

The Necessity to Perform a “Traditional” Fault Tree Analysis Process when Conducting a Model-based Safety Assessment

Klaus Fritz and Nikolaus Kurz
Diehl Aerospace GmbH

Eric Peterson
Electron International II Inc

ABSTRACT

Fault tree analyses and the associated safety assessment process plays an essential role in demonstrating acceptable avionic system compliance to the system safety requirements derived from safety related regulations associated with the civil aircraft certification process (e.g. 14CFR/CS §25.1309). SAE ARP4754A and SAE ARP4761 are established industry guidelines for the safety process and fault tree methodology applicable to civil aircraft certification based on techniques which have now been in use for decades.

System model-based techniques, used for some time in system and software development, are now being applied in the safety assessment process. These system behavior models of functions with their associated dependencies and assignments have been supplemented with failure modes and effects to “automatically” generate fault tree like outputs. These system model-based fault trees are intended to become integral to the safety assessment process.

This paper contrasts the “traditional” fault tree analyses process with that for the system model-based approach for application during the development and verification stages of a project. Each approach will be evaluated for scope, capabilities, equivalence and their adequacy in showing compliance to certification safety process requirements.

CITATION: Fritz, K., Kurz, N. and Peterson, E., "The Necessity to Perform a “Traditional” Fault Tree Analysis Process when Conducting a Model-based Safety Assessment," *SAE Int. J. Aerosp.* 5(1):2012, doi:10.4271/2012-01-2130.

INTRODUCTION

Purpose and Scope of Fault Tree Analyses

The fault tree analysis and the process associated with the generation of fault trees is widely used for analysis of avionic systems as a demonstration of compliance to the system safety requirements derived from safety related regulations associated with the civil aircraft certification process (e.g. 14CFR/CS §25.1309). The industry guidance referenced by the regulatory advisory material describes a process for development of civil aircraft and systems (e.g. SAE ARP4754A) which tightly interacts with the safety assessment process. Industry guidelines for safety assessment methodologies including the functional hazard assessment (FHA) and the fault tree analysis (FTA) methodology are provided in SAE ARP4761. The acceptable means of compliance (AMC) definition and guidance provided by the 14CFR/CS AMC §25.1309, ARP4754A and ARP4761 inherently defines a relationship between the process and the

methodology, such that the analysis is integral to the process and vice-versa, the process requires the analysis.

Safety objectives for an aircraft or system are established through performance of a functional hazard assessment (FHA). The FHA systematically and comprehensively examines functions resulting in the identification and severity of failure conditions to provide the starting point for the safety process.

Fault tree analyses provide a hierarchical and graphical analysis format to evaluate safety objectives determined through the FHA, i.e. single failure conditions or undesired events into single or combinations of contributory causes. A fault tree analysis may be performed during the development and verification stages of a project. During the development stage, an FTA considers the architecture, design concepts and available data in an iterative, systematic examination to determine acceptability of the planned architecture and implementation. As a verification tool, the FTA confirms that the implemented system continues to satisfy the identified safety objectives. The results of the fault tree analyses are

reported in either preliminary system safety assessments (PSSA) or system safety assessments (SSA) depending upon the project stage.

Introduction to Model-based Safety Assessment

Model-based safety assessment is a process based on a system or functional behavior model utilizing methods or associated variants known from industry guidance intended to showing compliance to the safety related regulations of aircraft certification (e.g. 14CFR/CS §25.1309, [6]).

In the model-based safety assessment process, computer hosted modeling tools are used to create a system model which integrates both functional behavior as well as failure characteristic behavior. These modeling tools then perform semi-automatically or automatically, a reduction of each system model element failure effect contribution to the identified failure conditions. The resulting Boolean reduction (i.e. cutset) of failure effect contribution output may be presented in tabular or graphic format.

The model-based safety assessment process is considered fundamentally different to traditional approaches. Specific regulation [6] or guidance on process [1] and methods [2] on the model-based safety assessment approach is currently not available, i.e. the general regulation is applicable, which explicitly permits different approaches if compliance to the §25.1309 can be shown (e.g. refer to [6], AMC, 1b).

The model-based processes are also conducted iteratively supporting development and verification project stages. During the development stage, the hierarchical character of functional models can be used to develop architectures into detailed design models considering functional behavior and failure models. The verification stage combines potentials of functional and failure mode testing.

This paper specifically discusses performing a model-based safety assessment approach in combination with a “fault tree analysis” used to show compliance to system safety requirements. This approach will be discussed in comparison to the “traditional” process using fault tree analysis.

Analytical Approaches - Deductive and Inductive

Safety analysis methods generally follow either “deductive” (top-down) or “inductive” (bottom-up) analysis approaches. Deductive methods are applied to determine how a failure can occur in a certain way (e.g. FTA), while inductive methods can be applied to determine what system failures are possible (e.g. FMEA/FMES). The basic difference between deductive and inductive methods is the “direction” of the analysis.

Deduction

Deduction constitutes reasoning from the general to the specific, i.e. concludes backwardly the causes of an event. In

a deductive system analysis, it is postulated that the system itself has failed in a certain way, and an attempt is made to find out what modes of system or subsystem (component) behavior contribute to this failure. The event, an undesired failure event derived from the FHA, is first defined for which causes are to be resolved. The event is resolved into its immediate and necessary sufficient causal events and related to the causal events by appropriate logic (e.g. logic-AND/OR). This stepwise resolution of events into immediate causal events proceeds until basic causes (primary causes) are identified. A typical of deductive analyses is e.g. an aircraft accident investigation: “What chain of events caused the accident?” [4, 5]

Induction

Induction involves reasoning from individual cases to a general conclusion, i.e. produces forwardly the consequences of an event. If, in the consideration of a certain system, a particular fault or initiating condition is postulated and an attempt to ascertain the effect of that fault or condition on system operation is made, an inductive system analysis is being conducted. An initiating event is first defined which can have undesired consequences. Subsequent events are identified which define possible progressions of the initiating event. Possible realizations of the subsequent events are defined. The consequence of each scenario is described.

In everyday language the inductive techniques provide answers to the generic question, “What happens if...?” More formally, the process consists of assuming particular states for components, generally failed states, and then analyzing the effects on the system. More generally, a given initiating event is assumed, such as a pipe rupture, and the consequences of the event are analyzed. Inductive approaches are also termed bottom-up approaches that start at the bottom, i.e. at the failure initiators and basic event initiators, and then proceed upwards to determine the resulting system effects of a given initiator. Inductive approaches thus start at a possible basic cause and then analyze the resulting effects. A set of possible causes are analyzed for their effects. [4, 5]

Analysis Logic Approaches - Success or Failure

The operation of a system can be considered from two standpoints: the various ways for a system or function success can be enumerated or the various ways for a system or function failure can be enumerated. Those two fundamentally different approaches are used by design and safety disciplines, respectively. Designers are working towards success, while safety analysts resolve failure scenarios.

Success logic

Success of a system or function refers to its general specification and tends to be associated with, for example, efficiency, performance, functional output, usefulness, etc. There can be various degrees of success, reaching from

minimum acceptable success to total success. In practice, the level of success represents a compromise between various overlapping and opposing optimization parameters.

Modeling approaches as used for system development activities, generally follow a success approach. Functions and their interdependencies and relations are modeled to simulate operation of the system. Success is defined as appropriate reaction of a system or function based on condition, state, sensor data and input commands. Within avionics systems, system reconfiguration following failure (loss) or unavailability of functions is also considered a functional model using the success logic approach.

Failure logic

Failure of a system or function coincides within certain analogous points with success. Failure may also be expressed within various degrees, e.g. sub-function failure, function failure or system failure, but is generally easier to define. Although in some cases failure logic approach is, similar to the success logic, also not that easy to define, it is generally easier especially through the identification of failures thresholds. Discretization and quantification of failure events is generally simpler and the “failure mindset” of the analyst probes for weakness and gaps [4, 5]. The fault tree analysis method uses the failure logic.

“TRADITIONAL” FAULT TREE ANALYSIS AND PROCESS

Applicable and relevant references

The traditional fault tree analysis process and methodology is defined by a chain of references to regulation and guidance documents including the 14CFR/CS §25.1309 [6] and the associated AMC, SAE ARP4754A [1], and SAE ARP4761 [2].

ARP4761 references the NUREG-0492 [3] for specific questions related to the fault tree analysis. The NUREG-0492 is more or less replaced by a newer version, the AFTH [4], now issued by NASA specifically addressing aerospace applications. Additional (informal) information on fault tree analysis is provided by [4] and [5], created in line supporting the AFTH.

This paper is not intended to repeat or correct that material, but to provide references and summarize relevant aspects for the readers convenience.

Fault tree analysis method

A Fault Tree Analysis (FTA) is a structured, deductive failure analysis which focuses on one particular undesired event and provides a method for determining causes of this event. In other words, a Fault Tree Analysis is a “top-down” system evaluation procedure in which a qualitative model for a particular undesired event is formed and then evaluated. The analyst begins with an undesired top level hazard event and systematically determines all credible single faults and

failure combinations of the system functional blocks at the next lower level which could cause this event.

The analysis proceeds down through successively more detailed (i.e., lower) levels of the design until a Primary Event is uncovered or until the top level hazard event requirement has been satisfied. A Primary Event is defined as an event which for one reason or another has not been further developed (i.e., the event does not need to be broken down to a finer level of detail in order to show that the system under analysis complies with applicable safety requirements). A Primary Event may be internal or external to the system under analysis and can be attributed to hardware failures/errors or software errors.

The analyst is encouraged to discontinue the FTA analysis when sufficient detail to satisfy the top level hazard requirement has been identified.

The fault tree graphical representation is hierarchical and takes its name from the branching that it displays. It is this format which makes this analysis a visibility tool for both engineering and the certification authority. As one of a family of safety assessment techniques for assuring that the system/equipment will accomplish its intended safety functions, fault tree analysis is concerned with ensuring that design safety aspects are identified and controlled [2].

For detailed reading on the fault tree analysis methodology refer to ARP4761 [2], AFTH [4] and other FTA material [3], [5].

Process of generating fault trees

The value of the fault tree analysis is not only the existence and the graphical representation of the result, but mainly the general process from the proof concept of an architecture and design through its development stage (preliminary system safety assessment) until showing compliance of a final design to safety requirements at the end of the safety verification stage (system safety assessment). In other words, use of the expression “fault tree analysis” commonly refers to using the method within a specific process throughout the project stages from first concepts until certification (and beyond) [1], [2].

During the process of detailing the system definition from the top-level architecture down to an implementation specification for hardware and software, the fault tree analysis also becomes more detailed with every development step. The fault tree analysis supports by providing focus on safety relevant aspects of the design and failure rate budgeting. Applying the method will subsequently lead to success (compliant) and failure (non-compliant) causing an iterative proceeding which influences the architecture the design and the implementation to be finally compliant to safety requirements.

Every aircraft, system or functional hazard is transformed to safety objectives within the FHA method and process. Safety objectives generate individual fault tree analyses and the associated process is performed for any of the hazards separately, although individual branches of the trees may be