STAMP/STPAを用いた
リスクマネジメントフレームワークの提案

2017年11月29日

金 勳熙(Kim Hoonhee)、酒井 直彦、阿野 基貴

株式会社電通国際情報サービス

ISID (Information Services International-Dentsu, Ltd.)

ISID概要

ISIDは誠実を旨とし、革新的で創造性あふれる専門家集団として、情報技術の先進的活用により顧客企業と社会の発展に貢献します。

企業情報

商　　号	：	株式会社　電通国際情報サービス Information Services International-Dentsu, Ltd.
本　　社	：	東京都港区港南2-17-1
代 表 者	：	代表取締役社長　釜井　節生
設　　立	：	1975年12月11日 （株式会社電通と米国「General Electric Company」の合弁 2000年11月　東証1部上場
資 本 金	：	81億8050万円
連結売上	：	79,783百万円（2016年12月期）
従 業 員	：	連結　2,635名（2016年12月末現在）
U R L	：	www.isid.co.jp

GE ×dentsu

事業内容

- コンサルティング・サービス
- ソフトウェア・プロダクト販売/サポート
  - ・自社開発ソフトウェアの販売/サポート
  - ・国内外ベンダーのソフトウェアの販売・サポート
- システム・インテグレーション・サービス
  - ・アプリケーション・システムの設計/開発
  - ・ハードウェアの選定/調達
  - ・システム・インフラの構築サービス
- アウトソーシング・サービス

ソリューション

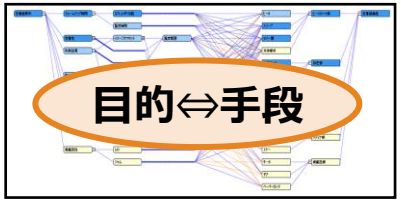
- **エンジニアリングソリューション**
- ビジネスソリューション
- 金融ソリューション
- コミュニケーションITソリューション

iQUAVIS（アイクアビス）とは

◆ 論理的に考えて、複雑なつながりを整理して、手順に落とし込むための、
「見える化」を支援するシステム

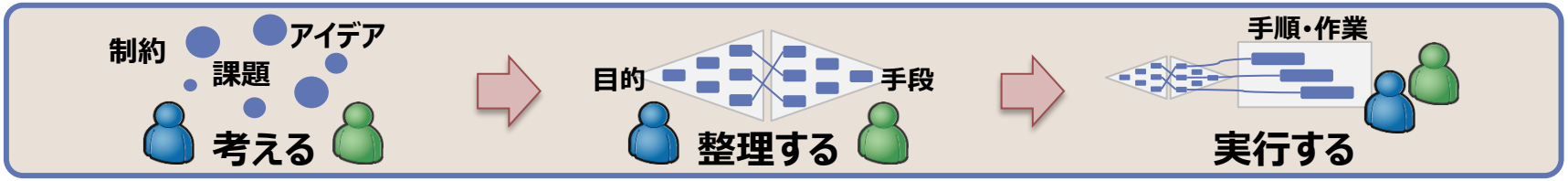
iQUAVIS

- モノ・サービスの成り立ちの見える化
- プロセスの見える化

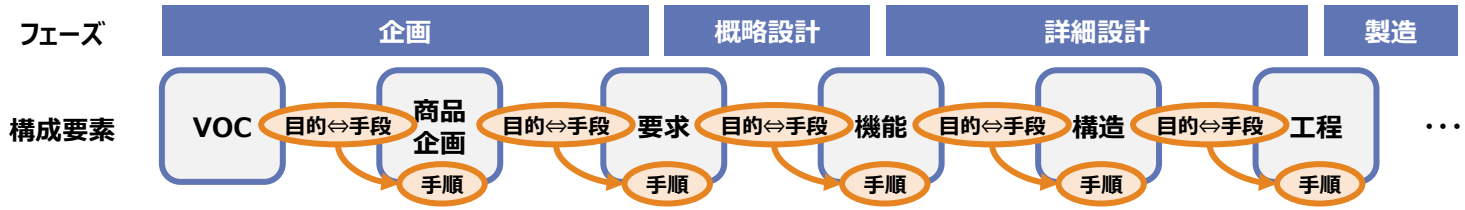


目的達成の手段を
抽象的に捉えて
構造化して考える

実際の制約を考慮し
目的達成の手順・作業
を具体化・実施する



【適用例】製造業の開発業務



目次

1. Motivation

- 製品の複雑化 ⇒ 統合的な観点が必要
- 設計作業量の膨大化 ⇒ 既存手法との違いを理解し低負荷の作業追加で留めたい

2. Background

- 開発現場で使われているリスク管理ツール (FMEA/DRBFM/FTA/HAZOP)
- 弊社(ISID)のリスク管理手法について紹介
  - (システム)ブロック図作成・機能の見える化
  - 機能ベースのリスク抽出・検討　【技術リスク管理】
  - リスク対策の日程の見える化　【日程リスク管理】

3. STAMP/STPAを用いたリスクマネジメントフレームワーク

- STAMP/STPAの適用
- (ISIDの)リスクマネジメントフレームワークへSTAMP/STPAを導入

4. 今後に向けて

5. まとめ

1. Motivation

- 製品の複雑化 ⇒ 統合的な観点が必要
- 設計作業量の膨大化 ⇒ 既存手法との違いを理解し低負荷の作業追加で留めたい

2. Background

- 開発現場で使われているリスク管理ツール (FMEA/DRBFM/FTA/HAZOP)
- 弊社(ISID)のリスク管理手法について紹介
  - (システム)ブロック図作成・機能の見える化
  - 機能ベースのリスク抽出・検討　【技術リスク管理】
  - リスク対策の日程の見える化　【日程リスク管理】

3. STAMP/STPAを用いたリスクマネジメントフレームワーク

- STAMP/STPAの適用
- (ISIDの)リスクマネジメントフレームワークへSTAMP/STPAを導入

4. 今後に向けて

5. まとめ

1. Motivation

製品間コンバージェンスや機械製品のIT化に伴い、製品の複雑化が増している。

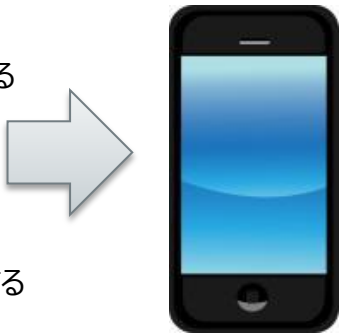
■ 製品間コンバージェンスの例

遠い所の人と話す

残したい瞬間をイメージで保存する

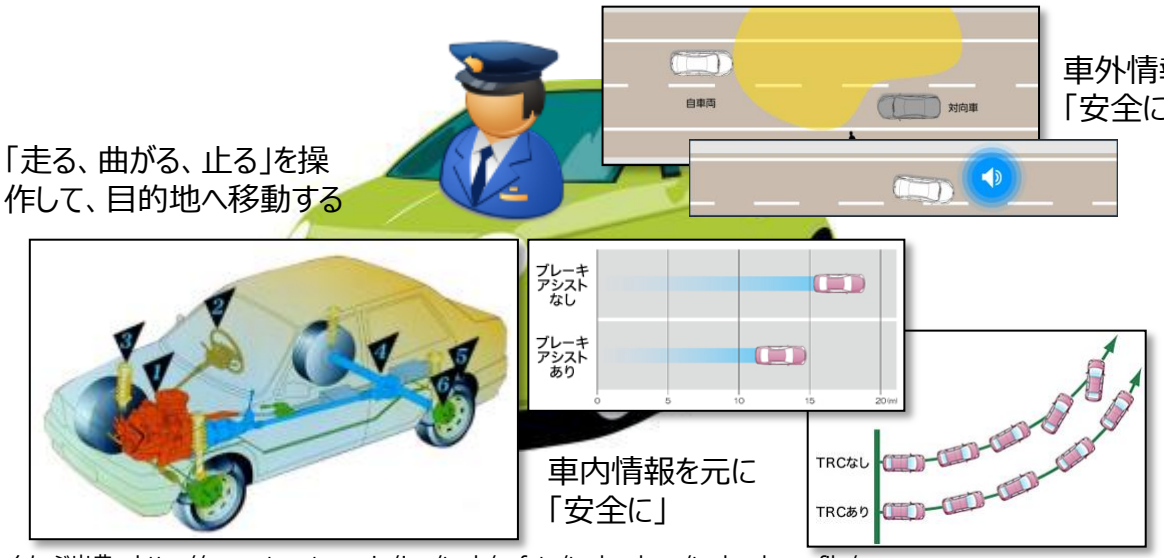
ゲームを楽しむ

情報を取得・分析・加工・入力する



■ 機械製品の電子化・IT化の例

「走る、曲がる、止る」を操作して、目的地へ移動する



車外情報を元に「安全に」

車内情報を元に「安全に」

イメージ出典：http://www.toyota.co.jp/jpn/tech/safety/technology/technology_file/

「快適に」目的地へ移動する

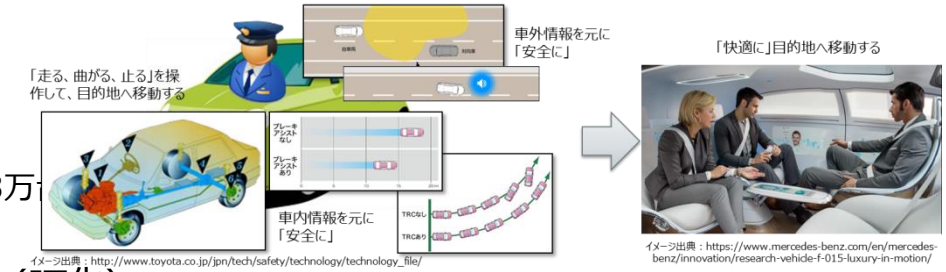
イメージ出典：https://www.mercedes-benz.com/en/mercedes-benz/innovation/research-vehicle-f-015-luxury-in-motion/

1. Motivation

製品が複雑化することで、開発時想定外の問題が発生している。

- **スマホ**(製品間コンバージェンスの例)
  - 複数機能を同時に動かせた場合、片方の機能が不安定になる。
    - 電話しながらゲームをすると、電話が途切れる / よく切れる。
  - 以前は問題にならなかったことが浮き彫りになる。
    - 電話中でもないのに、スマホが熱くなって火傷をする / 火事になる。

- **自動車**(機械製品の電子化・IT化の例)
  - 電子部品やそれに関する処置による不具合 (電子化)
    - ハイブリッドシステムの電力変換機の制御ソフトが不適切。(35万台)
    - 電子部品保護用のシール剤が熱で軟化し他部品へ浸入・エンスト(3万
    - 電子部品の配線や接続部の固定が不適切で、機能欠落(2万台)
  - 先進技術(Advanced Safety Vehicle)機能搭載の不具合 (IT化)
    - 衝突被害軽減ブレーキ(H26 0件 ⇒ H27 4件)、定速走行 (H26 1件 ⇒ H27 2件)で増加。
    - 今後、ASV機能搭載車両の増加と共に不具合件数の増加も考えられる。



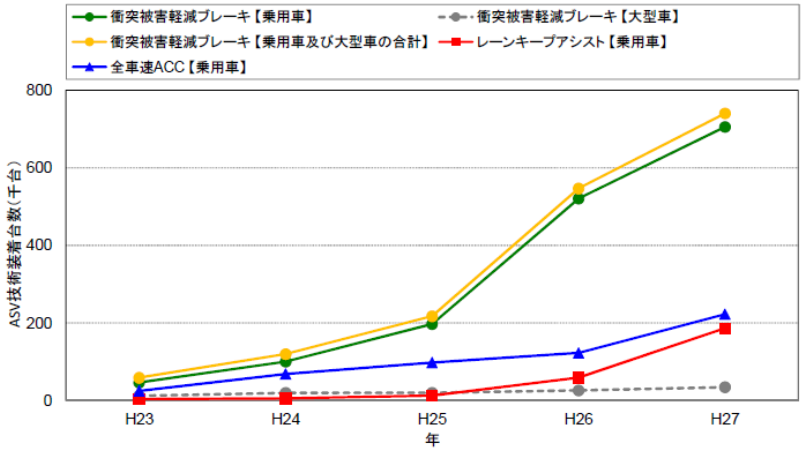


図 1-26 ASV 技術の装着台数（平成 23 年～平成 27 年）

出典：国土交通省「平成27年度リコール届出内容の分析結果について」
http://www.mlit.go.jp/jidosha/carinf/rcl/data.html

1. Motivation

これから益々「(技術横断の)システム観点」での開発手法・アプローチが必要になる。

- **STAMP(STPA/CAST)は全体システム観点で物事を捉えられる手法の一つである。**
  比較的新しい手法であるため、開発現場への導入には注意すべきところがある。

- **手法・方法論導入の際、大事なこと**

  a. 方法論の位置づけ、導入の目的を明確にすること
  : 今までのやり方と何がどう違って、どんなベネフィットがあるかを明確に伝える。

  b. 現場に新たな負担を与えないこと
  : 開発プロセス(設計手順書、レビュー)の中で、既に山ほどのチェックリストや方法論が盛り込まれているので、「STAMPが良いことは分るが、現状の業務を回すだけで精一杯」という反応になりかねない。

  c. 方法論の推進担当者が明確に存在すること
  : 導入する方法論を理解し自社のプロセスに合わせて展開できる推進担当者が明確に存在すること。
  そして、方法論の推進業務が推進担当者の業務目標として設定されて、やっと能動的に動くことになる。

  d. 事例(Best Practice)を作り・横展開、開発プロセスに載せること
  : 携わっている製品・部品へ適用して事例を作り、上へ報告することで、他部署への展開を促す。
  そして、既存開発プロセスに新たな(重い)負担にならない形で載せる。

- **本発表は、STAMPの位置づけを明確(a)にし、既存手法(プロセス)と適切に組合わせられること(b, d) を示し、開発現場への展開するための準備を目的にする。**

1. Motivation

- 製品の複雑化 ⇒ 統合的な観点が必要
- 設計作業量の膨大化 ⇒ 既存手法との違いを理解し低負荷の作業追加で留めたい

2. Background

- 開発現場で使われているリスク管理ツール (FMEA/DRBFM/FTA/HAZOP)
- 弊社(ISID)のリスク管理手法について紹介
  - (システム)ブロック図作成・機能の見える化
  - 機能ベースのリスク抽出・検討　【技術リスク管理】
  - リスク対策の日程の見える化　【日程リスク管理】

3. STAMP/STPAを用いたリスクマネジメントフレームワーク

- STAMP/STPAの適用
- (ISIDの)リスクマネジメントフレームワークへSTAMP/STPAを導入

4. 今後に向けて

5. まとめ

2. Background

多くの企業で製品、開発フェーズに合ったリスク管理手法を使い分けている。

- **開発現場で広く使われているリスク管理手法**
  - FMEA (Failure Mode and Effect Analysis) ：故障モードと影響解析
    - 壊れても被害が少なくする、壊れる可能性を低くするための対策が講じられているかを管理する手法

部品	機能	故障モード	要因	影響					設計対策	評価対策	製造対策
				影響詳細	影響度	頻度	検出	RPN			
後部赤外センサー	後部の障害物の在りかを検知する	赤外線の受光ができない	赤外センサーが壊れた。	後進時障害との衝突	7	3	5	105	赤外線の発光状態をチェックする回路を組み込む		
			赤外センサーが受光はできたが、何らかの原因で十分な受光ができなかった。	後進時障害との衝突	7	3	5	105	キャリブレーション方法やタイミングを定義し、製品に反映する。		

  - DRBFM (Design Review Based on Failure Mode)
    - 量産品から変更点を起点にFMEA実施することで、既存FMEAから信頼性・効率をアップを図った手法。

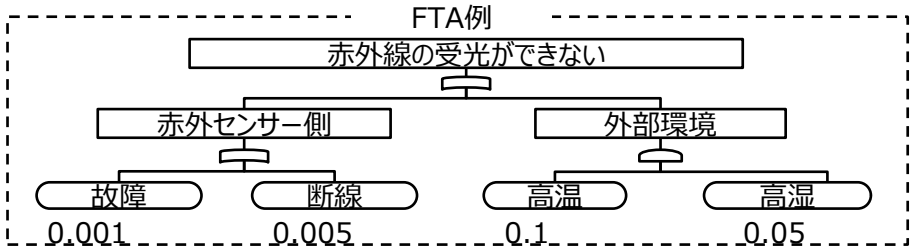
部品(変更点)	機能	心配点	要因	影響					設計対策	評価対策	製造対策
				影響詳細	影響度	頻度	検出	RPN			
後部赤外センサー	後部の障害物の在りかを検知する	赤外線の受光ができない	赤外センサーが壊れた。	後進時障害との衝突	7	3	5	105	赤外線の発光状態をチェックする回路を組み込む		
			赤外センサーが受光はしたが、何らかの原因で十分な受光ができなかった。	後進時障害との衝突	7	3	5	105	キャリブレーション方法やタイミングを定義し、製品に反映する。		

- 故障のパターンのその原因と影響・対策(優先度含め)を講じることが目的。

2. Background

多くの企業で製品、開発フェーズに合ったリスク管理手法を使い分けている。

- **開発現場で広く使われているリスク管理手法**
  - FTA (Fault Tree Analysis)
    - 望ましくない事象(Top Event)を定義し、ツリー形式でその発生原因・確率などを用いてHazardを評価・特定する手法。



  - HAZOP (Hazards and Operability analysis)
    - ガイドワードを使って、設計意図からの「ずれ」や「想定外」の事象を見つける
      - 「赤外線の受光の検知が・・・」

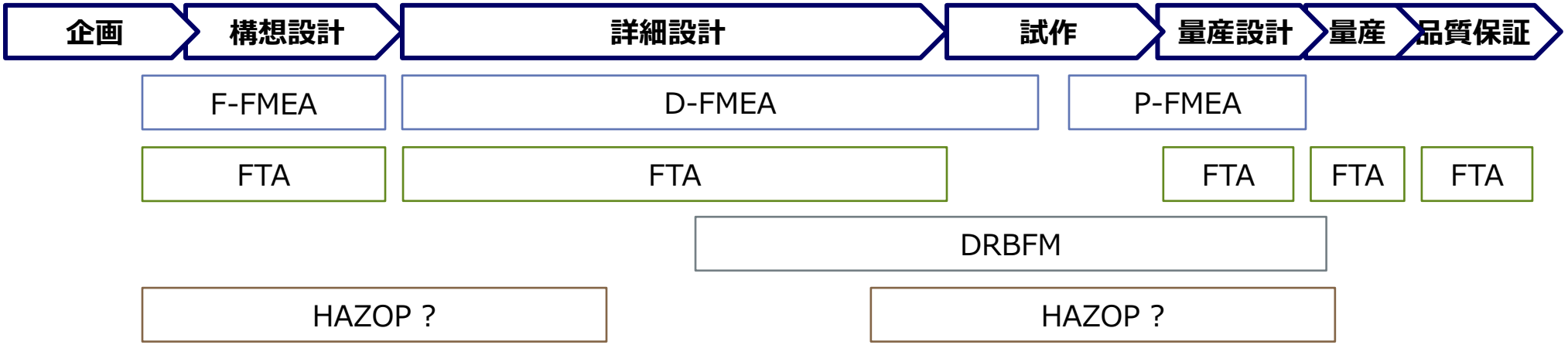
ガイドワード		外れ	原因	影響
存在	no	できない		
逆	reverse	続く		
空間	more	–		
	less	–		
	as well as	–		
	part of	–		
時間	early	早い		
	late	遅い		
	before	–		
	after	–		
その他	other than	外部からのストレスによりできない		

  - 故障(モード)やその原因(確率含め)を考えることが目的。

2. Background

既存リスク管理手法の特徴から各開発プロセスでどんなことが求められているかを検討。

■ 既存ツールの開発プロセス上での位置づけ



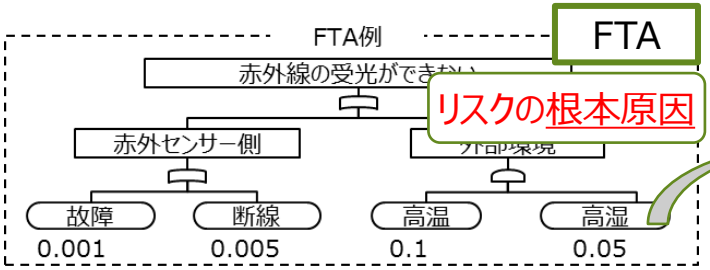
■ 各手法の特徴及び開発プロセス上で求められていること

手法	特徴	主な開発プロセス	各開発プロセスで求められていること
FMEA	・部品を機能観点で機能喪失時、その影響や対策を検討できる。 ・全ての機能(部品)に対し検討するため時間はかかるが、リスクの高い製品開発には向いている。	製品・量産設計	機能不全時のリスクや対策を検討したい
FTA	・ある事象(故障)に対する原因を論理的かつ定量的に分析できる。 ・ミッションクリティカルな機能や故障・不具合原因分析の際よく用いられる。	ほぼ全領域	現象の根本原因を分析したい
DRBFM	・量産品から変更点を起点に関連する所だけを検討できる。 ・部品数が非常に多く、検討工数がかかる製品に向いているが、部品(機能)間影響を知っている必要がある。	詳細・量産設計	変更点を中心に効率よく、機能不全時のリスクや対策を検討したい
HAZOP	・MECEなガイドワードを用い、設計意図からのズレを抽出できる。 ・化学プラント用手法として定着されているが、医療分野へも広げている。	構想設計	MECEにリスクを洗い出したい

2. Background

最近の製品トレンド(コンバージェンス、電子化・IT化)に既存リスク管理手法では足りない点がる。

- **各手法の役割と足りない所**



FTA

リスクの根本原因

☆全体システム観点でのリスク抽出

FMEA (DRBFM)

部品	機能	故障モード	要因	影響					設計対策	評価対策	製造対策
				影響詳細	影響度	頻度	検出	RPM			
後部赤外センサー	後部の障害物の在りかを検知する	赤外線の受光ができない	赤外センサーが壊れた。	後進時障害との衝突	7	3	5		赤外線の発光状態をチェックする回路を組み込む		
			赤外センサーが受光はできたが、何らかの原因で十分な受光ができなかった。	後進時障害との衝突	7	3	5		キャリブレーション方法やタイミングを定義し、製品に反映する。		

HAZOP

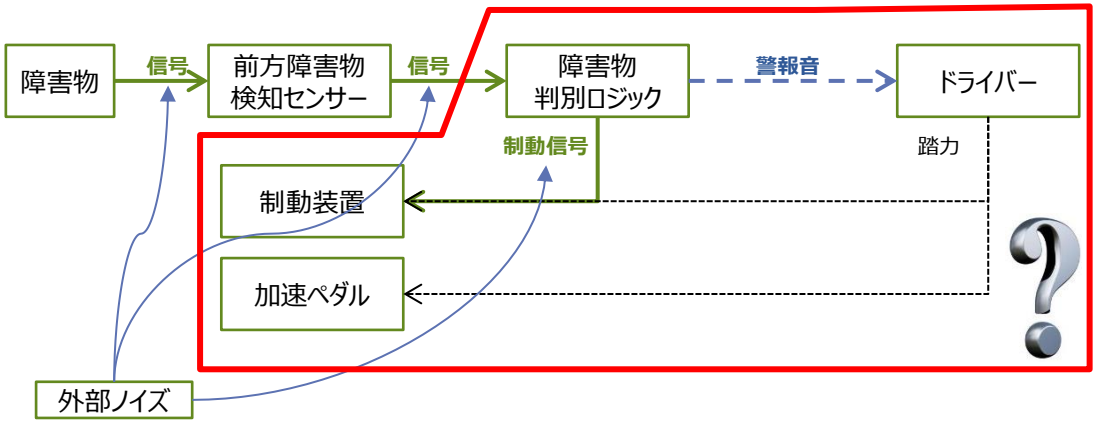
MECEなリスク抽出

ガイドワード		外れ	原因
存在	no	できない	
逆	reverse	続く	
空間	more	–	
	less	–	
	as well as	–	
	part of	–	
時間	early	早い	
	late	遅い	
	before	–	
	after	–	
その他	other than	外部からのストレスによりできない	

☆ **制御/制御対象の相互作用観点**でのリスク抽出

効率良い対策検討

- **上記手法だけでは検討漏れしやすいリスクは無いか**

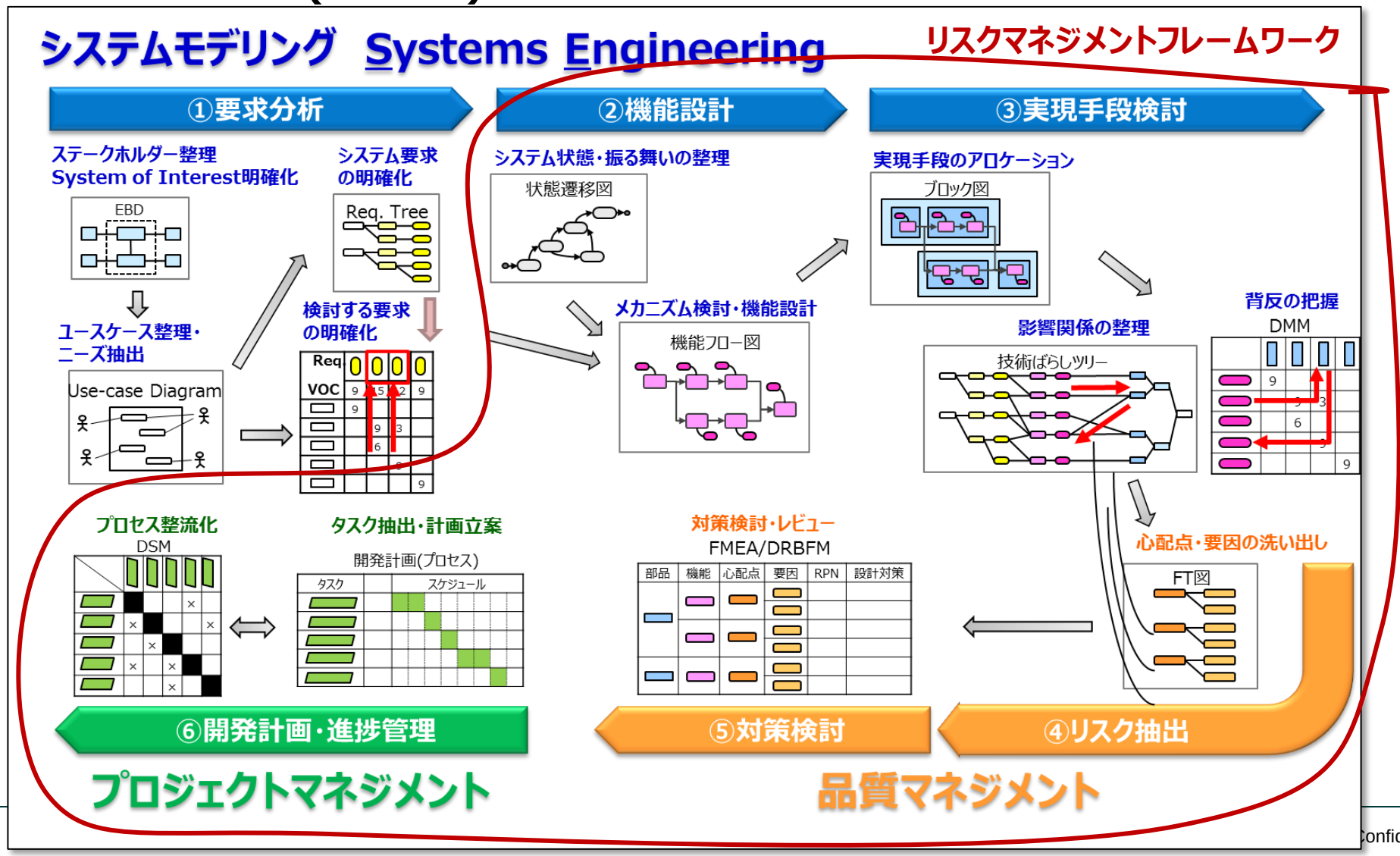


構成要素	リスク抽出観点		リスク	影響
前方障害物検知センサー	入力	誤信号	何らかの影響でないにも関らず	障害物がないにも関らず、急な制動がかかる
		不十分な強度の信号	表面汚れにより信号が弱まる	障害物があるにも関らず認識できない
	出力		何らかの原因で信号が遅れる	制動装置の動作開始が遅れる
障害物判別ロジック	入力		信号が入ってこない	障害物があるにも関らず認識できない
	判断処理		判断処理に時間がかかる	制動装置の動作開始が遅れる
	出力		警報音を鳴らさずに制動信号だけ送るケースがある	ドライバーが認識できない状態で制動がかかる
			警報音だけ鳴らし制動信号は送らない	ドライバーが制動をかけず衝突の可能性がある
制動装置	他装置と反対の操作		制動がかかっている状態だが、何らかの原因で制動がかからず、MAXで制動し続ける	制動装置に甚大な損傷を起こす可能性がある

2. Background

既存リスク管理手法に加え、リスク抽出・対策検討/管理手法を提案してきた。

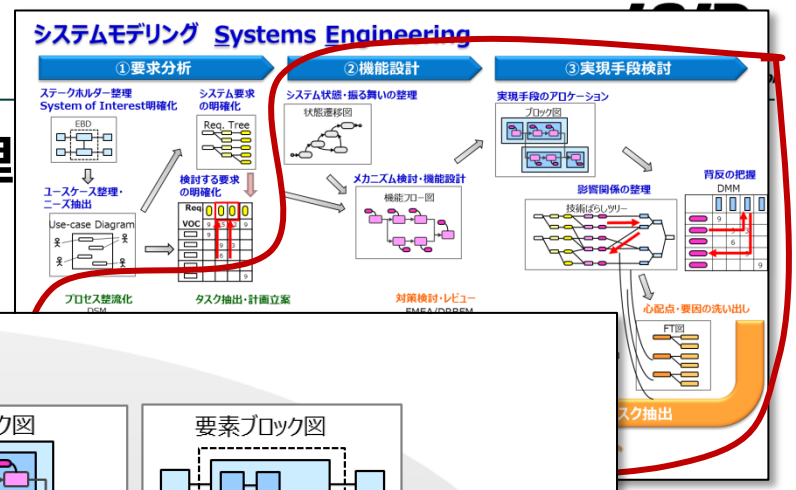
- **設計検討フレーム (ISID案)**

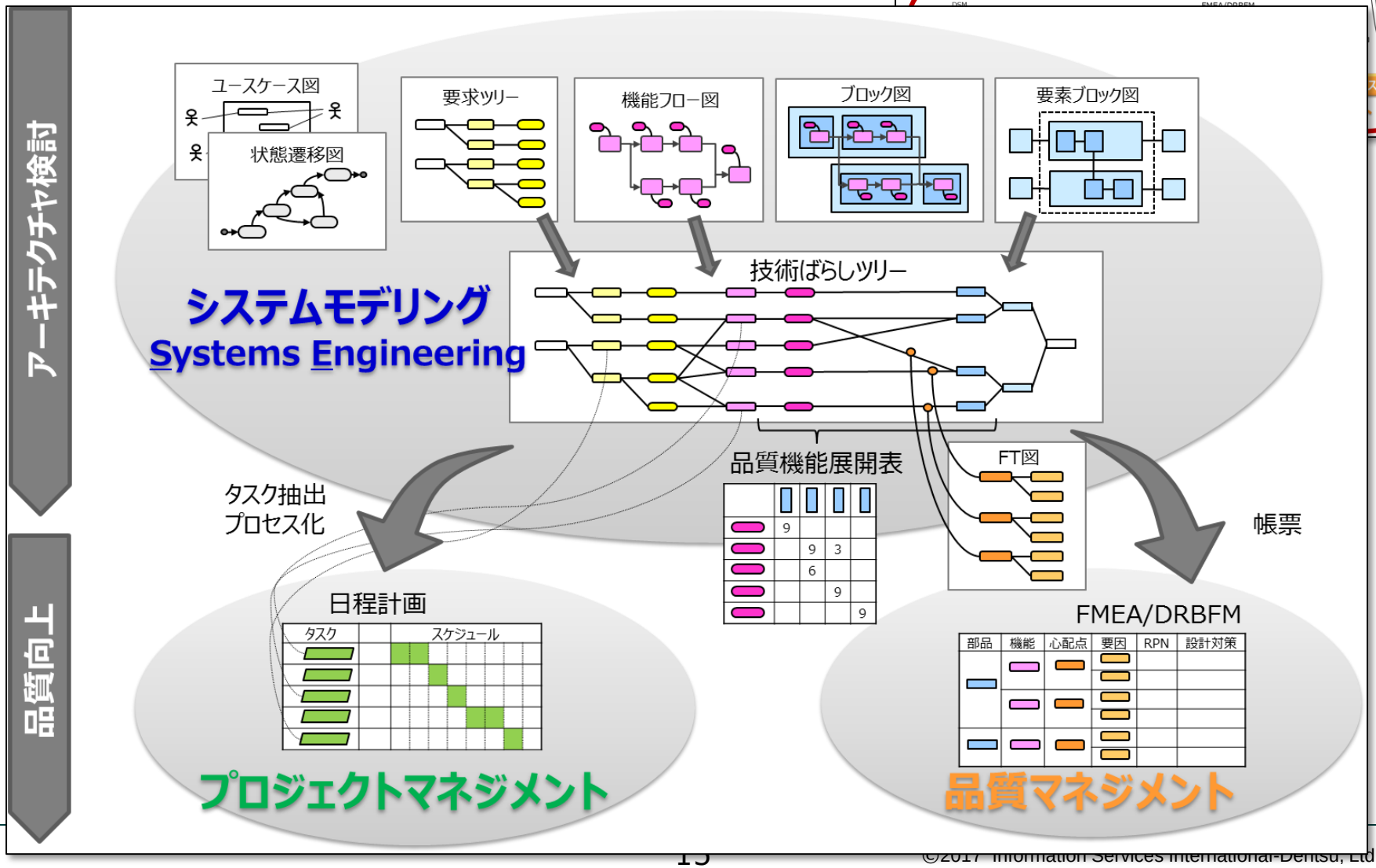


2. Background

既存リスク管理手法に加え、リスク抽出・対策検討/管理

- 設計検討フレーム (ISID案)

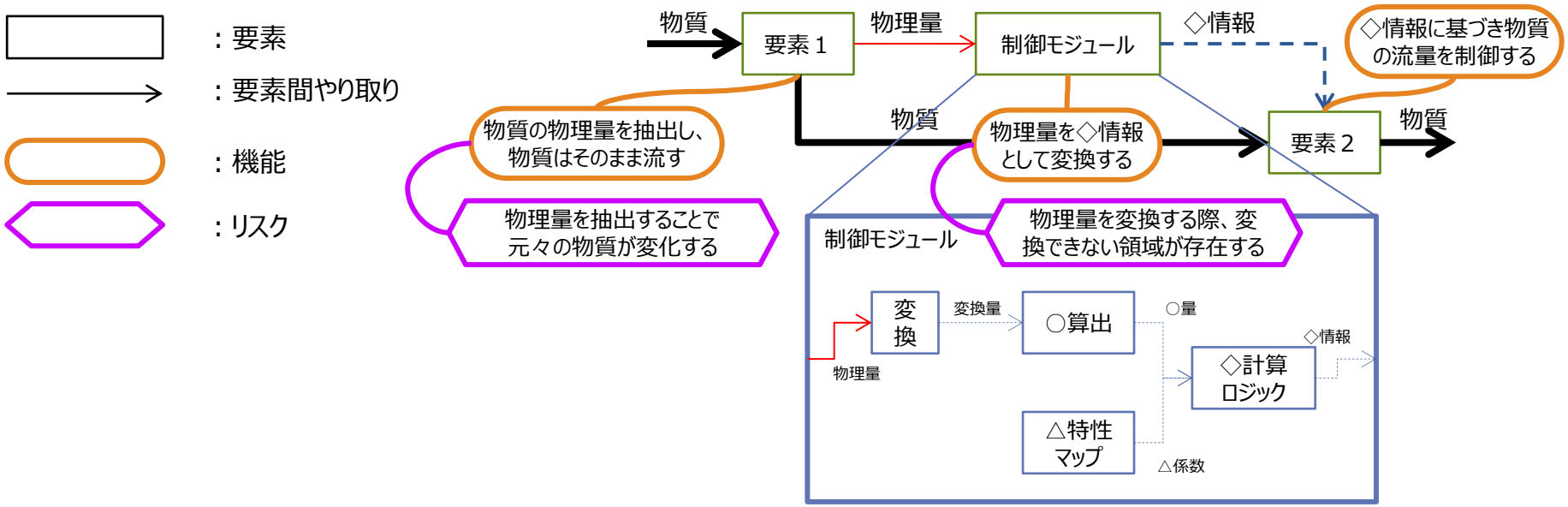




2. Background

既存リスク管理手法に加え、リスク抽出・対策検討/管理手法を提案してきた。

- **要素ブロック図**
  - システム構成要素や要素間やりとりされるもの(物質、情報、物理量)を見える化する手法



- **機能の見える化**
  - 要素の役割を機能として捉え直すことで、本来あるべき設計案(機能の妥当性)を検討させる。
- **機能をベースにリスク抽出**
  - 要素ではなく機能をベースにリスクを抽出することで、要素固有のリスクではなく、機能(実現方式)自体のリスクを検討することが可能になる。

2. Background

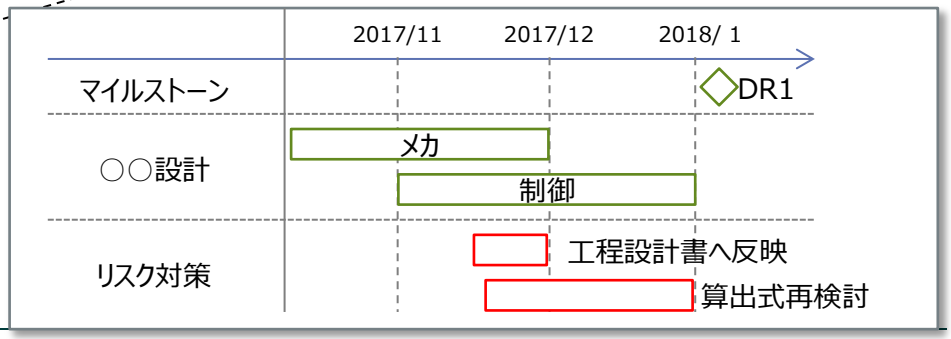
既存リスク管理手法に加え、リスク抽出・対策検討/管理手法を提案してきた。

- **要素ブロック図のリスク情報をFMEA(DRBFM)シートへ　　【技術リスク管理】**
  - ブロック図で抽出したリスク情報とFMEAシートのリスク情報とを連動させることで、**システム観点でのリスク抽出を実現**している。

部品	機能	リスク	要因	影響					設計対策	評価対策	製造対策
				影響詳細	影響度	頻度	検出	RPN			
要素１	物質の物理量を検出し、物質をそのまま流す	物理量を抽出することで、元々の物質が変化する	抽出時に物質のある一定の量を抽出・測定後廃棄するため	物質が常にもとの量より少なくなる	5	5	3	75	抽出される分を考慮して、物質を投入することを工程設計書に反映	…	…
制御モジュール	物理量を◇情報として変換する	物理量を変化する際、変換できない領域が存在する	変換時に使う○算出式で特異点が存在する	◇情報を算出できず、物質の流量を制御できない領域が発生する	9	3	7	189	算出式で特異点がないように式を立て直す	…	…
要素２	◇情報に基づき物質の流量を制御する	…	…	…	…	…	…	…	…	…	…

- **FMEAシートの対策を日程表へ　　【日程リスク管理】**
  - 技術リスク・対策の実施日や実施状況を見える化することで、**他日程への影響が確認**できる。

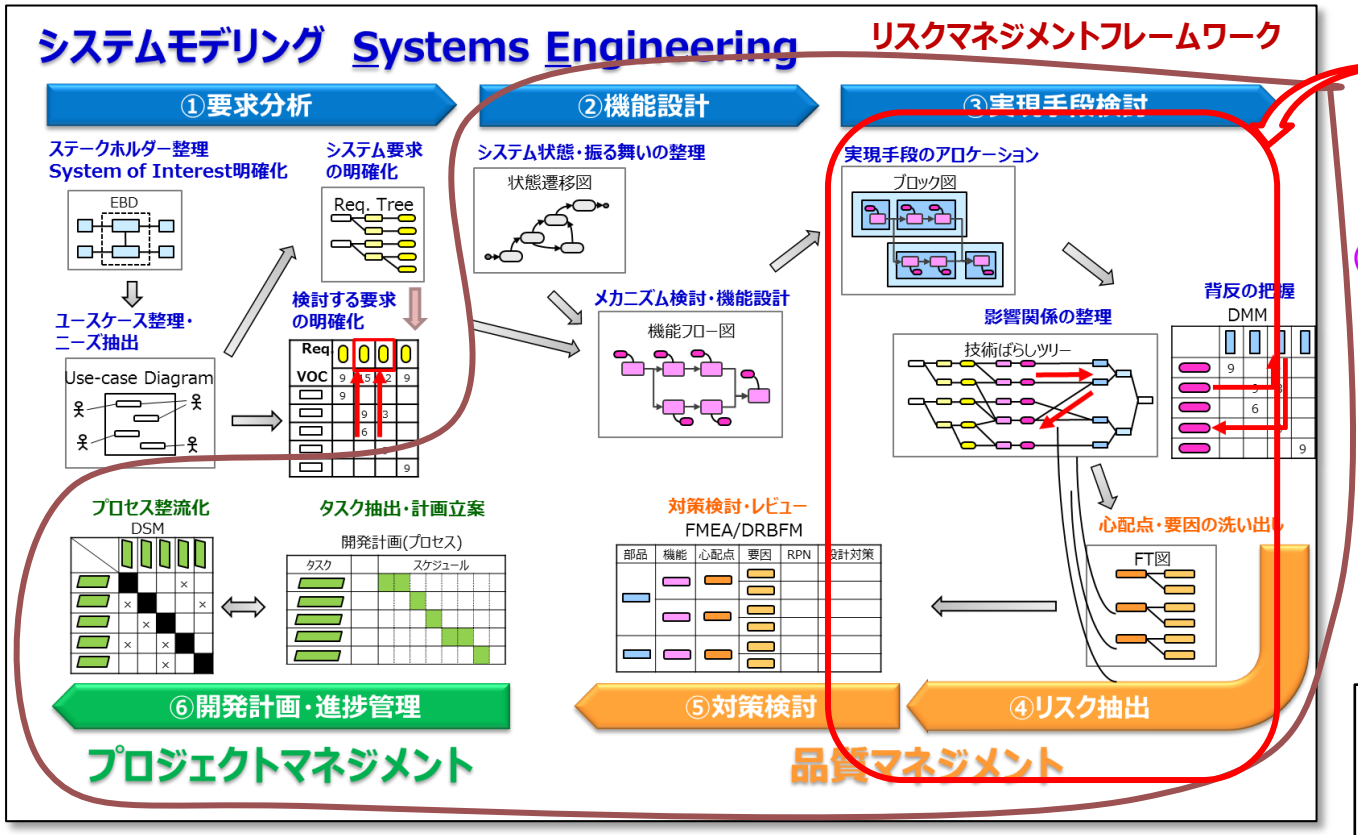
設計対策				
対策	担当	完了日	状況	結果
抽出される分を考慮して、物質を投入する	阿野	2017/11/29	完了	工程設計書へ反映
算出式で特異点がないように式を立て直す	酒井	2017/12/25	50%	中間レポート.ppt
…	金	2018/1/30	10%	方針検討中

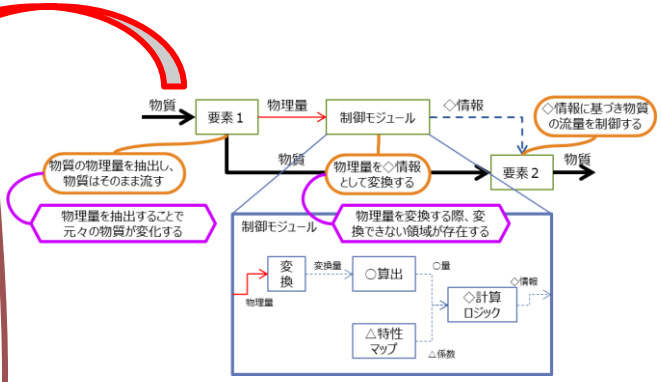


2. Background

(ISIDの)設計検討の足りない所にSTPA手法を取り入れてみた。

- **本発表で提案するリスクマネジメントフレームワーク**





☆ STPA

制御/制御対象の
相互作用観点でのリスク抽出

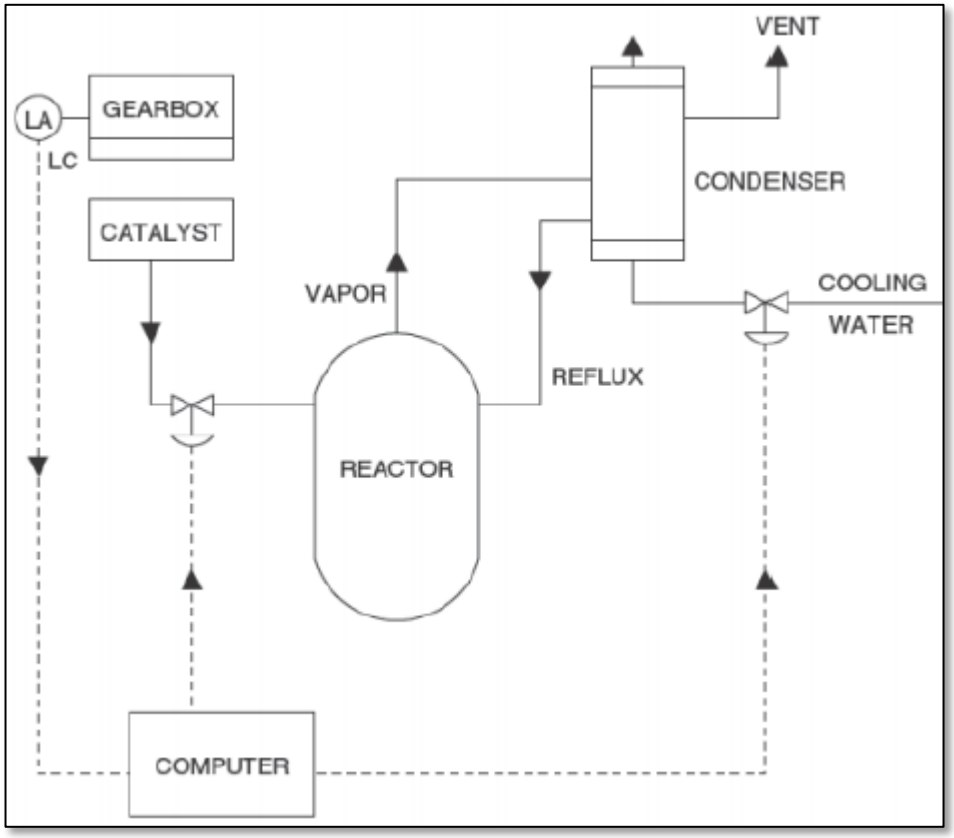
Step 0. アクシデント、ハザード、安全制約を定義
Step 0. コントロールストラクチャー図を定義
Step 1. UCAを抽出
Step 2. HCFを抽出

1. Motivation
   - 製品の複雑化 ⇒ 統合的な観点が必要
   - 設計作業量の膨大化 ⇒ 既存手法との違いを理解し低負荷の作業追加で留めたい
2. Background
   - 開発現場で使われているリスク管理ツール (FMEA/DRBFM/FTA/HAZOP)
   - 弊社(ISID)のリスク管理手法について紹介
     - (システム)ブロック図作成・機能の見える化
     - 機能ベースのリスク抽出・検討　【技術リスク管理】
     - リスク対策の日程の見える化　【日程リスク管理】
3. **STAMP/STPAを用いたリスクマネジメントフレームワーク**
   - STAMP/STPAの適用
   - (ISIDの)リスクマネジメントフレームワークへSTAMP/STPAを導入
4. 今後に向けて
5. まとめ

3. STAMP/STPAの適用

第１回STAMPワークショップ「STAMP/STPA Intermediate Tutorial」を例にしてみた。

- **STAMP/STPAの適用**

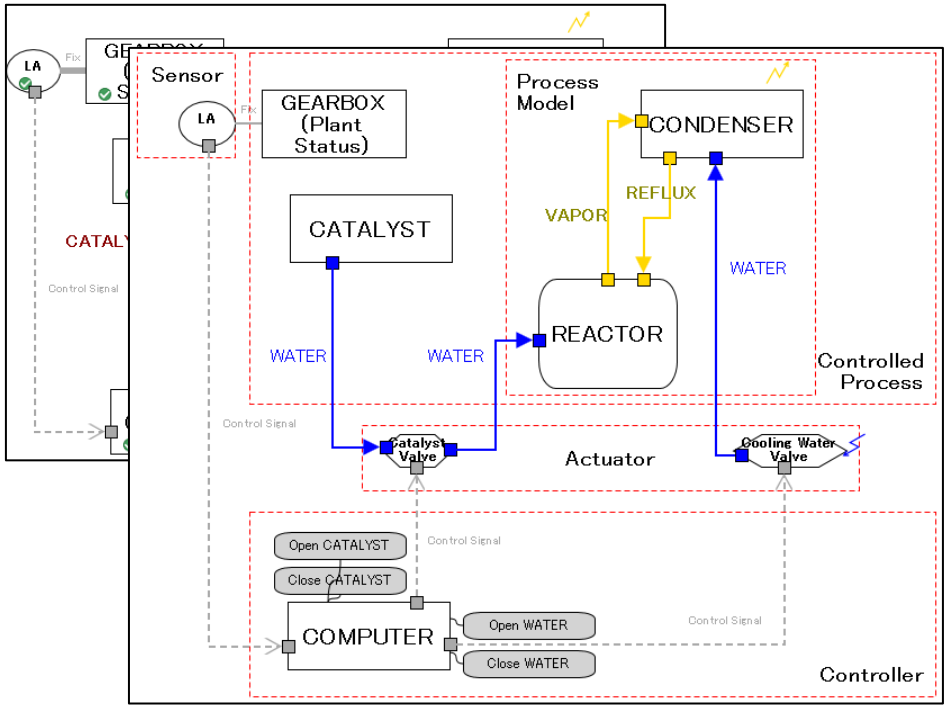


出典： [STAMP/STPA Intermediate Tutorial] **[John Thomas, 2016]**

Step 0-1. Identify accidents and hazards

Accidents	Hazards
(A1) People die from toxic chemical	(H1) Toxic chemical is released
(A2) Economic Loss	(H2) Unable to produce chemical X

Step 0-2. Draw the control structure



3. STAMP/STPAの適用

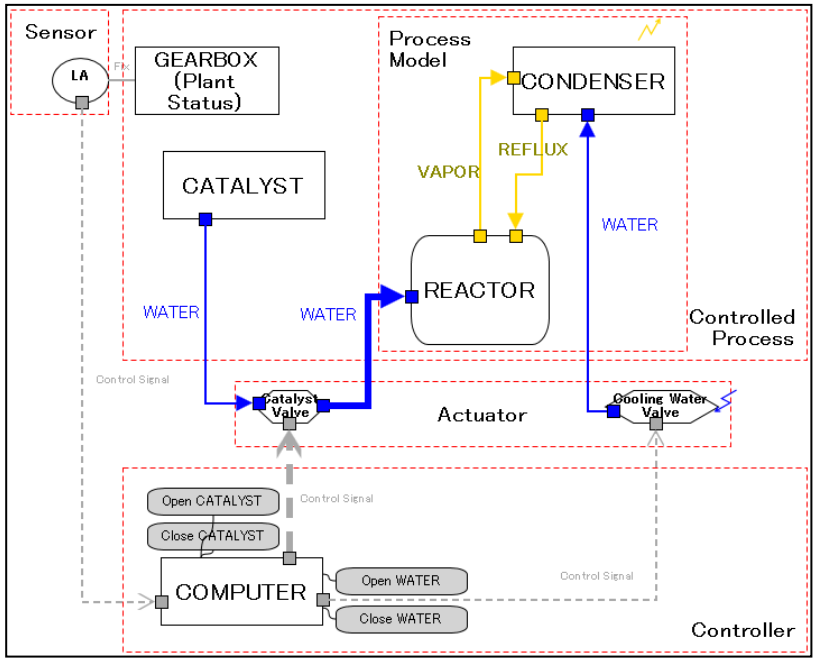
第１回STAMPワークショップ「STAMP/STPA Intermediate Tutorial」を例にしてみた。

- **STAMP/STPAの適用**

Hazards

(H1) Toxic chemical is released
(H2) Unable to produce chemical X

Step 1. Identify unsafe control



Toxic Catalyst (だけ)が流れる状況 **(H1)**

Unsafe Control Act	Guide word	Guide Image	STPA: Not Providing causes hazard	Providing causes hazard	Incorrect Timing / Order	Stopped Too Soon / Applied Too Long
				Control Action / Target control		
Functions						
Close WATER				☆CATALYSTだけ開かれる	☆CATALYSTより早く閉じられる	
Open WATER			☆CATALYSTだけ開かれる		☆CATALYSTより遅く開かれる	☆開かれる作業が早く中断され、CATALYSTだけ開かれる
Open CATALYST				☆WATERが開かれていない	☆早く開かれる	
Close CATALYST			☆閉じられない		☆遅く閉じられる	☆閉じられる作業が早く中断され、CATALYSTだけ開かれる

☆ CATALYST 関連動作起因の UCA

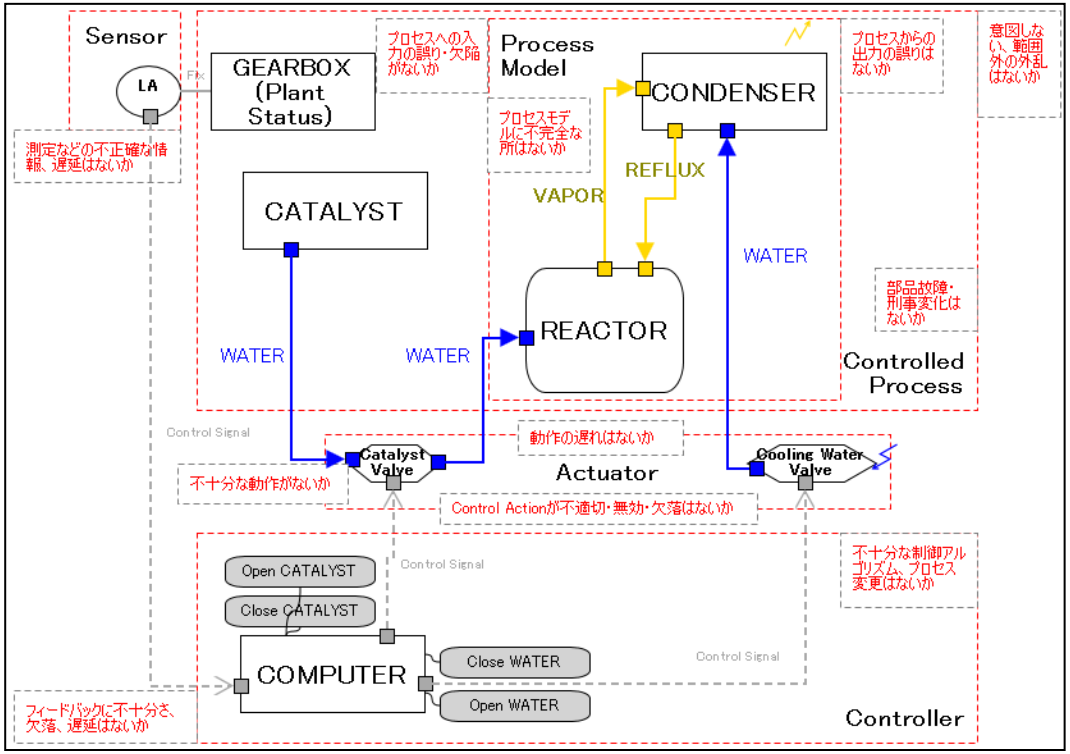
☆ WATER 関連動作起因の UCA

3. STAMP/STPAの適用

第１回STAMPワークショップ「STAMP/STPA Intermediate Tutorial」を例にしてみた。

- **STAMP/STPAの適用**

Step 2. Identify accident causal scenarios



Toxic Catalyst (だけ)が流れる状況

Unsafe Control Act	Guide word / Image	STPA: Not Providing causes hazard	Providing causes hazard	Incorrect Timing / Order	Stopped Too Soon / Applied Too Long
Functions					
Close WATER			☆CATALYSTだけ開かれる	☆CATALYSTより早く閉じられる	
Open WATER		☆CATALYSTだけ開かれる		☆CATALYSTより遅く開かれる	☆開かれる作業が早く中断され、CATALYSTだけ開かれる
Open CATALYST			☆WATERが開かれていない	☆早く開かれる	
Close CATALYST		☆閉じられない		☆遅く閉じられる	☆閉じられる作業が早く中断され、CATALYSTだけ開かれる

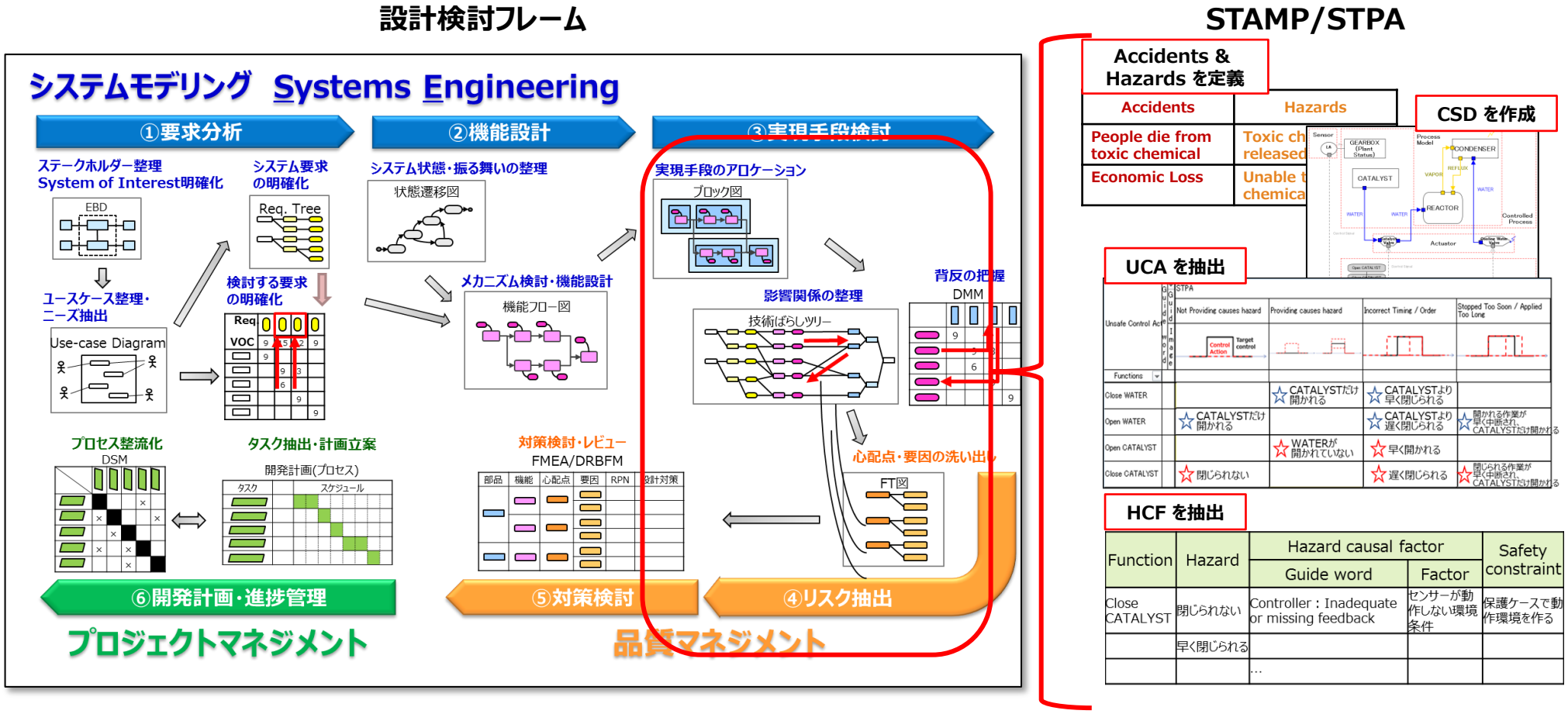
Function	Hazard	Hazard causal factor		Safety constraint
		Guide word	Factor	
Close CATALYST	閉じられない	Controller：Inadequate or missing feedback	センサーが動作しない環境条件	保護ケースで動作環境を作る
	早く閉じられる			
		…		

Hazard causal factor 抽出のためのガイドワード(上図赤字)を表示

3. STAMP/STPAの適用

第１回STAMPワークショップ「STAMP/STPA Intermediate Tutorial」を例にしてみた。

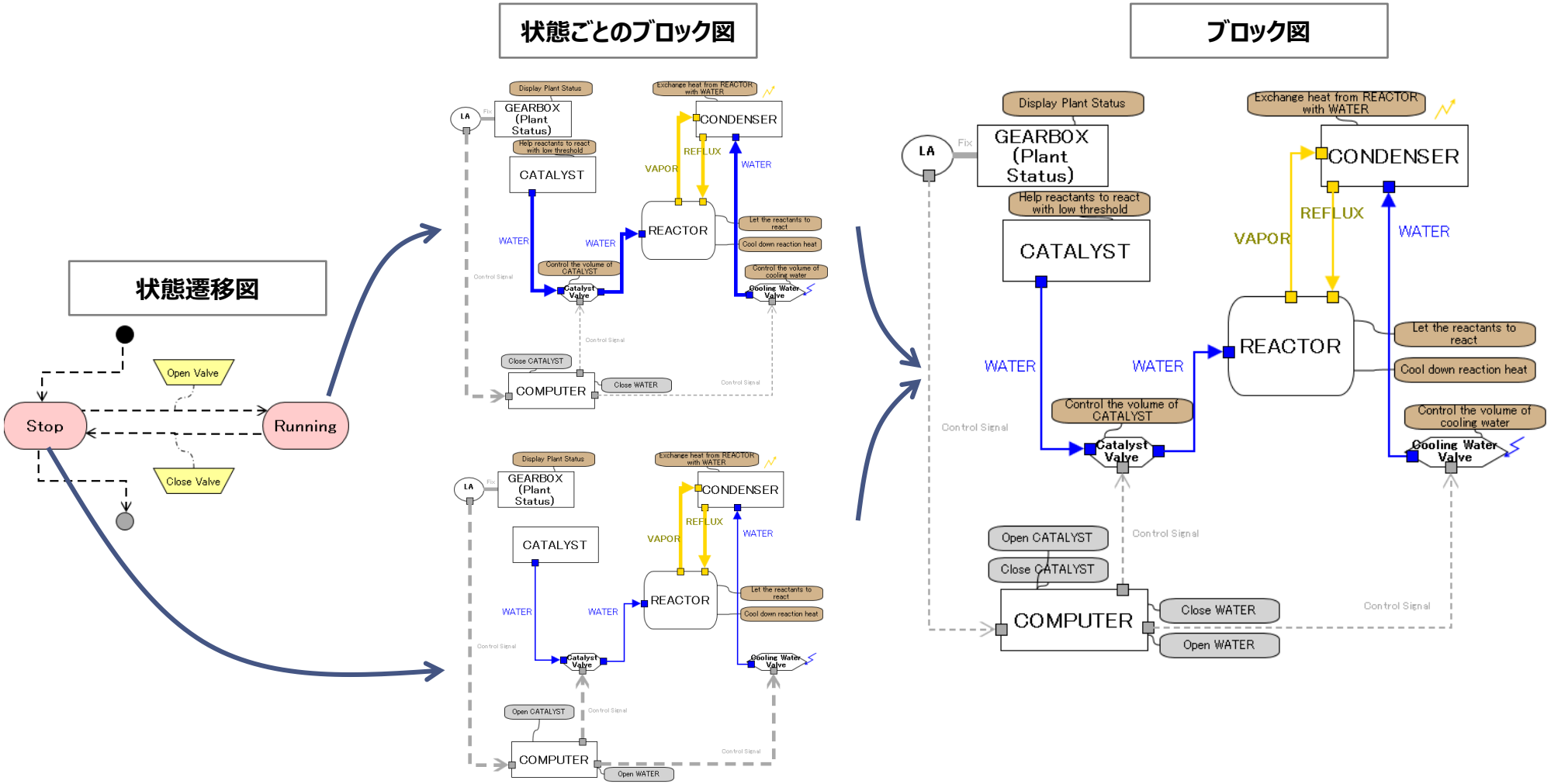
- (ISIDの)リスクマネジメントフレームワークへSTAMP/STPAを導入



3. STAMP/STPAの適用

第１回STAMPワークショップ「STAMP/STPA Intermediate Tutorial」を例にしてみた。

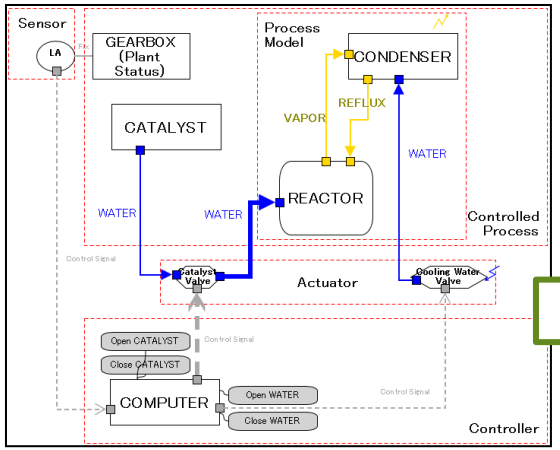
- (ISIDの)リスクマネジメントフレームワークへSTAMP/STPAを導入

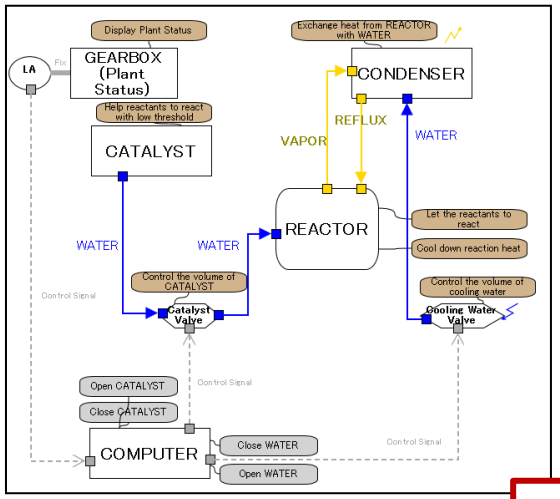


3. STAMP/STPAの適用

第１回STAMPワークショップ「STAMP/STPA Intermediate Tutorial」を例にしてみた。

- (ISIDの)リスクマネジメントフレームワークへSTAMP/STPAを導入

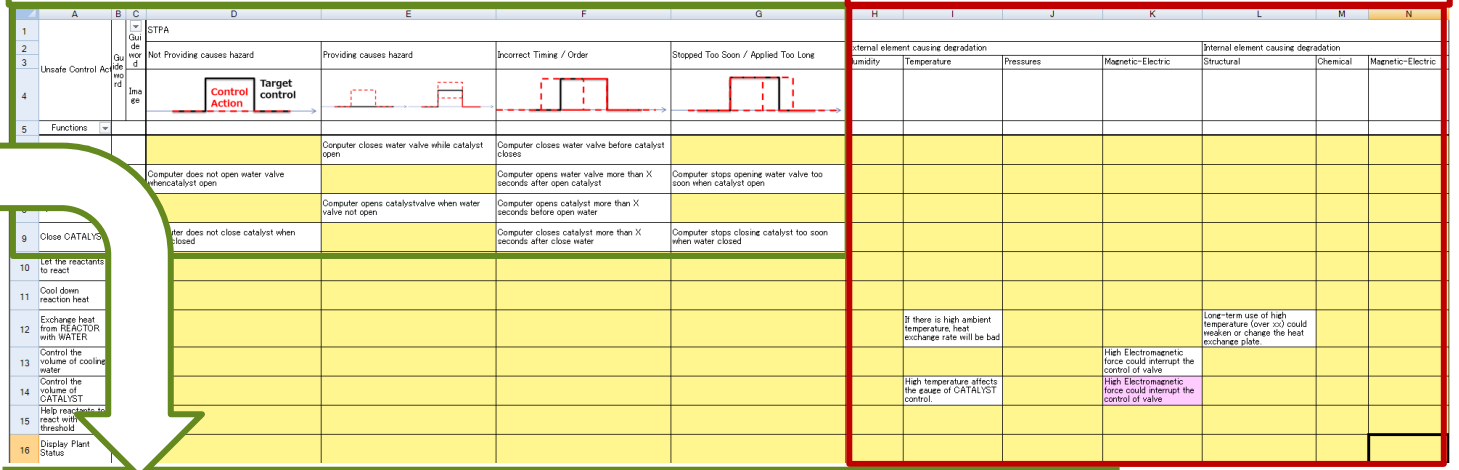




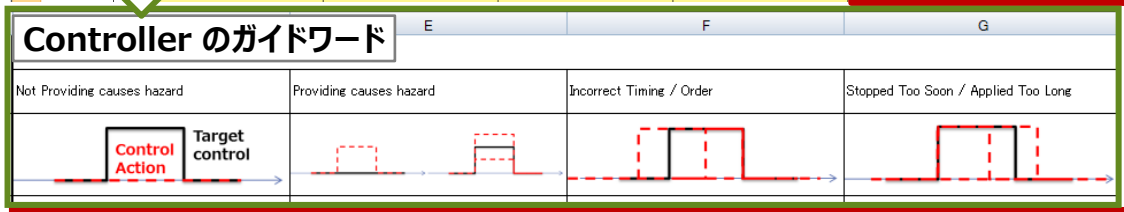
(Guide wordを参考に) Controller の UCA、Controlled Process の Risk を抽出

Guide word for identifying UCAs

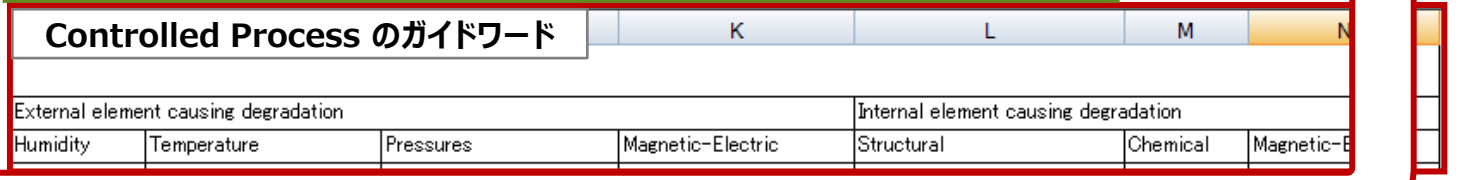
Guide word for failure or Risk



Controller のガイドワード



Controlled Process のガイドワード



3. STAMP/STPAの適用

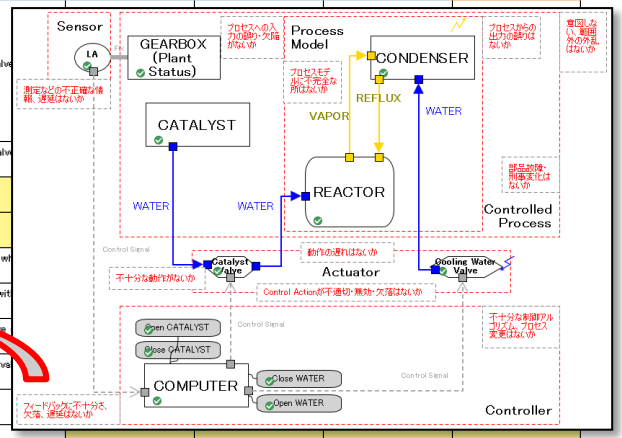
第１回STAMPワークショップ「STAMP/STPA Intermediate Tutorial」を例にしてみた。

- **(ISIDの)リスクマネジメントフレームワークへSTAMP/STPAを導入**

(Guide wordを参考に) 各 UCA の HCF を抽出

Component	Function Control	UCA / Risk	Causal Factor	Influence	Safety ConCountermeasure・Task

	Component		Function	Guide word	Unsafe Control Action / Risk	Hazard / Risk Causal Factor		Influence					Safe Constraint / Countermeasure	Countermeasure task			
						Guide word	Factor	Details	S	O	D	RPN		Task details	Person in charge	Due date	Progress
1						HCF のガイドワード											
2				Providing causes hazard	Conputer closes water valve while catalyst open	Controller : Missing or wrong communication with a	Because ...	Fire	9	3	3	81					
3																	
4			Close WATER										Computermust not close water valve while catalyst valve open				
5				Incorrect Timing / Order	Computer closes water valve before catalyst closes	Controller : Feedback delays	Because ...	Fire	7	5	5	175	Computermust not close water valve before catalyst valve closes				
6				Humidity	New Issue		New Issue										
7				Temperature	New Issue												
8		COMPUTER		Not Providing causes hazard	Computer does not open water valve whencatalyst open	Controller : Feedback delays	Because ...	Breakdown of ...	7	3	5	105	Computer must open water valve wh catalyst valve is open				
9			Open WATER	Incorrect Timing / Order	Computer opens water valve more than X seconds after open catalyst	Controller : Control input or external information wr	Because ...	Breakdown of					Computermust open water valve wit catalyst valve open				
10				Stopped Too Soon / Applied Too Long	Computer stops opening water valve too soon when catalyst open	Controller : Control input or external information wr	Because ...	Breakdown of ...	7	3	3	63	Computer must open catal certain time passed.				
11			Open CATALYST	Providing causes hazard	Computer opens catalystvalve when water valve not open	Controller : Control input or external information wr	Because ...	Fire	7	5	9	315	Computermust not open catalyst va water valve not open				
12	System			Incorrect Timing / Order	Computer opens catalyst more than X seconds before open water		Because ...	Fire	7	5	7	245	...				
13				Not Providing causes hazard	Computer does not close catalyst when water closed		Because ...	Fire	5	5	7	175	...				
14			Close CATALYST	Incorrect Timing / Order	Computer closes catalyst more than X seconds after close water		Because ...	Breakdown of ...	5	3	5	75	...				
15				Stopped Too Soon / Applied Too Long	Computer stops closing catalyst too soon when water closed		Because ...	Breakdown of ...	5	5	9	225	...				
16		GEARBOX (Plant Status)	Display Plant Status														
17		CATALYST	Help reactants to react with low threshold														
18		REACTOR	Let the reactants to react														
19			Cool down reaction heat														
20		CONDENSER	Exchange heat from REACTOR with WATER	Temperature	If there is high ambient temperature, heat exchange rate will be bad		Low heat exhaust	New Issue	5	3	3	45	Generate blow to heated components to evacuate	Function Evaluation (Experiment or CAE)	Kim Hoonhee	11/29	0 %
21				Structural	Long-term use or high temperature (over xxx) could weaken or change the heat exchange plate.												
22		LA															
23		Catalyst Valve	Control the volume of CATALYST	Temperature	High temperature affects the gauge of CATALYST control.		exposed to the	New Issue	5	5	5	125	Block from external environment by placing air gap between gauge and environment	New Task	Kawaguchi Hiroshi	11/21	0 %
24				Magnetic-Electric	High Electromagnetic force could interrupt the control of valve		from external EM	New Issue	5	3	9	135	Make the metal cabinet surrounding the valve	New Task	Nakajima Myu	11/24	0 %
25		Cooling Water Valve	Control the volume of cooling water	Magnetic-Electric	High Electromagnetic force could interrupt the control of valve		from external EM	New Issue	5	3	9	135	Make the metal cabinet surrounding the valve	New Task	Nakajima Myu	11/24	0 %

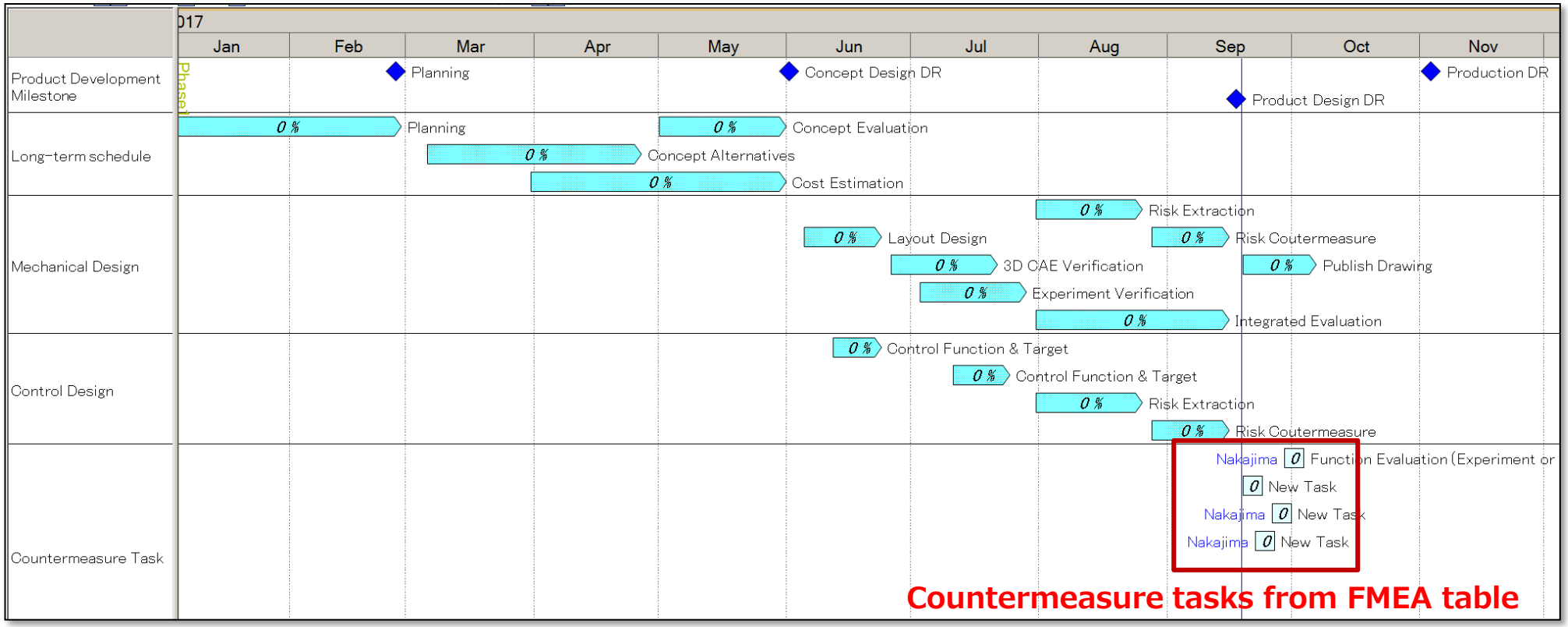


3. STAMP/STPAの適用

第１回STAMPワークショップ「STAMP/STPA Intermediate Tutorial」を例にしてみた。

- (ISIDの)リスクマネジメントフレームワークへSTAMP/STPAを導入

各 UCA や リスクに対する Safety Constraint もしくは対策の計画を開発日程に載せ、実行可能な計画作成

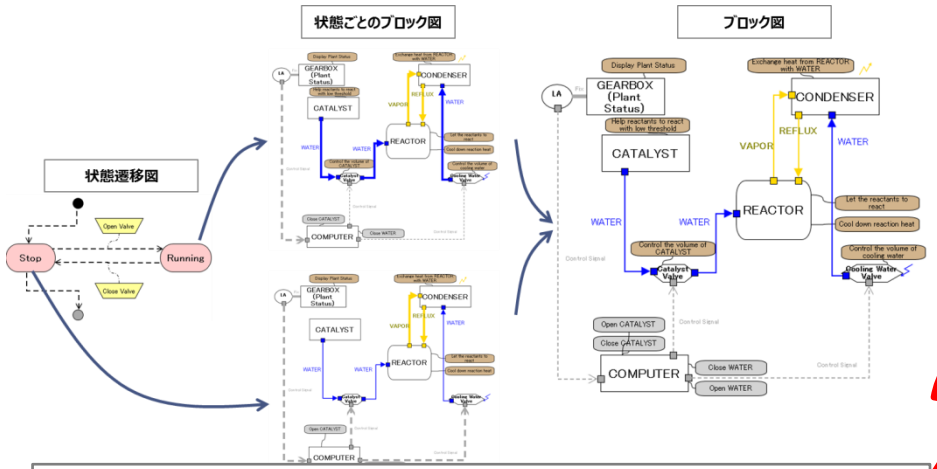


3. STAMP/STPAの適用

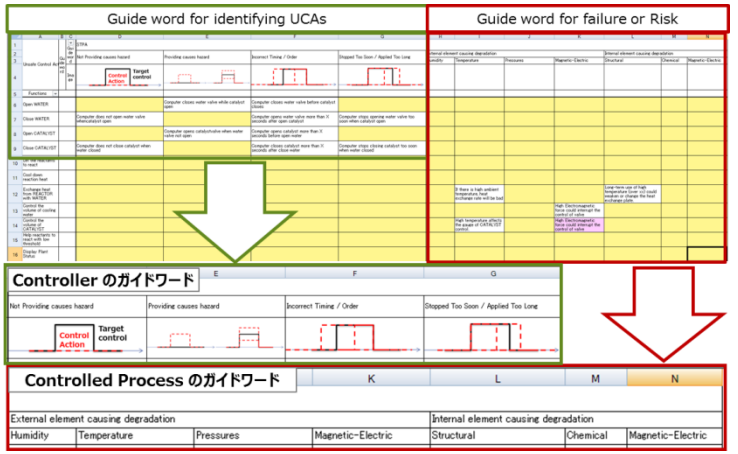
第１回STAMPワークショップ「STAMP/STPA Intermediate Tutorial」を例にしてみた。

- (ISIDの)リスクマネジメントフレームワークへSTAMP/STPAを導入 (まとめ)

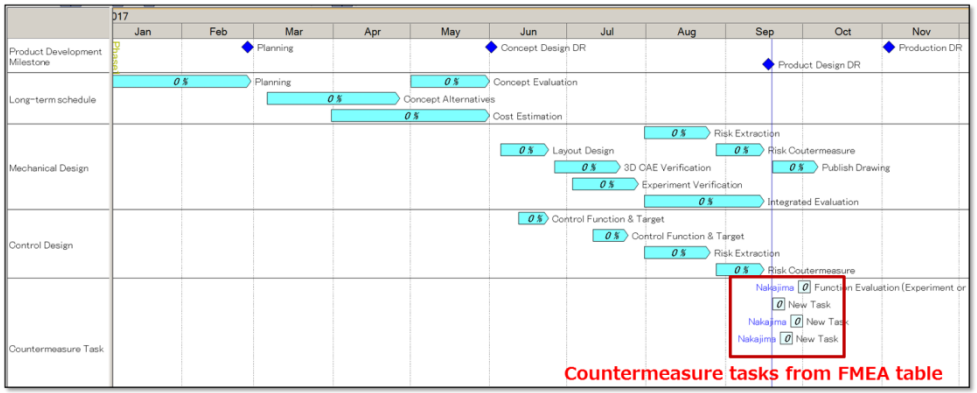
システム(Controller – Controlled Process)の見える化



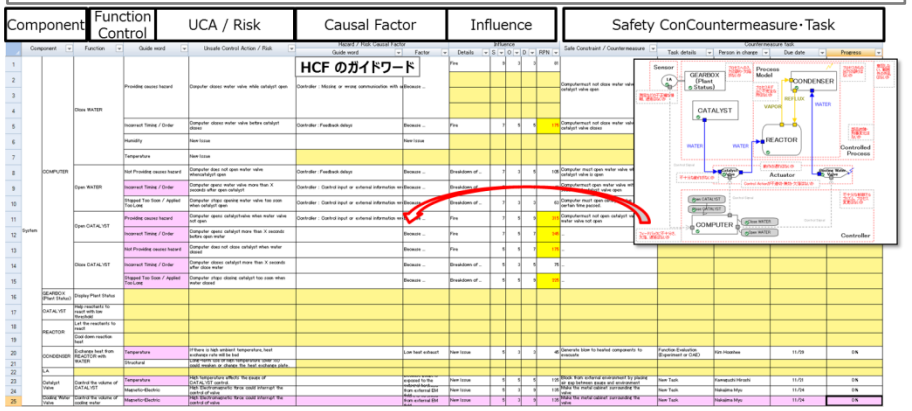
システムのUCAやリスク(心配点)を抽出



対策の(日程)リスクを見せる化・管理



(技術)リスク(心配点)を評価し、その原因や対策を検討



1. Motivation

- 製品の複雑化 ⇒ 統合的な観点が必要
- 設計作業量の膨大化 ⇒ 既存手法との違いを理解し低負荷の作業追加で留めたい

2. Background

- 開発現場で使われているリスク管理ツール (FMEA/DRBFM/FTA/HAZOP)
- 弊社(ISID)のリスク管理手法について紹介
  - (システム)ブロック図作成・機能の見える化
  - 機能ベースのリスク抽出・検討　【技術リスク管理】
  - リスク対策の日程の見える化　【日程リスク管理】

3. STAMP/STPAを用いたリスクマネジメントフレームワーク

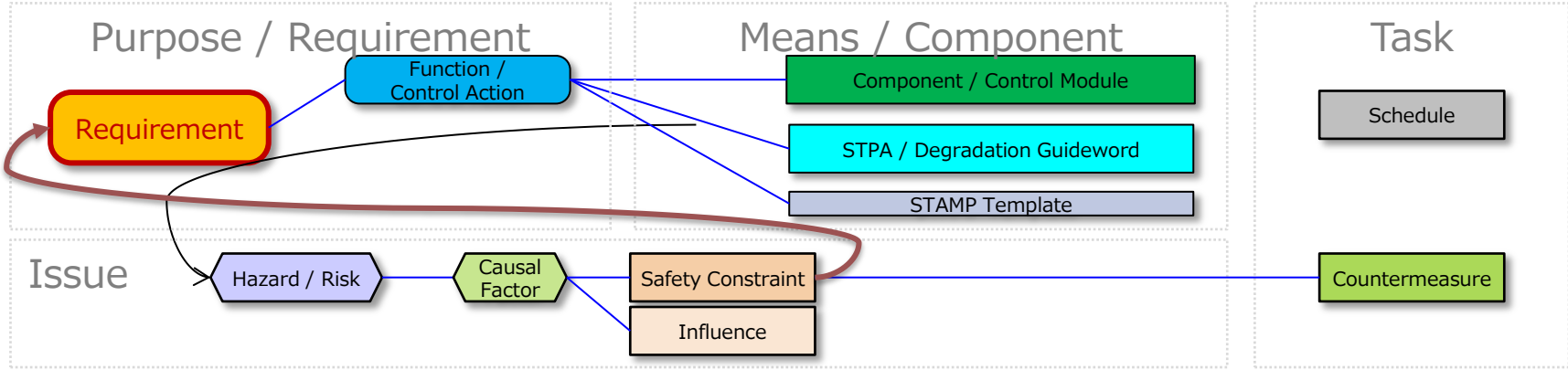
- STAMP/STPAの適用
- (ISIDの)リスクマネジメントフレームワークへSTAMP/STPAを導入

4. 今後に向けて

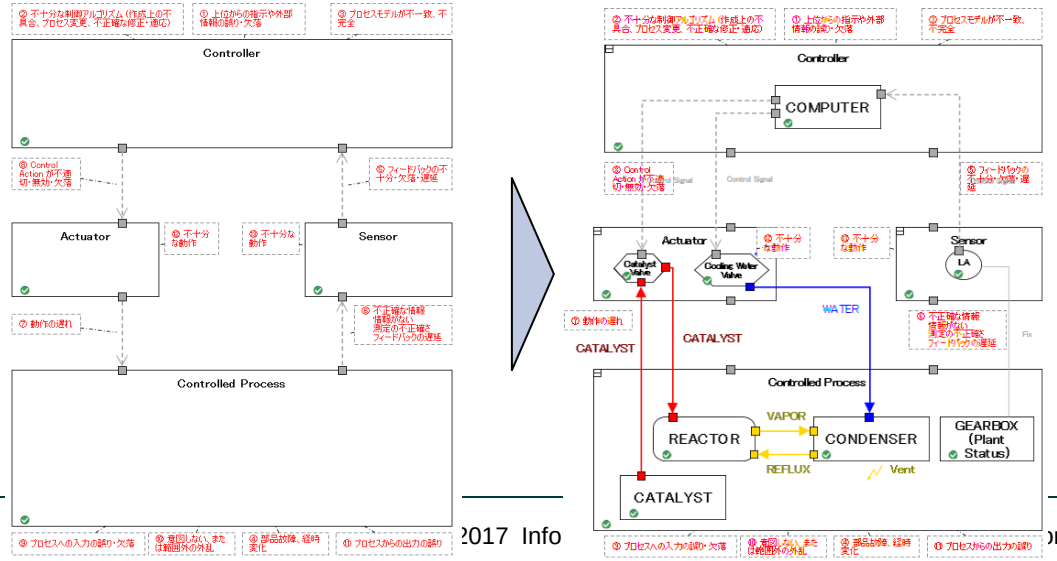
5. まとめ

4. 今後に向けて

- Hazard の対策を製品の要求や設計へ反映するための**データ構造**を引き続き検討。
  - Rationaleの残し方、Hazard Scenario の残し方など



- 開発現場でSTAMP/STPAの**実運用を見据えた ITツール側の準備**
  - 便利なテンプレートの用意
  - 実例・ガイドの提供



5. まとめ

- 製品開発のトレンドとして、複数製品のコンバージェンス、機械製品の電子化・IT化が進んでいる。複数のコンポーネントが複雑に連携するシステム開発には、STAMPのようなシステム観点で物事を捉える手法が必要になる。
- 企業でよく使われているリスク抽出・管理ツールとして、FTA / FMEA / DRBFM / HAZOP などがあるが、**全体システム観点でリスクや要因を抽出する機能が物足りない**。
- 本発表では、上記手法とSTAMPの位置づけを明確にし、弊社(ISID)で取り組んでいるブロック図作成 / 構成要素の機能化 / 機能ベースのリスク抽出 / リスク対策の日程管理の流れを紹介しながら、STAMP(STPA)手法の導入を試みた。
  - **企業への導入が広がっているFMEA**に、STAMPのガイドワードを用いることで、**制御/制御対象物間制御信号の有無・遅延などの観点**からもリスク/要因抽出・検討が可能になることが分った。
- 今後、対策(or Safety Constraint)から新たに得られた要求や評価条件などの取り扱いを検討し、現場へ活用するための ITツール側の準備を進める。

参考文献

- はじめてのSTAMP/STPA ～システム試行に基づく新しい安全性解析手法～ [IPA,2016]
- Engineering a Safer World [Nancy Leveson, 2012]
- STPA Primer [Nancy Leveson(MIT), 2015]
- Integral Operation on Safety and Security Analysis using Hazop with other Analysis method including FTA, FMEA, STAMP/STPA, FRAM and other method [Kiyoshi Ogawa, 2017]
- トヨタ式未然防止手法 GD3 [吉村達彦, 2002]
- 平成27年度リコール届出内容の分析結果について [国土交通省, 2015]
- STAMP/STPA Intermediate Tutorial [John Thomas, 2016]

ご清聴ありがとうございました。