A Systematic Approach to Conducting FHA

Jian Wang(✉)

AECC CAE, Shanghai, China
jian.wang@gmx.de

Abstract. To develop a complex, safety-critical system, it is of great importance to identify the safety requirements at the earlier stage of system development. Functional Hazard Assessment technique is commonly used in order to identify top-level safety requirements based on the system functions. In this article, we present a systematic approach to conducting FHA starting from the list of system function, based on which the functional Failure Conditions are identified, then each Failure Condition is classified based on its Failure Effect. Different Failure Effects are categorised to different level of Severity, to which a safety goal is associated. By studying the chain from Failure Condition to Failure Effect, to Severity, and to the associated safety goal, the safety requirements for each Failure Condition can be determined at the end of Functional Hazard Assessment.

Keywords: Complex System Safety Assessment · Functional Hazard Assessment · Failure Condition · Failure Effect · Severity

1 Introduction

In the paradigm of complex system development, lack of sufficient safety feature usually leads to product redesign at a very high cost in terms of money, time, and business reputation. A bitter lesson learnt recently in the aviation industry is the redesign of the notorious Maneuvering Characteristics Augmentation System (MCAS) in the Boeing 737 MAX series aircraft. This made people realize again the importance of identifying safety requirements at the earlier stage of system development, and validating safety requirements in the course of system design evolution.

In a top-down approach of system development, the capture and validation of safety requirements is in principle of iterative nature, mainly using Preliminary System Safety Assessment (PSSA) and Functional Hazard Assessment (FHA) techniques. Although the role of PSSA and FHA in the system development process has been effectively illustrated in SAE ARP4754A [6], the interaction between these two techniques has not been explained in detail. The guidelines and methods for conducting PSSA and FHA have been explained in SAE ARP4761 [5]. Noticeably, SAE ARP4761 is fairly old, and revision A (or SAE ARP4761A) was initiated since 2004 but is still in the state of Work In Progress (WIP) at the time of this article.

According to SAE ARP4761 [5], which was published in 1996, PSSA is defined as 'A systematic evaluation of a proposed system architecture and implementation based

D. Krob et al. (Eds.): CSD&M 2023, LNEE 1085, pp. 37–46, 2023.
https://doi.org/10.1007/978-981-99-6511-3_4

on the Functional Hazard Assessment and failure condition classification to determine safety requirements for all items'. With many years of industrial practice of safety work thereafter, this definition was slightly modified, as in SAE ARP4754A [6] published in 2010, to 'A systematic evaluation of a proposed system architecture and its implementation, based on the Functional Hazard Assessment and Failure Condition classification, to determine safety requirements for systems and items'. Comparing these two definitions of PSSA, we noticed that, PSSA can be applied at both system and item levels of system design (i.e., at system, sub-system, all the way down to the item level) in order to determine the safety requirements at different levels. Yet another important message can be drawn from the aforementioned two definitions is that PSSA should be conducted based on the result of FHA. Indeed, PSSA has at least two purposes:

1. Confirming that the proposed system architecture and its implementation is safe;
2. Allocating safety requirements to the lower level specified in system architecture (system or item).

While the result of FHA severs as part of the inputs to the work of PSSA, the definition of FHA, also given in SAE ARP4754A [6], 'A systematic, comprehensive examination of functions to identify and classify Failure Conditions of those functions according to their severity.', does not tell too much about the input information for conducting FHA, and what would be the outcome of FHA. Indeed, it is even improperly expressed in this definition that the classification of identified Failure Conditions is based on their severity. In practice, after being identified, Failure Conditions are first assessed in order to determine their Failure Effects, then different Failure Effects are further classified according to their Severity. Another important outcome of FHA would be the safety requirements determined for each identified Failure Condition.

Although SAE ARP4761 [5] provided guidelines and methods for conducting FHA, it has become out-dated compared to the industrial experience accumulated after it was published. In the rest of this article, we would like to share our experience on how to conduct FHA, starting from examining the necessary input information, identifying Failure Conditions (FC), assessing Failure Effects (FE) for each identified FC, classifying the Severity of each FE, and last but not least, determining the safety requirements for each identified FC.

FHA can be conducted at any level of the system architecture of any system, regardless if it is at aircraft, car, rocket, nuclear reactor, chemical process, aircraft engine, braking system, control system or at an item level. In order to keep the description as general as possible, in the rest of this article, we call the system under the study of FHA as the Subject System (SS).

2 Review of Input Data of FHA

Given the background and context of FHA in Sect. 1, now it's time to check if the necessary information is available in order to start FHA. As given in its definition, FHA is 'a systematic, comprehensive examination of functions …', the starting point of FHA is usually a list of expected functions prescribed to the Subject System (SS) by the system development process at a higher level. Depending on the location of SS in the

overall system architecture, the prescribed functions can come from captured customer requirements, or as a result of functional analysis at the same level as that of SS.

Some other information, such as the system operational environment/context, overall system architecture, etc. would also be available at this stage, and would be useful when identifying the Failure Conditions and assessing its Failure Effects as described in Sect. 3 and 4.

In short, the following are the list of information/documentation necessary to conduct FHA:

1. List of Functions with description and inter-relationship between Functions limited to the abstraction level of SS;
2. Operating environment/context of SS, e.g., the flight phase definition in case that SS represents an aircraft;
3. System architecture description not necessarily exhausted to details but sufficient to the level of SS;

Taking the Braking System of a vehicle as an example of Subject System, which serves to slow down or stop the vehicle by converting the kinetic energy of the vehicle into heat energy through friction. At the system architecture design stage, a Braking System has been identified as one of the sub-systems of the vehicle, and its functions have been determined as:

1. Apply Braking Force
   The system should be able to apply the necessary braking force required to slow down or stop the vehicle.
2. .Maintain Braking Force
   The system should maintain the braking force even under different driving conditions and situations, such as uneven road surfaces, emergency stops, etc.
3. Distribute Braking Force.
   The system should distribute the braking force evenly among all the wheels to ensure stable and safe braking.

It is very important to keep in mind, that at the stage of specifying the vehicle architecture down to the level of Braking System, together with the other systems like the Engine System, Transmission System, Electrical System, Suspension System, Steering System and Fuel System at the same level, it is not necessary to consider how to realise (or implement) the functions of Braking System, with even more detailed design at lower-level, such as Anti-lock Braking System (ABS), Parking Brake, Hydraulic or Pneumatic System, Brake Discs/Drums, Brake Pads/Shoes, Brake Calipers/Wheel Cylinders, or Brake Lines and Hoses, etc.

Another good example is the Engine Electronic Control System (EECS) for an aircraft engine as a Subject System. As the most complex system of an aircraft engine, in order to keep the engine performance within a safe and efficient margin, the functions of the EECS usually include:

1. Fuel Control
   EECS modulates the fuel flow into the Combustion Chamber of an engine;
2. Engine Geometry Control

For jet engine featured with variable-geometry structure, EECS adjusts the vanes angle at different engine stages according to the engine operating conditions;

3. Heat Management
   EECS monitors the fuel and oil temperature and pressure, and take actions (applying cooling air, changing the fluid circulation path, etc.) accordingly;
4. Engine Health Monitoring and Annunciation
   EECS monitors the engine conditions and operating parameters, detects any abnormality or malfunction, applies any necessary mitigation actions, annunciates the engine states to the flight crew if necessary;
5. Thrust/Power Management
   EECS determines the Thrust/Power level and control mode of the engine based on aircraft demand and current engine operating condition;
6. Engine Protection
   EECS may determine any emergency threats (over-speed, over-temperature, extreme vibration, inclement weather condition, volcanic ash, single event effect, etc.) and take proper action in order to protect engine from potential damage;
7. Engine Start-up and shut-down
   EECS manages the engine start-up and shut-down procedures;
8. Bleed Regulation
   EECS regulate the engine bleeds from different stages for the purpose of cooling, anti-icing, performance and customer service;

   Again, at this stage of engine architecture design, there is no need to consider how to realise (or implement) the functions of EECS with different types of sensors, actuators, electronic controller or software.

3 Identification of Functional Failure Conditions (FC)

The input data as described in Sect. 2 should suffice to start the work of FHA beginning with the identification of Failure Conditions (FC). SAE ARP4754A [6] agrees with the definition of Failure Conditions from AMC 25.1309 in EASA CS-25 [3] as: 'A condition having an effect on the aeroplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events.'. Obviously, this definition of FC is limited to the aircraft (Aeroplane as specified by EASA CS-25 [3], or Transport Category Airplanes as specified by 14 CFR Part 25 from FAA)[1]. As we have determined in Sect. 1 to apply FHA at any given Subject System (SS), a generalisation to this definition is necessary. For this purpose, we simply consider Failure Condition as a state of an SS, in which the SS cannot perform its intended functions. So far, we are not interested in 'what is the cause of the Failure Condition', or 'how the function is affected'.

One way to identify the Failure Conditions is to start with the functions of the SS by which it is expected to perform. For that an examination to List of Functions as described in Sect. 2 would be a good practice. In this context, any type of malfunction, including

[1] Noticeably, the Failure Conditions defined in EASA AMC 25.1309 is not dedicated for the purpose of conducting FHA.

loss of function, can be considered as an FC. In general, different type of malfunction can be identified by considering different aspects of a function, such as whether it is about the.

1. Magnitude
   a. too high, strong, long?
   b. too low, weak, short?
   c. oscillating?
   d. drifting?
2. Timing
   a. too early?
   b. too late?
   c. less frequent?
   d. or too often?
3. Grade
   a. totally lost?
   b. partially lost?
4. Duration
   a. last too long?
   b. last too short?

A Failure Condition can also be identified as a result of multiple dysfunctions while the mechanism is not yet understood at the time of assessment, e.g., set on fire, become over-temperature, etc. However, the phenomenon of such Failure Condition would be observable, or measurable. We shall talk about such kind of Failure Condition later in Sect. 4.

4 Assess Failure Effect of Functional FC

Unlike the common guidelines as presented in SAE ARP4761 [5], we tend to emphasise the difference between Failure Conditions and their Failure Effect (FE): an FC is simply a situation in which the Subject System cannot perform its indented function; however, the Failure Effect is considered as the consequence at the SS level or at the level above the SS in the system architecture, given the condition when SS remains in such situation.

The Failure Effect of an FC is usually measurable, or observable, and should be assessed at least to the same level of the Subject System (SS), but preferably be assessed at levels higher than that of SS, provided sufficient evidence/assumption are available in order to support such assessment. This is mainly due to the fact that at higher level, the consequence of the FC would be easier to observe, and in most cases, more concrete regulatory restrictions or constraints are imposed by different authorities or institutes, and will therefore facilitate the determination of safety requirements of FC, which is discussed in Sect. 6 of this article. For example, given the type certification regulation available at the aircraft-level, such as CCAR Part 25, FAA 14 CFR Part 25, and EASA CS-25, the Failure Effect of an SS as aircraft would be sufficiently assessed at the same level as at aircraft-level; while given the type certification regulation only available at the engine-level, such as CCAR Part 33, FAA 14 CFR Part 33, and EASA CS-E, the Failure

Effect of an SS as Engine Electronic Control System (EECS) should not be limited at EECS-level, but preferably be extended up to the engine-level.

Given a phrase of failure description, sometimes it may not be easy to tell if the failure description is an FC or an FE to a Subject System. This is mainly due to the fact that an FE of a Subject System would become the Failure Condition of another SS at higher level. In this situation, the assessor is advised to keep firmly at the level of the Subject System, and try to identify the causal relationship between the failure description and the expected function of the SS. If the described failure can be directly related to an expected function of the SS, then this failure description is an FC to the SS; or, If the described failure can be related to the errors of lower-level function/components of the SS, then the failure description is an FE to the SS. For example, consider Aircraft Engine as an SS, a failure description of 'Loss of Thrust Control' is directly related to the function of 'generating thrust according to received command', which is one of the functions of an Aircraft Engine, therefore 'Loss of Thrust Control' is an FC to the Aircraft Engine; on the other hand, consider Engine Electronic Control System (EECS) as an SS, the same failure description of 'Loss of Thrust Control' is caused by different errors in lower-level components of EECS, therefore 'Loss of Thrust Control' is an FE of EECS.

For a set of FCs, although it is possible to assess the Failure Effects for different FC at different levels in the system architecture higher or the same level as that of SS, it should be kept in mind that in principle, all the Failure Effects should be assessed at the same level. This is due to the fact that the Failure Effects will be categorised based on their Severity as described in Sect. 5 at a specific level.

If a Failure Condition is identified as a result of multiple dysfunctions in SS, as described in Sect. 3, they are usually described based on its effect to the SS. In this case, such Failure Condition can also be considered as the Failure Effect at the same level of SS in the system architecture. Unless we assess the Failure Effect at a higher level for the SS, it is not necessary to assess such FC for its FE any further, since in this case, such FC would be identical to its FE.

5 Categorisation of Failure Effects Based on Severity

We define Severity as a set of categories inversely related to the Failure Effects. It is worthwhile to emphasise that the relationship between Severity and Failure Effect are inverse relation since this relationship are not causal, and are merely subjective.

For example, AC 25.1309-1A [1] from FAA proposed Severity categories of 'Minor', 'Major', and 'Catastrophic' at aircraft-level such that:

1. Minor:
   Not significantly reduce airplane safety, may involve crew actions that are well within their capabilities;
2. Major:
   large reduction in safety margins, or reduction in functional capabilities, or higher workload on crew, or adverse effects on occupants;
3. Catastrophic:
   prevent continued safe flight and landing.

Note that, the Severity categories defined here setup a relationship to a set of Failure Effects at the aircraft-level.

While CS-E 510 [2] from EASA proposed Severity categories of 'Minor', 'Major', and 'Hazardous' at aircraft engine level such as:

1. Minor:
   partial or complete loss of thrust or power from the Engine;
2. Major:
   any effect between 'Minor' and 'Hazardous';
3. Hazardous:
   in case of the following effects:
   a. Non-containment of high-energy debris;
   b. Concentration of toxic products in the Engine bleed air for the cabin sufficient to incapacitate crew or passengers;
   c. Significant thrust in the opposite direction to that commanded by the pilot;
   d. Uncontrolled fire;
   e. Failure of the Engine mount system leading to inadvertent Engine separation;
   f. Release of the propeller by the Engine, if applicable;
   g. Complete inability to shut the Engine down.

Obviously, the Severity categories defined here setup a relationship to a set of Failure Effects at the aircraft engine level.

Apart from the above Severity categories proposed in the civil aviation industry, other industrial area may propose Severity categories based on their own safety practice. For example, in automotive industry, the Severity categories are proposed in 'ISO 26262, part 3, appendix B, classification of the severity factor', according to the book of 'Functional Safety for Road Vehicles – New Challenges and Solutions for E-mobility and Automated Driving' [4] as:

1. light and moderate injuries (S1)
2. severe/serious injuries possibly life-threatening, survival is likely (S2)
3. life-threatening injuries (survival uncertain) or deadly injuries (S3)

Again, the Severity categories defined here setup a relationship to a set of Failure Effects at the road vehicle level.

The reason of specifying different Severity categories is that the safety practice of different industries tends to setup a safety goal in terms of probability, qualitatively and/or quantitatively, based on a common degree of Severity which can be related to the Failure Effect. In this way, individual system developer can describe the Failure Effect to their own product at their own ease. Figure 1 is the safety goals as an example in civil aviation industry according to different FAA regulations or EASA specifications for aircraft and aircraft engines.

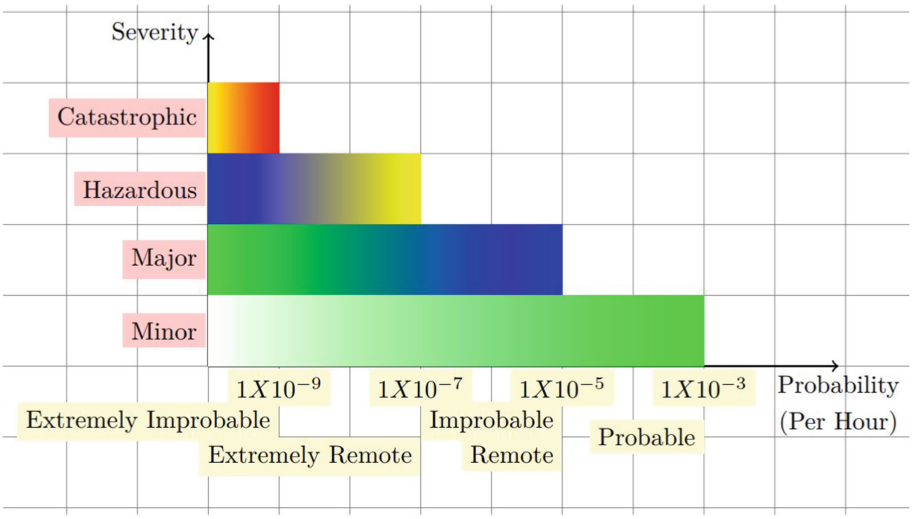

Fig. 1. Safety Goals Depending on Severity in terms of Probability in Aviation Industry

6 Determine Safety Goal for Each Failure Effect

Having explained the relations between Functions and functional Failure Conditions, between functional Failure Conditions and Failure Effects, and between Failure Effects and Severity, now we are ready to determine the safety requirement for each identified Failure Condition, which is the major purpose of FHA. Next, we will explain this procedure using a generic example.

Table 1 represents the identified Failure Conditions (FCs) related to the Function of our Subject System (SS), and for Failure Condition its associated Failure Effect to the level of SS or higher in the system architecture. Remember, the Failure Effect should remain to the same level for all Failure Conditions, as we have emphasised in Sect. 4.

Table 1. Identified Functional Failure Conditions and Effects

Function	Failure Condition	Failure Effect@Level
F1	FC1-1	E1
	FC1-2	E2
F2	FC2-1	E3
	FC2-2	E1
F3	FC3-1	E3
	FC3-2	E1
F4	FC4-1	E2
	FC4-2	E1

Re-organise the Failure Conditions in Table 1 based on their Failure Effect at a given level and associated Severity would result in Table 2, in which the contribution of each Failure Condition to associated safety goals are clearly concluded.

Table 2. Functional Failure Conditions and Safety Goals

Failure Condition	Failure Effect@Level	Safety Goal@Severity
FC1-1	E1	$<1 \times 10^{-5}$ per Hour@S1
FC2-2		
FC3-2		
FC4-2		
FC1-2	E2	$<1 \times 10^{-7}$ per Hour@S2
FC4-1		
FC2-1	E3	$<1 \times 10^{-5}$ per Hour@S1
FC3-1		

In the next step, we can evenly distribute the safety goal to the associated Failure Conditions as their initial safety requirements (Table 3). These initial safety requirements can be modified to more realistic safety requirements when more experience becomes available in the course of system development.

Table 3. Safety Requirement for each Failure Condition

Failure Condition	Requirement	Safety Goal@Severity
FC1-1	$<2.5 \times 10^{-6}$ per Hour	$<1 \times 10^{-5}$ per Hour@S1
FC2-2	$<2.5 \times 10^{-6}$ per Hour	
FC3-2	$<2.5 \times 10^{-6}$ per Hour	
FC4-2	$<2.5 \times 10^{-6}$ per Hour	
FC1-2	$<5.0 \times 10^{-8}$ per Hour	$<1 \times 10^{-7}$ per Hour@S2
FC4-1	$<5.0 \times 10^{-8}$ per Hour	
FC2-1	$<5.0 \times 10^{-6}$ per Hour	$<1 \times 10^{-5}$ per Hour@S1
FC3-1	$<5.0 \times 10^{-6}$ per Hour	

7 Conclusion

So far, we have presented a generic and systematic approach to determine the safety requirements using the Functional Hazard Assessment technique. Different from the common approach in the literature, we differentiate the significance of Failure Condition

from its Failure Effect in that, a Failure Condition is usually related to the intended function to be performed by the Subject System; and the Failure Effect is an observable, measurable phenomenon at the level of SS or higher, as a result of an FC. Usually, the Failure Effect is assessed at the level where a set of Severity categories, and their associated safety goal are well defined, and commonly accepted. With these chains of relationship, we finally set up the relationship between the Failure Conditions and the Severity categories with definite safety goals, based on which the safety requirements for each Failure Conditions can be determined. Last but not least, the safety requirements for each Failure Conditions can be easily adjusted in the course of system development.

References

1. ANM-110: System Design and Analysis. Advisory Circular, AC25.1309-1A, Federal Aviation Administration (1988)
2. EASA: Certification Specifications and Acceptable Means of Compliance for Engines (CS-E). CS, CS-E, amendment 6, European Union Aviation Safety Agency. Annex VII to ED Decision 2020/006/R (2020)
3. EASA: Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes (CS-25). CS, CS-25, amendment 27, European Union Aviation Safety Agency, January 2023. Annex to ED Decision 2021/015/R. Amendment 27 was originally released on 24 Nov 2021, and is replaced by this edition with correction to its original release. The date of entry in force remains unchanged
4. Ross, H.-L.: Functional Safety for Road Vehicles – New Challenges and Solutions for E-mobility and Automated Driving. Springer International Publishing Switzerland. Translation from the German language edition: Funktionale Sicherheit im Automobil: ISO 26262, Systemengineering auf Basis eines Sicherheitslebenszyklus und bewährten Managementsystemen (2016)
5. SAE: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. Aerospace Recommended Practice, ARP 4761, SAE International (1996)
6. SAE: Guidelines for Development of Civil Aircraft and Systems. Aerospace Recommended Practice, ARP 4754A, SAE International (2010)