タイトル：STPA 分析での「状況（Context)」の考え方と取り扱い方法

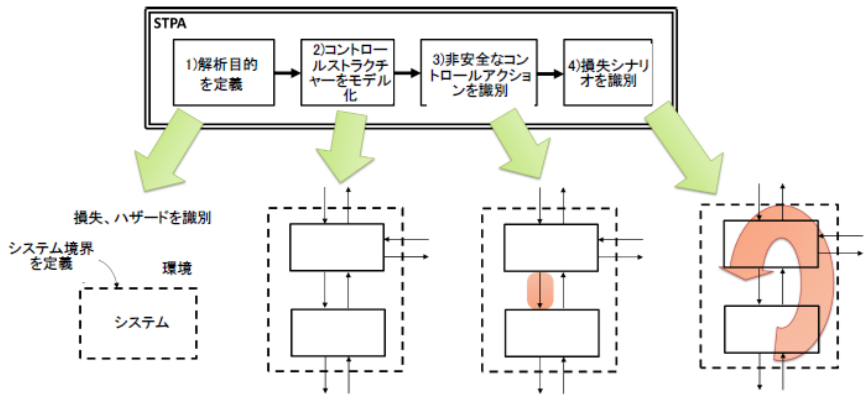
まえがき

STAMP・STPA という新しい安全分析手法に注目が集まっている。その手順は、下図に示すような四つのステップからなっている。この手順での大きな特徴は、Step-3 の非安全コントロールアクション（UCA）と Step-4 の損失シナリオ(LS)が、自然言語で表現されることである。

従来の FTA や FMEA では、キーワード（単語）による事象の記述が主であり、記載のあいまいさが軽減され、事象の経緯（シナリオ）の表現が厳格になっており、その審査やレビューがしやすいが、専門知識のない人にはわかりにくいという課題がある。

一方で、STPA でのシナリオによる事象の説明は、深い専門知識を持たなくとも理解しやすい。一方で、自然言語特有のあいまいさが残ることが問題になる。特に、シナリオ内に含められている暗黙の状況設定が残されがちな点に注意が必要である。この記事と同じコラムに掲載の「UCA(Unsafe Control Action)の識別のコツ」では、UCA での状況（Context）の明示的表現の大事さが指摘されている。

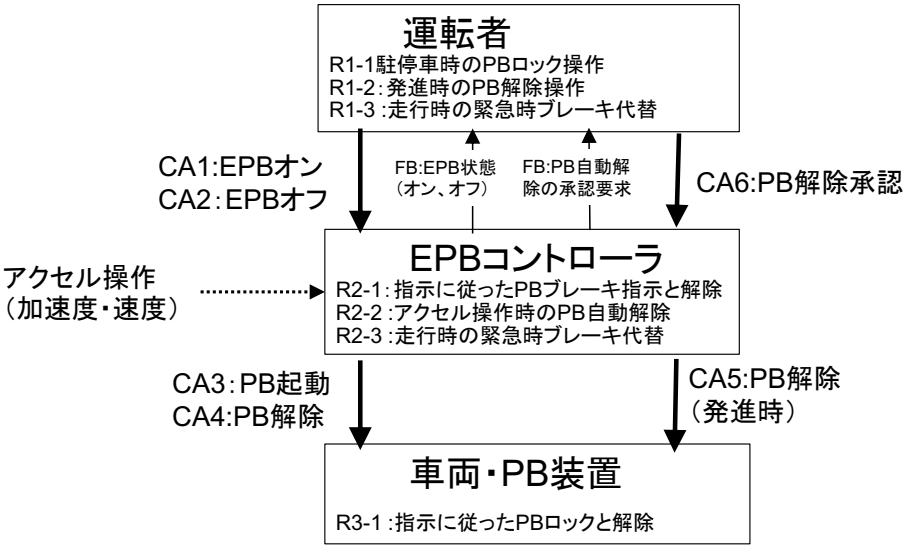
本稿では、STPA 全体にわたっての「状況」の明示的表現の大事さと、同時に、いろいろな表現方法があることを例示したい。併せて、自動車の電子制御の安全規格 ISO 26262 の関連規格である ISO 21448 （SOTIF、意図した機能の性能限界や合理的に予見可能なミスユースに係る規格)での事故シナリオの表現との関連も例示する。



STPA の四つの手順（STPA Handbook）https://psas.scripts.mit.edu/home/books-and-handbooks/

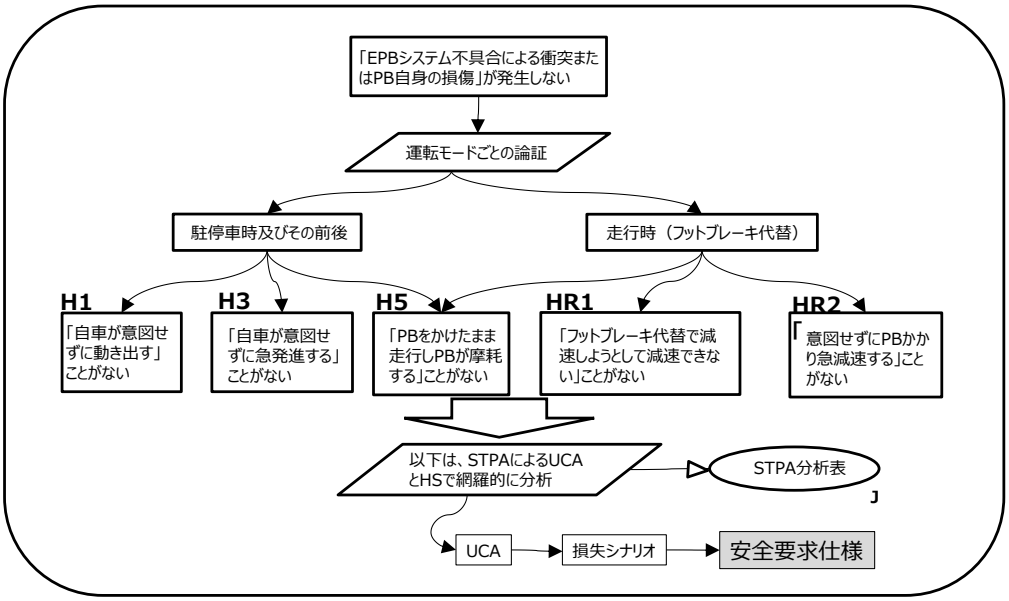
EPB システム（パーキングブレーキの電子制御）の事例

ここでは、安全工学誌掲載の「システミック思考による複雑システムの安全分析」（Vol.62,No.3,2023）で紹介した EPB システムの安全分析事例を紹介する。EPB では、下図に示すように運転者はコンピュータを介して電子制御で PB(パーキングブレーキ)を制御する。そこで、仮想的な機能として、発進時の PB 解除忘れの防止のために、アクセルを踏んだ際に PB がかかっていた場合、コンピュータが判断して自動解除する機能を付け加えてみた。この機能は、コンピュータが自分で判断するのではなく、「解除が必要な場合に運転者の許可を得てから解除指示を出す」という人間優先制御の考え方を取っている。



EPB システムの制御構造図（人間優先の制御アクション（CA））

ところが、PB は駐停車時だけでなく、道路走行時に通常ブレーキの代替として使われる場合もあることに気が付く。この場合、通常ブレーキを踏んでいるつもりでアクセルを踏んだりするとブレーキが利かないと判断し、代わりに PB を操作するといった操作ミスが考えられる。その際は、せっかく操作した PB が解除されてしまうことになる。つまり、PB 解除というのは「状況」依存で、安全にも危険にもなってしまう。STPA 分析の UCA を考える場合にそれがハザードに至るかどうかは状況依存ということである。そのために、UCA ごとに「状況」を定義するのではなく、下図のように、事故につながるハザード状態の時点で、「状況」を駐停車時と運転時に分類してから STPA 分析を進めてみた。このような整理により UCA や続く LS のシナリオ記載が容易になる。



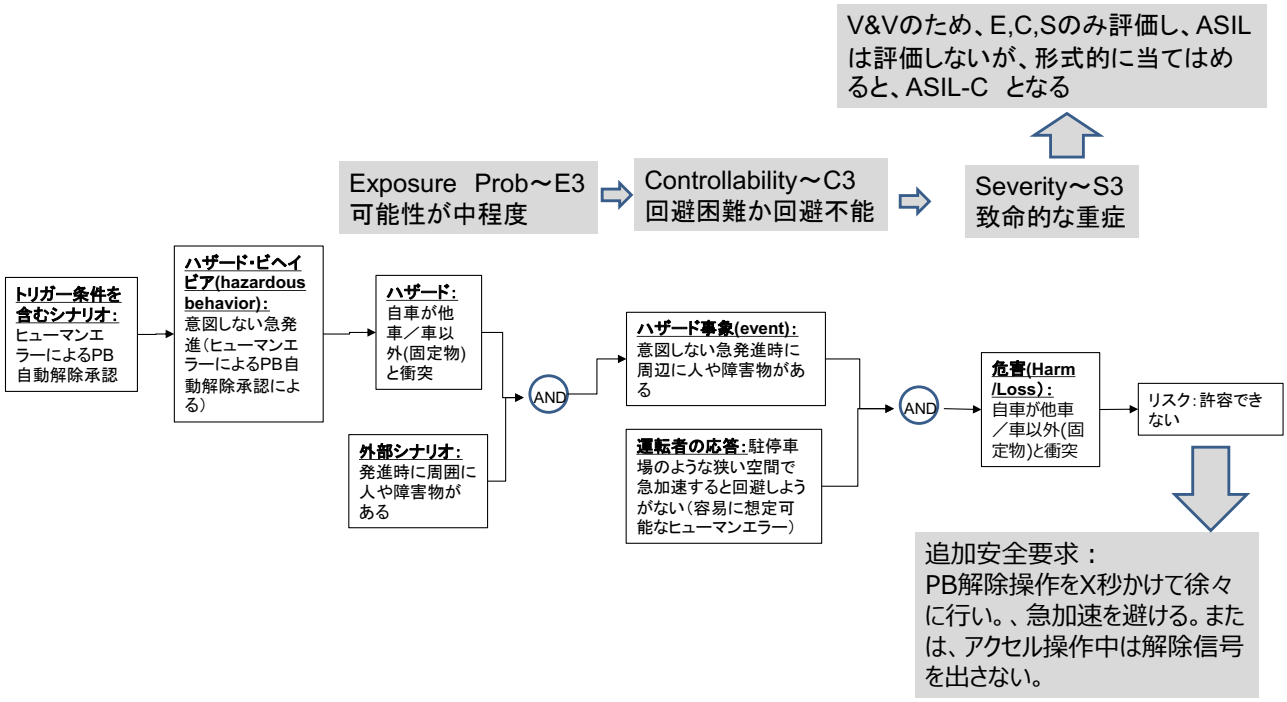
GSN（Goal Structure Network）による安全論証（網羅性の確認）

また、LS の分析の際にも「状況」の明示化が必要になることもある。ここでは、「自動車の周辺に人や障害物がある場合」と「自動車の中に運転手がいる場合」という「状況」を追加している。(別の LS では、「坂道に駐車する場合」などの「状況」も必要になる。これらの「状況」は、LS の中に書いてもよいし、UCA の中に書くという選択肢もある。この柔軟さが STPA の便利さであるが、同時に、暗黙の仮定として見逃してしまうこともあるという点に気をつけなければならない。この「状況」の明示化と LS の組み合わせは、このシナリオのリスク評価にも役立てることができる。ISO 26262 で定義されている SEC 評価（Severity（過酷度)、Exposure（曝露可能性)、Controllability（制御可能性））は複数の専門家の定性的評価に頼らざるを得ないが、その際の評価の客観性に利用することができる。シナリオで想定している「状況」を明示化しておくことで、専門家の評価での暗黙の想定を防ぎ、評価のばらつきを抑えることができる。下記の表は論文から引用した STPA で識別した LS に「状況」を明示化し、さらに、SEC 評価をした例である。このような UCA,LS のシナリオと「状況」の記載は、複数人の SEC 評価の際にも有効であった。

コントロールアクション	コントローラと被コントローラ	UCA（N)	UCA(P)	損失シナリオ（LS)	外部環境条件	運転手の有無	過酷度（S)	暴露可能性(E)	回避可能性(C)	ASIL	コンポーネント安全要求
CA6 PB解除承認	運転者→EPBコントローラ	UCA6N：PB解除しないまま走行し、PBの劣化につながる（H5)	UCA6P：発進時に運転者がアクセルを踏んだままで、PB解除承認し、急加速し衝突（H3)	UCA6N-LS1:EPBコントローラ用のアクセル状態検出器の不良またはアルゴリズム不適切で、解除信号が出ない	周辺に人や障害物がある	車内に限定できる	S0	E2	C1	対象外(QM)	・PBをかけたままの走行を許容する（UCA6NP-HS1,HS2に対して） ・PB解除操作をX秒かけて徐々に行い、急加速を避ける。または、アクセル操作中は解除信号を出さない。 （参考） (S3,E3,C3)→ASIL-C相当 (S3,E3,C1)→ASIL-A相当
				UCA6N-LS2:運転者が解除指示を認知し忘れてPB解除承認を出さない。	周辺に人や障害物がある	車内に限定できる	S0	E2	C1	対象外(QM)	
				UCA6P-LS2:アクセルを踏んだままで（ヒューマンエラー）PB解除承認を出して急加速し衝突する。	周辺に人や障害物がある	車内に限定できる	S3（意図しない解除は急発進で近くに人がいれば致命的な障害につながる）	E3（容易に考えられるUCA）	C3（アクセルONで急に解除されると回避しようがない）	ASIL-C	

リスク評価を含んだ STPA 分析表(Step-3,4)

最後に、上記で明示化した「状況」と自然言語で記述したシナリオは、ISO 21448 で要求されるイベントツリー（ET）に似た論理表現に直接変換することが容易にできる。下図のように、今回注目している PB 自動解除承認のヒューマンエラーがトリガー事象となり、その直接的な結果がハザードビヘイビア（危険な行動）としての急発進につながる。さらには、外部状況として「周囲に人や障害物がある」という仮定と、運転者の応答としての「急加速のための回避可能性の難しさ」が重なって、最終的な「衝突という危害」につながるというシナリオが論理的・客観的な形で表現できる。同時に、曝露可能性、回避可能性、過酷度も表に従ってシナリオ図上に表現できる。ISO 21448 では ASIL までは要求されてはいないが、ISO 26262 に従った ASIL 評価も可能である。すでに示した STPA に基づいた LS（状況を追加的に明示化したもの）の表と、下記のイベントツリーのように表現した図は同じ内容になってはいるが、図としてのわかり易さは下記の方が優れているかもしれない。



ISO 21448 の記載様式にそった表現

あとがき

以上のように「状況」の明示化は重要ではあるが、方法は一つではないことがわかる。取り組む問題に応じた選択が必要であるが、STPA を ISO 21448 (SOTIF)の中で使うためには、STPA で導出された LS(損失シナリオ)の中で暗黙的に仮定されている「状況」をきちんと明示し、ISO 21448 で要求されるイベントツリー的な表示に必要な情報として整理しておくことが重要である。同時に、STPA でのシナリオをすべてレビューすることで、ISO 21448 ではあいまいなままになっている「トリガー条件」の導出根拠とその網羅性まで主張することも可能になる。

今回の EPB システムの安全分析は短い仮想問題ではあるが、冒頭述べた STPA での自然言語によるシナリオ記載の柔軟さという長所とあいまいさが残るという短所を、ISO 21448 (SOTIF)の要求様式を通して融合・昇華した事例になっているのかもしれない。

以上（2025/10/19　兼本　茂）