## 3.3 テストパターンの整備に関する教訓（T3）

教訓 T3

### 現場をよく知り、現場の知識を集約し、現場の動きをシミュレートできるようにすべし！



#### 問題

ある鉄道会社の制御系システムの事例である。駅に出入りする列車の運転は、駅に設置してある列車制御システムにより制御が行われている。折返し運転のある駅で、A 列車が折返しホームに入り、乗客の乗降後、出発時間となったので、元来た方向に出発していった。同じホームを使用する B 列車が A 列車の出発後、反対方向から近づいて来た。しかし、A 列車が出発していったにも関わらず、ホーム手前の信号機が B 列車の「進入」を表示しなかったため、B 列車は、ブレーキが自動で動作し駅の手前で停止してしまった（図 3.3－1）。

#### 原因

直接の原因は、列車制御システムのソフトウェアのバグである。先行の A 列車の出発完了にも関わらず、A 列車に対する制御信号が出続けてしまったため、続行の B 列車がホームに接近したにも関わらず、B 列車の制御信号の表示ができなかったためである。

制御系システムは、一般に、制御対象の様々な「処理の動きとタイミング」をすべて捉え、その動きすべてに明確な制御・指示（コントロール）ができなければならない。

このような列車の動きを想定した本番と同じようなテスト環境を準備することは、困難であるため、システムの本稼働が開始する前に実列車を用いてテストを行ってはいたが、今回の事象のようなケースのテストは行っていなかった。

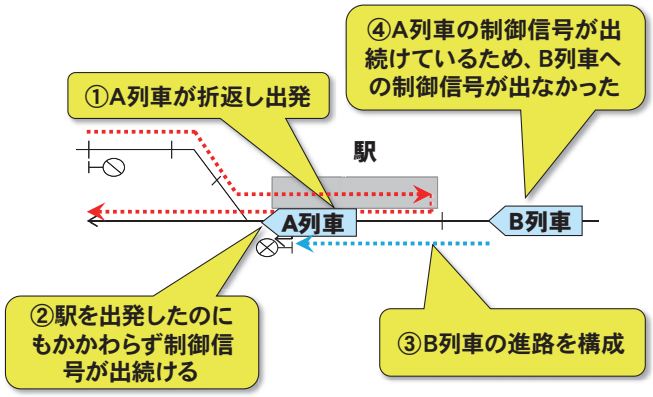


図 3.3－1　駅での障害発生状況

今回の事象を分析すると、根本原因は以下であることが分かった。

【原因 1】有識者（ベテラン社員を含む）により、以下のとおり制御信号の機能確認を行っても、まだ洗い出せていない機能が存在する。（機能要件漏れ）

- 有識者（ベテラン社員を含む）による要件確認。
  機能要件作成時にあらゆるパターンの洗い出しを有識者に実施。
- 有識者による要件&テスト仕様レビュー。
- 有識者による思いもよらない入力テストを実施。（意地悪テストの実施）。

【原因2】列車の動き、信号システムの動作などを総合的にテストできる環境、つまり、組込みソフトウェアを持った制御システムと列車などの動作のすべてのテストが行えるテスト環境ができていない。

## 対策

直接の対策として、駅の列車制御システムの制御信号送信プログラムを改修した。

今回のように、列車の運転を考慮したテストを行わなかったことにより、重大な列車運転阻害を招く可能性がある。まさしく、「現場」を熟知することが、「安全、信頼」を堅牢なものとする条件である。

【原因 1】については、従来から行ってきていた作業に加えて、一度設計された「機器の動き（列車の運転）」のパターンを知識データベースとして蓄積し、そこに、さらに新しい動き、機能漏れの動きを追加登録していく。これにより、すべての「機器の動き」のパターンを知識データベース上で把握することが可能になり、暗黙知が形式知化される。

【原因 2】については、本番環境と全く同じテスト環境を用意し、すべてのタイミングの問題点を実機や操作員で確認することは不可能である。そこで【原因 1】の制御装置の動きのパターンの知識データベース化が進めば、シミュレーション・システムの強化が可能になる。

制御系システムのシミュレーション・システムの開発を行うためには、現実の制御装置のプロセスを分かりやすく可視化し、プロセスの骨子を見極めてモデリングする。特に、微妙なタイミングを問題にするテストは、実機で再現することは難しいが、シミュレーションでは容易に再現することが可能である。

【補足説明】知識データベース

知識データベースとは、ここでは過去の制御装置、移動装置、操作員の「動き」のパターンを記録することを指す。この制御系システムに新しい要件を追加する場合、この知識データベースの記録や、有識者からの新たな知識を参照すると、設計時の考慮漏れやリスクの洗い出しができることを目指したものである。

## 効果

以下の効果を得ることができる。

- 知識データベースにより、機能漏れを防ぐことができる。
- シミュレーションにより、特殊ケースでの障害を防ぐことができる。

これにより、堅牢な「安全、信頼」の制御系システムを構築でき、事例で起きた社会インフラの混乱回避が期待される。

今回の事例は鉄道についてであるが、このような制御系システムは、工場における生産ライン制御、電力の供給ライン管理制御、通信の交換機制御など、世の中に数多く存在している。多くの制御システムにおいても、今回の列車の運転にあたる被制御機器の動作について熟知し、その動作に対するテスト項目をたてテストするだけでなく、シミュレータを使用したテストも行うことは、制御システムの品質を高める上で欠くべからざるものである。まさしく、「現場」を熟知することが、「安全、信頼」を堅牢なものとする制御システムの条件である。

## 教訓

現場をよく知り、現場の知識を集約し、現場の動きをシミュレートできるようにする、そのためには、機能要件の蓄積と実地テストができないためのシミュレータテストを考慮することによって、障害を予防することが重要である。