

講演 4. 規格適合で求められるトレーサビリティの重要性について

鉄道認証室

※長谷川 智紀 田代 維史 渡邊 朝紀

服部 鉄範（客員専門調査員） 森 崇（客員専門調査員）

1. はじめに

近年、海外における鉄道関連プロジェクトにおいて、ISO (International Organization for Standardization, 英) や IEC (International Electrotechnical Commission, 英) に代表される国際規格、地域規格である欧州規格 (EN : European Norm, 仏) への規格適合が求められる。特に、RAMS (Reliability, Availability, Maintainability and Safety, 英) 規格として知られている IEC 62278¹⁾ や EN 50126²⁾、Safety Case 規格で知られている IEC 62425³⁾ や EN 50129⁴⁾、そしてソフトウェア規格として知られている IEC 62279⁵⁾ や EN 50128⁶⁾ が要求される。

交通安全環境研究所では、鉄道分野で国内初となる認証機関として、NRCC (NTSEL Railway Certification Center) を立ち上げ、IEC 62278、IEC 62279 及び IEC 62425 等の規格適合に関する認証業務を平成 23 年度から開始し、平成 24 年度に製品評価技術機構 (NITE : National Institute of Technology and Evaluation, 英) 認定センター (IAJapan : International Accreditation Japan, 英) より IEC 62425 に対する製品認証機関として認定を受けた。現在、認定を受けている規格は IEC 62278、IEC 62279、IEC 62280⁷⁾ 及び IEC 62425 の 4 規格になる。

これまで、令和元年 10 月 1 日現在、32 件の認証書の発行を行ってきたところであるが、旧来からの日本国内向けのやり方では、規格適合が困難になる可能性が高いことが分かってきた。

特に、前述の規格で共通として求められているものとして、トレーサビリティがあるが、旧来からの日本国内向けのやり方ではトレーサビリティを確保することが難しいと著者としては感じている。

そこで、本発表では、旧来からの日本国内向けのやり方においてなじみのない、トレーサビリティについて、その意義と重要性、並びに階層的な仕様と要件の細かさの平均化が求められる意義について紹介する。

て、その意義と重要性、並びに階層的な仕様と要件の細かさの平均化が求められる意義について紹介する。

2. トレーサビリティとその重要性

2. 1. トレーサビリティとは

業界や用途によってトレーサビリティの意味する内容は変わってくる。食品の世界では、「食品の移動を把握できること」⁸⁾を指し、計量の世界では、「個々の校正が測定不確かさに寄与する、文書化された切れ目のない校正の連鎖を通じて、測定結果を計量参照に関連付けることができる測定結果の性質」⁹⁾を指す。

そのため、本報告では、IEC 62278、IEC 62279、IEC 62425 において求められているトレーサビリティについて述べる事とする。

これらの規格におけるトレーサビリティとは、以下の点について確認することである。

- ・ 全ての要件が適切に満たされていること
- ・ 追跡不可能な事項が入り込んでいないこと

なお、IEC 62278 では、トレーサビリティについて明示的に要求はされていないが、図 1 に示す Verification 及び Validation において次のように定義がされており、実質的にトレーサビリティを求めている。

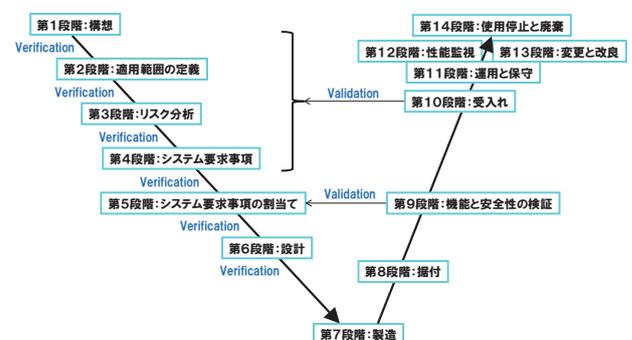


図 1 RAMS 規格の V スキーム

- **Verification** : 指定された要件が満たされていることの客観的証拠の調査及び提供による確認
- **Validation** : 特定の使用目的の特定の要件が満たされていることの客観的証拠の調査及び提供による確認

また、IEC 62425 では、**Verification** 及び **Validation** において次のように定義がされている。

- **Verification** : 検討中の段階の要件が、前の段階の出力を満たし、検討中の段階の出力がその要件を満たしていることを、分析及びテストにより証明する行為
- **Validation** : 製品が全ての要件を満たしていることを、テスト及び分析により証明する行為

このように、設定した要件が、各開発段階における入力・出力間で満たされおり、かつ製品が設定した要件を満たしているかを追跡すること、これがトレーサビリティである。これにより、要件の抜け漏れを防ぐことを規格は求めている。

2. 2. トレーサビリティを用いる意義

旧来からの日本国内向けのやり方においては、「ノウハウ」、「経験」、「暗黙知」に基づき安全性要件 (Safety Requirements) や試験計画 (Test Plan) が作られる傾向がある。この方法では、属人的になりやすい傾向があり、トレーサビリティがとりづらい仕組みになっている。ただし、属人的な要員が当該製品に対して終始一貫として携わることにより、当該要員によってトレーサビリティがとれてきた経緯がある。

しかし、少子高齢化がすすみ、従来の技術伝承のひとつである OJT (On the Job Training, 英) では、技術伝承の時間の確保が困難になりつつある。また、ノウハウをもつ要員の退職等もあり、旧来からの日本国内向けのやり方が限界に近づきつつある。¹⁰⁾

そこで、海外向け鉄道製品にかかわらず、属人的な仕様からの脱却とともに、仕様書の可読性を高める必要がある。その対策として、上位文書から下位文書へ、または下位文書から上位文書へ要件の追跡を可能とさせるトレーサビリティの確保が必要となる。標準的な関係を図 2 に示す。

ただし、トレーサビリティを確保するにあたっては、その手法に決まりがない。そのため、トレースを取るにあたり、次に示す注意すべき事項がある。なお、ここでは、要件の細かさを「粒度」と呼ぶこととする。

- 上位文書と下位文書の間で要件の粒度
- 複数の要件を、ひとつの要件のように記述
ひとつ目は、図 3 に示すように、上位・下位文書間で粒度が大きく違うため、トレース先が多くなり、トレース先のトレーサビリティの確実性が落ちることである。

ふたつ目は、図 4 に示すように、要件を複雑にすることにより、トレース元のトレーサビリティの確実性が落ちることである。

このように、トレーサビリティの確実性を高めるにあたっては、要件の記述方法に工夫が必要であり、その一手法として、**Formal Method** (形式手法) や構造化仕様があげられる。

そこで、次章では、このうち構造化仕様について述べる。

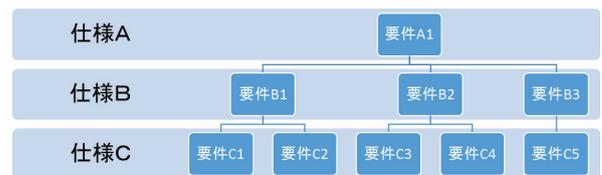


図 2 標準的な仕様の上下関係



図 3 仕様書間で粒度の差が大きい場合



図 4 複数の要件を一つの要件と表現した場合

3. 階層的仕様と粒度の平均化

RAMS 規格等では、仕様の階層的構築が求められている。これは、例えば、Software Requirements からソースコードを作った場合、図 3 に示すように、一つの要件から多数のソースコードとトレースを取ることにになり、

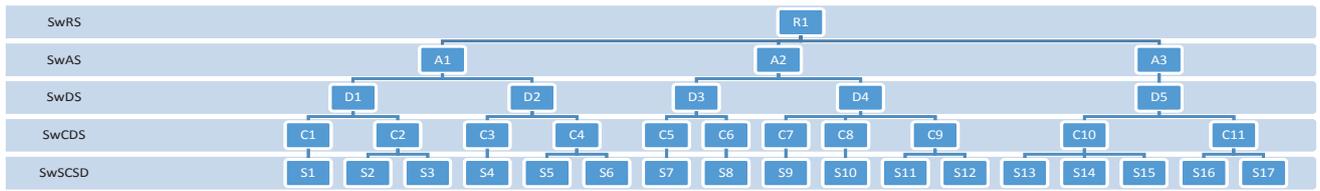


図5 IEC 62279 の階層的仕様を用いた要件の構造例

要件に対する網羅性が低くなる可能性が生じる。また、Software Requirements を詳細に作成する必要があり、要件の網羅性が低くなる可能性がある。

そこで、規格では、仕様を段階的に細かくする階層的仕様による開発が求められている。例えば、IEC 62279 では、求められているドキュメントとして次のものが挙げられる。

- Software Requirements Specification (SwRS)
- Software Architecture Specification (SwAS)
- Software Design Specification (SwDS)
- Software Component Design Specification (SwCDS)
- Software Source Code and supporting documentation (SwSCSD)

このように階層毎に文書を複数作成することにより、仕様書間の粒度の差を極力少なくし、要件のトレーサビリティを確保しやすくすることができる。(図5)

また、各仕様書の要件が整理されることになるため、仕様書における要件の実現を確認するテストの網羅性を確保することが可能になる。IEC 62279 では次のテスト関係のドキュメントが求められ、それらは各種仕様書とトレーサビリティが求められる。(図6及び図7)

- Overall Software Test Specification (OSwTS)
- Overall Software Test Report (OSwTR)
- Software/Hardware Integration Test Specification (SwHwITS)
- Software/Hardware Integration Test Report (SwHwITR)

- Software Integration Test Specification (SwITS)
- Software Integration Test Report (SwITR)
- Software Component Test Specification (SwCTS)
- Software Component Test Report (SwCTR)

なお、システムレベルにおいては、RAMS 活動の成果物として IEC 62278 において規定はされ、要件とのトレーサビリティを求めているが、IEC 62279 のような文書同士の明確なトレーサビリティに関する記述は見当たらない。

そのため、現状における RAMS 活動として作成すべき文書が不明確であることから、RAMS 活動を行う関係者によっては、規格の解釈により各文書において要件の粒度に違いが生じてしまう状況が見られる。

トレーサビリティを確保するためにも、各要件の粒度は均等になるよう仕様書を作成することが望ましいと考える。

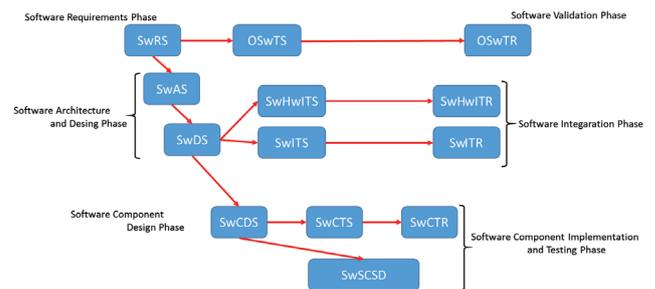


図6 IEC 62279 におけるトレーサビリティの関係

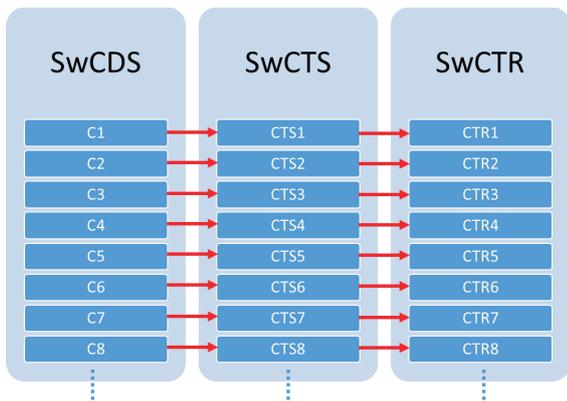


図7 仕様書、テスト仕様書及びテスト報告書の関係
(SwCDS、SwCTS 及び SwCTR の場合)

4. まとめ

これまで鉄道認機関設立以降対応した認証審査を踏まえ、規格適合におけるトレーサビリティの意義と重要性、並びに階層的な仕様と粒度の平均化に係る意義について述べた。

トレーサビリティの確実性を高めるにあたって、階層的仕様による上位・下位文書間の差を少なくするとともに、各仕様における要件の粒度を平均化することが重要であることを述べた。

海外向け鉄道製品にかかわらず、トレーサビリティは製品品質の確保において重要な活動であると考えられるため、国内向け製品に対しても積極的な適用、及びさらなる取り組みの向上を検討いただくことによって、これまでの国内向けのやり方の限界へのブレークスルーの一助になるとともに、国内向け鉄道製品及び海外向け鉄道製品の区別無い設計開発の構築を期待する。

参考文献

- 1) IEC 62278:2002: “Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)”
- 2) EN 50126:1999: “Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS). Basic requirements and generic process”
- 3) IEC 62425:2007: “Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling”

- 4) EN 50129:2003: “Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling”
- 5) IEC 62279:2015: “Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems”
- 6) EN 50128:2011: “Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems”
- 7) IEC 62280:2014: “Railway applications - Communication, signalling and processing systems - Safety related communication in transmission systems”
- 8) <http://www.maff.go.jp/j/syouan/seisaku/trace/>
- 9) <https://www.nite.go.jp/iajapan/aboutus/gijutsu/trace.html>
- 10) 長谷川ら: “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”, pp.17-20, 交通安全環境研究所フォーラム 2018, 2018年12月