IAF0530 (MSc)
IAF9530 (PhD)

Süsteemide usaldusväärsus ja veakindlus
Dependability and fault tolerance

Lecture 3

Gert Jervan
Department of Computer Engineering (ATI)
Tallinn University of Technology (TTÜ)

The rest of the course

- Topic selection:
  - 6+2 PhD students, 9 MSc students
  - Complete list on the course website
- Draft of the report + introductory presentation of the topic:
  - March 28
- Presentations:
  - April 25 – May 16 (mandatory presence in 3 out of 4)
- Final report:
  - May 30
- Final discussions + examination:
  - June 5-6 (if needed, individually)
- No lectures on March 7, March 21!

2

Safety Requirements

Definitions of Safety

- Informally
  - "Nothing bad will happen"
- N. Leveson, Safeware
  - "Freedom from accidents or losses"
  - But no system can be completely safe in absolute sense…
  - Focus is on making systems safe enough, given limited resources
  - Emphasis on accidents, rather than risk
- N. Storey, Safety-Critical Computer Systems:
  - "System will not endanger human life or environment"
  - More emphasis on removing hazards than actual accidents…
- Safety-critical system
  - System that has the potential to cause accidents

4

Safety requirements

- In order to determine safety requirements:
  - Identification of the hazards associated with the system
  - Classification of these hazards
  - Determination of methods for dealing with the hazards
  - Assignment of appropriate reliability and availability requirements
  - Determination of an appropriate safety integrity level
  - Specification of development methods appropriate to this integrity level

5

The Role of Standards

- Helping staff to ensure that a product meets a certain level of quality
- Helping to establish that a product has been developed using methods of known effectiveness
- Promoting a uniformity of approach between different teams
- Providing guidance on design and development techniques
- Providing some legal basis in the case of a dispute
- **Some standards:** ANSI/ISA S84 (Functional safety of safety instrumented systems for the process industry sector); IEC EN 61508 (Functional safety of electrical/electronic/ programmable electronic safety related systems); IEC 61511 (Safety instrumented systems for the process industry sector); IEC 62061 (Safety of machinery); EN 50128 (Railway applications - Software for railway control and protection); EN 50129 (Railway applications - Safety related electronic systems for signalling; EN 50402 (Fixed gas detection systems); Defence Standard 00-56 Issue 2 - accident consequence

6

Conflicting requirements

- High performance v low cost
- Reliability ≠ safety

BUT

- System must be reliable AND safe
- Hazard analysis and risk analysis to identify acceptable levels of safety and reliability

7

Hazard Analysis

Hazards & Risk Definitions

Definitions

- Hazard
  - Situation with actual or potential danger to people, environment or material, of a certain severity
  - e.g. lock that prevents elevator door from opening is not activated
- Incident (near miss)
  - Unplanned event that involves no damage or loss, but has the potential to be an accident in different circumstances
  - e.g. elevator door opens while the elevator is missing but nobody is leaning against it

Definitions (cont.)

- Accident
  - Unplanned event that results in a certain level of damage or loss to human life or the environment
  - e.g. elevator door opens and someone falls to the shaft
- Risk
  - Combination of the severity of a specified hazardous event with its probability of occurrence over a specified duration

Risk Assessment

- Risk = penalty x likelihood
  - Penalty can be measured in money, lives, injuries, amount of deadline…
  - Likelihood is the probability that a particular hazard will be activated and result in an undesirable outcome
  - Pareto ranking: 80% of problems are from 20% of the risks…

Risk Assessment (cont.)

- Example of risk calculation
  - Failure of a particular component results in chemical leak that could kill 500 people
  - Estimate that component will fail once every 10,000 years

    risk = penalty x (probability per year)
    = 500 x (0.0001)
    = 0.05 deaths per year

- But rare and costly events are a problem
  - E.g. infinite penalty multiplied by near-zero probability?
  - Must guard against catastrophic penalties event for near-zero probability

Risk

- A combination of the likelihood af an accident and the severity of the potential consequences
- The harm that can result if a threat is actualised
- Acceptable/tolerable risk: The Ford Pinto case (1968)

BENEFITS
Savings: 180 burn deaths, 180 serious burn injuries, 2,100 burned vehicles.
Unit Cost: $200,000 per death, $67,000 per injury, $700 per vehicle.
Total Benefit: 180 X ($200,000) + 180 X ($67,000) + $2,100 X ($700) = $49.5 million.

COSTS
Sales: 11 million cars, 1.5 million light trucks.
Unit Cost: $11 per car, $11 per truck.
Total Cost: 11,000,000 X ($11) + 1,500,000 X ($11) = $137 million.

Acceptability of Risk

- ALARP (As Low As is Reasonably Possible)
  - If risk can be easily reduced, it should be
  - Conversely, a system with significant risk may be acceptable if it offers sufficient benefit and if further reduction of risk is impractical
- Ethical considerations
  - Determining risk and its acceptability involves moral judgement
  - Society’s view not determined by logical rules
  - Perception that accidents involving large numbers of deaths are perceived as more serious than smaller accidents, though they may occur less frequently

Conflicting Requirements – Safety and Reliability

- A system can be unreliable but safe
  - If it does not behave according to specification but still does not cause an accident
- A system can be unsafe but reliable
  - If it can cause harm but faults occur with very low probability
- Fail Safe
  - System designed to fail in a safe state
    e.g. trains stop in case of signal failure
  - affects availability – 100% safe but 0% available..
- Fail Operational
  - System designed to keep working even if something fails
  - usually using redundancy
- Fail-over to reduced capability system
  - Mechanical backup

15

Hazards

Hazards Overview

Hazards

- A Hazard is a system state that could lead to:
  - Loss of life
  - Loss of property
  - Release of energy
  - Release of dangerous materials
- Hazards are the *states* we have to avoid
- An accident is a loss event:
  - System in hazard state, ***and***
  - Change in the operating environment
- Classification
  - Severity
  - Nature

17

Hazard Categories for Civil Aircraft

DESCRIPTION	CATEGORY	DEFINITION	PROBABILITY
CATASTROPHIC	I	Loss of Lives, Loss of Aircraft	10^{-9}/hr
HAZARDOUS	II	Severe Injuries, Major aircraft Damage	10^{-7}/hr
MAJOR	III	Minor injury, minor aircraft or system damage	10^{-5}/hr
MINOR	IV	Less than minor injury, less than minor aircraft or system damage	10^{-3}/hr
NO EFFECT	V	No change to operational capability	10^{-2}/hr

© G.F. Marsters

18

Hazard Categories for Civil Aircraft

Frequency of Occurrence	Level	Specific Item	Fleet or Inventory	Failure Probability per Flight Hour
Frequent	A	Likely to occur frequently	Continuously experienced	$\geq 1 \times 10^{-3}$
Reasonably Probable	B	Will occur several times in the life of each item	Will occur frequently	$< 1 \times 10^{-3}$ to $\geq 1 \times 10^{-5}$
Remote	C	Unlikely but possible to occur in the life of an item	Unlikely but can reasonably be expected to occur	$< 1 \times 10^{-5}$ to $\geq 1 \times 10^{-7}$
Extremely Remote	D	So unlikely it can be assumed that the occurrence may not be experienced	Unlikely to occur, but possible	$< 10^{-7}$ to $\geq 1 \times 10^{-9}$
Extremely Improbable	E	Should never happen in the life of all the items in the fleet	Not expected to occur during life of all aircraft of this type	$<1 \times 10^{-9}$

Risk from lightning is 5×10^{-7} deaths per person year

19

Hazard Risk Index

Probability	Severity Classification			
	Catastrophic	Hazardous	Major	Minor
Frequent	1	3	7	13
Reasonably Probable	2	5	9	16
Remote	4	6	11	18
Extremely Remote	8	10	14	19
Extremely Improbable	12	15	17	20

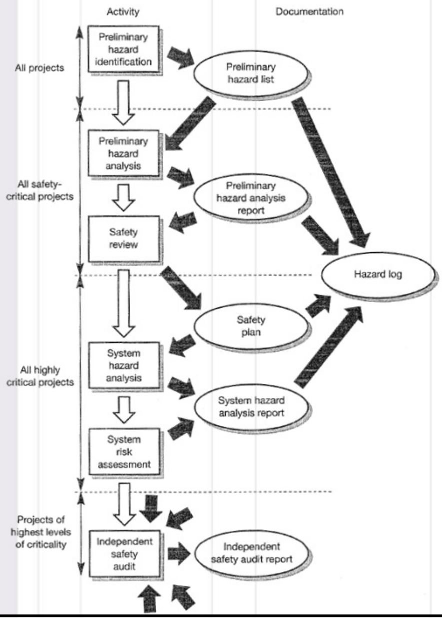
- Acceptable - only ALARP actions considered
- Acceptable - use ALARP principle and consider further investigations
- Not acceptable - risk reducing measures required

20

Hazards

Hazard Analysis

Hazard analysis lifecycle



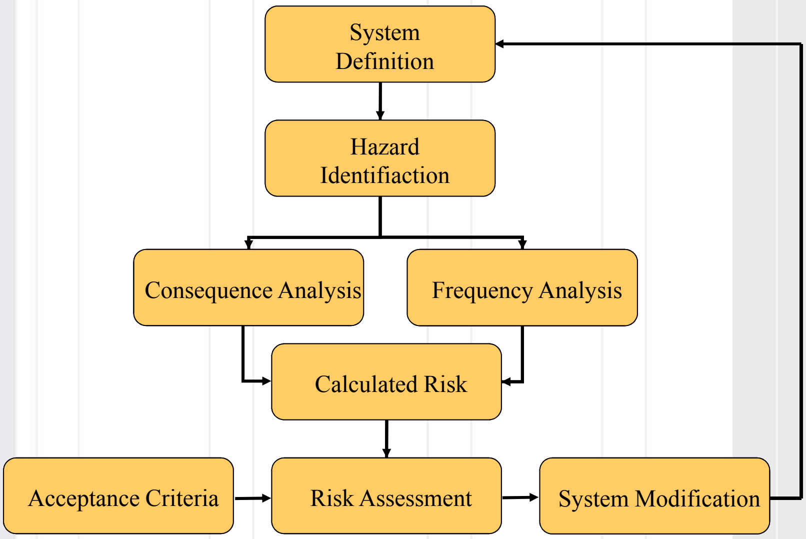
- Preliminary hazard identification: is the system safety related?
- Preliminary hazard analysis: determine the integrity levels of each major function
- Safety plan: how will the safety be achieved and who is responsible (staff names!)
- System hazard analysis: FMEA, HAZOP, event trees, fault trees, reliability block diagrams, Markov modeling

22

Hazard Analysis

- The purpose
  - Identify events that may lead to accidents
  - Determine impact on system
  - Performed throughout the life cycle
- Analytical Techniques
  - Failure modes and effects analysis (FMEA)
  - FMECA: Failure modes, effects and criticality analysis (FMECA)
  - ETA: Event tree analysis (ETA)
  - FTA: Fault tree analysis (FTA)
  - HAZOP: Hazard and operability studies (HAZOP)
- Standards

Hazard and Risk Analysis Process



Preliminary Hazard Identification

- First activity in safety process, performed during early requirements analysis (concept definition)
- Identifies potential hazard sources and accidents
- Sources of information include
  - system concept and operational environment
  - incident data of previous in-service operation and similar systems
  - technology and domain specific analyses and checklists
- Method is group-based and dependent on experience
- Process is largely informal
- Output is Preliminary Hazard List

Preliminary Hazard Analysis

- Refines hazards and accidents based on design proposal
- Performed using a system model that defines
  - scope and boundary of system
  - operating modes
  - system inputs, outputs and functions
  - preliminary internal structure
- Techniques for Preliminary Hazard Analysis include
  - Hazard and Operability Studies
  - Functional Failure Analysis
- Output is initial Hazard Log

Hazard Analysis

Failure Mode and Effects Analysis (FMEA)

Failure Modes, Effects and Criticality Analysis (FMECA)

Failure Mode and Effects Analysis

- **Failure modes and effects analysis** (FEMA) considers the failure of any component within a system and tracks the effects of this failure to determine its ultimate consequences.
  - Probably the most commonly used technique
  - Looks for consequences of component failures (forward chaining technique)

FMEA

- Manual analysis
  - Identify component, module or system failures
  - Determine consequences
  - Performed bottom-up
- Outputs
  - Spreadsheet noting each
    - failure mode
    - possible causes
    - consequences
    - possible remedies
  - Usually computer records kept
- Standardised by IEC (International Electrotechnical Commission)

29

FMEA

- Notes
  - Can be applied at any stage of the design process and at any level within the system
  - Teams of four to eight engineers
- Limitations:
  - Lot of unnecessary work, it considers all components/failure modes
  - Requires expert knowledge to decide what to analyze
  - Usually do not consider multiple failures

30

FMEA Example

FMEA for a microswitch

Ref No.	Unit	Failure mode	Possible cause	Local effects	System effects	Remedial action
1	Tool guard switch	Open-circuit contacts	(a) faulty component (b) excessive current (c) extreme temperature	Failure to detect tool guard in place	Prevents use of machine – system fails safe	Select switch for high reliability and low probability of dangerous failure. Rigid quality control on switch procurement
2		Short-circuit contacts	(a) faulty component (b) excessive current	System incorrectly senses guard to be closed	Allows machine to be used when guard is absent – dangerous failure	Modify software to detect switch failure and take appropriate action
3		Excessive switch-bounce	(a) ageing effects (b) prolonged high currents	Slight delay in sensing state of guard	Negligible	Ensure hardware design prevents excessive current through switch

31

Failure Modes, Effects and Criticality Analysis

- FMECA:
  - Extension to FMEA
  - Takes into account importance of each component
  - Determines probability/frequency of occurrence of failures
- Problems
  - Measuring reliability of components difficult
  - Models often too simplistic
  - Tool support needed
- Used as input to fault tree analysis
  - Standardised

32

Background

- FMECA was one of the first systematic techniques for failure analysis
- FMECA was developed by the U.S. Military. The first guideline was Military Procedure MIL-P-1629 “Procedures for performing a failure mode, effects and criticality analysis” dated November 9, 1949
- FMECA is the most widely used reliability analysis technique in the initial stages of product/system development
- FMECA is usually performed during the conceptual and initial design phases of the system in order to assure that all potential failure modes have been considered and the proper provisions have been made to eliminate these failures

What can FMECA be used for?

- Assist in selecting design alternatives with high reliability and high safety potential during the early design phases
- Ensure that all conceivable failure modes and their effects on operational success of the system have been considered
- List potential failures and identify the severity of their effects
- Develop early criteria for test planning and requirements for test equipment
- Provide historical documentation for future reference to aid in analysis of field failures and consideration of design changes
- Provide a basis for maintenance planning
- Provide a basis for quantitative reliability and availability analyses.

Types of FMECA

- **Design FMECA** is carried out to eliminate failures during equipment design, taking into account all types of failures during the whole life-span of the equipment
- **Process FMECA** is focused on problems stemming from how the equipment is manufactured, maintained or operated
- **System FMECA** looks for potential problems and bottlenecks in larger processes, such as entire production lines

FME(C)A Chart

Failure Modes and Effect Analysis								
Product Name: DeWalt Tradesman Drill				Part name: Rear Vent				
Function	Failure Mode	Effects of Failure	Causes of Failure	Current Controls	S	O	D	RPN
Allow Additional Air Flow	Filter Blocked	Overheated Motor	User Error	Visual Inspection	4	1	5	20
Prevent Dangerous Usage	Filter Not In Place	Larger Opening to Motor	User Error	Visual Inspection	8	4	1	32
Filter dust	Defective Filter	Additional dust flows into shell	Poor Materials	Visual Inspection	1	1	7	7

S = Severity rating (1 to 10)
O = Occurrence frequency (1 to 10)
D = Detection Rating (1 to 10)
RPN = Risk Priority Number (1 to 1000)

Severity Rating

Rank	*Severity class*	*Description*
10	Catastrophic	Failure results in major injury or death of personnel.
7-9	Critical	Failure results in minor injury to personnel, personnel exposure to harmful chemicals or radiation, or fire or a release of chemical to the environment.
4-6	Major	Failure results in a low level of exposure to personnel, or activates facility alarm system.
1-3	Minor	Failure results in minor system damage but does not cause injury to personnel, allow any kind of exposure to operational or service personnel or allow any release of chemicals into the environment

37

Detection Rating

Rank	*Description*
1-2	Very high probability that the defect will be detected. Verification and/or controls will almost certainly detect the existence of a deficiency or defect.
3-4	High probability that the defect will be detected. Verification and/or controls have a good chance of detecting the existence of a deficiency/defect.
5-7	Moderate probability that the defect will be detected. Verification and/or controls are likely to detect the existence of a deficiency or defect.
8-9	Low probability that the defect will be detected. Verification and/or control not likely to detect the existence of a deficiency or defect.
10	Very low (or zero) probability that the defect will be detected. Verification and/or controls will not or cannot detect the existence of a deficiency/defect.

38

Risk Ranking

- Risk Matrix
- Risk Ranking:
  - O = the rank of the occurrence of the failure mode
  - S = the rank of the severity of the failure mode
  - D = the rank of the likelihood the the failure will be detected before the system reaches the end-user/customer.
  - All ranks are given on a scale from 1 to 10. The risk priority
  - number (RPN) is defined as

    RPN = S × O × D
  - The smaller the RPN the better – and – the larger the worse.

Hazard Analysis

Hazard & Operability Analysis
(HAZOP)

Hazard & Operability Analysis

- HAZOP:
  - Developed in Chemical industry
  - Applied successfully in other domains
  - "What if" analysis for system parameters
  - E.g., suppose "temperature" of "reactor" "rises", what happens to system?
  - System realization of perturbation or sensitivity analysis
  - Requires flow model of operating plant

41

Hazard & Operability Analysis

- Flowing items are "entities"
- Entities have characteristic properties known as "attributes"
- Analysis based on possible deviations of attribute values
- "Guide words" used to guide the analysis— designed to capture dimensions of variation
- Supplementary adjectives add temporal element
- Different word sets for different applications

42

HAZOP examples

- Guide words:
  - no, more, less, early, late, before, ...

Interpretation examples:

- Signal arrives too late
- Incomplete data transmitted / only part of the intended activity occurs

- Attributes:
  - Data flow, data rate, response time, ...

43

HAZOP guide word interpretations

Guide word	*Chemical plant*	*Computer-based system*
No	No part of the intended result is achieved	No data or control signal exchanged
More	A quantitative increase in the physical quantity	A signal magnitude or a data rate is too high
Less	A quantitative decrease in the physical quantity	A signal magnitude or a data rate is too low
As well as	The intended activity occurs, but with additional results	Redundant data sent in addition to intended value
Part of	Only part of the intended activity occurs	Incomplete data transmitted
Reverse	The opposite of what was intended occurs, for example reverse flow within a pipe	Polarity of magnitude changes reversed
Other than	No part of the intended activity occurs, and something else happens instead	Data complete but incorrect
Early	Not used	Signal arrives too early with reference to clock time
Late	Not used	Signal arrives too late with reference to clock time
Before	Not used	Signal arrives earlier than intended within a sequence
After	Not used	Signal arrives later than intended within a sequence

44

HAZOP attributes

Attribute	*Guide word*	*Possible meaning*
Data flow	More	More data is passed than expected
	Less	Less data is passed than expected
Data rate	More	The data rate is too high
	Less	The data rate is too low
Data value	More	The data value is too high
	Less	The data value is too low
Repetition time	More	The time between output updates is too high
	Less	The time between output updates is too low
Response time	More	The response time is longer than required
	Less	The response time is shorter than required

© Gert Jervan

45

HAZOP Example

Item	*Inter-connection*	*Attribute*	*Guide word*	*Cause*	*Consequence*	*Recommendation*
1	Sensor supply line	Supply voltage	No	PSU, regulator or cable fault	Lack of sensor signal detected and system shuts down	
2			More	Regulator fault	Possible damage to sensor	Consider overvoltage protection
3			Less	PSU or regulator fault	Incorrect temperature reading	Include voltage monitoring
4		Sensor current	More	Sensor fault	Incorrect temperature reading, possible loading of supply	Monitor supply current
5			Less	Sensor fault	Incorrect temperature reading	As above
6	Sensor output	Voltage	No	PSU, sensor or cable fault	Lack of sensor signal detected and system shuts down	
7			More	Sensor fault	Temperature reading too high – results in decrease in plant efficiency	Consider use of duplicate sensor
8			Less	Sensor mounted incorrectly or sensor failure	Temperature reading too low – could result in overheating and possible plant failure	As above

© Gert Jervan

46

Hazard Analysis

Fault Tree Analysis
(FTA)

Fault Tree Analysis

- Fault tree analysis (FTA) is a top-down approach to failure analysis, starting with a potential undesirable event (accident) called a TOP event, and then determining all the ways it can happen.
- The analysis proceeds by determining how the TOP event can be caused by individual or combined lower level failures or events.
- The causes of the TOP event are “connected” through logic gates
- FTA is the most commonly used technique for causal analysis in risk and reliability studies.

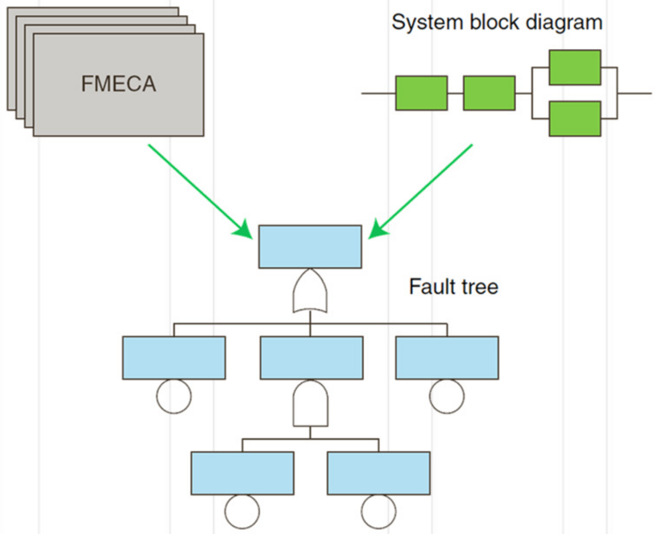
48

History

- FTA was first used by Bell Telephone Laboratories in connection with the safety analysis of the Minuteman missile launch control system in 1962
- Technique improved by Boeing Company
- Extensively used and extended during the Reactor safety study (WASH 1400)

49

Preparations for FTA



50

Boundary Conditions

- The physical boundaries of the system (Which parts of the system are included in the analysis, and which parts are not?)
- The initial conditions (What is the operational stat of the system when the TOP event is occurring?)
- Boundary conditions with respect to external stresses (What type of external stresses should be included in the analysis – war, sabotage, earthquake, lightning, etc?)
- The level of resolution (How detailed should the analysis be?)

51

Fault Tree Construction

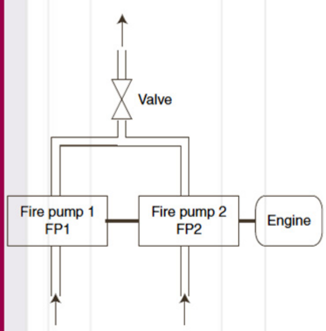
- Define the TOP event in a clear and unambiguous way.
  Should always answer:
  What e.g., "Fire"
  Where e.g., "in the process oxidation reactor"
  When e.g., "during normal operation"
- What are the immediate, necessary, and sufficient events and conditions causing the TOP event?
- Connect via a logic gate
- Proceed in this way to an appropriate level (= basic events)
- Appropriate level:
  - Independent basic events
  - Events for which we have failure data

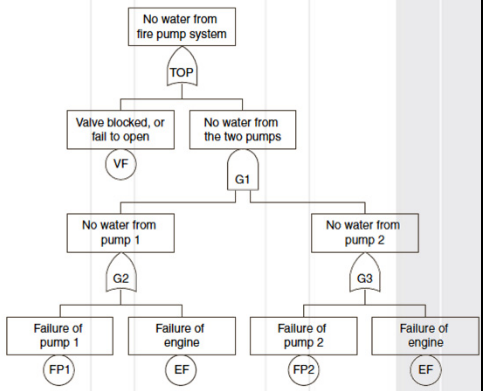
52

Fault Tree Symbols

Logic gates	OR-gate	The OR-gate indicates that the output event occurs if any of the input events occur
	AND-gate	The AND-gate indicates that the output event occurs only if all the input events occur at the same time
Input events (states)		The basic event represents a basic equipment failure that requires no further development of failure causes
		The undeveloped event represents an event that is not examined further because information is unavailable or because its consequences are insignificant
Description of state		The comment rectangle is for supplementary information
Transfer symbols	Transfer out Transfer in	The transfer-out symbol indicates that the fault tree is developed further at the occurrence of the corresponding transfer-in symbol

Fault Tree Example



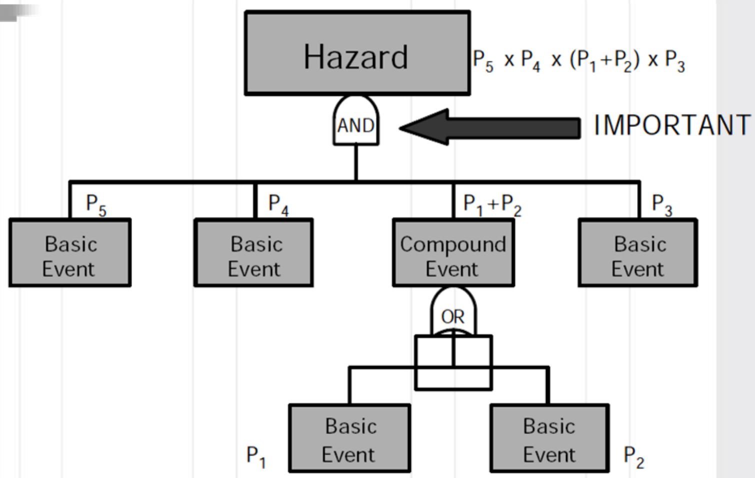


Elementary Fault Tree Analysis

- Assignment of probabilities to specific events
- Computation of probabilities for compound events
- Sophisticated dependability analysis possible
- Extensive, elaborate, established technique
- Provides:
  - Mechanism for showing that design will meet dependability requirements

55

Fault Trees and Probabilities



56

Practical Fault Trees

- Developed by human analysis
- Tend to be *very* large for real systems
- Evolve as insight is gained
- Many analysis techniques possible:
  - Hazard probability can be calculated if probabilities associated with all basic events
  - Tables of probabilities available for degradation faults for common components
  - Recall, infeasible for design faults

Hazard Analysis

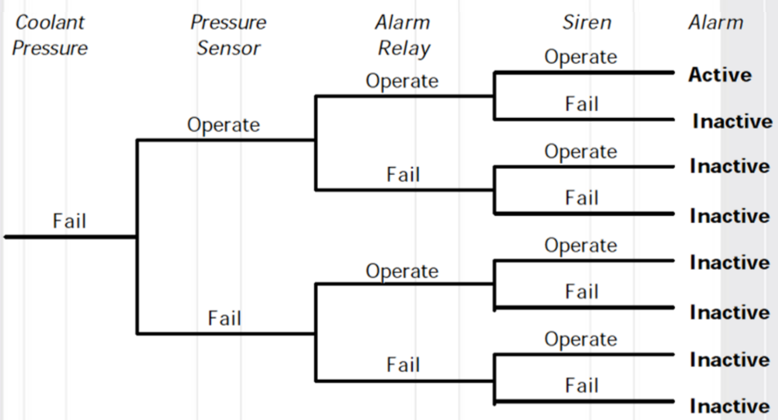
Event Tree Analysis
(ETA)

Event Trees

- Event sequences that follow from some initial event of interest, usually a component failure
- Downstream events follow from original event and subsequent events of other components
- E.g. Chemical plant pressure sensor sounds siren when pressure drops to unsafe level

59

Event Tree



60

Barriers

- Most well designed systems have one or more barriers that are implemented to stop or reduce the consequences of potential accidental events. The probability that an accidental event will lead to unwanted consequences will therefore depend on whether these barriers are functioning or not.
- The consequences may also depend on additional events and factors. Examples include:
  - Whether a gas release is ignited or not
  - Whether or not there are people present when the accidental event occurs
  - The wind direction when the accidental event occurs
- Barriers may be technical and/or administrative (organizational).

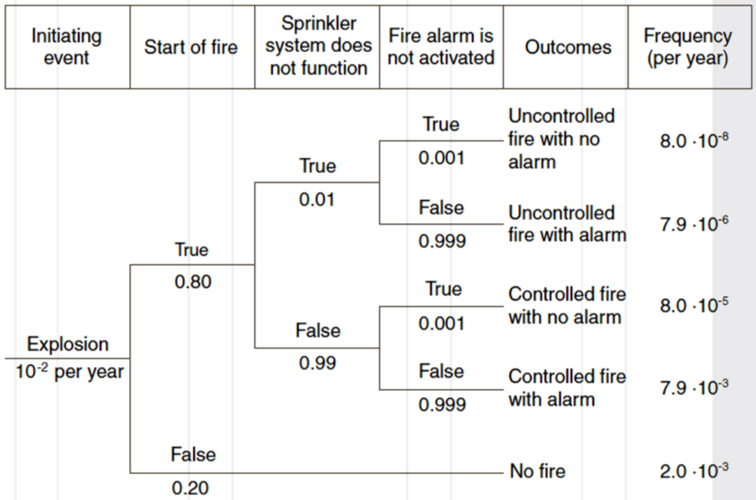
61

Event Tree Analysis

- An event tree analysis (ETA) is an inductive procedure that shows all possible outcomes resulting from an accidental (initiating) event, taking into account whether installed safety barriers are functioning or not, and additional events and factors.
- By studying all relevant accidental events (that have been identified by a preliminary hazard analysis, a HAZOP, or some other technique), the 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.

62

ETA Example



© Gert Jervan

63

ETA Pros and Cons

- Positive
  - 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
- Negative
  - No standard for the graphical representation of the event tree
  - Only one initiating event can be studied in each analysis
  - 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

© Gert Jervan

64

Hazard Analysis in the Life Cycle

- FME(C)A
  - Used to generate event trees and fault trees
- FME(C)A, FTA, ETA
  - Appropriate when functional design complete
- Preliminary HAZOP
  - Early in the life-cycle
  - Identify hazards, take account of them in the design
- Full HAZOP
  - Later in the life-cycle
  - Identify further hazards, feed back into design design

65