Journal of the Korea Academia-Industrial cooperation Society
Vol. 22, No. 9 pp. 35-43, 2021

https://doi.org/10.5762/KAIS.2021.22.9.35
ISSN 1975-4701 / eISSN 2288-4688

A Quantitative Risk Assessment for Public Commercial Unmanned Aerial Systems

See Yeon Kim[1], Alfonsus Julanto Endharta[1*], Jongwoon Kim[2]
[1]R&D Center, Nemosys Co.
[2]CEO, Nemosys Co.

공공 상업용 무인 항공 시스템의 정량적 위험도 평가 연구

김시연[1], 엔드하르타 알폰수스 주란토[1*], 김종운[2]
[1]네모시스(주) R&D센터, [2]네모시스(주) 대표이사

Abstract This study proposes a quantitative risk-assessment method based on problem tree analysis to estimate the safety-related hazard risk in the operation of a commercial unmanned aerial system (UAS). The basis of the problem tree analysis is Fault Tree Analysis (FTA) and Event Tree Analysis (ETA). A crash accident of a UAS was used as an example of a safety-related hazard, and the possible causes of the crash were listed. The occurrence probabilities were derived through FTA, while the consequences of the accident were analyzed through ETA. The risk of the crash accident was assessed, and the general procedure can be considered in a pre-flight risk assessment before operation. A crash accident due to aircraft loss of communication (LOC) was used as an illustration. Aircraft LOC can be caused by propulsion-system failure or malfunction, weather, wind, wind shear or turbulence, vehicle degradation, and electromagnetic interference (EMI). The scenarios for ETA were arranged, and the accident criticality was analyzed.

요 약 본 연구에서는 상업용 무인 항공 시스템(UAS, Unmanned Aircraft System) 운용 시 안전과 관련된 위험요인의 위험도 추정을 위한 문제 수목 분석에 기초한 정량적 위험도 평가 방법을 제안하였다. 문제 수목 분석의 기본은 결함 수목 분석(FTA, Fault Tree Analysis)과 사건 수목 분석(ETA, Event Tree Analysis)이다. UAS의 추락사고는 안전과 관련된 위험사건의 예로 본 논문에서 사용되었으며 추락을 발생시킬 수 있는 위험요인 중 하나의 위험요인의 원인을 나열하였다. 발생확률은 FTA를 통해 도출되며, 사고 결과는 ETA를 통해 분석된다. 무인 항공 시스템에서 발생할 수 있는 사고의 위험도 평가를 위한 절차를 제안하였으며, 운용 단계에서 운용하기 전에 사전 비행 위험도 평가 시 적용할 수 있다. UAS 통신 끊김(LOC, Loss of Communication)으로 인한 추락 사고가 예로 사용된다. UAS의 LOC은 추진 시스템 고장 또는 오작동, 날씨, 바람, 바람 전단 또는 난류, 차량 성능 저하 상태 및 전자파 간섭(EMI, electromagnetic interference)에 의해 발생할 수 있습니다. ETA에 대한 시나리오를 선정하고 사고의 치명도 또는 리스크를 분석한다.

Keywords : Crash Scenario, ETA, FTA, Risk Assessment, UAV

본 연구는 국토교통과학기술진흥원의 지원으로 수행되었습니다. (과제번호 21DPIW-C153653-03)
*Corresponding Author : Alfonsus Julanto Endharta(Nemosys Co.)
email: alfon@nemosys.kr
Received August 6, 2021 Revised September 2, 2021
Accepted September 3, 2021 Published September 30, 2021

1. Introduction

Unmanned aerial system (UAS) is structural system which consists of an unmanned aerial vehicle (UAV), a ground-based controller, and a network communication system. UAS technology covers everything from the aerodynamics of the drone, materials in the manufacture of the physical UAV, to the circuit boards, chipset and software, which are the brains of the drone [1]. There are many types of UAV (or drones) and the popularity of drones started increasing due to the feature of the aerial photography and videography in the system. Such UAVs are usually small in size and owned by individuals. As the needs of mobility and the technology of automation in service industry increases, the features on UAS improves and the size of the UAV increases to fulfill the feature capabilities. Larger UAV with autonomous flight operation program is considered for commercial with various features, such as firefighting, emergency surveillance, and postal delivery in difficult access area. U.S. Federal Aviation Administration (FAA) Aerospace reported that there were 1,136,513 recreational UAVs and 488,043 commercial UAVs registered in 2020 and analyzed that the annual growth rates are 4.5% for the recreational UAVs and 32%for the commercial UAVs [2].

As the growth of the UAV operation improves rapidly and more features and distinct applications among UAVs develops in the future, it is crucial to manage the safety risk of all types of UAV operations. Although the existing airspace regulation is used as the base of the aircraft safety management system, the appropriate safety policy or risk management requires further study on the safety-related hazards due to the insufficient incident data. As more varied applications and features are considered in the development of the UAV, the more safety-related hazards should be considered, and the risk assessment should be studied for the corresponding UAV. Belcastro et al. studied the hazard identification and analysis for UAS operation [3]. The commercial and public small UAV (less than 25 kg) was considered in the analysis and summarized the list of hazards based on the historical incidents collected from various sources including government accident reports ad media reports. Barr et al. proposed a preliminary safety risk assessment of small UAS and considered two approaches: qualitative approach and probabilistic model-based risk estimation approach [4].

In this study, a risk assessment method based on a problem tree is proposed to evaluate the safety risk of a commercial UAS. The problem tree is the combination of Fault Tree Analysis (FTA) and Event Tree Analysis (ETA). Problem tree analysis is central to many forms of project planning and is well developed among development agencies. Problem tree analysis (also called Situational analysis or just Problem analysis) helps to find solutions by mapping out the anatomy of cause and effect around an issue in a similar way to a Mind map, but with more structure [5].

In this study, the problem tree models the possible causes and effects of an UAS accident. FTA considers the possible chain of accident causes, such as the UAV component failures and the errors of the component failure prevention method applied in the design. ETA considers the external factors, especially which are unable to control or more unpredictable, which may affect the accident severity in various possible scenario.

The paper is organized as follows. Section 2 briefly explains the risk assessment method. Section 3 shows the proposed problem tree analysis, including FTA and ETA. Section 4 shows the sample illustration of the proposed method by considering a crash accident of a delivery service UAS. Section 5 concludes the paper.

2. Risk Assessment

Risk assessment process is performed to provide assurances that the risks associated with the operation of UAS have been managed to acceptable levels. The risk assessment can be used to show the important safety risks and issues, to identify the improvement opportunities, to make the recommendations on how to prevent or to mitigate the future problems and to identify the safety requirements to include in the system requirements and performance documents. Risk assessment method is universally applied in any system to improve the system operation quality and safety. Since the international standard ISO/TC 20/SC 16 which covers the safety-related management for UAS is under development, any other international standard comprising a safety management and a risk assessment process, such as ISO 12100, ANSI/RIA R15.06, MIL-STD-882E, and ISO/TR 14121-2, can be considered.

In general, a risk assessment comprises risk identification, estimation, and evaluation. Risk analysis is a systematic and structured process, which can be represented as in Fig. 1.

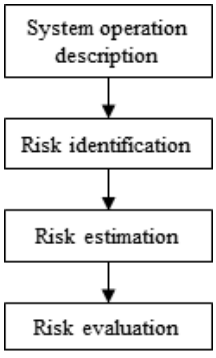

Fig. 1. Risk assessment procedure

Before the risk assessment is performed, the target system, the risk assessment range, and the objectives should be defined clearly. For an illustration of the risk assessment in this paper, we consider the autonomous commercial UAV for rural area postal delivery. The safety related risks will be analyzed, and the objective is to define the safe design of UAV which satisfies the acceptance level.

Based on the defined system and analysis description, the system operation should be clearly described so that the list of undesired or hazardous situations can be obtained thoroughly. The undesired or hazardous situations are regarded as risks which should be assessed. The safety related hazardous events during UAS operation are considered. Based on FAA, the hazards related to UAS operation include the collision with airplane, birds, and buildings.

2.1 Risk estimation

The criticality of the safety hazard occurrence is defined as the safety risk. Generally, the criticality is the combination of the occurrence probability and the severity of the hazard. The risks can be estimated quantitatively or qualitatively. The qualitative risk estimation can be performed through hazard analysis, where the risks are estimated through expert experience. The quantitative risk estimation can be performed through FTA and ETA. The values needed in the FTA and ETA can be obtained through reliability prediction, failure data analysis, failure data library, and expert experience. FTA is used to estimate the occurrence probability, while ETA is to estimate the severity of the hazard occurrence. The details on FTA and ETA can be seen in the Subsection 3.1 and 3.2.

2.2 Risk evaluation

After the occurrence probability and the severity are estimated, the hazard risk (criticality) is estimated. Based on the risk estimation, the system safety is evaluated based on the risk evaluation. If the system risk is within the acceptance range, the system is classified as a

safe system. Otherwise, one or more safety measures and mitigation methods must be applied in the system until the system safety reaches the safety acceptance level.

3. Problem Tree Analysis

The developed problem tree includes the fault tree and event tree. The fault tree represents the possible causes of an accident, while the event tree represents the possible outputs and the risks of the accident. The possible causes and effects need to be clear to effectively show the relation between the causes and effects of the hazardous event. Problem tree analysis diagram can be seen in Fig. 2.

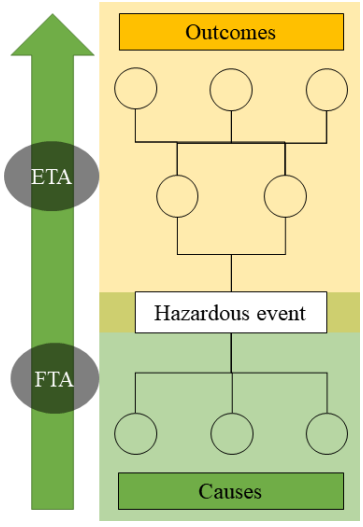

Fig. 2. Problem tree analysis illustration

3.1 Fault Tree Analysis (FTA)

FTA is an in-depth analysis technique to identify all possible combinations of failure which can lead to the loss of the system integrity and is commonly used in Reliability, Availability, Maintainability and Safety (RAMS) analysis. FTA is a top-down analysis through various lower levels of the design until the occurrence probability of the top event (the hazardous event) can be predicted.

FTA was initially used by US Air Force on the weapon system according to Clemens[6] and Javadi et al.[7]. Then, FTA has been considered in reliability engineering in various sectors and companies to improve the system reliability, availability, maintainability, and safety. US Federal Aviation Administration (FAA) published a change to airworthiness regulations for transport category aircraft in the Federal Register FR 5665, adopted failure probability criteria for aircraft systems and equipment, and led to extensive use of FTA in civil aviation[8]. FAA established a risk management policy and hazard analysis in a range of critical activities beyond aircraft certification, including air traffic control and modernization of the US National Airspace System, which led to the publication of the FAA System Safety Handbook which describes the use of FTA in various types of formal hazard analysis.

The diagram of FTA consists of nodes which represents the event causes and gates which show the relationship among the event nodes. While there are many types of gates in FTA, the most common gates in FTA are AND gate and OR gate. More gates can be seen in [9]. When the output event occurs because all input events occur, AND gate is considered. When the output event can occur because one of the input events occur, OR gate is considered to show the relationship. The illustration of AND gate and OR gate is shown in Fig. 3. After all input events and the occurrence probability values are estimated, the occurrence probability of the top event (hazardous event) can be estimated.

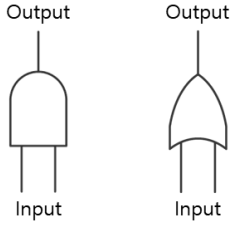

Fig. 3. AND gate (left) and OR gate (right)

3.2 Event Tree Analysis (ETA)

Different from FTA, ETA is an inductive analysis technique which shows all possible outcomes resulting from an accidental (initiating) event, considering whether installed safety barriers are functioning or not, and additional events and factors[8]. By analyzing the hazardous events from FTA, ETA can be performed to identify all potential accident scenarios and sequences in a complex system. Design and procedural weaknesses can be identified, and probabilities of the various outcomes from an accidental event can be determined.

ETA is also illustrated as a diagram and the sample general diagram can be seen in Fig. 4. After all occurrence probability of the events and factors, such as the probability that the barrier does not function, in the considered scenario are defined, the probability of all outcomes can be estimated through the multiplication of the probabilities of the events and the factors. In addition, based on the experts, past data, or the risk acceptance criteria, the severity of each outcome can be defined. Then, the risk (criticality) can be estimated by multiplying the occurrence probability and the severity of the outcomes.

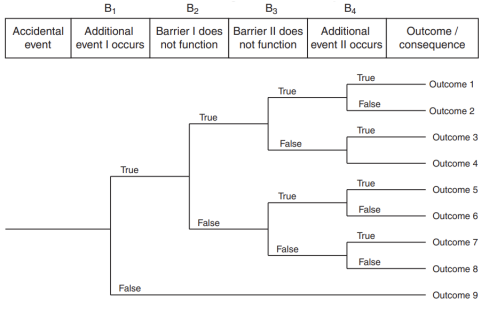

Fig. 4. General ETA diagram (Rausand and Hoyland, 2004)

4. Case: UAS for Delivery Service

We consider the hazards summarized in Belcastro et al.[3] which related to the UAS for delivery service. Based on Belcastro et al.[3], the hazards considered for UAS for delivery service can be seen in Table 1.

Table 1. Hazards related to UAS crash accident

Hazard	Possible Factors
Aircraft loss of control (LOC)	• Propulsion system failure/ malfunction • Weather (rain, snow/ icing, thunderstorms, etc.) • Wind/ wind shear/ turbulence • Vehicle degraded condition • Electromagnetic interference (EMI) • Unsuccessful launch • Flight Control system design/ validation errors/ inadequacy • Flight Control system SW implementation/ verification error/ inadequacy • Unexpected obstacle encounter resulting in unstable/ aggressive avoidance maneuver • Bird strike • Others
Aircraft fly-away/ geofence non-conformance	• Loss of communication/ control link • Erroneous waypoints • GPS failure/ errors • Autopilot error/ malfunction • Pilot error
Loss communication/ control link	• EMI at vehicle • Signal obscureness • Frequency/ BW overlap • Failure in ground control system (GCS)
Loss of navigation capability	• Onboard navigation system failure/ malfunction • Loss/ erroneous GPS signal • Ground station set-up error
Unsuccessful landing	• Unstable approach • Remote pilot error
Unintentional/ unsuccessful flight termination	• Pilot error in flight termination • Flight termination system error/ failure/ malfunction • Unexpected wind/ weather • Failure on command link from operator
Failure/ inability to avoid collision mid-flight	• Pilot error/ poor judgement • Wind/weather

Hazard	Possible Factors
	• Erroneous waypoints • Inaccurate GPS signal • Inadequate navigation/ tracking
Hostile remote takeover and control of UAS	• Lack of data/ cyber security by operator
Rogue/ noncompliant UAS	• Inability by traffic management system to stop rogue/ noncompliant operation of UAS • Inability to detect/ contain rogue UAS • Ineffective methods to detect/ contain rogue UAS
Erroneous autonomous decisions/ actions by UAS	• Inadequate sensor integrity management for critical decision-making • Inadequate system validation and software verification

Most of the hazards in Table 1 may result in the mid-air collision with another UAS, mid-air collision with manned aircraft, crash into building. Obstacles and injuring people, and the crash debris injuring people on the ground or causing fire.

In this study, we focus on the aircraft loss of control (LOC) and consider it as the hazardous (top) event in the FTA. The factors related to system, such as the system or component failures, malfunctions, and errors, are classified as the internal factors and are considered in the lower levels of the FTA because such factors are minimized through the reliable system design and the occurrence probability is less erratic at each operation. While the external factors, such as the weather and bird strike, are considered in the ETA since the occurrence probability is usually different at each flight operation depending on the time and place.

The internal factors are the propulsion system failure and the flight control (FC) system failure. The propulsion system failure is affected by the failure of the motors, electric speed controller (ESC), and the propeller. The FC system failure is affected by the hardware (receiver module, transmitter module, and antenna) failure and software error.

The failure rate defined by the product manufacturer, obtained from the historical data in the field, or from the similar projects can be used as the input values for the corresponding component failure probabilities in the FTA. Thus, through FTA, the aircraft loss of control (LOC) occurrence probability can be estimated. In this study, for illustration only, we assume the failure probabilities shown in Table 2 for the FTA. As shown in FTA diagram in Fig. 5, the top event (aircraft LOC) occurrence probability is 0.097083.

Table 2. FTA input example

System	Component	Failure probability
Propulsion system	Motor	0.01
	ESC	0.01
	Propeller	0.04
	Battery	0.01
Flight Control (FC) system	Receiver	0.01
	Transmitter	0.01
	Antenna	0.01
	Software	0.001

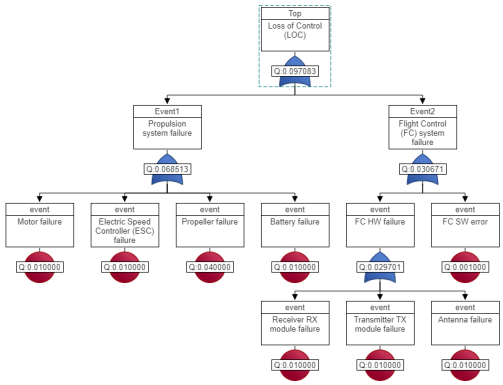

Fig. 5. FTA diagram for crash due to aircraft LOC

The occurrence probabilities of the external factors are sometimes difficult to decide, more erratic, and varied depending on time and place. Thus, we prefer to make a possible scenario by combining all possible events.

We know that before we fly the UAV, we must

check the environment requirements, such as the weather is clear, the wind speed fits the UAV flight requirements, there is no wind shear or sudden gust, and there is no birds. Thus, we assume that if the weather suddenly changes into raining, snowing or storm, if the wind speed suddenly increases during the flight, if there is wind shear which is undetected before the flight, and if there are birds suddenly flying nearby, the crash occurrence probability improves significantly. Therefore, for each possible event, we need to estimate the probability of these changes and the probability of crash occurrence from these events. For illustration, we consider the possible events for each external factor which affects the possibility of the UAV crash as shown in Table 3. Four possible events in the sudden weather change, three possible events in the wind speed change, two possible events in the wind shear or gust possibility, and two in the bird visibility. Based on this illustration sample, there are 4 × 3 × 2 × 2 = 48 scenarios.

Table 3. ETA input example

Factor	Events	Value	Crash prob.
Sudden weather change probability	To thunderstorm	0.05	1
	To snowing	0.05	1
	To raining	0.2	1
	None	0.7	0
Wind speed change probability	〉10 m/s	0.05	1
	5 – 10 m/s	0.15	0.5
	No change	0.8	0
Wind shear/gust possibility	Yes	0.5	1
	No	0.5	0
Bird visibility	Yes	0.3	1
	No	0.7	0

We estimate the severity of the crash accident due to the aircraft LOC by expected number of injured person. Table 4 shows the maximum population density per squared km. The location of the UAS operation will determine the criticality (risk) of the crash accident.

Table 4. Maximum population density (persons per km^2)

Area category	Maximum population density (person per km^2)
Congested	500,000
Urban	100,000
Sub-urban	10,000
Rural	100

Fig. 6 shows the partial of ETA diagram considering the scenario and input values in Table 3. If the crash accident scenario is the sudden weather change to thunderstorm during the flight, the wind speed change to more than 10 m/s, there is a possible wind shear or gust, and there are birds in the vicinity, then the scenario occurrence probability is the multiplication of these occurrence probability, which is 0.05 × 0.05 × 0.5 × 0.3 = 0.000375. Based on Table 3, the events in this scenario cause the crash accident, thus, multiply the scenario occurrence probability (0.000375) with the corresponding crash occurrence probability (1 × 1 × 1 × 1 = 1), the crash occurrence probability through the first scenario is 0.000375. The second scenario is that the sudden weather change to thunderstorm during the flight, the wind speed change to more than 10 m/s, there is a possible wind shear or gust, and there is no birds in the vicinity, thus, the crash occurrence probability is (0.05 × 0.05 × 0.5 × 0.7) × (1 × 1 × 1 × 0) = 0.

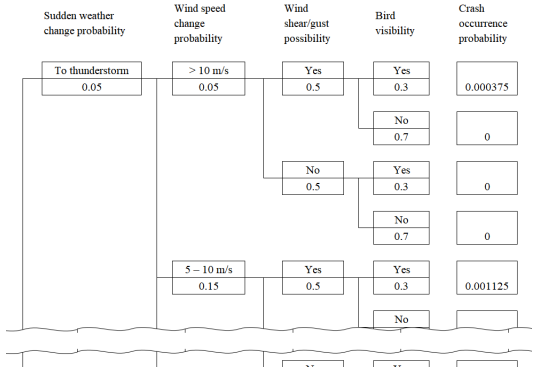

Fig. 6. ETA diagram for crash due to aircraft LOC

Considering all scenarios in the ETA, the crash occurrence probabilities for each scenario and the total of all crash occurrence probabilities represents the overall crash occurrence probability is 0.009. Based on the ETA result, the crash occurrence probability is 0.009. Multiplied by the aircraft LOC probability from FTA (0.097083), the probability that the crash accident due to aircraft LOC is 0.097083 × 0.009 = 0.000873747. Depending on the location of UAV operation, the criticality of the crash accident due to the aircraft LOC is 0.000873747 × maximum population density. Table 5 shows the summary of the criticality per area category.

Table 5. Criticality of crash due to aircraft LOC

Area category	Criticality
Congested	436.8735
Urban	87.3747
Sub-urban	8.73747
Rural	0.087375

Based on the risk assessment result, we can infer that the criticality of the crash accident due to the aircraft LOC is the highest in a congested area and the lowest in the rural area. The result of this example shows that the UAS is safe for used in rural area based on the crash accident criticality level. However, it cannot be generalized for the other hazards and the problem tree analysis should be performed separately for all other hazards.

5. Conclusion

The paper studied a quantitative risk assessment method combining FTA and ETA. A crash accident of the commercial UAS is considered as an illustration. FTA results in the estimation of the crash occurrence probability due to the aircraft LOC and ETA results in the various severity considering the environment (weather, wind, and bird availability) change scenario. The risk assessment result shows that the criticality of the crash accident due to the aircraft LOC is the highest if the UAS is operated in the congested area and the lowest if it is operated in the rural area.

Several research studies can be directed in the future related to this study. One would consider the real UAS and the component failure data for FTA to show the performance of the manufactured UAS. Another is to develop a software which apply the problem tree analysis.

References

[1] F. Corrigan, How Do Drones Work and What is Drone Technology [Internet]. DroneZon, 2020 [cited 2021 Sep. 6], Available From: https://www.dronezon.com/learn-about-drones-quadcopters/what-is-drone-technology-or-how-does-drone-technology-work/ (accessed Sep. 5, 2021)

[2] U.S. Federal Aviation Administration [Internet]. FAA Aerospace Forecast, Fiscal Years 2021-2041. Available From: https://www.faa.gov/data_research/aviation/aerospace_forecasts/ (accessed Jul. 30, 2021)

[3] C. M. Belcastro, R. L. Newman, J. K. Evans, D. H. Klyde, L. C. Barr, E. Ancel, "Hazards Identification and Analysis for Unmanned Aircraft System Operations", *Proceeding of 17th AIAA Aviation Technology, Integration, and Operations Conference*, AIAA Aviation Forum, USA, June 2017. DOI: http://dx.doi.org/10.2514/6.2017-3269

[4] L. C. Barr, R. L. Newman, E. Ancel, C. M. Belcastro, J. V. Foster, J. K. Evans, "Preliminary Risk Assessment for Small Unmanned Aircraft Systems", *Proceeding of 17th AIAA Aviation Technology, Integration, and Operations Conference*, AIAA Aviation Forum, USA, June 2017. DOI: http://dx.doi.org/10.2514/6.2017-3272

[5] ODI. Planning tools: Problem Tree Analysis [Internet]. ODI, 2009 [cited 2021 Sep. 6], Available From: https://odi.org/en/publications/planning-tools-problem-tree-analysis/ (accessed Sep. 5, 2021)

[6] P. L. Clemens, Fault Tree Analysis, 4th Ed., 2002.

[7] M. Javadi, A. Nobakht, A. Meskabashee, September 2011. "Fault tree analysis approach in reliability assessment of power system", *International Journal of Multidisciplinary Sciences and Engineering*, Vol.2, No.6, pp.46-50, Sep. 2011.

[8] H. Haroonabadi, M. Haghifam, "Generation reliability evaluation in power markets using Monte Carlo simulation and neural networks", *Proceeding of 15th International Conf. on Intelligent Systems Applications to Power Systems*, Curitiba, 2009. DOI: http://dx.doi.org/10.1109/ISAP.2009.5352864

[9] M. Rausand, A. Hoyland, System Reliability Theory: Models, Statistical Methods, and Applications, 2nd Ed., John Wiley & Sons, Hoboken, 2004.

See Yeon Kim [Regular member]

• Jan. 2019 ~ current : Nemosys Co., R&D Center, Researcher

〈Research Interests〉
RAMS, Railway

Alfonsus Julanto Endharta [Regular member]

• Feb. 2019 : Sepuluh Nopember Institute of Technology, MS
• Feb. 2016 : Pusan National University, Ph.D
• Mar. 2016 ~ Feb. 2017 : Pusan National University, Researcher
• Mar. 2017 ~ Feb. 2019 : POSTECH, Research Professor
• Mar. 2019 ~ current : Nemosys Co., Principal Researcher

〈Research Interests〉
RAMS, Lifetime Data Analysis, Railway

Jongwoon Kim [Regular member]

• Feb. 1997 : Pusan National University, MS
• Feb. 2003 : Pusan National University Ph.D
• Apr. 2003 ~ Dec. 2005 : Hyundai Rotem
• Dec. 2005 ~ current : Korea Railroad Research Institute, Principal Researcher
• Feb. 2016 ~ current : Nemosys Co., CEO

〈Research Interests〉
RAMS, Railway