Reliability Engineering

Notes 10

Safety

- Safety is a property of a system that reflects the system's ability to operate, normally or abnormally, without danger of causing human injury or death and without damage to the system's environment.
- Degree of freedom from harm or danger.

Safety

- Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

System safety

- The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.
- A planned, disciplined and systematic approach to preventing or reducing accidents throughout the lifecycle of a system.

Safety and Reliability

- Safety and reliability are related but distinct
- In general, reliability and availability are necessary but not sufficient conditions for system safety.
- Reliability is concerned with conformance to a given specification and delivery of service.
- Safety is concerned with ensuring system cannot cause damage irrespective of whether or not it conforms to its specification.
- System reliability is essential for safety but is not enough.
- Reliable systems can be unsafe

- In theory, safe systems may be unreliable, while reliable systems may be unsafe. Nevertheless, systems can be designed in order to be both safe and reliable.
- There may be dormant faults in a system that are undetected for many years and only rarely arise.
- If the system specification is incorrect then the system can behave as specified but still cause an accident.

- Reliability may thus be determined by the probability of failure per demand, whilst safety is also determined by the consequences of these failures.
- Safety is the attribute of a system - e.g. a nuclear power plant - to be free from the occurrence of accidents, i.e. from the undesired events that lead to catastrophic consequences such as health and environmental effects of radiation and radioactive contamination. Safety is achieved through the use of reliable structures, components, systems and procedures.

Event Tree Analysis History

- Event Tree Analysis was first introduced in 1975 for the nuclear regulatory commission; this is basically the reactor safety study.
- It can be applied to a wide range of systems including: nuclear power plants, spacecraft, chemical plants.
- This technique may be applied to a system early in the design process to identify potential issues that may arise, rather than correcting the issues after they occur.

Event Tree Analysis

- An event tree analysis (ETA) is an inductive procedure that shows all possible outcomes resulting from an initiating (accidental) event. Taking into account whether installed safety barriers are functioning or not, and additional events and factors.
- Initiating event (IE): Failure or undesired event that initiates the start of an accident sequence.
- Event tree is that inductive approach when you start with a event and then ask what will happen next given a system configuration.
- ETA can be used 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.

Event Tree Analysis

- Event trees are graphical representations of binary logic models which identify and can quantify possible consequences resulting from an initiating event (e.g. component failure)
- The construction of an event tree is sequential, left-right in the usual event tree convention. Analysis starts at the initiating event and the consequences of this event are then followed through a series of possible branches.
- The questions defining the branches are placed across the top of the tree and are sometimes called nodes. The answers are usually binary (e.g. ‘yes’ or ‘no’), with the convention usually adopted of upward branches signifying ‘yes’ and downward ones for ‘no’

Event Tree Analysis

- An event tree is a logical diagram which displays possible event sequences following a specified critical event in a system. An event tree analysis (ETA) is a method for systematic analysis of a system after a critical event has occurred. The result of an ETA is a list of possible event sequences that follows the initiating event. The critical, initiating event may be a technical failure or some human error.

Event Tree Analysis

- Event tree analysis evaluates potential accident outcomes that might result following an equipment failure or process upset known as an initiating event. It is a “forward-thinking” process, i.e. the analyst begins with an initiating event and develops the following sequences of events that describes potential accidents, accounting for both the successes and failures
- It uses Boolean logic to evaluate a sequence of events

Event Tree Analysis

- Finds all outcomes from an initiating event
- Analyzes the accidental progression according to the safety functions.
- Each event in the tree (success or failure of the safety function) is conditional on the occurrence of the previous event.

Event Tree Analysis

- Event Tree Analysis (ETA) is a method that examines the consequences of a particular event. Starting from an initial event, the tree is divided into two branches, whereby the upper one represents a positive and the lower one a negative development.
- Event trees are usually drawn from left to right.
- basically a binary form of decision tree
- binary form that fail or failure or success.

Event Tree Analysis

- The aim of ETA is the identification of possible damage events. ETA has been effectively implemented to analyse the cause of accidents and to identify hazards for a top-event. This method can be applied qualitatively by obtaining the possible outcomes and quantitatively by evaluating the probability of occurrence.
- Consequences can be direct (e.g., fire, explosion) or indirect (e.g., domino incidents)

Event Tree Analysis

- When defining an accident event, we should answer the following questions:
- What type of event is it? (e.g., leak, fire)
- Where does the event take place? (e.g., in the control room)
- When does the event occur? (e.g., during normal operation, during maintenance)

Event Tree Analysis

- An accidental event is defined as the first significant deviation from a normal situation that may lead to unwanted consequences (e.g., gas leak, falling object, start of fire) An accidental event may lead to many different consequences. The potential consequences may be illustrated by a consequence spectrum
- An accidental event may be caused by:
- System or equipment failure
- Human error
- Process upset

Event Tree Analysis

- The purpose of ETA is to evaluate all of the possible outcomes that can result from an initiating event.
- Generally, there are many different outcomes possible from an initiating event, depending upon whether design safety systems work properly or malfunction when needed.
- ETA provides a probabilistic risk assessment (PRA) of the risk associated with each potential outcome.

Event Tree Analysis

- In most applications only two alternatives (“true” and “false”) are considered.
- In practice, many event trees are ended before the “final” consequences are reached. Including these “final” consequences may give very large event trees that are impractical for visualization

Event Tree Analysis

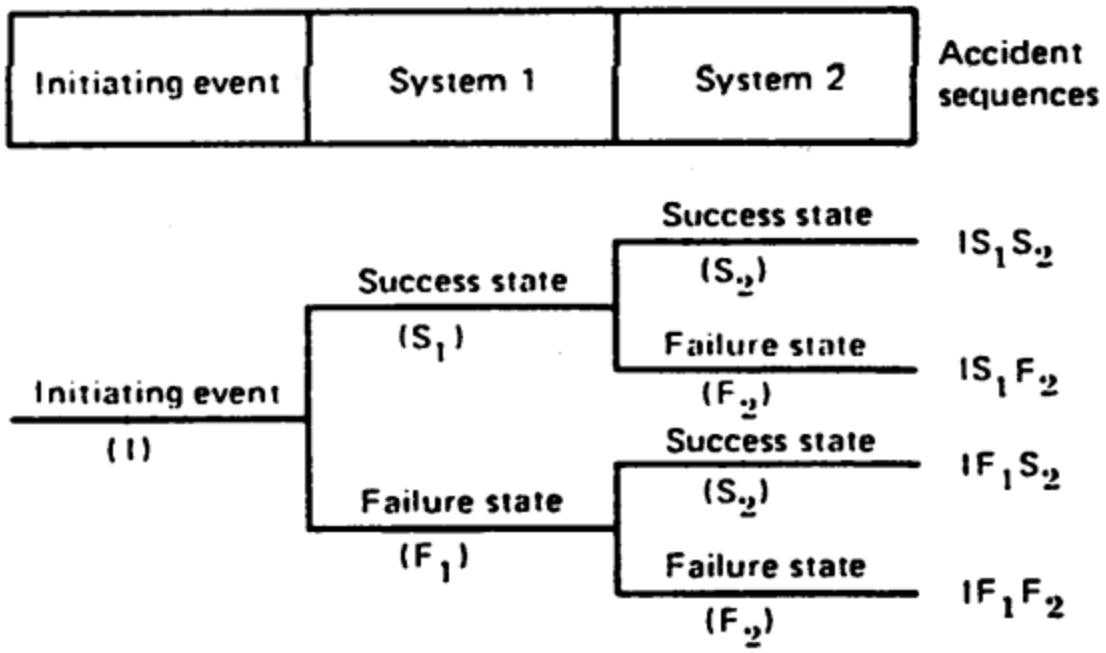
- Event trees are used to follow the potential course of events as the event moves through the various safety systems. The probability of success or failure of each safety intervention is used to determine the overall probability of each final outcome.

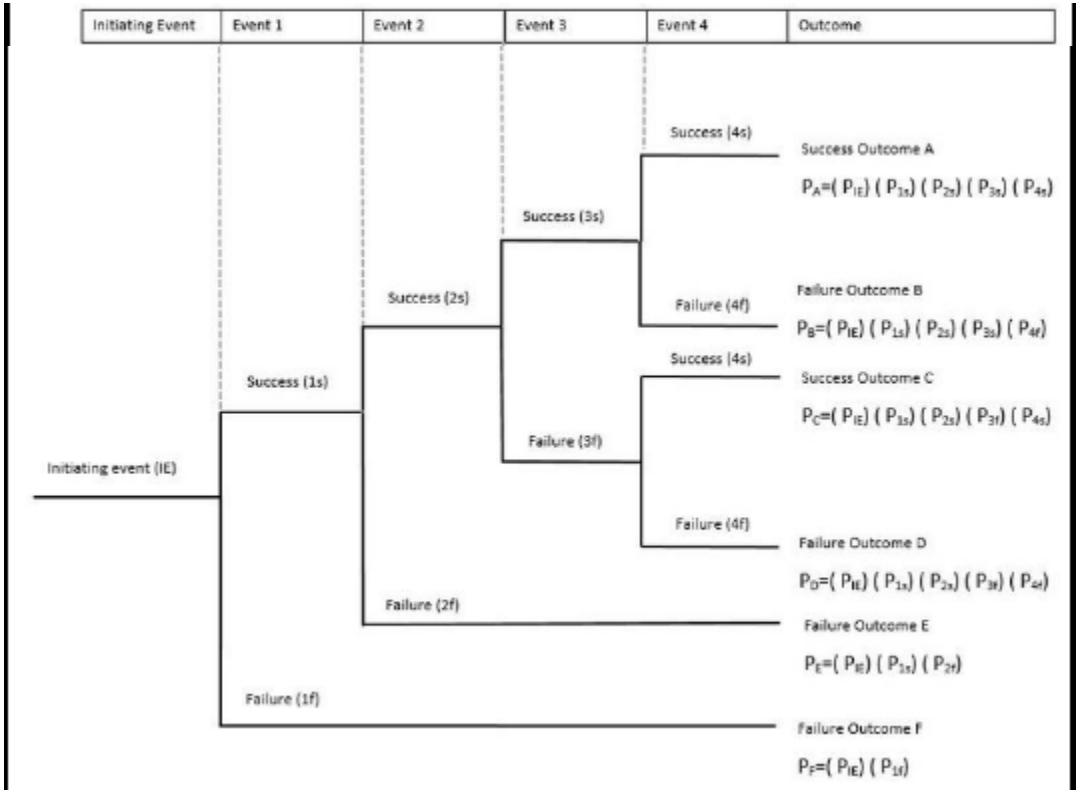
Event Tree Analysis

- work forward.
- Identifies how a failure can occur and the probability of occurrence
- Success – upward
- Failure – downward

Event Tree Analysis

- You go forward in that manner at every if the first that means, configuration or first layer fails then what is the second item or second subsystem which will act depending on the first one fails. So, then there also failure and success will take place and eventually you will have a have a tree like structure. Suppose, in the kitchen there is leakage of gas so, then there must be detection system. So, detection system may be successful or failure and again if decision system is successful then what will happen the immediately that means, the some actions will be taken and that other actions will become successful or failure and in this manner it will continue.


Initiating event
System 1
System 2
Accident sequences
Initiating event
(I)
Success state
(S1)
Failure state
(F1)
Success state
(S2)
Failure state
(F2)
Success state
(S2)
Failure state
(F2)
IS1S2
IS1F2
IF1S2
IF1F2


Initiating Event
Event 1
Event 2
Event 3
Event 4
Outcome
Initiating event (IE)
Success (1s)
Failure (1f)
Success (2s)
Failure (2f)
Success (3s)
Failure (3f)
Success (4s)
Success Outcome A
$P_A=(P_{IE})(P_{1s})(P_{2s})(P_{3s})(P_{4s})$
Failure (4f)
Failure Outcome B
$P_B=(P_{IE})(P_{1s})(P_{2s})(P_{3s})(P_{4f})$
Success (4s)
Success Outcome C
$P_C=(P_{IE})(P_{1s})(P_{2s})(P_{3f})(P_{4s})$
Failure (4f)
Failure Outcome D
$P_D=(P_{IE})(P_{1s})(P_{2s})(P_{3f})(P_{4f})$
Failure Outcome E
$P_E=(P_{IE})(P_{1s})(P_{2f})$
Failure Outcome F
$P_F=(P_{IE})(P_{1f})$

Steps

- 1. Identification of a relevant initiating event (which may give rise to unwanted consequences).
- 2. Identification of the barriers and safety functions which are designed to prevent the occurrence of the initiating event, or to reduce the consequences of this event.
- 3. Construction of the event tree.
- 4. Description of the resulting event sequences.
- 5. Calculation of probabilities/frequencies for the identified consequences.
- 6. Compilation and presentation of the results from the analysis.

Advantages

- Visualize event chains following an accidental event
- Visualize barriers and sequence of activation
- Good basis for evaluating the need for new / improved procedures and safety functions
- Strength of the event tree is that it portrays the event outcomes in a systematic, logical, self-documenting form that is easily audited by others
- Logical and arithmetic computations are simple and the format is usually compact
- Indicating outcomes that lead directly to failures with no interventing protective measures

- It is widely used and well accepted and can be used for cross-discipline system analysis.
- An event tree is clear and logical and therefore simple to understand
- It can be used to diagnose system difficulties

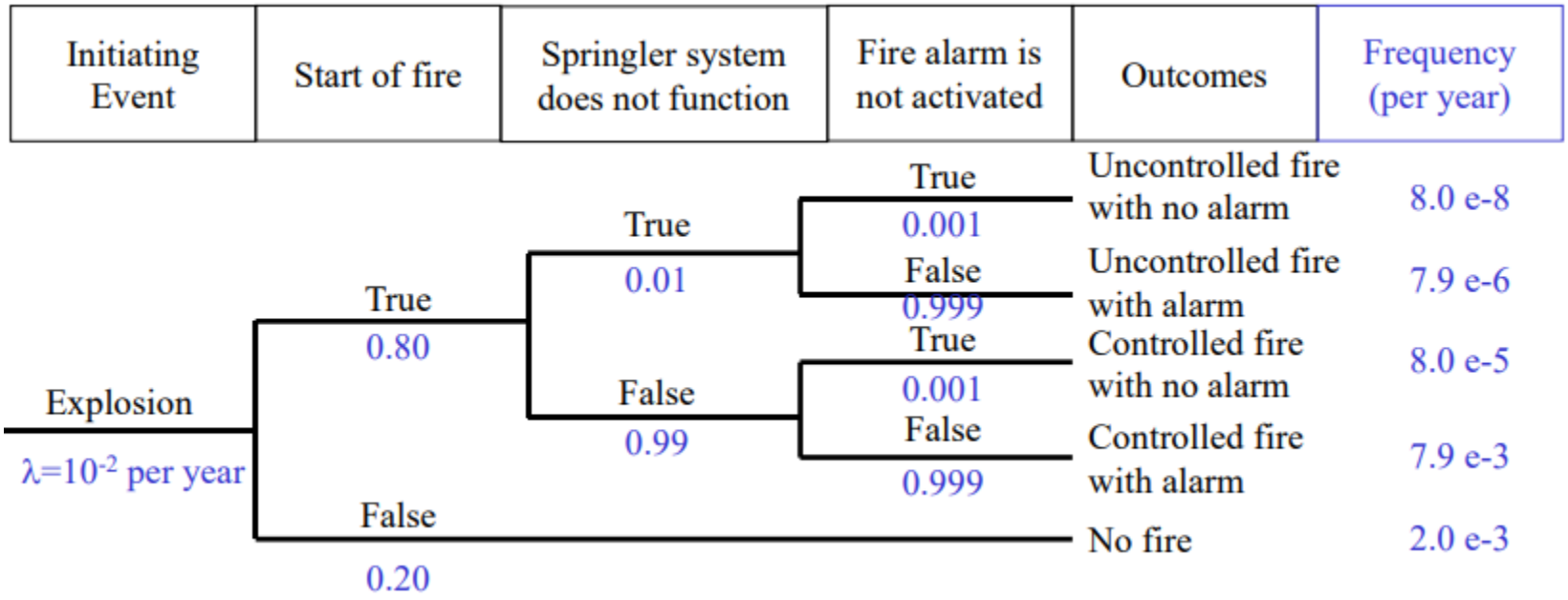
Disadvantages

- ETA can become very extensive for longer paths
- Each ETA only takes one initial event into account.
- Easy to overlook subtle system dependencies
- Not well suited for handling common cause failures in the quantitative analyses
- The event tree does not show acts of omission

- It is not efficient where many events must occur in combination, as it results in many redundant branches
- All events are assumed to be independent which can lead to missing systematic and common-mode failures
- As the technique uses binary logic it may not work for some accident scenarios which include uncertainty such as human error or adverse weather conditions

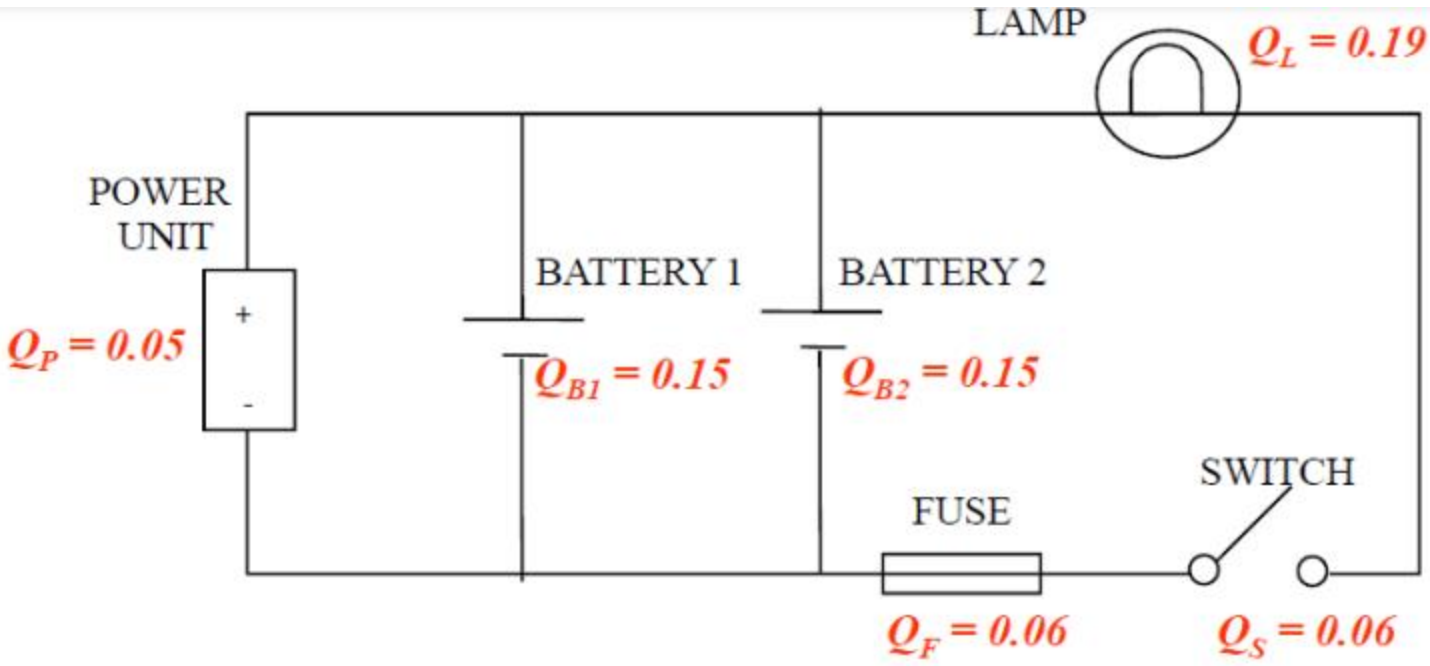
- The goal of quantitative event tree analysis is to determine the probability of possible negative outcomes that can cause harm and result from the chosen initiating event.
- If the events are independent;
- Overall path probability = (probability of event 1) × (probability of event 2) × ... × (probability of event n)
- Event Tree Analysis makes it easy to see what pathway creating the biggest probability of failure for a specific system

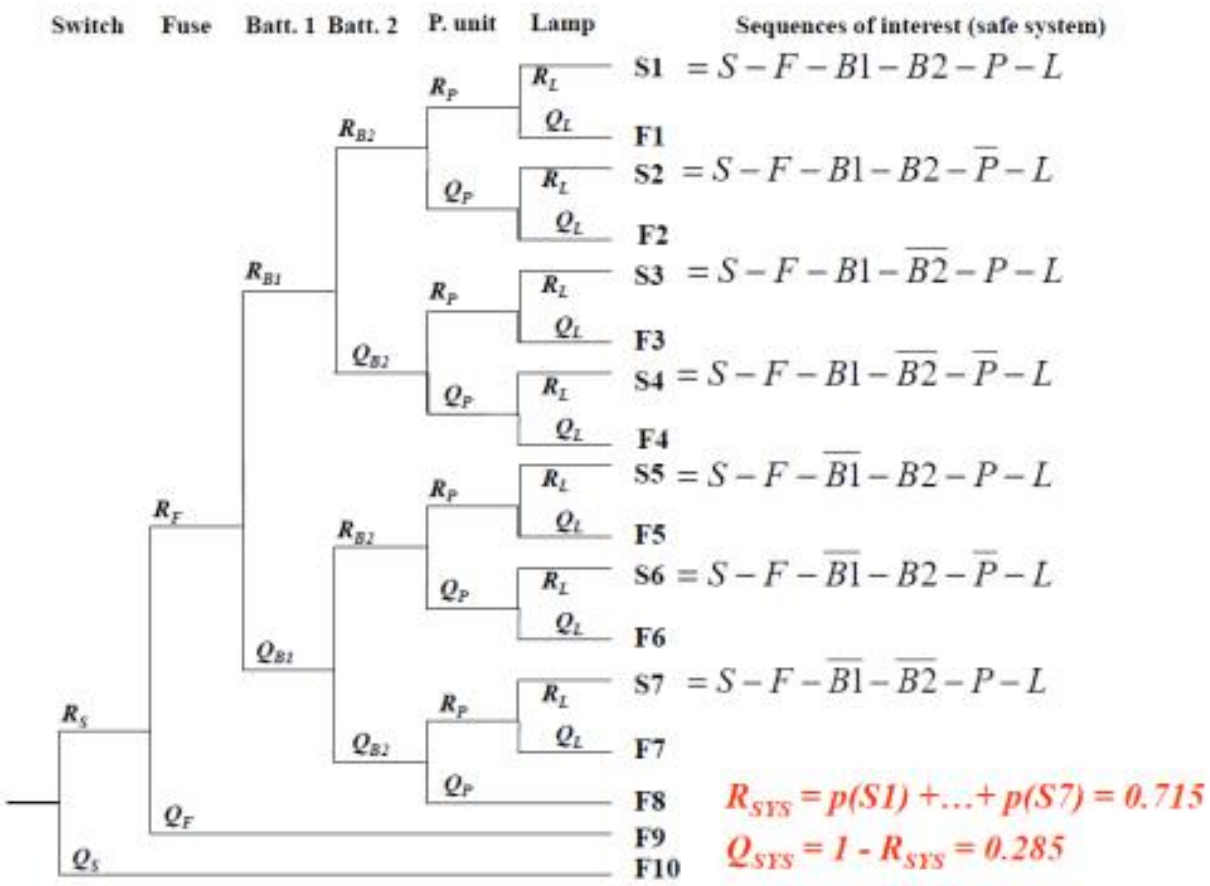
- Sometimes the frequency of the initiating event is given.
- λ denotes the frequency of the initiating event
- The probability of “Outcome 1” is:
- $= P(B1 \cap B2 \cap B3 \cap B4)$
- The frequency of “Outcome 1” is:
- $\lambda \cdot P(B1 \cap B2 \cap B3 \cap B4)$


Initiating Event
Start of fire
Springler system does not function
Fire alarm is not activated
Outcomes
Frequency (per year)
Explosion
λ=10-2 per year
True
0.80
False
0.20
True
0.01
False
0.99
True
0.001
False
0.999
True
0.001
False
0.999
Uncontrolled fire with no alarm
8.0 e-8
Uncontrolled fire with alarm
7.9 e-6
Controlled fire with no alarm
8.0 e-5
Controlled fire with alarm
7.9 e-3
No fire
2.0 e-3

Example

- The system represented in the figure illustrates the operation of a lamp fed by two batteries and a power unit. In order to have energy in the circuit it is enough that one of the energy sources (i.e., battery 1, battery 2, power unit) , works. Build the event tree for the event “failure of the lighting system” and compute its probability based on the component probabilities indicated on the Figure.


LAMP
$Q_L = 0.19$
POWER
UNIT
+
-
$Q_P = 0.05$
BATTERY 1
BATTERY 2
$Q_{B1} = 0.15$
$Q_{B2} = 0.15$
SWITCH
FUSE
$Q_F = 0.06$
$Q_S = 0.06$


Switch
Fuse
Batt. 1
Batt. 2
P. unit
Lamp
Sequences of interest (safe system)
R_S
Q_S
R_F
Q_F
R_{B1}
Q_{B1}
R_{B2}
Q_{B2}
R_P
Q_P
R_L
Q_L
S1 $= S - F - B1 - B2 - P - L$
F1
S2 $= S - F - B1 - B2 - \overline{P} - L$
F2
S3 $= S - F - B1 - \overline{B2} - P - L$
F3
S4 $= S - F - B1 - \overline{B2} - \overline{P} - L$
F4
S5 $= S - F - \overline{B1} - B2 - P - L$
F5
S6 $= S - F - \overline{B1} - B2 - \overline{P} - L$
F6
S7 $= S - F - \overline{B1} - \overline{B2} - P - L$
F7
F8
F9
F10
$R_{SYS} = p(S1) + \ldots + p(S7) = 0.715$
$Q_{SYS} = 1 - R_{SYS} = 0.285$

Resources

- Marvin Rausand, Chapter 3 Event Tree Analysis, RAMS Group Department of Production and Quality Engineering, NTNU Norwegian University of Science and Technology, Slides related to the book System Reliability Theory Models, Statistical Methods, and Applications Wiley, 2004 , Marvin Rausand and Arnljot Hoyland
- https://hazard.logu.tuhh.de/sites/default/files/2019-02/Event%20Tree%20Analysis_0.pdf
- https://hazard.logu.tuhh.de/node/34
- Event Tree Analysis Lecture 15, Prof. Jhareswar Maiti, Industrial Safety Engineering, Department of Industrial and Systems Engineering Indian Institute of Technology Kharagpur
- https://moodle.univangers.fr/pluginfile.php/2071728/mod_resource/content/1/Reliability%20Engineering-%20ISMP%20%20Chap%203%20-%20ETA.pdf
- Event Probability and Failure Frequency Analysis Lecture Notes, En Sup Yoon, 2009_2nd semester
- Event tree analysis , Prof. Enrico Zio , Politecnico di Milano Dipartimento di Energia

- Event Trees, https://web.mst.edu › dludlow › classes › che258
- Chapter 3 - Qualitative System Analysis, Jørn Vatn, TPK4120 - Lecture summary.
- https://slideplayer.com/slide/3280828/
- https://www.coursehero.com/file/21749171/Event-Tree-Analysis-in-Risk-Assessment/
- Event Tree Analysis Best Practices in Dam and Levee Safety Risk Analysis Part A – Risk Analysis Basics Chapter A-5 July 2019, https://www.usbr.gov/ssle/damsafety/risk/BestPractices/Presentations/A5-EventTreeAnalysisPP.pdf
- https://www.asems.mod.uk/toolkit/event-tree-analysis
- https://en.wikipedia.org/wiki/Event_tree_analysis
- Hazard Analysis Techniques for System Safety, Clifton A. Ericson, II , 2005, JOHN WILEY & SONS, INC., PUBLICATION
- Event & Fault Tree Analysis (ETA & FTA) Exercise lesson Dr. Zhe Yang Politecnico di Milano Dipartimento di Energia

Resources

- https://www.slideshare.net/software-engineering-book/ch12-safety-engineering
- Traditional Hazard Analysis,
- https://ocw.mit.edu/courses/aeronautics-and-astronautics/16-863j-system-safety-spring-2016/lecture-notes/MIT16_863JS16_LecNotes4.pdf
- Introdution to Safety Engineering, Michal Sojka, Czech Technical University in Prague, January 8, 2020, https://wiki.control.fel.cvut.cz/psr/prednasky/safety/safety-intro.pdf
- Designing for safety, Eric Marsden, https://risk-engineering.org/static/PDF/slides-design-for-safety.pdf
- Safety, Reliability and Software Based System Requirements, P.-J. Courtois AVN, Brussels
- 63JF12_Class5BasDesign.pdf
-

- http://www.applied-statistics.org/functional-safety-reliability-vs-safety.html
- Industrial Safety Engineering, Prof. Jhareswar Maiti, Department of Industrial and Systems Engineering Indian Institute of Technology, Kharagpur, Lecture – 02 Key Concepts and Terminologies
- Lecture 5, Basic Design for Safety Principles, https://ocw.mak.ac.ug/courses/aeronautics-and-astronautics/16-63j-system-safety-fall-2012/lecture-notes/MIT16
- ACCIDENT & INJURY PREVENTION Course Slides, Instructor: Kerrie Murphy, Edmonds Community College