

IEC61508に則ったシステム安全に関する取り組み

○ [土] 井上 淳太(西日本旅客鉄道株式会社)

田口 研治 相馬 大輔(独立行政法人産業技術総合研究所)

The measure about the system safety in accordance with IEC61508

○Junta Inoue, (West Japan Railway Company)

Kenji Taguchi, Daisuke Souma(Advanced Industrial Science And Technology)

We are advancing development and introduction of the train approach alarm system which utilized GPS as a hard measure against Railroad human body obstacle accident. Although this system is introduced as auxiliary equipment, when a railroad human body obstacle accident occurs temporarily from playing the role of protecting a human life, it is recognized as accountability being called for also about equipment.

キーワード: IEC61508, GPS式列車接近警報装置, FTA, FMEA

Key Word: IEC61508, GPS type train proximity warning device, FTA, FMEA

1. はじめに

当社では触車事故防止のハード対策として、GPSを活用した列車接近警報システムの開発・導入を進めている。

本システムは補助装置として導入されているものの人命を守るという役割を担っていることから仮に触車事故が発生した場合、装置に関しても説明責任が求められると認識している。そこで、安全性を意識したGPS式列車接近警報システムの構築について、独立行政法人産業技術総合研究所(以下産総研)様に第三者機関として関与いただきながら以下のような取り組みを実施したのでその概要を報告する。

2. システム構築における課題

2.1 システムとは

近年、エレクトロニクスの急速な進展に伴い大規模なソフトウェアとGPS、センサ、通信デバイス等が融合して高機能で様々な付加価値を提供するシステムが我々の生活に多く登場するようになってきている。こういったシステムの特徴は、デジタル処理をベースに周辺デバイスと機能統合している点が特徴であり、その機能統合を実現する手段としてソフトウェアが活躍している。

近年、鉄道においても、鉄道固有技術に依存しない

汎用技術や汎用ネットワークを用いたシステム(汎用システムと表現している)が運輸、車両、施設、電気の各部門において導入されており、人手に依存していた業務がシステムに置き換わるなど業務の効率化が進められている。

2. 2 V字モデル

一般にシステム構築は、図-1のようなV字モデルのプロセスを経て構築される。システム構築は発注者が要求仕様を定義するフェーズからスタートし、受注者(メーカー)による設計・実装・テストを経て完成に至る。従って、前工程である発注者の要求仕様が精緻に記載されていなければ必然的に後工程に悪影響を及ぼす為に安全性の高いシステムを構築する為には要求仕様の精度を向上させる必要がある。

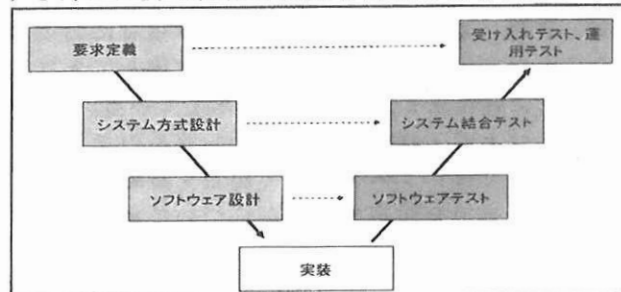


図-1 V字モデル

2.3 要求仕様を我流で書く

この汎用システムは、鉄道固有技術に依存しない為、ユーザー部門毎で構築されるのが一般的である。構築にあたっては、要求仕様を精緻に書く技術が求められるが、これまで社内における要求仕様に関する教育システムはなく、我流で作成しているのが現状であり改善すべき課題であると認識している。

3. 要求仕様に起因するシステムトラブル

要求仕様があいまいであったり、漏れがあることでシステムトラブルに至る例は少なくない。図-2は要求仕様がどのシステム構築フェーズで発見されたかを表したものであるが、最終テスト工程において発見されているケースもある。後工程で発見されれば、前工程に立ち戻って再設計、実装、テストというフェーズを再度とる必要があり、手戻りともいえる。システム構築には、納期がつきものであり、スケジュールプレッシャーがシステムの安全性に悪影響を及ぼすことも限らない。以上のことから、安全性の高いシステム構築を目指すためには、まず、発注者自身が要求仕様を精緻に書くことが前提であると認識した。

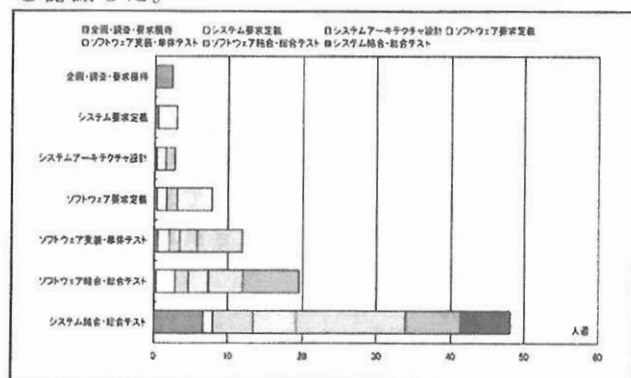


図-2 工程別不具合発見数比率

4. 要求仕様を精緻に作成

4. 1 IEC 61508

IEC 61508とは、電子機器システムに関する国際システム安全規格でシステム構築の工程をシステムのコンセプトから始まり、設計、据付、運用、保守、修理、変更、廃棄に至る全16項目におよぼ安全ライフサイクルから成り立つと定義して各フェーズ毎に文書作成と文書管理を要求している。

図-3は上流工程について抜粋したものである。フェーズAでは、リスクとして想定する範囲をあらかじめどこまでを想定するのかについて謳われており、物理的設備、サブシステム、ヒューマンエラー等について記載することが求められている。次にフェーズBでは障害の発生、誤使用時におけるリスクの発生、危険事象に至るまでのシーケンスの確定、さらには危険事象の可能性の評価をしてリスクの見積りと評価をすることが求められている。そして、

フェーズCにおいてフェーズBにおいて見積もった危険源について安全機能を特定すること、確定した個々の危険源に関して必要なリスク低減を確定することを要求仕様に明記するように謳われている。つまり、安全性の高いシステムを構築するためには仕様書作成の前段階に安全分析を実施することが必要であり、頭で想定している安全対策を文章で要求仕様書に記載するだけでは不十分であると認識することができる。

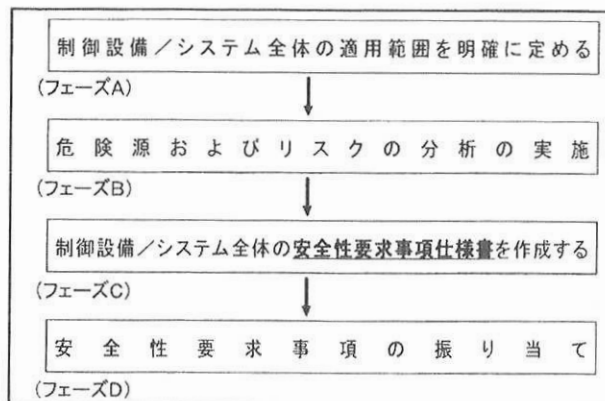


図-3 IEC 61508の上流工程

4. 2 ハザード分析

IEC 61508では各工程における実施要件について記載はされているものの、要件を満たすための手段や考え方については丁寧な記載がない。そこで、米国のシステム安全の第一人者であるナンシー・G・レブソンの考え方を参考とすることとした。

ハザード分析に際しては、システム、サブシステム間のインタフェースを調査し相互的な作用が全体システムにどのように影響を与えるかを判断する為に環境、人間による操作及び機器に関連する個々のハザード分析を要求しており、その為に分析に必要な技術や知識としては、システム及びサブシステムに関するハードの知識、信頼性技術、安全技術、アプリケーション技術、運用及びシステム管理者の実態・知識を挙げており、多面的な角度から分析が必要であるとしている。以上の分析を踏まえて、要求仕様に盛り込むべき事項としては、ヒューマンインタフェース要件、セーフティクリティカルなコンポーネントの識別、セーフティクリティカルなソフトウェア要件が必要であると言及している。従って、要求仕様の作成前にシステム及びシステム間の分析からスタートすることとした。

5. 危険源及びリスク分析

5. 1 FTA、FMEA

一般にFTAは、トップダウン手法で、FMEAはボトムアップ手法の為に両方を組み合わせて実施することが有用であるとされている。

FTAについては、組み合わせによる影響を評価
 できることからシステムとそれを操作する人の関係
 の中でどのようなリスクが潜在しているかを分析す
 るのに有用である。人との関係を分析することが主
 体であるので我々事業者が主体となって実施するこ
 ととした。

一方、FMEAについては個々のコンポーネントについて故障や誤りといった不具合が発生した場合に全体のシステムにどのような遷移し、結果としてリスクが顕在化するかどうかという観点で分析する為にコンポーネント自体にノウハウのあるメーカー主体で実施することとした。

5. 2GPS式列車接近警報システム

本装置は、あくまでも列車見張員による列車接近連絡を基本として補助装置的な役割を担う位置づけで列車見張員へ携帯させている。列車接近連絡になんらかのヒューマンエラー、例えば、列車の接近連絡を怠った場合においてもGPS式列車接近警報システム（以下GPS式列近とする）の携帯端末が鳴動することで列車の接近を最終的に認識することが可能となり、触車事故を防止することが可能となる。（図-4、図-5）

《コンポーネントの主な機能》

- ・ 列車情報伝達装置

列車情報である列車番号、線別、軌道回路等を上位装置から取得して制御サーバーへ送信する

- ・ 制御サーバー

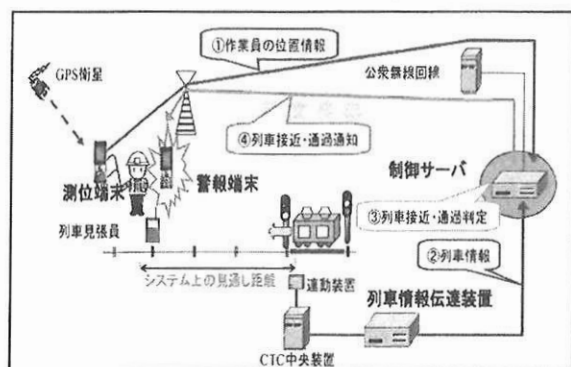
列車情報伝達装置から列車情報、携帯端末から作業員の位置を取得して列車接近判定を行うと共に携帯端末へ接近情報を報知する。

- 警報端末

制御サーバーと一定周期で常時通信を行うと共に、制御サーバーからの警報通知を受けて、保守係員に対して音声と警報音により接近情報を報知する。

- ・ 測位端末

GPS情報を基に作業員の位置を算出して制御サーバーに送信する。



图—4 GPS式列近



图-5 携带端末

6. FTAの実施

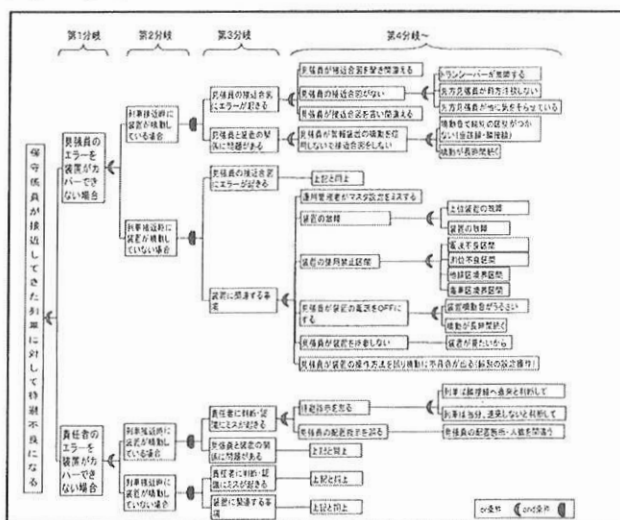
6. 1 分析の着眼点

本装置の目的は、列車見張員がGPS式列車を所持することで列車の接近を装置の警報からも取得することが可能になり、ヒューマンエラーが生じた場合でも列車の接近を適切に認識でき、待避不良に至らないことである。

逆に待避不良に至るケースとしては、装置と人の関係の中で問題が生じている場合と想定できる。従って、装置と人の関係に注目して分析をすることとした。

6. 2 第 1 分岐～第 3 分岐

人の問題についてはヒューマンエラーとした。一方、装置については、列車見張員が所持する端末が鳴動しているにも関わらず見張員が適切に行動せずに待避不良に至るケースがあると想定して、分析を進めることとした。装置が鳴動していない場合においては、装置に起因する問題なので装置に関連する事項と分析した。



图—6 FTA

6. 3 対策の方向性

FTAから浮かび上がった課題については分類化して、追加機能として要求仕様に盛り込む必要のある項目について絞り込みを行った。

《要求仕様へ盛り込む事項》

- ・ 鳴動パターン

作業員と列車の位置状況における鳴動パターンの網羅性検証が必要と認識した。

- ・ 鳴動音の設定

ユーザー検証が可能なように音量可変設定が必要であると認識した。

- ・ 使用禁止区間

運用ルールで対処する前に注意喚起機能を付加することが必要と認識した。

- ・ 運用・保守

マスタデータの入力値チェック、アクセス権限の設定が必要であると認識した。

7. FMEAの実施

7. 1 分析の実施

本システムは、ソフトウェアに様々な処理を行っていることから、ソフトウェアが何らかの原因により異常なふるまい（ここでは、ハザードと定義した）が生じた場合、最終的にどのような影響が生じるかという観点で抽出した。なお、各項目の概要は以下の通りである。

表ー1 FMEA

コンポーネント	機能	ハザード	原因	局所影響	最終影響
サーバー	作業員位置算出	キロ程、エリア算出機能の停止	・バグ ・ハード障害	サーバー内でキロ程エリア算出できない	使用できない
		マスタから基礎データを読めない	・バグ ・ハード障害 ・その他	サーバー内で基礎データを読めない	・誤鳴動 ・鳴動遅延 ・鳴動せず
		マスタから基礎データを照って読む	・バグ	サーバー内で基礎データを照って読む	・誤鳴動 ・鳴動遅延 ・鳴動せず
		マスタから基礎データを避れて読む	・バグ ・過負荷 ・ネットワーク障害	サーバー内で基礎データを避れて読む	・誤鳴動 ・鳴動遅延 ・鳴動せず
		キロ程メモリに書けない	・ハード障害	サーバー内で基礎データをメモリに書けない	・誤鳴動 ・鳴動遅延 ・鳴動せず

- ・ 機能

ソフトウェアのタスクレベルでのふるまいを抽出した。

- ・ ハザード

処理不能、処理停止、誤処理、遅延処理という観点で機能が遷移する可能性があるかどうかを検証して、あると想定される場合には明記することとした。

- ・ 原因

ハザードを起こす原因としては、バグ、過負荷、ハード障害、ネットワーク不具合で大部分を占めるであろうと想定してあらかじめ項目に明記して選択することとした。

- ・ 局所影響

ハザードにより直接的に生じる影響を明記した。

- ・ 最終影響

ハザードにより最終的に生じる影響を明記した。なお、最終影響としては危険側遷移である誤鳴動、

鳴動せず、鳴動遅延を重大影響として考慮することとした。

7. 2 対策の方向性

ソフトウェアに処理遅延、誤処理、処理停止に3つのハザードが生じるとシステムが危険側に遷移することが分かっている。しかし、ソフトウェアにハザードが生じていることを検知することは難しい。そこで、ハザードの原因となる事象を抽出し、その原因となる事象が発生したことによりハザードを検知できないか検討した。

《要求仕様へ盛り込む事項》

- ・ ハードに過負荷が生じた場合

監視端末からサーバーのCPUに過負荷が生じていることを検知してユーザーが所持している携帯端末にハザードを通知する。

- ・ ハードが故障した場合

監視端末及びユーザーが所持する携帯端末においてハードの故障を検知してハザードをユーザーに通知する。

- ・ バグに関して

ソフトウェアは人間の産物故にバグのないソフトウェアは理想であるものの、完全にバグがないシステム構築するのは難しいと認識している。一方で、ソフトウェアの品質向上の観点からは、設計の品質を向上させ、しっかりとしたテストを実施することは重要であるとされている。

従って、バグに対しては要求仕様の提示だけでなく、テストフェーズの中で事業者としての有効となるような関与を現在、検討している。

8. さいごに

本取り組みを通じて、安全要求仕様の記述においては前段階の分析の重要性を理解することができた。又、頭で分かっているつもりでも仕様書に漏れが結果として生じており、分析の重要性を身も持って体感することができた。まだまだ、本取り組みは途についたばかりであり、システムの安全性向上にむけて一歩ずつ課題を克服していきたいと考えている。

最後に（独）産総研の田口様、相馬様には様々な面でご指導いただきましたことを厚くお礼申し上げる次第である。

参考文献

- 1) IEC 61508
- 2) ナンシー・G・レバソン セーフウェア
- 3) 経産省 H22 組込みシステム産業の実態把握調査
- 4) 安全技術応用研究会 安全システム構築