

## 講演 4. 鉄道製品に関する安全関連規格に対して適合するための留意点について

鉄道認証室

※長谷川 智紀

渡邊 朝紀

田代 維史

### 1. はじめに

アジアや南米等で大量輸送及び環境対策として鉄道が注目され、多くのプロジェクトが立ち上げられている。国内の鉄道製品メーカーはこの市場動向へ対応するため、海外展開を進めている。日本の鉄道製品は世界に誇る安全性・信頼性を有しているが、この海外展開において、国内での取引との違いのひとつとして国際規格等への適合が求められる点がある。

規格には、大きく分けて、プロセス規格と製品規格とがある。前者は業務プロセスへの要求事項を挙げた国際標準化機構（ISO : International Organization for Standardization）が発行する ISO 9001 に代表されるものだが、ここでは技術仕様規格と機能安全規格からなる後者を取り上げる。このうち、技術仕様規格については、仕様を満たすことを試験により確認することで、国内鉄道製品メーカーも対応をしてきていた。しかし、機能安全規格については、製品開発プロセスに関係する規格であることから、国内鉄道製品メーカーは対応に苦慮してきた。特に、機能安全規格については第三者認証機関による認証が必須になることが多く、海外の認証機関とのやりとりが発生し、言語障壁も加わって、対応に多くの時間を要するといった課題が近年浮上した。これが、国内初となる当所の認証機関 NRCC（NTSEL Railway Certification Center）の発足の背景である。

NRCC 発足後、6 年間が経過し、審査経験を通じて、多くの知見を得た。そこで本講演では、機能安全規格である鉄道製品の安全関連規格への規格適合の意義とともに、適合の活動において望ましいと思われる点について述べることにする。

### 2. 規格適合を行う意義とは<sup>1)</sup>

#### 2. 1. 海外向けに対する規格適合の意義

欧州では、製造者であるメーカーに対する厳格責任の導入の声が高まり、1968 年頃から欧州委員会におい

て製造物責任（PL : Product Liability）に関する草案の検討が開始され、紆余曲折を経て 1985 年に PL 指令（欠陥製造物に対する賠償責任に関する加盟国の法律、規制及び行政規定の等質化についての欧州諸共同体（EC : European Communities）閣僚理事会指令）が成立した。この指令の主な内容は以下の通りであり、3 年以内に国内 PL 法を制定することを加盟国に要請した。

- ・ 被害者は損害の発生、欠陥の存在、因果関係の立証責任がある。（従来と異なり、被害者によるメーカーの責任の立証が不要となった）
- ・ 賠償金額の上限：多数の加盟国で上限なし
- ・ 以下のいずれかをメーカーが立証できた場合、メーカーが製造物責任を問われない。
  - a) 流通させなかったこと
  - b) 流通時点では欠陥がなかったこと
  - c) 販売目的で製造された物でなかったこと
  - d) 規制当局の指示で欠陥が発生したこと
  - e) 当時の科学・技術的水準では、欠陥の発見は不可能だったこと（開発危険の抗弁）
  - f) 部品の場合、完成品側の設計に欠陥があったこと

一方、英国では、1994 年に Railway Safety Case Regulations が導入され、鉄道事業者には、他者に受け入れられる Safety Case の作成が必須となった。ここで求められる Safety Case には、以下の事項が含まれる。

- (a) 安全施策
- (b) 起こり得るリスクの評価
- (c) 安全管理システム

このように、鉄道事業者及びメーカーは鉄道運行や製品の安全性・信頼性が確実であることを証明しなければならなくなった。

そこで、これらの証明方法の規格化が欧州電気標準化委員会（CENELEC : Comité Européen de

Normalisation Electrotechnique, 仏) において開始し、1999年に欧州規格 (EN : European Norm, 仏) として機能安全規格である EN 50126 (RAMS : Reliability, Availability, Maintainability and Safety, 英) が発行され、その後、具体的な活動や作成すべき文書群を定めた、EN 50128 (ソフトウェア)、EN 50129 (Safety Case)、EN 50129-1 及び EN 50129-2 (安全関連伝送) が発行された。

国際規格としては、これら EN 規格をベースとして、国際電気標準会議 (IEC : International Electrotechnical Commission, 英) が発行する規格として、IEC 62278 (RAMS)、IEC 62279 (ソフトウェア)、IEC 62425 (Safety Case)、IEC 62280-1 及び IEC 62280-2 (安全関連伝送、現在は統合され IEC 62280) が発行されている。

国際規格は欧州 PL 法の範疇外ではあるが、近年の国際鉄道市場においては、システムインテグレータやメーカーは、規格適合説明を行うことにより、鉄道運行や製品の安全性・信頼性が確実であることを証明することが求められ、言い換えると、鉄道製品等を輸出するにあたり、これら規格に積極的に適合することが不可欠となりつつある。

## 2. 2. 国内向けに対する規格適合の意義

現在、少子高齢化が進むに伴い技術継承が課題である。従来の技術継承のひとつである OJT (On the Job Training) は、時間的余裕が少なく十分な継承ができない状況が起きつつある。

また、技術継承において、その技術の背景も含めて継承されないことにより、新しい技術を取り入れる際、過去の経緯に立ち返る事が困難で、適切な対処ができない恐れが高まる事になる。

鉄道製品の安全関連規格への適合では、後述するように、「ノウハウ・経験・暗黙知」を明文化する必要があるとともに、その対応を行った理由等も明文化される。そのため、当該製品に対処した技術が明文化され、技術継承のための資料として用いることができる。

また、技術継承を目的として規格適合を国内向けに対して実施することにより、海外向け・国内向けといった個別文書の作成の手間を省く事が可能になる。

## 3. 国内メーカーの規格適合における留意点

鉄道製品等を輸出するにあたり、規格適合の必要性については、前述したとおりであるが、国内の鉄道製品等のメーカーが規格適合を行うに当たり、国内向け品質活動をそのまま適用するには課題がある。そこで、これまで鉄道認証機関設立以降対応した認証審査を踏まえ、国内の鉄道製品等のメーカーが規格適合の活動において望ましいと思われる点について述べる。

### 3. 1. PDCA サイクル

PDCA (Plan Do Check Action) は ISO 9001 において求められる活動であるが、鉄道の安全関連規格では、図 1 に示す通り、製品毎に求められる RAMS ライフサイクル全体に対して、PDCA が求められる<sup>2)</sup>。PDCA の各段階において国内メーカーが対応すべき点は以下の通りである。

#### 3. 1. 1. Plan

規格適合で求められる Plan は、Safety Plan、RAM (Reliability, Availability and Maintainability) Plan、Verification Plan、Validation Plan 等がある。これらを、製品毎に作る必要があるが、日本国内向けの製品においては、製品毎に明文化した形で作成されていないことが多いため、規格適合を行うにあたっては Plan を規格が求めている内容に沿って改めて作成することから始めることになる。

Plan は、規格適合を行うための基礎となるべき部分となることから、国内向け・海外向け問わず作成することが、規格適合を迅速に進めるためには必要不可欠である。また、Plan において RAMS ライフサイクル全般に用いる規格で要求している Technique / Measure の適用・非適用の宣言と、規格で Highly Recommend とされている Technique / Measure を

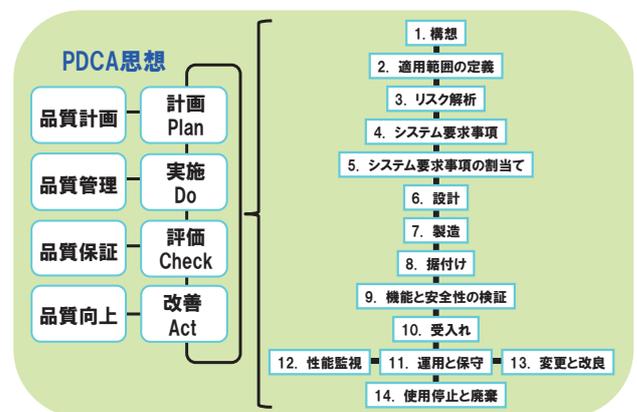


図 1 RAMS ライフサイクルと PDCA

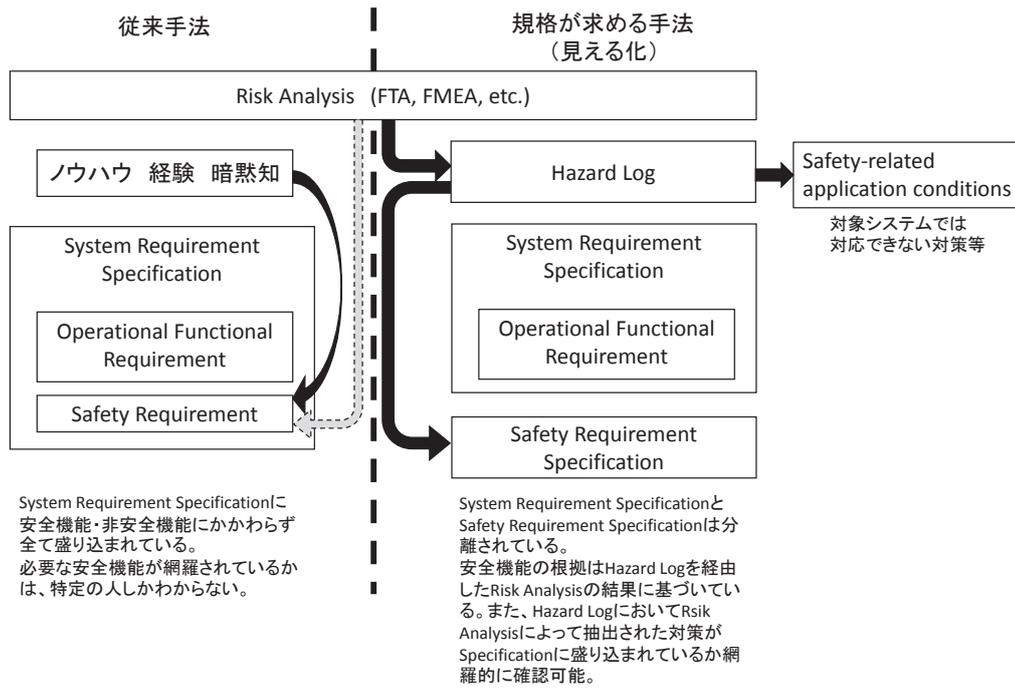


図2 従来手法と規格が求める手法との違い

非適用とした場合のその理由を記述する必要がある。

### 3. 1. 2. Do

規格適合で求められる Do は、Plan に基づき、開発を行うことである。このとき、Safety Analysis、RAM Analysis、System Requirement Specification、Safety Requirement Specification 等の設計開発文書が作成される。

Do で求められることは、Plan に基づき、Analysis、Requirement Specification、Test Specification 及び Test Report を実施・作成するとともに、これらのドキュメント間において計画や仕様等とのトレーサビリティが取れていることである。

旧来からの日本国内向けのやり方では、FTA (Fault Tree Analysis) や FMEA (Failure Mode and Effects Analysis) 等の Risk Analysis は行われているものの、System Requirement Specification は Operational Functional Requirement と Safety Requirement を含んだ形になっているため、Risk Analysis の結果と System Requirement Specification へのリンクが薄い。一方、Safety Requirement が今までの経験やノウハウ等から属人的に作られる傾向がある。そのため、これらを見える化することを目的としている規格への適合を行うにあたっては、旧来のやり方で実施した文書の「行間」あるいは「暗黙知」の内容を明文化する必要が生じる。(図2 参照)

### 3. 1. 3. Check

規格適合で求められる Check は、図3に示すとおり Verification と Validation である。ISO 9001 では、Design Review や照査・承認により対応をしていると考えられるが、鉄道の安全関連規格では、Verification Plan 及び Validation Plan に基づき、Verification 及び Validation を実施することが求められるとともに、規格で要求している Technique/Measure を適用することが求められている。

各 RAMS ライフサイクルの段階における Verification は重要であり、Verification の形骸化によりチェック漏れが生じると、その後の RAMS ライフサイクルの段階において漏れ等が顕在化すると修正箇所が広範囲に広がることになる。そのため、Verification を形骸化することは、規格適合の工数を

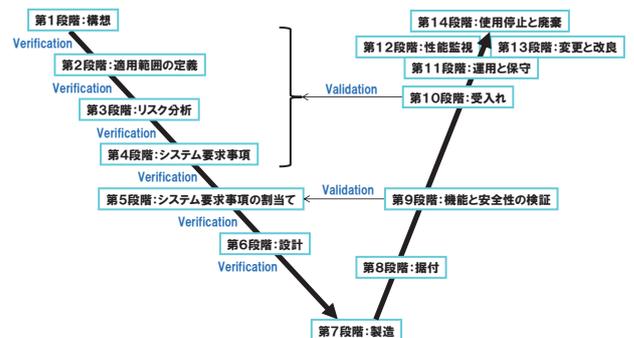


図3 RAMS 規格のVスキーム

結果的に増やすことになるため、Verification を確実に実施することが書類の変更に伴う工数を減らすことになる。

### 3. 1. 4. Action

規格適合で求められる Action は、Verification や Validation で指摘された内容に対し、改善を実施することである。Specification に対する改善や、Plan に対する改善、トレーサビリティに対する改善等が挙げられる。

前節で述べたとおり、上流の文書に影響する指摘が生じた場合、多くのドキュメントに対し影響を受ける可能性がある。そのため、各 RAMS ライフサイクルの段階において十分な Check を実施し、必要な Action を実施しておくことが、規格適合の工数を減らすことになる。

### 3. 2. Plan を積極的に変更

前節において、Check と Action の重要性を述べた。Check と Action の対象には Plan が含まれることがあるが、Plan の変更は多くの文書に影響を与える可能性があるため、消極的になる傾向がある。

しかし、Plan の変更を放置すると、RAMS ライフサイクルの段階を進んだ際、矛盾が大きくなり、結果的に修正を行う必要が出てくる。必要であれば、Plan の変更を積極的に実施するとともに、Plan の変更により影響をうける文書を最小化する工夫を検討することも必要である。

### 3. 3. 規格適合を行う開発体制

前節までは規格適合を行うに当たり実施すべきプロセス及び作成すべき文書に関する事項について述べたが、本節では、それを実行する開発体制の重要性について述べる。

規格適合を実施するに当たり、規格に基づく開発体制を構築する必要がある。規格では Designer、Verifier 及び Validator 等の独立性を求める場合がある。これに加え、RAMS 規格を遂行するにあたり、RAMS 管理者といった役割の要員を設定することがある。

日本のメーカーでは、設計者に、それも属人的に多くのノウハウが存在していることが多い。規格適合では、設計者のノウハウを明文化する必要があるとともに、設計者に対し Verification や Validation によって生じた指摘を実施させる必要がある。すなわち、RAMS 管理者から設計者に対し指示を出すことにな

るが、そのためには、RAMS 管理者に強力な指示権限を付与する必要がある。

規格適合に対し積極的に対応する権限を配分するこのような開発体制を構築することが出来れば、規格適合活動をより効率的に推進できると考えられる。

### 3. 4. 「ない」の明文化

設計図書類など、日本企業の従来の業務記録の仕方においては、実施不要と判断された技法や業務プロセスが記録として残されることが多い。しかし規格適合の審査においては、その様な記録の確認が必要となる場面がしばしば生じる。

実施しなかった事実の記録がないケースとして次の2点が考えられる。

- ・ 実施の可否を検討した結果、実施の必要がないため、実施不要。
- ・ 実施の可否を検討せず、未実施。

ここで、規格適合の観点では、前者と後者では意味が大きく異なる。すなわち、前者は明確に実施しなくてもよいことになるが、後者は実施すべきところを実施していない可能性があることになる。

そのため、Plan において、実施することが計画されている事項で、実施しなかった場合は、実施しない理由とともに、その記録を残すことが重要である。

## 4. おわりに

これまで鉄道認証機関設立以降対応した認証審査を踏まえ、規格適合の意義と活動において望ましいと思われる点について述べた。

国内向け品質活動に付け加える形で規格適合を行うと、実績ある既存の設計開発のプロセスに対し、多くの歪み生じると考えられるが、ノウハウや暗黙知の明文化を行う上でも、戦後米国発の品質管理を多くの企業が取り入れて自らの強みとしたように、是非とも、国内向け品質活動そのものに対し鉄道製品の安全関連規格の要素を盛り込んだ設計開発のプロセスの構築を検討いただきたい。

### 参考文献

- 1) 渡邊朝紀，“鉄道製品の調達と RAMS”，pp.17-20, 交通安全環境研究所フォーラム 2017, 2017 年 11 月
- 2) 田代維史，“鉄道の安全関連国際規格の動向と規格適合性認証”，pp.53-56, 交通安全環境研究所フォーラム 2014, 2014 年 11 月