

STAMP および STAMP ツールの Tips

■便利な操作方法

図や表の文字サイズを変更する

ツールとして常に有効にする方法ではなく、プロジェクトファイル毎の設定です。

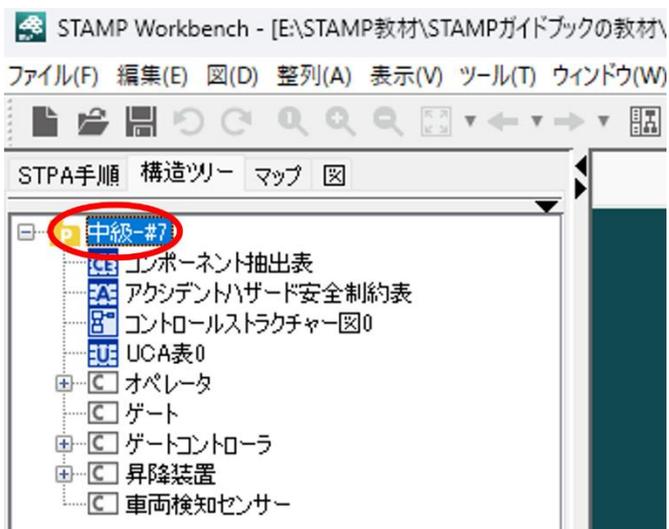
1. STAMP Workbench で、文字サイズを変更したいプロジェクトファイル (.stmp ファイル) を開く。



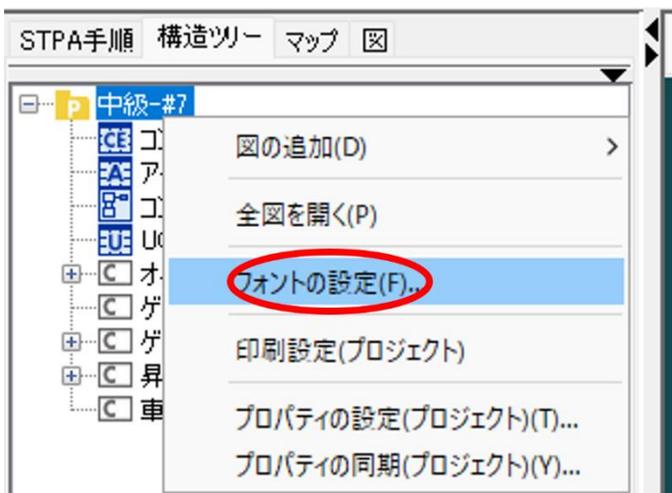
2. 左上プロジェクトビューのタブに STPA 手順/構造ツリー/マップ/図 があります。「構造ツリー」タブを選択。



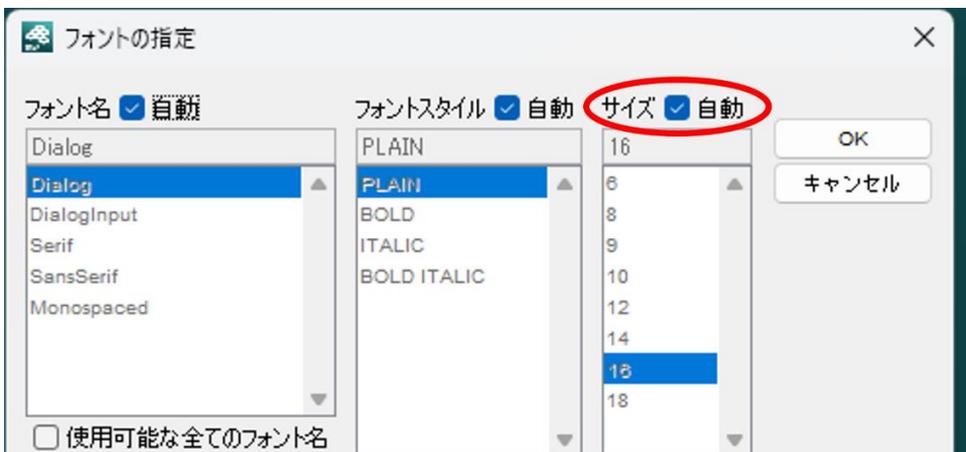
3. プロジェクトファイル名を選択し、コンテキストメニューを開く（右クリック）。
下図では「中級-#7」がプロジェクトファイル名。



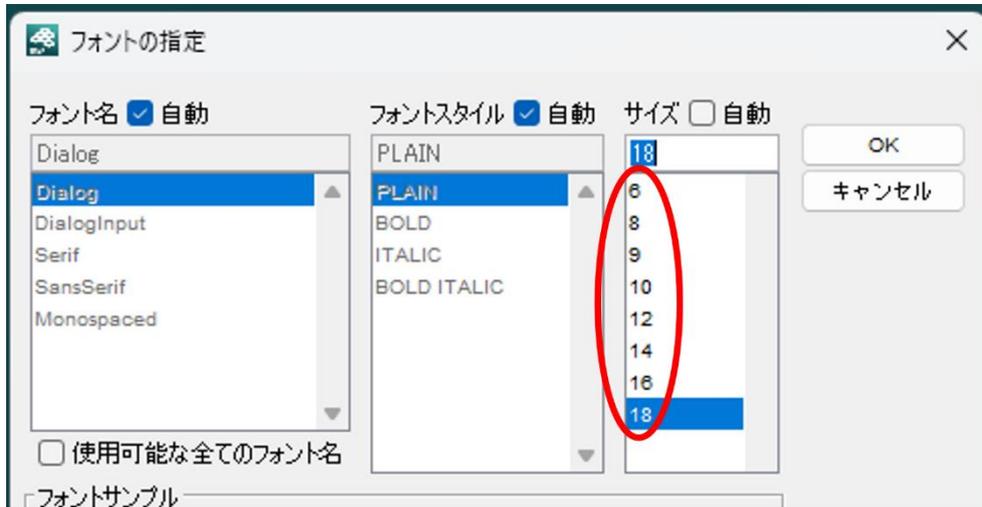
4. プルダウンメニューから、「フォントの設定」を選択。



5. 「フォントの指定」ダイアログで、「自動」が選択されているので、オフにする。



6. 文字フォントのサイズを数字で選択。デフォルトは16。



設定できるサイズは6から18まで。

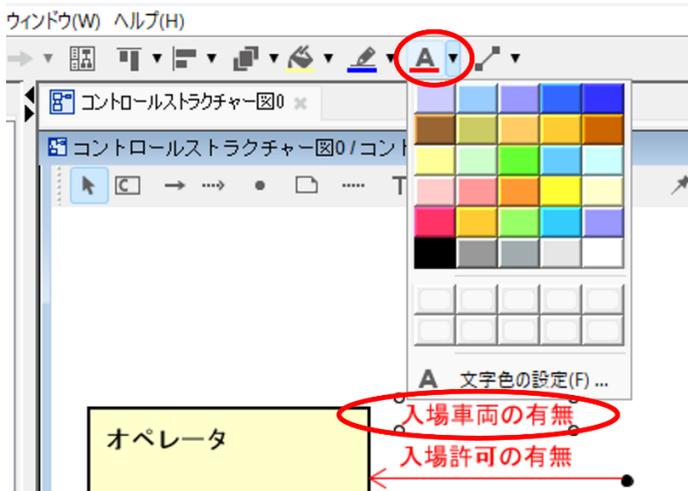
OKを押して確定する。

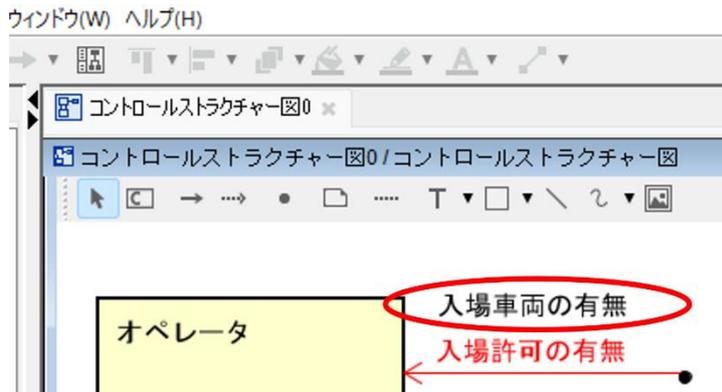
選択したフォント指定はすべての図や表に適用される。別の方法を使って、CS図上の一部の文字列のみ文字色やフォントを変更することもできる。

目立つように一部の文字だけ文字色を変更する

コントロールストラクチャー図 (CS 図) において一部の文字列のみ文字色やフォントを変更することができます。全ての表で一部の文字単位で文字色を変更する機能はありません。

CS 図やコントロールループ図において、CA、FB、input、output など色を変更したいコンポーネントや文字列を選択して、ツール画面にある帯状のツールバーで「文字色の設定」を押して色を選択する。変更できるのは文字色とフォント種類で、文字サイズは変更できない。





変更できない例：文字単位で色を変更

あいうえお

変更できる例：文字列全体の色とフォントの変更

あいうえお

input/output 線の操作方法

STAMP のコントロールストラクチャー図 (CS 図、CLD) において、input/output は、外界からシステム内のコンポーネントへの入力/システム内のコンポーネントから外界への出力を意味します。

CS 図、あるいはコントロールループ図 (CL 図、CLD) において、コンポーネント間の線は制御 (CA) またはフィードバック (FB) であり、input/output は入力元や出力先のコンポーネントが現れません。

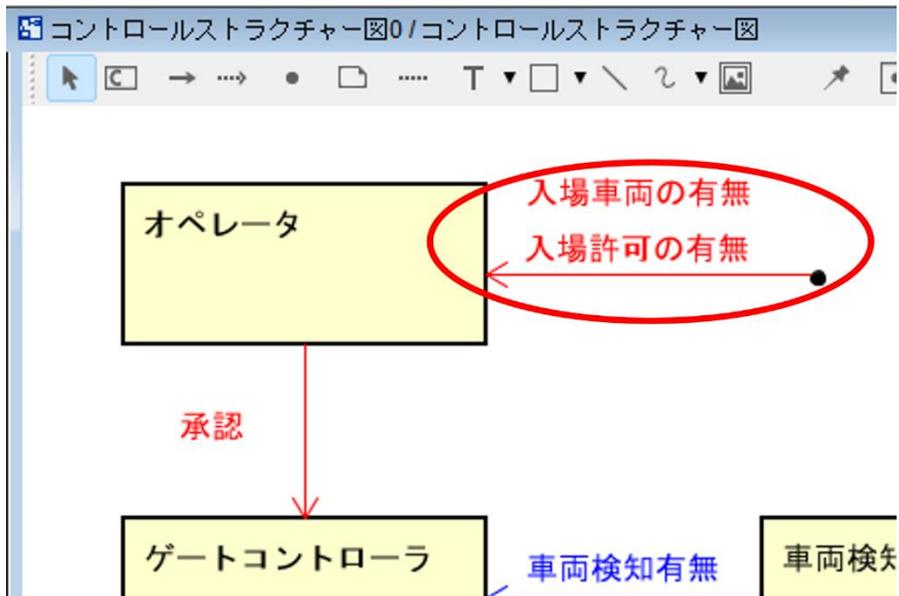
但し、「外界モデル」の項に記したように、外界の何との input/output かを示したいときには外界モデルというコンポーネントを配置して、その外界モデルコンポーネントとシステム内コンポーネントの間を input/output 線で結ぶ方法もあります。

その場合、STAMP Workbench では input/output 線が CA 線 (赤い矢印線) または FB 線 (青い矢印線) で結ばれるので、線の色を黒に変更すると良いです。

CA、FB、input/output の違いを線の色で明確に区別することをお勧めします。

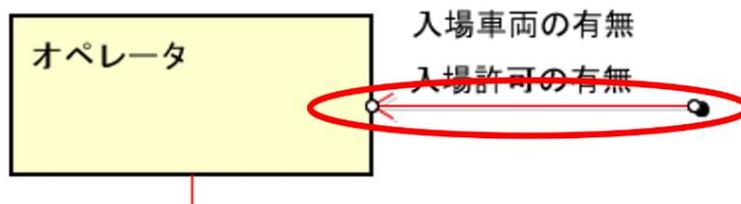
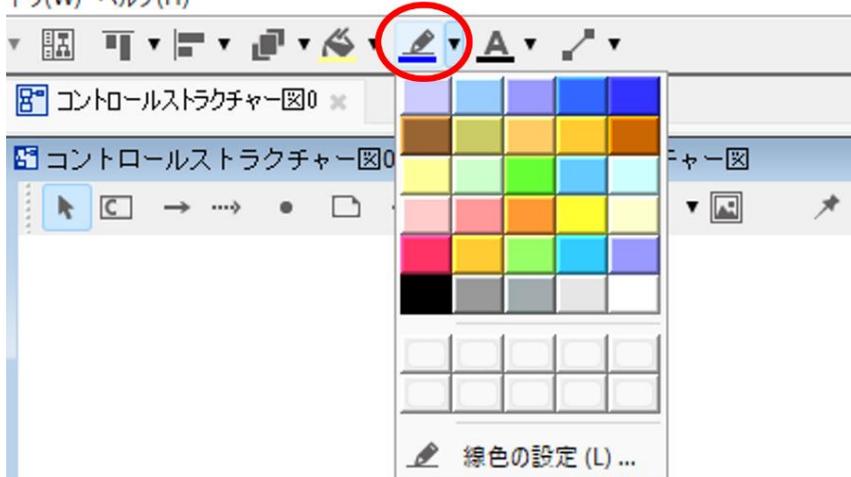
この対策はツールが自動的にサポートすることが望ましいですが現状サポートできていません。

下図では、input の文字も線も CA と同じ赤になっているので、CA と勘違いし易い。

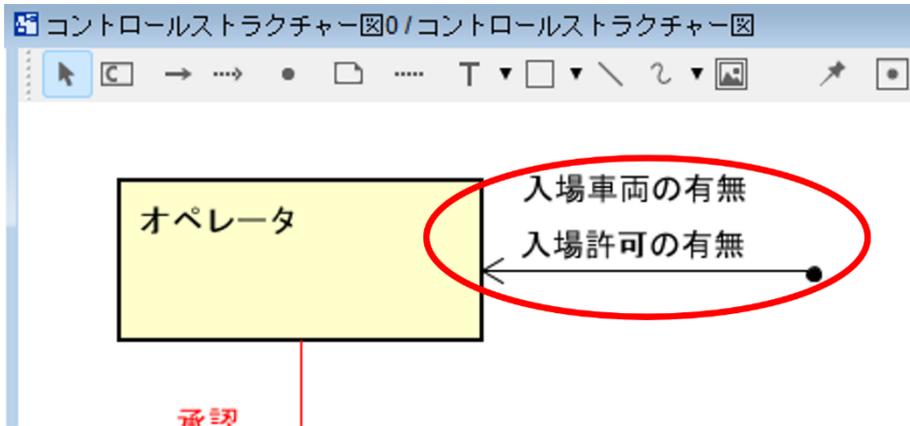


変更したい線を選択すると線色変更のボタンが有効になる

ドウ(W) ヘルプ(H)



下図では外界からの input の文字色と線色の両方を黒に変更した。CS 図上で CA と input の違いが明確になった。

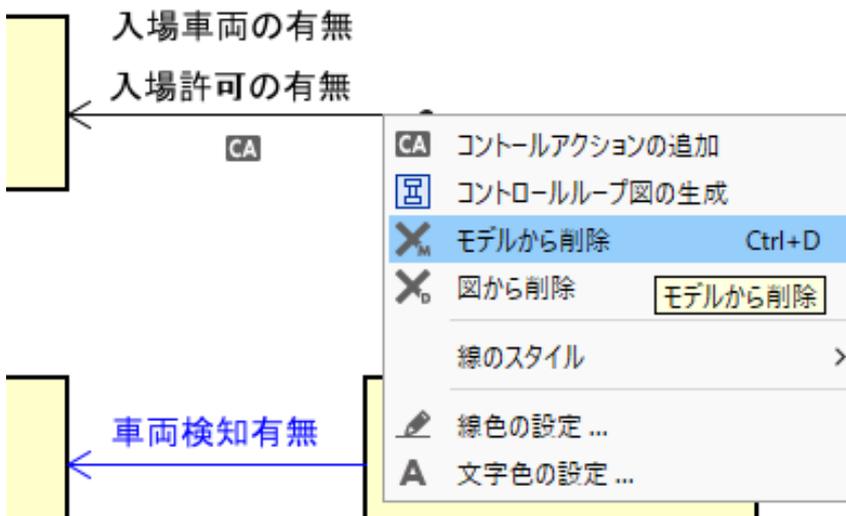


図から削除／モデルから削除

コントロールストラクチャー図（CS 図）を編集する際、コンポーネントや CA/FB 線などを削除する場合、削除対象を選択してからコンテキストメニューを開く（右クリックする）と、「モデルから削除（Ctrl+D）」と「図から削除（Delete）」を選択できる。

「モデルから削除（Ctrl+D）」を選択することをお勧めします。

「図から削除（Delete）」とすると見かけ上は見えなくなりますが、モデルとして残っている（コンポーネント抽出表にも残っている）ので、後で何らかの編集をしているときに図に復活することがあり戸惑うことが有り得ます。不要と判断したら「モデルから削除（Ctrl+D）」を選択することをお勧めします。



Excel に変換して列を増やす

UCA 表や対策表に列を増やしたいことがあります。例えば、

- UCA 表にメモを残したい。UCA を考えるときには原因を考えないようにするが、思いつくことはある。あとのステップのために思いついたことをメモしておきたい。
- 対策表に、自社（自プロジェクト）独自の ID などの情報をつけておきたい。

等々、STAMP Workbench への機能拡張要望が多々あります。STAMP Workbench は汎用的かつ基本的な機能を実装しており、とりあえずたいていの場合は事足りることを想定しているため、IPA による機能拡張予定はありません。このような要望については、次の 2 通りの対応策があります。

【対応策 1】

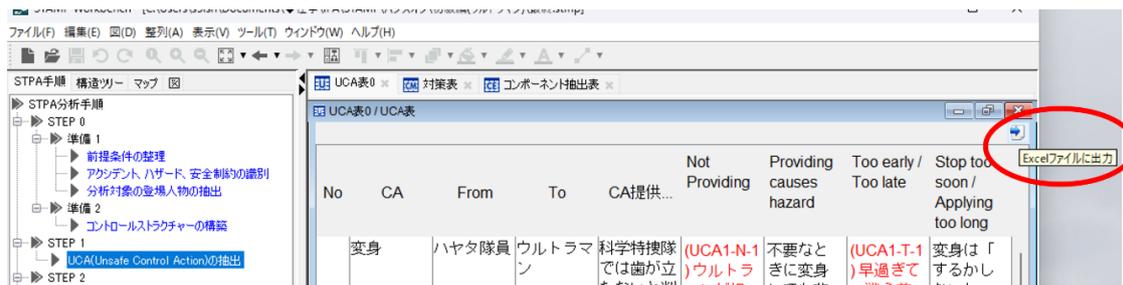
利用者様自身が（IPA がオープンソースとして公開している）ソースコードを改編して機能追加することも可能です。モデリングツール一般に精通していない技術者様でも、実は、列を追加する程度の改編は然程ハードルの高いものではありません。プログラミングの腕に覚えのある方ならば、ソースコードにザックリ目を通していただければお判りいただけるかと思えます。ソースコード改編後のビルド方法も公開しています。改編して利用されている事例は国内外から報告されています。

【対応策 2】

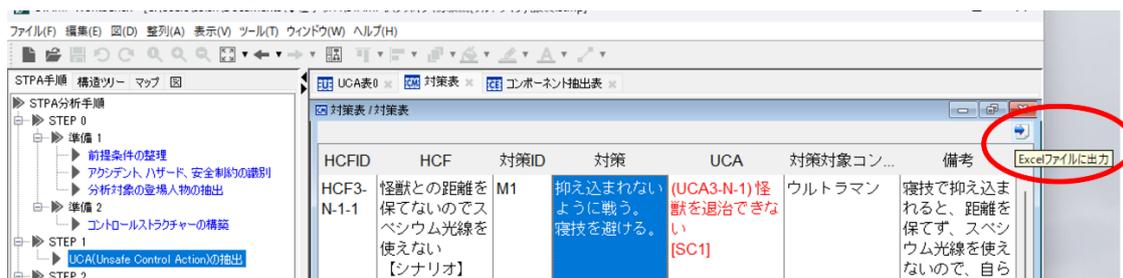
STAMP Workbench で作成した表を Excel 出力して、Excel 上で列追加する。

(1) UCA 表や対策表ウィンドウの右上にある「右向き矢印」を押す。

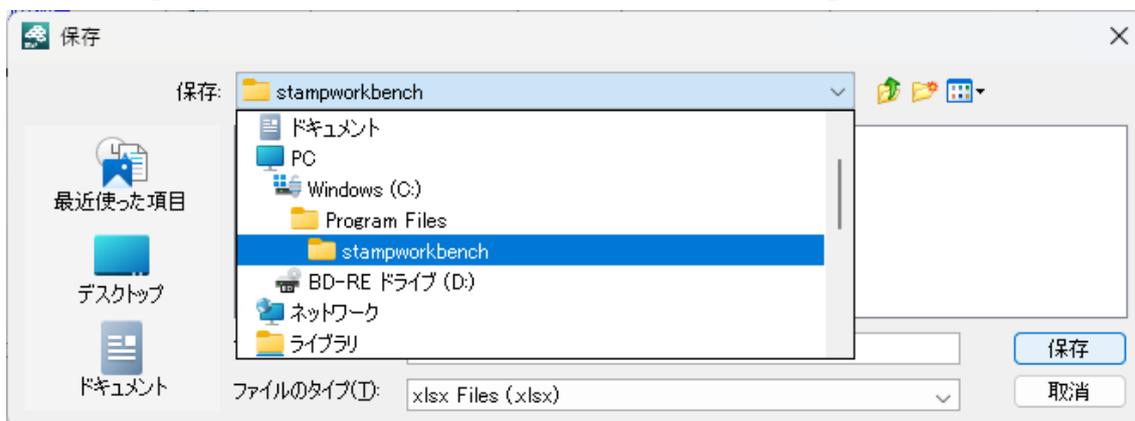
下図は UCA 表の場合。



対策表の場合も同じ。



(2) 「保存」のウィンドウを開いたら、保存先を選択して「保存」ボタンを押す。



保存先に Excel 表 (.xlsx ファイル) が保存されるので、Excel を起動して任意に列追加などを行う。

注意事項

STAMP Workbench から Excel へのエクスポート機能は有るが、Excel から STAMP Workbench へのインポート機能は無い。

Excel で編集した内容を自動的に STAMP Workbench に取り込むことはできない点に注意のこと。

デフォルトの保存先フォルダーは Program Files フォルダーなので書き込みできません。必ず、プロジェクトファイル (.stmp ファイル) と同じフォルダーなど、書き込み可能なフォルダーを選択してください。

CS 図の CA,FB に番号を付ける

CS 図を見て議論するとき CA,FB に番号があると話が早いです。

CA,FB の番号振り直しは次のようにすると簡単です。

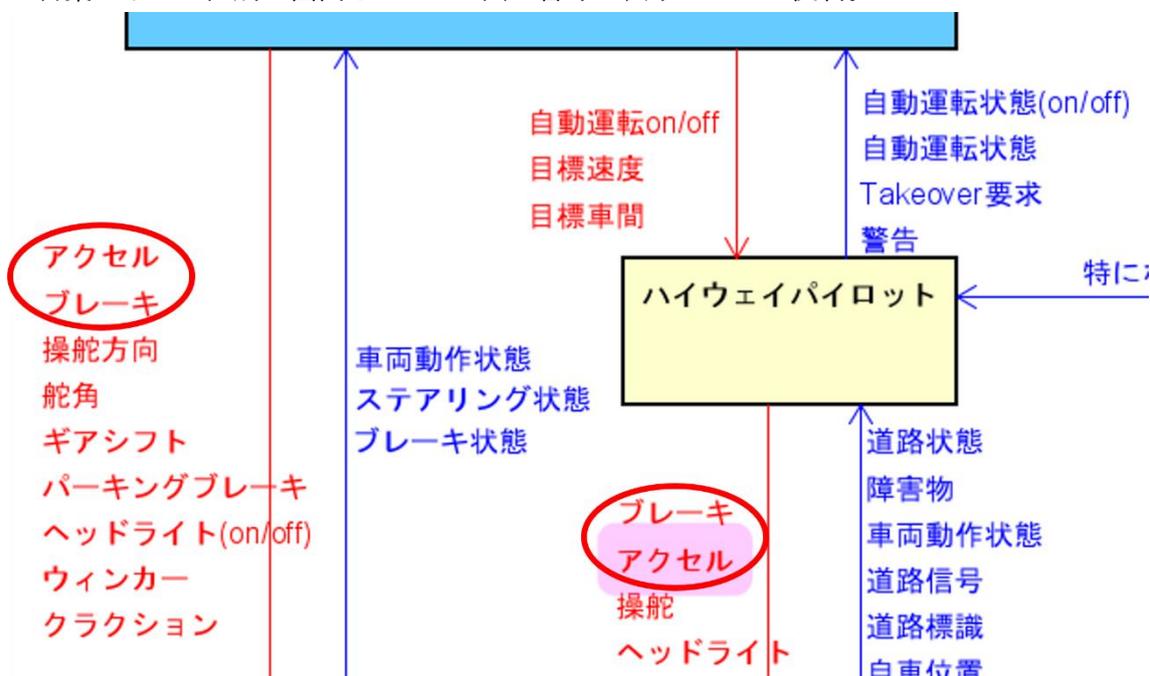
1. CS 図で直接 CA,FB の名前を編集して"CA n "のように適当に番号を振る。
2. UCA 表で CA を"CA n "の n に合わせてドラッグ&ドロップで上下に移動する。
CA を押して掴み、挿入したい横線のところまで上下にマウスカースルを移動して放す。
または、
3. UCA 表の最左列の CA 番号に合わせて、名前に付けた"CA n "の n を修正する。

ツールへの要望

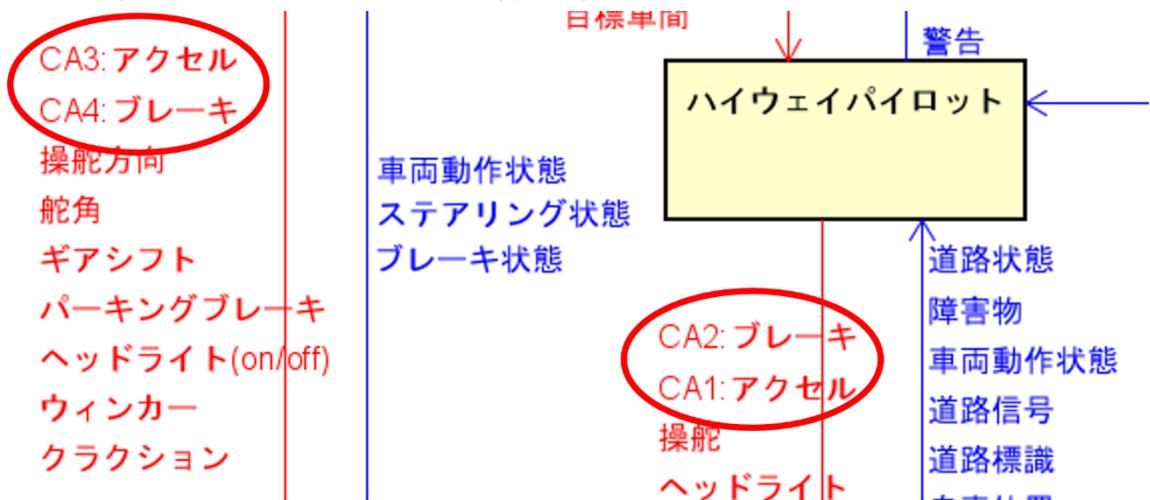
UCA の番号はUCA 表で整理できるが、FB の番号はCS 図かコンポーネント抽出表でやるしかないので不整合が出そうな気がする。できることなら、(一般的にはCA とFB は対になるので) コントロールループを成すCA と対応付くFB が同じ番号になると良いが、自動的にナンバリングするのは難しそう。せめて、番号の重複を無くすくらいはできると良い。

この対策はツールが自動的にサポートすることが望ましいが現状サポートできていません。

下図のように「アクセル」や「ブレーキ」といった同名のCA があるときなど、レビュー時に言葉だけでは区別が面倒なのでCS 図に番号が表示されると便利。



CS 図の中でCA1、CA2、・・・のように番号を振る。



UCA 表で順番が上下逆なのが気になる。

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
11	ウインカー	ドライバー	車両プラットフォーム					
12	CA2:ブレーキ	ハイウェイパイロット	車両プラットフォーム	前方車両が差し迫っている	(UCA12-N-1) ブレーキ指示しない[VH1] [SC1]	(UCA12-P-1) ブレーキ指示量が不足[VH1] [SC1]	(UCA12-T-1) ブレーキ指示が遅い[VH1] [SC1]	
13	CA1:アクセル	ハイウェイパイロット	車両プラットフォーム					
14	操舵	ハイウェイパイロット	車両プラットフォーム					

UCA 表で No 欄の番号を選択してドラッグし、移動したいところまでマウスカーソルを移動してドロップする。

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
11	ウインカー	ドライバー	車両プラットフォーム					
12	CA2:ブレーキ	ハイウェイパイロット	車両プラットフォーム	前方車両が差し迫っている	(UCA12-N-1) ブレーキ指示しない[VH1] [SC1]	(UCA12-P-1) ブレーキ指示量が不足[VH1] [SC1]	(UCA12-T-1) ブレーキ指示が遅い[VH1] [SC1]	
13	CA1:アクセル	ハイウェイパイロット	車両プラットフォーム					
14	操舵	ハイウェイパイロット	車両プラットフォーム					

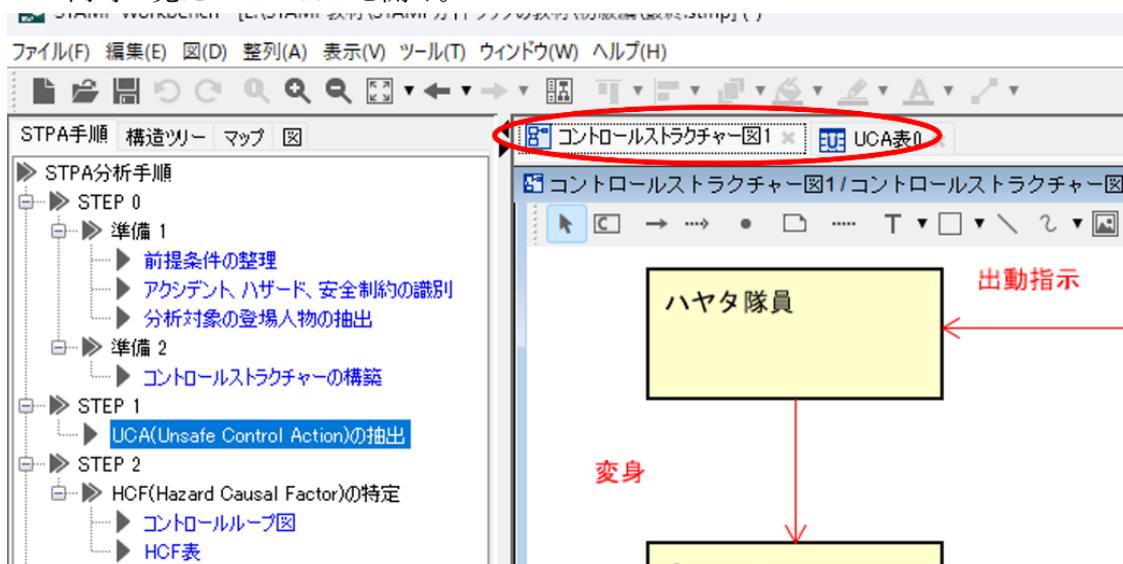
UCA 表の中の UCA 番号 (UCA12-N-1 など) は自動的に変わるので、手作業での修正は不要。同時に、対策表の中の UCA 番号なども自動的に変わるので、UCA 表以外に対して手作業での修正は不要。

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
11	ウインカー	ドライバー	車両プラットフォーム					
12	CA1:アクセル	ハイウェイパイロット	車両プラットフォーム					
13	CA2:ブレーキ	ハイウェイパイロット	車両プラットフォーム	前方車両が差し迫っている	(UCA13-N-1) ブレーキ指示しない[VH1] [SC1]	(UCA13-P-1) ブレーキ指示量が不足[VH1] [SC1]	(UCA13-T-1) ブレーキ指示が遅い[VH1] [SC1]	
14	操舵	ハイウェイパイロット	車両プラットフォーム					

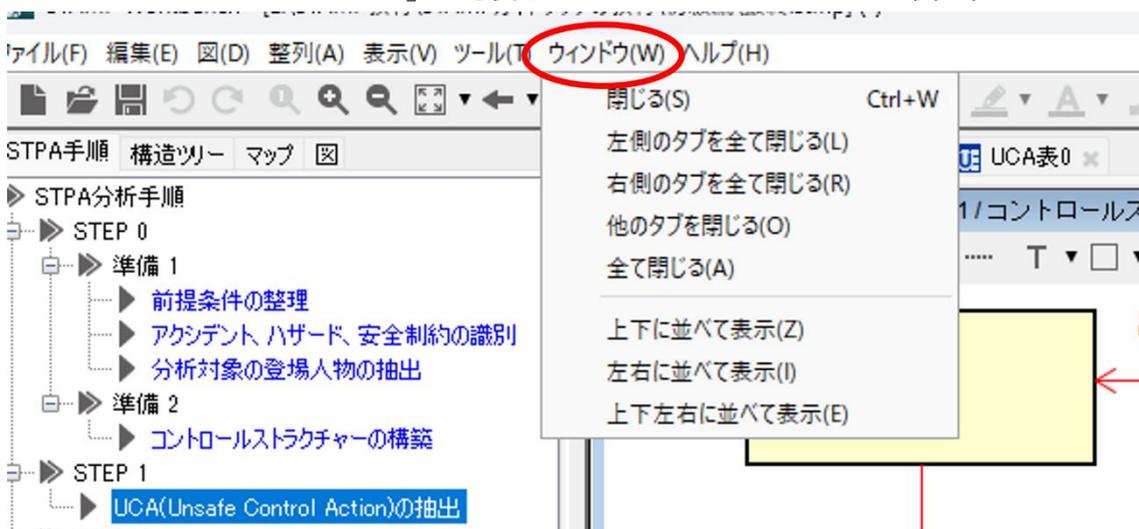
一画面に複数 window を表示する、CS 図と UCA 表を同時に見ながら UCA を考える

STAMP Workbench を用いて分析（思考）するとき、異なる画面を行ったり来たりするのは思考の妨げになるので、関係する情報を一度に見たくなります。そういうときには STAMP Workbench の「ウィンドウ」機能を用いて、1 画面内に複数の Window を表示することが有効です。

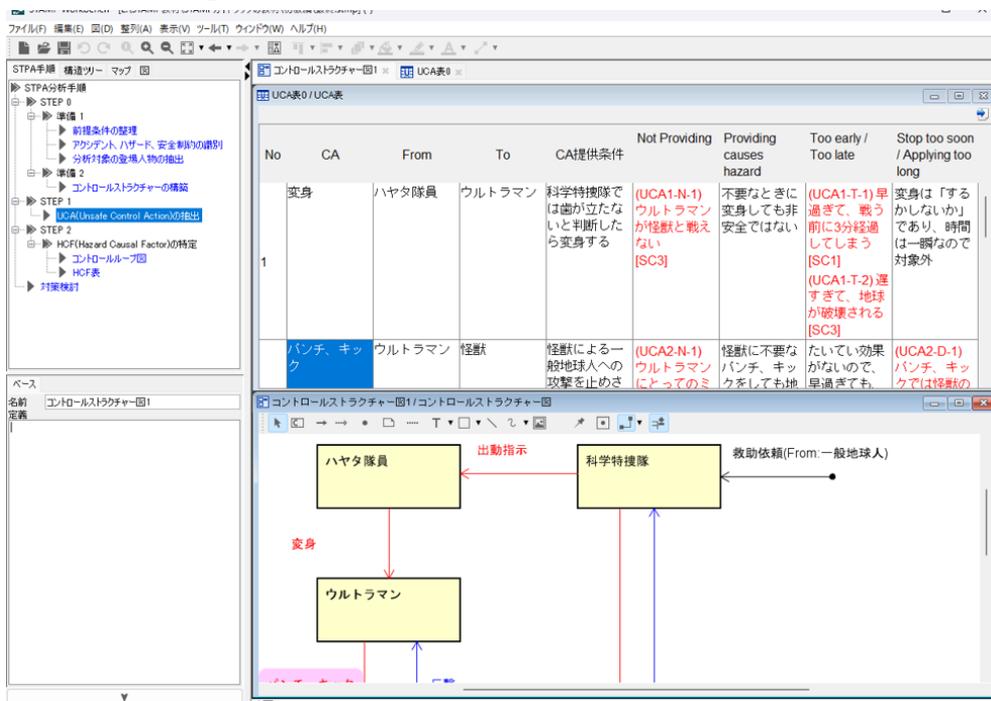
1. 同時に見たい Window を開く。



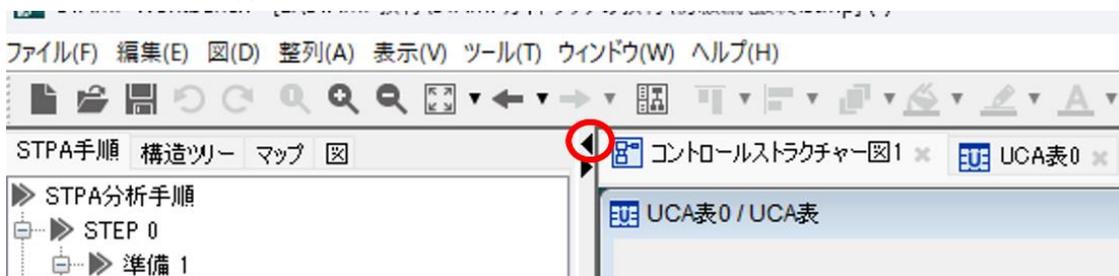
2. ツールバーの「ウィンドウ」を選択してポップアップウィンドウを開く。



3. ポップアップウィンドウで、「上下に並べて表示」、「左右に並べて表示」、「上下左右に並べて表示」から並べたい配置を選ぶ。



4. 画面を最大化するため、左側のプロジェクトペインを隠す。プロジェクトペインの右上の◀ボタンを押す。



5. マルチウィンドウになったら、それぞれのウィンドウサイズを変更したり、配置を変えて、見易くする。

下図の1枚目は2つの Window を同時に表示。2枚目は3つの Window を同時に表示。1枚目の図では、CS 図と UCA 表を同時に見ながら UCA を考えるときに良く使うものと思われる。この例では、CS 図の中の着目する CA に関するコントロールループのみを表示している。2枚目の図では、コントロールループと UCA を見ながら HCF やシナリオを考えるとときに有効。

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	変身	ハヤタ隊員	ウルトラマン	科学特捜隊では歯が立たないと判断したら変身する	(UCA1-N-1)ウルトラマンが怪獣と戦えない [SC3]	不要なときに変身しても非安全ではない	(UCA1-T-1) 早過ぎて、戦う前に3分経過してしまう [SC1] (UCA1-T-2) 遅すぎて、地球が破壊される [SC3]	変身は「するかしないか」であり、時間は一瞬なので対象外
2	パンチ、キック	ウルトラマン	怪獣	怪獣による一般地球人への攻撃を止めさせる必要があると判断	(UCA2-N-1)ウルトラマンにとってのミッション未達。但し、地球にとって非安全ではないので、以降の分析の対象外 [SC5]	怪獣に不要なパンチ、キックをしても地球防衛にとって非安全ではない	たいして効果がないので、早過ぎても、遅すぎても非安全ではない	(UCA2-D-1)パンチ、キックでは怪獣の攻撃を止められないという判断が遅れ、スペシウム光線を使う機会を逃す [SC1]
	スペシウム光線	ウルトラマン	怪獣	パンチ、キックでは3分以内に退治できないと判断。怪獣に密着してい	(UCA3-N-1)怪獣を退治できない [SC1]	殺さなくても退治できるのに怪獣を殺してしまうが、地球防衛にとって	早過ぎると殺さなくても退治できるのに怪獣を殺してしまうが、地球防	(UCA3-D-1)光線照射時間が短くて怪獣を倒せない [SC1]

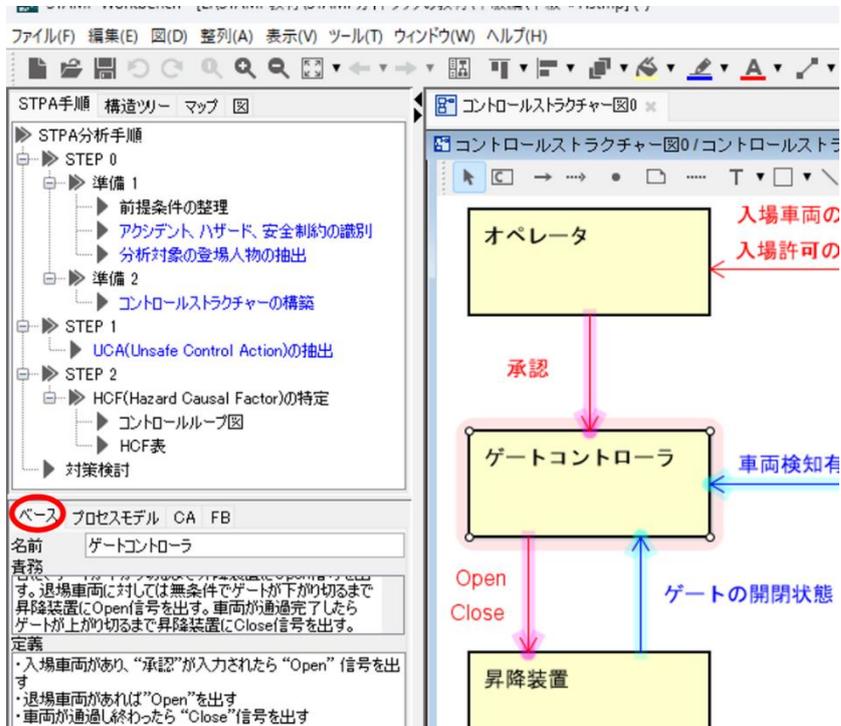
ID	HCF	ヒントワード	シナリオ
HCF1-T-1	怪獣が現れる前に変身してしまう。怪獣がすぐに現れなかったため3分経過してしまう	(4)コミッションエラー	怪獣に破壊行為を始めさせないため、怪獣の出現に先回りして変身したが、怪獣の出現が遅れた

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	変身	ハヤタ隊員	ウルトラマン	科学特捜隊では歯が立たないと判断したら変身する	(UCA1-N-1)ウルトラマンが怪獣と戦えない [SC3]	不要なときに変身しても非安全ではない	(UCA1-T-1) 早過ぎて、戦う前に3分経過してしまう [SC1] (UCA1-T-2) 遅すぎて、地球が破壊される [SC3]	変身は「するかしないか」であり、時間は一瞬なので対象外
2	パンチ、キック	ウルトラマン	怪獣	怪獣による一般地球人への攻撃を止めさせる必要があると判断	(UCA2-N-1)ウルトラマンにとってのミッション未達。但し、地球にとって非安全ではないので、以降の分析の対象外 [SC5]	怪獣に不要なパンチ、キックをしても地球防衛にとって非安全ではない	たいして効果がないので、早過ぎても、遅すぎても非安全ではない	(UCA2-D-1)パンチ、キックでは怪獣の攻撃を止められないという判断が遅れ、スペシウム光線を使う機会を逃す [SC1]
	スペシウム光線	ウルトラマン	怪獣	パンチ、キックでは3分以内に退治できないと判断。	(UCA3-N-1)怪獣を退治できない [SC1]	殺さなくても退治できるのに怪獣を殺してしまうが	早過ぎると殺さなくても退治できるのに怪獣を殺し	(UCA3-D-1)光線照射時間が短くて怪獣を倒せない [SC1]

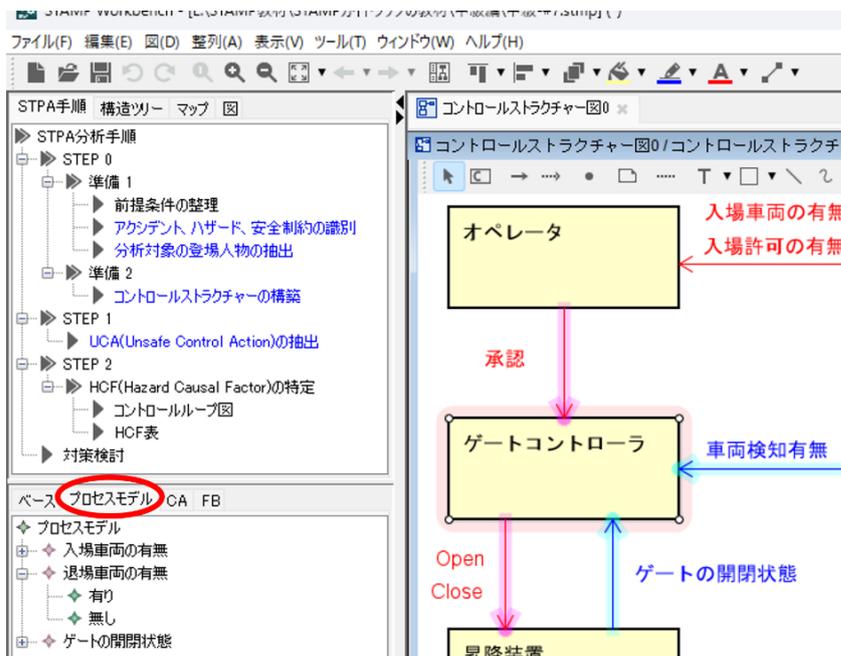
CS 図を見ながらコンポーネントの責務を確認する、プロセスモデルを入力する

CS 図を見ながら CA や UCA を考えているとき、考えている最中の対象コンポーネントの責務や input/output などを確認する場合、コンポーネント抽出表を見れば書いてあるが、画面を変えずにサッと確認したいことがある。その場合は、画面左下のペインに表示させることができる。

1. CS 図で対象コンポーネントを選択。
2. 画面左下のペインでベースタグを押す（デフォルトはベースタグの画面が表示されている）。

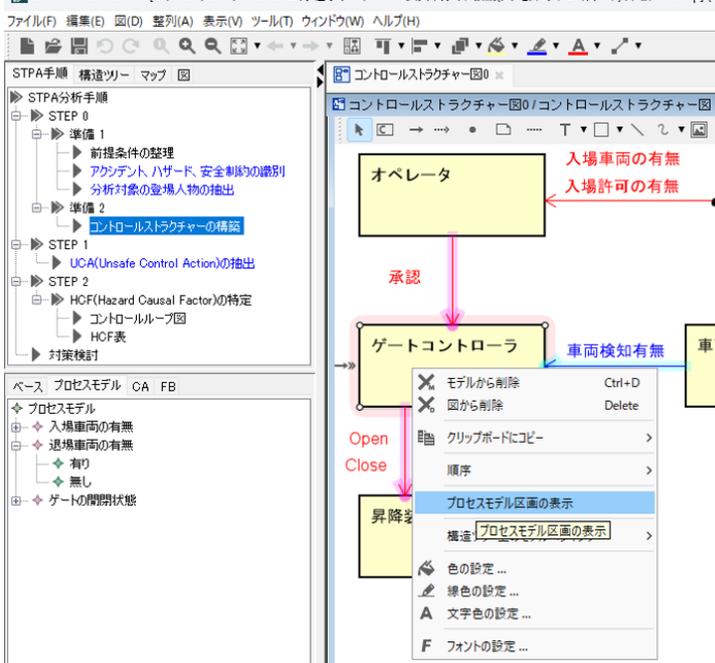


3. プロセスモデルの入力もこの画面のプロセスモデルタグを押してから入力、編集できる。

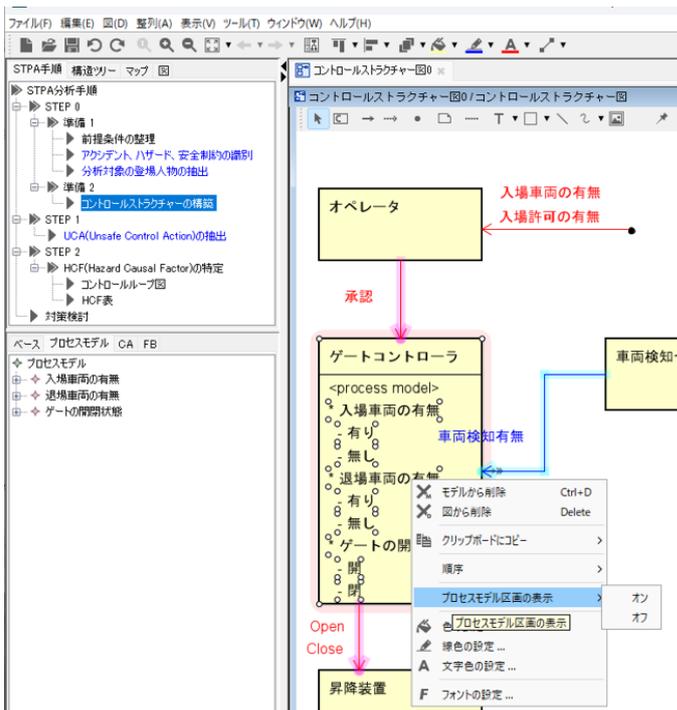


プロセスモデルを表示する

プロセスモデルをコンポーネント内に表示するには、CS 図でコンポーネントを選択し、コンテキストメニューを開き（右クリック）、「プロセスモデル区画の表示」を選択する。



プロセスモデルをコンポーネント内に表示すると、表示する分だけコンポーネントが大きくなるので、CS 図内でのコンポーネント配置を再度編集する必要がある。プロセスモデルを表示してみて見難いと思ったら、「プロセスモデル区画の表示」をオフにして戻せば良い。



分析している最中に、一時的にプロセスモデルを表示したいと思った時だけ表示するのも良い。UCA を識別するときにはプロセスモデルの表示がとても有用だが、分析結果をレビューするときには相互作用に注目して欲しいのでプロセスモデルの表示は目障り、というケースもある。

Power Point では難しいことですが、STAMP Workbench はモデリングツールなので、表示のオン/オフ切り替えは容易ですし、切り替えの際に修正ミスも有り得ません。利用場面に応じて柔軟に切り替えてご利用ください。

■STAMP 及びツールのノウハウ

UCA はコントロールループで考える

UCA を識別するときには、CA と FB から成るコントロールループの単位を対象として考える。

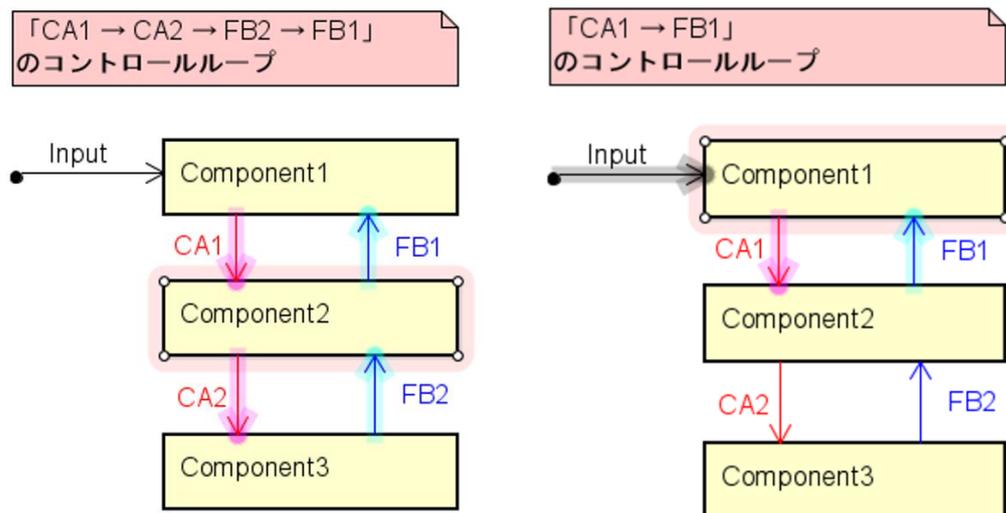
下図のような CS 図において、外界からの input をトリガーとして、必ず「CA1 → CA2 → FB2 → FB1」の順番となるシステムもあります。その場合、CA1 に関する UCA を識別するのに「CA1 → FB1」のコントロールループで考えるのか、「CA1 → CA2 → FB2 → FB1」のコントロールループで考えるのか、悩ましいことがあります。

結論から言うと、UCA の識別においてはどちらでも構いません。

但し、ハザードシナリオを抽出する際には、「CA1 → CA2 → FB2 → FB1」のコントロールループの方が考え易いかもしれません。

UCA の識別では「CA1 → FB1」のコントロールループで考えて、ハザードシナリオの抽出では「CA1 → CA2 → FB2 → FB1」のコントロールループで考える、というのでも構いません。

STAMP/STPA は柔軟な手法であって、このような細かなルールを強制しません。



UCA の識別では原因を考えない（思いついても我慢）

UCA を識別するときには原因を考えないようにします。原因を考えながら UCA を識別しようとすると、原因を思いつかないケースでは UCA が識別できなくなります。原因を先に考えたら、対象システムについての知見が有るか否かに分析結果が依存することになります。

UCA の識別では、4 つのガイドワードを参考にして、漏れの無い『観点』から論理的に識別します。STAMP/STPA において、『観点』として漏れが無いことを示せることが重要で、

分析の有効性を説明する際の肝となります。

それでも原因を思いつくことはあります。それは不必要な思いつきではなく、次のステップで HCF やハザードシナリオを特定する際にとっても有用な思いつきです。その貴重な思いつきは捨てることなくメモに残しておき、次のステップに役立てます。

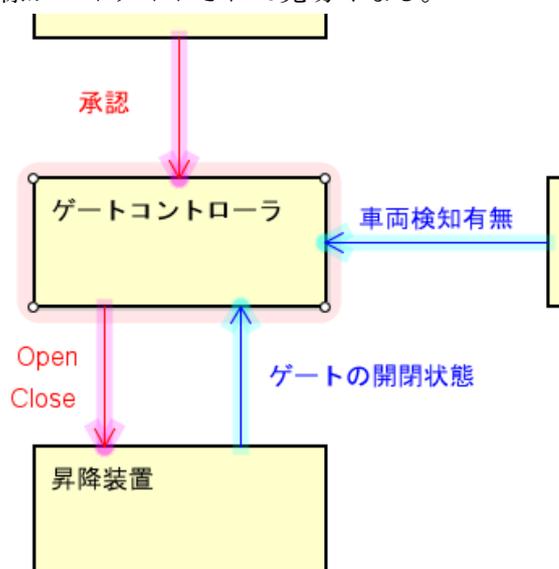
大事なことは、UCA を識別するときには先に原因を考えない。思いついてもその原因だけに捕らわれないように我慢することです。

コントロールループ図は必要？

コントロールループ図（CL 図、CLD）は必ずしも描かなくても良いです。

コントロールループ図を描く目的は、CA・FB からなるコントロールループの中に存在し得るハザード要因（HCF）を探しやすくすることです。CS 図でコンポーネントの数が多く、少し複雑な場合には着目する CA のコントロールループが見つらなくなるため、対象コントロールループだけを抜き出してコントロールループ図を作成します。しかし、それほど複雑な CS 図でなかったり、コントロールループを見失うことが無い CS 図ならば、コントロールループ図を作成する意味がありません。

下図では、Open/Close の CA を含むコントロールループは、Open/Close の CA とゲート開閉状態の FB から成ることが明確なので CL 図を作成するまでもない。下図のように対象 CA を発出するコンポーネントを選択すると、そのコンポーネントが直接関与する CA 線と FB 線がハイライトされて見易くなる。



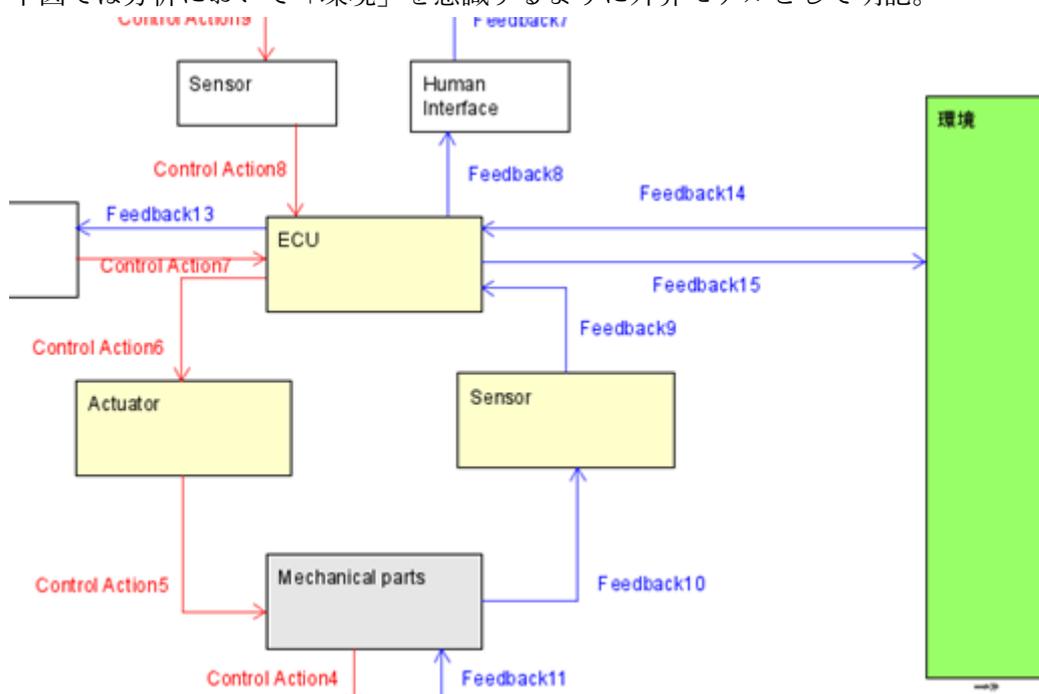
外界モデル

コントロールストラクチャー図（CS 図、CSD）やコントロールループ図（CL 図、CLD）

において、一般的にはシステム外のコンポーネントは記述しません。しかし、外界の何とのインタラクション（何から input を受け取る／何に対して output を発出する）かを記述しておきたい場合もあります。その場合は、外界モデルとしてコンポーネントを記述する方法が都合が良いでしょう。

但し、気を付けて欲しいことは、外界モデルとの CA や FB のやり取りは無いはずで、外界モデルとのやり取りは input/output だけになります。CA や FB が出てきたときにはシステム境界の定義が曖昧になっていると考えられるので、現在の分析対象範囲はどこまでなのかを再確認してください。

下図では分析において「環境」を意識するように外界モデルとして明記。



対策表の備考欄にシナリオをコピーする

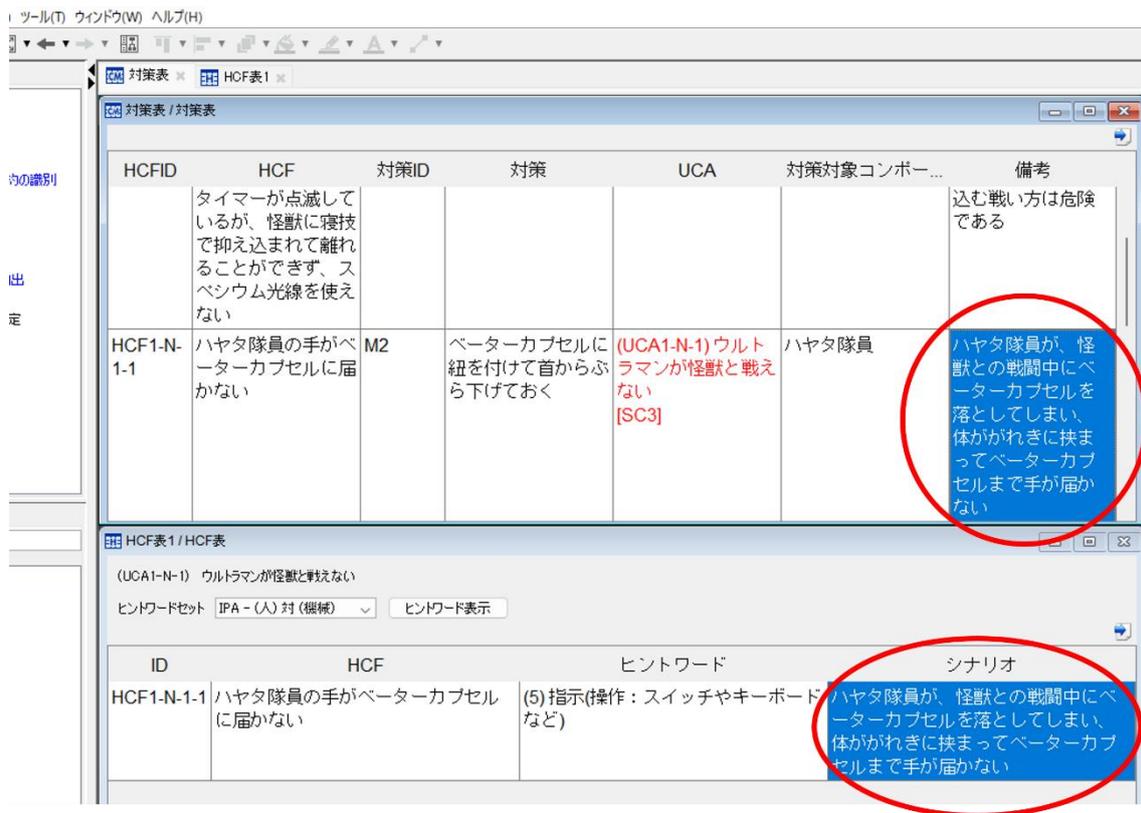
対策表の備考欄に、手動で HCF のシナリオをコピーしている。

ツールへの要望

このコピー作業を自動化するか、対策表に列を追加してシナリオが自動的に表示されると良い。

この対策はツールが自動的にサポートすることが望ましいが現状サポートできていません。

下図では、HCF 表と対策表の 2 つの Window を上下に並べて 2 画面表示しているが、対策表の備考欄にシナリオをコピーしておけば 2 画面表示しなくても済む。



対策表に【機能】【運用】【教育】など分類を記載した

対策のところに【機能】【運用】【教育】など分類を記載し後から見やすくした。

対策表を Excel 出力して、列を増やし、それぞれの対策に【機能】【運用】【教育】などの分類を記載して、後で他の人が対策表を見たときに、次の開発ステージであるコンポーネント設計に対するコンポーネント安全制約なのか、運用で考慮するという対策なのか、設計者・運用担当者に対して教育すべき事項なのか、が分かるようにした。

このように自社独自、自プロジェクト独自の ID や分類などを表に追加する機能は STAMP workbench に備わっていないので、Excel ファイルに出力してから Excel で列を追加して対応した。

人のコミュニケーションの対策例 3way コミュニケーション

人のコミュニケーションの対策例として 3way コミュニケーションという方法がある。

3way コミュニケーションとは **伝達→復唱→確認** のこと。

(「指示する」、「指示を復唱する」、「指示をもう 1 回繰り返して確認する」)

伝達：「〇〇してください」

復唱：「〇〇ですね？」

確認：「はい、〇〇です」

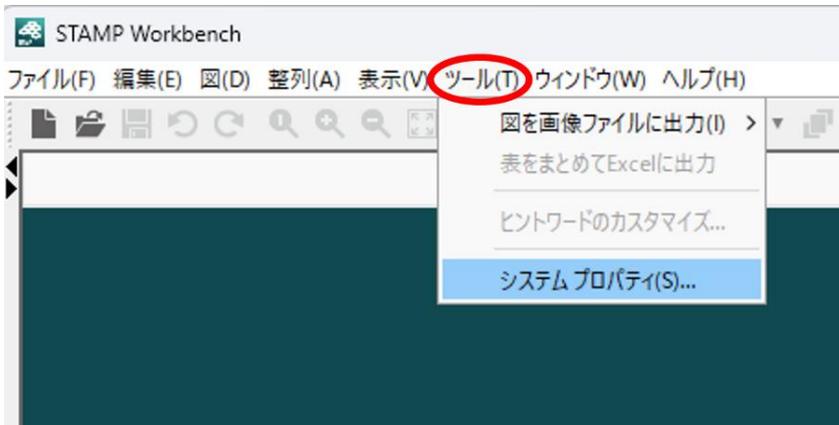
原子力業界では一つの操作ミスが重大なトラブルに繋がったり、地域住民の信頼を損ねることに成り得るためコミュニケーションは重要な課題として捉えられており、3way コミュニケーションが行われているそうだが、3way コミュニケーションの伝達→復唱→確認という一連の流れは原子力業界以外でも重要な指示に対して有効と考えられる。対策例として参考にして欲しい。

■注意事項

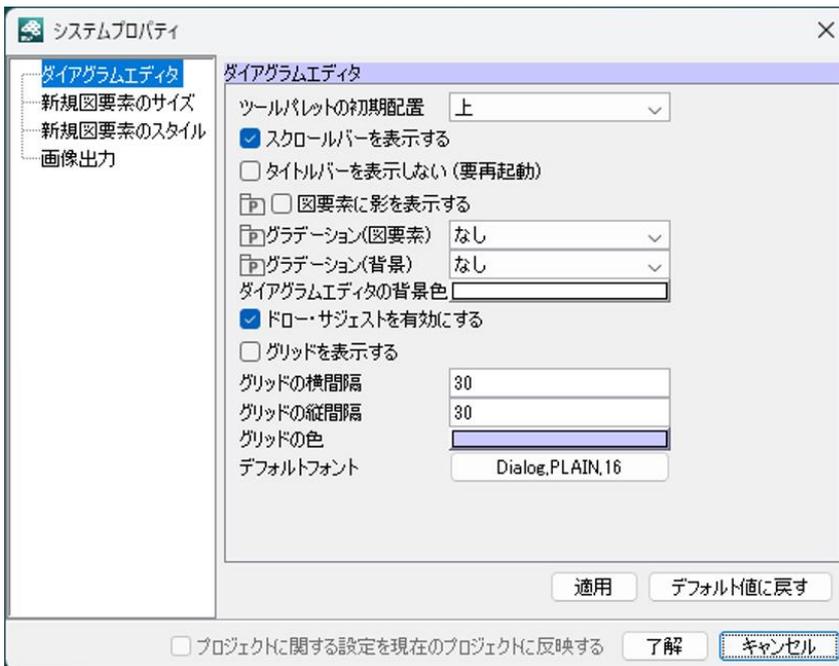
ダークモード（ハイコントラストモード）

Windows の設定で「ハイコントラストモード」を有効にして、「ハイコントラスト：黒」とすると一部の文字が読めない問題が確認されています。STAMP Workbench は「ハイコントラストモード」での文字・図形色自動変更に対応していないため、黒地に黒文字／黒線のような設定となり文字が読めなくなる現象です。ツール -> システムプロパティの「ダイアグラムエディタ」や「新規図要素のスタイル」で背景・図形・線・文字の色を選択することをお試しください。

1. システムプロパティ画面を起動



2. 「ダイアグラムエディタ」で背景や図要素の色を変更



3. 「新規図要素のスタイル」で文字・線色を変更



Excel 出力時の問題

MS Office の性能限界への対応方法です。Excel では既定の列幅最大値が 255 文字 (MS Office のバージョンに依る) となっているため、STAMP Workbench で表の列幅 (セル幅) を 256 文字以上にした場合、Excel 出力時にエラーが発生する可能性があります。

4K 以上のディスプレイで高解像度設定し、かつ縮小表示して、STAMP Workbench のウィンドウを全画面表示し、更にセル幅が 255 文字を超えるようにした場合、STAMP Workbench の表を Excel 出力したときにエラーが発生します。但し、エラー発生時に STAMP Workbench が保持するデータが壊れたり、失われたりすることはありません。

Excel 出力を実施する前に、STAMP Workbench のウィンドウ幅を少し小さめに変更することで問題を回避できます。