第 2 回 STAMP ワークショップ発表概要

タイトル

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

Suggestion of Risk Management Framework by using STAMP/STPA.

著者・発表者

電通国際情報サービス　金 勲熙、阿野 基貴、酒井 直彦

ISID　Hoonhee KIM, Motoki ANO, Naohiko SAKAI

概要

自動車を含め多くの製造業では、既存のリスク抽出・管理方法として、FTA や FMEA・DRBFM などが多く用いられている。今回の講演では、既存のリスク抽出・管理方法に STAMP/STPA を用いることで、メカ観点でのリスクだけでなく制御観点でのハザードを共に抽出・管理できることを示したい。そして、各リスク・ハザードの原因・対策・対策の実現状況/日程までを共に管理(見える化)することで、技術的なリスク管理だけでなく、開発日程面でのリスク管理もできるフレームワークを提案する。

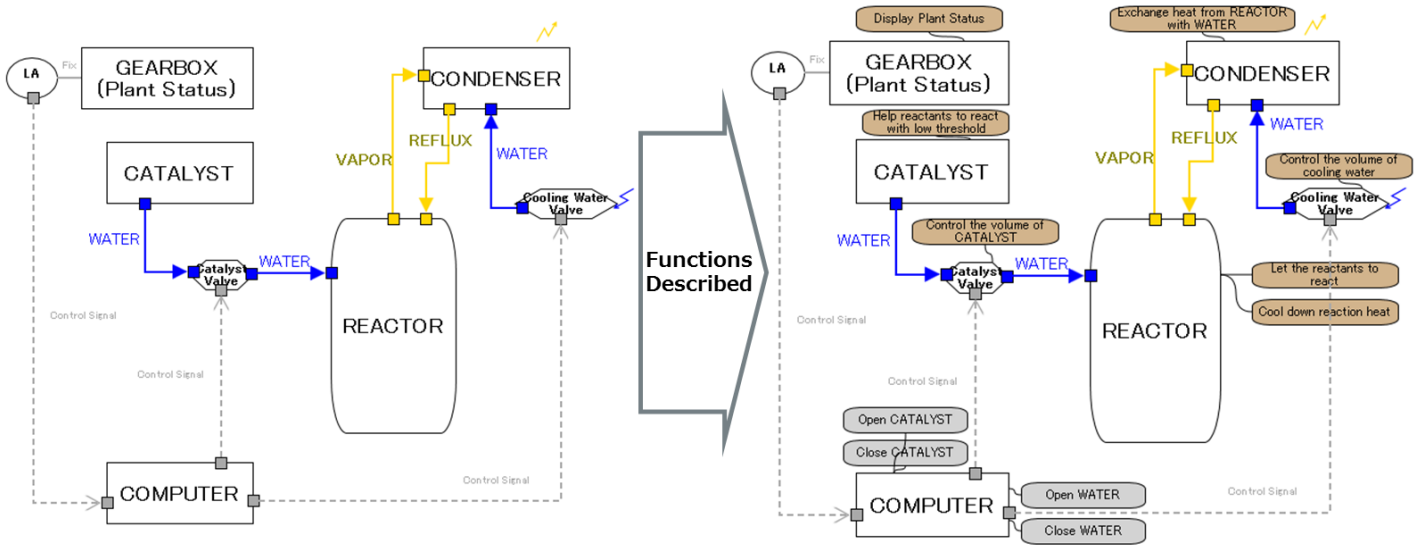

Figure 1 Control Structure Diagram に機能を明記

Figure 1 は、STAMP/STPA Intermediate Tutorial の事例として紹介されている Control Structure Diagram である。コントローラ(COMPUTER)に制御コマンド(Open/Close WATER/CATALYST)に加え、各コンポーネントに対してもの機能を明記している。

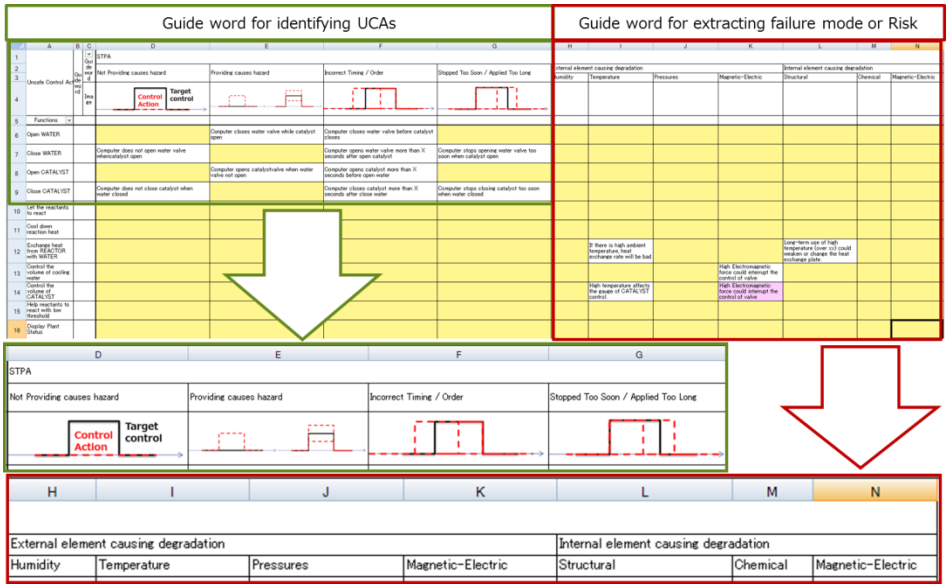

Figure 2 Guide word を参考に制御コマンドから UCA、機能からリスクを抽出

Figure 2 では、STPA のガイドワードを用いて各制御コマンドに対する UCA を抽出(緑色)し、物理観点(環境から受ける外部から影響を与える要素、コンポーネント内部で影響を起こす要素)から各機能のリスク(赤色)を抽出している。Figure 3 では、抽出された UCA やリスクを FMEA 形式に合わせ、影響分析(RPN)や原因・対策・タスクを並べている。

Component	Function Control	UCA / Risk (Effect - RPN)			Cause・Countermeasure・Task					
Component	Function	Guide word	Unsafe Control Action / Risk Details	RPN	Hazard / Risk Causal Factor	Safe Constraint / Countermeasure	Countermeasure task Task details	Person in charge	Due date	Progress
System	GEARBOX (Plant Status)	Display Plant Status								
	CATALYST	Help reactants to react with low threshold								
	REACTOR	Let the reactants to react								
		Cool down reaction heat								
	CONDENSER	Exchange heat from REACTOR with WATER	Temperature	If there is high ambient temperature, heat exchange rate will be bad	200	Low heat exhaust	Generate blow to heated components to evacuate	Function Evaluation (Experiment or CAE)	Nakajima Myu	9/29	0 %
			Structural	Long-term use of high temperature (over xx) could weaken or change the heat exchange plate.	100						
	COMPUTER	Open WATER	Providing causes hazard	Computer closes water valve while catalyst open	150	Because ...	Computermust not close water valve while catalyst valve open				
			Incorrect Timing / Order	Computer closes water valve before catalyst closes	150	Because ...	Computermust not close water valve before catalyst valve closes				
		Close WATER	Not Providing causes hazard	Computer does not open water valve whencatalyst open	120	Because ...	Computer must open water valve whenever catalyst valve is open				
			Incorrect Timing / Order	Computer opens water valve more than X seconds after open catalyst	100	Because ...	Computermust open water valve within X seconds of catalyst valve open				
			Stopped Too Soon / Applied Too Long	Computer stops opening water valve too soon when catalyst open	80	Because ...	Computer must open catalyst valve after a certain time passed.				
		Open CATALYST	Providing causes hazard	Computer opens catalystvalve when water valve not open	60	Because ...	Computermust not open catalyst valve when water valve not open				
			Incorrect Timing / Order	Computer opens catalyst more than X seconds before open water	20	Because ...	..				
		Close CATALYST	Not Providing causes hazard	Computer does not close catalyst when water closed	20	Because ...	..				
			Incorrect Timing / Order	Computer closes catalyst more than X seconds after close water	20	Because ...	..				
			Stopped Too Soon / Applied Too Long	Computer stops closing catalyst too soon when water closed	20	Because ...	..				
	LA										
	Catalyst Valve	Control the volume of CATALYST	Temperature	High temperature affects the gauge of CATALYST control.	250	Because gauge is exposed to the external heat.	Block from external environment by placing air gap between gauge and environment	New Task	Nakajima Myu	9/22	0 %
			Magnetic-Electric	High Electromagnetic force could interrupt the control of valve	400	There is no shield from external EM field.	Make the metal cabinet surrounding the valve	New Task	Nakajima Myu	9/26	0 %
	Cooling Water Valve	Control the volume of cooling water	Magnetic-Electric	High Electromagnetic force could interrupt the control of valve	400	There is no shield from external EM field.	Make the metal cabinet surrounding the valve	New Task	Nakajima Myu	9/26	0 %

Figure 3　STAMP/STPA を取り入れた FMEA 表

FMEA 表から影響が大きいリスクに対しては対策が取られ、具体的なタスクまで落とすことが多い。そのタスクに担当者、期限、進捗を見える化し管理すること(Figure 4)で、開発現場では他の日程とも兼ね合いながら、確実なリスク管理が可能になる。

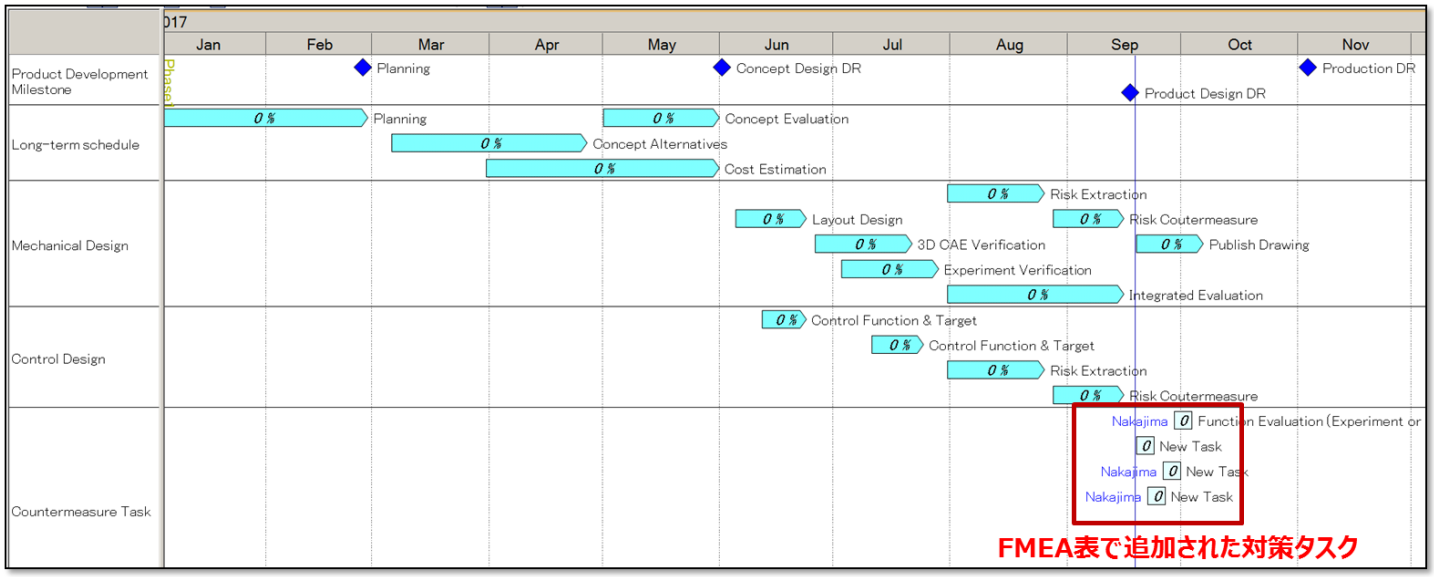

Figure 4 対策タスクを全体の開発日程に載せて、全体業務を見える化

キーワード

(1) STAMP/STPA

(2) FMEA

(3) Risk Management

(4) Block Diagram