89. Functional control structure model for the complex systems and its application in system safety analysis

Jianbo Hu[1], **Lei Zheng**[2]
College of Material Management and Safety Engineering, Air Force Engineering University,
Xi'an 710051, China
[1]Corresponding author
E-mail: [1]*jian_bo_h@163.com*, [2]*zhenglei-happy@163.com*

(Received 23 December 2015; received in revised form 15 April 2016; accepted 22 April 2016)

Abstract. The safety problem for the complex system is regarded as a control problem other than probability one, where the overall functional control structure model of the complex system could be configured in terms of the relationships among their functional labels. The hazards are due to the unsafe control actions (UCA), or the malfunctional control action (MCA). Meanwhile, UCA and MCA are due to the error feedback information (EFI), the error environment variables (EEV), the error state variables (ESE), the error command inputs (ECI), the error working modes (EWM), and the error process models (EPM), etc. Every function or component would be described as 10 labels, which are the input command (IC), the feedback to the upper level (FU), the control action (CA), the feedback from the lower levels (FL), the external input command (EC), the process model (PM), other related state variable (SV), the precondition (PC), the resource and the executing condition (RE) of the system, and the environment variable (EV). The aircraft wheel brake system's control structure model is given to show its effectiveness.

Keywords: functional control structure model, system safety analysis, wheel brake system.

1. Introduction

Accidents are becoming more and more complicated with the development of complex system and their causes might be the interaction among components and the various external factors of the operating condition and environment, except from the faults of the components.

In the view of system engineering [1], accidents are caused by the interaction among various functions or components resulting from the unsafe control action due to uncertain factors, such as time, model, resource and information. In the view of control engineering [2], the unsafe control actions resulting in accidents could be explained by models and information relationship, such as inadequacy models, varying environment, insufficient precondition and incomplete information, and can be regarded as the loss of control due to the oversize disturbance or unknown uncertainty. Thus, analyzing the system safety associated with modeling and control could be an effective way and might be extended to the quantitative analysis, such as system simulation [3, 4]. Recently, many researchers have use new accident models to consider the safety for the complex system. Nancy proposed STAMP and STPA [5, 6] and widely applied into the safety analysis for many complex systems [7-9].

Nancy's results are based on the Functional Control Structure Model (FCSM), but she did not provide the way to establish FCSM for any complex system. Only some simple feedback loop was discussed [5, 6]. Moreover, STAMP and SPTA are qualitative. In fact, the obtained FCSM could be used to system safety's quantitative analysis only if the models and data obtained from the detailed designing information could be used to establish the system safety's quantitative analyzing circumstances, especially in safety simulation [3, 4]. Furthermore, STAMP and STPA without functional labels are very different from the FRAM [10] with functional labels such that they are usually 'think of what you do' and less of systematicness and completeness. Totally, STAMP/STPA might be an effective way to handle these complex systems' safety, but many lacks should be notified as follows.

1) STAMP/STPA is a procedure other than a method. The formal description of any function is not perfectly defined to identify the unsafe control action. It is very necessary to propose an

effective way in methodology to configure the functional control structure model for the complex system.

2) STAMP/STPA is modeled qualitatively without mathematic model such that the functional control structure and its properties could not be verified, and the unsafe control actions and malfunctional control actions could not be identified directly by the dynamic analysis and the system simulation.

3) STAMP/STPA does not use the state space to describe its variables such that the configuration of the functional control structure model is chaotic in the process of identifying the unsafe control action. It is very necessary to build STAMP/STPA in systemic programmer with the state spaces variables.

In this paper, FCSM would be established using functional labels such that the system's safety analysis could be performed by analyzing the properties for the particular labels' direction, starting points and end points. FCSM for system safety analysis is configured to identify the unsafe control action and malfunctional control action. The model might be used qualitatively or quantitatively such that it is not only a method, but also a program for the safety analysis of the complex system.

2. A formal description of the function or component (FDFC)

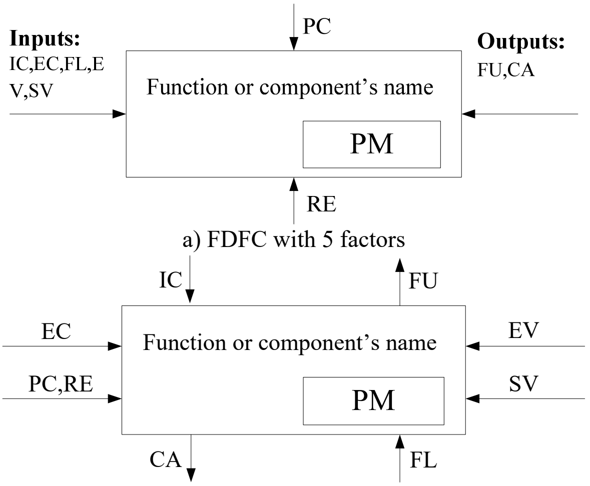
As shown in [10], the function may be defined for the specified function or components as 'the specified task of the specified function or component is finished by someone or automation under the specified conditions and within the specified time'.

The labels used in FRAM [10] could be re-considered to propose FDFC in the view of system safety such that they could describe the typical control structure relationship and are convenient for the system safety analysis.

Firstly, it is necessary for system safety analysis to describe the function or component's specified task within the specified time and under the specified condition. The specified task not only generates the control action necessary to the lower levels and the feedback to the upper levels, but also receives the associated information from the other functions or the related systems. The specified time is required to provide the proper control action, feedback and any other inputs or outputs timely (without delay, too soon, too long or out of sequence) and to stop providing timely (without delay, too soon, too late or out of sequence). The model has considered the limited conditions other than all possible conditions, so the specified conditions are required to ensure the effectiveness of the model and an effective model should be reconfigured under the specified operation conditions.

Meanwhile, every function or component has its inputs, outputs, preconditions, necessary resource and executing conditions. One function or component's inputs might be its input commands from the upper levels, the external control commands from the related systems which might be conflicted with each other, the feedbacks from the lower levels, the environment variables from the related systems which might affect its properties, the related state variables which is used to specify its process model. One function or component's outputs might be its control actions to the lower levels and the feedbacks to the upper levels. One function or component's precondition is the necessarily existed condition before its execution, which might be the outputs and logical compositions of the other functions or components. One function or component's resource is the necessarily existing powers or materials in its execution, which might be controlled by the other systems.

Simply, it is clear that there are five factors in relation with 10 labels must be considered for a function or component, i.e. its input, output, precondition, resource and model, as shown in Fig. 1(a). Meanwhile, as shown in Fig. 1(b), a function or component should be labeled with 10 labels, named as Input Command (IC), Feedback to the Upper level (FU), Control Action(CA), Feedback from the Lower level (FL), External input Command (EC), Precondition (PC), other related State Variable (SV), Environment Variable (EV), Resource and Executing condition (RE), and Process Model (PM), respectively. The labels and their meanings associated to the relative factors are shown in table 1.



a) FDFC with 5 factors

b) FDFC with 10 labels

Fig. 1. FDFC's 10 labels and 5 factors

Table 1. The labels, meaning and factors

No.	Name	Label	Meaning	Factors
1	Input command	IC	The command to the specified function or component	Input
2	External input command	EC	The control commands from the other channels, which might conflict with IC	Input
3	Feedback from the lower level	FL	Feedback from the lower levels to the specified function or component	Input
4	Environment variable	EV	Variables describing the operating environment of the specified function or component	Input
5	Other related state variable	SV	The related state variables used by the function or component process model	Input
6	Control action	CA	Control action generated by the function or component to control the lower levels	Output
7	Feedback to the upper level	FU	The feedback from the function or component to the upper level	Output
8	Process model	PM	The process model used to generate CA and FU	Model
9	Precondition	PC	The necessary preconditions for a function or component	PC
10	Resource and executing condition	RE	The necessary resource and executing conditions for the specified function or component	RE

3. Functional control structure model (FCSM) of the system

Ordinarily, any system consists of various functions or components, and its FCSM could be configured by connecting various FDFC's labels and considering the relationship among systems and environment conditions. Firstly, ICs, CAs, FUs, FLs and ECs connect each other from one FDFC to another according to their directions defined by the system working principle. Secondly, SVs are used by the system and generated by the other systems. Thirdly, EVs are used by the system and given by the operation environment. Lastly, PC and RE are the precondition or resource of the function under the specified SVs and EVs.

The method of establishing FCSM from multiple FDFC is very similar to not only that of drawing the plan and control chart [11], but also that of drawing program flow chart [12]. Here, FCSM's constitution, rules and steps should be considered comprehensively.

Firstly, FCSM is consist of FDFCs, directional lines and signal marking variables. The relationship among functions or components can be described clearly by FCSM, while the time-sequence relationship and the related interaction would be appeared in various FDFC's models. The directional lines are used to connect the labels of various FDFC according to the system working principle. Every line has its specific starting point and multiple end points. For example, CA and IC can be connected each other with the direction line CA→IC, while FU and FL can be connected each other with the direction line FU→FL. The signal's marking variables are used to declare the signal's name within the directional line. The signals may be the inputs, outputs, preconditions, executing conditions and resources of the specified functions or components.

Secondly, the steps in generating FCSM from FDFCs are shown as Fig. 2 and contain four stages. Stage 1: Decompose the system into various functions or components, which has its inputs, outputs, resources, preconditions and models, and complies with its working principles. Stage 2: For every function or component, list its labels and form the functional detailed lists with their name, type, label and direction as Table 2. Stage 3: From the upper functions or components to the lower ones, connect various functions or components to form FCSM according to their labels and functional detailed lists. Stage 4: Check the obtained lists and modify the FCSM as shown in Fig. 2.

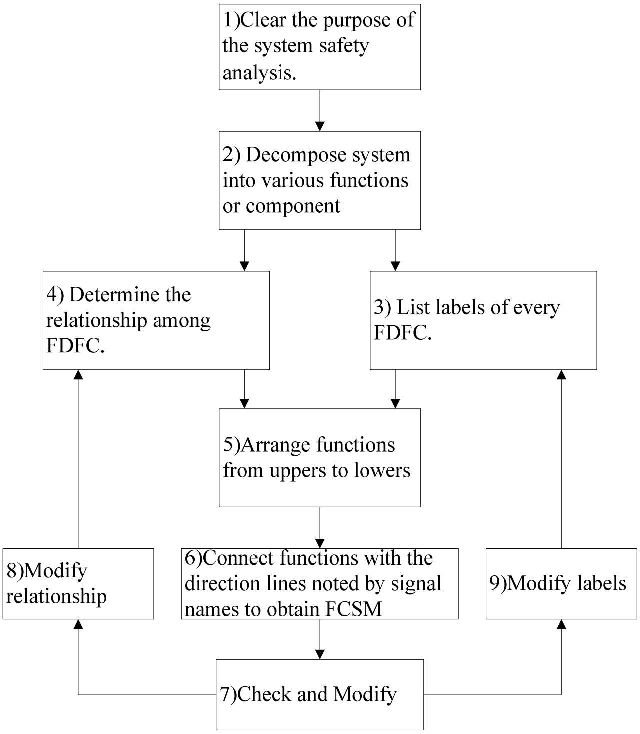

1)Clear the purpose of the system safety analysis.
2) Decompose system into various functions or component
4) Determine the relationship among FDFC.
3) List labels of every FDFC.
5)Arrange functions from uppers to lowers
8)Modify relationship
6)Connect functions with the direction lines noted by signal names to obtain FCSM
9)Modify labels
7)Check and Modify

Fig. 2. FCSM's general steps

Fig. 3 shows the FCSM of the aircraft wheel brake system [13]. The system consists of 4 functions or components, named as FC (Flight Crew), BSCU (Brake System Control Unit), WBSH (WBS Hydraulics) and Wheels. It is a logic system because its inputs, outputs and process models are mainly logic ones. It is complex because it is not only an integrated system of electrics, mechanics and hydraulics, but also a man-machine interaction system. Its FCSM could be obtained from the lists as shown in Table 2.

Table 2. The variables of the aircraft wheel brake system

No	Name	Label	Variable	Directions
1	FC	CA	Brake (pedal)	FC→BSCU FC→WBSH
			BSCU power on/off	FC→BSCU
			Arm and set disarm	FC→BSCU
		PC	Normal/Alternate braking mode	WBSH→FC
		FL	Fault detected	BSCU→FC
			Activated status	BSCU→FC
			Armed status	BSCU→FC
			Programmed deceleration rate	BSCU→FC
		SV	Flight phase (landing, TRO, Taxi, takeoff)	A/C→FC
			Status of other brake mechanism	A/C→FC
			A/C ground speed	A/C→FC
		EV	Runway length	Weather
			Statues of runway (wet or icy)	Weather
2	BSCU	CA	Open/close green shutoff valve	BSCU→WBSH
			Green meter valve position command	BSCU→WBSH
			Open/close blue anti-skid valve	BSCU→WBSH
		IC	Brake (pedal)	FC→BSCU
			BSCU power on/off	FC→BSCU
			Arm and set/disarm for autobrake	FC→BSCU
		FU	Fault detected	BSCU→FC
			Activated status	BSCU→FC
			Armed status	BSCU→FC
			Programmed deceleration rate	BSCU→FC
		FL	Wheel speed	Wheel→BSCU
		SV	Autobrake triggers (touchdown, RTO)	A/C→BSCU
3	WBSH	IC	Brake (pedal)-manual brake	FC→WBSU
			Open/close green shutoff valve	BSCU→WBSH
			Green meter valve position command	BSCU→WBSH
			Open/close blue anti-skid valve	BSCU→WBSH
		CA	Braking force	WBSH→Wheels
		PC	Preconditions	WBSH→CREW
4	Aircraft physical system	IC	Braking force	WBSH→Wheels
		FU	Wheel speed	Wheels→BSCU

As shown in Table 2, any FU of one function or component will have a corresponding FL of the other function or component, and some CA of one function or component will have IC of the other function or component. Meanwhile, in Fig. 3, M1 is the model of flight crew, such as ‘Autobrake Armed/Not Armed’. M2 is the model of BSCU, such as ‘Valve command’. M3 is the model of WBSH, such as ‘Alternate/Normal mode switch’. M4 is the model of Aircraft Physical System, such as ‘A/C speed’. EV is the environment variables of the flight crew, such as ‘Runway length’. SV1 is the related state variables of the flight crew, such as ‘Flight status’. SV2 is the related state variables of BSCU, such as ‘Touchdown’. PC is the working mode of WBS, such as ‘Normal braking mode’. CA1 is the control action from flight crew to BSCU, such as ‘BSCU on/off’. CA2 is the control action from BSCU to WBSH, such as ‘Open/close green shutoff valve’. CA3 is the control action from WBSH to the wheel, such as ‘Braking force’. F1 is the feedback from BSCU to flight crew, such as ‘Armed status’. F2 is the feedback from Aircraft Physical System to BSCU, such as ‘Wheel speed’.

In similar way, FCSM could be obtained from any complex system. Fig. 4 is some – type

Aircraft Flying Control System (AFCS) [14], which is composed of Flight Crew(FC), Automatic Control System (ACS), Fly by Wire (FBW), FBW Hydraulics(FBWH), Control Surface (CS), Monitor Indicators (MI), Monitors and Controllers (MC), Fling Meters (FM), Aircraft Motion Sensors (AMS) and Aircraft. It is a mixed system because its inputs, outputs and process models are mixed ones, such as logical events, motions' dynamics and faults' detecting. It is complex because it is not only an integrated system with multi-redundant electrics, mechanics and hydraulics, but also a man-machine interaction system with multi-various modes.

There are three modes to control aircraft's motion. In ACS mode, ACS receives the automatic control commands from flight crew and sends the control action to FBW resulting in control action passed to FBWH, while FBWH generates the control action to CS resulting in aircraft motions. The specific automatic control mode should be defined by MC. It must receive the feedback signals from AMS. It is noted that ACS mode has its specified preconditions about flight status, altitudes and speeds. In FBW mode, FBW receives the stick displacement electrical signal from flight crew and sends control action to FBWH to control CS resulting in aircraft motions. FBW is multi-redundant channels and must be monitored and controlled correctly by MC to obtain the proper working channel. It must receive the feedback signals from AMS. It is noted that FBW mode must be switch to the Manual mode if there is fatal fault in FBW, such as two FBW channels are successive malfunctional. In Manual mode, CS directly received the stick displacement mechanical control action from flight crew resulting in aircraft motion.

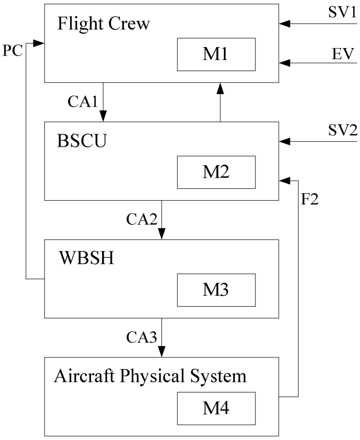


Fig. 3. The CSM of the aircraft wheel brake system

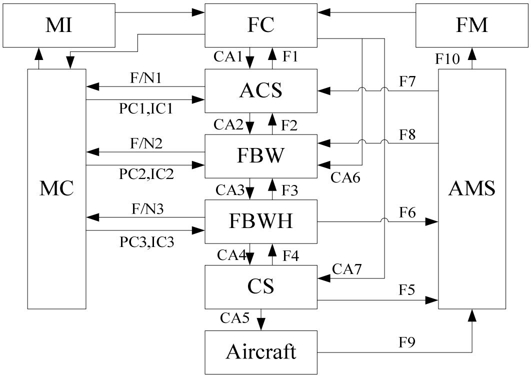


Fig. 4. The FCSM of the aircraft flying control system

4. Hazards and factors

Accident is caused by one of hazards and one accident may be caused by one of many hazards. One hazard may be caused by the composition of the above 10 labels for some functions or components. Every label has a start point and an end point. The information on this label's end point or starting point should be provided or stop timely, in order and effectively. For the convenient of system safety analysis, five Classes of factors are named by "Control Action", "Feedback", "Variable", "Aided Control" and "Model", respectively.

Firstly, for the control action, the necessary control action must be provided when it is necessary and stopped when it is not necessary, and should be provided and stopped timely. If not, it is an unsafe control action (UCA) and might cause hazards. As shown in Table 3, UCA might be caused in four cases. Meanwhile, the provided control action must be followed or executed. If not, it is a malfunctional control action (MCA) and might cause hazards. As shown in Table 3, the malfunctional control action might be caused by the other four cases. MCA means that the control action was provided but not followed or executed. UCA and MCA are regarded as Class "Control Action".

Table 3. Classes, error and causes

No	Classes	Error or unsafe	Types	Causes
1	Control action	UCA (4)	Provided when it is no necessary (PNN)	The control action is provided when there is a contradiction at the current condition
			Not provided when it is necessary (NPN)	The control action is not provided when there is necessary at the current condition
			Provided too late, too soon or out of sequence (PLSS)	The control action is provided too late, too soon and out of sequence, resulting in the unexpected conditions
			Stopped too soon, applied too long (SSAL)	The control action is stopped too soon or applied too long, resulting in the unexpected conditions
		MCA (4)	Conflict with EC (CEC)	The specified control conflicts with EC
			Inadequate PC (IPC)	The control action cannot execute in the specified PC
			Out of CA's capacity (OCC)	Under the current condition, the control action's capacity is not enough to finish IC
			Out of the lower model's variation (OMV)	The control action's requirement does not assign with the scope of the controlled model's variation
2	Feedback	EFU (5) EFL (5)	Not provided when it is necessary (NPN)	The feedback information is not provided (providing) when it is necessary
			Provided but incorrect (PBI)	The feedback information is provided (providing) but incorrect
			Measured (measuring) but inaccurate (MBI)	The feedback information is measured (measuring) but inaccurate such that the feedback information conflict with the other variables to trigger the working mode and to announce improperly
			Provided (providing) but too late or too soon (PLS)	The feedback information is provided (providing) but too late to sample correctly or too soon to sample timely
			Provided (providing) but missing (PMI)	The feedback information is missing, such as digital information
3	Variables	EEV (5)	Not provided when it is necessary (NPN)	The environment variables from the related systems are not provided when it is necessary
			Provided but incorrect (PBI)	The environment variables from the related systems are provided but incorrect
			Measured (measuring) but inaccurate (MBI)	The environment variables from the related systems are measured but inaccurate such that the providing environment variables conflict with the other variables to trigger the working mode and to announce improperly
			Provided (providing) but too late or too soon (PLS)	The environment variables from the related systems are provided but too late to sample correctly or too soon to sample timely
			Provided (providing) but missing (PMI)	The feedback information is missing, such as digital information
		ESV (5)	Not provided when it is necessary (NPN)	The state variables from the total system are not provided when it is necessary
			Provided but incorrect (PBI)	The state variables from the total system are provided but incorrect

			Measured (measuring) but inaccurate (MBI)	The state variables from the total system are measured but inaccurate such that the providing state variables conflict with the other variables to trigger the working mode and to announce improperly
			Provided (providing) but too late or too soon (PLS)	The state variables from the total system are provided but too late to sample correctly or too soon to sample timely
			Provided (providing) but missing (PMI)	The feedback information is missing, such as digital information
4	Aided control	EEC (4)	Provided when it is no necessary (PNN)	The external control action is provided when there is a contradiction with CA
			Not provided when it is necessary (NPN)	The external control action is not provided when it is necessary at the current condition
			Provided too late, too soon or out of sequence (PLSS)	The external control action is provided too late, too soon and out of sequence, resulting in the unexpected conditions
			Stopped too soon, applied too long (SSAL)	The external control action is stopped too soon or applied too long, resulting in. the unexpected conditions
		EPC (4)	Provided when it is no necessary (PNN)	The precondition is provided when there is a contradiction with CA's requirement
			Not provided when it is necessary (NPN)	The precondition is not provided when it is necessary for the current CA
			Provided too late, too soon or out of sequence (PLSS)	The precondition is provided too late, too soon and out of sequence, resulting in the loss of CA
			Stopped too soon, applied too long (SSAL)	The precondition is stopped too soon or applied too long, resulting in the loss of CA
		ECI (4)	Provided when it is no necessary (PNN)	The command inputs are provided when there is a contradiction at the current conditions
			Not provided when it is necessary (NPN)	The command inputs are not provided when it is necessary for the current conditions
			Provided too early, too late, too soon or out of sequence (PELSS)	The command inputs are provided too early, too late, too soon and out of sequence, resulting in the loss of control
			Stopped too soon, applied too long (SSAL)	The command inputs are stopped too soon or applied too long, resulting in the loss of control
		ERE (2)	Not provided when it is necessary (NPN)	The RE is not provided continuously when it is necessary for the current conditions
			Provided but lower in the capacity (PLC)	The RE is provided but its capacity is lower than the required one
5	Model	EPM (3)	Model inconsistent (MICS)	The chosen model cannot meet the actual condition, resulting from the errors of the environment variables, the related state variables and the working mode
			Model incorrect (MICR)	The model is incorrect such that the model cannot work properly
			Model incomplete (MICM)	The model is incomplete such that there is not a proper model under the specified conditions

Secondly, for the feedback information, the necessary one from the uppers (EFU) must be provided timely, accurately and correctly. If not, it is an error feedback information and might cause hazards. As shown in Table 3, EFU might be caused in five cases. Meanwhile, the necessary feedback to the lowers (EFL) must be provided adequately without missing and delay. If not, it is a malfunctional feedback information and might cause hazards. As shown in Table 3, EFL might be caused by the other five cases. EFU and EFL are regarded as Class "Feedback".

Thirdly, for environment variables, the necessary environment variables from the other system must be provided timely, correctly and completely. If not, it is an error environment variable (EEV) and might cause hazards. As shown in Table 3, EEV might be caused in five cases. Meanwhile, the necessary state variables from the total system must be provided timely, correctly and completely. If not, it is an error state variable (ESV) and might cause hazards. As shown in Table 2, ESV might be caused by the other five cases. EEV and ESV are regarded as Class "Variable".

Fourthly, for ex-control action, the necessary external control action must be provided when it is necessary and stopped when it is not necessary, and should be provided and stopped timely. If not, it is an error external control(EEC) action and might cause hazards. As shown in Table 3, EEC might be caused in four cases. Meanwhile, the necessary preconditions must be provided when it is necessary and stopped when it is not necessary, and should be provided and stopped timely. If not, it is an error precondition (EPC) and might cause hazards. As shown in Table 3, EPC might be caused by the other four cases. Furthermore, the necessary command input must be provided when it is necessary and stopped when it is not necessary, and should be provided and stopped timely. If not, it is an error command input (ECI) and might cause hazards. As shown in Table 3, ECI might be caused by the other four cases. Finally, the necessary resource and executing condition for a function or component must be provided when it is necessary, and should be provided effectively and continuously. If not, it is an error resource and executing condition (ERE) and might cause hazards. As shown in Table 3, ERE might be caused by the other two cases. EEC, EPC, ECI and ERE are regarded as Class "Aided Control".

Fifthly, in the model factors, the process model should consider the predicted uncertainty and various disturbances, sufficiently. If not, it is an error process model (EPM) and might cause hazards. As shown in Table 3, EPM might be caused by three cases.

5. Function-Hazards tree and its qualitative analysis for safety

Obviously, the hazards resulting from the types of Table 3 might be shown in Fig. 5, it is very like 'Fault-tree' in the traditional safety analysis, named as Function-Hazard-Tree (FHT), and can be used qualitatively to analysis safety. From FHT, the compositions of EFIs, MFIs, EEVs, ESVs, EECs, ECIs, EPCs and EPMs, resulting from the designing errors, requirement flaws, software error, interaction among other control action or various failures, can generate UCA and MCA.

For the particular system, its FCSM can be built up by the methods given in the Section 3. For example, Fig. 6 shows the FCSM of the aircraft wheel brake system. Meanwhile, in order to analyze the cause of UCA and MCA, FCSM for the specified behavior (flight crew or Autobrake, in this example), which is consist of five factors as shown in Fig. 5, must be considered. The five factors in Fig. 6 are given in Table 4. Furthermore, UCA and MCA can be discovered qualitatively according to the possible compositions as shown in Table 5.

It is noted that quantitative analysis for the safety would implement easily based on FCSM and FHT. Firstly, UCA and MCA resulting from the FHT and its qualitative analysis might be used to determine the design requirement to eliminate or mitigated the influence of UCA and MCA. Secondly, some non-identifying new UCA and MCA would be discovered quantitatively by considering the possible compositions of EFIs, MFIs, EEVs, ESVs, EECs, ECIs, EREs, EPCs, and EPMs from FCSM. Lastly, Quantitative analysis for every UCA and MCA might be useful to discover EFIs, MFIs, EEVs, ESVs, EECs, ECIs, EREs, EPCs, and EPMs as completely as possible.

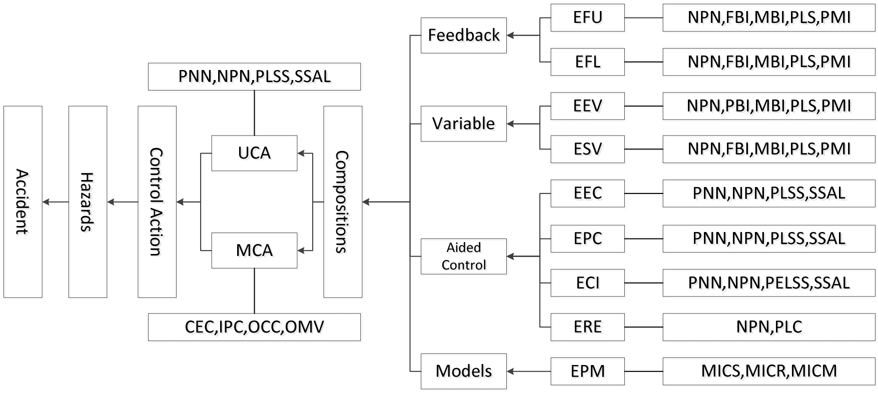


Fig. 5. Function Hazards tree

Table 4. Classes in Fig. 6

No.	Classes	Contents
1	Control action	Manual brake command
2	Aided-control	Normal/Alternate braking mode
3	Feedback	Autobrake activated status
		Autobrake armed status
		Autobrake deceleration rate
		Fault detected
4	Variables	Flight status
		Actual deceleration rate
		Wheel speed
		Runway length
		Other brake mechanisms' status
5	Model	Auto-brake Armed/Not armed
		Auto-brake deceleration rate
		Auto-brake activation status
		WBS Normal/Alternate braking mode
		BSCU power on/off
		Manual provided/Not provided
		Flight status (touchdown, rejected takeoff, taxi, etc.)
		Aircraft status (speed, deceleration rate, etc.)

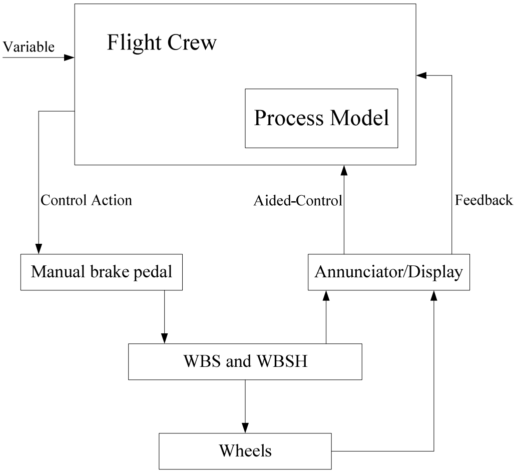


Fig. 6. The control process model of aircraft wheel brake system for flight crew

Table 5. Hazards and factors

<table>
<tr><td>H-1</td><td colspan="6">Inadequate aircraft deceleration upon landing, rejected takeoff, or taxing</td></tr>
<tr><td>H-2</td><td colspan="6">Aircraft maneuvers out of safe regions</td></tr>
<tr><td>No.</td><td>Control</td><td>Feedback</td><td>Variable</td><td>Ex-control</td><td>Model</td><td>Hazard</td></tr>
<tr><td>1</td><td>Manual barking</td><td>BSCU Fault detected</td><td>Flight status</td><td>Auto-brake</td><td>BSCU fault/ no fault</td><td>H-1, H-2</td></tr>
<tr><td colspan="7">UCA: Crew does not provide manual braking during landing when Auto-brake is not providing braking.
Due to:
EFL: Fault detect of BSCU is not provided during landing when BSCU is fault.
ESV: Flight state is not provided during landing.
EPM: The process model of BSCU fault/no fault is incorrect.</td></tr>
<tr><td>2</td><td>Manual braking</td><td>The feeling of the pedal pressure</td><td>Flight status</td><td>Auto-brake</td><td>BSCU fault/ no fault</td><td>H-1, H-2</td></tr>
<tr><td colspan="7">UCA: Manual braking provided with insufficient pedal pressure, resulting in inadequate deceleration during landing.
Due to:
EFL: The feeling of the pedal pressure by pilots is not correct or too late.
ESV: Flight state is not provided during landing.
EPM: The process model of BSCU fault/no fault is incorrect.</td></tr>
<tr><td>3</td><td>Manual braking</td><td>touchdown</td><td>Flight status</td><td>Auto-brake</td><td>Manual braking provided/ not provided</td><td>H-1, H-2</td></tr>
<tr><td colspan="7">UCA: Manual braking applied before touchdown causes wheel lockup, loss of control, tire burst.
Due to:
EFL: The feeling of the pedal pressure by pilots is incorrect or too late.
ESV: Flight state is incorrect.
EPM: The process model of manual braking provided/ not provided is incorrect.</td></tr>
<tr><td>4</td><td>Manual braking</td><td>Taxi speed runway length</td><td>Flight status</td><td>Auto-brake</td><td>A/C ground speed</td><td>H-1, H-2</td></tr>
<tr><td colspan="7">UCA: Manual braking command is stopped before safe taxi speed is reached, resulting in over-speed or overshoot.
Due to:
EFL: The runway is too short or noted by pilots too late.
ESV: Flight state is not provided during taxing
EPM: The process model of A/C ground speed is incorrect.</td></tr>
<tr><td>…</td><td>…</td><td>…</td><td>…</td><td>...</td><td>…</td><td>…</td></tr>
</table>

6. Conclusion

The safety problem for the complex system is regarded as a control problem and the FCSM for the specified system was established in terms of its FDFCs. Based on the viewpoint that the hazards are due to UCA or MCA, a FHT is obtained from five classes "Control Action", "Feedback", "Variable", "Aided Control" and "Model". Control Action might be UCA and MCA, feedback might be EFU and EFL. Variable might be EEV, ESV. Aided-control might be EEC, ECI, EPC, ERE. Model might be three cases of EPM. The aircraft wheel brake system's control structure model is given to show its effectiveness.

Furthermore, the quantitative analysis should be researched. In fact, based on FCSM, we can obtain the designed simulation system for the particular system to establish the total FCSM with detailed mathematic model for every model, detailed signal properties for every connection label. Various error models should be established for every label's starting point and end one. Next we will contribute an article for the quantitative analysis of the specified system.

It is noted that Nancy's research report [13, 15] indicated that STAMP/STPA might be instead of the analysis method suggested in SAE ARP 4761 [16] such that the analysis will be more general. Meanwhile, the requirements of FAA-AC25.1309 [17] are more covering, but there is no effective way to check if the particular systems, equipment have been compliance with these requirements. Here, FCSM based on FDFCs could find more comprehensive safety requirement resulting in more safe system.

References

[1] **Miller Frederic P., Vandome Agnes F., McBrewster John** Systems Engineering. Alphascript Publishing, 2013.

[2] **Ogata Katsuhiko** Modern Control Engineering. Pearson Custom Publishing, 2009.

[3] **Shouyi Liao** Research on Methodology of Agent-Based Modeling and Simulation for Complex System and Application. National University of Defense Technology, 2005.

[4] **Alexander Robert, Kazakov Dimitar, Kelly Tim** System of systems hazard analysis using simulation and machine learning. Computer Safety, Reliability and Security, 2006, p. 1-14.

[5] **Leveson Nancy** A STPA Primer. Version 1, MIT SERL, http://sunny.mit.edu/STPA-Primer-v0.pdf, 2014.

[6] **Leveson Nancy** A new accident model for engineering safer systems. Safety Science, Vol. 42, Issue 4, 2004, p. 237-270.

[7] **Thomas John** Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis. Ph.D. Dissertation, MIT Engineering Systems Division, 2013.

[8] **Stringfellow Margaret V.** Accident Analysis and Hazard Analysis for Human for Organizational Factors. Ph.D. Thesis, MIT, 2010.

[9] **Thornberry Cameron L.** Extending the Human Controller Methodology in Systems-Theoretic Process Analysis (STPA). Master Thesis, MIT, 2014.

[10] **Hollnagel E.** FRAM: The Functional Resonance Analysis Method. Ashgate Publishing Limited, Denmark, 2012.

[11] **Yinghuai Cao, Jian Yin, Chunmei Liang** Military Operation Reserch. National Defense Industry Press, 2013.

[12] **Williams Laurie A.** An Introduction to Software Engineering. Williams Publishing, 2013.

[13] **Leveson Nancy, Fleming Cody, Thomas John** A Comparison of SAE ARP 4761 and STPA Safety Assessment Processes. MIT PSAS Technical Report.

[14] **Cai Manyi** A typical flying control system. AFEE, 2001, p. 78-90, (in Chinese).

[15] **Fleming Cody, Nancy G. Leveson** Improving hazard analysis and certification of integrated modular avionics. Journal of Aerospace Information Systems, Vol. 11, Issue 6, 2014, p. 397-411.

[16] Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. SAE ARP 4761, 1996.

[17] Advisory Circular. AC 25.1309-1A, System Design and Analysis, AC 25.1309-1A, FAA, 1988.