STPA のロスとハザードの識別におけるプロセス改善のための提案

2026 年 1 月 13 日

1. 全体のあらまし

STPA (System Theoretic Process Analysis) [1] のステップのうち、特に難しいのが、ロスとハザードの識別です。例えば、複数の分析者で意見が分かれる、後のステップでロスとハザードの変更が必要になるなどの課題があります。本稿では、ロスとハザードの識別のプロセスを改善するための方法論の確立を目指します。

1.1. 現状の課題

STPA のステップのうち、ロスとハザードの識別では、以下のような課題があります。

- 複数の分析者で意見が分かれる。
- 後のステップでロスとハザードの変更が必要になる。
- ハザードは「システムの状態」であるべきである [1] が、これに合致するハザードを見つけるのが難しい。

1.2. 現状の課題の原因

現状の問題点の原因として、以下のものが考えられます。

- ロスとハザードを識別するステップの方法論が確立されていない。例えば STPA Handbook では、ロスの識別について、利害関係者の利害関係を識別する [1] ということ以外をほとんど言っていない。
- 複数の分析者がいるとき、それぞれの分析者が異なる前提条件を思い描いており、前提条件が共有されていない。

1.3. 解決策

解決策として、以下のような形式のドキュメントを残すことが考えられます。この形式のドキュメントを、本稿では「因果記法」とします。

- 前提条件をあらかじめ明記する。
- 前提条件は if-else-endif という記法で記述する。これにより、ある前提条件を採用しない場合についても議論することができる。
- 因果関係を時系列で整理する。
- 因果関係のそれぞれの要素は、単位文（後述）に整理する。これにより、ロスとハザードが複雑または複合的な記述になることを防ぐ。

- 因果関係のそれぞれの要素のうちから、ロスとハザードにふさわしいものを選ぶ。
- 因果関係のそれぞれの要素のうち、前提条件と矛盾するものがあれば、ロスと判断できる。
- 因果関係のそれぞれの要素も if-else-endif という記法で記述する。これにより、ある状況が発生しなかった場合についても議論することができる。
- 議論の過程を文書内にコメントとして残す。これにより、議論が堂々巡りになることを防ぐことができる。

2. 実際の事例

2.1. 前提条件をあらかじめ明記する

以下の例のように、前提条件をあらかじめ明記することができます。if-else-endif という形式を使います。else があることにより、ある前提に対する反対のケースを考慮することができます。

```
if <会社の信用>が{失われてはならない}
else
endif
```

また、以下の例のように、安全分析の方針を、前提条件として記述することもできます。

```
if <分析の対象>が{ルーターに限定される}
else
endif
```

2.2. 因果関係を時系列で整理する

以下の例のように、因果関係を時系列で整理することができます。

安全分析者はもともと、「インターネット接続が長時間停止する」というロスと「ルーターの設定異常により正常な通信ができない状態」というハザードを想定していました。そこで、ハザードを「ルーターの設定が異常である」と「ルーターが正常な通信ができない」という 2 個の単位文に分割しました。これにより、ハザードが複合的な記述になることを防ぐことができます。このように、複合的な記述を単位文に分割することを、本稿では「複合要因の個別化」と言います。

また、新たな要因を検討すべきときは、すぐに追加することができます。

```
if <ルーターの設定>が{異常である}
    if <ルーター>が{正常な通信ができない}
        if <インターネット接続>が{長時間停止する}
        else
        endif
    else
```

```
    endif
else
endif
```

2.3. 因果関係のそれぞれの要素のうちから、ロスとハザードにふさわしいものを選ぶ

因果関係を整理したら、ロスとハザードにふさわしいものを選びます。因果関係があるので、ハザードが先、ロスが後になるように選びます。詳細は STPA Handbook [1] などを参照してください。

```
if <ルーターの設定>が{異常である} [ハザード]
    if <ルーター>が{正常な通信ができない}
        if <インターネット接続>が{長時間停止する} [ロス]
        else
        endif
    else
    endif
else
endif
```

2.4. 因果関係のそれぞれの要素のうち、前提条件と矛盾するものがあれば、ロスと判断できる

因果関係のそれぞれの要素のうち、前提条件と矛盾するものがあれば、ロスと判断することができます。以下の例では、「会社の信用が失われてはならない」という前提条件をあらかじめ設定することで、「会社の信用が失われる」という単位文をロスであると判断することができます。

```
if <会社の信用>が{失われてはならない}
    if <インターネット接続>が{長時間停止する}
        if <社外の人を対象としたセミナー>が{開催中である}
            if <社外の人を対象としたセミナー>が{中断される}
                if <会社の信用>が{失われる} [ロス]
                else
                endif
            else
            endif
        else
        endif
    else
```

```
    endif
else
endif
```

2.5. 因果関係のそれぞれの要素も if-else-endif という記法で記述する。これにより、ある状況が発生しなかった場合についても議論することができる

因果関係のそれぞれの要素も if-else-endif で記述します。これにより、ある状況が発生しなかった場合についても考慮することができます。以下の例では、ルーターの設定が異常であるが、ルーターが正常に通信している場合について、検討のうえコメントを記載しています。コメントは # という記号で表します。

```
if <ルーターの設定>が{異常である}
    if <ルーター>が{正常な通信ができない}
        if <インターネット接続>が{長時間停止する}
        else
        endif
    else
        # ルーターの設定が異常であっても、
        # ルーターがたまたまうまく動いていることがありうる。
        # 潜在的には良くない状況であるが、さしあたり問題がない。
    endif
else
endif
```

2.6. 議論の過程を文書内にコメントとして残す。これにより、議論が堂々巡りになることを防ぐことができる

議論の過程を文書内にコメントとして残すことで、議論が堂々巡りになることを防ぐことができます。コメントは # という記号で表します。

```
if <会社の信用>が{失われてはならない}
    if <分析の対象>が{ルーターに限定される}
        if <ルーターの設定>が{異常である} [ハザード]
            if <ルーター>が{正常な通信ができない}
                if <インターネット接続>が{長時間停止する} [ロス]
                    # 分析の対象をルーターに限定したので、
                    # 「インターネット接続が長時間停止する」ことをロスとする。
                    # 会社の信用などは、分析の対象外とする。
```

```
                else
                endif
            else
            endif
        else
        endif
    else
        if <インターネット接続>が{長時間停止する} [ハザード]
            if <社外の人を対象としたセミナー>が{開催中である}
                if <社外の人を対象としたセミナー>が{中断される}
                    if <会社の信用>が{失われる} [ロス]
                        # 分析の対象をルーターに限定しない場合、
                        # 「会社の信用が失われてはならない」という前提に従って。
                        # 「会社の信用が失われる」をロスとする。
                    else
                    endif
                else
                endif
            else
            endif
        else
        endif
    endif
else
endif
```

3. 参考文献

[1] Nancy G. Leveson. John P. Thomas. *STPA Handbook*. 2018