Journal of Systems Engineering and Electronics
Vol. 35, No. 3, June 2024, pp.689 – 706

Risk identification and safety assessment of human-computer interaction in integrated avionics based on STAMP

ZHAO Changxiao[1], LI Hao[2], ZHANG Wei[1], DAI Jun[1], and DONG Lei[3,*]

1. School of Safety Science and Engineering, Civil Aviation University of China, Tianjin 300300, China;
2. Shenzhen Dajiang Innovation Technology Co., Ltd., Shenzhen 518057, China;
3. Key Laboratory of Civil Aircraft Airworthiness Technology, Civil Aviation Administration of China, Tianjin 300300, China

Abstract: To solve the problem of risk identification and quantitative assessment for human-computer interaction (HCI) in complex avionics systems, an HCI safety analysis framework based on system-theoretical process analysis (STPA) and cognitive reliability and error analysis method (CREAM) is proposed. STPA-CREAM can identify unsafe control actions and find the causal path during the interaction of avionics systems and pilot with the help of formal verification tools automatically. The common performance conditions (CPC) of avionics systems in the aviation environment is established and a quantitative analysis of human failure is carried out. Taking the head-up display (HUD) system interaction process as an example, a case analysis is carried out, the layered safety control structure and formal model of the HUD interaction process are established. For the interactive behavior "Pilots approaching with HUD", four unsafe control actions and 35 causal scenarios are identified and the impact of common performance conditions at different levels on the pilot decision model are analyzed. The results show that HUD's HCI level gradually improves as the scores of CPC increase, and the quality of crew member cooperation and time sufficiency of the task is the key to its HCI. Through case analysis, it is shown that STPA-CREAM can quantitatively assess the hazards in HCI and identify the key factors that impact safety.

Keywords: avionics, human-computer interaction (HCI), safety assessment, system-theoretic accident model and process, human reliability analysis.

DOI: 10.23919/JSEE.2024.000031

1. Introduction

According to statistics, more than 60% of catastrophic civilian aircraft accidents are due to human factors [1]. Therefore, many new technologies have emerged to reduce the pilot's workload, improve the pilot's situational awareness, such as head-up display systems [2], cockpit touch screens [3] and even artificial intelligence co-pilot technology [4]. The applications of new technologies have brought new human-computer interaction (HCI) modes, and greatly increased the complexity of airborne systems. Identifying HCI risks and quantitatively assessing their impact on aircraft safety have become key issues in the development of airborne devices. In May 2019, the Federal Aviation Administration (FAA) issued Advisory Circular AC00-74, which sets out the requirements for considering human factors assessment of avionics systems in civil aircraft during the design phase [5]. Safety evaluation standards widely used in the aircraft field include Society of Automotive Engineers (SAE) Aerospace Recommended Pratice (ARP) 4761 for civil aircraft and MIL-STD-882E for military aircraft which at its core is based on the decomposition and validation of safety metrics based on a dual "V" system. These standards, assuming the relative independence of the components of each function of the airborne system, are unable to effectively evaluate an integrated avionics system [6] with shared resources, nor do they cover the assessment of HCI related risks. Some new safety assessment theories have been introduced into the field of airborne systems. In project of Dassault 7x, the model-based safety analysis techniques were used, by which the fault model extension of the system model was carried out by using the formal method. The safety analysis workload of the iterative design in complex systems was greatly reduced [7]. Subsequently, fault behavior description methods such as hierarchically performed hazard origin and propagation studies (HIP-HOPS) [8], fault extension based on complex network models [9], and formalized modeling languages such as system modeling language (SysML), architecture analysis and design language (AADL), and AltaRica [10] begin to be used for the aircraft safety analysis domain. In terms of human factors, the civil aircraft industry has clear airworthiness requirements for devices

Manuscript received August 25, 2022.
*Corresponding author.
This work was supported by the National Key Research and Development Program of China (2021YFB1600601), the Joint Funds of the National Natural Science Foundation of China and the Civil Aviation Administration of China (U1933106), the Scientific Research Project of Tianjin Educational Committee (2019KJ134), and the Natural Science Foundation of Tianjin, Intelligent Civil Aviation Program (21JCQNJC00900).

with human-computer interfaces, such as the FAR 25.1302, and some scholars have also analyzed HCI risks in airborne systems. Han et al. [11] identified the human error in shipboard landings, assessed the reliability of HCI, and has subsequently proposed a simulation method based on the control theory. Thomas [12] examined the elements of the human-computer interface in the aircraft cockpit that affect the distribution of the pilot's attention. These studies have all regarded human factors as independent issues and failed to incorporate them into the overall aircraft safety assessment system, lacking a uniform safety assessment framework covering HCI analysis.

Levenson had proposed the system-theoretical process analysis (STPA) [13]. It characterizes the system's safety problem as the emergence of the system, which is controlled by constraining the behavior and interaction of system components [14]. STPA, as a safety analysis framework that can be combined with different quantitative analysis methods, has been used and yielded great results in chemical, nuclear power and rail transit applications. In terms of onboard systems, Hu et al. [15] introduced STPA to model the wheel braking system and analyzed the unsafe control behaviors of the system. In Castilho's work [16], STPA was used to identify the hazards of crosswind takeoffs with light aircraft and the mitigating actions that could make its execution safer. Zhao et al. [17] presented STPA-UPPAAL and STPA-Bayes safety analysis and evaluation model respectively with the head-up display (HUD) system as an example. It can be seen that STPA, as a safety analysis framework, can be combined with different analytical features. The human reliability analysis (HRA) model can quantify human behavior and safety impacts, which can be combined with STPA. According to the development time of HRA, it has developed three generations [18]: the representative method of the 1st generation is the technique for human error rate prediction (THERP) which breaks down human behavior into specific operational steps along the course of events, and then calculates the probability of failure for this event by getting the corresponding human failure probability values under experts' judgment. The representative method for the 2nd generation is the cognitive reliability and error analysis method (CREAM) which argues that human behavior is not random but depends on the actual interaction scenarios. Human factors reliability in the current scenario is calculated based on multiple factors of the interaction scenario. The representative approach of the 3rd generation is the information, decision, and action in crew (IDAC), which builds a dynamic simulation system to simulate the dynamics of the scenario and the changes in human behavior to characterize the dynamics of human factors reliability.

The analysis of the human factor model reveals that THERP mainly focuses on the analysis of human output behavior and lacks the analysis of the human behavioral influences. CREAM mainly focuses on the identification of failure causes and the mechanisms. It emphasizes more on the influence of interactive scenarios on human behavior. Compared with the previous two generations of methods, IDAC establishes a simulation-based dynamic analysis method, which mainly focuses on dynamic simulation and change. Although it overcomes the limitation of the lack of dynamic analysis in the previous two generations and introduces system simulation instead of album judgment, so far, there are still limitations in simulation data and calculations that make it difficult to perform accurate simulations. At the same time, this method is not used in the same framework as traditional methods such as fault trees and can only be applied to interactive analysis under specific conditions.

Although CREAM is the method of the second generation, it is the most widely used. Its basic data is accumulated over years of research, which has certain reliability and has been applied in human factor analysis in many safety-demanding fields. At the same time, to make CREAM better applied to practical engineering, in the past three years, many scholars have carried out in-depth research and improvement. Akyuz et al. [19] used CREAM to assess human reliability along with the cargo loading process on-board LPG tanker ships and systematically predict human error potentials for designated tasks and determine the required safety control levels. Ahn et al. [20] introduced a new framework based CREAM applicable to the maritime industry, and fuzzy multiple attributive group decision-making method, Bayesian networks and evidential reasoning are employed for enhancing the reliability of human error quantification. Zhou et al. [21] had enhanced HRA model to provide more reliable results of personnel performance failure. Zhang et al. [22] proposed the predicted mean vote-CREAM (PMV-CREAM) method using the PMV index calculated by using human factors and dynamic environmental data to effectively analyze the dynamic human factors reliability of manned submersibles. Xi et al. [23] developed a human factors analysis tool SAFPHR based on CREAM and probabilistic model detection to dynamically analyze community pharmacy dispensing systems to predict medication error rates. It can be seen that through improvements and research, the CREAM method has been embraced in several fields as an effective method for quantifying human factors.

In the above research, some scholars introduced formalization into STPA analysis, effectively reducing the dependence on human experience and workload. However, the above analysis paid more attention to the impact of the system itself and did not consider the impact of human reliability. At the same time, the above research on CREAM did not consider the connection with the system safety analysis, and tended to manual calculation, resulting in a large workload.

For the above reasons, this paper, considering the safety critical avionics system and the safety assessment standard SAE ARP 4761, combines STPA and CREAM to create a detailed interaction model for safety analysis of HCI in the airborne system. Compared with CREAM, STPA-CREAM fully considers the impact of multi-party interactions on the risk of human-caused interactions by establishing a hierarchical safety control structure of the airborne system. At the same time, STPA-CREAM uses formal verification to replace CREAM's antecedent-consequence matrix to determine the causal path of each hazard and gives multiple causal paths to improve the efficiency of the analysis.

In summary, this paper takes both the complexity of airborne systems and the characteristics of multiparty interactions into consideration to solve the problem of HCI identification and safety assessment. An HCI safety analysis method STPA-CREAM is proposed based on system engineering and human factor reliability. STPA-CREAM formal modeling and quantitative analysis are the key and difficulty of this paper. Compared with previous studies based on basic STPA framework analysis [24,25], the STPA-CREAM method has richer descriptions of artificial controllers by integrating human factors into system safety analysis, increases human failure models and basic failure probability, and provides indicators for analyzing interaction scenarios and HCI safety analysis and evaluation. Finally, a case study is presented with airborne head-up display system HCI as an example.

2. Preliminaries

2.1 STPA

STPA introduces a systems theory based approach that views the object of analysis as a whole, rather than the sum of its parts, and the traditional cause-and-effect model has been extended not only to include directly related failure events or component failures but also to incorporate more complex processes and unsafe interactions between system components. The STPA technique regards safety as a dynamic control problem rather than a failure prevention problem [13], and its analysis steps are shown in Fig. 1.

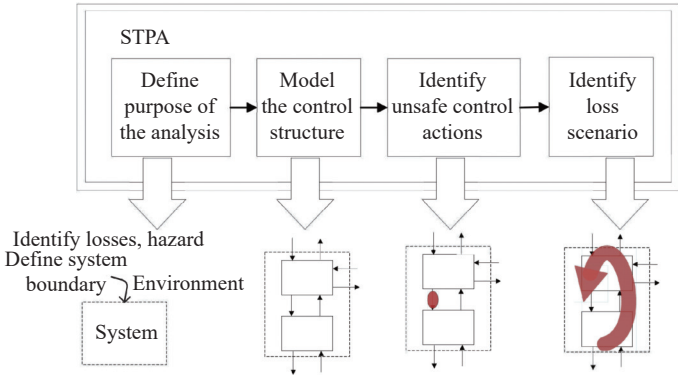


Fig. 1 Overview of the basic STPA method

STPA is divided into four steps: (i) defining the purpose of the analysis; (ii) establishing a safety control structure with a hierarchical control system; (iii) identifying the unsafe control action (UCA) in the control structure and verifying how such actions can lead to system loss; (iv) analyzing the causal scenarios that may lead to UCA, which can be further used to generate additional requirements, identify mitigation measures, and better system architecture, etc.

2.2 CREAM method

The CREAM, a representative method of the second generation of HRA, quantifies the probability of a possible failure state by introducing common performance conditions (CPCs) and analyzing specific impacts. The CREAM can be applied in four steps. Firstly, the failure modes of activities are identified, and the interactive tasks are decomposed into four basic cognitive functions, namely, observation, interpretation, planning, and execution, and their possible failure modes are identified. After years of development of the CREAM method, a more plausible failure probability interval of the failure probabilities of basic human cognitive functions has been given. The failure of basic cognitive function has been given by Hollnagel [26] who integrated multiple data sources from different fields. The data is shown in Table 1, which is used as the basic dataset in this paper.

Table 1 Failure of basic cognitive function

Generic failure type	Basic human error probability	Basic human error probability
Observe	O_FMEA_1: wrong object	1.0E−3
	O_FMEA_2: wrong identification	7.0E−2
	O_FMEA_3: missed observation	7.0E−2

Continued

Generic failure type	Basic human error probability	Basic human error probability
Interpretation	I_FMEA_1: faulty diagnosis or incomplete diagnosis	2.0E−1
	I_FMEA_2: decision error or incomplete decision	1.0E−2
	I_FMEA_3: delayed interpretation	1.0E−2
Planning	P_FMEA_1: priority error	1.0E−2
	P_FMEA_2: inadequate plan or inappropriate plan	1.0E−2
Execution	E_FMEA_1: action of wrong type	3.0E−3
	E_FMEA_2: action on wrong object	5.0E−4
	E_FMEA_3: action with wrong sequence	3.0E−3
	E_FMEA_4: incomplete action or missed action	3.0E−2
	E_FMEA_5: action at the wrong time	3.0E−3

The CREAM method suggests that human misbehavior is the result of the interaction of various situational factors, and the failure probability correction method can be adapted for different scenarios. We adopt the same classification criteria as literature [21,26] and divide it into nine categories of CPCs. Therefore, a correction of the basic failure probability is achieved by evaluating the current operating scenario using the CPC model. Finally, different control modes are divided according to the occurrence probability of series/parallel calculation based on the causative path.

3. STPA-CREAM framework

STPA can well describe the multi-party interaction within the system, but it does not define the human processing model. CREAM has a complete definition of human processing mode, including human basic cognitive functions, basic failure modes, failure rates, and human factor evaluation, but it simplifies HCI into a single control chain to deal with, which is too simple. Also, both of the above are manual analyses. When the iterative design is carried out, it is easy to face problems such as heavy workload and easy to make mistakes. If the two methods are combined and modeling and analysis are performed through formal verification tools at the same time, not only can the HCI process of a complex system be described well, but also automated analysis can be realized, reducing the workload of iterative design and improving efficiency. The STPA-CREAM analysis framework is shown in Fig. 2.

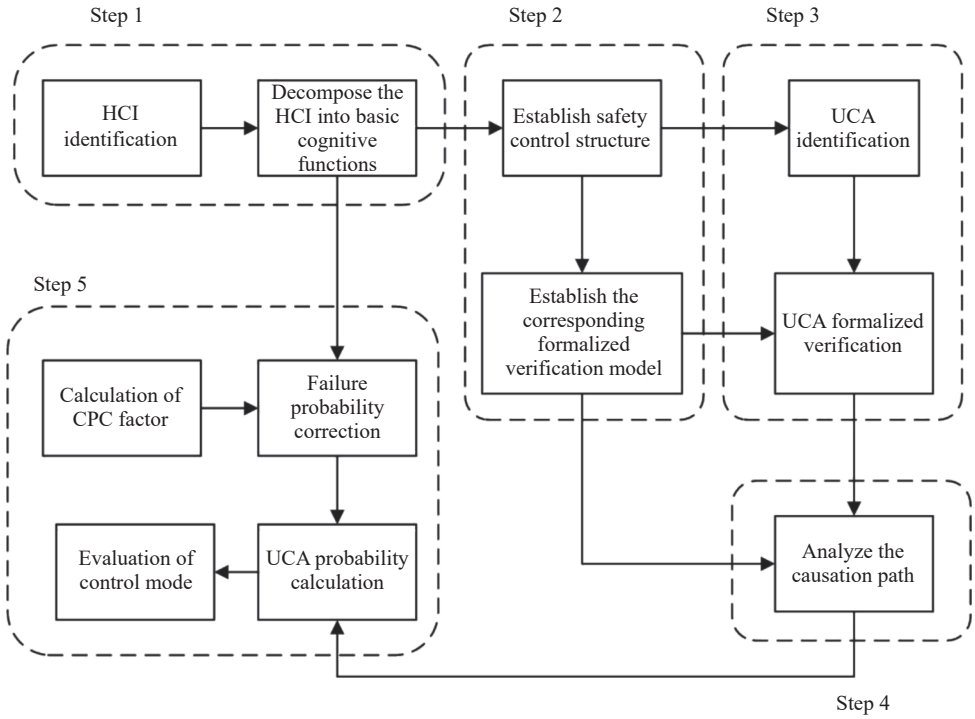


Fig. 2 STPA-CREAM analysis framework

Based on the STPA-CREAM method, the analysis step can be divided into five steps.

Step 1 HCI tasks identification and decomposition: Define purpose of the analysis and use the method given by CREAM to decompose the HCI tasks of the airborne system under different scenarios into combinations of basic cognitive functions and to obtain their possible failure modes and basic failure probabilities.

Step 2 STPA-CREAM modeling: use STPA's safety control structure to capture the details of the HCI process, it treats the interaction process as a control feedback loop, rather than a simplified control chain. At the same time, the human processing model of CREAM is integrated into the interaction modeling, and the possible failure modes of the human operation process are fully considered to analyze the possible hazards in the HCI process. The entire STPA-CREAM modeling process is implemented through formal verification tools to facilitate subsequent automated verification and analysis of hazards.

Step 3 HCI risk identification and verification: according to STPA technique, identify potential UCAs during the HCI process, and use formal verification tools to verify them.

Step 4 Causal path search: with the help of a formal verification tool, the causal path of UCA after verification is searched automatically. It can improve the efficiency of analysis and reduce the dependence on the analysis experience of analysts.

Setp 5 STPA-CREAM quantitative analysis: after determining the causal path, a quantitative analysis of each unsafe control action is required to determine whether the corresponding HCI process under the current design is in an acceptable state.

Step 2 and Step 5 are the main innovations of this paper. They show how to combine STPA and CREAM from the perspective of modeling and quantitative analysis and integrate automation tools to realize automatic analysis and calculation of HCI hazards.

The STPA-CREAM method is an extension based on original STPA. The comparison between the two methods is shown in Table 2.

Table 2 Comparison between original STPA and STPA-CREAM

Step of original STPA method	Step of STPA-CREAM method
Define purpose of the analysis	(i) Define purpose of the analysis (ii) HCI tasks identification and decomposition
Model control structure	(i) Model control structure integrated with CREAM (ii) UPPAAL modeling integrated with CREAM
Identify UCA	(i) Identify UCA (ii) Verify UCA with UPPAAL
Identify loss scenario	Identify loss scenario by UPPAAL
/	Perform UCA quantitative analysis

3.1 STPA-CREAM modeling

The first step of STPA-modeling is to build a hierarchical safety control structure to capture the details of the HCI process. Safety control structure consists of four modules: controllers, actuators, sensors and the controlled process. Each module is composed of four parts: architecture, process model, control algorithm and failure model, as shown in Fig. 3, wherein the controller may be a human operator or a system component.

For system components, the architecture is mainly used to describe the physical structure and data flow paths within the components, and to define the inputs and outputs of the module; the process model contains all operating states and output variables inside the components as well as their set of values; control algorithm includes state transfer function and the output function inside the component; the failure model describes the failure model of the component and its effects.

To define the human operators, CREAM is introduced to model HCI to improve the construction of the human processing model. The architecture represents the operation task flow and defines the input and output of the operation task. The process model describes all the operating status and task output variables and their value sets. The control algorithm refers to the human judgment and thinking mode. The failure model describes the failure model of human operation and its impact, which are composed of the failure modes of CREAM's four basic cognitive functions.

CREAM mainly focuses on the identification of failure causes and the study of mechanisms and emphasizes more on the influence of interactive scenarios on human behavior. Compared with other HRA methods, it is the most widely used and its basic data is accumulated over years of research and has been applied in several safety-critical fields. This is the reason for choosing CREAM. Next, use formal verification tools to establish HCI model based on the STPA safety control structure to facilitate subsequent automated verification and analysis of hazards. Due to the complexity and multiparty interaction of the airborne system, as well as the real-time nature of HCI, the formal verification tools UPPAAL is chosen.

UPPAAL is a formal verification tool based on time automata, including editors, simulators and verifiers. It can model and simulate real-time systems, as well as automatically verify system-related properties. Compared with other tools, UPPAAL has a complete graphical interactive interface, which can automatically verify and give counter-example paths. At the same time, it can also consider time in modeling and analysis. Due to its

high efficiency and convenience, UPPAAL has been widely used in several fields and has been demonstrated to be effective in combination with STPA to carry out automated verification of unsafe control behaviors [17].

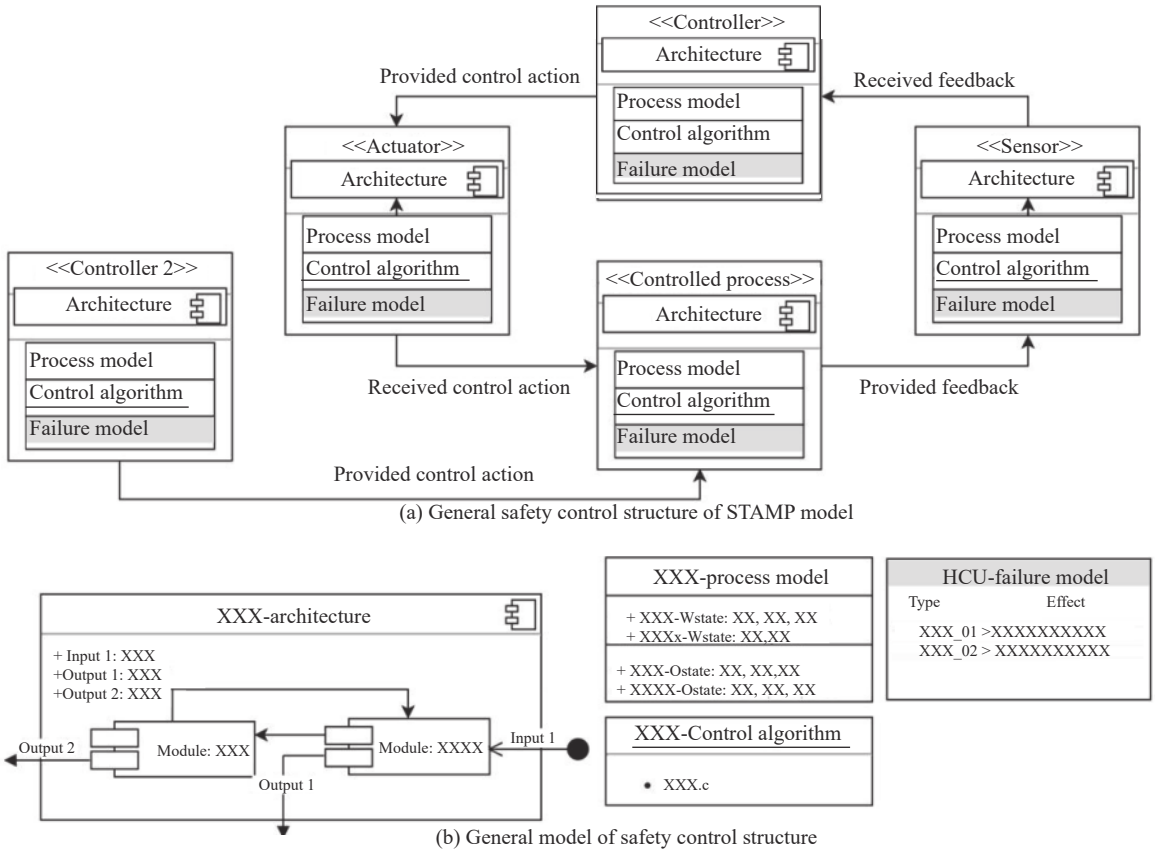


Fig. 3 Schematic diagram of the safety control structure

In UPPAAL, a complex real-time system is a network of time-automated machines which is composed of some time automatons that collaborate [27,28]. Each time automaton corresponds to a template, and each template consists of several locations. Communication between the templates can be done via synchronization, in which "!" means send and "?" means receive. Position shifting can be conditionally triggered by using clock to constrain time and guard as well as using update to assign values and change the corresponding data. In addition, invariant and rate of exponential are used to further constrain and define the temporal properties of the position.

The modeling process is as follows. Firstly the system-level UPPAAL model is declared. Then, the controller, actuator, sensor and the UPPAAL template according to the safety control structure are established respectively. Next, the detailed physical architecture of each component is modeled, and the modules in the architecture are defined as locations and the variables for the corresponding locations and the control algorithms are declared, while location transfers and boundaries, namely, data flow paths, are defined through supervision, updates, and clocks. Finally, failure modes are declared and injected into the model.

UPPAAL uses the Backus-Naur form (BNF) to describe the relevant properties of the model, conducts automated validation via time automaton network accessibility analysis and gives the corresponding causal paths [29].

3.2 STPA-CREAM quantitative analysis

After determining the cause path, it is necessary to evaluate each unsafe control behavior to determine whether it is in an acceptable state. In the HCI process, the failure probability of UCA changes with the change of the environment, and it needs to be modified under specific scenarios. Therefore, this paper selects nine types of CPC to analyze the current interactive scenarios. By scoring nine CPCs and calculating the failure impact factors of different CPCs on basic cognitive functions, the effects of different interaction scenarios on interaction tasks, which are composed of basic cognitive functions, are obtained,

and the failure probability can be corrected. Finally, UCA is evaluated according to the calculated failure probability. The whole process consists of four steps. Next, it will be divided into two parts to introduce.

3.2.1 Calculation of CPC failure impact factor and probability correction

HCI analysis requires a human factors error evaluation on the UCA during the interaction process, and after determining the causal path of each interaction hazard, it is necessary to obtain the failure probability of each failure mode to complete the quantitative analysis. The CREAM method holds that the failure probability of cognitive functions varies as the environment changes and requires probabilistic correction in different application scenarios. In this paper, nine types of CPC are set for the airborne system characteristics, in conjunction with the CREAM method.

We adapt the CPCs defined in the CREAM method [26] and map them to the actual application scenarios which is the HCI in complex avionics systems. The specific explanation is as follows: organizational integrity (CPC1) mainly covers the units involved in the interaction process such as the degree of specialization in the division of responsibilities within the airlines, and the integrity of safety regulations. Working condition (CPC2) refers to the working environment of the cockpit. The perfection of human-computer interface and operation support (CPC3) is used to analyze the use of HCI equipment, human-computer distribution balance as well as the equipment safety and reliability in flight. The availability of the plan (CPC4) refers to the completeness and reasonableness of operating manuals, emergency procedures, and routines, etc. The number of concurrent targets (CPC5) includes the number of contingencies occurring during the mission and the difficulty of the task. Time sufficiency (CPC6) considers the amount of time provided to the pilot to handle the interaction task and the intensity of the interaction. Adequacy of training and experience (CPC7) includes pilot training time, training content, and experience with the equipment. The quality of crew member cooperation (CPC8) includes the manner, quality, frequency, and level of trust in member communication and interaction. Circadian rhythm (CPC9) refers to the pilot's work time range.

There are two categories based on CPC1 to CPC8 ratings and scoring range:

(i) A three-level CPC (CPC2/ CPC4/ CPC5/ CPC6/ CPC7), with levels 1/2/3 corresponding to advantageous/ compatible/incompatible;

(ii) A four-level CPC (CPC1/CPC3/CPC8), with levels 1/2/3/4, corresponding to very effective/effective/inefficient/deffective.

CPC9 does not require a rating, and includes two levels, day and night, corresponding to the time interval of [1,8,18,24].

Level (3 levels or 4 levels) is a general attribute of CPC, whether each CPC belongs to three levels or four levels depends on the impact of the CPC on human reliability. This is determined by reference to original CREAM reliability data and the collection and analysis of avionics system HCI accident data.

The expectation effects of each CPC level and the basic effect weighting factors on basic cognitive function are also determined, as shown in Table 3.

Table 3 Relationship between CPCs and reliability

Number	Level	Effect	Weighting factor of cognitive function (base value)			
			Observe	Interpretation	Planning	Execution
1	Very efficient	Increase	1.0	1.0	0.8	0.8
	Efficient	Neutral	1.0	1.0	1.0	1.0
	Inefficient	Decrease	1.0	1.0	1.2	1.2
	Deficient	Decrease	1.0	1.0	2.0	2.0
2	Advantageous	Increase	0.8	0.8	1.0	0.8
	Compatible	Neutral	1.0	1.0	1.0	1.0
	Incompatible	Decrease	2.0	2.0	1.0	2.0
3	Very efficient	Increase	0.5	1.0	1.0	0.5
	Efficient	Neutral	1.0	1.0	1.0	1.0
	Inefficient	Neutral	1.0	1.0	1.0	1.0
	Deficient	Decrease	5.0	1.0	1.0	5.0

Continued

Number	Level	Effect	Weighting factor of cognitive function (base value)			
			Observe	Interpretation	Planning	Execution
4	Advantageous	Increase	0.8	1.0	0.5	0.8
	Compatible	Neutral	1.0	1.0	1.0	1.0
	Incompatible	Decrease	2.0	1.0	5.0	2.0
5	Advantageous	Increase	1.0	1.0	1.0	1.0
	Compatible	Neutral	1.0	1.0	1.0	1.0
	Incompatible	Decrease	2.0	2.0	5.0	2.0
6	Advantageous	Increase	0.5	0.5	0.5	0.5
	Compatible	Neutral	1.0	1.0	1.0	1.0
	Incompatible	Decrease	5.0	5.0	5.0	5.0
7	Advantageous	Increase	0.8	0.5	0.5	0.8
	Compatible	Neutral	1.0	1.0	1.0	1.0
	Incompatible	Decrease	2.0	5.0	5.0	2.0
8	Very efficient	Increase	0.5	0.5	0.5	0.5
	Efficient	Neutral	1.0	1.0	1.0	1.0
	Inefficient	Neutral	1.0	1.0	1.0	1.0
	Deficient	Decrease	2.0	2.0	2.0	5.0
9	Day	Neutral	1.0	1.0	1.0	1.0
	Night	Decrease	1.2	1.2	1.2	1.2

In Table 3 1−9 corresponding to CPC1−CPC9 respectively, are used to evaluate the interaction scenarios, where the impact weighting factors describe the effects of different CPC on four basic categories of cognitive function and the values derive from the results of relevant human factors research [20,21,26]. These researches use the basic probability of cognitive failure as the first approximation, with a weighting factor of 1 when the effect of CPC on cognitive function is weak; weighting factor less than 1 when positive; weighting factor greater than 1 when negative.

Different levels of CPC in different interaction scenarios will directly affect the pilot's cognitive control patterns and expected effect of reliability performance under the current scenarios. By scoring the nine CPC on the interaction scenarios, the total failure factor of CPC on basic cognitive function is calculated, and the failure probability is modified. From Subsection 3.2, it is clear that the different level grades have overlapping scoring intervals (CPC9 only relates to hours of work and does not require ratings, thus it does not need taking into consideration), hence it is inevitable to face its inherent uncertainty.

Fuzzification is to decompose the input variables of a system into one or more fuzzy sets and use a membership function to fuzz the data to generate fuzzy perception with multiple inputs, which can effectively solve the fuzzy phenomena that exist in reality and deal with uncertainty. The trapezoidal fuzzy numbers are the most commonly used fuzzy numbers, which are applied in this study.

The membership function for trapezoidal fuzzy numbers is as follows:

$$\mu(x)=\begin{cases}0, & 0\leqslant x\leqslant a, x\geqslant d\\ (x-a)/(b-a), & a<x<b\\ 1, & b\leqslant x\leqslant c\\ (d-x)/(d-c), & c<x<d\end{cases} \tag{1}$$

where a, b, c, d are the interval critical values of the function. They are determined as follows:

(i) Assume that the value range of each CPC score is [0, 100], and collect experts' opinions: CPC score and CPC level for two different categories of CPC;

(ii) Based on the collected data, the method-fuzzy statistical experiment is used to determine the corresponding degree of membership for each CPC score;

(iii) Determine the values of a, b, c, and d by fitting the CPC score and the corresponding degree of membership.

The universes of a discourse of the fuzzy sets for each CPC which has four levels are [0, 30], [10, 60] [40, 90], and [70, 100], $[a,b,c,d]$=[40,60,70,90] as shown in Fig. 4(a)

and the universes of the discourse of the fuzzy sets for each CPC which has three levels are [0, 40], [10, 90] and [60, 100], [a,b,c,d]=[10,40,60,90] as shown in Fig. 4(b), which are obtained by taking logarithm operations based on the probability intervals in Table 3.

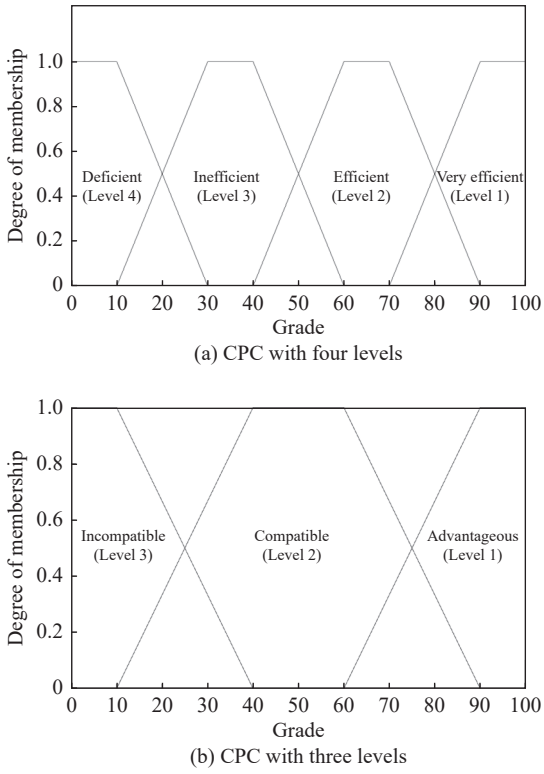


Fig. 4 CPC membership function

Once the fuzzification procedure is completed, the next step is to perform the defuzzification procedure to obtain the cognitive failure probability (CFP) after correction. Different from the traditional defuzzification procedure, the entire human factor reliability analysis in this paper is based on the CREAM method, the model gives the basic failure mode and the corresponding basic failure probability. In this defuzzification procedure, we only need to calculate the membership degree of each CPC through the membership function based on the actual score and use them to correct the basic failure probability of the cognitive function to obtain the failure probability in the actual environment. The operation steps are as follows:

The CPC1−CPC8 are scored according to the interaction scenarios, and the results S = [s_1, s_2,⋯, s_8] are brought into the corresponding membership function, which calculates different levels of membership respectively [a_i,b_i,c_i,d_i], i corresponds to the serial number of CPC. If CPC has only three levels, the membership of level 4 defaults to 0, and each CPC's all rank memberships sum to 1. Next, the failure effect factor for each CPC on the output of the four basic cognitive functions [Ocpc$_i$, Icpc$_i$, Pcpc$_i$, Ecpc$_i$] is calculated. The formula is as follows:

if $i \in [1,8]$,

$$\begin{cases} O\text{cpc}_i = a_i \cdot O_{i1} + b_i \cdot O_{i2} + c_i \cdot O_{i3} + d_i \cdot O_{i4} \\ I\text{cpc}_i = a_i \cdot I_{i1} + b_i \cdot I_{i2} + c_i \cdot I_{i3} + d_i \cdot I_{i4} \\ P\text{cpc}_i = a_i \cdot P_{i1} + b_i \cdot P_{i2} + c_i \cdot P_{i3} + d_i \cdot P_{i4} \\ E\text{cpc}_i = a_i \cdot E_{i1} + b_i \cdot E_{i2} + c_i \cdot E_{i3} + d_i \cdot E_{i4} \end{cases}, \tag{2}$$

if $i = 9$,

$$\begin{cases} \text{Time} = \text{day} \\ O\text{cpc}_i = O_{i1}, I\text{cpc}_i = I_{i1}, P\text{cpc}_i = P_{i1}, E\text{cpc}_i = E_{i1} \\ \text{Time} = \text{night} \\ O\text{cpc}_i = O_{i2}, I\text{cpc}_i = I_{i2}, P\text{cpc}_i = P_{i2}, E\text{cpc}_i = E_{i2} \end{cases}, \tag{3}$$

where [O_{ij} , I_{ij} , P_{ij} , E_{ij}] is the basic value of weighting factors of cognitive function for each CPC on the four basic cognitive functions at levels 1−4, i corresponds to the serial number of CPC, j corresponds to the different levels. Once the failure effect factors for CPC are calculated, the total factors for the failure effect of all CPC on cognitive function [OCPC, ICPC, PCPC, ECPC] can be calculated. The formula is as follows:

$$\begin{cases} \text{OCPC} = \prod_{i=1}^{i=9} O\text{cpc}_i \text{ICPC} = \prod_{i=1}^{i=9} I\text{cpc}_i \\ \text{PCPC} = \prod_{i=1}^{i=9} P\text{cpc}_i \text{ECPC} = \prod_{i=1}^{i=9} E\text{cpc}_i \end{cases}. \tag{4}$$

Finally, the CFP is corrected. If the basic failure probability for the four cognitive functions is [Ocfp, Icfp, Pcfp, Ecfp], then the failure probability value after correction is [OCFP, ICFP, PCFP, ECFP].

3.2.2 UCA probability calculation and evaluation of control mode

Once the correction is complete, the quantitative evaluation needs to be performed. This paper uses Bayesian network, a tool that can be used to directly calculate based on the analysis results of STPA and UPPAAL [17,29] with higher analytical efficiency and greater accuracy, to implement automated calculations. It is implemented as follows:

Firstly, the basic cognitive function failure patterns involved in the human error causation path retrieved by UPPAAL are transformed into root nodes and the UCA is transformed into a leaf node.

Secondly, these nodes are connected according to the structure of the causal path of the UCA, configure the conditional probability distribution table of each node connection, and get the Bayesian model of UCA, which is used to calculate.

Finally, the failure probability of cognitive function is injected into the root node as a priori probability, and the probability of occurrence of UCA can be subsequently calculated automatically.

Once the calculation is complete, the pilot's current state control mode can be evaluated based on the result of probability (P) according to these standard coming from the CREAM method [24], which has four levels, as follows:

(i) Strategic: $0.000\,05 < P < 0.01$.

When the control mode is in a strategic control mode, pilots have enough time to observe and analyze changes in the situation, and they can observe higher-level tasks and goals in advance. Their cognition and behavior are affected less by the current situational environment. The current HCI design is better and has reached the established requirements.

(ii) Tactical: $0.001 < P < 1.0$

When the control mode is in a tactical control mode, pilots' cognitive or behavioral activities are carried out along the plan, which is greatly affected by the procedures or rules. The current HCI design is acceptable and can be further improved.

(iii) Opportunistic: $0.01 < P < 0.5$

When the control mode is in opportunistic control mode, the system can provide pilots with limited time and space for judgment or dealing. The reason may be that pilots do not fully understand or misunderstand the current situation. The scene is too chaotic, and the pilot mainly relies on their perception or experience of the current situation to take further actions. The current HCI design is poor and needs to be modified.

(iv) Scrambled: $0.1 < P < 1.0$

When the control mode is in scrambled control mode, pilots' ability to think and judge their cognitive behavior is lost and repeats activity purposelessly "try after fail". The current HCI design is not very poor and needs to be redesigned.

Therefore, before the evaluation, it is necessary to use fuzzy mathematical methods to process the calculated UCA probability to resolve the uncertainty. Similarly, the membership function of the control mode is obtained by taking logarithm operations based on the probability intervals above, as shown in Fig. 5.

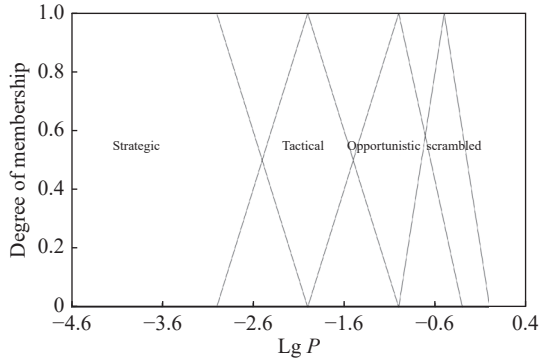


Fig. 5 Control mode and membership functions

4. Case study

4.1 HUD-HCI tasks identification and decomposition

Based on the analysis of a HUD manual and flight manual, the interaction scenarios during the approach using the HUD are obtained. The scenarios consist of two main parts: HUD calibration and data input before approach, and flight parameter observation and monitoring during the approach, with 47 steps in total. Under these scenarios, only the standard interaction process is considered, and it is assumed that the 47 steps of flight parameter observation and monitoring during the approach are sequentially conducted. After combination, 20 subtasks are obtained, including 11 pre-approaches and nine mid-approaches. This paper takes the 11 interactive subtasks before the HUD approach as the object of analysis, and the task decomposition results are shown in Table 4. The "*" indicates the basic cogntive function which each cognitive activity can be decomposed into.

Table 4 Decomposition result of interactive task

Number	Cognitive activity	Basic cognitive function			
		Observe	Interpretation	Planning	Execution
1	Operate HCU				*
2	Calibrate HCU				*
3	Input runway				*
4	Confirm runway	*			
5	Input altitude				*
6	Confirm altitude	*			
7	Input glide angle				*
8	Confirm glide angle	*			

Continued

Number	Cognitive activity	Basic cognitive function			
		Observe	Interpretation	Planning	Execution
9	Input display mode				*
10	Confirm display mode	*			
11	Decide		*		

4.2 HUD-HCI STPA-CREAM modeling

The pre-approach HUD safety control structure is defined according to HUD application scenarios and HUD system technical documentation, as shown in Fig. 6.

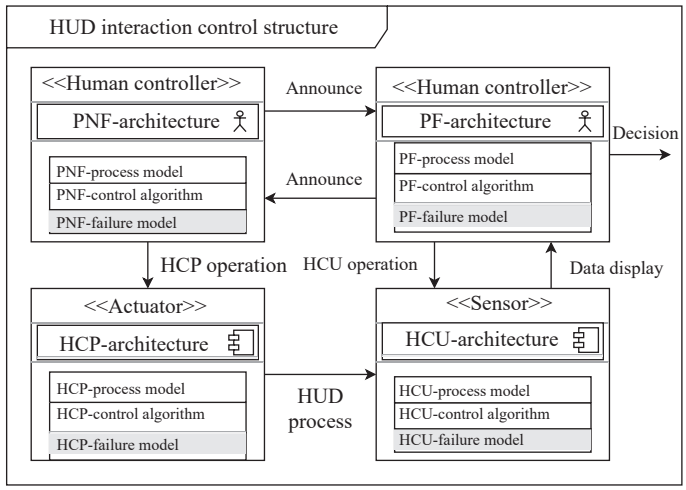


Fig. 6 HUD hierarchical safety control structure

It consists of four parts:

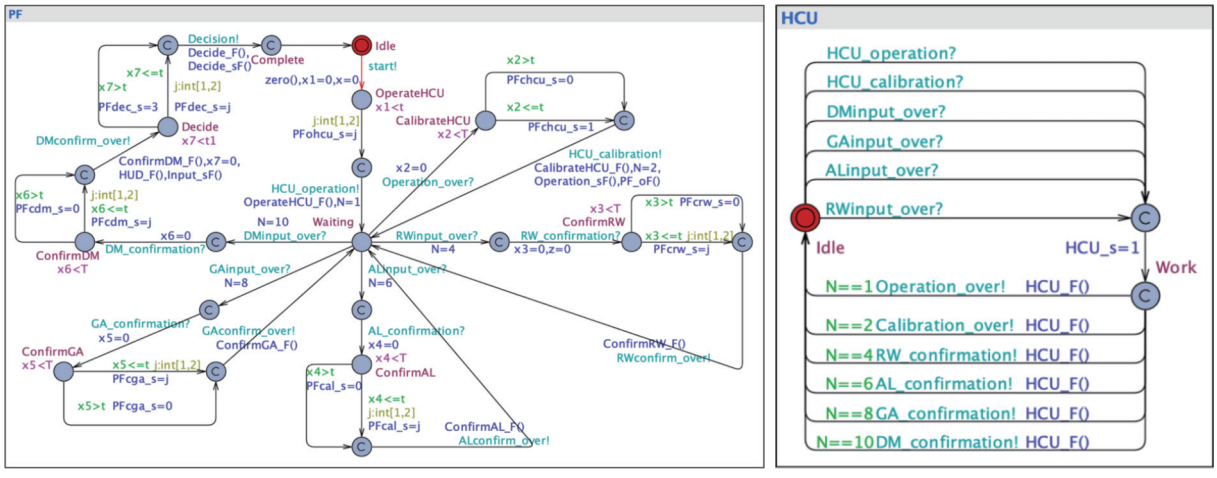
(i) Artificial controllers: pilot not flying (PNF);

(ii) Actuators: HUD control panel (HCP);

(iii) Sensors: HUD combiner unit (HCU);

(iv) Artificial controllers: pilot flying (PF).

The PF lays down the HCU and calibrates it. Once the calibration is complete, the PNF will receive the relevant data, and the HCP sends commands to the other HUD components. Then, the data will be projected to HCU to display flight and guidance information for PF, and PF will make the decision after confirmation. The corresponding UPPAAL model is built based on the safety control structure of the HCI and the detailed interaction process for the validation of the relevant properties, as shown in Fig. 7, and the variable meanings are shown in Table 5.



(a) PF (b) HCU

Fig. 7 UPPAAL failure expansion model of HUD system

Table 5 Meaning of UPAAL variables

Variable	Meaning
HCP_s	Status of HCP
HCU_s	Status of HCU
operation_s	Output status of operating
input_s	Output status of inputting and confirming
decide_s	Output status of deciding
PFohcu_s	Status of putting down HCU
PFchcu_s	Status of calibrating HCU
PNFirw_s	Status of inputting runway
PFcrw_s	Status of confirming runway
PNFial_s	Status of inputting altitude
PFcal_s	Status of confirming altitude
PNFiga_s	Status of inputting glide angle
PFcga_s	Status of confirming glide angle
PNFidm_s	Status of inputting display mode
PFcdm_s	Status of confirming display mode
PFdec_s	Status of deciding

In the UPPAAL model, the temporal order of the operational steps in the interaction process is indicated by using the position shifting and the changes of shaping variable N. At the same time, the component state variables are differentiated by using clock variables to inject the component's failure information. t represents the maximum time limit of the component's task execution. When the clock variable is less than or equal to t, the task is considered to be in the executed state which includes two kinds: correct execution and incorrect execution; when the clock variable is greater than t, the task is considered to be unexecuted. After modeling is complete, the correctness of the interaction model is analyzed, both logically and temporally, to confirm that the model satisfies the defined functional properties. The model satisfies all functional property requirements as validated by UPPAAL.

4.3 HUD-HCI risk identification and verification

After the completeness of the modeling of HCI, the unsafe control behavior during the interaction process is identified and verified. "Using HUD to approach" is taken as the control behavior, and STPA is used to identify potential UCA, according to the STPA handbook, a control action can be unsafe in the following ways:

(i) Not providing the control action leading to a hazard.

(ii) Providing the control action leading to a hazard.

(iii) Providing a potentially safe control action but too early, too late, or in the wrong order.

(iv) The control action lasting too long or being stopped too soon.

After the completion of UCA identification, safety and human factor reliability experts are invited to review the identification results.

Four potential UCA during HUD interactions are identified through STPA, are shown in Table 6. Next, in order to further verify the presence of UCAs, the UCAs will be described by using the BNF syntax, and formalized verification through UPPAAL is performed.

Table 6 UCA

Type	UCA description
Not providing causes hazard	(UCA-1) When the HUD system is operating normally, the pilot decides not to use the HUD for the approach
Providing causes hazard	(UCA-2) When the HUD system is not operating normally, the pilot decides to use the HUD for the approach
Too early, too late, out of order	(UCA-3) When the HUD system is operating normally, the pilot decides to use the HUD for the approach too late (UCA-4) When the HUD system is not operating normally, the pilot decides not to use the HUD for the approach too late
Stop too soon, applied too long	N/A

4.4 Causal path search

The UPPAAL-based path algorithm "PathSet" is used to retrieve the human error-induced paths that lead to unsafe control behaviors, which are shown in Fig. 8.

The algorithm principle is as follows: after each simulation of the system, the note command will be triggered. After receiving the command, the PathSet will judge whether the current system state meets the retrieved safety property P. If yes, PathSet will enter the Compare location; otherwise, PathSet sends the noted command to return to the Idle position. After receiving the noted command, the system will re-simulate the operation.

The function Scompare( ) in the compare position is used to compare the current system state parameters with the existing human error induced paths. If they are different, PathSet enters the add position. On the contrary, it sends the noted command and returns to the Idle position. The function Mupdate( ) in Add position is used to update and record the latest human error induced paths. After the update is completed, PathSet enters the check position, which is responsible for determining the cycle number of comparison. After the loop ends, PathSet enters the over position, and the path retrieval ends.

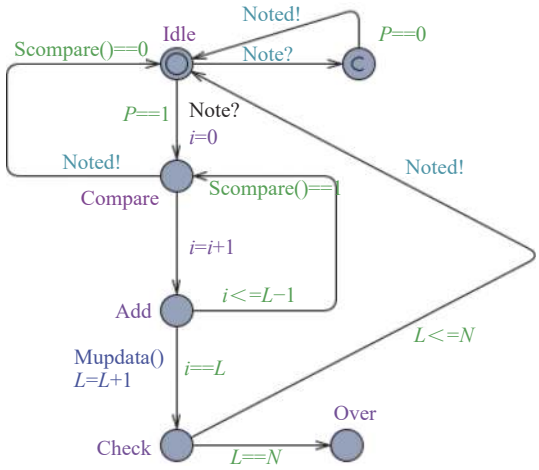


Fig. 8 UPPAAL-based path algorithm "PathSet"

In the verifier of UPPAAL, all paths satisfying the property P are retrieved through the BNF statement: "E< >P and PathSet. Over". Taking "UCA-2: HUD Approach by Pilot with HUD system not operating properly" as an example, there are three categories human error induced paths, the results are shown in Table 7, the meanings of other variables are shown in Table 5.

Table 7 Human error induced paths of UCA 2

Category	HCP_s and HCU_s	operation_s	Input_s	Decide_s
01	Correctly executed	Incorrectly executed	Correctly executed	Incorrectly executed
02	Correctly executed	Incorrectly executed	Incorrectly executed	Incorrectly executed
03	Correctly executed	Correctly executed	Incorrectly executed	Incorrectly executed

For the above three causal paths, the further analysis of "PF operation=incorrectly executed" and "PNF and PF input and confirmation= incorrectly executed" is performed.

For "PF operation=incorrectly executed", there are three cases, as shown in Table 8. For "PNF and PF input and confirmation= incorrectly executed", there are eight cases, as shown in Table 9. The meanings of variables are shown in Table 5.

Table 8 "PF operation=incorrectly executed" analysis results

Case	PF put down HCU (PFohcu_s)	PF calibrate HCU (PFchcu_s)
01	Correctly executed	Not executed
02	Incorrectly executed	Correctly executed
03	Incorrectly executed	Not executed

Table 9 "PNF and PF input and confirmation= incorrectly executed" analysis results

Case	PNFirw_s and PFcrw_s	PNFial_s and PFcal_s	PNFiga_s and PFcga_s	PNFidm_s and PFcdm_s
01	Not executed	Not executed/correctly executed/incorrectly executed	Not executed/correctly executed/incorrectly executed	Not executed/correctly executed/incorrectly executed
02	Incorrectly executed	Not executed/correctly executed/incorrectly executed	Not executed/correctly executed/incorrectly executed	Not executed/correctly executed/incorrectly executed
03	Not executed/correctly executed/incorrectly executed	Not executed	Not executed/correctly executed/incorrectly executed	Not executed/correctly executed/incorrectly executed
04	Not executed/correctly executed/incorrectly executed	Incorrectly executed	Not executed/correctly executed/incorrectly executed	Not executed/correctly executed/incorrectly executed
05	Not executed/correctly executed/incorrectly executed	Not executed/correctly executed/incorrectly executed	Incorrectly executed	Not executed/correctly executed/incorrectly executed
06	Not executed/correctly executed/incorrectly executed	Not executed/correctly executed/incorrectly executed	Not executed	Not executed/correctly executed/incorrectly executed
07	Not executed/correctly executed/incorrectly executed	Not executed/correctly executed/incorrectly executed	Not executed/correctly executed/incorrectly executed	Incorrectly executed
08	Not executed/correctly executed/incorrectly executed	Not executed/correctly executed/incorrectly executed	Not executed/correctly executed/incorrectly executed	Not executed

In summary, the causative scenarios that lead to the occurrence of UCA-2 have 35 cases under three major categories.

4.5 HUD-HCI STPA-CREAM quantitative analysis

Four different levels of interaction scenarios (worse/poor/fair/better) are selected, where CPC 1−CPC 8 are rated 40/60/80/90 respectively, and CPC9 defaults to night. The total factors of CPC's failure impact on basic cognitive function are calculated respectively at different interaction levels, and the failure probability of PNF and PF is modified, the results are shown in Table 10. Also, they are converted to the corresponding Bayesian network model based on the analysis results of UCA-2 under Subsection 4.4, as shown in Fig. 9.

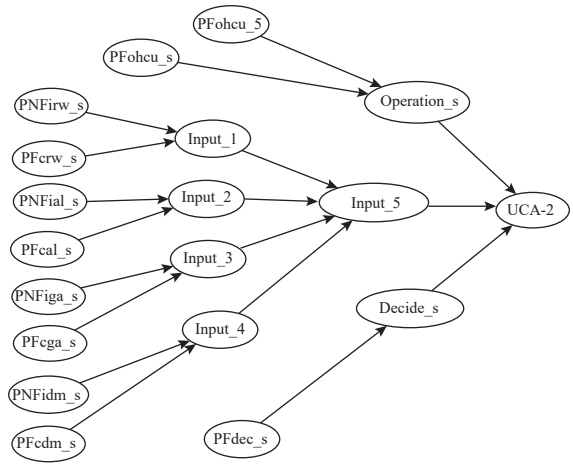


Fig. 9 Bayesian network model of UCA-2

The relationship between Table 10 and Table 7−Table 9 is as follows:

(i) E_FMEA_1 or O_FMEA_1 of each cognitive activity in Table 10 is the failure mode of "the correspon ding cognitive activity=incorrectly executed" in Table 8 and Table 9;

(ii) E_FMEA_4 or O_FMEA_3 of each cognitive activity in Table 10 is the failure mode of "the corresponding cognitive activity= not executed" in Table 8 and Table 9;

(iii) I_FMEA_2 and I_FMEA_3 of each cognitive activity in Table 10 is the failure mode of "PF decision = incorrectly executed" in Table 7.

Table 10 Probability of revision of PNF and PF

Role	Cognitive activity	Failure mode	Basic human error probability	Corrected failure probability with different CPC (1−8) initial scores			
				40	60	80	90
PNF	Input runway	E_FMEA_1	3.0E−3	4.32E−3	3.6E−3	7.908E−4	1.8432E−4
		E_FMEA_4	3.0E−2	4.32E−2	3.6E−2	7.908E−3	1.8432E−3
	Input altitude	E_FMEA_1	3.0E−3	4.32E−3	3.6E−3	7.908E−4	1.8432E−4
		E_FMEA_4	3.0E−2	4.32E−2	3.6E−2	7.908E−3	1.8432E−3
	Input glide angle	E_FMEA_1	3.0E−3	4.32E−3	3.6E−3	7.908E−4	1.8432E−4
		E_FMEA_4	3.0E−2	4.32E−2	3.6E−2	7.908E−3	1.8432E−3
	Input display mode	E_FMEA_1	3.0E−3	4.32E−3	3.6E−3	7.908E−4	1.8432E−4
		E_FMEA_4	3.0E−2	4.32E−2	3.6E−2	7.908E−3	1.8432E−3
PF	Operate HCU	E_FMEA_1	3.0E−3	4.32E−3	3.6E−3	7.908E−4	1.8432E−4
	Calibration HCU	E_FMEA_4	3.0E−2	4.32E−2	3.6E−2	7.908E−3	1.8432E−3
	Confirm runway	O_FMEA_1	1.0E−3	1.2E−3	1.2E−3	2.929E−4	0.768E−4
		O_FMEA_3	7.0E−2	8.4E−2	8.4E−2	2.0503E−2	5.376E−3
	Confirm altitude	O_FMEA_1	1.0E−3	1.2E−3	1.2E−3	2.929E−4	0.768E−4
		O_FMEA_3	7.0E−2	8.4E−2	8.4E−2	2.0503E−2	5.376E−3
	Confirm glide angle	O_FMEA_1	1.0E−3	1.2E−3	1.2E−3	2.929E−4	0.768E−4
		O_FMEA_3	7.0E−2	8.4E−2	8.4E−2	2.0503E−2	5.376E−3
	Confirm display mode	O_FMEA_1	1.0E−3	1.2E−3	1.2E−3	2.929E−4	0.768E−4
		O_FMEA_3	7.0E−2	8.4E−2	8.4E−2	2.0503E−2	5.376E−3
	Decide	I_FMEA_2	1.0E−2	1.2E−2	1.2E−2	3.467E−3	1.2E−3
		I_FMEA_3	1.0E−2	1.2E−2	1.2E−2	3.467E−3	1.2E−3

Assigning the corrected probability in Table 10 to the root nodes in the BN model in Fig. 10, the occurrence probability of UCA-2 in this scenario can be calculated by using the Bayesian Network and the control state of the pilot UCA-2 in this scenario can be obtained, as shown in Table 11.

Table 11 STPA-CREAM result of UCA-2

%

CPC grade	Probability of UCA-2	Control mode			
		Strategic	Tactical	Opportunistic	Scrambled
40	0.072 372 704	0	14	86	0
60	0.062 440 184	0	20	80	0
80	0.012 772 005	0	89	11	0
90	0.003 264 311	49	51	0	0

According to the above results, it can be concluded that the control mode is predominantly opportunistic at both the initial score of 40 and 60. In this scenario, the HUD system can provide the pilot with limited time and margin for judgment and operation, thus the pilots can only react and respond through the perception of the current environment or experience. The interaction process is inadequate, so HCI errors are prone to occur, and further development of the HCI design is needed. When the initial score is 80, the pilot's control mode is mainly strategic, and the pilot's cognition or behavior in this scenario is conducted according to the plan, where the pilot is less affected by the environment and the level of interaction is average. When the initial score is 90, the control mode is roughly half strategic and half tactical, and under this scenario, the pilot will have enough time to observe and analyze changing situation and be able to observe higher-level tasks and objectives in advance, with a good level of interaction and less susceptibility to human factors errors.

4.6 Result analysis

By analyzing the sensitivity of CPC in the HUD HCI process, the weak links in the process can be identified and measures and recommendations can be subsequently put forward for their improvement. Fig. 10 shows a schematic representation of the sensitivity of CPC1-CPC8 under four different levels of interaction scenarios. The analysis reveals that as the level of interaction scenario increases, i.e., the initial CPC-8 score, the probability of UCA-2 occurrence gradually decreases, the pilot's UCA-2 control state shows an overall tendency to improve, shifting from opportunistic to strategic and tactical with the trend from chaos to uniformity.

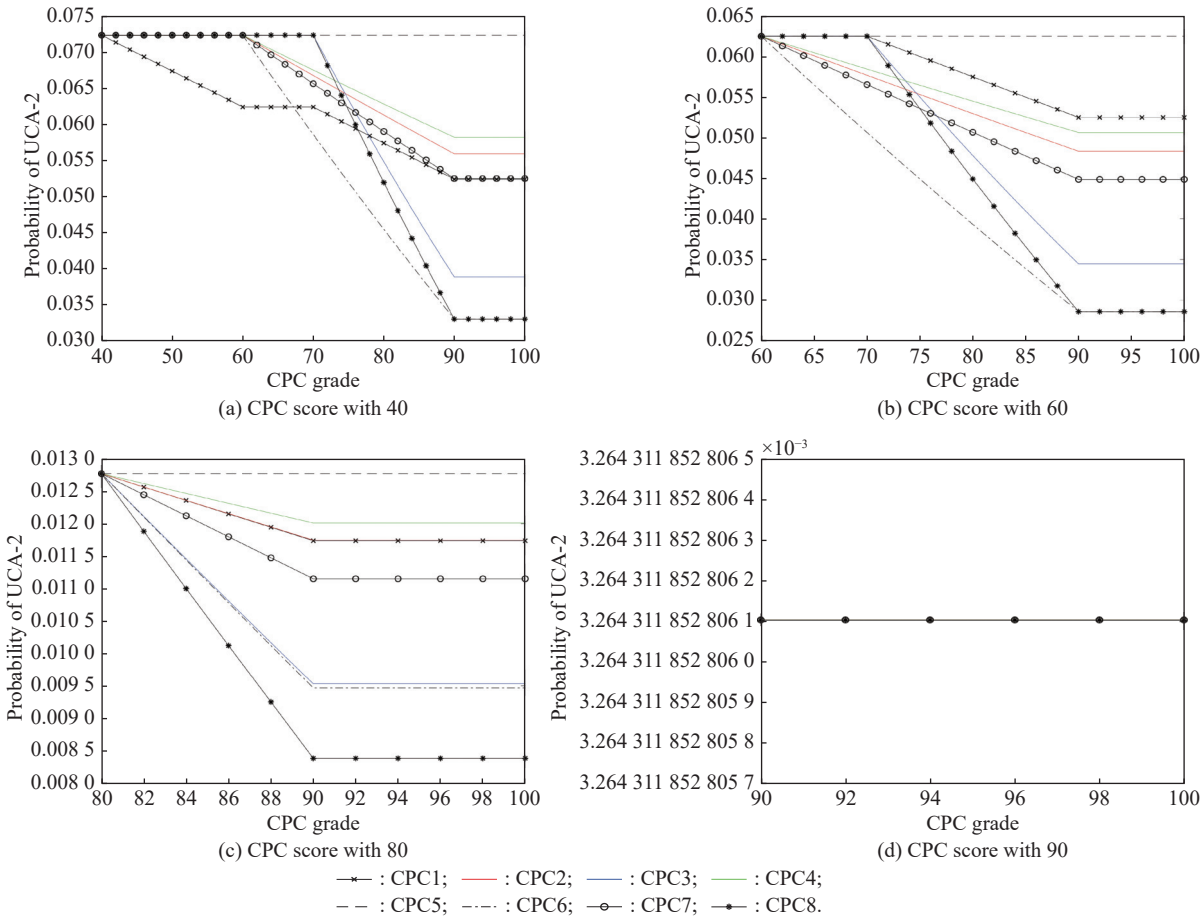


Fig. 10 Change in the probability of UCA-2 occurrence with different CPC score

The comparative analysis results are as follows:

(i) When the initial scores of CPC are all 40, the degree of the CPC impact is CPC6>CPC8>CPC3>CPC7>CPC1>CPC2>CPC4>CPC5. In this case, improving CPC6 (time sufficiency) is the most effective way.

(ii) When the initial scores of CPC8 are all 60, the degree of the CPC impact is CPC8>CPC3>CPC6>CPC7>CPC2>CPC4>CPC1>CPC5. In this case, improving CPC8 (the cooperation quality of crew members) is the most effective way.

(iii) When the initial scores of CPC are all 80, the CPC impact degree is CPC8>CPC6>CPC3>CPC7>CPC2= CPC1>CPC4>CPC5. In this case, improving CPC8 (the cooperation quality of crew members) is the most effective way.

(iv) When the initial CPC scores are all 90, raising the CPC again essentially does not affect human factors errors.

In conclusion, the CPC8 (quality of crew member cooperation) and CPC6 (time sufficiency) of CPC present the biggest impact. Therefore, improving the rapport between pilots, such as increasing the frequency of communication among crew members, developing a consistent form of communication, enhancing the trust and cooperation between pilots and co-pilots, as well as increasing the execution time of each interactive task can effectively reduce the occurrence of UCA-2 and improve HUD HCI process.

5. Conclusions

Considering the high safety of the avionics system and the safety assessment standard SAE ARP 4761, this paper combines STPA and CREAM to create a detailed interaction model for safety analysis of HCI in the airborne system.

Similar with CREAM for HRA [20], this paper adopts fuzzy multiple attributive group decision-making method and Bayesian networks and evidential reasoning to enhance the reliability of human error quantification. However, the difference is that STPA-CREAM describes the HCI process through a hierarchical security control structure, not an operation chain. This avoids excessive simplification of the model and makes it closer to the actual scene. At the same time, through the safety control structure, the influence of multi-party interaction on HRA can be fully considered, and more cause scenarios can be identified.

Compared with STPA for HCI [30], both of them use the safety control structure to identify the UCA in the HCI and analyze the corresponding cause scenario, and then the difference is that STPA-CREAM improves the description of the human failure model by introducing CPC. At the same time, the membership function is used to fuzzify the human factor reliability data, thereby generating the fuzzy perception of multiple inputs, and dealing with the human uncertainty during HCI.

Compared with recent research for HCI in aircraft [31], this research is based on adaptive control of though-rational (ACT-R) theory and Bayesian network to model the pilot perception model and simulates situational awareness through Simulink to discuss the mechanism of accident evolution along with possible preventive measures. However, this article uses STPA and CREAM to establish a pilot man-made failure model. Then use the formal verification UPPAAL to automate the qualitative analysis of the HCI process and identify the UCA in the process. Finally, a Bayesian model is performed on each UCA. Quantitative analysis and simulation are used to find suitable mitigation measures. Through comparison, it is found that the former research is superior to this article in simulation, but the analysis of human factors is not included in the overall aircraft system safety assessment system. This article is based on the safety assessment standard SAE ARP 4761 to analyze HCI in complex avionics systems, the human factor reliability data from CREAM is the data accumulated through the development of the three generations of HRA and has a certain degree of confidence. At the same time, the latest model-based safety analysis method —formal verification is introduced, which improves the analysis efficiency and reduces the influence of subjective factors on the analysis process.

The chief research conclusions can be summed up below:

(i) A formalized safety analysis framework based on the STPA-CREAM method is proposed for the problem of HCI in airborne systems.

(ii) Based on the CREAM method and fuzzification, a model of common performance conditions and human caused failure probability correction is developed for the airborne interaction environment. It can identify the hazard of HCI process, carry out quantitative analysis, judge whether it is in a safe state, and then identify the weak links in the interaction scenario, and give the modification suggestions.

(iii) Taking the head-up display system HCI as an example, four potential unsafe control behaviors are identified for the control behavior “using the HUD to approach”, and through the formalized verification of STPA, it is found that all four unsafe control behaviors exist.

(iv) Using the example of “UCA-2: HUD approach by pilot in case of HUD system malfunction”, detailed analyses reveal that as the level of the interaction scenario increases (increment of CPC score), the control state of UCA-2 gradually shifts from opportunistic to strategic and tactical, with the trend from chaos to uniformity.

(v) Developing a consistent form of communication, enhancing the trust and cooperation between pilots and co-pilots, as well as increasing the execution time of each interactive task can effectively reduce the occurrence of UCA-2 and improve the level of HUD HCI.

References

[1] SINGH S, KUMAR R, KUMAR U. Modelling factors affecting human operator failure probability in railway maintenance tasks: an ISM-based analysis. International Journal of System Assurance Engineering and Management, 2015, 6(2): 129–138.

[2] ZHANG F K, DONG H Y. Research on formal modeling and safety analysis method of head-up display system for civil aircraft based on AltaRica. Proc. of the 3rd International Conference on Circuits, System and Simulation, 2019. DOI: 10.1109/CIRSYSSIM.2019.8935566.

[3] WATKINS C B, NILSON C, TAYLOR S, et al. Development of touchscreen displays for the gulfstream g500 and g600 symmctry™ flight deck. Proc. of the IEEE/AIAA 37th Digital Avionics Systems Conference, 2018. DOI: 10.1109/DASC.2018.8569532.

[4] MENZENSKI J. Enhancing cognitive assistants with low-cost computer vision. Proc. of the IEEE/AIAA 37th Digital Avionics Systems Conference, 2018. DOI: 10.1109/DASC/DASC.2018.8569224.

[5] CARROLL M, REBENSKY S, WILT D, et al. Integrating uncertified information from the electronic flight bag into the aircraft panel: impacts on pilot response. International Journal of Human-Computer Interaction, 2020, 37(7): 1–12.

[6] YANG H Y, SUN Y C, LI L B, et al. Safety analysis of integrated modular avionics system based on FTGPN method. International Journal of Aerospace Engineering, 2020, 2020: 8811565.

[7] PENG Q B, ZHANG H L. Model-based requirements analysis method for manned space engineering. Systems Engineering and Electronics, 2023, 45(11): 3532–3543. (in Chinese)

[8] SHARVIA S, PAPADOPOULOS Y. Integrating model checking with HiP-HOPS in model-based safety analysis. Reliability Engineering System Safety, 2015, 135: 64–80.

[9] LIU X F, AN S Q. Failure propagation analysis of aircraft engine systems based on complex network. Procedia Engineering, 2014, 80: 506−521.

[10] DONG H Y, CAO Z Y, ZHAI Z J, et al. Availability assessment of avionics display system based on MBSA using fault dependent matrix. IOP Conference Series: Materials Science and Engineering, 2020, 751: 012076.

[11] HAN S, WANG T F, CHEN J Q, et al. Towards the human–machine interaction: strategies, design, and human reliability assessment of crews' response to daily cargo ship navigation tasks. Sustainability, 2021, 13(15): 8173–8190.

[12] THOMAS P R. Performance, characteristics, and error rates of cursor control devices for aircraft cockpit interaction. International Journal of Human-Computer Studies, 2018, 109: 41–53.

[13] LEVESON N. Engineering a safer world: systems thinking applied to safety. Cambridge: MIT Press, 2011.

[14] LI Y H, GAO Y. Safety analysis for civil aircraft system based on STPA-ANP mode. Systems Engineering and Electronics, 2022, 44(9): 2986–2994. (in Chinese)

[15] HU J B, LEI Z, XU S K. Safety analysis of wheel brake system based on STAMP/STPA and Monte Carlo simulation. Journal of Systems Engineering and Electronics, 2018, 29(6): 1327–1339.

[16] CASTILHO D S, URBINA L, ANDRADE D D. STPA for continuous controls: a flight testing study of aircraft cross-wind takeoffs. Safety Science, 2018, 108: 129–139.

[17] ZHAO C X, LI H, DONG L. Safety analysis and evaluation of airborne HUD system based on STPA-bayes model. Systems Engineering and Electronics 2020, 42(5): 1083–1092.

[18] PAN X, WANG H X, LIN Y, et al. HEP quantification strategy based on modified CREAM. Journal of Systems Engineering and Electronics, 2019, 30(4): 815–822.

[19] AKYUZ E, CELIK M. Application of CREAM human reliability model to cargo loading process of LPG tankers. Journal of Loss Prevention in the Process Industries, 2015, 34: 39–48.

[20] AHN S I, KURT R E. Application of a CREAM based framework to assess human reliability in emergency response to engine room fires on ships. Ocean Engineering, 2020, 216: 108078.

[21] ZHOU Q, WONG Y D, HUI S L, et al. A fuzzy and Bayesian network CREAM model for human reliability analysis–the case of tanker shipping. Safety Science, 2018, 105: 149–157.

[22] ZHANG S, HE W P, CHEN D K, et al. A dynamic human reliability assessment approach for manned submersibles using PMV-CREAM. International Journal of Naval Architecture and Ocean Engineering, 2019, 11(2): 782–795.

[23] XI Z, MATTHEW L B, CHRISTOPHERR D, et al. The development of a next-generation human reliability analysis: systems analysis for formal pharmaceutical human reliability. Reliability Engineering & System Safety, 2020, 202: 106327.

[24] LI H. Research on safety analysis method of airborne display system based on the STAMP theory. Tianjin: Civil Aviation University of China, 2020. (in Chinese)

[25] BAUMGART S, FROBERG J, PUNNEKKAT S. A state-based extension to STPA for safety-critical system-of-systems. Proc. of the 4th International Conference on System Reliability and Safety, 2019: 246−254.

[26] HOLLNAGEL E. Cognitive reliability and error analysis method. Oxford: Elsevier Science Ltd, 1998.

[27] LIU J C, DONG L, ZHAO C X, et al. Simulation and verification of DIMA dynamic reconfiguration based on formal method. Systems Engineering and Electronics, 2022, 44(4): 1282–1290. (in Chinese)

[28] JIANG Q, ZHU C L, WANG S Q. Qualitative analysis for state/event fault trees using formal model checking. Journal of Systems Engineering and Electronics, 2019, 30(5): 959–973.

[29] DAVID A, LARSEN K G, LEGAY A, et al. UPPAAL SMC tutorial. International Journal on Software Tools for Technology Transfer, 2015, 17: 397–415.

[30] SUN M S, SANG H L, SEUNG S K, et al. STPA-based hazard and importance analysis on NPP safety I&C systems focusing on human–system. Reliability Engineering and System Safety, 2021, 213: 107698.

[31] ZHANG X, SUN Y C, ZHANG Y J, et al. Multi-agent modelling and situational awareness analysis of human-computer interaction in the aircraft cockpit: a case study. Simulation Modelling Practice and Theory, 2021, 111: 102355.

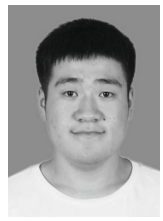
Biographies

ZHAO Changxiao was born in 1989. He received his Ph.D. degree from Behang University, Beijing, China, in 2013. He is currently an associate professor in Civil Aviation university of China. His research interests are safety assessment of the integrated modular avionics.

E-mail: cxzhao@cauc.edu.cn

LI Hao was born in 1995. He received his M.S. degree from Civil Aviation University of China, Tianjin, China, in 2020. He is working in Shenzhen Dajiang Innovation Technology Co., Ltd. His research interests are risk identification of the human-computer interaction and safety analysis.
E-mail: damienleeh@foxmail.com

ZHANG Wei was born in 1998. He received his M.S. degree from Civil Aviation University of China, Tianjin, China, in 2023. His research interest is safety assessment of the integrated modular avionics.
E-mail: wzhang_7154@163.com



DAI Jun was born in 1999. He received his B.E. degree from Civil Aviation University of China, Tianjin, China, in 2021. He is currently pursuing his Ph.D. degree in Civil Aviation University of China. His research interest is airborne network safety assessment.
E-mail: 171542305@cauc.edu.cn

DONG Lei was born in 1983. He received his Ph.D. degree from Behang University, Bejing, China, in 2013. He is currently an associate professor in Civil Aviation University of China. His research interest is airworthiness certification of the complex avionics.
E-mail: dlcauc@126.com