FTA and Markov Analysis Comparison Applied to N219 Aircraft Hydraulic System based on Fail to Generate Hydraulic Power

Yoga Yulasmana
Universitas Nurtanio, Bandung, Indonesia

e-mail: **yyulasmana@gmail.com**

Abstract— In general, this paper contained a safety assessment conducted on the N219 Aircraft hydraulic system to ensure that its systems meet the safety requirements. Further, the safety requirements will be established by the aviation authority as a certification basis for satisfying the CASR Part 23 according to the N219 category as a commuter aircraft. To conduct a safety assessment process on this system, this paper follows the process outlined in SAE ARP4761 document. It encompasses Functional Hazard Assessment (FHA), Preliminary System Safety Assessment (PSSA), and System Safety Assessment (SSA). Afterward, this paper will focus on quantitative analysis for SSA process based on fail to generate hydraulic power failure condition. In particular, the quantitative analysis for this process will use Fault Tree Analysis (FTA) and Markov Analysis (MA) to make a comparative evaluation. Since N219 Aircraft still in the phase of getting a Type Certificate, the comparative results obtained from both methods can be taken into consideration in the development of the N219 Aircraft for the military version. Furthermore, the quantitative analysis comparison results from this paper are expected to be applied to other failure conditions due to modification or additional components of the N219 Aircraft existing system.

Keywords— Safety Assessment, Fault Tree Analysis, Markov Analysis, Hydraulic System, Quantitative Analysis

I. INTRODUCTION

The hydraulic systems of an aircraft must be both safe and reliable to be able to fulfill the function for extended periods without risk of failure. N219 itself has a general specification are intended for multi-purpose missions in remote areas and very compatible for military aircraft specification. It's demanding that N219 be operated in semi-prepared airstrips which suitable to conditions in Indonesia's archipelago. It's well-established these specifications are inseparable from braking and steering system which are generated by the hydraulic system. Here become the main excuse the hydraulic system is chosen to be of particular concern in this research paper as one of the systems to be assessed from some attached systems in N219 aircraft.

Currently, a Fault Tree Analysis (FTA) is widely used as safety quantitative analysis method. In this paper also apply a Markov Analysis (MA) into the safety assessment analysis method along with the FTA as comparative data verification and improvement.

II. LITERATURE REVIEW

The following are some literature related to Fault Tree Analysis (FTA) and Markov Analysis (MA) as part of the safety assessment analysis method in this paper.

A failure state of the flight control system is modeled and analyzed by MA and FTA respectively, and the results show that the MA method has a higher accuracy of quantitative

Received August 9th, 2019; Revised August 23rd, 2019; Accepted September 4th, 2019

analysis of the sequence-related events. This method also overcomes the shortcomings of the static analysis features of the FTA [1].

However, as an objective comparison between FTA and MA with each of their advantages and disadvantages will be a particular concern [2].

The advantages of FTA are complex systems can be handled by decomposing the systems into separate parts (each with their own fault tree), the model can be understood by non-specialists. Nevertheless, the disadvantages of FTA are generally aimed at one specific top-event so different models are needed for different top events like safe and dangerous system failures, sequential events cannot be modeled using traditional fault trees, interactions between events cannot be modeled.

The other side, the advantages of MA are very detailed, complete system description in one model can show different repair scenarios and can model sequence dependencies. Such advantages yet must be paid for which are analysis is complex, models are hard to construct and to verify especially for non-specialists, models can become very large (measured in the number of states) and in general for each system change, a completely new model has to be created.

A comparison of these different quantitative techniques shows that MA covers most aspects for quantitative safety evaluation, although MA is more complex but has more accurate analysis results than FTA. Both analysis techniques are well-proven techniques, they have been around for many years. The results of these two approaches are some relative conclusions [3].

From these scholarly papers, this paper draws a conclusion to take consideration in terms of implementing the MA be a complementary technique and as one of the safety analysis method other than FTA which has been mostly only used in System Safety Analysis (SSA) quantitative method, such as applied in Indonesian Aerospace manufacture (due to time efficiency objective).

A. Safety Objective

When certifying a new aircraft and its systems, the aircraft designer must conduct a comprehensive assessment of the potential failure. A logical and acceptable inverse relationship must exist between the average probability per flight hour and the severity of failure condition effects [4].

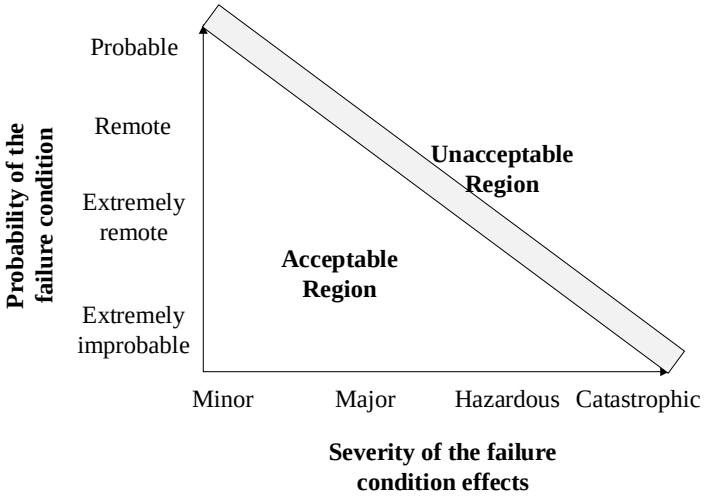

Figure 1. Safety objective for probability and severity of failure condition [4].

The document of SAE ARP4761 describes guidelines and methods of performing the safety assessment for civil aircraft. It is primarily associated with showing compliance with part 23 for section 1309. This document presents guidelines for conducting an industry-accepted safety assessment consisting of FHA, PSSA, and SSA.

The safety assessment process includes requirements generation and verification which supports the aircraft development activities. This process provides a methodology to evaluate aircraft functions and the design of systems performing these functions to determine that the associated hazards have been properly addressed.

The safety assessment processes are detailed in ARP4761. Functional Hazard Assessment (FHA) examines aircraft and system functions to identify potential functional failures. System Safety Assessment (SSA) collects, analyzes, and documents verification that the aircraft and systems, as implemented, meet the safety requirements established by the FHA.

FHA can be divided into Aircraft level FHA and System level FHA, each functional failure condition is allocated an allowable probability target in accordance with the safety criteria. This probability target is the design objective for the completed system [5].

SSA is a systematic and comprehensive assessment of the architecture, design, and installation of the systems to ensure that relevant safety requirements are met. SSA focuses on verifying whether the design can meet the qualitative and quantitative safety requirements from FHA.

B. Safety Analysis Methods

Safety assessment analysis methods provide the analyst a means for quantitatively assessing the safety of a design using FTA and MA methods.

FTA is a deductive failure analysis which focuses on one particular undesired event and provides a method for determining causes of this event, FTA is a "top-down" system evaluation procedure in which a qualitative model for a particular undesired event is formed and then evaluated. Fault tree calculations are based on Boolean algebra, probability theory, and reliability theory [6].

MA is a method to calculates the probability of the system being in various states as a function of time. MA can be used to model the operation, or failure, of complex system designs, provides a very detailed mathematical model of system failure states, state transitions, and timing. The MA process evaluates the probability of jumping from one known state into the next logical state until the system has reached the final state.

III. SAFETY ASSESSMENT PROCESS

A malfunction or loss of a function of an N219 hydraulic system can contribute to the failure condition which will have an effect on the aircraft and its occupants, both are direct and consequential. This situation may affect a continued safe flight and landing for the N219 aircraft. Therefore an examination of functions is needed to identify and classify failure conditions.

A. N219 Aircraft level FHA

At this stage the discussion focused on the identification of the aircraft function to control aircraft on the ground because the function is generated by braking and steering system, then the system that contributes to generating these systems are obtained and sourced from the hydraulic power system.

B. N219 System level FHA

Safety requirements for system functions are determined by identifying and classifying associated functional failure conditions. The discussion is emphasized on the identification of functions directly related to the hydraulic power, braking and steering control system.

TABLE 1
SYSTEM FUNCTIONS

System	Function
Hydraulic Power System	To generate and transmit hydraulic power (for wheel brakes and nose wheel steering operation).

Furthermore, the system FHA will be based on the analysis from failure conditions of its functions, by considering single and multiple failure modes in normal and degraded environments.

TABLE 2
HYDRAULIC POWER SYSTEM, TO GENERATE AND TRANSMIT HYDRAULIC POWER

System: Hydraulic Power System.				Function: To generate and transmit hydraulic power.		
No.	Failure Condition	Flight Phase	Detection	Effect of Failure	Safety Objective	Remarks
1.1	Fail to generate hydraulic power.	Reject Take-off (RTO), Landing.	Message on PFD.	Aircraft cannot be braked and steered resulting from total loss of hydraulic power. Loss of steering function.	Hazardous/ ≤ 1.0 x E-07	Assumed no power on the accumulators. Crew action: Use reverse thrust for braking aircraft.
1.2	Generate low hydraulic pressure.	Reject Take-off (RTO), Landing.	Message on PFD	No pressure was transmitted to the accumulators. Brake and steering system use existing accumulator pressure.	Major/ ≤ 1.0 x E-05	-

Hereinafter, the critical failure condition will be analyzed associated with N219 hydraulic system FHA. In this case, fail to generate hydraulic power is a critical failure condition due to it has a safety objective greater than Major, as suggested on AC 23.1309 paragraph 16(b) Safety Assessment.

C. Basic Event Probability of Failure

The basic events represent the probability of failure of a piece of equipment or component in the system. These failure probabilities are a function of both the failure rate (λ) for the event being modeled and exposure time. The total exposure time for hydraulic power, braking and steering system are 0.14 hours. These numbers are used for calculating the failure probability of each basic event on FTA and MA.

TABLE 3
BASIC EVENT FOR FAIL TO GENERATE HYDRAULIC POWER

Failure Condition	Reliability Parameters		Probability
Hydraulic accumulator 1 leakage	Failure Rate	2.32E-06	3.248E-07
Hydraulic accumulator 2 leakage	Failure Rate	2.32E-06	3.248E-07
Steering accumulator leakage	Failure Rate	2.32E-06	3.248E-07
Hydraulic reservoir leakage	Failure Rate	3.37E-06	4.718E-07
Bootstrap reservoir fails to maintain hydraulic pressure	Failure Rate	6.2654E-05	8.7716E-06
Motor driven hydraulic pump improper output	Failure Rate	9.921E-05	1.3889E-05
Pressure relief valve stuck closed	Failure Rate	9.20E-07	1.2881E-07
Non-return valve stuck closed	Failure Rate	5.20E-06	7.28E-07

D. Fault Tree Analysis

After defining the system design and operation which acquire from design data (drawings, schematics, procedures, diagrams, etc.). Descriptively define the problem and establish the correct undesired event for the analysis. Furthermore, the undesired event has a failure condition

classification of Catastrophic or Hazardous (critical failure condition) which will become the top-level event in a fault tree.

FTA systematically determines all basic events (single faults) and failure combinations of the system functional blocks at the next lower level which could cause the undesired event.

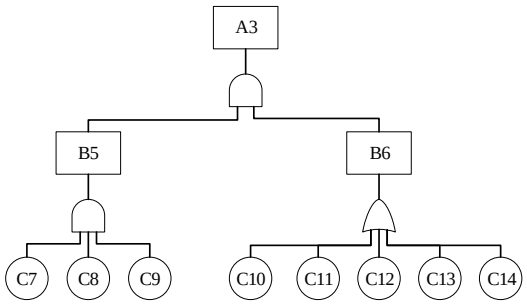

Figure 2. FTA Overview, Top Undesired Event: Fail to generate hydraulic power

TABLE 4
EVENT SYMBOL OF FAILURE CONDITION

Event	Failure Condition
A3	Fail to generate hydraulic power
B5	Total loss of secondary hydraulic power
B6	Loss of main hydraulic power
C7	Hydraulic accumulator 1 leakage
C8	Hydraulic accumulator 2 leakage
C9	Steering accumulator leakage
C10	Hydraulic reservoir leakage
C11	Bootstrap reservoir fails to maintain hydraulic pressure
C12	Motor driven hydraulic pump improper output
C13	Pressure relief valve stuck closed
C14	Non-return valve stuck closed

TABLE 5
LOGIC STRUCTURE OF FAILURE PROBABILITY

Event	Logic Gate	Description
A3	AND	B5 . B6
B5	AND	C7 . C8 . C9
B6	OR	C10 + C11 + C12 + C13 + C14

Top Event	Failure Condtion	Minimal Cut Set	Probability
A3	Fail to generate hydraulic power	[C7 . C8 . C9] . [C10 + C11 + C12 + C13 + C14]	8.2199E-25

E. Markov Analysis

A Markov process is completely characterized by its transition probability matrix, which is developed from the transition diagram. Events involve failure of components. The transitional probabilities between states are a function of the failure rates of the various system components. A set of first-order differential equations is developed by describing the probability of being in each state in terms of the transitional probabilities from and to each state.

Markov model with two components system failure is defined as the failure of components A and B. The assumption that the failure rate of components A and B respectively is λ_a and λ_b, both components fail will be λ_c. The safety analysis for this paper also will involve more than two components system depending on the considerations of the failure condition to be observed.

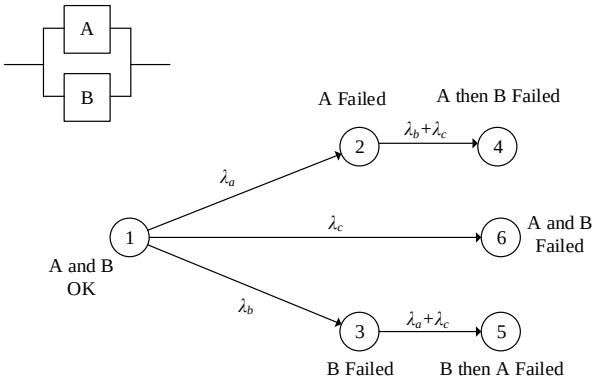

Figure 3. Markov diagram for two components system – parallel

Two component system - parallel equivalent with “B5” and “B6” in the output of “A3” AND Gate in FTA model.

TABLE 6
MARKOV DIAGRAM SOLUTION FOR EACH STATE

System Differential Equations	Solution
$\frac{dP_1(t)}{dt} = -(\lambda_a + \lambda_b + \lambda_c)\, P_1(t)$	$P_1(t) = e^{-(\lambda_a+\lambda_b+\lambda_c)t}$
$\frac{dP_2(t)}{dt} = \lambda_a\, P_1(t) - (\lambda_b + \lambda_c)P_2(t)$	$P_2(t) = e^{-(\lambda_b+\lambda_c)t} - e^{-(\lambda_a+\lambda_b+\lambda_c)t}$
$\frac{dP_3(t)}{dt} = \lambda_b P_1(t) - (\lambda_a + \lambda_c)P_3(t)$	$P_3(t) = e^{-(\lambda_a+\lambda_c)t} - e^{-(\lambda_a+\lambda_b+\lambda_c)t}$
$\frac{dP_4(t)}{dt} = (\lambda_b + \lambda_c)P_2(t)$	$P_4(t) = \frac{\lambda_a}{\lambda_a+\lambda_b+\lambda_c} - e^{-(\lambda_b+\lambda_c)t} + \frac{\lambda_b+\lambda_c}{\lambda_a+\lambda_b+\lambda_c} e^{-(\lambda_a+\lambda_b+\lambda_c)t}$
$\frac{dP_5(t)}{dt} = (\lambda_a + \lambda_c)P_3(t)$	$P_5(t) = \frac{\lambda_b}{\lambda_a+\lambda_b+\lambda_c} - e^{-(\lambda_a+\lambda_c)t} + \frac{\lambda_a+\lambda_c}{\lambda_a+\lambda_b+\lambda_c} e^{-(\lambda_a+\lambda_b+\lambda_c)t}$
$\frac{dP_6(t)}{dt} = \lambda_c\, P_1(t)$	$P_6(t) = \frac{\lambda_c}{\lambda_a+\lambda_b+\lambda_c}\left(1 - e^{-(\lambda_a+\lambda_b+\lambda_c)t}\right)$

As the table above, showing the solution obtained based on each state of the Markov diagram for the two components system - parallel. The solution obtained depends on the number of components and diagram form in parallel or series, the solution of the rest of the other Markov diagrams in this paper are not shown here due to the complexity of the writing and space required.

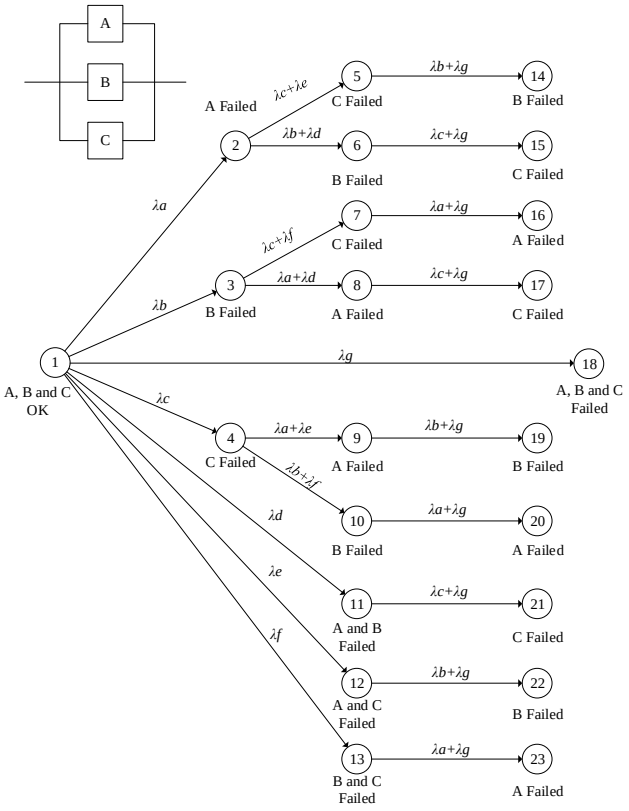

Figure 4. Markov diagram for three components system – parallel

Three component system parallel equivalent with “C7”, “C8”, and “C9” in the output of “B5” AND Gate in FTA model. So on, the Markov diagram for five component system series

will equivalent with. “C10”, “C11”, “C12”, “C13”, and “C14” in output of “B6” OR Gate in FTA model.

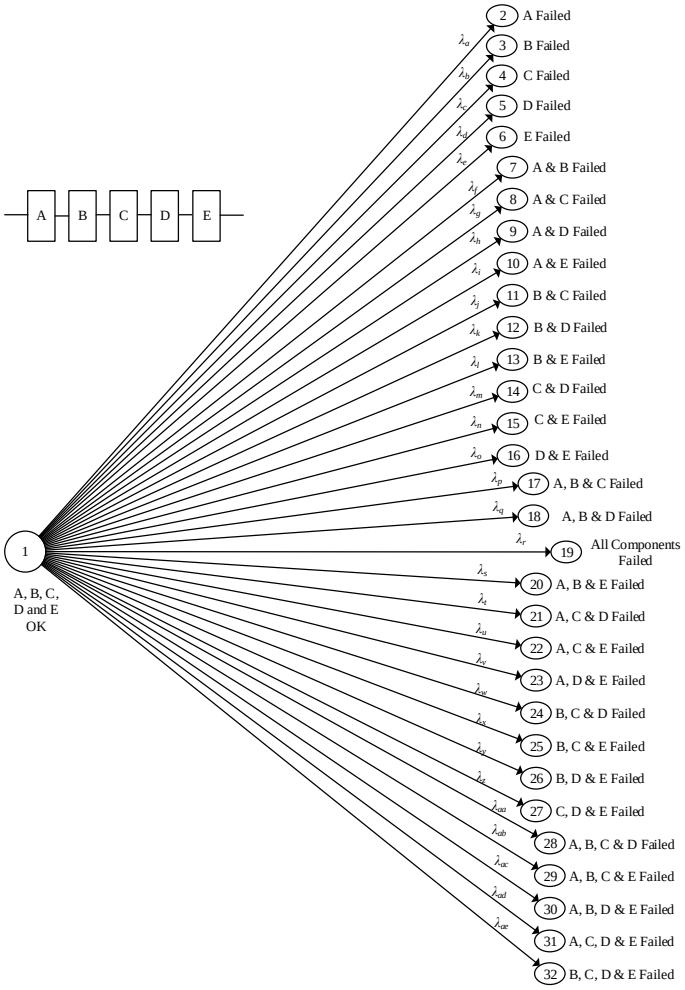

Figure 5. Five components system – series

IV. SAFETY ASSESSMENT ANALYSIS

A. FTA and MA Comparison

TABLE 7
PROBABILITY OF FAIL TO GENERATE HYDRAULIC POWER

t (hours)	Probability FTA	Probability MA
1	8.2200E-25	8.2197E-25
10	8.2200E-24	8.2190E-24
100	8.2200E-23	8.2101E-23
1000	8.2200E-22	8.1222E-22
10000	8.2200E-21	7.3083E-21
100000	8.2200E-20	3.1153E-20
1000000	8.2200E-19	3.4265E-20

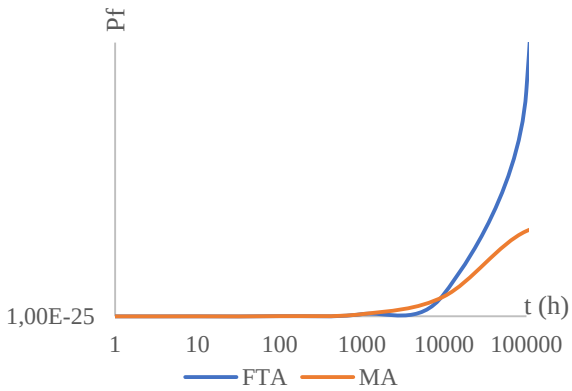

Figure 6. FTA and MA comparison

B. Critical Failure Condition Verification

Based on quantitative calculations FTA and MA that have been carried out, it can be concluded that the critical failure condition for fail to generate hydraulic power in hydraulic power system on N219 Aircraft meet safety requirements.

V. CONCLUSIONS

The comparative results obtained from the FTA and MA methods show that there is no significant difference. The results comparison difference only found in the higher time variables in the system. These results indicate that MA can be used as a validation method for FTAs as well, and vice versa. This endeavor is to conduct a comprehensive evaluation to verify the overall safety of the system and to cover all the specific safety considerations.

As the results of MA calculation, the MA has a higher solubility than FTA, wherefrom MA has a predominance of the solution for the scenario of failure conditions in sequence accuracy which can be obtained from each state calculations. MA can handle this scheme for components which installed either series or parallel in detail and generate a probability value for a system that fails sequentially and/or simultaneously using only one Markov modeling.

REFERENCE

[1] Jianzhong, Y. and Julian, Z. (2011): Application Research of Markov in Flight Control System Safety Analysis, Procedia Engineering 17 (2011) 515 – 520.
[2] Rouvroye, J.L. (2001): Enhanced Markov Analysis as A Method to Assess Safety in the Process Industry, Eindhoven: Technische Universiteit Eindhoven.
[3] Andrews, J.D. and Ericson, C.A. (2000): Fault Tree and Markov Analysis Applied to Various Design Complexities, 18th International System Safety Conference September 11-16 2000, Fort Worth Texas, Radisson Plaza.
[4] Kritzinger, D. (2016): Aircraft System Safety: Assessments for Initial Airworthiness Certification, Elsevier Ltd, UK.
[5] Federal Aviation Administration (2011): System Safety Analysis and Assessment for Part 23 Airplanes, ACE-100, Small Airplane Directorate.
[6] Society of Automotive Engineers Inc. (1996): SAE ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, Warrendale, PA, SAE International.
[7] Society of Automotive Engineers Inc. (1996): SAE ARP4754 Certification Considerations for Highly-integrated or Complex Aircraft Systems, Warrendale, PA, SAE International.
[8] Republic of Indonesia, Ministry of Transportation (2014): Airworthiness Standards: Normal, Utility, Acrobatic, and Commuter Category Airplanes, Amendment 2, Indonesia.

Yoga Yulasmana, S.T., M.T. A graduate Bachelor of Engineering degree from Nurtanio University in 2015, Bandung. At the same time completed studies in the Aircraft Maintenance Training Organization (AMTO) program for General Licenses A1 and A4. Once, used to work at Cathay Pacific Engineering, later on, took postgraduate studies at Institut Teknologi Bandung, earned a Master of Engineering degree in 2018. Some interest research fields include aircraft design, aircraft operational, reliability, availability, maintainability, and safety. Currently active as a lecturer at Nurtanio University and also an instructor at Unnur Aero Maintenance Training Organization (UAMTC) Bandung.

Received August 9th, 2019; Revised August 23rd, 2019; Accepted September 4th, 2019