

タイトル：UCA(Unsafe Control Action)の識別のコツ

STPA HANDBOOK [1] では、「UCA は5つの部分から構成される」としています。そのことが、航空機のブレーキシステム制御ユニット（BSCU: Brake System Control Unit）を例題として、次のような具体例を使って示されています。

| | | | | |
|-----------------------|-----------------|----------------------|---------------------------------|-------------------|
| <u>BSCU Autobrake</u> | <u>provides</u> | <u>Brake command</u> | <u>during a normal takeoff.</u> | <u>[H-4.3]</u> |
| <Source> | <Type> | <Control Action> | <Context> | <Link to Hazards> |

注1：<> は、UCA の構成要素を表す。

注2：H-4.3 は、「離陸中、V1 を超過後に減速が生じる」というハザードである。

※V1：離陸滑走中に機体にトラブルがあった場合に、離陸を中止するか否かを決定する速度。

上記の例は、日本語として自然な文となるように順番を変えると次のようになるでしょう。

通常の離陸時に、BSCU が、 ブレーキコマンドを 与えることにより、 [H-4.3]のハザードになる。
<状況> <コントローラ> <コントロールアクション> <ガイドワード> <ハザード>

UCA を識別するステップは、この「5つの部分」を「ひな型」として、これに当てはめていく作業と考えると分かりやすいです。

考えていく順番は、次のようにすると良いと思います。

- ① STAMP/STPA のステップ1 で識別した<ハザード>を一つ取り上げる。
- ② <コントロールアクション>を一つ取り上げる。（これで、<コントローラ>も特定されます。）
- ③ 4つの<ガイドワード>のうち、一つを取り上げる。

ここまでは、ほぼ機械的な作業でできます。冒頭の例について、①～③までを行った状態を書いてみます。

BACU が、ブレーキコマンドを与えることにより、[H-4.3]のハザードになる。

ここまででは、何を言っているのかわからない文になる場合が多いと思います。

そこで、最後に、

- ④ 論理的に意味が通る文となるような<状況>を考える。

という作業をします。この作業は、過去の経験や知識、常識、想像力が必要になります。

これにより、以下のような UCA が一つ完成します。

通常の離陸時に、BSCU が、ブレーキコマンドを与えることにより、[H-4.3]のハザードになる。

以上の①～④の手順を、

全てのハザード × 全てのコントロールアクション × 4つのガイドワード

の組合せについて繰り返すことで、「UCA の識別」の作業を完成できます。

【UCA の識別に関する注意点】

上のようなやり方で UCA を識別していきますが、UCA を識別するステップでは「この UCA は現実により得るのか？」ということは考えません。上の例でいえば、「通常の離陸時にブレーキコマンドが実行されることなんて、あり得るか？」ということは、いったん脇に置いておいて、UCA として識別しておきます※。

UCA が現実により起こり得るシナリオは、STAMP/STPA の 4 番目のステップで検討します。

UCA の識別のステップでは、その検討対象として、論理的にハザードにより得るような<コントロールアクション>、<ガイドワード>、<状況>の組合せを洗い出しておくことになります。

※なぜそのようにするのかは、UCA の分析と、ハザードシナリオの分析との役割を分けるため、という理解で良いと思います。したがって、識別した UCA が、論理的には成立するが現実的に起こり得ないことが明白な場合は、その判断理由をメモに残した上で UCA としてはオミットしても問題ありません。

【STAMP/STPA において UCA の識別が必要な理由】

STAMP/STPA は、ターゲットとする「ハザード」が発生し得るシナリオを分析するものです。そのシナリオに基づいた対策検討が可能となる場所に価値があります。その「ハザードが発生し得るシナリオの分析」のネタ（検討対象）となるのが UCA です。

UCA を用いず、コントロールストラクチャー図を眺めながら「ハザードが発生し得るシナリオ」を考えても良いのですが、それだと検討する観点が偏ったり、大きな抜けが生じたりする恐れがあります。

UCA は、上に示したように、ひな型に沿って比較的機械的な作業で識別するので、これによって客観性や網羅性、説明性をある程度確保していると言えます。

[1]：“STPA HANDBOOK”, Nancy G. Leveson, John P. Thomas,

http://psas.scripts.mit.edu/home/get_file.php?name=STPA_Handbook.pdf, March 2018, P.37

(2025/11/5 向山 輝)