

GPS 式列車接近警報装置の信頼性向上の取り組み

○ 正 [土] 原納 悠☆ 正 [土] 溝口 敦司 正 [土] 島田 喜久雄

正 [土] 井上 淳太 (西日本旅客鉄道株式会社)

田口 研治 岡本 圭史 大崎 人士 (独立行政法人産業技術総合研究所)

RELIABILITY IMPROVEMENT MEASURES FOR A TRAIN APPROACH ALARM SYSTEM WITH GPS-LINKED MOBILE PHONES

Yutaka HARANOU, Atsushi MIZOGUCHI, Kikuo SHIMADA, Junta INOUE

Technical Research and Development Dept. West Japan Railway Company

2-4-24, Shibata, Kita-ku, OSAKA City

Kenji TAGUCHI, Keishi OKAMOTO, Hitoshi OSAKI National Institute of Advanced Industrial Science and Technology.

JR West has developed and implemented the GPS-linked train approach alarm system and put it in practice to prevent such dangerous situations, as the workers on the track are exposed to the risk of being hit by an oncoming train. Whenever a train is in the track circuit next to a work site, this system can detect an approaching train by the control unit and make mobile phones warn to the workers.

Key Words: train approach alarm system, lookout, GPS-linked mobile phone, Centralized Train Control system

1. はじめに

JR 西日本では、触車事故防止のため、見張員の業務のバックアップを目的とし「GPS 式列車接近警報装置」(以下、「GPS 式列近」という)を導入している。GPS 式列近は、制御サーバにおいて列車接近を判定し、現場の携帯電話を警報鳴動させるシステムである。現在、ソフトウェアの開発のプロセスにおいて産業技術総合研究所の協力のもと、標準化プロセスを参考に、より信頼性の高いシステムの構築に取り組んでいる。本論文ではその概要について報告する。

2. GPS 式列近の概要

GPS 式列近の概要を図 1 に、現場使用状況を図 2 にそれぞれ示す。

見張員が所持する GPS 携帯(以下、「測位端末」という)を用いて GPS 測位により見張員位置情報を作成するとともに、CTC 装置から取得した軌道回路に関する情報および列車を管理する列車番号情報より列車の在線を示す列車在線位置情報を列車情報伝達装置にて作成する。

各々の位置情報は一定周期で制御サーバに伝達され、接近有無の判定が行われる。接近と判定されれば、公衆無線回線を通じて現場見張員が持つ警報用携帯電話(以下、「警報端末」という)に接近情報を通知し、警報音、音声(「上り接近」「下り接近」)、及びバイブレーションを動作させる。

機能については、次の 6 項目とした。

- ①見張員位置の検知機能(測位端末)
- ②制御サーバと警報端末・測位端末との通信機能
- ③列車在線位置の検知機能(列車情報伝達装置)
- ④列車接近通過の判定機能(制御サーバ)
- ⑤列車接近の警報機能(警報端末)
- ⑥システム異常の検知機能(制御サーバ)

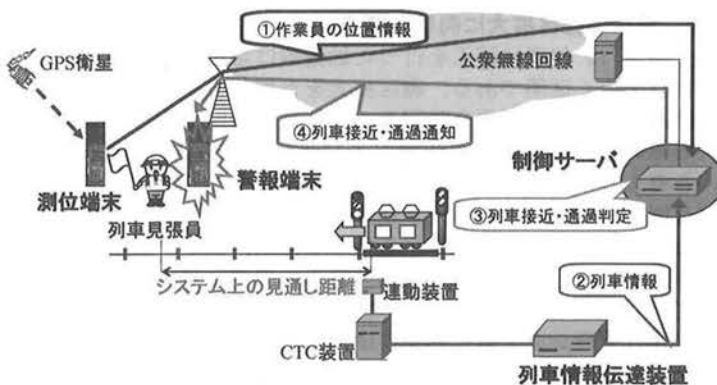


図 1. GPS 式列近概要

なお、CTC 装置は情報伝送システムであり、フェールセーフ性を備えたシステムではないため、CTC を活用した列車接近警報装置では見張員の代わりを行うことはできない。よって、GPS 式列近は保安装置ではなく列車見張を補完する装置となる。



図 2. GPS 式列近使用状況

3. 導入の状況

図3に示すとおり、平成19年度にまず伯備線の新郷～伯耆大山駅間約50kmにて導入を行った。平成20年度には、上期に伯備線の倉敷～新郷駅間約90km、奈良線の木津～京都駅間約40km、下期に宇野線の岡山～宇野駅間約40km、山陰線の園部～西出雲駅間約360km、呉線の三原～海田市駅間約90kmにおいて導入を行った。平成22年度には山陽線の三原～下関駅間約300kmにおいて導入を行った。現在は、山陰線・津山線・加古川線・舞鶴線・桜井線・和歌山線計約360kmへの導入へ向け順次整備を進めている。



図3. GPS式列近導入状況

4. 更なる線区拡大に向けた開発

平成19年度に導入を行った伯備線は常用閉そく式で自動閉そく区間である。線区拡大を目指して、駅間が1軌道回路となる単線自動閉そく(特殊)線区である和歌山線の粉河～田井ノ瀬駅間および運行管理システム[※]等を導入した北陸線等で開発を行ってきたところであるが、今回、近畿圏における列車往来が非常に多い区間(おおむね5分に1本以上列車が走行する区間、以下、高密度線区という)向けの新たなシステムの開発に着手したので、以下にこの新システムの開発について述べる。

※運行管理システム：列車の進路を自動制御するとともに、臨時列車等のダイヤを管理する機能や自動旅客案内機能を付加したシステム。また、列車高密度線区に対応するため高速で情報処理を行うことが可能である。

4.1 高密度線区での課題

これまでに開発したシステムのままで高密度線区へ展開を行うと、接近鳴動が鳴り止むまでに次列車に対し接近鳴動するなど、鳴動時間が長くなり、現場での線路立入の補助装置としての役割を果たさないことが予想された。そのため、開発の段階において、鳴動時間を短くするために接近鳴動の判定処理を大きく変更する必要が生じ、サーバを分離・追加させ他データを取り込むことでこの問題の解決することとしたが、これまでに開発したシステムに比べ仕様が複雑化することとなった。このため、発注および開発の段階において、システム自体の仕様および信頼性を受発注者が理解することが非常に重要であると考えられた。

5. 発注者としての問題認識

ソフトウェアの開発時における課題として、発注者と受注者間の意思疎通の困難さがある。例えば、受発注者間での要求仕様書の解釈に関する齟齬は、製品の信頼性低下など、利用者の要求を満たさない情報システムを生むこととなる。実際「情報システムの信頼性向上に関するガイドライン」においても、信頼性・安全性の水準を含む様々な事柄に関し、受発注者間で合意することと記載されている。

受発注者間の意思疎通の困難さの要因として、曖昧さ・抜けなどの要求仕様書の不備や、受注者が作成する資料が発注者に見えにくく、開発がブラックボックス化していることなどが挙げられる。前者の要因のうち、信頼性の要件定義など、特に専門的分析を必要とするものは、専門知識を持った第三者による分析及び発注者への技術移転が有効である。後者の要因に対しては、発注者側が自身に見える資料の作成を受注者側へ要求することが妥当であろう。

6. 信頼性を向上させるために

一般に信頼性・安全性の高いシステムの開発は、開発プロセス、開発方法論、開発ツール・プログラミング言語、保証技術、評価技術などの多くの技術要素により構成されている。本論文で示す研究は、既に開発したシステムに対してより、仕様が複雑になった部分を含む、新規システムの開発に対して、より信頼性、安全性を担保できる開発方法論の研究開発である。我々が今回注目したのは、発注者の発注プロセスにおける信頼性・安全性分析である。発注者が発注仕様書を作成する際に、運用を含んだシステムに対して、十分な分析を行うのは、システムの信頼性向上に対して非常に重要である(図4)。システム開発においては、システム境界を明確にすることは機能仕様の分析において必要な作業である。その際に、システムに関連しないが、運用に関連する要件も同時に獲得する必要がある。特に、今回開発の補助装置は見張員という人間系を含むシステムであるので、システムの機能要件とシステムの運用要件を同時に獲得することにより、信頼性、安全性の向上が望まれる。

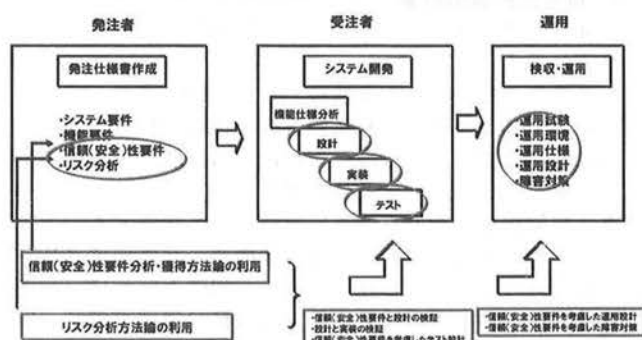


図4. 高信頼システム開発における注意点

7. 信頼性を向上させるシステムの構築

安全性が重要である原子力発電、航空機、宇宙開発、自動車、鉄道といった様々な分野において利用されている方法論としては、潜在的故障モードとその原因と影響を同定するための、定性的な方法論である FMEA (Failure Modes and Effects Analysis)⁶⁾ や、定義されたトップ事象(故障)にいたる原因を分析する演繹的

な手法である FTA (Fault Tree Analysis)¹¹⁾ が知られている。これらの分析方法を用いることで、システムの信頼性・安全性の向上が見込まれる。

自動車関連では、安全分析の手法を含む、様々な規格が策定されている。それらにおいては、安全分析プロセスが明確に定義されており、実際に利用することが容易である。よって、本研究においては、これらの手法を参考に信頼性向上に取り組んだ。

7.1 今回の報告の範囲

本研究において用いられた分析工程は図5に示すとおりである。

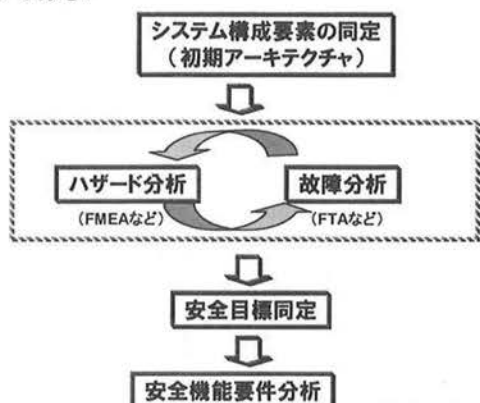


図5. 分析工程図

ここでのシステムの安全性の分析とは、安全機能要件の定義までを指す。最初に、システムの構成要素（機能単位）を同定し、対象システムの安全分析のための、初期アーキテクチャを記述する。次にハザードの分析と故障の分析を行う。分析された各ハザードに対して、安全目標を同定する。最後に、安全目標を満たす安全機能要件を分析・獲得・定義する。

初期アーキテクチャは、安全分析のためのものであり、システム設計が進むにつれて、より詳細化される。プロセスの後工程において、変更等があった場合には、再度、分析をする必要がある。安全目標は安全性を確保するために達成すべき目標である。それに対して、安全機能要件は、安全目標を満たす機能要件である。機能要件は、抽象度が高いものからより詳細なものへと分解され、最終的には詳細安全機能要件として定義が行われる。この要件分析方法は、通常、要求工学におけるゴール指向要求分析（例えば KAOS）において用いられるものである¹²⁾。

本論文では特に、ハザードの同定と分析について述べる。ハザードの同定と分析のために、初期アーキテクチャにおいて同定された各機能単位とその操作環境に対して、ハザードの分析を行った。ハザードに対しては、その概要、運用環境などに注目して分析した。それに加えて、FMEA で用いられるアイテムの故障モード、潜在的故障原因、故障影響、検知方法、保証方法について分析を行った。

7.2 分析工程

7.2.1 アーキテクチャの指定

アーキテクチャを「警報端末」「測位端末」「制御サーバ」「列車情報伝達装置」「CTC 装置」等に据えて分析を行った（図6）。

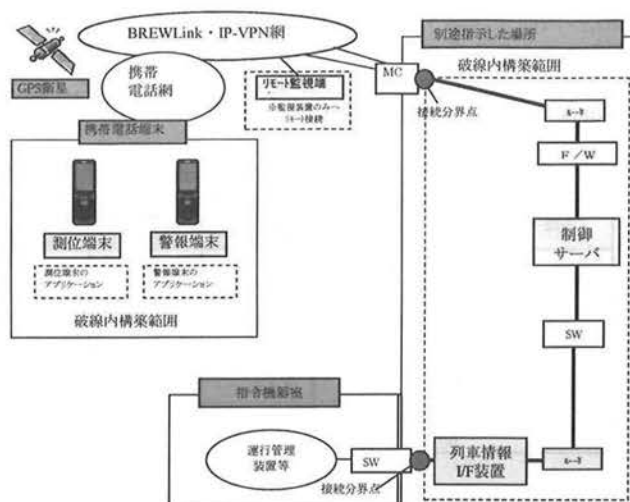


図6. 初期アーキテクチャ図

7.2.2 ハザード分析

1) FMEA

ハザード分析として、初期アーキテクチャの要素毎に、まず FMEA 分析を行った。警報端末の FMEA 分析例の一部を以下表1に示す。

表1. FMEA 表

アイテム	機能	故障モード	故障影響	故障原因	評価 (危険度)	
警報端末	作業員に 「列車接近」 「列車在線」 を知らせる。	鳴動指示情報 取得通信 不可能	作業員が列車 接近を 認識せず、 待避しない。	「警報端末」が 通信しない。	A	
警報端末		鳴動指示情報 取得通信 誤り		作業員が通信不能 区間で使用した。	A	
警報端末				「警報端末」が 処理が誤る。	A	
警報端末				作業員が通信誤り 区間で使用した。	A	

この分析により、初期アーキテクチャの要素毎の故障モードを明確化した。基本的には、故障モードとしては「情報を取得不可能」もしくは「情報取得が遅れる」の2点である。この2点を初期アーキテクチャの要素毎に分析を行った。アーキテクチャの要素によってはこれらの故障モードの想定をしていなかったが、初期アーキテクチャの要素を網羅的に分析することで、いずれの要素においてもこの2点が故障モードに該当するという分析結果を得た。

2) FMEA の拡張

自動車における安全対策においては、運転手の運転環境と運転者によるハザードに対する対抗策については分析・規定できるが、必ずしもそれを強要することはできない。実際の本システムを運用した場合の問題点の原因としては、初期アーキテクチャの要素自体が故障した場合と、人間系が関与する場合（見張員の使用位置等）がある。例えば、トンネル内等に見張員がいる場合等、本システム自体の利用が不可能な場合である。それに対して、本システムの運用においては、見張員に対して運用規則を策定し、遵守させることにより、見張員の安全を保障する必要がある。運用に関する要件は、通常、システムの開発が終了した後、設計、実施するものであるが、それでは、システム開発における安全要件の分析との関連が非常にあいまいである。それに対して、システムの安全分析を行う時点において、運用面での要件を同時に分析することにより、システムの安全性と運用の安

全性の両面を保証することが可能になる。よってこれを明確にできるよう、FMEA表における故障原因に「見張員の使用環境条件」を許すよう拡張して分析を行った。拡張FMEA分析例の一部を以下表2に示す。

表2. 拡張FMEA表

故障モード	故障原因	原因大別	対策 (ハード)	対策 (運用)
鳴動指示情報取得 通信 不可能	「警報端末」が 通信しない。	アーキ テクチャ	○	
	作業員が通信不能 区間で使用した。	作業員環境		○
鳴動指示情報取得 通信 誤り	「警報端末」が 処理が誤る。	アーキ テクチャ	○	
	作業員が通信誤り 区間で使用した。	作業員環境		○

この時、運用でカバーする故障原因であっても、技術の進歩によりシステム化が可能な場合があるので今後の課題として挙げておくことが重要である。

7.2.3 安全目標

前章において安全目標が同定されたので、次に、その安全要件を満たす安全機能要件を導き出す。ここでは、安全目標図として、安全目標を上位ノードとし、その安全機能要件を下位ノードとする樹状図を図8に示す。本システムの最上位の安全目標は「見張員の触車事故防止」である。それに対して、「鳴動指示情報取得通信不可能」という故障モードに対して、「「警報端末」が確実に鳴動し見張員に伝わる」という安全目標が対応し、それに対して、「列車接近時警報端末確実に鳴動指示」「列車在線時警報端末へ確実に鳴動指示」「警報端末警報指示受信時確実に鳴動」が安全機能要件として分析できた。これらの機能により、上位の安全目標が満たされるものと分析した。

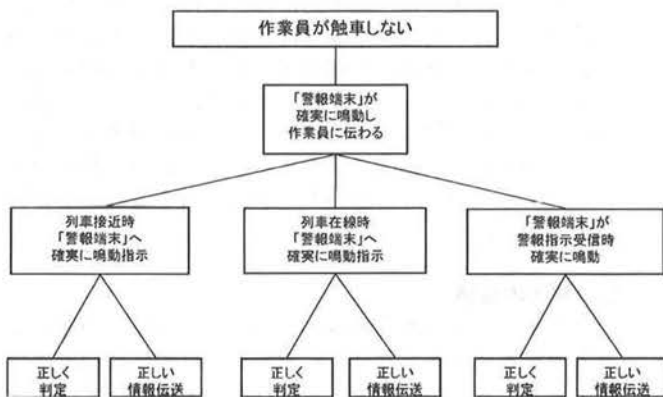


図8. 安全目標図

8. おわりに

高密度線区用のGPS式列近のシステム構築における信頼性向上のための取組として紹介させて頂いた。アーキテクチャの全ての要素に対して網羅的にハザード分析を行うことで、想定外のハザードを発見した。

安全分析の結果、故障原因のリストが作成されたことにより、万一装置が故障した場合でも、故障となる原因に対しての分析が容易になり、受発注者とも早急な対応が可能になる。また、当補助装置の機能として実現が不可能なものは、実際の現場での運用ルールでカバーする

こととなるが、その運用ルール作成のための故障原因が同定できたことにより、現場で本システムを使用するうえでの注意点が明確となったうえでの開発が可能となった。

仕様が複雑化するにつれシステム自体の信頼性に十分配慮しなければならないが、それを開発段階において発注者側が確実に分析し、メーカーと分析を共有し、仕様・運用ルールを決定することが安全性の向上に大きく貢献し、さらなるシステムの改良点等も明確になると考えられる。

ハザード分析を基に要求仕様を確定させ、その結果を忠実に反映させながら開発を行い、高密度線区において試使用を開始する予定である。

最後に、開発に際して多大な御協力を頂いている関係箇所の皆様に厚く御礼申し上げる。

参考文献

- 1) 川添雅弘, 清水郁夫: GPS 携帯電話を活用した列車接近警報装置, 第60回土木学会年講, 2005.9
- 2) 溝口敦司, 井手寅三郎: GPS 携帯電話を活用した列車接近警報システムの開発, JREA, 50巻6号, pp.22-24, 2007.6
- 3) 溝口敦司, 井上淳太: GPS 携帯電話を活用した列車接近警報システムの開発と深度化, JREA, 52巻6号, pp.32-35, 2009.6
- 4) 溝口敦司, 井上淳太: GPS 携帯を活用した列車接近警報システムの開発, J-Rail2009
- 5) ISO 26262/DIS Part 1 ~ 10 "Road Vehicles - Functional safety -", 2009
- 6) IEC 60812, "Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)", edition 2.0, 2006-01 (2006)
- 7) IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems", 2000
- 8) EN 50128, "Railway Applications: Software for Railway Control and Protection Systems", 1999
- 9) IEC 62278, "Railway Applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)", 2002-09.
- 10) 平栗滋人: 信号システムの RAMS 分析, RRR, pp 12-15, 2008
- 11) IEC 61025, "Fault tree analysis (FTA)", edition 2.0, 2006-12
- 12) A. van. Lamsweerde, "Requirements Engineering", John Wiley & Sons, 2009