ATLANTIS PRESS

Advances in Engineering Research, volume 149

2nd International Conference on Mechanical, Electronic, Control and Automation Engineering (MECAE 2018)

A Safety-Security Integrated Analysis Approach

Xinyu Sun

School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China;

sunxinyu_92@163.com

Keywords: safety; security; fault tree; attack tree; risk analysis.

Abstract. A large number of computer, communication and control technologies are applied in train operation control system, which brings the internal and external security risks to the urban rail traffic, especially under the background that security incidents of industrial control system occur frequently, security of operation control system of urban rail train need high attention, but the traditional safety analysis methods do not consider malicious and subjective security risk. This paper analyzes the relationship between the safety and security and necessity of comprehensive analysis of safety and security is defined. A comprehensive analysis method of security and safety based on extended fault tree is proposed. The extended fault tree model integrates the fault tree with displaying safety failure logic, and the attack tree with describing the security attack behaviors, and the analysis model based on the extended fault tree is established. The extended fault tree model is able to analyze the effect of security risk for safety and operational efficiency of train control system in this paper, which has important guiding significance for analysis work of operation risk of train control system. In addition, the fault tree and attack tree can be quickly established with small adjustments, which make it a simple and intuitive method.

1. Introduction

With the deepening of urbanization, the urban rail transit system has become the main body of urban passenger transit with the advantages of large volume, fast speed, safety, punctuality, and energy saving and so on. By the end of December 31, 2017, China' 32 cities have opened rail transit facilities, the total operation mileages reach 4,750 kilometers, ranked first in the world. Urban rail transits are the infrastructures which bear upon national economy and the people's livelihood, and the security of daily operation must be guaranteed. Safety in the urban rail transit development has deep accumulation, however, with the wide application of information technology in recent years, the security situation is becoming increasingly serious, especially after "Stuxnet" virus causes control system of nuclear facilities to fail in 2010, this incident causes the high attention all over the world.

As the "brain" and "nervous central" of the urban rail transit, the train operation control system has critical requirements for safety control. The safety concerns the functional failure caused by random and unexpected faults, and a large number of control mechanisms with "failure-safety" concept are applied to the design of the train control system. At the beginning of the development of rail transit, security has not attracted the attention of the industry. Urban rail transit as national critical infrastructure about the national economy and people's livelihood, risk identification, risk analysis and corresponding risk response of security and other core technologies is urgent to be developed. In-depth and comprehensive security risk analysis is the primary problem.

This paper proposes a comprehensive analysis method of safety and security based on extended fault tree, this method is established based on existing analysis theory and results of safety, along with the security analysis method, and the comprehensive analysis of the two is realized.

2. Safety

2.1 Concept of Safety

The definition of safety is "no unacceptable risk" in IEC 61508" safety of electrical/electronic/programmable electronic security system", and it mainly aims at problems that

system failure causes person or environment to be harmed, and emphasizes the reliability of the system [2]. The standard for safety is targeted to the internals of the system, due to random errors, system errors, environmental effect, operation errors, and software defects and failure caused by software defects. The accidents caused by these random and unexpected system failures will affect the environment.

The urban rail transit system CBTC with excessive demands as an example, the ATP sub-system based on safety requirements, which must ensure the system in train operating speed can't exceed the highest speed, the highest speed is required by movement authorization and temporary speed limit, so as not to cause the train to abnormally drive and traffic accidents occur under over-speed condition. When the maximum speed limit is exceeded, the system automatically implements the emergency brake and carries out the over-speed protection. This is a typical safety requirement.

From another perspective, likewise ATP over speed protection function, if the train operation speed does not exceed maximum speed of system, but the maximum speed limit of system itself increases after malicious tampering, this scenario is the same as the scenario for security from the results, but this system failure caused by malicious tampering belongs to security field. However, the IEC 61508, which is followed by the rail transit industry, does not discuss and guide the system function failure problems caused by the security attack.

2.2 Risk Evolution Path of Safety

Hazard identification is the first step in the safety management. EN 50126 defines the hazard as "the physical condition which causes potential casualties (harm)" [3]. At the system boundary, when some conditions are met, the hazard is triggered, which may develop into a safety accident [4].

Figure.1 shows the development path of safety accidents from system failure to accident. The system failures of safety all exist within the system, but the causes of system failures, it is possible that unexpected operation, misuse, weather as well as environmental factors, it is possible that the random hardware, software failure directly cause system failure, so the line from "fault trigger" to "system failure" is the dotted line in Figure.1, and it indicates unnecessary condition.

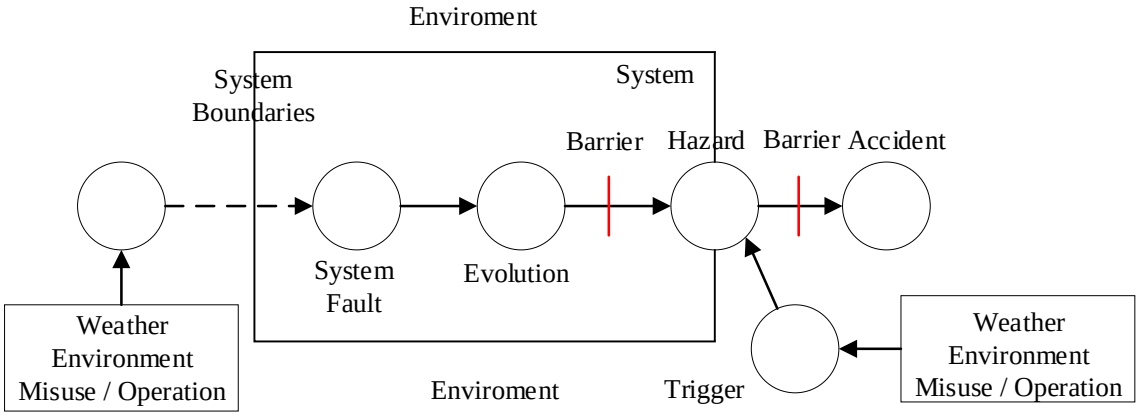

Figure.1 Evolution Path of Safety Accident

When the system failure occurs, the system security risk also ensues, and it evolves in the system. The system where the fault exists will shift to another state to some extent, at this time, the system usually has the monitoring and detection mechanism to protect this abnormal state from becoming the hazard located at the system boundary. If the protection is missing or invalid, the system failure may evolve into a hazard. If existing hazards have not been found, meanwhile protection is missing or invalid, the hazard at the boundary of the system may cause potential safety accident of casualties under certain conditions.

3. Security

3.1 Concept of Security

ISO/IEC 27002 defines security as "keeping information confidentiality, integrity, and availability; which can also include authenticity, verifiability, non-repudiation and reliability and so on. Therefore,

security is mainly aimed at the usability, confidentiality, and integrity of the system, and prevents the system from being impaired caused by intentional or malicious external environment factors [5].

The concept of security threats is similar to hazards in safety, and the threat is a potential factor or event which potentially damage institutions and their assets [6]. When there are some security threats, the attackers can achieve the aim of malicious attacks with the vulnerabilities of the system.

The direct consequence of security accidents is the steal and destruction of resources and information in the system. If these resources and information are further utilized, which may reveal security-related information and even affect the abnormal execution of the system functions. The improper execution of information leak and system functions can cause damage to the system itself and the environment. Figure 2 shows a comparison relationship between security, safety in incentives (malicious attacks and unforeseen accidents) and consequences.

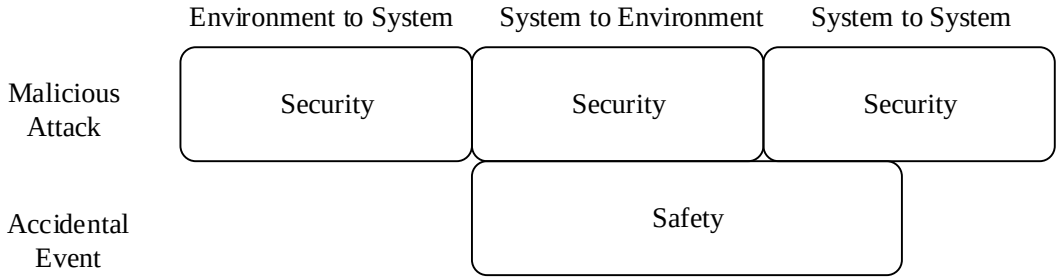

Figure 2 Relations between Safety and Security with System/Environment/Incentives

Similarly, taking the ATP system in the CBTC system as an example, it is required that information of maximum speed limit of the ATP system cannot be changed and destroyed by the unauthorized operation. Otherwise, changes of this kind of security information, such as the increase of maximum speed limit, and it may make the system to cause accidents while system exercising its normal function. The reduction of speed limit may lead to frequent emergency braking of trains, the increase of speed limit may cause the train to overs peed and traffic accidents occur in serious cases. It can be seen that the threat of security to the operational security of rail transit cannot be ignored.

3.2 Evolution Path of Security Risk

As can be seen from the type of security attack, security incidents start from the vulnerability of the system, launching malicious attacks on the system specifically, and their main purposes are to destroy or use system function and steal information of the system. Similarly, the evolution path of security accident can be illustrated by the flowchart shown in Figure.3.

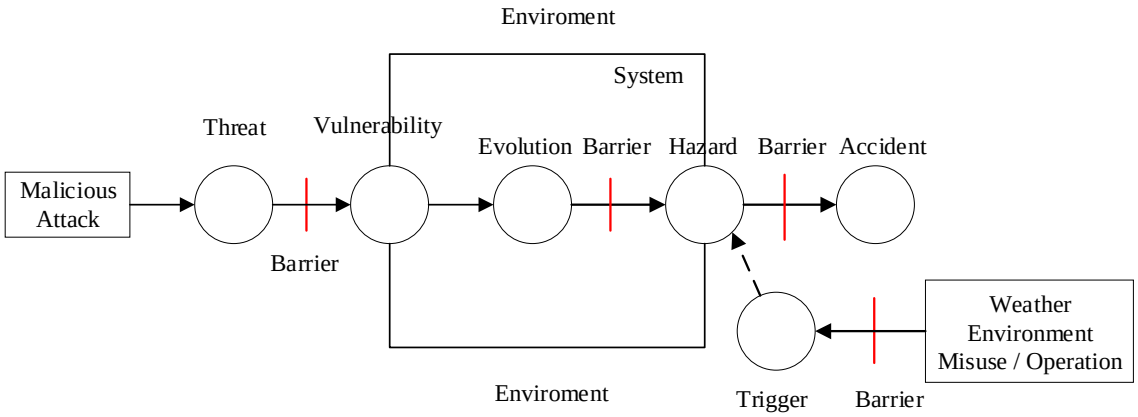

Figure.3 Evolution Path of Security Accident

The security attacks are intentional and malicious attacks, so the external malicious attacks are the sources of security accidents. Systems usually use firewalls and other means protect and control common malicious attacks, but if lack control means or attackers break and bypass the control means, the attacker can scan and take advantage of system vulnerabilities to launch malicious attacks. After malicious attacks happened, the system state transforms, then monitoring and protective measures

should be in the system to prevent the system from further evolving hazards. When protective barriers are absent, bypassed or fail, the hazard of system boundary is formed. At this time, the hazard is almost indistinguishable from the hazard of safety, under certain conditions; and the hazard can develop into safety accidents.

From types of accidents, in addition, "potential casualties condition" caused by safety, security threat can also cause safety accidents cause by information leak and use.

3.3 Relations Between Safety and Security

It can be seen from the risk evolution path that the differences and similarities between the two have the integration possibility. Figure.4 shows the evolution path of the two accidents and their relationship with the environment and system simultaneously. It can be seen that the main difference of evolution paths of the two is the starting point, and the evolution path after fault or attack is similar.

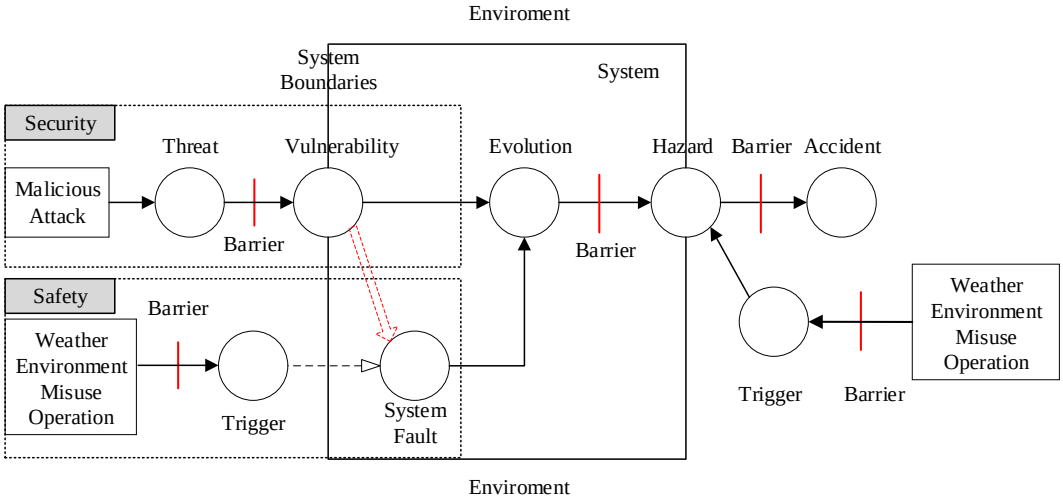

Figure.4 Comparison of Evolution Paths of Security Accidents and Safety Accidents

Security does not come from random, unexpected failures within the system, but come from malicious behavior outside the system. After the attack occurred, the evolution process of security risk in the system is determined by the system characteristics and can cause the hazard of the accident, the two are almost identical. For example, an over speed protection failure accident may be caused by the functional fault of a key control system, or it may be because attackers shut down the function. When the function is closed, "over speed protection function shut down" may become result in accident hazards, regardless of the hazards from the safety and security, the results are the same.

It can be found from Figure.4 that the safety and security analysis can be connected via one link: the "weak link" part of evolution paths of security risks can connect with "system failure" safety, as shown in the red arrow. When a malicious attack occurs, the attacked target mostly starts with a defect and failure state of the system function. The analysis path of security can be as shown in the figure based on this idea; part and safety path merge after entering the system. In this way, as well as taking advantage of mature results in the security field and dig deeper into the security threats, determine the effect of security on safety, and the repetitive work in the process of safety analysis can be reduced as well.

4. Comprehensive Analysis of Safety and Security

The methods of system safety modeling usually only consider the random fault of equipment and software, and the analyses of the system security usually only consider the attack target of malicious attack behaviors. In this paper, an extended fault tree analysis method based on fault tree and attack tree structure is proposed, and a comprehensive analysis method of safety and security is carried out.

4.1 Integration of Fault Tree and Attack Tree

4.1.1 Safety Analysis Based on Fault Tree

As a safety analysis method, FTA (Fault Tree Analysis) uses logical deduction to identify and evaluate system hazards from top to bottom. It is a world-recognized simple and effective method to analyze system reliability and safety.

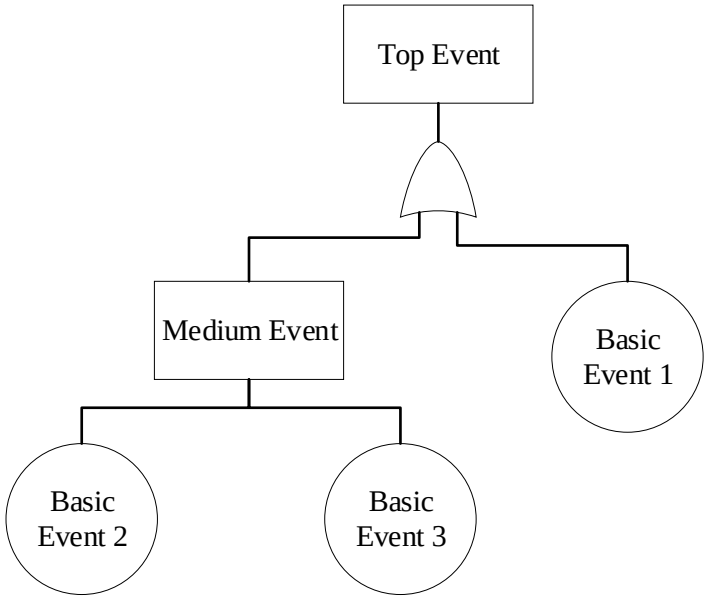

Figure.5 Example of a Fault Tree

When fault tree is used to analyze system security problem, first of all, a system's most unexpected events need to be found, such as the important function failure of the system, the safety of device use, as the top event of the fault tree, namely analysis target. Then according to the system structure and relationship, from top to bottom, layer by layer analyze top event caused by various factors and causes, establish a logical relationship with logic gates and complete fault tree model. The structure of the fault tree is formed by some basic symbols. Figure.5 shows an example of a fault tree.

4.1.2 Security Analysis Based on Extended Attack Tree

Attack tree modeling is a widely used risk analysis method in the security field. The attack tree is inspired by the fault tree in function security and describes the formation process of attack, which is a graphical modeling and analysis method. The root node of the attack tree represents the attacker's final attack goal, and the leaf node represents the specific attack event. The attack tree is generally used to describe the process of security threats and possibly implemented security attacks of the information system.

There are multilevel nodes for attack tree, including root and leaf nodes. The root node represents the attack target, the leaf node represents the method to achieve the target, the leaf node represents the method to achieve the attack goal, the node between the root node and the leaf node represents the intermediate state or sub-target of the attack. This research adopts an extended attack tree model proposed by Masera and Nai, this model not only describes the attack means and path, and the weak link and the specific attack condition of system is added to the model, the nodes in the system are divided into vulnerability node, assertion node, and operation node, and provides a clearer description for security attacks [7].

The vulnerability node (vulnerability) - describes the vulnerability of the system, such as a vulnerability of the 802.11 protocol.

The operation node (operation) describes the operations performed by attackers or authorized persons, such as attacker starting DoS (Denial of Service) attack.

The assertion node (assertion) is the step that describes any assumption, result, or request steps in the attack process, for example, the users have authority X.

The extended attack tree, which is made up of three kinds of nodes, is from system vulnerability, attack condition, attacker's operation three aspects; more comprehensively describes cause and attack behavior of security attack. In the extended fault tree, the vulnerability node is marked with ellipse; operation node is marked with hexagon; the assertion node is marked with rectangle. Figure.6 shows an extended attack tree example.

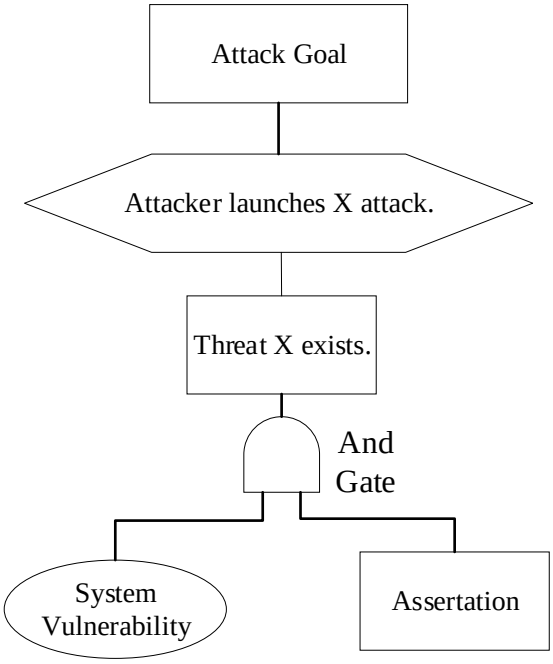

Figure.6 Example of an Extended Attack Tree

Each attack has a final goal or a final motivation. For example, the ultimate goal of DoS attack network server is to prevent someone from obtaining the information provided by this network server. This ultimate goal can be defined as the goal of the attack tree. The structure of the attack tree can also be regarded as a series of lower-level attack trees, which is called a micro-attack tree or meta-attack tree in the definition of the model.

4.1.3 Comprehensive Analysis Based on Extended Fault Tree

The fault tree and the extended attack tree are introduced earlier (it is called the attack tree later), the integration concept of the two can be introduced below. A complete fault tree describes how a series of events cause the occurrence of the top events, such as bottom-up failure of a component, how after a series of events occur; eventually lead to a system function failure event. Similarly, the attack tree describes how an attack can break through attack entrance, make a breakthrough at detection and protection, and realize the damage to system function. So, when the goal of attack tree is the event of the fault tree, the fault tree and attack tree can be integrated by "the top event of the attack tree is the basic event or intermediate event of the fault tree." this combining point.

In this way, a selected fault tree and a micro-attack tree can be combined with the following steps:

(1) The sub-tree $e_{i\_subtree}$ of the fault tree from the event e_i is separated from the fault tree.

(2) A and B with two inputs or the gate (it is called the merged gate later) are connected to the event e_i, that is to say, e_i is the output of the merged gate.

(3) The micro-attack tree MA_k is connected to the input A of the merged gate. As mentioned earlier, we consider the final goal of the attack tree as an event that occurred when the attack was successfully implemented. In this way, we follow the rules of forming fault tree, that is, namely the input and output of each logic gate should be an event.

(4) The goal of the micro-attack tree MA_k is modified to "successfully attack and cause e_i to occur." In this way, we avoid the condition that the input and output of the merged gate are the same events.

(5) The fault sub-tree $e_{i\_subtree}$ as the input B of the merged gate to complete the merge of the fault tree and attack tree.

This formed fault tree is called extended fault tree, as shown in Figure 7 below. The micro-attack tree also needs to be further transformed to complete extended fault tree with consistent format due to the difference of the symbol. It can be found that the process of identifying the micro-attack tree based on the fault tree event is also the process of identifying the security threat, and the fault tree event provides a new clue for the security analysis.

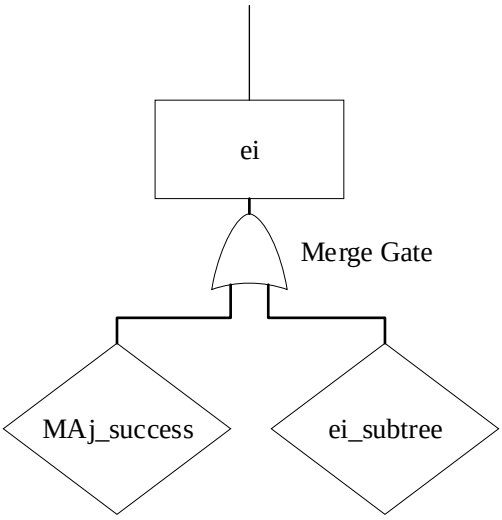

Figure 7 Extended Fault Tree

4.2 Probability Calculation of Top Event of Extended Fault Tree

The events in the fault tree all have a probability value, as long as you know the probability of the corresponding leaf node to calculate the occurrence probability of a higher level event.

4.2.1 Influencing Factors of Top Event of Attack Tree

The occurrence probability of the final goal of the attack tree is determined by the every leaf node of the attack tree. Among them, the vulnerability node and assertion node depend on the system's own property, and the probability of operation node depends on the attribute of the attack behavior. The probability of the occurrence and success of the attack is influenced by various factors, such as attack motive, attack resources, environmental factors, and the subjective probability of the elements that constitute the attack tree. In the actual quantitative calculation, due to the lack of a large number of objective security attack data, these probabilities are usually determined according to experts' opinions.

4.2.2 Probability Calculation of Top Event

The occurrence probability of the top event of the extended fault tree can be calculated based on the previous series of definition, analysis, calculation, integration, the probability calculation of the extended fault tree will consider the intermediate events caused by malicious attacks from the security perspective. This paragraph takes the fault tree used in the traditional CBTC system safety analysis as an example to show the probability calculation method of the extended fault tree.

Figure.8 shows the fault tree [8] of a typical CBTC system on mobile authorization MA calculation function failure under the ZC switching scene. It can be seen from the figure that how the top event "MA is longer than actuality" is logically related to low-level events. First, the MA exception may be calculation error, code error or communication error; calculation error and communication errors may be caused by functional failures of other subsystems or devices. The occurrence probability of E2, E5, E7 and E8 event underlined in the figure are known, and other probabilities need to be calculated according to their relationship with the basic events. These probabilities are usually calculated based on reliability properties of a component in security analysis, namely Mean Time between Failure (MTBF). There is no underline to show the calculation probability.

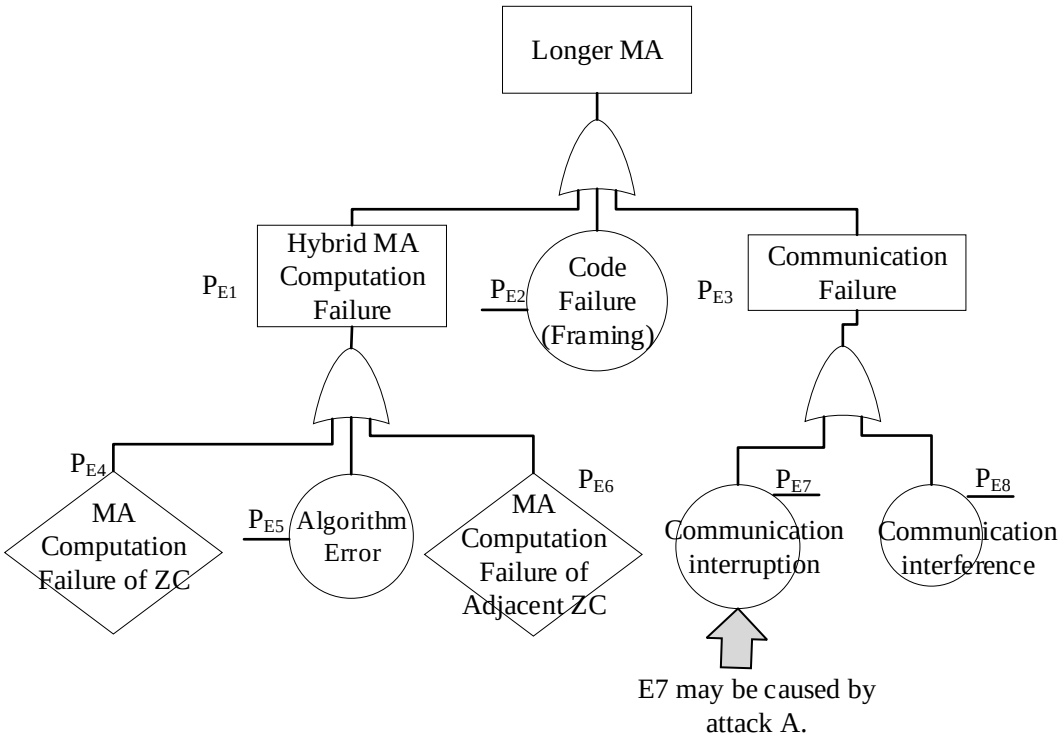

Figure 8 Fault Tree Example - MA is Longer than the Actual Length

According to the previous analysis, the intermediate event or the basic event of the original fault tree may be the top event of the attack tree in the extended fault trees. The intermediate event and basic event of the fault tree may be caused by malicious security attacks in this example. Here, only E7 "communication interruption" as the possible output of an attack tree is analyzed, and show the usage of the extended fault tree. In order to calculate the probability of the top event of the extended fault tree, the occurrence probability of E7 must be calculated.

First, the extended fault trees need to be constructed based on the previous method.

The E7 communication interruption event may be caused by malicious attacks. It can be seen from the previous definition that there should be an attack tree, and it contains all possible attack behaviors that can cause E7 occur. From the perspective of security, the communication interruption event may be because attackers launch network attack, resulting in the network channel resources nervous or normal communication is disturbed by other signals and can't normally transmit; this kind of attack can be called DoS attack.

In this way, one attack tree which takes "communication interruption" as the attack goal can be established. The form of attack tree expanded by Figure 9 shows the attack process which aims at E7 communication interruption. The vulnerability is the vulnerability of openness and communication protocol WLAN network in this attack tree, which causes other signals access the network, assertion is that attackers are capable of launching DoS attacks and wireless bandwidth is limited, the operation is that attacker launch DoS attack. The attackers find system vulnerability V1 "other data can access the WLAN network, meanwhile the system property make the assertion" wireless bandwidth limit" is established, the attackers make assertion "attackers have the ability to launch DoS attack" established, these three conditions form "network services can be interrupted" assertion, it's also a threat. When attackers launch attack operations, it is possible to achieve the goal of "communication interruption".

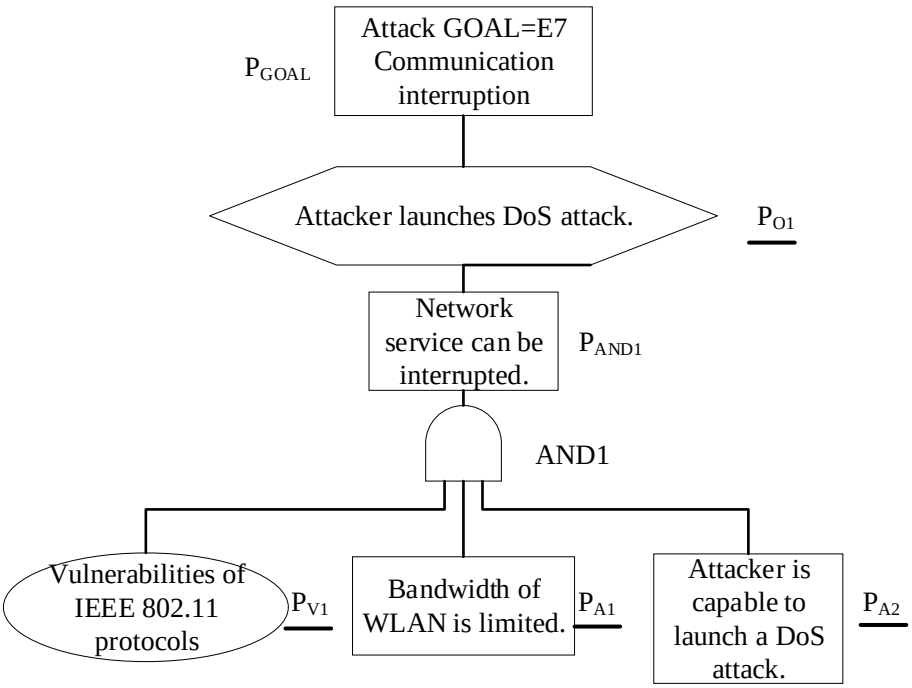

Figure 9 Extended Attack Tree of Communication Interruption

The only difference between the attack tree and standard fault tree shown in Figure.9 is: all the probabilities of underlying events are known in the fault tree, but the operation nodes of the attackers in the attack tree, as an intermediate node, its probability is known as well. In order to ensure that standard structure of fault tree "all the underlying event probabilities are known and the intermediate event probabilities are unknown", the logical structure of the operation node is transformed into the equivalent structure shown in Figure.10.

In.Op1 represents the input of operation 1 in the figure before transformation, and Out.Op1 represents the output of operation 1, and P_{O1} represents the occurrence probability of an operation. In the transformed graph, operation 1 is decomposed into an assertion node and an operation node connected by a gate in the figure after transformation.

Operation node with known probability after transformation has become bottom event without branch, and it conforms to standard structure of fault tree, all the operation nodes in the attack tree can carry out this transformation, the transformation of attack tree is shown in Figure.11. The forming attack tree can also be called a micro-attack tree; a micro-attack tree can be directly used for the attack goal with the same condition.

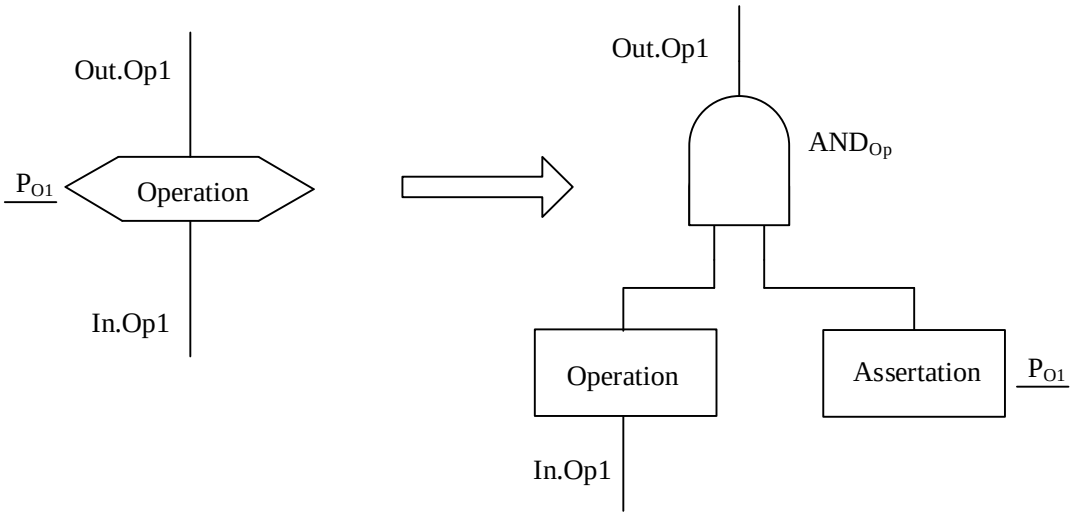

Figure 10 Transformation of the Operation Node

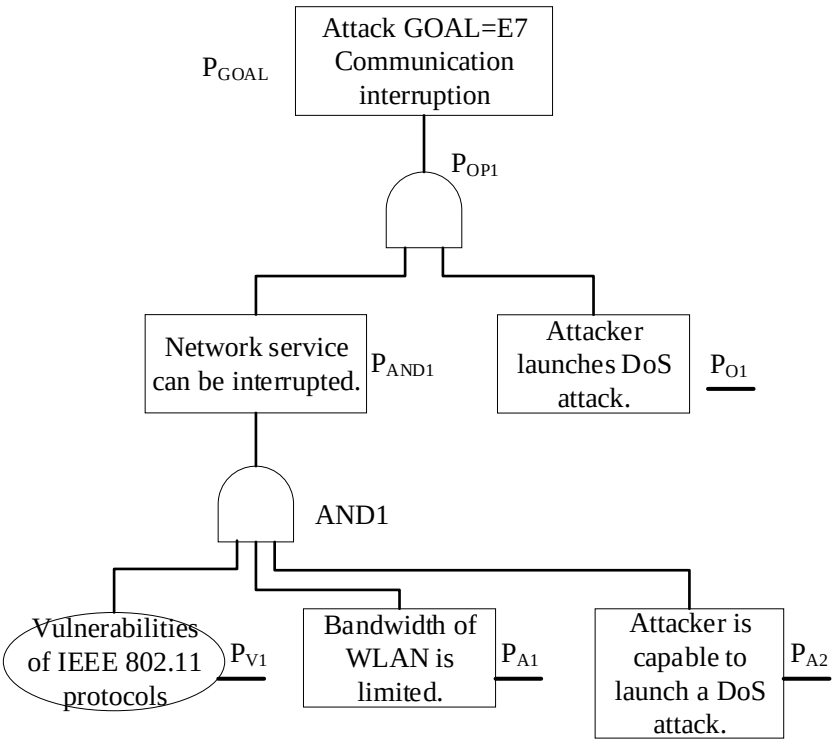

Figure.11 Transformed Attack Tree

After the transformation of the attack tree is completed, the event E7 in the fault tree can as the attack tree of the final goal, and it can be integrated into the structure of the fault tree, and the extended fault tree is formed, as shown in Figure.12. The original event E7 in the fault tree and the micro-attack tree OP1 of the security branch are connected by one or gate, the M1 "communication interference" event after an output together and one merge (merge). At this time, the communication interference M1 sub-tree contains security and functional security analysis. The occurrence probability of the top event of the extended fault tree will change, and the contribution of malicious attacks in security will also be reflected in the extended fault tree.

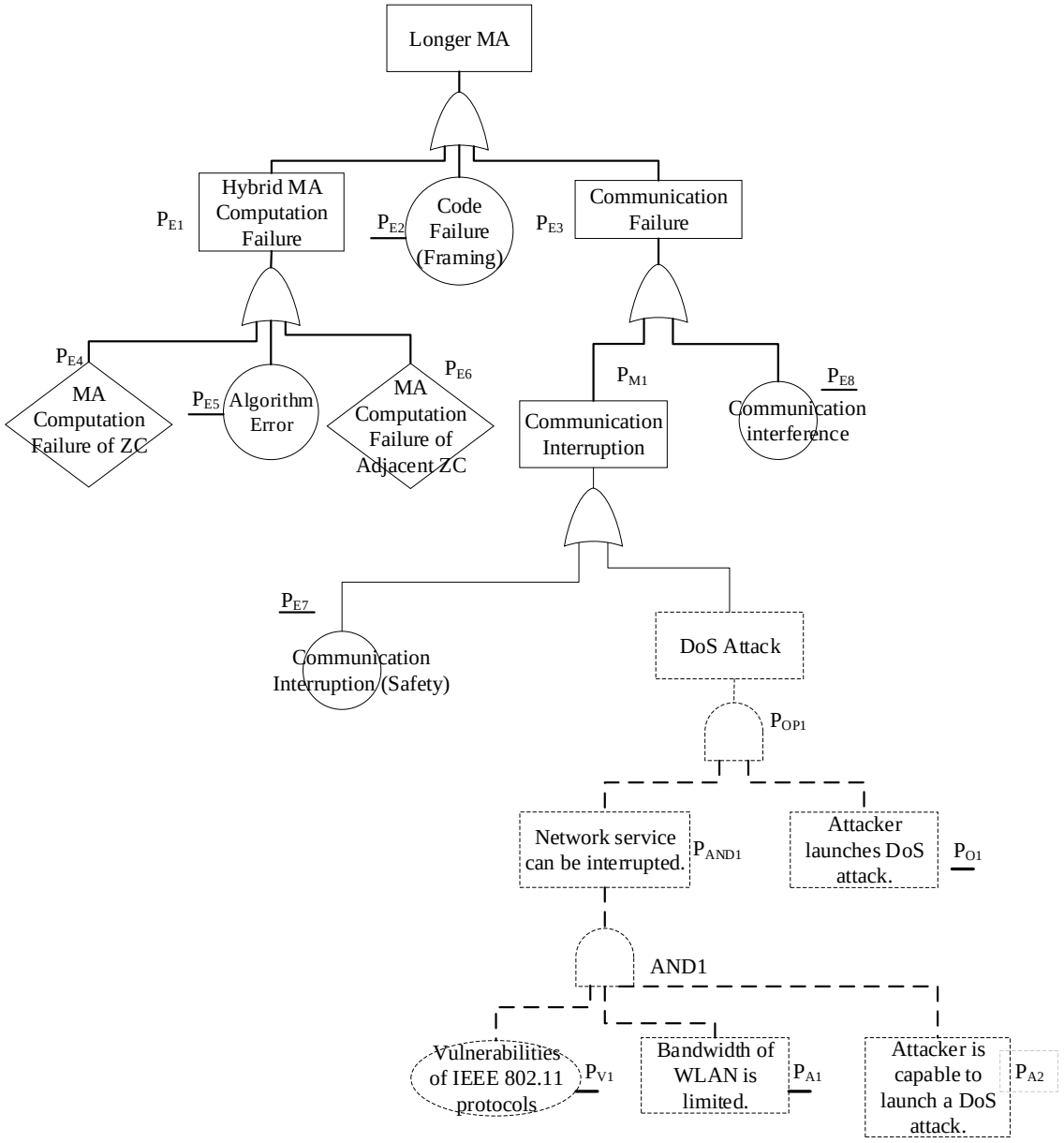

Figure.12 Extended Fault Tree - MA is Longer than the Actual Length

5. Conclusion

The security problems of industrial control system have become increasingly prominent in recent years, but the theory and method of security analysis for the train operation control system of urban rail transit have not been formed yet. This paper proposes a comprehensive analysis method of safety and security based on extended fault tree to explore the effect of security attack on system security. This method combines the fault tree describing the security failure logic and the attack tree which describing the security attack behaviors, the fault tree event and the top event of attack tree as the joint points, the analysis model based on extended fault tree is established.

The comprehensive analysis method proposed by this paper provides a new approach for the security of urban rail transit. Security is incorporated into analysis framework of safety, which provides more comprehensive threats identification and vulnerability analysis for the system. The approach has guiding significance to improve the risk management and coping mechanism of urban rail transit operation. The attack tree can be directly connected to the fault tree and complete the establishment of the model by simple consistency adjustment, and the method is visual and simple.

References

[1]. Wei Yijun. The 32 cities in China's mainland have opened rail transmit- the total operation mileage ranks first in the world [EB/OL].
http://news.sina.com.cn/o/2017-12-01/doc-ifyphtze3230087.shtml,2017-12-1/2017-12-20.

[2]. IEC. IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems[S]. General Requirements, 2010: 12-25.

[3]. CENELEC EN 50126: Railway applications-The specification and demonstration of Reliability [J]. Availability, Maintainability and Safety (RAMS), 1999.

[4]. Network Rail Yellow Book-Engineering Safety Management Issue 3[R]. London: Railtrack PLC, 2000:9-12.

[5]. ISO/IEC 27002. Code of Practice for Information Security Management[S], International Organization for Standardization, 2007.

[6]. RSSB. Guidance on Hazard Identification and Classification[S]. Rail Safety and Standards Board Limited, 2014: 19-20

[7]. Nai Fovino I, Masera M, Cian ADe. Integrating cyber-attacks within fault trees [J]. Reliab Eng Syst Saf 2009; 94(9):1394–402.

[8]. Yan Fei, Zhao Xianqiong, Tang Tao. Research on functional safety analysis and modelling method[C], Proceedings of China system simulation technology and its application the academic annual conference, Beijing 2011, Beijing: China System Simulation Association, 2011: 115-160.