タイトル：STAMP/STPA での損失（Loss,Accident）の峻別とは

まえがき

Engineering a Safer World（邦訳：システム理論による安全工学、共立出版、2025 年）での STAMP 理論の実践的成功例として、第 14 章 SUBSAFE、米国海軍の潜水艦安全プログラムの成功事例が紹介されている。これは、1963 年に起きた原子力潜水艦スレッシャー号の深海潜水テスト中での沈没事故をきっかけに作られた原子力潜水艦の安全プログラムである。民間人まで含めて 129 名を失った深刻な事故であったが、この契機に作られた SUBSAFE というプログラムのおかげで、その後 50 年以上にわたり原子力潜水艦の致命的な事故を防いでいる。年代的に、STAMP 理論が出てくる前の安全プログラムであり、システム安全の実践例と言うべきかもしれないが、STAMP 理論の考え方の基礎となっている事例であり、1 章を割いて説明されている。

その成功例の基礎となる考え方で大事なものの一つは、システムの安全目標を次のように絞り込むことであった。

・潜水艦の船体の防水の完全性
・浸水ハザードのコントロールと回復のために重要なシステムの運用性（operability）と完全性（integrity）（注：ここでのサブシステムの運用性と完全性とは、事故の際に中央制御室から遠隔で制御できることと考えてよい）

これらの安全目標は、STAMP の中では、「損失」の裏返しの表現といえる。「損失」としては、完全な防水性の破綻（浸水による沈没）、及び、浸水ハザードのコントロール不能、といった表現になる。どちらの表現が良いかはケースバイケースでの判断になるが、安全目標の方がわかり易いことが多いかもしれない。

安全目標を峻別することの大事さを、上記著書では、以下のように表現している。

『焦点を絞ることによって、SUBSAFE プログラムは、この明記された目的以外に焦点を広げたり弱めたりすることはない。たとえば、ミッションの達成は大事ではあるが、SUBSAFE の焦点ではない。同様に、火災安全、兵器の安全、労働者の安全衛生、原子炉システムの安全は SUBSAFE には**含まれない**。』

さらに、あとがきで STAMP の基本理念を以下のように述べている。

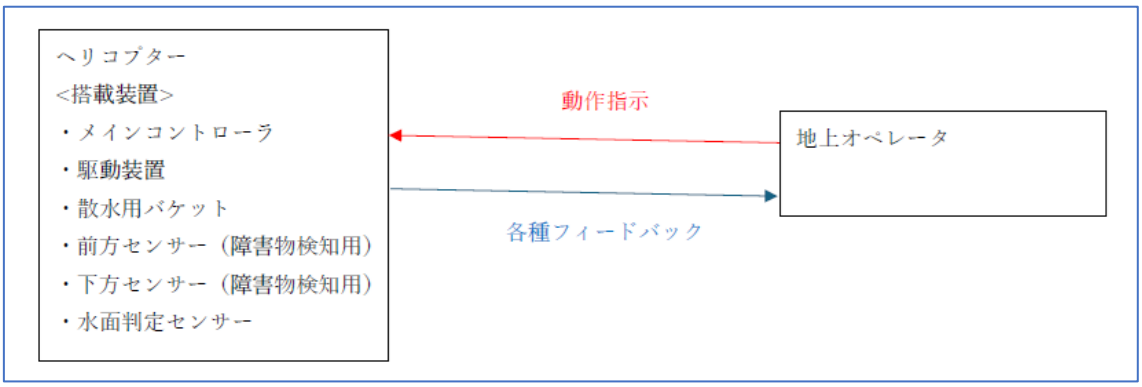
『本書は、「故障の防止」から「振る舞いに関する安全制約の強化」へ、「信頼性の確保」から「安全のコントロール」へと焦点を変えた、安全工学の新しいアプローチを提案する。』

時折議論される安全分析とセキュリティ分析の違いで、前者が「安全のコントロール」に向かっているのに対して、後者は、まだ、「信頼性の確保」にとどまっているということもできよう。本メモでは、最近 JASA 安全性向上委員会で始めた STAMP/STPA の教育的事例や実践例の作成における試行錯誤の経緯を紹介し、STAMP/STPA での「損失」の定

義の重要さに気づいてもらうために作成した。

（1） 自動運転ヘリコプターによる山林火災の消火システム

システム構成概要



当初の損失

A1　ヘリコプターが墜落する
A2　ヘリコプターの降下時に、真下の人、車両などを押しつぶす
A3　ヘリコプターが消火ポイント、または給水ポイントに到着しない
A4　給水時に、ヘリコプターが入水する
A5　"消火できない or 消火が遅れる
A6　前方の他の飛行体と衝突する
A7　ヘリコプターが給水できない。（ミッション未達）
A8　ヘリコプターが目標高度に存在しない。（ミッション未達）

冒頭の安全目標の焦点化という趣旨に沿って、「損失」を絞り込んでみる。A1,A2,A6 以外は、ミッション未達（機能の未達）であり、損失ではあるが、最も防ぐべき損失としては省いてもよい。また、無人地への墜落は許容するとすると、1 件の追加を含めて下記 3 件が大事な「損失」となる。A2,A6 は他者への危害、A9 は自分自身の喪失と考えて、「損失」を絞り込みことができる。A1 の墜落という表現ではなく、墜落以外の緊急着陸も含めて損失と考えて分析に含める。

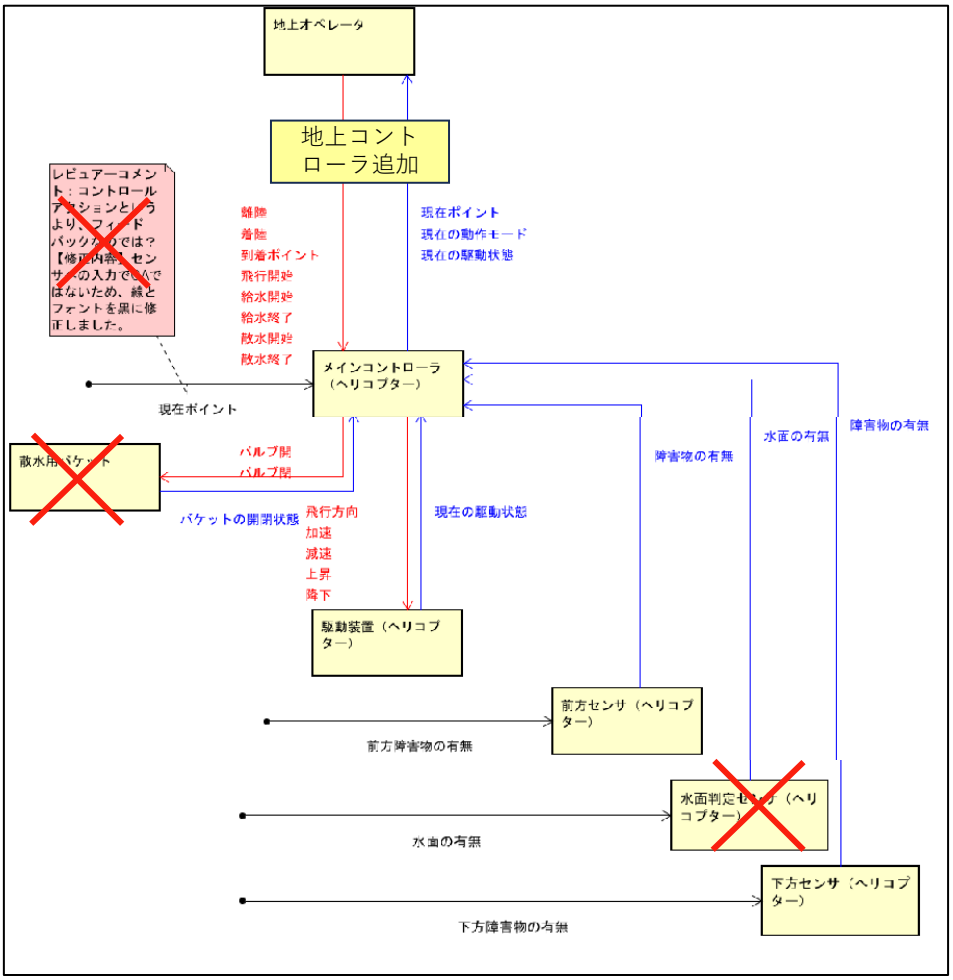
絞り込み後の損失

A2　ヘリコプターが墜落し、真下の人、車両などを押しつぶす、または、火災を誘発する
A6　前方の他の飛行体または静止物（電線など）と衝突する
A9　ヘリコプターが基地に帰還しない（追加）

制御構造図は、この損失の防止のために必要な機能を考えて作成すべきである。尚、自動運転といっても、目的地までの経路を自動策定するには、飛行経路の法的な限界、地形的

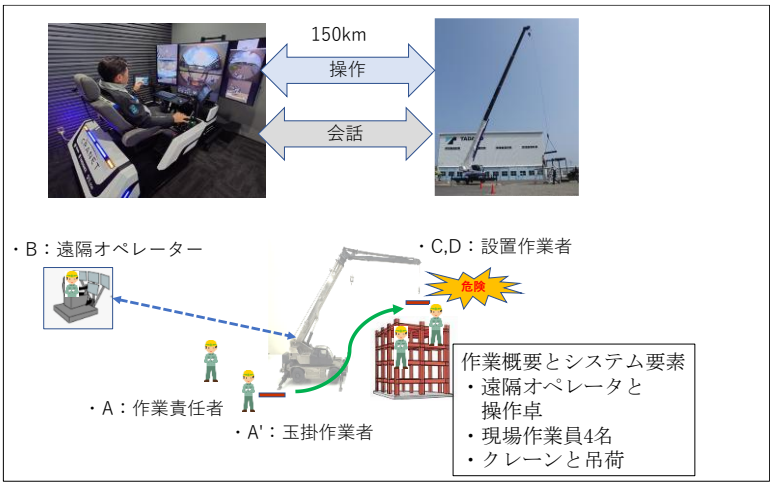
な配慮（市街地上空を避ける）、環境への配慮（送電線などに配慮して高度を高くするなど）、機械による自動経路作成で限界があることを考慮しないといけない。また、緊急帰還など、地上でのオペレータによるマニュアル指示の必要性を考えて、地上側のコントローラを挿入した。複数の自動ヘリコプターの存在は当然仮定しないといけないので、自動ヘリコプター間の相互通信は、本来は、この制御構造図に入っている必要がある。当初作成した制御構造図に若干の修正を加えて概念図を下記に示す。

絞り込み後の制御構造図（コントロールアクションは絞り込み前なので無視すること）



（2） リモートクレーン制御システムの安全分析（2025 年安全工学論文）

システムの概要を示すポンチ絵は、制御構造図作成のような詳細に先立って、関係者の理解を得るために必須のものと言える。下記は、2025 年の安全工学誌の創設として投稿したリモートクレーン制御システムの安全分析で示した例である。



この分析での安全目標の裏返しとしての「損失」は下記のように定義されている。ただし、STPA による分析は、「A1:ブームや吊荷との衝突により人や構造物が損傷する」という損失だけに注目して行っている。論文執筆の時点では、A2-A4 の損失の定義に深く立ち入って議論してこなかったが、いま見直してみると、例えば、「A3：吊荷の落下」のような損失は、A1 の中に含まれており、実際の STPA 分析の中での損失シナリオとして、「急な操作や突風などでワイアが切断して吊荷が落下する」といったシナリオは導出されている。一方で、ワイア切断のような事故では、経年劣化による強度低下のような問題もあるが、これは、ハザードとして挙げられていない。(安全距離の問題にしか着目していない)

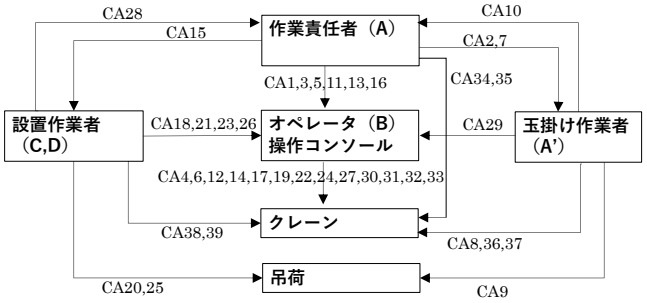
前メモで解説したように、多くの事故では、事前にハザードとして認識されていない兆候事象（ここではワイア強度低下）はしばしばある訳で、そのために、予防保全対策としての定期検査のようなものが機械の保全技術として確立されている。従って、後付けでよいので、STPA でのハザードとして、「安全距離が少なすぎる」といった他に、「機器の劣化」のような兆候事象も入れるべきであろう。

アクシデントID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A1	ブームや吊荷との衝突により人や構造物が損傷する	H1	ブームや吊荷と人や構造物との安全距離が保てない	SC1	ブームや吊荷と人や構造物との安全距離を保たなければならない
A2	クレーン本体の転倒により人や構造物が損傷する	H2	クレーン本体のバランスが不安定	SC2	クレーン本体のバランスを安定させなければならない
A3	吊荷の落下により人、構造物、吊荷が損傷する	H3	吊荷が不安定	SC3	吊荷を安定させなければならない
A4	吊荷が損傷する	H4	吊荷に外力が加わる	SC4	吊荷に外力をかけない

このアクシデント（損失）を防ぐための制御構造図を下記に示す。ここでは、分析に用いた 37 個の CA（コントロールアクション）のみ表示している。FB までいれると複雑になりすぎるためである。分析した結果をレビューアに理解してもらうためには、このような工夫も必要であり、ツール（STAMP Workbench）の改善も望まれるところである。

今回のリモートクレーン制御システム設計への STPA の適用は、STPA の最終目標であるシステムならびにコンポーネントの安全対策の導出まで行った。さらに、

実際の設計技術者が、STPA を使って安全分析まで行った上に、コンサルテーションに協力した JASA 安全性向上委員会のメンバーが、レビューアとしての立場で、分析結果を評価した。STPA による安全分析は、研究目的での施行例は多くあるが、実システムの開発に役立てるという点では、稀有な事例かもしれない。そこから得られたノウハウは、この分析で活用した STAMP Workbench というツールの改善に役立ててゆくことで、STPA の利用をさらに促進することができよう。



CA1 作業開始指示
CA2 作業開始指示
CA3 玉掛位置へフック移動指示
CA4 玉掛け位置へフック移動
CA5 フック停止指示
CA6 フック停止操作
CA7 玉掛け開始指示
CA8 玉掛作業：フック
CA9 玉掛作業：吊荷
CA10 玉掛完了報告
CA11 吊荷の地切り指示：巻上
CA12 地切り操作：巻上
CA13 地切り停止指示：巻上停止
CA14 地切り停止操作：巻上停止
CA15 作業開始指示：設置場所指示
CA16 吊荷移動指示：設置位置へ
CA17 吊荷移動：設置位置へ
CA18 吊荷停止指示、微調整含む：設置位置
CA19 吊荷停止操作、微調整含む
CA20 吊荷の設置、固定
CA21 玉外しのため巻下指示
CA22 巻下操作：玉外しのため
CA23 巻下停止指示
CA24 巻下停止操作
CA25 玉外し作業：吊荷側
CA26 玉外し完了報告
CA27 フック退避操作、次の荷へ移動
CA28 設置完了報告
CA29 フック停止指示
CA30 操作停止、操作信号通信遮断
CA31 操作停止解除
CA32 動力源停止
CA33 動力源始動
CA34 非常停止　無線スイッチで操作緩停止
CA35 緊急停止、動力源停止　クレーン本体のスイッチ
CA36 非常停止　無線スイッチで操作緩停止
CA37 緊急停止、動力源停止　クレーン本体のスイッチ
CA38 非常停止　無線スイッチで操作緩停止
CA39 緊急停止、動力源0停止　クレーン本体のスイッチ

あとがき

STAMP/STPA の出発点である「損失」の定義についていくつかの事例をもとに考察した。本来の STAMP の思想に沿って考えると、

1）安全目標である「損失の低減」の明確化と峻別

2）損失を生み出す損失シナリオの体系的な導出

3）損失シナリオに基づいて、それを低減するための安全対策の導出と体系化

という 3 ステップの達成である。これを、透明性をもった論理で達成（導出）することが目的である。ハザード、安全制約、制御構造図、ＵＣＡなどはそのための手段であるが、STPA は、その手段を具体的に挙げている点で、安全分析の実用性を高めている貴重な方法論といえよう。しかし、この手順にこだわりすぎると、本来の最初の 3 ステップの達成に至らない。SUBSAFE という安全管理プログラムは、ハザードやＵＣＡを使わずに、STAMP の思想に沿って安全目標を達成した成功事例である。

今後、いろいろな Toy　Problem ではない事例の安全分析を、STPA を通して行うことで、本来の STPA 分析の在り方を考えてゆくことが大事になる。

以上（2025/7/22　兼本　茂）