(23)Title

Suggestion of Risk Management Framework by using STAMP/STPA.

Speaker, Authors

Information Services International-Dentsu, Ltd. Hoonhee KIM, Motoki ANO, Naohiko SAKAI

Abstract

In manufacturing industries including automobiles, FTA, FMEA, DRBFM, etc. are broadly used as a risk extraction and management tools. In this presentation, I would like to explain that by applying STAMP / STPA to a risk management method, we can extract and manage hazards and risks not only from mechanical point of view but also control point of view. In addition, here we suggest a framework which is enable us to manage not only technical risk but also schedule risk by visualizing the causes / measures / task progress / schedule of each risk and hazard together.

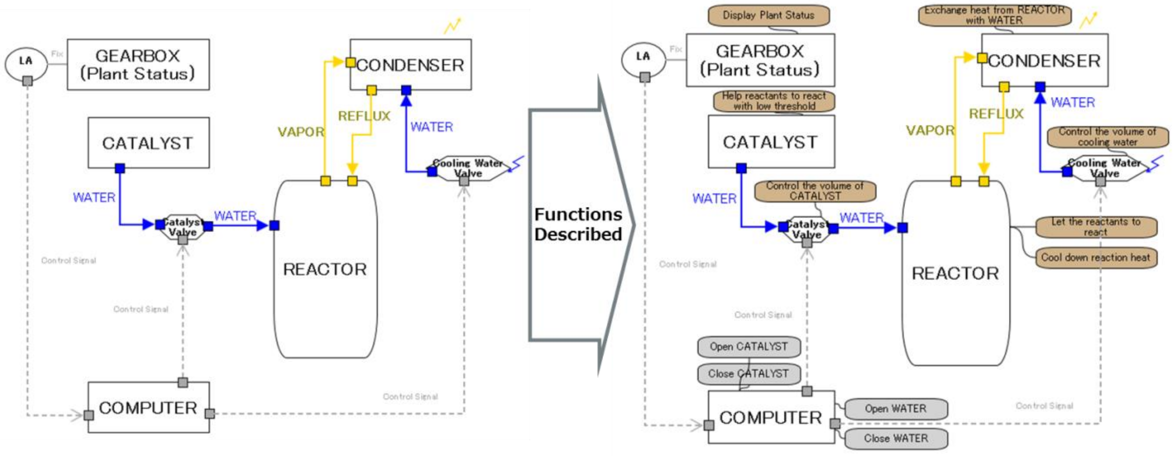
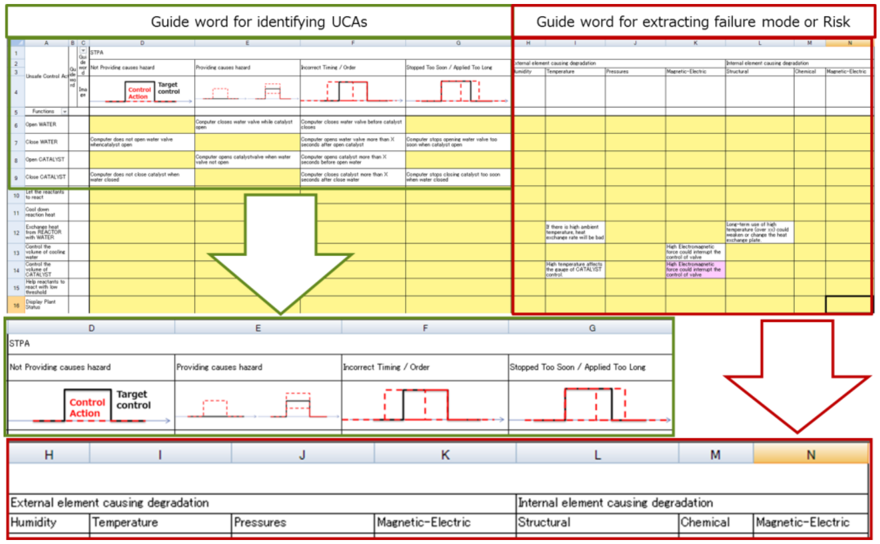


Figure 3 Function of each component is described on Control Structure Diagram

Figure 1 is a Control Structure Diagram introduced from “STAMP / STPA Intermediate Tutorial”. In addition to the control command (Open / Close WATER / CATALYST) to the controller (COMPUTER), the function of each component is also specified.


Guide word for identifying UCAs
Guide word for extracting failure mode or Risk
Control Action
Target control

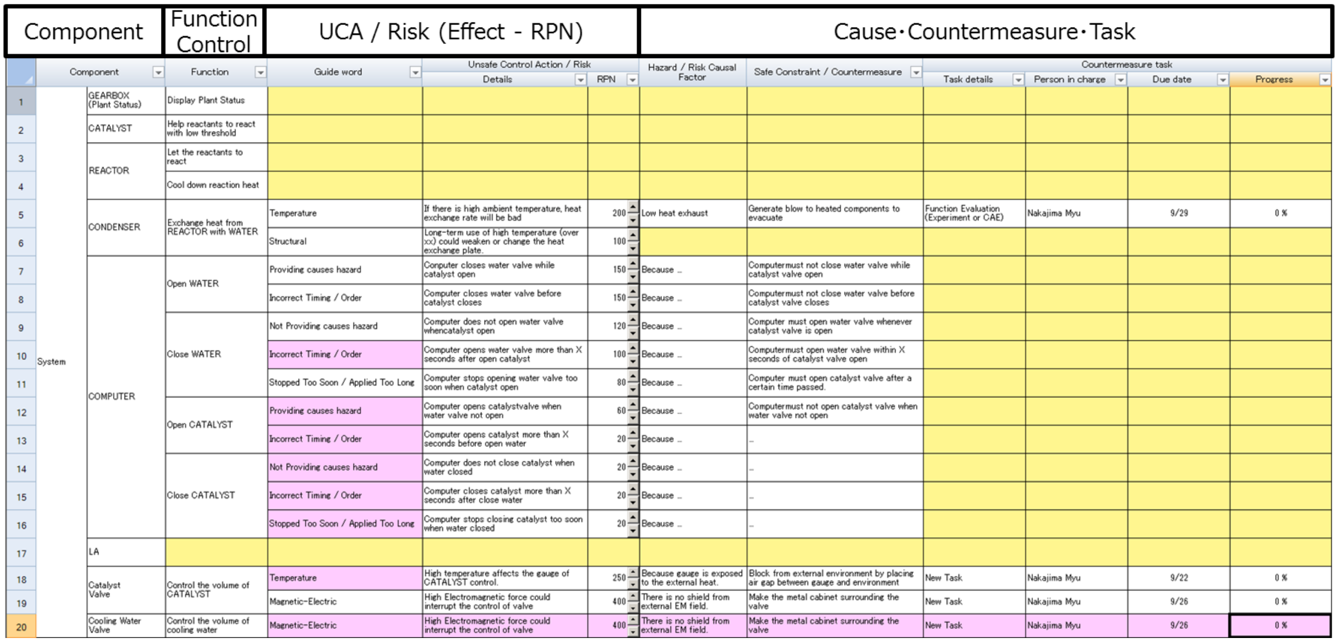
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1				STPA										
2	Unsafe Control Act	Guide word	Guide word	Not Providing causes hazard	Providing causes hazard	Incorrect Timing / Order	Stopped Too Soon / Applied Too Long	xternal element causing degradation				Internal element causing degradation		
3								lumidity	Temperature	Pressures	Magnetic-Electric	Structural	Chemical	Magnetic-Electric
4			Image	Control Action Target control										
5	Functions													
6	Open WATER				Computer closes water valve while catalyst open	Computer closes water valve before catalyst closes								
7	Close WATER			Computer does not open water valve whencatalyst open		Computer opens water valve more than X seconds after open catalyst	Computer stops opening water valve too soon when catalyst open							
8	Open CATALYST				Computer opens catalystvalve when water valve not open	Computer opens catalyst more than X seconds before open water								
9	Close CATALYST			Computer does not close catalyst when water closed		Computer closes catalyst more than X seconds after close water	Computer stops closing catalyst too soon when water closed							
10	Let the reactants to react													
11	Cool down reaction heat													
12	Exchange heat from REACTOR with WATER								If there is high ambient temperature, heat exchange rate will be bad			Long-term use of high temperature (over xx) could weaken or change the heat exchange plate.		
13	Control the volume of cooling water										High Electromagnetic force could interrupt the control of valve			
14	Control the volume of CATALYST								High temperature affects the gauge of CATALYST control.		High Electromagnetic force could interrupt the control of valve			
15	Help reactants to react with low threshold													
16	Display Plant Status													

D	E	F	G
STPA			
Not Providing causes hazard	Providing causes hazard	Incorrect Timing / Order	Stopped Too Soon / Applied Too Long
Control Action Target control			

H	I	J	K	L	M	N
External element causing degradation				Internal element causing degradation		
Humidity	Temperature	Pressures	Magnetic-Electric	Structural	Chemical	Magnetic-Electric

Figure 4 In reference to guide word, UCAs and risks are extracted from control command and function respectively.

In Figure 2, the UCA for each control command is extracted (green) using the guide word of STPA and the risk (red) of each function is extracted from the physical viewpoint (stress from the environment, component aging / deterioration) . In Figure 3, the extracted UCAs are applied to the FMEA format, and the impact analysis (RPN), causes, measures, tasks are arranged.



	Component		Function Control	UCA / Risk (Effect - RPN)			Cause・Countermeasure・Task					
					Unsafe Control Action / Risk				Countermeasure task			
	Component		Function	Guide word	Details	RPN	Hazard / Risk Causal Factor	Safe Constraint / Countermeasure	Task details	Person in charge	Due date	Progress
1	System	GEARBOX (Plant Status)	Display Plant Status									
2		CATALYST	Help reactants to react with low threshold									
3		REACTOR	Let the reactants to react									
4			Cool down reaction heat									
5		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 %
6				Structural	Long-term use of high temperature (over xx) could weaken or change the heat exchange plate.	100						
7		COMPUTER	Open WATER	Providing causes hazard	Conputer closes water valve while catalyst open	150	Because …	Computermust not close water valve while catalyst valve open				
8				Incorrect Timing / Order	Computer closes water valve before catalyst closes	150	Because …	Computermust not close water valve before catalyst valve closes				
9			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				
10				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				
11				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.				
12			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				
13				Incorrect Timing / Order	Computer opens catalyst more than X seconds before open water	20	Because …	…				
14			Close CATALYST	Not Providing causes hazard	Computer does not close catalyst when water closed	20	Because …	…				
15				Incorrect Timing / Order	Computer closes catalyst more than X seconds after close water	20	Because …	…				
16				Stopped Too Soon / Applied Too Long	Computer stops closing catalyst too soon when water closed	20	Because …	…				
17		LA										
18		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 %
19				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 %
20		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 5 FMEA Table with STAMP/STPA applied

Countermeasures are taken against risks that are heavily influenced by the FMEA table and broken down to specific work tasks. By visualizing and managing the tasks with the person in charge, the deadline, and the progress (Figure 4), it is possible to manage risks "certainly" at the development site while balancing other schedules.

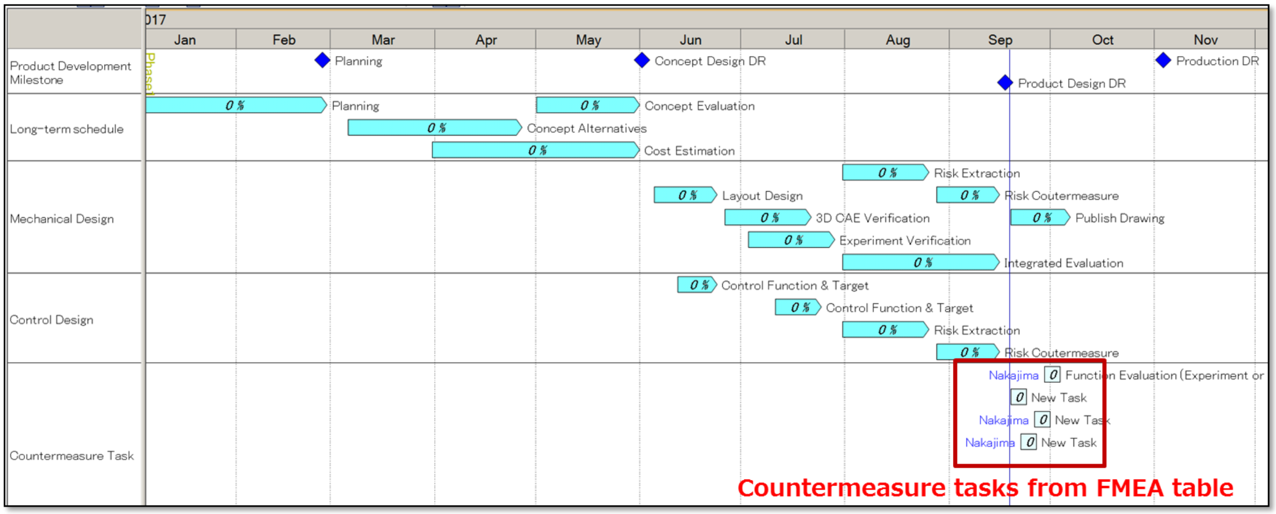


Figure 6 Visualizing of countermeasure tasks on the whole development schedule

Keywords

(1) STAMP/STPA

(2) FMEA

(3) Risk Management

(4) Block Diagram