가능하다. 특히, 단말에 보수자의 위치를 특정할 수 있기 때문에 보수작업관리의 효율화를 도모할 수 있으며, 열차 운행상황과 열차 접근경보를 전달하면 작업자의 안전확보의 측면에서 효과를 기대할 수 있다.

□■□□□

철도 정보전송을 위한 프로토콜 엔지니어링 기술

황종규, 이재호 | 한국철도기술연구원 | 전가신호연구본부

1. 서론

철도 신호제어장치들은 각자 고유기능을 수행함으로써 철도시스템의 안전운행을 도모하고 있다. 따라서 대부분의 신호장치는 바이탈한 제어장치로서 안전측 동작(Fail-safe)을 보장하기 위하여 기존에는 기계적 또는 전기적인 계전기 로직에 의해 각 장치 고유의 기능을 수행하였다. 그러나 최근에 들어 전자, 컴퓨터, 통신 기술의 발달에 따라 철도신호제어장치들도 전자화된 장치들로 대체되어가고 있는 추세이다. 이처럼 신호제어장치들이 전자화되어감에 따라 각 장치간 인터페이스를 위한 링크도 디지털 통신채널로 대체되어가고 있다. 따라서 이러한 각 장치간 인터페이스를 위한 통신링크에 대한 중요성이 증대되고 있다.

대부분의 철도신호제어장치들은 온도, 진동, EMI 등의 운용환경이 가혹한 선로변에서도 안전하게 동작하여야 하므로 안전동작을 위한 높은 신뢰성이 신호장치 뿐만 아니라 신호장치간의 통신링크에도 필수적으로 요구되는 사항이다. 이러한 바이탈한 신호제어시스템들 사이의 정보전송을 위한 보다 높은 신뢰성을 갖는 표준화된 프로토콜이 필요하게 되었다[2][3]. 지금까지 적용되어오고 있는 철도신호시스템을 위한 통신 프로토콜은 대부분 비정형적인 방법(Informal Method)에 의해 설계 및 구현되어져왔다. 이러한 비정형적인 방법에 의해 개발된 프로토콜은 오류와 비효율성을 내포하고 있을 수 있으며, 이러한 프로토콜이 바이탈한 철도신호시스템에 적용되게되면 치명적인 결함이나 사고를 발생시킬 수 있다. 따라서, 새롭게 설계 및 표준화될 철도신호용 프로토콜은 정형적인 방법(Formal Method)에 의해 설계 및 구현되어져야 한다[1][5].

본 고에서는 이러한 철도제어시스템처럼 바이탈한 제어시스템을 위한 프로토콜의 설계를 위한 정형기법에 의한 프로토콜 엔지니어링 기술 일반과 철도신호용 프로토콜에 적합한 프로토콜 정형검정(Formal Verification) 방법론을 소개하고, 이러한 방법론이 실제 어떻게 적용되는지 예를 들어 설명한다.

2. 정형기법에 의한 프로토콜 엔지니어링 개발과정

전자기술과 정보기술의 급속한 발전은 컴퓨터망의 획기적인 발전과 분산처리를 가능하게 하였으며, 그 결과 많은 컴퓨터 통신망들이 설계되고 구현되었다. 이러한 다양한 통신망을 경유하는 응용개체(Entity) 사이의 통신은 여러 종류의 서로 다른 형태를 취할 수 있다. 멀리 떨어진 개체들 사이에 대화를 할 수 있도록 정한 규칙을 통신 프로토콜(Communication Protocol)이라 한다. 즉 프로토콜이란 통신망의 다른 노드에서 동시에 수행되어 신뢰성 없는 채널을 통하여 통신하는 통신개체들 사이의 대화를 가능하

도록 하기 위해 정의한 규칙이다.

프로토콜 공학(Protocol Engineering)은 통신망에서 사용되는 프로토콜을 연구하는 분야로 프로토콜을 설계하고 구현할 때 발생되는 복잡성과 오류 발생을 제거하는 방법을 연구하는 분야이다. 그림 1은 프로토콜 개발과정을 나타낸 것으로, 각 개발 단계는 사용자 요구사항 분석 단계, 프로토콜 설계 단계, 서비스 명세 단계, 프로토콜 명세 단계, 프로토콜 검정 단계, 프로토콜 구현 단계, 프로토콜 적합성시험 단계로 나뉘어진다.

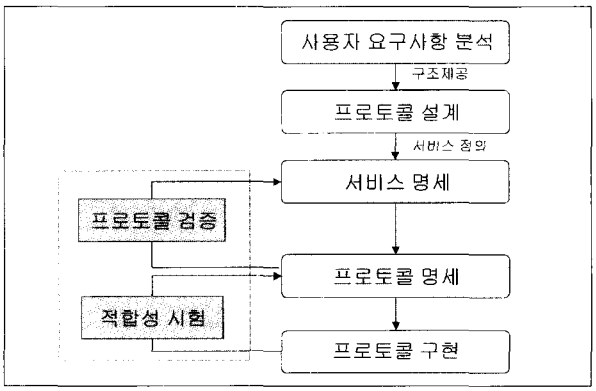


그림 1. 프로토콜 개발 과정

사용자 요구사항 분석 단계에서는 사용자 요구사항을 상세화, 공식화하고 설계자와 사용자 사이에서 프로토콜의 일반적 구조와 기능을 분석한다. 그리고 이러한 요구사항을 만족시키도록 프로토콜 계층을 설계한다. 프로토콜 설계 단계에서는 사용자 요구사항 분석 단계로부터 프로토콜 구조를 제공받아 프로토콜에 대한 전반적인 구조적 설계를 하게 된다. 명세화 단계에서는 프로토콜 개발 도구를 이용하여 프로토콜을 기능적 모듈로 분리시켜 서비스와 프로토콜을 기술하고 검정하며 PDU(Protocol Data Unit)을 정의한다. 명세 단계는 인접계층 사이의 기본동작을 정의하는 서비스 명세 단계와 개체의 인터페이스가 명세된 서비스의 방법에 대한 프로토콜 명세 단계로 나눌 수 있다. 서비스 명세 단계에서는 서비스 프리미티브의 집합과 매개변수들 그리고 서비스 프리미티브의 순서가 정의되고, 프로토콜 명세 단계에서는 각 통신 시스템 구성요소에 존재하는 프로토콜 개체의 동작을 정의하며 프로토콜에 대한 검정과 성능분석이 수행된다. 프로토콜 구현 단계에서는 추상적인 명세를 더욱 상세화하고 구현하는 단계로서 실행코드가 생성된다. 이러한 구현제품은 표준의 요구사항을 만족하는지 시험하는 적합성시험을 수행함으로써 그 오류를 검출한다.

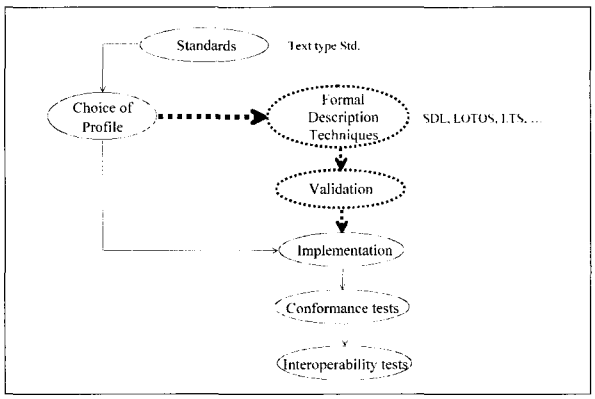


그림 2. 정형기법에 의한 프로토콜 개발

이러한 프로토콜 개발과정에서 프로토콜 명세의 정확성을 검증하는 부분은 일반적인 산업용 프로토콜의 설계 및 개발 과정에서 비정형적인 방법에 의해 수행되어져왔다. 하지만 정보통신관련 시스템들이 기능적인 면에서 복잡해지고 규모면에서 광범위해짐에 따라 프로토콜 명세의 무결성 및 완전성을 검사하여 신뢰성 있는 프로토콜의 개발 방법으로 정형기법(Formal Method)의 사용이 필수 불가결하게 되었다. 정형기법 중 가장 핵심적인 기술인 검증기술은 주어진 프로토콜 사양과 그 하위 계층에서 제공되는 서비스 사양에 근거하여 통신개체들의 상호동작이 주어진 서비스 사양에 만족하는가를 시험하는 과정으로, 프로토콜의 필수적인 정확성(Correctness) 특성을 만족하는가에 대한 프로토콜 사양을 분석하는 과정이다. 그림 2의 오른쪽 두 부분이 이러한 프로토콜의 정형검정 단계이다. 즉, 정형검정을 위해서는 서비스 명세를 형식기술언어(Formal Description Language)로 명세화하고 이를 바탕으로 정형검정하는 과정을 말한다. 이때 형식기술언어에 의해 명세화하는 과정을 FDT(Formal Description

Technique)이라 하며, 대표적인 형식명세언어에는 SDL, ESTELLE, LOTOS 등이 있다[4]-[8].

철도신호용 프로토콜의 경우 다른 어떠한 프로토콜들보다 높은 신뢰성과 안전성이 요구되어진다. 따라서 이러한 정보통신 분야에 일부 적용되고 있는 정형검정 기술을 철도신호용 프로토콜에 적용하여 정확성을 검증하는 것은 매우 유용한 방법이다. 따라서 다음절에서 이러한 철도신호용 프로토콜의 정형검정에 적절한 방법을 검토하고자 한다.

3. 모형검사를 이용한 프로토콜의 검정

통신 프로토콜에 대한 사용자의 요구사항이 복잡화, 다양화, 대형화되어짐에 따라 개발에 따르는 어려움은 더욱 증대되었고, 비정형적 방법에 의한 개발은 많은 오류나 결함을 내포할 수 있다. 특히 철도신호시스템 같은 바이탈 제어시스템에 적용을 위해서는 이러함 오류나 결함이 제어되어져야 한다. 이에 따라 일반적으로 바이탈 제어시스템의 설계나 정보통신관련 프로토콜의 설계에 적용되어오던 정형기법을 프로토콜 설계에 적용한 철도신호용 프로토콜의 정형검증을 위한 방법론을 제시한다.

프로토콜이 적절한 통신을 하기 위해서는 프로토콜 상태의 Deadlock, 비정상적인 도달 등과 같은 잠재적인 설계에러가 없어야 하며, 사용자 요구사항과 일치하는지 결정하고, 다른 프로세서와의 원활한 통신이 이루어지는지 검사해야 한다. 프로토콜 검정은 프로토콜 명세의 정확성, 안전성과 필연성을 검증하는 것으로 모형검사(Model Checking)에서 보다 구체적으로 검정해야 할 프로토콜의 특성은 안전성(Safety)과 필연성(Liveness)이며 이 두 특성을 이루는 구성요소는 다음과 같이 네 가지가 있다[5].

- ▶ Deadlock : 한 상태에서 다른 어떤 상태로의 천이가 존재하지 않기 때문에 다음 행위를 할 수 없는 경우. 즉, 그 상태에서 나가는 천이가 존재하지 않는다.
- ▶ Livelock : 프로토콜 상태들의 부분집합 내에서 그 상태들만을 무한히 반복적으로 천이하는 경우로써 그 부분집합 이외의 다른 상태로의 천이가 존재하지 않는다.
- ▶ Reachability : 프로토콜이 작동되기 시작할 때, 즉 프로토콜의 시작에서 정의되어지는 특별한 상태로써 초기상태가 존재하는데 이 초기상태로부터 프로토콜은 정의된 천이의 순서에 의해 일부 또는 모든 다른 상태에 도달하게 된다. 프로토콜이 정의된 천이와 상태로 도달하면 그 천이와 상태에 대한 명세는 올바른 프로토콜이다.
- ▶ Liveness : 프로토콜의 어떤 정당한 특성이 결국 만족되어지는 것으로, 결국에는 도달되어야 하는 상태와 반드시 발생하야 하는 행위를 나타낸다.

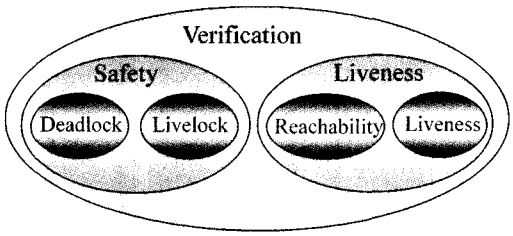


그림 3. 프로토콜 정형검정 대상

안전성 특성은 Deadlock이나 Livelock과 같이 절대로 발생되어서는 안 되는 상태나 행위를 프로토콜에서 배제하는 특성을 나타는 것이고, 필연성은 프로토콜이 초기 상태로부터 정의된 천이의 순서에 의해 결국에는 도달되어져야 하는 상태와 반드시 발생해야 하는 행위 즉, Reach-ability와 Liveness를 만족하는 특성으로서, 이러한 안전성과 필연성 검증을 프로토콜의 정형검증 기준으로 사용되게 된다.

이러한 대상들을 검정하기 위해서는 설계한 프로토콜을 형식언어(Formal Specification Language)로 표현하여야 하는데, 철도신호용 프로토콜을 위해서 중간모델인 LTS(Labeled Transition System)로 프로토콜을 명세화한다. 이 LTS의 경우는 시스템의 상태천이에 대한 모델링을 위한 형식언어로 프로토콜 같은 순차적인 프로세스의 표현에 적절하다. 그리고 이 형식명세를 바탕으로 정형검증을 위해서는 형식명세가 안전성과 필연성 특성을 만족하는지를 분석하는 과정이 필요하다. 이러한 과정이 모형

검사(Model Checking) 기법으로, 일반적으로 시제논리에 기반을 둔 방법들이 많이 사용되어 왔으나 시스템 요소의 증가에 따라 상태가 기하급수적으로 증가하는 상태폭발 문제가 있어, 철도신호용 프로토콜의 검증을 위해서는 프로토콜 행위특성을 가장 강력하게 표현하는 Modal μ-calculus 논리를 이용하여 프로토콜 명세의 특성(안전성과 필연성)을 정의한, 이 논리식에 따라 Solve 알고리즘[7]을 적용하여 모형검사를 수행한다. 그리고 정형검증이 마무리된 후 실제로 프로토콜이 구현되었을 경우, 구현된 프로토콜이 정확하게 구현되었는지 시험을 위한 시험계열 생성을 위해 I/O FSM(Input/Output Finite State Machine)으로 모델링하고 이를 바탕으로 시험계열을 생성하여 구현된 프로토콜의 적합성을 검사하게 된다[9].

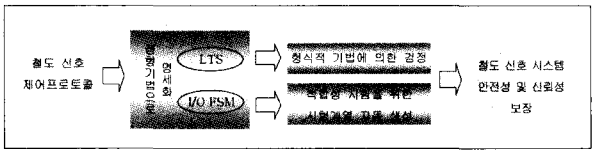


그림 4. 프로토콜의 정형검증 절차

4. 철도신호용 프로토콜의 정형검정 예

본 절에서는 위에서 기술한 프로토콜의 안전성과 필연성 특성을 표현하는 Modal μ-calculus 식으로부터 철도신호제어용 프로토콜의 완전성을 검정하는 방법을 설명한다. Modal μ-calculus는 통신 프로토콜의 안전성과 필연성 특성을 표현하는 최소 및 최대 고정점 연산자를 사용함으로써 Temporal 특성을 표현하는 강력한 로직이다. Modal μ-calculus에서, 구문은 원자명제(Atomic Propositions), (논리곱 : Conjunction), (논리합 : Disjunction), [ ](필연성 : Necessity), 〈〉(가능성 : Possibility), ν(최대 고정점 : Greatest Fixed Point) 및 μ(최소 고정점 : Least Fixed Point)로 구성된다. 안전성은 프로토콜의 부당한 상태 즉, Deadlock이나 Livelock과 같은 상태를 배제하는 특성이고, 필연성은 통신 프로토콜에서 Reachability와 Liveness를 만족시키는 특성이다. 만약 다음의 Modal μ-calculus 논리식이 각각 참이라면, 이것은 설계된 통신 프로토콜의 안전성과 필연성이 정확히 검정되었다는 것을 의미한다.

▶ 상태에 대한 안전성 : $\nu Z.\Phi \wedge [-]Z$
▶ 행위에 대한 안전성 : $\nu Z.\Phi[k]ff \wedge [-]Z$
▶ 상태에 대한 필연성 : $\mu Z.\Phi \vee (\langle - \rangle tt \wedge [-]Z)$
▶ 행위에 대한 필연성 : $\mu Z.\Phi \langle - \rangle tt \wedge [k]Z$

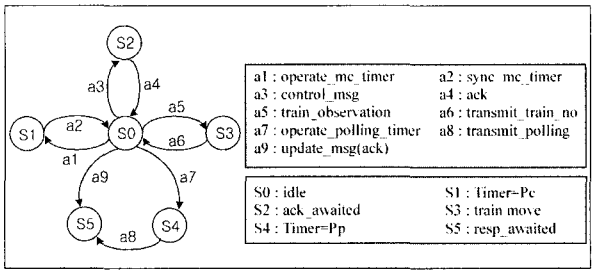


그림 5. 철도신호용 프로토콜의 LTS 모델링

예를 들어, 행위 a7이 발생하면 반드시 a8이 발생하고 Deadlock과 Livelock이 없음을 나타내는 Modal μ-calculus의 논리식은 다음과 같으며, 이 식이 참이 됨을 모형검사 알고리즘인 Solve 알고리즘을 적용하여 검증하면 된다.

$$\nu Z.(\mu Y.A \vee (\langle - \rangle tt \wedge [-]Z \quad 단, A=\{S0\}$$

그림 6은 Solve 알고리즘의 초기화 규칙에 의해 초기화된 비트-벡터, 계수기 및 배열 M을 나타낸다. 그리고 그림 7은 배열 M[i]가 공집합(Empty)이 될 때까지 갱신알고리즘을 적용하여 비트-벡터와 카운터를 갱신한 결과로 검정대상인 Deadlock 및 Livelock을 판단할 수 있다. Deadlock은 비트-벡터의 요소에 의해 판단되는데, 그림 7의 결과에서, 원소명제(Atomic Proposition) A와 관련된 X2 요소를 제외하고 모든 비트-벡터는 1로 갱신되어 설계된 프로토콜의 LTS모델에서 Deadlock이 없음을 발견할 수 있다. 또한, Livelock은 계수기(C)의 요소를 통하여 검지 될 수 있다. 그림 7의 결과 계수기의 모든 요소가 0으로

갱신되어 LTS모델에서 Livelock이 없음을 발견할 수 있다. 이들 결과로부터, 설계된 프로토콜에 대한 위 표현된 LTS 모델은 논리식 $\nu Z.(\mu Y.A \vee (\langle - \rangle tt \wedge [-]Y)) \wedge [-]Z$, $A = \{S0\}$을 만족하므로, 이 프로토콜은 완전성을 만족하는 적정한 모델로 검정되었다.

X	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8
S0	0	1	0	0	0	1	1	1
S1	0	0	0	0	0	1	1	1
S2	0	0	0	0	0	1	1	1
S3	0	0	0	0	0	1	1	1
S4	0	0	0	0	0	1	1	1
S5	0	0	0	0	0	1	1	1

C	X_3	X_4
S0	2	4
S1	2	1
S2	2	1
S3	2	1
S4	2	1
S5	2	1

M[1]=<<S0, X2>, <S0, X6>, <S1, X6>, <S2, X6>, <S3, X6>, <S4, X6>, <S5, X6>>
M[2]=< >

그림 6. 비트-벡터, 계수기 및 배열M(i)(초기상태)

X	X_1	X_2	X_3	X_4	X_5	X_6	X_7
S0	1	1	1	1	1	1	1
S1	1	0	1	1	1	1	1
S2	1	0	1	1	1	1	1
S3	1	0	1	1	1	1	1
S4	1	0	1	1	1	1	1
S5	1	0	1	1	1	1	1

C	X_1	X_2
S0	0	0
S1	0	0
S2	0	0
S3	0	0
S4	0	0
S5	0	0

M[1]=< >
M[2]=< >

그림 7 비트-벡터, 계수기 및 배열M(i)(결과)

5. 결론

전자 및 통신기술의 발달에 따라 철도신호제어장치들도 전자화된 장치들로 대체되어가고 있고 신호설비들간 통신 링크에 의해 신호제어시스템의 통합화 및 지능화되어가고 있다. 이에 따라 신호설비들간 안전적이고 효율적인 정보전송을 위한 표준화된 통신 프로토콜이 필요하게 되었다. 하지만 지금까지 적용되어오고 있는 철도신호시스템을 위한 프로토콜은 대부분 비정형적인 방법에 의해 설계 및 구현되어져왔으나, 본 고에서는 정보통신분야의 프로토콜의 설계 및 검증에 적용되고 있는 정형기법에 의한 프로토콜 설계 및 검증과정을 고찰하였다.

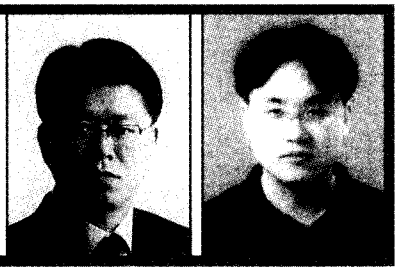
이러한 프로토콜의 정형검증 방법은 정보통신분야의 프로토콜들처럼 기능적인 면에서 복잡하고 규모면에서 광범위해짐에 따라 프로토콜의 무결성과 완전성을 검증하여 보다 신뢰성 있는 프로토콜을 개발하기 위한 방법론의 하나로, 철도신호시스템처럼 바이탈한 제어시스템을 위한 프로토콜의 설계 및 검증에도 매우 효과적인 방법이다. 따라서 본 고에서는 이러한 프로토콜 개발의 일반적인 과정과 이러한 정형검증을 통한 방법론을 간략하게 고찰하였고, 이를 바탕으로 철도신호용 프로토콜의 설계 및 검증에 적합한 방법론을 제시하였다. 그리고 실제 철도신호용 프로토콜의 검증을 이 방법론에 적용한 예를 설명하였다. 즉, 비정형적인 방법을 사용함으로써 설계된 프로토콜 내에 포함 가능성이 있는 모호성을 제거하기 위하여, LTS로 명세화하고 모형검사 알고리즘을 통하여 안전성과 필연성을 검정하는 정형검증기법을 적용하여 프로토콜의 안전성 및 필연성을 검정한 예를 설명하였으며, 이러한 정형검증을 통해 설계된 철도신호용 프로토콜이 실제 철도현장에 적용됨으로써 신호시스템의 안전성, 신뢰성 및 유지보수의 효율성의 증가가 기대되어진다.

참고 문헌

1. 한국전자통신연구원, '정보통신 프로토콜 공학', 1998.
2. 철도용품 규격, '철도 6330-3328 : 열차집중제어장치와 전자연동장치간 정보전송방식(Protocol)', 철도청, 2002.
3. 황종규, 이재호, '철도신호시스템을 위한 새로운 통신 프로토콜의 성능해석 및 검증', 전기학회논문지, 53B권 6호, pp.380-387, 2004년 6월.
4. 박용범, 김태균, 김성운, 'LTS 명세 검증을 위한 모델 검증기 개발', 한국정보처리학회 논문지 제5권 제4호, pp. 995-1004, 1998년 4월.

5. D. Schwabe, 'Formal Techniques for the Specification and Verification of Protocol', Ph.D Thesis, Univ. of California Los Angeles, Apr., 1981.
6. D. Kozan, 'Results on the Prepositional mu-calculus', Theoretical Computer Science, 27: 333-354, December 1983.
7. R. Cleaveland, 'Tableau-based Model-Checking in the Propositional Mu-Calculus', Acta Informatica 27 : 725-727, 1990.
8. O. Burkart and B. Steffen, 'Model Checking the Full Modal Mu-Calculus for Infinite Sequential Processes', LFCS Report ECS-LFCS-97-355, 1997.
9. P. V. Koppol and K. C. Tai, 'Conformance Testing Protocol specification as Labeled Transition system', International Workshop Protocol Test System, IWPTS95, pp.143-158, Eery, France, 1995.

열차무선시스템 최신 연구 동향



김백현, 신덕호 | 한국철도기술연구원 | 전기신호연구본부

1. 서론

최근에는 이동체 통신이나 컴퓨터 등의 정보통신기술이 현저하게 발전을 거듭하고 있으며, 열차의 고속화 고밀도화를 도모하기 위해 열차제어 분야에 무선을 이용하는 시스템의 개발이 프랑스, 독일, 영국, 이탈리아, 일본, 미국 등의 철도선진국에서 활발히 수행되어지고 있다. 무선을 이용한 열차제어시스템의 기술개발은 철도에 커다란 경제적 이득을 창출할 가능성을 지니고 있기 때문에, 전 세계적으로 많은 연구가 이루어지고 있다. 특히, 유럽의 경우 통화 단일화와 회원국간의 비관세 교역 등의 경제적인 제도뿐 아니라, 철도분야에 있어서도 유럽횡단고속철도망(Trans-European High Speed Rail Network)의 구축을 위한 신호시스템의 표준화를 위해 유럽연합과 국제철도연합(UIC: Union Internationale des Chemins de fer)의 지원하에 ETCS 프로젝트가 수행되었다.

ETCS는 상호운용성(interoperatibility)을 목표로 하여 지상-차상간의 전송방식으로 현재의 기술 한계와 미래의 가능한 기술 개발 능력을 고려하여, 기능적인 측면에 의해 Level 1, Level 2, Level 3로 분류하여 추진되고 있다. 국제철도연합은 EIRENE(European Integrated Radio Enhanced NEtwork) 프로젝트를 통해 철도에 적용하기 위한 무선통신 시스템의 표준화를 위한 요구 조건을 도출하였으며, 도출된 사양에 따르는 무선 시스템 프로토콜의 상세 기술, 개발, 시험 및 유효화를 위해 MORANE(MObile RAdio for railway Networks in Europe) 프로젝트를 수행하였다. 그 결과, ETCS Level 2에서의 정보 전송 및 ETCS Level 3에서의 열차 검지 및 정보 전송에 적용하기 위한 무선통신 시스템으로서 GSM-R(Global System for Mobile communication - for Railways)을 채택하였다.

GSM-R은 유럽의 이동통신표준인 GSM을 기초로 하여 철도분야에서의 사용을 목적으로 별도의 주파수 대역(876~880/921~925 MHz)을 할당하고 그룹통화(VGCS: Voice Group Call Service), 방송통화(VBS: Voice Broadcast Service) 및 우선순위(eMLPP: enhanced MultiLevel Precedence and Preemption) 등의 기능을 추가한 무선통신 시스템으로 다음과 같은 이유로 GSM-R