

© Gert Jervan, TTÜ/ATI

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

Department of computer Engineering  
ati.ttu.ee

IAF0030

## Arvutitehnika erikursus I

Süsteemide usaldusväärsus ja veakindlus  
Dependability and fault tolerance

**Loengud 2 ja 3**  
**Safety, Hazards, Risks**

**gert.jervan@pld.ttu.ee**


Tallinn University of Technology  
Department of Computer Engineering  
Estonia

© Gert Jervan, TTÜ/ATI

IAF0030 - Arvutitehnika erikursus I

## Lecture Outline

- ✓ Dependability
- ✓ Safety Requirements
- ✓ Hazards
- ✓ Hazard Analysis
- ✓ Risks
- ✓ Risk Analysis
- ✓ Risk Management
- ✓ Safety & SILs
- ✓ Risk Reduction & Design



1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

2

© Gert Jervan, TTÜ/ATI

IAF0030 - Arvutitehnika erikursus I

## Dependability: an integrating concept

- ✓ **Dependability** is a property of a system that justifies placing one's reliance on it.
- ✓ High reliability and high availability

**Dependability**

- attributes
  - Availability
  - Reliability
  - Safety
  - Confidentiality
  - Integrity
  - Maintainability
- means
  - Fault prevention
  - Fault tolerance
  - Fault removal
  - Fault forecasting
- threats
  - Faults
  - Errors
  - Failures

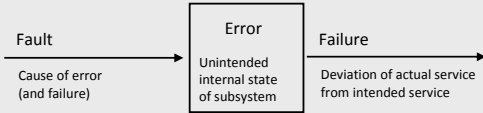
1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

3

© Gert Jervan, TTÜ/ATI

IAF0030 - Arvutitehnika erikursus I

## Threats: Faults, Errors & Failures



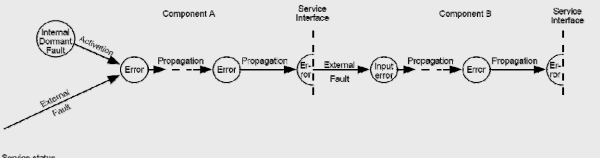
1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

4

© Gert Jervan, TTÜ/ATI

IAF0030 - Arvutitehnika erikursus I

## The pathology of failure



1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

5

© Gert Jervan, TTÜ/ATI

IAF0030 - Arvutitehnika erikursus I

## Three-universe model

- ✓ **Physical universe: where the faults occur**
  - Physical entities: semiconductor devices, mechanical elements, displays, printers, power supplies
  - A fault is a physical defect or alteration of some component in the physical universe
- ✓ **Informational universe: where the error occurs**
  - Units of information: bits, data words
  - An error has occurred when some unit of information becomes incorrect
- ✓ **External (user's universe): where failures occur**
  - User sees the effects of faults and errors
  - The failure is any deviation from the desired or expected behavior

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

6

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Causes of faults

✓ Problems at any stages of the design process can result in faults within the system.

```

    graph LR
      SM[Specification Mistakes] --> SF[Software Faults]
      IM[Implementation Mistakes] --> SF
      ED[External Disturbances] --> SF
      CD[Component Defects] --> HF[Hardware Faults]
      SF --> E[Errors]
      HF --> E
      E --> SysF[System Failures]
    
```

TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

7

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Causes of faults, cont.

- ✓ Specification mistakes
  - Incorrect algorithms, architectures, hardware or software design specifications
    - Example: the designer of a digital circuit incorrectly specified the timing characteristics of some of the circuit's components
- ✓ Implementation mistakes
  - Implementation: process of turning the hardware and software designs into physical hardware and actual code
  - Poor design, poor component selection, poor construction, software coding mistakes
    - Examples: software coding error, a printed circuit board is constructed such that adjacent lines of a circuit are shorted together

TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

8

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Causes of faults, cont.

- ✓ Component defects
  - Manufacturing imperfections, random device defects, component wear-out
  - Most commonly considered causes of faults
    - Examples: bonds breaking within the circuit, corrosion of the metal
- ✓ External disturbance
  - Radiation, electromagnetic interference, operator mistakes, environmental extremes, battle damage
    - Example: lightning

TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

9

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Elementary fault classes

```

    graph LR
      FAULTS --- POC[PHASE OF CREATION OR OCCURENCE]
      FAULTS --- SB[SYSTEM BOUNDARIES]
      FAULTS --- DOMAIN
      FAULTS --- PC[PHENOMENOLOGICAL CAUSE]
      FAULTS --- INTENT
      FAULTS --- PERSISTENCE
      POC --- DF[DEVELOPMENTAL FAULTS]
      POC --- OF[OPERATIONAL FAULTS]
      SB --- IF[INTERNAL FAULTS]
      SB --- EF[EXTERNAL FAULTS]
      DOMAIN --- HF[HARDWARE FAULTS]
      DOMAIN --- SF[SOFTWARE FAULTS]
      PC --- NF[NATURAL FAULTS]
      PC --- HMF[HUMAN-MADE FAULTS]
      INTENT --- ADF[ACCIDENTAL, OR NON-MALICIOUS DELIBERATE FAULTS]
      INTENT --- DMF[DELIBERATELY MALICIOUS FAULTS]
      PERSISTENCE --- PF[PERMANENT FAULTS]
      PERSISTENCE --- TF[TRANSIENT FAULTS]
    
```

TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

10

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Classification of faults

TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

11

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Failure modes

```

    graph LR
      DOMAIN --- VF[VALUE FAILURES]
      DOMAIN --- TF[TIMING FAILURES]
      CONTROLABILITY --- CF[CONTROLLED FAILURES]
      CONTROLABILITY --- UCF[UNCONTROLLED FAILURES]
      CONSISTENCY --- CCF[CONSISTENT FAILURES]
      CONSISTENCY --- ICCF[INCONSISTENT FAILURES]
      CONSEQUENCES --- MF[MINOR FAILURES]
      CONSEQUENCES --- CFAT[CATASTROPHIC FAILURES]
      VF --- FS[FAILURE SYMPTOMS]
      TF --- FS
      CF --- FS
      UCF --- FS
      CCF --- FS
      ICCF --- FS
      MF --- FS
      CFAT --- FS
      FS --- FA[FALSE ALARM]
      FS --- DS[DEGRADED SERVICE]
      FS --- SS[SAFE SHUTDOWN]
      FS --- SF[SIGNALLED FAILURE]
      FS --- CR[CRASH FAILURE]
      FS --- US[UNSIGNALLED FAILURE]
      FS --- DF[DECEPTIVE FAILURE]
      FS --- BF[BYZANTINE FAILURE]
      FS --- FS2[FAILURE SEVERITIES]
    
```

TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

12

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Failure modes, cont.

- ✓ Failure domain
  - Value failures : incorrect value delivered at interface
  - Timing failures : right result at the wrong time (usually late)
- ✓ Failure consistency
  - Consistent failures : all nodes see the same, possibly wrong, result
  - Inconsistent failures : different nodes see different results
- ✓ Failure consequences
  - Benign failures : essentially loss of utility of the system
  - Malign failures : significantly more than loss of utility of the system; catastrophic, e.g. airplane crash
- ✓ Failure oftenness (failure frequency and persistency)
  - Permanent failure : system ceases operation until it is repaired
  - Transient failure : system continues to operate
    - Frequently occurring transient failures are called intermittent

13

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Dependability

14

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Dependability attributes

- ✓ **Availability:** readiness for correct service
- ✓ **Reliability:** continuity of correct service
- ✓ **Safety:** absence of catastrophic consequences on the user(s) and the environment
- ✓ **Confidentiality:** absence of unauthorized disclosure of information
- ✓ **Integrity:** absence of improper system alterations
- ✓ **Maintainability:** ability to undergo, modifications, and repairs
- ✓ **Security:** the concurrent existence of (a) availability for authorized users only, (b) confidentiality, and (c) integrity with 'improper' taken as meaning 'unauthorized'.

15

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Dependability

16

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Means to achieve dependability

- ✓ **Fault-prevention:** how to prevent, by **construction**, fault occurrence.
- ✓ **Fault-tolerance:** how to provide, by **redundancy**, service complying with the specification in spite of faults having occurred or occurring.
- ✓ **Fault-removal:** how to minimize, by **verification and validation**, the presence of latent faults.
- ✓ **Fault-forecasting:** how to minimize, by **evaluation**, the presence, the creation and the consequences of faults.

17

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Means to achieve dependability, cont.

18

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Fault prevention

- ✓ Attained by quality control techniques
  - Software
    - Structured/object oriented programming
    - Information hiding
    - Modularization
  - Hardware
    - Rigorous design rules
    - Shielding
    - Radiation hardening
    - "Foolproof" packaging
- ✓ Note:
  - Malicious faults can also be prevented; Example: firewalls

TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

19

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Fault tolerance

- ✓ **Fault tolerance** is the ability of a system to continue to perform its functions (deliver correct service), even when one or more components have failed.
  - **Masking**: the use of sufficient redundancy may allow recovery without explicit error detection.
  - **Reconfiguration**: eliminating a faulty entity from a system and restoring the system to some operational condition or state.
    - Error **detection**: recognizing that an error has occurred
    - Error **location**: determining which module produced the error
    - Error **containment**: preventing the errors from propagating
    - Error **recovery**: regaining operational status

TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

20

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## The concept of redundancy

- ✓ Definition
  - **Redundancy** is the addition of information, resources, or time beyond what is needed for normal system operation.
- ✓ Digital filter example
  - Software redundancy: lines of software to perform a validity checks
  - Hardware redundancy : if more memory needed for the software checks
  - Time redundancy: each filter calculation performed twice to detect faults
  - Information redundancy: output using with a simple parity bit

```

graph LR
  Input --> ADC[Analog-to-digital converter]
  ADC --> Microprocessor
  Microprocessor --> DAC[Digital-to-analog converter]
  DAC --> Output
  
```

TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

21

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Error detection

- ✓ Two ways to detect errors:
  1. a priori knowledge about intended state
  2. comparing results of two redundant computational channels
- ✓ Notes
  - Errors can happen in the **value domain** and/or in the **time domain**.
  - The probability that an error is detected, provided it is present, is called the **error detection coverage**.
  - The time interval between the start of an error and the detection of an error is the **error detection latency**.

TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

22

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## A priori Knowledge flexibility vs. error-detection coverage

- ✓ **Syntactic knowledge about code space**
  - Parity bits, CRC
- ✓ **Assertions and acceptance tests**
  - Valid data values, properties of the controlled object
    - Development of physical processes, plausibility of data sets
- ✓ **Activation patterns of computation**
  - Regularity in execution pattern, e.g., frequency of updates
    - Limited by the update frequency and clock synchronisation
    - Event every second, on the second -> detect missing event
- ✓ **Worst case execution time of tasks**
  - Must be known to calculate real-time schedules
  - A priori information about the execution of a task can be used for detecting task errors

TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

23

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Redundant Computations

Type of Redundancy	Implementation	Type of Detected Errors
Time redundancy	Same software executed on the same hardware during two different time-intervals	Errors caused by transient physical faults in hardware with a duration less than one execution time slot
Hardware redundancy	The same software executes on two independent hardware channels	Errors caused by transient and permanent physical hardware errors
Diverse software on the same hardware	Different software versions are executed on the same hardware during two different time intervals	Errors caused by independent software faults and transient physical faults in the hardware with a duration less than one execution time slot
Diverse software on diverse hardware	Two different versions of software are executed on two independent hardware channels	Errors caused by independent software faults and by transient and permanent physical hardware faults

TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

24

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Recovery

- ✓ Definition
  - **Recovery** transforms a system state that contains one or more errors and (possibly) faults into a state without detected errors and faults that can be activated again.
- ✓ Consists of
  - Error handling
    - **Rollback**: returning to a saved state (checkpoint)
    - **Compensation**: enough redundancy to eliminate the error
    - **Rollforward**: the state without errors is a new state
  - Fault handling
    - **Fault diagnosis**: identifies the cause of errors, location and type
    - **Fault isolation**: physical or logical exclusion of the faulty components
    - **System reconfiguration**: switches in spares or re-assigns tasks
    - **System reinitialization**: checks, updates and records the new configuration

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 25

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Fault removal

- ✓ **Verification**: "Are we building the system right?"
  - Static: does not exercise the system
    - Static analysis: inspections, walkthroughs, model checking
  - Dynamic
    - Symbolic execution: inputs are symbolic
    - Testing: actual inputs
  - Fault injection
- ✓ **Validation**: "Are we building the right system?"
  - Checking the specification

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 26

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Fault Forecasting

- ✓ Evaluation of the system behavior with respect to fault occurrence
  - **Qualitative** evaluation
    - Identifies, classifies, ranks the failure modes or the event combinations that lead to system failures
    - Example methods: Failure mode and effect analysis, fault-tree analysis
  - **Quantitative** evaluation
    - Evaluates in terms of probabilities the extent to which some of the dependability are satisfied (measures dependability)
    - Example methods: Markov chains, reliability block diagrams

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 27

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY Department of computer Engineering  [ati.ttu.ee](http://ati.ttu.ee)

## Safety Requirements

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 29

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 30

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

31

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

32

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

Department of computer Engineering  
ati.ttu.ee

## Hazard Analysis

Hazards & Risk Definitions

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

34

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

35

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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...

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

36

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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
 
$$\text{risk} = \text{penalty} \times (\text{probability per year})$$

$$= 500 \times (0.0001)$$

$$= 0.05 \text{ deaths per year}$$
- ✓ 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

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY 37

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY 38

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY 39

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

Department of computer Engineering  
ati.ttu.ee

## Hazards

### Hazards Overview

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY 41

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Hazard Categories for Civil Aircraft

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

© G.F. Marsters

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY 42

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

### 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	$< 1 \times 10^{-9}$

© G.F. Marsters

Risk from lightning is  $5 \times 10^{-7}$  deaths per person year

43

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

### 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

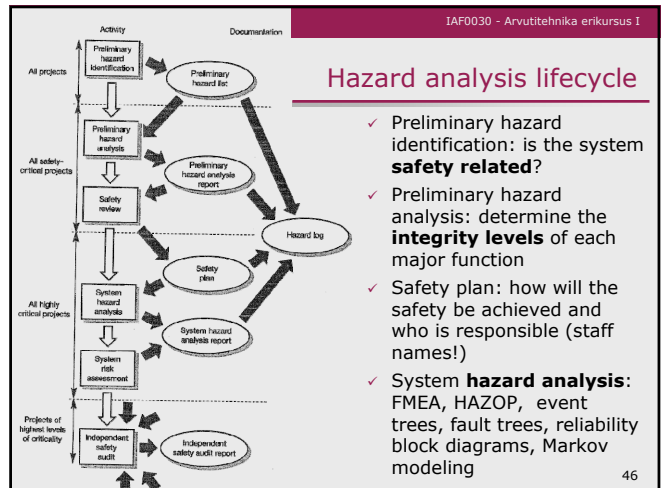
- Acceptable - only ALARP actions considered
- Acceptable - use ALARP principle and consider further investigations
- Not acceptable - risk reducing measures required

44

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY Department of computer Engineering ati.ttu.ee

## Hazards

### Hazard Analysis

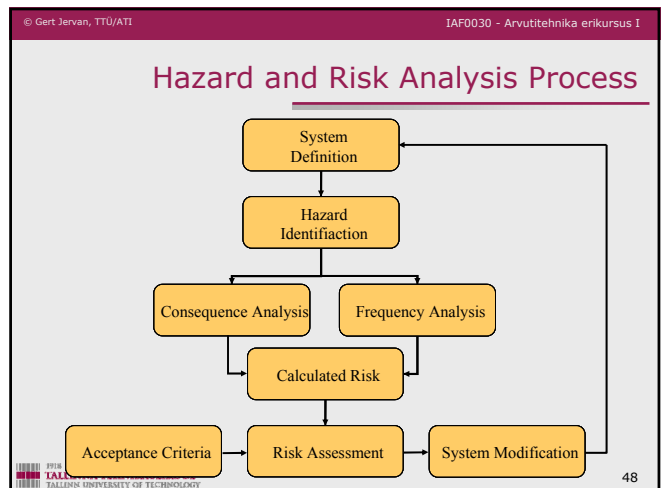


© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

### 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

47



© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

49

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

50

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

Department of computer Engineering  
ati.ttu.ee

## Hazard Analysis

Failure Mode and Effects Analysis (FMEA)

Failure Modes, Effects and Criticality Analysis (FMECA)

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Failure Mode and Effects Analysis

- ✓ **Failure modes and effects analysis (FMEA)** 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)

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

52

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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)

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

53

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

54

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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	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
			(b) excessive current			
2		Short-circuit contacts	(a) faulty component	System incorrectly senses guard is absent – dangerous failure	Allows machine to be used when guard is absent – dangerous failure	Rigid quality control on switch procurement
			(b) excessive current			
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

55

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

56

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

57

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

58

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

59

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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)

60

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 61

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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.

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 62

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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
 
$$RPN = S \times O \times D$$
  - The smaller the RPN the better – and – the larger the worse.

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 63

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY Department of computer Engineering [ati.ttu.ee](http://ati.ttu.ee)

## Hazard Analysis

### Hazard & Operability Analysis (HAZOP)

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 65

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 66

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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, ...

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 67

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 68

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## HAZOP attributes

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

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 69

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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	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

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 70

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY

Department of computer Engineering  
ati.ttu.ee

## Hazard Analysis

Fault Tree Analysis (FTA)

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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.

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 72

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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)

73

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Preparations for FTA

74

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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?)

75

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

76

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Fault Tree Symbols

Logic gates	<p>OR-gate</p>	The OR-gate indicates that the output event occurs if any of the input events occur
	<p>AND-gate</p>	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	<p>Transfer out</p>	The transfer-out symbol indicates that the fault tree is developed further at the occurrence of the corresponding transfer-in symbol
	<p>Transfer in</p>	

77

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Fault Tree Example

78

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

79

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Fault Trees and Probabilities

80

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

81

Department of computer Engineering  
ati.ttu.ee

## Hazard Analysis

Event Tree Analysis (ETA)

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

83

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## Event Tree

Coolant Pressure	Pressure Sensor	Alarm Relay	Siren	Alarm	
Fail	Operate	Operate	Operate	Active	
			Fail	Inactive	
		Fail	Operate	Inactive	
			Fail	Inactive	
	Fail	Operate	Operate	Operate	Inactive
				Fail	Inactive
		Fail	Operate	Operate	Inactive
				Fail	Inactive

84

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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).

85

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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.

86

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## ETA Example

Initiating event	Start of fire	Sprinkler system does not function	Fire alarm is not activated	Outcomes	Frequency (per year)	
Explosion $10^{-2}$ per year	True 0.80	True 0.01	True	Uncontrolled fire with no alarm	$8.0 \cdot 10^{-8}$	
			False	Uncontrolled fire with alarm	$7.9 \cdot 10^{-6}$	
		False 0.99	True	Controlled fire with no alarm	$8.0 \cdot 10^{-2}$	
			False	Controlled fire with alarm	$7.9 \cdot 10^{-2}$	
	False 0.20				No fire	$2.0 \cdot 10^{-3}$

87

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

88

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

## 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

89

Department of computer Engineering  
ati.ttu.ee

1918  
TALLINNA TEHNIKAÜLIKOOL  
TALLINN UNIVERSITY OF TECHNOLOGY

## Risk Analysis

90