Research on safety modeling and analysis in information fusion system

Gang Xiao, Yanran Wang & Fang He

Aerospace Systems

ISSN 2523-3947

AS
DOI 10.1007/s42401-018-0011-2

Aerospace Systems
https://doi.org/10.1007/s42401-018-0011-2

ORIGINAL PAPER

Research on safety modeling and analysis in information fusion system

Gang Xiao[1] · Yanran Wang[1] · Fang He[1]

Received: 27 September 2018 / Revised: 31 October 2018 / Accepted: 13 November 2018

Abstract

Avionics system integration is a prominent trend in research and development of civil airplane. It can improve task effectiveness, function efficiency, and resource utilization of system. Information fusion, which includes function information fusion, processing information fusion, and sensor input fusion, is a core process of avionics system integration. Some researches about the impact of information fusion on system safety are done in avionics system which is shown as follows: (1) the concept of Mishap Dilution, Mishap Implication and Mishap Confusion (MD–MI–MC) is first defined in function information fusion of avionics system. (2) The model of multi-source MD–MI–MC is established based on hazard theory. (3) The function fusion of Automatic-Dependent Surveillance–Broadcast (ADS–B) and Traffic Collision Avoidance System (TCAS) is used as a typical example to analyze fusion system during the aircraft climbing or landing state. In this paper, the concept and model of multi-source MD–MI–MC are proposed for safety analysis of integrated avionics system. A fusion model with a variable sampling Variational Bayesian–Interacting Multiple Model (VSVB–IMM) algorithm is used to analyze. At last, a set of theory system and evaluation standards including the positive and negative earning analyses are built based on the presented MD–MI–MC theory and mechanism of integrated avionics.

Keywords System safety · Mishap dilution (MD) · Mishap implication (MI) · Mishap confusion (MC) · Information fusion

1 Introduction

With the advancement of science and technology, avionics system is developing towards complexity and integration. Avionics system integration [1] which is a system technology can improve task effectiveness, function efficiency, and resource utilization of system. Information fusion [2], which includes function information fusion, processing information fusion, and sensor input fusion, is a core process of avionics system integration.

For avionics system integration, the composition and structure of avionics system integration technology are described by Wang [3]. The impact of spatial and temporal integration choices on the communication performance is brought to light by Badache [4] to realize optimized system organization for avionics system integrating. The avionics software safety [5] is very important to warrant the safe operation of an avionics system. Many safety requirements are imposed by various standards and industrial regulations that must be met by the avionics software.

For information fusion, multisensor fusion and integration [6] is a rapidly evolving research area. The advantages gained through the use of redundant, complementary, or more timely information in a system can provide more reliable and accurate information. ADS–B [7] is known as the foundation of free flight by Federal Aviation Administration (FAA). TCAS [8] is airborne traffic alarm and collision avoidance system which is independent of air-traffic control on the ground. The fusion of ADS–B and TCAS data can improve the prediction accuracy of TCAS system [9], increase the rate of true alarm, and decrease the rate of false and missed alarm. There are many benefits in airspace alarm accuracy and flight safety by combining with TCAS II and ADS–B system.

However, when the integration of avionics system brings benefits, it will also lead to an increase in system complexity. The system failure in integrated avionics system may become dilution, implication, and confusion. Some researches focus

✉ Yanran Wang
yrwang501@sjtu.edu.cn

Gang Xiao
xiaogang@sjtu.edu.cn

Fang He
hefang@sjtu.edu.cn

[1] School of Aeronautics and Astronautics, Shanghai Jiao Tong University, 800 Dongchuan Road, Minhang District 200240, Shanghai, China

Published online: 21 November 2018

on safety analysis methods. Ding [10], who combines the advantages of support vector machine theory (SVM) and genetic algorithm (GA), proposes a smart fusion prediction method GASVM to evaluate the safety of the remaining life of the electronic device (RUL) prediction. Shen [11] introduced the systematic method of constructing security cases for the system through the Goal Structuring Notation (GSN), which opened up new research ideas for the certification of avionics systems.

In addition, for the safety design of the system, Xu Xianliang et al. [12] designed a security-centric IMA software architecture design theory, using the dangerous scene to evaluate the security of the IMA structure. From the perspective of airworthiness, the security issues of the IMA system were studied by CAI [13]. The shortcomings of traditional airworthiness certification and the main difficulties in integrating airworthiness certification of modular avionics are discussed. In addition, the problem between the authentication method and development practice is solved.

In this paper, the concept and model of multi-source MD–MI–MC are proposed for safety analysis of integrated avionics system. A fusion model with a VSVB–IMM algorithm is used to analyze. A theory system and evaluation standards are tested by real-engineering process of integrated surveillance avionics system. The positive and negative benefits of MD–MI–MC can be obtained quantitatively based on the presented integrated avionics theory and mechanism.

2 Theory of multi-source MD–MI–MC

2.1 Hazard theory

According to the definition of system security, a mishap is an event that actually causes property loss, injury, or death. Hazard is defined as the condition that may lead to property loss, injury, or death. From these definitions, hazards are the precursor of mishaps [14]. Hazards define mishaps. A mishap is an event that has already happened. That means that there is a direct link between hazard and mishap, as shown in Fig. 1.

Figure 1 shows that the hazards and mishaps are two independent states of the same phenomenon, and the two are connected through a state transition. These states can also be considered as prior and post-mortem states. The hazard is an event that may occur in one end of the state spectrum, and in the other end of the spectrum is an event that has actually occurred. A suitable metaphor is water, which has its own molecular formula, but can be liquid or solid, and the key to its conversion is temperature.

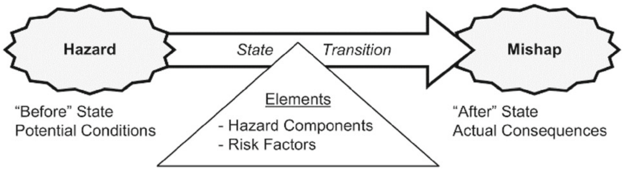

Fig. 1 Relationship between hazard and mishap

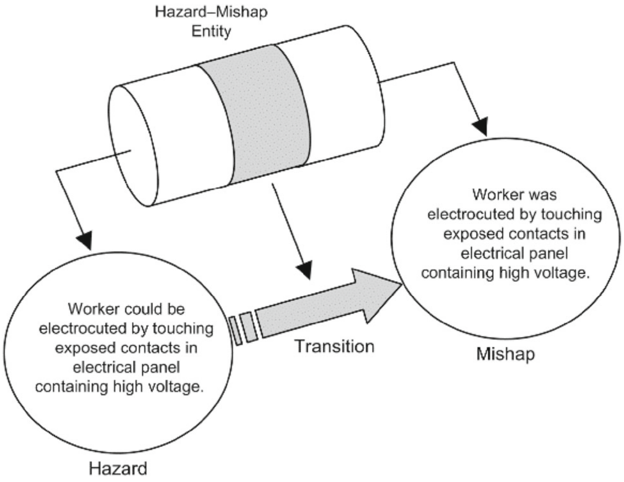
Hazard–Mishap
Entity
Worker was electrocuted by touching exposed contacts in electrical panel containing high voltage.
Worker could be electrocuted by touching exposed contacts in electrical panel containing high voltage.
Transition
Mishap
Hazard

Fig. 2 Different ends of the same entity

Figure 2 explains the relationship between hazards and mishaps in another way. In this sense, hazards and mishaps are opposite ends of the same entity. Some conversion events result in a transition from a hazard to a mishap, from a hypothetical to a real state.

The transition from a hazard to a mishap is based on two factors:

(1) Specific hazard components involved.
(2) Mishap risk represented by hazard components.

The hazard components are the items that constitutes the hazard, and the mishap risk is the probability of the mishap occurring and the severity of the loss caused by the mishaps.

Mishap risk is a straightforward concept, and the risk is usually defined as

$$\text{Risk} = \text{probability} \times \text{severity}. \tag{1}$$

The probability and severity of accidents can be analyzed both in qualitative and quantitative way. Time is introduced into the concept of danger as a factor in probability calculation. The definition of a hazard component is more complex. The hazards only include those elements that must be included, and are sufficient to make the mishap happen.

Hazards are usually composed of the following three basic components:

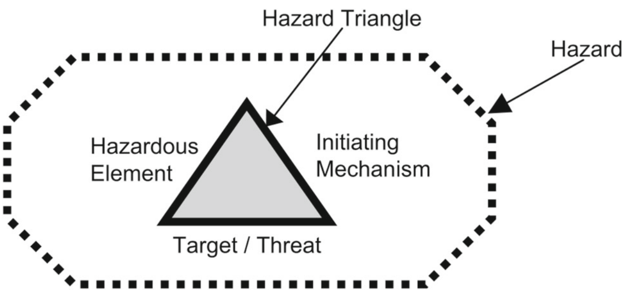

Fig. 3 Hazard triangle

(1) Hazardous element (HE). This is the basic resource that creates incentives for harm, such as the explosives used in the system.
(2) Initiating mechanism (IM). This is the trigger that causes the occurrence of the state transition.
(3) Target and threat (T/T). This part refers to the person or thing that is vulnerable, and describes the severity of the accident. It can also be understood as the consequences of the accident and the series of injuries and losses it anticipates.

For system security, the above three hazard components are known as hazard triangles which is shown in Fig. 3.

2.2 Modes and mechanisms of multi-source MD–MI–MC

2.2.1 Modes and mechanisms of MD

In the functional information fusion, MD leads to risk source composition and strength weakened. In addition, it also leads to the probability of safety accidents decreased.

The modes and mechanisms of MD are shown in Fig. 4. The small circles with color represent the harmful elements and trigger mechanisms and results, respectively. The area of the circle indicates the probability of its occurrence. Three phenomena of MD which are mishap not happen mishap not happen with the strength weakened and mishap happen, but the strength weakened is shown in Fig. 4.

Functional information fusion may lead to the hazardous element weakened and the triggering probability lower, so that the mishap will not occur or the seriousness of mishap is significantly reduced. The above process is called MD.

2.2.2 Modes and mechanisms of MI

The MI in the fusion of functional information results in the non-characterized or non-existent hazard sources. It can lead to the occurrence of a security incident, where the hazard cannot be found.

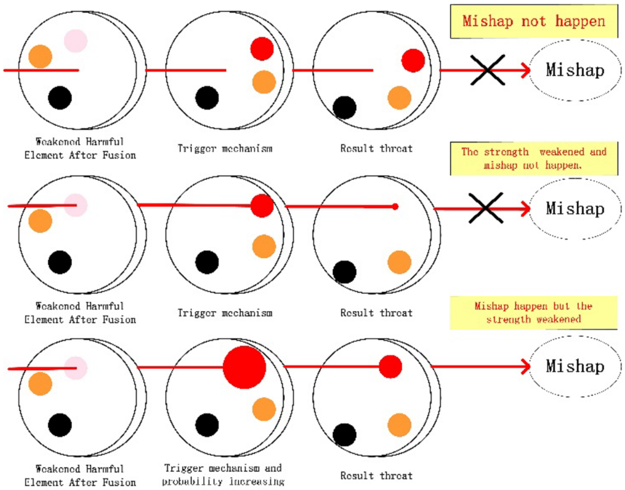
Mishap not happen
Mishap
Weakened Harmful Element After Fusion
Trigger mechanism
Result threat
The strength weakened and mishap not happen.
Mishap
Weakened Harmful Element After Fusion
Trigger mechanism
Result threat
Mishap happen but the strength weakened
Mishap
Weakened Harmful Element After Fusion
Trigger mechanism and probability increasing
Result threat

Fig. 4 Modes and mechanisms of MD

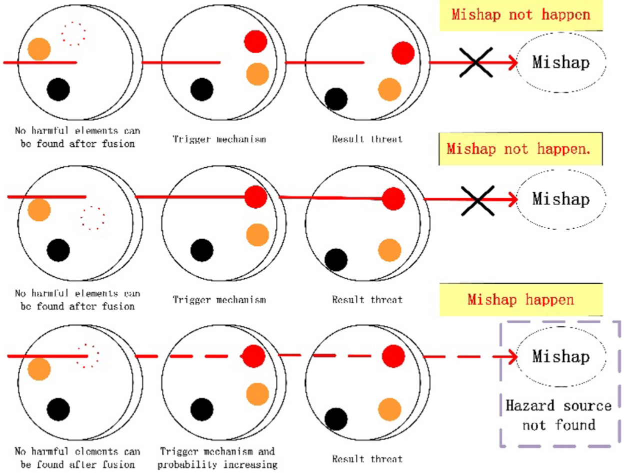
Mishap not happen
Mishap
No harmful elements can be found after fusion
Trigger mechanism
Result threat
Mishap not happen.
Mishap
No harmful elements can be found after fusion
Trigger mechanism
Result threat
Mishap happen
Mishap
Hazard source not found
No harmful elements can be found after fusion
Trigger mechanism and probability increasing
Result threat

Fig. 5 Modes and mechanisms of MI

The modes and mechanisms of MI are shown in Fig. 5. The small circles with color represent the harmful elements, trigger mechanisms, and results, respectively. The area of the circle indicates the probability of its occurrence. Three phenomena of MI which are mishap not happen with trigger mechanisms, mishap not happen without trigger mechanisms, and mishap happen, but hazard source not found is shown in Fig. 5.

2.2.3 Modes and mechanisms of MC

MC in functional information fusion causes random occurrence or disappearance of hazards. It leads to safety mishaps which are confused and uncertain, as shown in Fig. 6.

The modes and mechanisms of MC are shown in Fig. 6. The small circles with color represent the harmful elements, trigger mechanisms, and results, respectively. The area of the circle indicates the probability of its occurrence. Two phe-

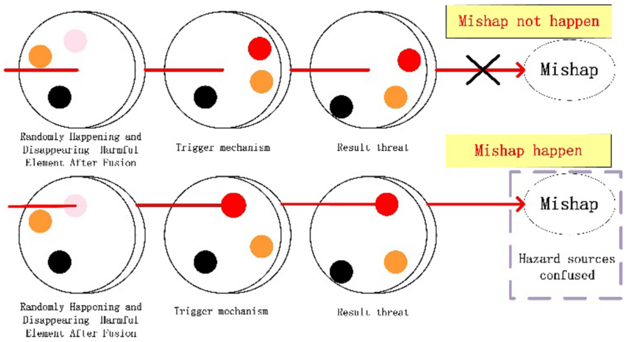
Mishap not happen
Mishap
Randomly Happening and Disappearing Harmful Element After Fusion
Trigger mechanism
Result threat
Mishap happen
Mishap
Hazard sources confused
Randomly Happening and Disappearing Harmful Element After Fusion
Trigger mechanism
Result threat

Fig. 6 Modes and mechanisms of MC

nomena of MC are mishap not happen and mishap happen, but hazard source confused is shown in Fig. 6.

2.3 Models of multi-source MD–MI–MC

When building a mathematical model, it is assumed that the following conditions are met:

(1) A mishap can be a source of danger, but the source of the danger is not just a mishap. Only consider the source of hazard, and do not consider human factors, environments, etc. (man–machine loop).
(2) The initiating mechanism is random and can be considered as a random variable. In this sense, a mishap caused by a hazard can be seen as a specific probability of a security incident.

In the model, the critical surface of mishap is described by a two-dimensional curve $G(X,Y)=0$, where:

(1) X which is the state parameter of the system may be multidimensional in practical problems. In mathematical model, it is simplified as a one-dimensional parameter. In addition, in this model, X can be understood as system-state instability. The larger X is, the higher the instability is, and the easier it is to trigger a security mishap.
(2) Y is the Initiating Mechanism. It is a random variable. It is also multidimensional in practical problems. There exists a probability density function $P(Y)$. It is simplified to 1 dimension in mathematical modeling, and in the simplified model, without loss of generality. We assume that the larger y, the more difficult the accident. Mathematically, it is expressed as a monotonically decreasing function, whose probability density function $P(Y)$ is Y.

$G(X,Y)$ is also called the mishap trigger decision function. As shown in Fig. 7, when $G(X,Y)>0$, there is a security accident, and when $G(X,Y)<0$, no security incident occurred.

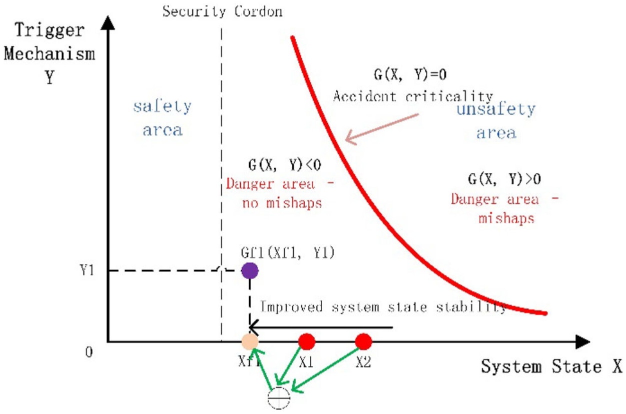

Fig. 7 Mishap triggering decision function

Function $G(X,Y)$ is the core of the model. It describes the relationship of hazard sources, triggering factors, and security events. The specific form of this function is determined by the specific physical problem. X, Y, and G are the three elements in the model of the mishap trigger decision function (corresponding to the hazard triangle).

In the avionics system, there are N independent sources of information that can be used independently (independently distributed) before functional information fusion. When the ith information source is used alone, it can be described according to the previous model system:

$$G_i(X_i, Y_i), i = 1 \ldots N. \tag{2}$$

The system function information can be defined as a mapping from ($X_1,\ldots X_N$; $Y_1,\ldots Y_N$; $G_1,\ldots,G_N$) to (X_f, Y_f, G_f):

$$\left(X_f, Y_f, G_f\right) = F(X_1, \ldots, X_N; Y_1, \ldots, Y_N; G_1, \ldots, G_N). \tag{3}$$

The model is a general model of functional information fusion for avionics systems.

2.3.1 MD model

After fusion $X_f \in D$, but $P\left(X_f\right) < P(X_i), i = 1, \ldots, N$. In other words, the integrated system state is still in the danger zone and the fault is characterized. However, the fusion reduces the probability of a mishap and this is MD. Because of the probability of mishap decreases, it is the positive benefit of MD. At the same time, faults can still be discovered and handled. The situation which the mishap implicit cannot be found will not happen. The mathematical model of MD is shown in Fig. 8.

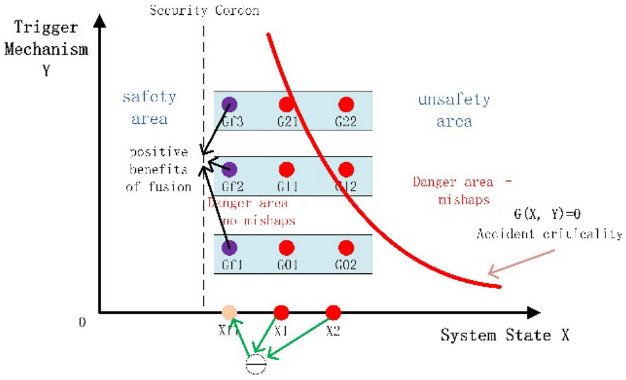

Fig. 8 Mathematical model of MD

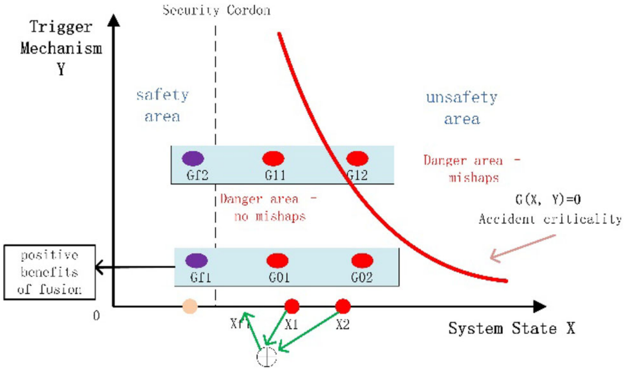

Fig. 9 Mathematical model of MI

2.3.2 MI model

If the situation is $X_f \in S$ after the fusion, in the other words is that the mishap is not characterized and no security event is triggered, it becomes a mishap implication. Because in the implied case, the system is in the security zone and no security events occur. This is a positive benefit for fusion. At the same time, because the mishap is not characterized, it cannot be found. When the environment changes to make y or G change (state migration), it may cause a mishap. This is a negative benefit, as shown in Fig. 9.

2.3.3 MC model

The fusion function F becomes a random mapping under certain conditions: if each subsystems X_i, Y_i, and G_i are given, the fused X_f, Y_f, and G_f become random variables. The approximate ranges and distributions can be inferred, but specific values cannot be determined. Suppose we know that the fused X_f, Y_f, and G_f, the state of each subsystem cannot be pushed back as well. The uncertain correspondence due to fusion can be understood as confusion. When confusion occurs, the specific benefits of its integration are also uncertain, as shown in Fig. 10.

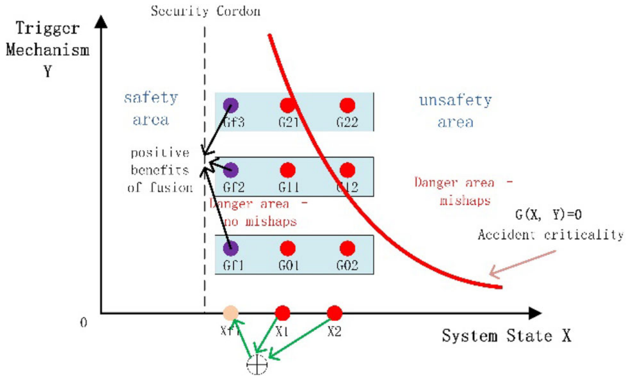

Fig. 10 Mathematical model of MC

3 Cases of multi-source MD–MI–MC

3.1 MD–MI–MC verification method

In the aircraft climbing or landing process, TCASII and ADS–B-fused system are taken as an example to study safety of information fusion. According to the functional information fusion model, the impact on the security and warning modes of TCASII and ADS–B is summarized. In this case, X is defined as the state of subsystem such as ADS–B or TCAS data without fusion process and X' is the output of fused system. Based on the safety feature model of the hazard triangle, by comparing the posterior probability $P(R|X)$ before fusion and the posterior probability $P\left(R|X'\right)$ after fusion, the positive and negative benefits of multi-source MD–MI–MC are indicated. The position parameter $X_i = \{x_i\}, i = 1, 2, \ldots, L$ can be obtained by the subsystem sensors such as ADS–B and TCAS. After fused by the fusion mechanism F, the output of fused system is X' which is defined as $X' = F(X_i)$. The output of system is R_j in which $R_j = 0$ means no alarm and $R_j = 1$ means alarm. The posterior probability $P(R|X)$ can be obtained as the following equation:

$$P\left(R_j|X\right) = \frac{P\left(X|R_j\right)P\left(R_j\right)}{P(X)}, \tag{4}$$

where $P(X)$ is the prior distribution of X which can be obtained by mishap mechanism or experimental simulation. $P\left(X|R_j\right)$ is the probability distributions of X in alarms or no alarms status. $P\left(R_j|X\right)$ is the probability of alarms or no alarms when the input condition is X.

Optimal information fusion criterion [15]: The estimation error covariance matrix $P_{ij}, i = 1, \ldots, L$ is obtained. The fusion is performed according to matrix weighted linear minimum variance criterion. There are ADS–B and TCAS two sensors in this paper, so $L = 2$. The process of fusion is in Eqs. (5, 6):

$$[A_1, \ldots, A_L] = [A_1, A_2] = [A_{\mathrm{TCAS}}, A_{\mathrm{ADS\text{-}B}}] = (e^T P^{-1} e)^{-1} e^T P^{-1} \tag{5}$$

$$X' = \sum_{i=1}^{L} A_i X_i = A_1 X_1 + A_2 X_2 = A_{\mathrm{TCAS}} X_{\mathrm{TCAS}} + A_{\mathrm{ADS\text{-}B}} X_{\mathrm{ADS\text{-}B}}. \tag{6}$$

In this case, every X_i is independent. ADS–B system uses GPS modules to achieve its position information and TCAS system uses Mode S to achieve its position information. The prior distribution of X' in fusion is $P\left(X'\right) = \sum_{i=1}^{L} A_i P(X_i)$. The posterior probability $P\left(R|X'\right)$ can be obtained as the following equation:

$$P\left(R_j|X'\right) = \frac{P\left(X'|R_j\right)P(R_j)}{P(X')}, \tag{7}$$

where $P(X')$ is the prior distribution of X' which can be obtained by mishap mechanism or experimental simulation. $P\left(X'|R_j\right)$ is the probability distributions of X' in alarms or no alarms status. $P\left(R_j|X'\right)$ is the probability of alarms or no alarms when the input condition is X'.

Then, the posterior probability $P(R|X)$ before fusion and the posterior probability $P\left(R|X'\right)$ are compared as follows.

(1) MD

The experiment environment is configured into the alarm area. The posterior probability $P\left(R_j = 1|X\right)$ before fusion and the posterior probability $P\left(R_j = 1|X'\right)$ can be obtained as Eqs. (4) and (7). When $P\left(R_j = 1|X\right) < P\left(R_j = 1|X'\right)$, it means that the leak alarm rate reduced. It is obvious that information fusion brings positive benefits to the system.

The experiment environment is configured into the no alarm area. The posterior probability $P\left(R_j = 0|X\right)$ before fusion and the posterior probability $P\left(R_j = 0|X'\right)$ can be obtained as Eqs. (4) and (7). When $P\left(R_j = 0|X\right) < P\left(R_j = 0|X'\right)$, it means that the false alarm rate reduced. It is obvious that information fusion brings positive benefits to the system.

(2) MI

The experiment environment is configured into the alarm or no alarm area. The posterior probability $P\left(R_j|X\right)$ before fusion and the posterior probability $P\left(R_j|X'\right)$ can be obtained as Eqs. (4) and (7). When $P\left(R_j|X\right) = P\left(R_j|X'\right)$, it means that the source of mishap is not characterized and does not appear. It is obvious that information fusion brings positive or negative benefits to the system.

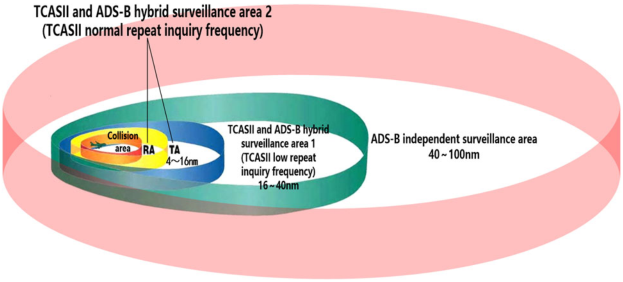
TCASII and ADS-B hybrid surveillance area 2
(TCASII normal repeat inquiry frequency)
Collision area
RA
TA
4~16nm
TCASII and ADS-B hybrid surveillance area 1
(TCASII low repeat inquiry frequency)
16~40nm
ADS-B independent surveillance area
40~100nm

Fig. 11 Flight scenario definition

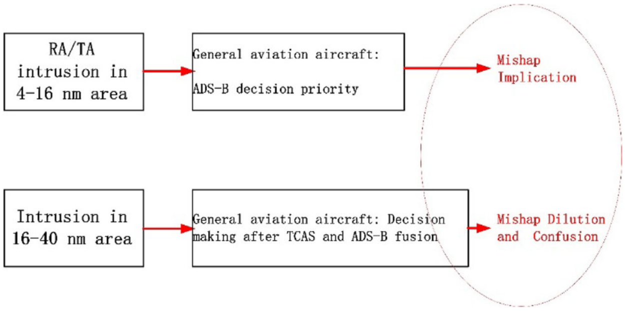
RA/TA intrusion in 4-16 nm area
General aviation aircraft: ADS-B decision priority
Mishap Implication
Intrusion in 16-40 nm area
General aviation aircraft: Decision making after TCAS and ADS-B fusion
Mishap Dilution and Confusion

Fig. 12 Special flight scenario

3.2 Flight scenario definition for simulation cases

TCASII and ADS–B-fused system is taken as an example to verify MD–MI–MC in the aircraft climbing or landing process. The flight scenario is defined, as shown in Fig. 11.

When the distance between this aircraft and the intruder is 4–16 nm, the aircraft is in TCASII and ADS–B hybrid surveillance area 2 in which TCASII has normal repeat inquiry frequency. When the distance between this aircraft and the intruder is 16–40 nm, the aircraft is in TCASII and ADS–B hybrid surveillance area 1 in which TCASII has low repeat inquiry frequency. When the distance between this aircraft and the intruder is 40–100 nm, the aircraft is in ADS–B-independent surveillance area. The TCASII and ADS–B hybrid surveillance area 1 and TCASII and ADS–B hybrid surveillance area 2 are chosen to verify MD–MI–MC, as shown in Fig. 12.

3.3 Verification for MD–MI–MC

The hardware module diagram of ADS–B and TCAS fusion system is shown in Fig. 13.

Algorithm diagram of ADS–B and TCAS fusion system is shown in Fig. 14.

The VSVB–IMM algorithm [9] is proposed to obtain the more precise data from TCAS and ADS–B fusion system. The parameters of simulation system are set in the following. Flight experience 3000 s, sampling period $T = 1$ s. Flight position: 98°00′00″E, 29°00′00″N, 4502 m height. It climbs

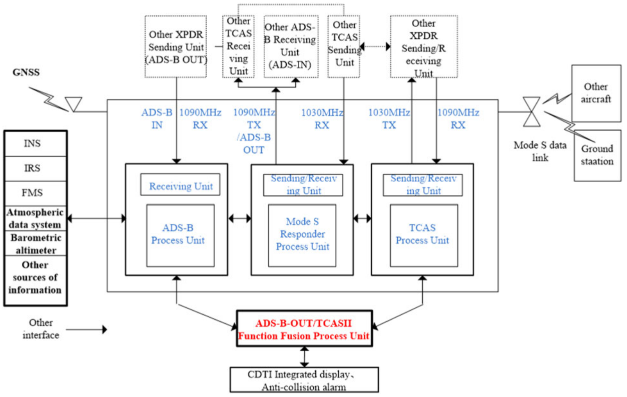

Fig. 13 Hardware module diagram of fusion system

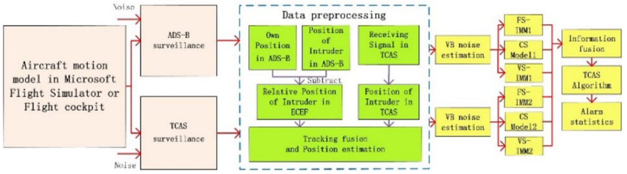

Fig. 14 System frame diagram

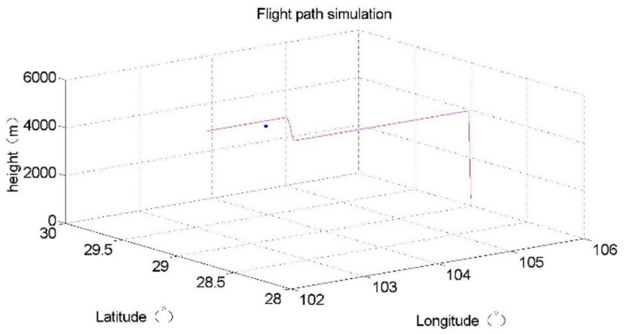

Fig. 15 Flight path simulation

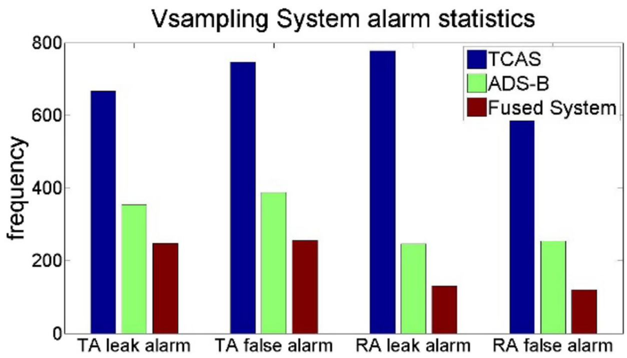

Fig. 16 System false alarm and leak alarm statistics graph

Table 1 Statistics of early alarm and hysteresis alarm during TA (35–45S), RA (<35S) in 200 experiments

Alarm type	System categories		
	TCAS	ADS–B	Fused system
False alarm (TA) (frequency)	667	335	248
Leak alarm (TA) (frequency)	747	389	256
False alarm (RA) (frequency)	778	247	131
Leak alarm (RA) (frequency)	790	254	120

from 300 m height and then cruises at constant height. The initial position of Intruder: 106°00′00″E, 29°00′00″N, 300 m height. TCAS's observation noise standard deviation is 50 m/s, and ADS–B's observation noise standard deviation is time-varying. Flight path simulation is shown in Fig. 15.

The experiment is repeated 300 times(10) independently. One of the statistics is the number of false alarm and leak alarm during the TA (CPA in 35–45 s) and RA (CPA < 35 s) period. Statistics for false alarm is that the actual time advances theory alarm time and exceeds the threshold value (can be set to a constant 1 s). Leak alarm is that the actual time hysteresis theory alarm time and exceeds the threshold value (1 s). In conjunction with Fig. 16 and Table 1, qualitative and quantitative analyses can be carried out that fusion system can reduce the incidence of false alarms, leak alarm in the TA and RA warning alarm interval. Leak alarm and delayed alarm compress avoidance response's time of system and pilot and thus seriously affect flight safety. Therefore, a more accurate alarm time can improve system security and bring forward earnings.

3.3.1 MD in 16–40 nm area

Figure 12 shows that MD can be found in 16–40 nm distance between this aircraft and the intruder. In this area, the decision is made by ADS–B and TCAS fusion system. The TCAS, ADS–B, and fusion system are chosen to be three independent processes to verify MD by injecting into the method proposed in "MD–MI–MC verification method".

The simulation experiment process of MD is shown in Fig. 17.

The aircraft is in the alarm area. The False Alarm (TA) of TCAS is set to FATATCAS. The False Alarm (TA) of ADS–B is set to FATAADSB. The False Alarm (TA) of fusion system is set to FATAFUSION. Independent simulations' number of TCAS is N_{TCAS}. Independent simulations' number of ADS–B is $N_{\text{ADS–B}}$. Independent simulations' number of fusion system is N_{fusion}. According to Eqs. (4), (8), (9), and (10), the value of $P\left(R_j = 1|X_{\text{TCAS}}\right)$ can be obtained:

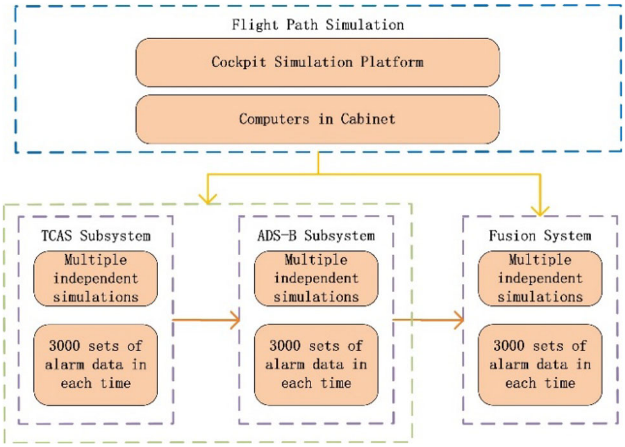
Flight Path Simulation
Cockpit Simulation Platform
Computers in Cabinet
TCAS Subsystem
Multiple independent simulations
3000 sets of alarm data in each time
ADS-B Subsystem
Multiple independent simulations
3000 sets of alarm data in each time
Fusion System
Multiple independent simulations
3000 sets of alarm data in each time

Fig. 17 Simulation experiment process of MD

$$P\left(X_{\text{TCAS}}|R_j = 1\right) = \frac{(3000 \times N_{\text{TCAS}} - \text{FATATCAS}) + (3000 \times N_{\text{fusion}} - \text{FATAFUSION})}{3000 \times (N_{\text{TCAS}} + N_{\text{ADS - B}} + N_{\text{fusion}})} \tag{8}$$

$$P\left(R_j = 1\right) = 1/2 \tag{9}$$

$$P(X) = \frac{3000 \times N_{\text{TCAS}} + 3000 \times N_{\text{fusion}}}{3000 \times (N_{\text{TCAS}} + N_{\text{ADS - B}} + N_{\text{fusion}})}. \tag{10}$$

According to Eqs. (4), (11), (12), and (13), the value of $P\left(R_j = 1|X_{\text{ADS - B}}\right)$ can be obtained:

$$P\left(X_{\text{TCAS}}|R_j = 1\right) = \frac{(3000 \times N_{\text{ADS - B}} - \text{FATAADSB}) + (3000 \times N_{\text{fusion}} - \text{FATAFUSION})}{3000 \times (N_{\text{TCAS}} + N_{\text{ADS - B}} + N_{\text{fusion}})} \tag{11}$$

$$P\left(R_j = 1\right) = 1/2 \tag{12}$$

$$P(X) = \frac{3000 \times N_{\text{ADS - B}} + 3000 \times N_{\text{fusion}}}{3000 \times (N_{\text{TCAS}} + N_{\text{ADS - B}} + N_{\text{fusion}})}. \tag{13}$$

According to Eqs. (4), (14), (15), and (16), the value of $P\left(R_j = 1|X_{\text{fusion}}\right)$ can be obtained:

$$P\left(X_{\text{TCAS}}|R_j = 1\right) = \frac{3000 \times N_{\text{fusion}} - \text{FATAFUSION}}{3000 \times (N_{\text{TCAS}} + N_{\text{ADS - B}} + N_{\text{fusion}})} \tag{14}$$

$$P\left(R_j = 1\right) = 1/2 \tag{15}$$

$$P(X) = \frac{3000 \times N_{\text{TCAS}} + 3000 \times N_{\text{fusion}}}{3000 \times (N_{\text{TCAS}} + N_{\text{ADS - B}} + N_{\text{fusion}})}. \tag{16}$$

According to Table 1, the data are substituted into the Eqs. (4), (8), (9), (10), (11), (12), (13), (14), (15), and (16). The results are shown as follows: $P\left(R_j = 1|X_{\text{TCAS}}\right) \approx 0.49963$, $P\left(R_j = 1|X_{\text{ADS - B}}\right) \approx 0.49965$, and $P\left(R_j = 1|X_{\text{fusion}}\right) \approx 0.49977$. In this flight scenario, $P\left(R_j = 1|X_{\text{TCAS}}\right) < P\left(R_j = 1|X_{\text{fusion}}\right)$ and $P\left(R_j = 1|X_{\text{ADS - B}}\right) < P\left(R_j = 1|X_{\text{fusion}}\right)$.

According to theory defined in 3.1, it means that the leak alarm rate reduced. It is obvious that information fusion brings positive benefits to the system. In 16–40 nm distance between this aircraft and the intruder, MD is found.

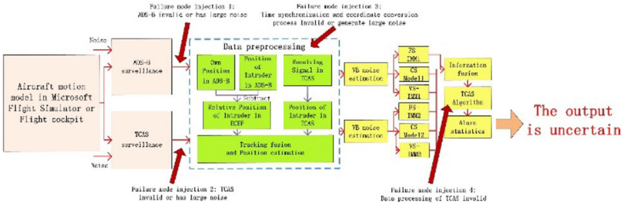
Failure mode injection 1:
ADS-B invalid or has large noise
Failure mode injection 3:
Time synchronization and coordinate conversion process Invalid or generate large noise
Noise
Aircraft motion model in Microsoft Flight Simulator or Flight cockpit
ADS-B surveillance
TCAS surveillance
Noise
Data preprocessing
Own Position in ADS-B
Position of Intruder in ADS-B
Receiving Signal in TCAS
Subtract
Relative Position of Intruder in ECEF
Position of Intruder in TCAS
Tracking fusion and Position estimation
VB noise estimation
VB noise estimation
FS IMM1
CS Model1
VS-IMM1
FS IMM2
CS Model2
VS-IMM2
Information fusion
TCAS Algorithm
Alarm statistics
The output is uncertain
Failure mode injection 2: TCAS invalid or has large noise
Failure mode injection 4:
Data processing of TCAS invalid

Fig. 18 Injecting failure mode in multiple

3.3.2 MC in 16–40 nm area

The failure mode is injected in multiple in the data link, which is shown in Fig. 18.

The large noise is injected into ADS–B terminal as failure mode injections 1 and 2 in Fig. 18. In addition, the alarm statistic is shown in Fig. 19 and Table 2.

The statistics of ten sets of data for leak alarm TA are shown in Table 3.

According to Table 3, $P(R|X)$ and $P\left(R|X'\right)$ can be obtained from the Eqs. (4), (8), (9), (10), (11), (12), (13), (14), (15), and (16). Comparing with the posterior probability $P(R|X)$ before fusion and the posterior probability $P\left(R|X'\right)$ after fusion in ten experiments, there are only seven times that $P\left(R_j = 1|X_{\text{TCAS}}\right) < P\left(R_j = 1|X_{\text{fusion}}\right)$ and 4 times that $P\left(R_j = 1|X_{\text{ADS - B}}\right) < P\left(R_j = 1|X_{\text{fusion}}\right)$. Therefore, the relationship between $P(R|X)$ and $P\left(R|X'\right)$ is uncertain. The source of failure mode is confused and uncertain. Therefore, in 16–40 nm distance between this aircraft and the intruder, MC is found.

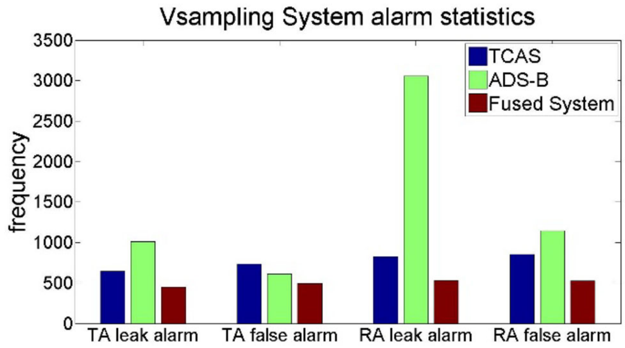

Fig. 19 System alarm statistics graph with large ADS–B noise

Table 2 Statistics of early alarm and hysteresis alarm during TA (35–45S), RA (<35S) in 300 experiments

Alarm type	System categories		
	TCAS	ADS–B	Fused system
False alarm (TA) (frequency)	647	1011	448
Leak alarm (TA) (frequency)	734	614	492
False alarm (RA) (frequency)	827	3058	531
Leak alarm (RA) (frequency)	825	1147	526

3.3.3 MI in 4–16 nm area

Figure 12 shows that MD can be found in 4–16 nm distance between this aircraft and the intruder. In this area, the decision is ADS–B subsystem priority. The ADS–B and fusion system is chosen to be two independent processes to verify MI by injecting into the method proposed in "MD–MI–MC verification method".

The simulation experiment process of MI is shown in Fig. 20.

According to Eqs. (4), (11), (12), and (13), the value of $P\left(R_j = 1|X_{\text{ADS - B}}\right)$ can be obtained. Fusion system is priority to use ADS–B data when both ADS–B and TCAS data valid. Therefore, $P\left(R_j = 1|X_{\text{fusion}}\right) = P\left(R_j = 1|X_{\text{ADS - B}}\right)$. It means that the source of TCAS failure is not characterized and does not appear. In 4–16 nm distance between this aircraft and the intruder, MI is found.

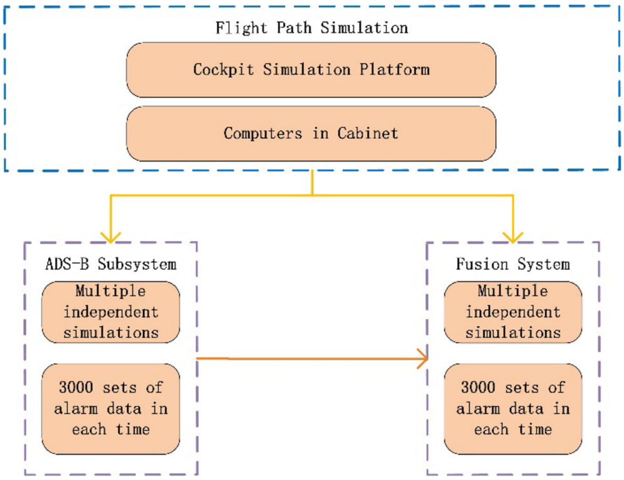
Flight Path Simulation
Cockpit Simulation Platform
Computers in Cabinet
ADS-B Subsystem
Multiple independent simulations
3000 sets of alarm data in each time
Fusion System
Multiple independent simulations
3000 sets of alarm data in each time

Fig. 20 Simulation experiment process of mishap implication

4 Conclusions

The contributions of this paper can be summarized as follows:

(1) The concept of MD–MI–MC is first defined in functional information fusion of avionics system.
The integrated technology brings benefits to avionics system, and meantime, it also brings MD–MI–MC and many uncertainly problems. MD in functional information fusion causes the mishap source composition and strength weakening which can also lead to the occurrence probability of accident decrease. In this case, the accident may not happen and the mishap is in diluted state. MI in functional information fusion causes the mishap source not be characterized and not revealed. In this case, the mishap source cannot be found when the accident occurs. MC in functional information fusion causes the mishap source in random concurrency or disappearance. In this case, the mishap source is confused and uncertain.

(2) The model of multi-source MD–MI–MC is established based on hazard theory.

Table 3 Statistics of leak alarm TA (35–45S) in 300 experiments

Number of experiments	1	2	3	4	5	6	7	8	9	10
TCAS	747	553	674	890	459	386	961	768	662	658
ADS–B	389	249	423	186	369	353	502	276	441	363
Fusion system	256	301	189	236	301	469	613	452	376	421

Based on the hazard theory, hazards are composed of three basic components: Hazardous Element (HE), Initiating Mechanism (IM), and Target and Threat (TT). The MD–MI–MC model is built, respectively, in the abstract concept based on the general model of functional information fusion of avionics system. In addition, the model can describe the MD–MI–MC process quantitatively with the mishap initiating decision function $G(X, Y)$.

(3) The functional fusion of Automatic-Dependent Surveillance–Broadcast (ADS–B) and Traffic Collision Avoidance System (TCAS) is used as a typical example to analyze fusion system during the aircraft climbing or landing state.

Based on the model of multi-source MD–MI–MC, a set of theories system is built to analyze the fusion of ADS–B and TCAS model. A fusion model with a VSVB–IMM algorithm in integrated surveillance avionics system is used to integrated display and the fusion system can significantly increase the range of traffic collision avoidance. The warning mode and the safety impact of ADS–B and TCAS II fusion system are proposed. According to Hazard Triangles Theory (HTT), the positive and negative benefits of MD–MI–MC are obtained from the theory system in functional information fusion system.

In this paper, the concept and model of multi-source MD–MI–MC are proposed for safety assessment of integrated avionics system. First, it is based on the general functional information fusion model, and then, the VSVB–IMM fusion method of ADS–B and TCAS II in integrated surveillance avionics system is used to analyze. At last, a theory system and evaluation standards are tested by real-engineering process of integrated surveillance avionics system. The positive and negative benefits of MD–MI–MC can be obtained quantitatively based on the presented integrated avionics theory and mechanism.

Acknowledgements This paper is sponsored by National Program on Key Basic Research Project (2014CB744903), National Natural Science Foundation of China (61673270), Shanghai Pujiang Program (16PJD028), Shanghai Industrial Strengthening Project (GYQJ-2017-5-08), Shanghai Science and Technology Committee Research Project (17DZ1204304) and Shanghai Engineering Research Center of Civil Aircraft Flight Testing.

References

1. Wang G, Gu Q, Wang M, Wang Y (2014) Research on integrated technology and model in avionics system. In: Digital avionics systems conference, pp 4A2-1–4A2-11
2. Mahler RP (2014) Advances in statistical multisource-multitarget information fusion. Artech House, Norwood
3. Wang G (2012) Integration technology for avionics system. In: Digital avionics systems conference, pp 7C6-1–7C6-9
4. Badache N, Jaffres-Runser K, Scharbarg JL, Fraboul C (2013) End-to-end delay analysis in an integrated modular avionics architecture. In: Emerging technologies and factory automation, pp 1–4
5. Wu J, Yue T, Ali S, Zhang H (2013) Ensuring safety of avionics software at the architecture design level: an industrial case study. In: International conference on quality software, pp 55–64
6. Luo RC, Ying CC, Chen O (2002) Multisensor fusion and integration: algorithms, applications, and future research directions. IEEE Sens J 2(2):107–119
7. Kunzi F (2011) ADS-B benefits to general aviation and barriers to implementation. Massachusetts Institute of Technology, Cambridge
8. Kuchar JE, Drumm AC (2007) The traffic alert and collision avoidance system. Linc Lab J 16(2):277
9. Wang Y, Xiao G, Dai Z (2017) Integrated display and simulation for automatic dependent surveillance-broadcast and traffic collision avoidance system data fusion. Sensors 17(11):2611
10. Ding C, Xu J, Xu L (2013) ISHM-based intelligent fusion prognostics for space avionics. Dialogues Cardiovasc Med Dcm 29(1):200–205
11. Shen X, Bai Y (2014) Architectural considerations in integrated modular avionics (IMA) system safety case construction. IEEE Aerosp Electron Syst Mag 29(10):26–33
12. An X (2012) Safety-centered architecture design method for IMA software. Comput Sci 39(3):128
13. Cai Y, Wang Z, Ou X, Zhu L (2011) Approach civil integrated modular avionics airworthiness certification by iterative incremental certification process. In: International conference on information science and engineering, pp 148–151
14. Ericson CA (2005) Hazard analysis techniques for system safety. Wiley, Hoboken
15. Deng Zili (2005) Optimal estimation theory with application: modeling, filtering, information fusion estimation, Chap. 6. Harbin Institute of Technology Press, Harbin, pp 377–385