangerous Failure (Unpredictable)	0.03	**2.00e-7**
	ZigBee Antenna	GW031	Inability to transmit and receive information	Failure with safe sate	0.4	2.67e-6
		GW032	Transmit and receive data errors	Dangerous Failure (Unpredictable)	0.4	**2.67e-6**

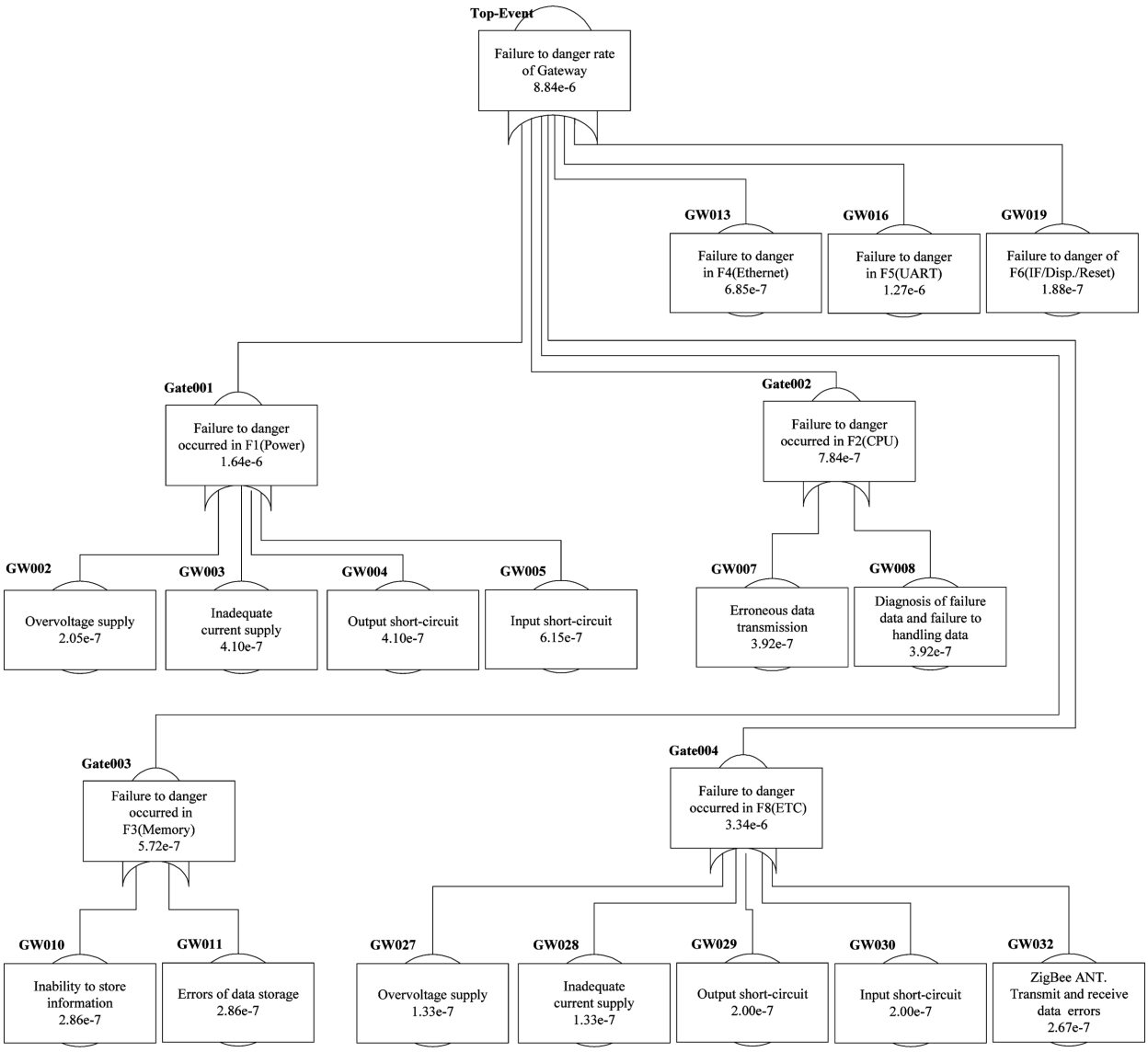

Fig. 3 Dangerous Failure FTA of the existing USN gateway

2.2.3 신뢰성 및 안전성 향상을 위한 설계보완

신뢰성 및 안전성 향상을 위해서는 각각의 평가결과에 대한 분석이 선행되어야 한다. 신뢰성은 모든 부품의 고장률에 종속되므로, 안전성 목표 만족을 위한 향상설계를 선행한다. Fig. 3의 Top-Event확률(Q) 8.84e-6을 SIL2수준인 1e-6/h미만으로 제어하기 위해서는 Gate001~004와 이벤트 GW013, 016, 019의 발생확률을 억제해야 한다. Fig. 3의 GW013, 016, 019외에 다른 이벤트의 발생확률을 억제하여 게이트웨이 위험측고장 발생빈도(Top-Event)를 억제할 수 있으나, Fig. 3의 FTA와 Fig. 2의 게이트웨이 RBD를 고려하여 보완대비 고장률을 가장 효과적으로 억제할 수 있는 기능블럭의 개선을 수행하였다.

따라서, 본 논문에서는 USN 게이트웨이의 기능블럭 중 전원(F1, F8), CPU(F2), Memory(F3), Reset(F6) 및 UART(F5)의 결함을 검출하여, 결함검출시 안전측으로 게이트웨이의 전원을 차단하는 Fig. 4의 결함검출 및 차단회로를 고장률이 1e-6/h로 설계하여 게이트웨이에 추가하였다.

Fig. 4의 결함검출 및 차단회로는 기존 게이트웨이의 주메모리와 중복된 주소를 갖도록 비교메모리를 내장하여, CPU가 데이터를 저장하는 경우 게이트웨이 주메모리와 비교메모리에 동일하게 기록된다. 기록된 정보를 CPU가 읽어 들일 때는 주메모리의 데이터만 데이터버스를 통해 전송되도록 버퍼를 구성하며, CPU의 데이터 읽기주기에 자동으로 Ex-OR게이트를 통해 주메모리와 결함검출 및 차단회로의 비교메모리정보가 하드웨어 적으로 비교된다. 만약 주메모리 또는 비교메모리에 결함이 발생하여 정보가 불일치 되면 결함검출 및 차단회로 내부에 내장된 회로차단기에 의해 게이트웨이 전체의 전원이 차단되도록 설계하여 게이트웨이가 예측하지 못하는 정보를 출력할 수 없도록 안전측(Fail Safe) 설계를 반영하였다. 마찬가지로 CPU의 Halt와 버스에러의

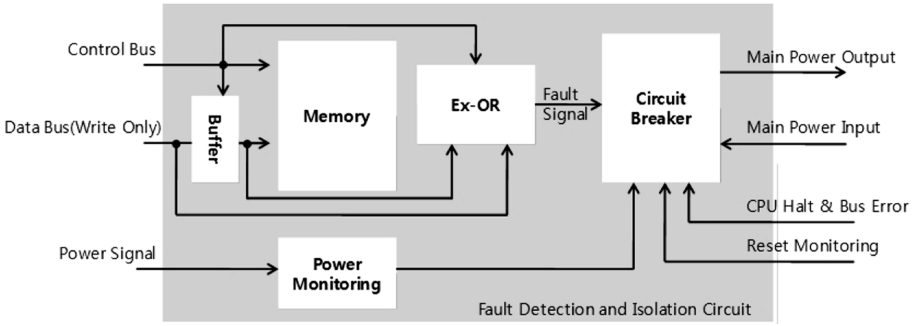

Fig. 4 Functional block diagram of fault detection and isolation circuit

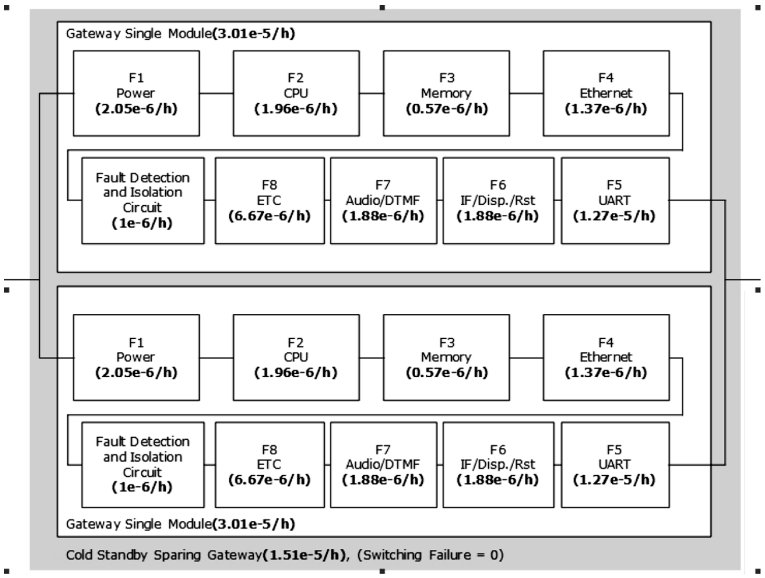

Fig. 5 RBD, which the Cold Standby Sparing implemented in the USN gateway embedding fault detection and isolation circuits.

발생, 의도하지 않은 Reset발생, 전원의 불량한 입력에 대해서도 결함검출 및 차단회로가 동작하여 위험측고장의 발생이 억제되도록 설계하였다[10].

2.2.4 설계보완된 USN Gateway의 신뢰성 및 안전성 평가

안전성목표의 만족을 위해 추가된 결함검출 및 차단회로의 고장률은 1e-6/h로써, 기존 게이트웨이의 고장률은 2.91e-5/h에서 3.01e-5/h로 증가하게 된다. 따라서 게이트웨이를 Cold Standby Sparing으로 구성하여 동작계 Gateway의 결함이 발생하여 차단되는 경우 대기계 Gateway가 동작을 수행하도록 하드웨어를 설계한다.

따라서, 단일계에 결함검출 및 차단회로가 추가하고, 단일계 게이트웨이를 이중(Cold Standby Sparing)으로 구성한 게이트웨이의 RBD는 Fig. 5와 같이 표현된다.

이때, Cold Standby Sparing의 신뢰도 산출은 미국 신뢰성센터(RAC, Reliability Analysis Center)의 신뢰도툴킷에서 제공하는 식(2)를 적용하였다[11].

$$\lambda_{Cold\ Standby} = \frac{1}{2}\lambda_{Single\ Module} \quad (2)$$

단일 게이트웨이에 결함검출 및 차단회로를 내장하여 CPU, 메모리, Reset, 전원공급, UART의 위험측고장을 안전측으로 차단하는 향상된 게이트웨이의 FTA를 Fig. 6과 같이 실시하여 전체장치의 위험측고장률이 9.52e-7/h로 제어됨을 입증하였다. Fig. 6의 게이트웨이 위험측고장 발생빈도 9.52e-7/h는 SIL을 정의하는 IEC 61508의 연속사용 응용환경(High-Demand Mode Application)에 대한 SIL2에 해당한다.

결함검출 및 차단회로를 내장한 USN 게이트웨이의 향상된 신뢰성과 안전성은 Table 5와 같이 Table 2에서 계획한 목표를 모두 만족함을 RBD와 FTA를 통해 입증하였다.

Table 5 Results of a quantitative evaluation of the USN Gateway, which reliability and safety have improved

	Failure Rate[/h]	MTBF[h]
Single Module	3.01e-5	33,223
Cold Standby Gateway	1.51e-5	66,445
Dangerous Failure	9.52e-7(SIL2)	N/A

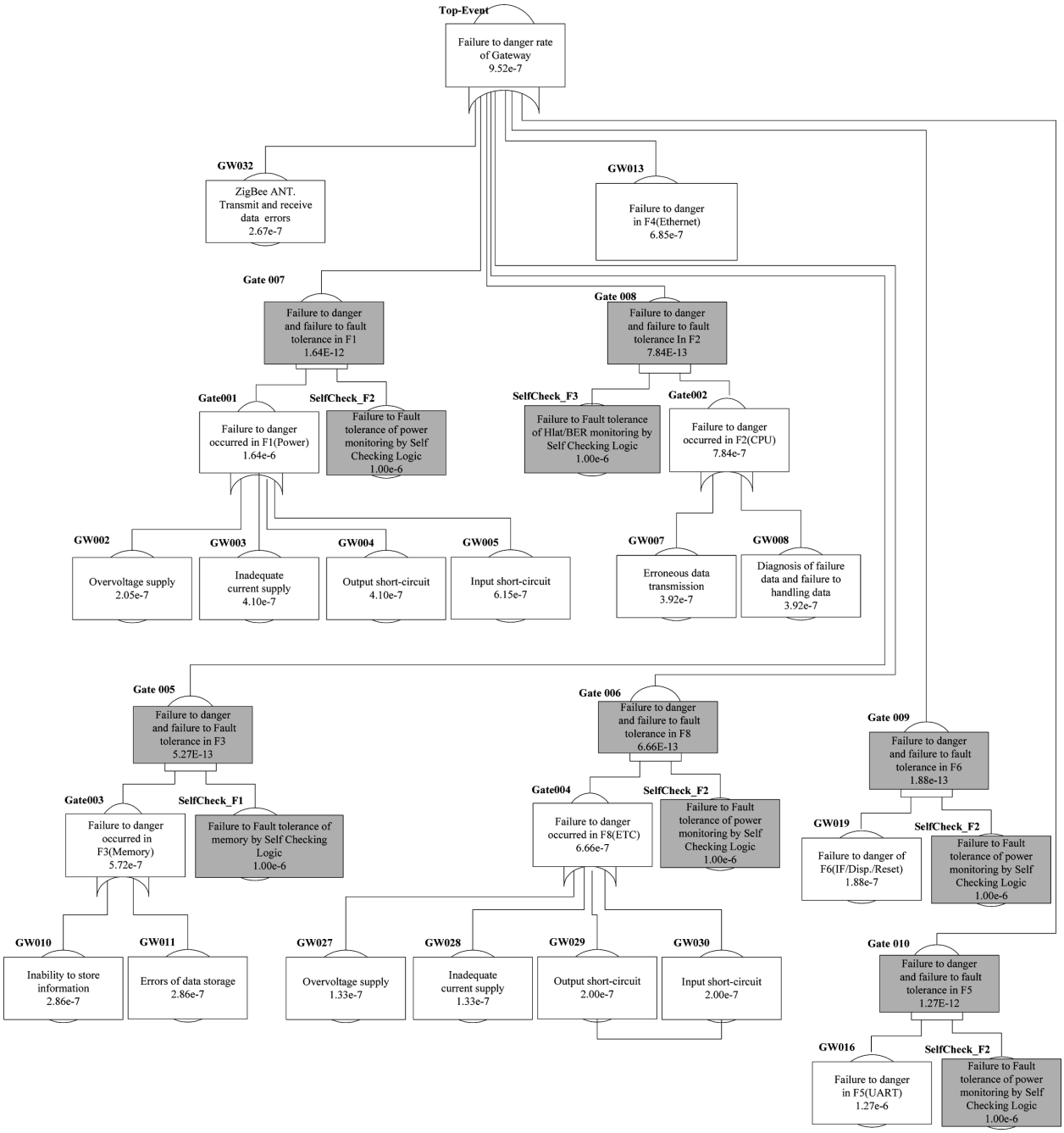

Fig. 6 Dangerous failure FTA of gateway in the form of Standby embedding fault detection and isolation circuits

3. 결 론

본 논문은 안전필수분야인 열차제어분야에 USN시스템을 도입하기 위한 신뢰성과 안전성향상방안을 게이트웨이를 대상으로 연구하였다. 신뢰성 및 안전성 향상을 위한 방법으로써 FMEA를 통해 위험측고장의 원인이 되는 고장모드의 발생빈도 억제를 위한 대책을 수립하였으며, 안전대책이 적용된 게이트웨이의 하드웨어를 다중화하여 신뢰도향상을 수행하였다.

과거의 사고경험을 바탕으로 설계요건을 강화하는 기존의 안전관리방식은 위험원의 위험도를 정량적으로 평가하여 안전을 확보하고 국제표준의 안전성 등급화(SIL)를 핵심으로 하는 IEC 61508 기반으로 발전되고 있으며, 또한 국내외 적으로 대부분의 안전필수 분야에서 IEC 61508기반의 신뢰성 및 안전성관리를 사용자가 요구하고 있다.

본 논문은 세계 최고수준 국내 IT기술의 안전필수분야 진출에 진입장벽으로 작용하고 있는 정량적 신뢰성 및 안전성 평가와 향상을 위한 방법을 USN 게이트웨이 사례를 통해

제시하였으며, 특히 기존 USN시스템에서 활용하고 있는 게이트웨이의 신뢰성과 안전성을 평가하고 향상을 위한 설계 방안을 제시함으로써, 열차제어를 포함한 철도와 IT기술 융합을 위한 방향을 제시하였다. 향후에는 USN시스템의 센서노드, 게이트웨이, 서버의 네트웍구조 전체에 대한 정량적 신뢰성 및 안전성평가에 대한 연구가 진행될 것이다.

후 기

본 연구는 한국철도기술연구원 주요사업 “ICT기반 열차운행 안전성 및 운용효율성 향상 기술개발” 과제로 수행되었습니다.

참고문헌

[1] IEC (1998) International Standard, Functional safety of electrical/electronic/programmable electronic safety-related systems (IEC 61508-1), pp. 23-26.
[2] IEC (2002) International Standard, Railway applications - Specification and demonstration of reliability, availability, maintainability and safety(RAMS)(IEC 62278), pp. 23-53.
[3] RSSB (2007) Engineering safety management(The Yellow Book), pp. 11-23.
[4] IEC (2007) International Standard, Railway applications - Communication, signaling and processing ystems - Safety related electronic systems for signaling, pp. 22-23.
[5] KRRI (2008) A Handbook for RAMS management of railway signaling, Appendix 3, pp. 5-6.
[6] IRSE (1992) Interrational technical committee, Report No.1, Safety system validation with regard to cross acceptance of signaling systems by the railways, Appendix A, pp. 43-45.
[7] D.K. Shin (2007) A Study on the safety demonstration of train control system, *Journal of the Korean society for railway*, 9(4), pp. 412-418.
[8] IEC (1998) International Standard, Functional safety of electrical/electronic/programmable electronic safety-related systems(IEC 61508-4), pp. 35.
[9] D.K. Shin (2007) A Study on reliability prediction for KOREA high speed train control system, *Journal of the Korean society for railway*, 9(4), pp. 419-424.
[10] D.K. Shin (2008) Railway Signaling - Self checking logic for standby sparing system, KOREA Patent No.10-0837597, 2008.06.05.
[11] RAC (2000) Reliability toolkit : Commercial practices edition, pp. 161.

접수일(2011년 1월 19일), 수정일(2011년 8월 3일),
게재확정일(2011년 9월 15일)