タイトル：STAMPのコントロールストラクチャーを考える

～コントロールストラクチャー作成の課題とその克服方法を、鉄道踏切事例を通じて解説～

まえがき

STAMP/STPAの実践にあたってよく言われるのは、制御構造図（コントロールストラクチャー）を作るのが難しいということである。制御構造図は、一言でいうと、「安全目標を達成するための機能を図で表現（可視化）する」ということであって、物理モデルでもシステムモデルでもない。ものづくりで大事なハードウェアを組み合わせた物理モデルから、安全目標を達成するための機能を分解・抽象化して組み合わせた機能モデルへ視点を変えて表現しなければならない。多くのエンジニアにとって、物理モデルは書きやすいが、機能モデルは難しいというのが実情であろう。

本稿では、IPAのシステム安全性・信頼性分析手法WGでまとめた「はじめてのSTAMP/STPA（実践編、2017年）」の中の鉄道踏切とりこ検知システムの分析事例を例に、制御構造図の作り方に関する経験を紹介する。ここで、“とりこ”とは、踏切が閉じた状態で、線路内に残された人や物などを意味する。この分析の後の2019年に、京浜急行の踏切内で動けなくなった大型トラックとの衝突事故が起きたが、これに記憶のある方もおられよう。ここには、とりこ検知装置が備わっており、570m手前の特殊信号発光機でとりこの存在に気づくことができる設計になっていた。時速120km/hの標準走行時の制動距離は517.5mであり、直ちに非常ブレーキをかければ停止可能な距離であったが、1.6秒の余裕しかなく、運転士は常用ブレーキでの停止を行ったため、停止が間に合わず衝突に至ってしまった。ただ、衝突はしたものの、ブレーキの効果はあり、人命の喪失までには至らなかったことは不幸中の幸いではあった。この事故の後、運転士の操作規定を変更し、「従来、特殊信号発光機の点滅を確認した場合、「速やかに停止」としていたが、今後、「直ちに非常ブレーキ」とする」という記事が出ている。「速やかに停止」だけでは、常用ブレーキ操作なのか、非常ブレーキも併用かの運転士の判断が必要とのことである。実際にどのような操作規定になったかは調べる伝手はなかったが、2023年頃に近所の踏切に下記のようなポスターがあり、一日だけであるが、監視員が無理な横断を抑制する安全キャンペーンのようなものが行われていた。年間18000件ものとりこ検知警報があるとのことで、急ブレーキによる乗客の転倒事故や、列車の運行遅れのような事態を考えると、単純に踏切事故を防ぐために非常ブレーキをかけて急停止するのでは問題解決には至らず、難しい判断が必要とされる。

本稿では、このような状況下でSTAMP/STPAがどのように役立つかを紹介してゆきたい。

図1　無理な鉄道踏切横断を避ける安全キャンペーンポスター

2017年のWGで最初に作成したのは、下記のような制御構造図である。とりこ検知装置の効果と事故防止効果を評価するためには、このような制御構造図は自然な形といえるかもしれない。

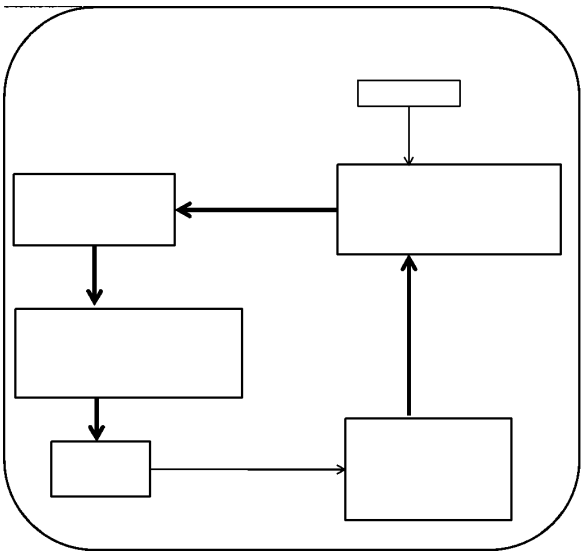

図2　コントロールストラクチャー図（初期のとりこ検知装置中心の案

一方で、「WGの中で、この制御構造図はSTAMPを見慣れた立場からは少し違っているようにみえる」とのコメントがあり、運転士を上位に据えた次図のような制御構造図を考えた。運転士中心の制御構造図という名称で報告書に載せているが、よくよく考えてみると、踏切事故を低減するという本来の目標からすると、とりこ検知装置そのものより、運転士の役割の方が大きく、次図のような制御構造図が自然であることが分かる。ここまで機能を抽象化して、事故防止効果を分析すると、特殊信号発光機を通してとりこの検知結果を知らせるだけでなく、今の通信技術の進歩を考えて、踏切内の映像を運転士に直接提示できれば、より効果的な運転操作ができる可能性まで指摘ができる。

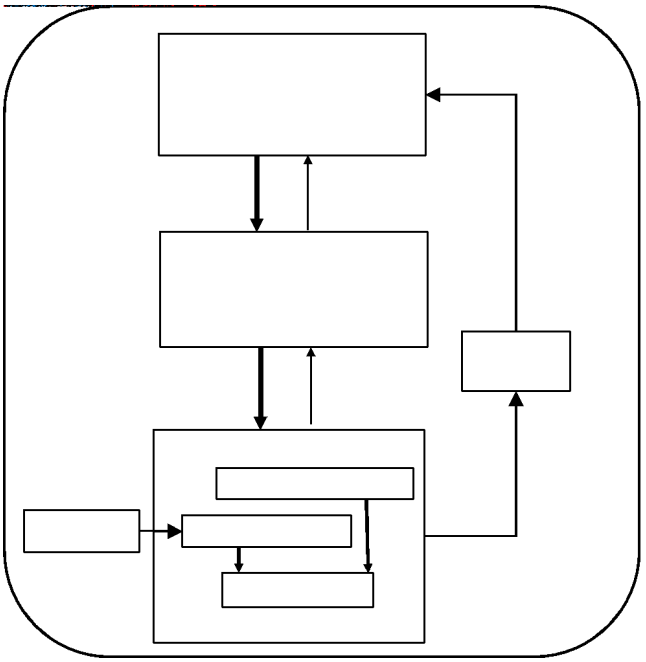

図3　コントロールストラクチャー図（運転士中心）

以上までが、2017年のWGで考えたことであり、安全工学誌の総説（Vol.62、No.3、2023年）で概説している。一方、前述のような2023年3月の京浜急行踏切での安全キャンペーンを見て、改めて制御構造図を考えてみると、下図のように、運転士のさらに上位の組織としての運転管理部門の安全責任がより大きいことが分かる。2017年の制御構造図での安全責任に追加すべき新たな安全責任を朱書きで示してある。運航速度の管理、緊急時の運転手順の整備、乗客の安全、利用者の利便性など多様な側面での安全管理が重要になる。

ここで示した三つの制御構造図は、どれが正しいかを単純に言えるものではないが、少なくとも、安全目標（とりこ検知装置の安全性、運転士の立場からの踏切事故の抑制、運行管理の立場からの踏切事故と乗客の安全

性、鉄道としての利便性など）を考慮したうえで、それを実現する制御構造図を描いてゆくことが必要になる。ハードウェアに注目したモデル図では、設計の詳細は分かっても、システムが本来果たすべき安全目標が見えにくくなる。つまり、安全目標が説明できるような機能モデルが必要になるということである。

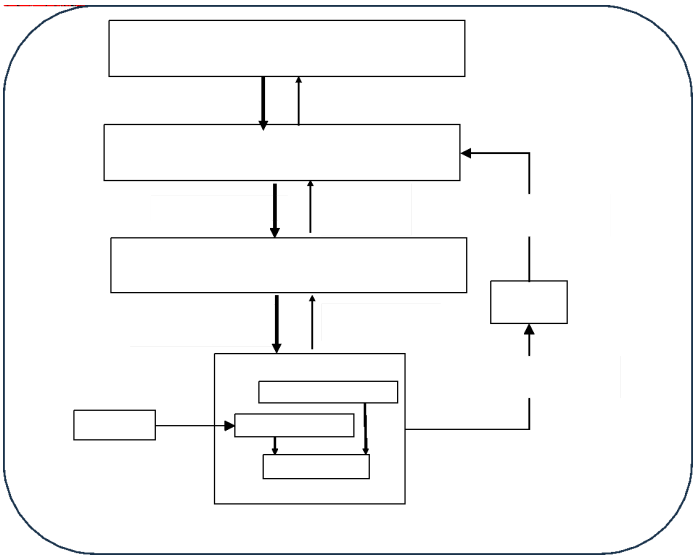

図4　コントロールストラクチャー図（管理部門の追加）

あとがき

STAMPでは、安全目標とそれを実現するための（安全）制御構造図の可視化が大事になる。「可視化」と書いたのは、制御構造図の各コンポーネントの安全責任が明確になっていること、安全責任を果たすための制御指示（コントロールアクション）と、それを作るためのフィードバック情報（FB）が明示化されることが必要なためである。コンポーネント間の矢印をすべて制御指示としてしまうのは、問題解決を煩雑にするだけであり、CAとFBの峻別も大事になる。

別コラムでも述べたように、安全目標と安全責任を明記した制御構造図だけでも、システム全体の安全性を改善するための十分に有効な手段となる。UCA（非安全コントロールアクション）やLS（Loss Scenarios）、コンポーネント安全対策などは、制御構図作成の後に、大事なものから順次作成・レビューをしながらシステム全体の安全を改善してゆくのも一策であろう。

以上（2025/8/22　兼本　茂）