Dependable Computer Systems

Part 5: Failure Modes and Models

Contents

- Recap from Part 3: Canonical Failure Classification
- Failure Mode Hierarchy
- Fault-Hypothesis, Failure Semantics, and Assumption Coverage
- Failure Hypothesis Estimation
- Overview of Safety Analysis Methods
- Comparison of Safety Analysis Methods

Recap from Part 3: Canonical Failure Classification

Failures

Recap:

A **(service) failure** is an event that occurs when the delivered service deviates from correct service.

- Thus, a *failure is a transition* from correct service to incorrect service.

Failure Mode Classification – Overview

- Domain:
  - content, early timing failure, late timing failure, halt failure, erratic failure
- Detectability:
  - signaled failures, unsignaled failures
- Consistency:
  - consistent failure, inconsistent failure
- Consequences:
  - minor failure, ..., catastrophic failure

Failure Mode Classification – Domain

- Content
- Early timing failure
- Late timing failure
- Halt failure
  - the external state becomes constant, i.e., system activity is no longer perceptible to the users
  - silent failure mode is a special kind of halt failure in that no service at all is delivered
- Erratic failure
  - not a halt failure, e.g., a babbling idiot failure

Failure Mode Classification – Consistency

When there are more than one users of a service.

- Consistent failure:
  - All users experience the same incorrect service.
- Inconsistent failure
  - Different users experience different incorrect services.

Failure Mode Classification – Consequences, e.g., Aircraft

Minor: 10E-5 per flight hour or greater

no significant reduction of aeroplane safety, a slight reduction in the safety margin

Major: between 10E-5 and 10E-7

significant reduction in safety margins or functional capabilities, significant increase in crew workload or discomfort for occupants

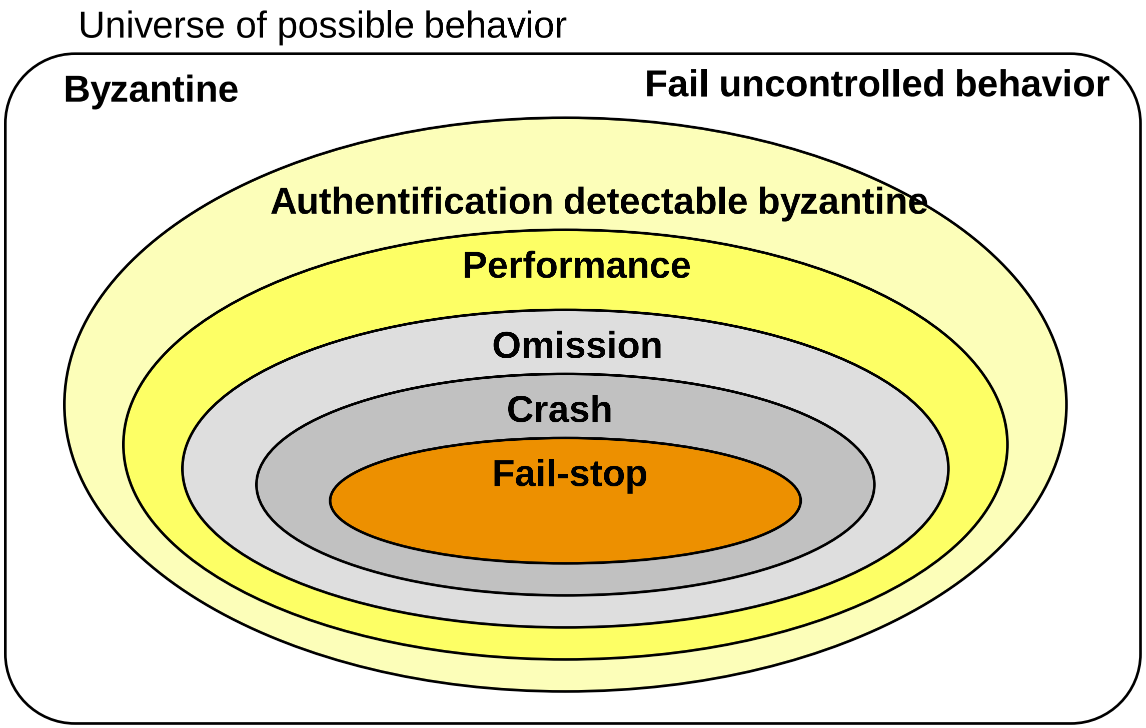
Hazardous: between 10E-7 and 10E-9

large reduction in safety margins or functional capabilities, causes serious or fatal injury to a relatively small number of occupants

Catastrophic: less than 10E-9

these failure conditions would prevent the continued safe flight and landing of the aircraft

Failure Mode Hierarchy


Universe of possible behavior
Byzantine
Fail uncontrolled behavior
Authentification detectable byzantine
Performance
Omission
Crash
Fail-stop

Based on the *strength* of the assumptions the failure modes form a hierarchy.

- byzantine failures are based on the weakest assumption (a non-assumption)
- fail-stop failures are based on the strongest assumptions (only correct results, information about the last correct state in case of a failure)

Failure Mode Hierarchy (cont.)

- **Byzantine or arbitrary failures:**
  there is no restriction on the behavior at the system interface, this mode is often called fail-uncontrolled
  (“two-faced” behavior, forging of messages)

- **Authentification detectable byzantine failures:**
  the only restriction on the behavior at the system interface is that messages of other systems cannot be forged
  (this failure mode applies only to distributed systems)

Failure Mode Hierarchy (cont.)

- **Performance failures:**
  under this failure mode systems deliver correct results in the value domain, in the time domain results may be early or late (early or late failures)

- **Omission failures:**
  a special class of performance failures where results are either correct or infinitely late (for distributed systems subdivision in send and receive omission failures)

Failure Mode Hierarchy (cont.)

- **Crash failures:**
  a special class of omission failures where a system does not deliver any subsequent results if it has exhibited an omission failure once
  (the system is said to have crashed)

- **Fail-Stop failures:**
  besides the restriction to crash failures it is required that other (correct) systems can detect whether the system has failed or not and can read the last correct state from a stable storage

Fault-Hypothesis, Failure Semantics, and Assumption Coverage

Fault-Hypothesis, etc.

Concepts

- **Fault hypothesis:**
  The fault hypothesis specifies anticipated faults which a server must be able to handle (also fault assumption).
- **Failure semantics:**
  A server exhibits a given failure semantics if the probability of failure modes which are not covered by the failure semantics is sufficiently low.
- **Assumption coverage:**
  Assumption coverage is defined as the probability that the possible failure modes defined by the failure semantics of a server proves to be true in practice conditions on the fact that the server has failed.

Fault-Hypothesis, etc. (cont.)

Importance of assumption coverage

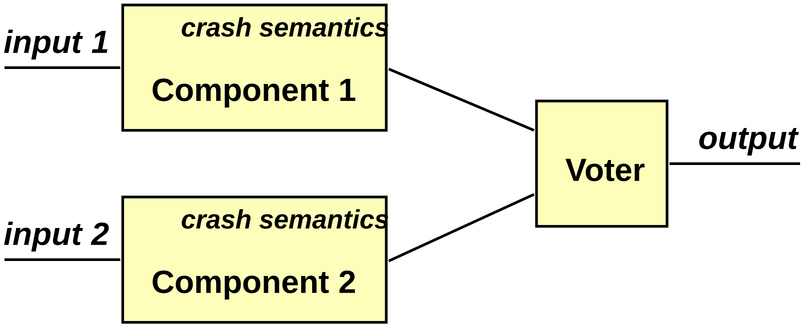
- The definition of a proper fault hypothesis, failure semantics and achievement of *sufficient* coverage is one of the most important factors.

- If the fault hypothesis (or failure semantics) is violated a system may fail as a whole.

Fault-Hypothesis, etc. (cont.)

Assumption Coverage Example

If component 1 or 2 violates its failure semantics the system fails, although it was designed to tolerate 1 component failure.



Fault-Hypothesis, etc. (cont.)

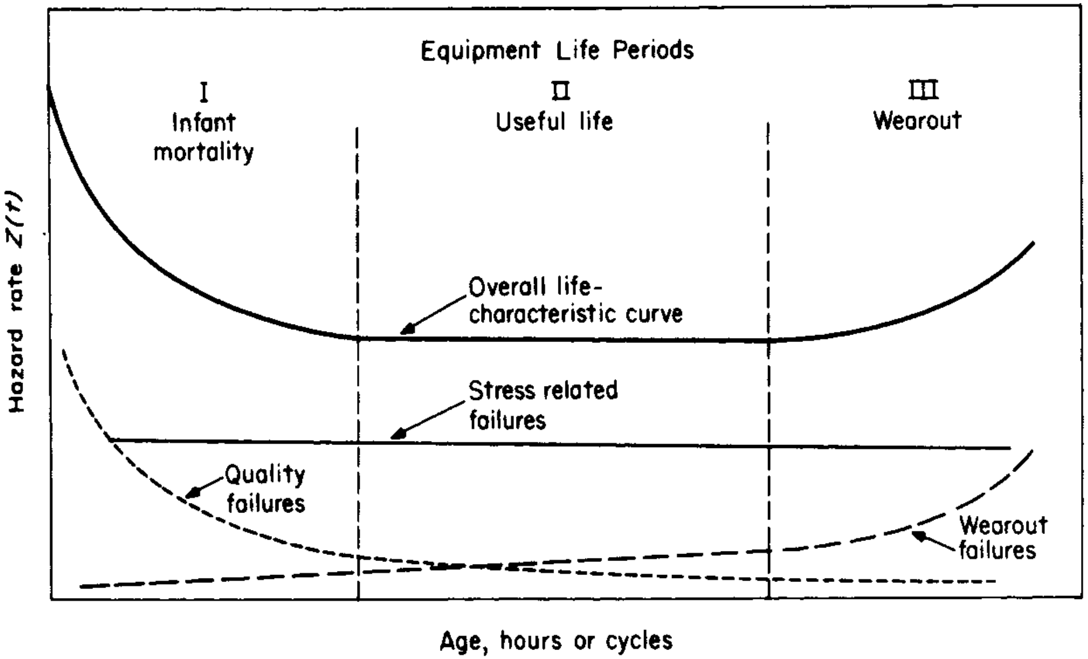
The Titanic or: violated assumption coverage

- **The fault hypothesis:**
  The Titanic was built to stay afloat if less or equal to 4 of the underwater departments were flooded.
- **Rationale of fault hypothesis:**
  This assumption was reasonable since previously there had never been an incident in which more than four compartments of a ship were damaged.
- **But:**
  Unfortunately, the iceberg ruptured five spaces, and the following events went down to history.

Failure Hypothesis Estimation

Life-characteristics curve (Bathtub curve)

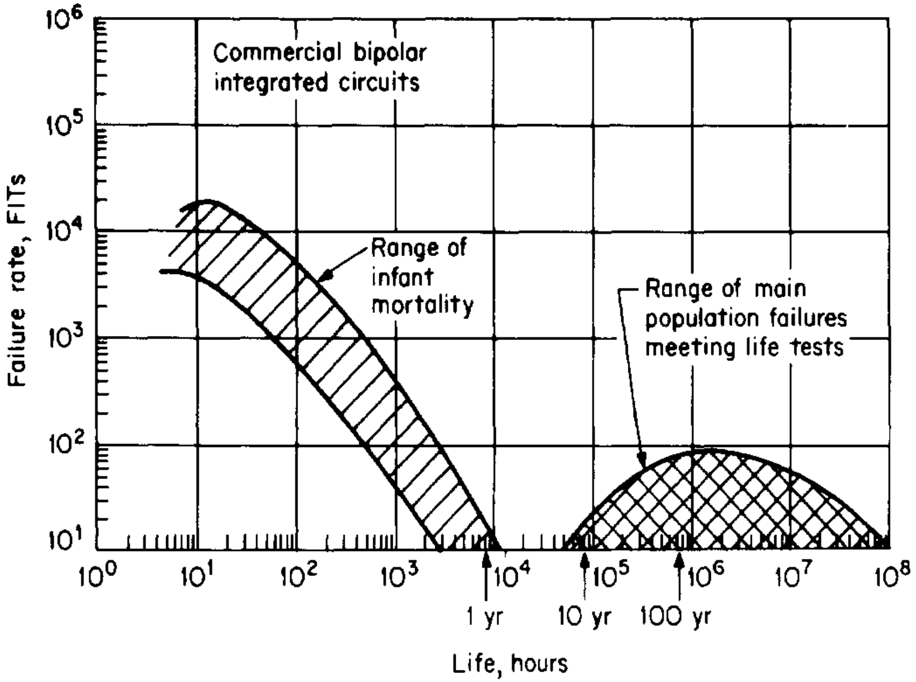
- For semiconductors, out of three terms describing the life characteristics only *infant mortality* and the *constant-failure-rate* region are of concern



Life-characteristics curve, showing the three components of failure

Semiconductor failure rate

- a typical failure rate distribution for semiconductors shows that wear out is of no concern



Semiconductor failure rate

Stress Tests

- semiconductor failures are stress dependent
- the most influential stress factor is temperature

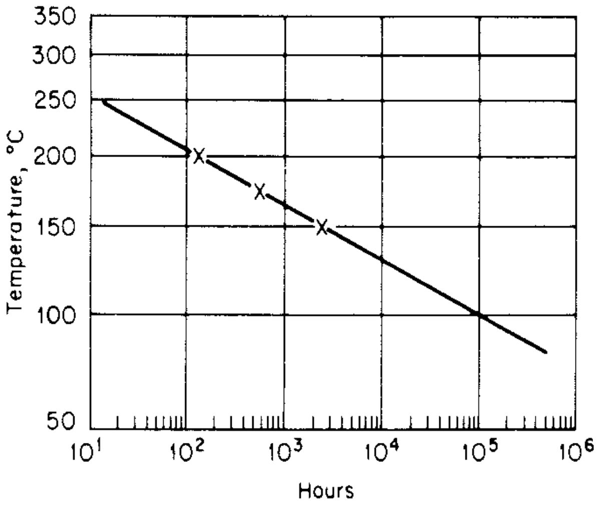
Stress Tests (cont.)

Arrhenius equation

- the basic relationship between the activation rate of failures and temperature is described by the Arrhenius equation

$$R = R_0 e^{-\frac{E_A}{kT}}$$

R_0 .. constant
T .. absolute temperature (K)
E_A .. activation energy (eV)
k .. Boltzmann’s constant 8.6 10^{-5} eV/K



Arrhenius plot (E_A = 1 eV)

Stress Tests (cont.)

Accelerated stress testing of semiconductors

- to remove freaks and infant-mortality failures (screening)
- to determine the expected failure rate

Accelerated conditions:

accelerated temperature

cycling of temperature

temperature and voltage stress

temperature, voltage and humidity stress

lowering of temperature

high temperature and current

α particles

high voltage gradients

Stress Tests (cont.)

Software stress

- For software there is no sound empirical and mathematical basis to use stress as a method to characterize the behavior of components.
  - it is currently unknown how to characterize stress for software
  - it is impossible to carry out accelerated stress tests to examine failure rates for software
  - for software there is no such relation as the Arrhenius equation which describes the activation rate of failures
  - there is no general possibility to “over-engineer” a system to handle conditions which are more stressful

Hardware/Software Interdependence

- software depends on hardware:
  - software requires hardware to execute (e.g. Intel's Pentium bug)

- hardware depends on software:
  - VLSI design uses software tools
  - PCB layout and routing by software tools
  - EMC analysis by software tools
  - hardware testers are software driven

Overview of Safety Analysis Methods

Safety Analysis (cont.)

Concepts

System Safety: is a subdiscipline of system engineering that applies scientific, management, and engineering principles to ensure adequate safety, throughout the operational life cycle, within the constraints of operational effectiveness, time and cost.

Safety: has been defined as “freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property”. safety has to be regarded as a relative term.

Software Safety: to ensure that the software will execute within a system context without resulting in unacceptable risk

Safety analysis

Overview

- includes complete life cycle of project/product (specification, design, maintenance, modification, ...)
- definition of responsibilities
- communication with other groups
- complete documentation
- analysis of complex processes
- management procedures (specialists, meetings, action reviews, time schedule, ...)

Safety Analysis (cont.)

Major topics of Safety analysis

- which (hazard analysis)
- how (accident sequencing)
- how likely (quantitative analysis)

Safety Analysis (cont.)

Safety analysis methodologies

- Preliminary Hazards Analysis (PHA)
- Hazards and Operability Study (HAZOP)
- Action Error Analysis (AEA)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Failure Modes and Effect Analysis (FMEA)
  Failure Modes, Effect and Criticality Analysis (FMECA)
- Cause-consequence analysis

Safety Analysis (cont.)

Preliminary hazard analysis (PHA)

- The first step in any safety program is to identify hazards and to categorize them with respect to criticality and probability

  - define system hazards
  - define critical states and failure modes
  - identify critical elements
  - determine consequences of hazardous events
  - estimate likelihood of hazardous events
  - issues to be analyzed in more detail

Safety Analysis (cont.)

Hazards and Operability Study (HAZOP)

Based on a systematic search to identify deviations that may cause hazards during system operation

Intention: for each part of the system a specification of the “intention” is made

Deviation: a search for deviations from intended behavior which may lead to hazards

Guide Words: Guide words on a check list are employed to uncover different types of deviations
(NO, NOT, MORE, LESS, AS WELL AS, PART OF, REVERSE, OTHER THAN)

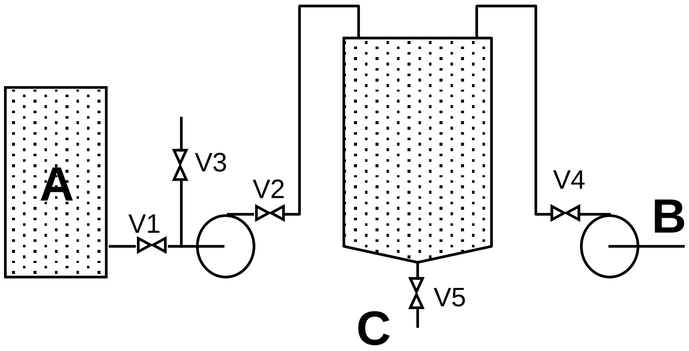
Team: the analysis is conducted by a team, comprising different specialists

Safety Analysis (cont.)

Example for HAZOP

- **Intention:** pump a specified amount of A to reaction tank B. Pumping of A is complete before B is pumped over.

NO or NOT
– the tank containing A is empty
– one of the pipe's two valves V1 or V2 is closed
– the pump is blocked, e.g. with frozen liquid
– the pump does not work (switched off, no power, ...)
– the pipe is broken
CONSEQUENCE is serious, a possible explosion



MORE
– the pump has a too high capacity
– the opening of the control valve is too large
CONSEQUENCE not serious, tank gets overfilled

AS WELL AS
– valve V3 is open, another liquid or gas gets pumped
– contaminants in the tank
–A is pumped to another place (leak in the connecting pipe)
CONSEQUENCE is serious, a possible explosion

. . .

Safety Analysis (cont.)

Action Error Analysis (AEA)

Considers the operational, maintenance, control and supervision actions performed by human beings. The potential mistakes in individual actions are studied.

- list steps in operational procedures (e.g. “press button A”)
- identification of possible errors for each step, using a check-list of errors
- assessment of the consequences of the errors
- investigations of causes of important errors
(action not taken, actions taken in wrong order, erroneous actions, actions applied to wrong object, late or early actions, ...)
- analysis of possible actions designed to gain control over these process
- relevant for software in the area of user interface design

Safety Analysis (cont.)

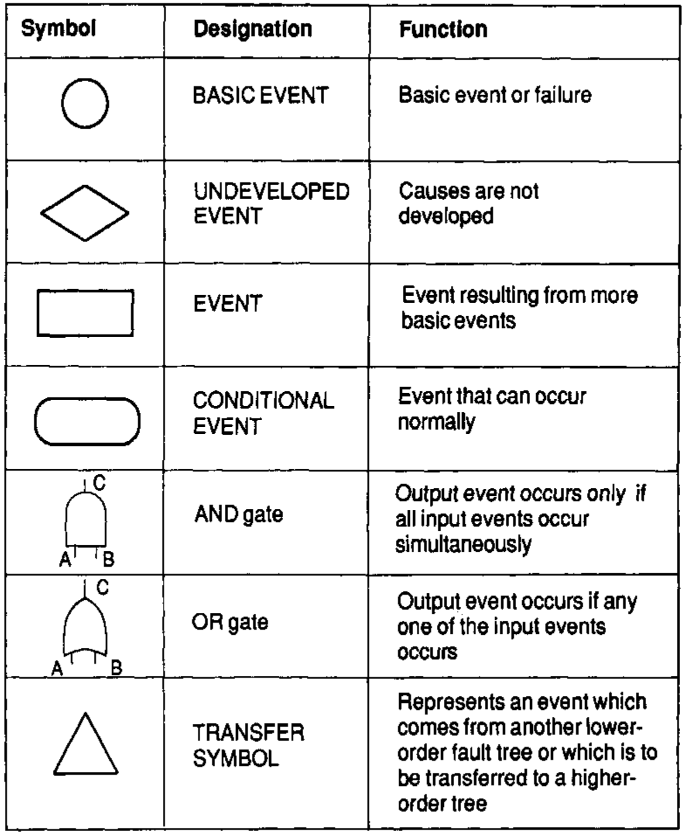
Fault Tree Analysis (FTA)

A graphical representation of logical combinations of causes that may lead to a hazard (top-event). Can be used as a quantitative method.

- identification of hazards (top-events)
- analysis to find credible combinations which can lead to the top-event
- graphical tree model of parallel and sequential faults
- uses a standardized set of symbols for Boolean logic
- expresses top-event as a consequence of AND/OR combination of basic events
- minimal cut set is used for quantitative analysis

Safety Analysis (cont.)

Symbols used in fault tree analysis

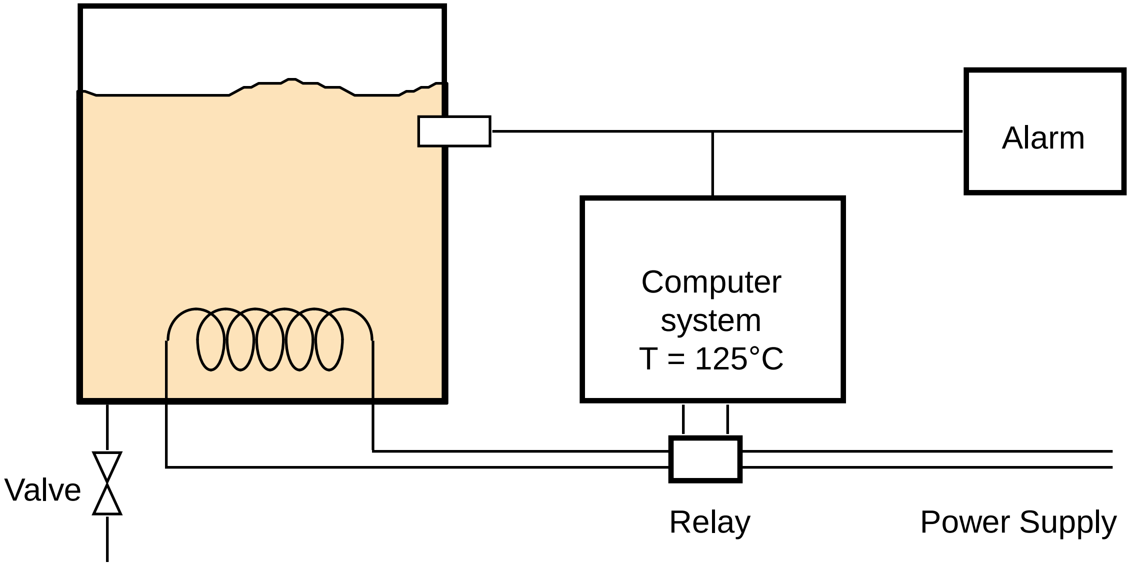


Symbol	Designation	Function
○	BASIC EVENT	Basic event or failure
◇	UNDEVELOPED EVENT	Causes are not developed
▭	EVENT	Event resulting from more basic events
⬭	CONDITIONAL EVENT	Event that can occur normally
C A B	AND gate	Output event occurs only if all input events occur simultaneously
C A B	OR gate	Output event occurs if any one of the input events occurs
△	TRANSFER SYMBOL	Represents an event which comes from another lower-order fault tree or which is to be transferred to a higher-order tree

Safety Analysis (cont.)

An Example for fault tree analysis

In a container two chemicals react with each other over a period of 10 hours at a temperature of 125 °C. If the temperature exceeds 175 °C toxic gas is emitted. The temperature is controlled by a computer system.

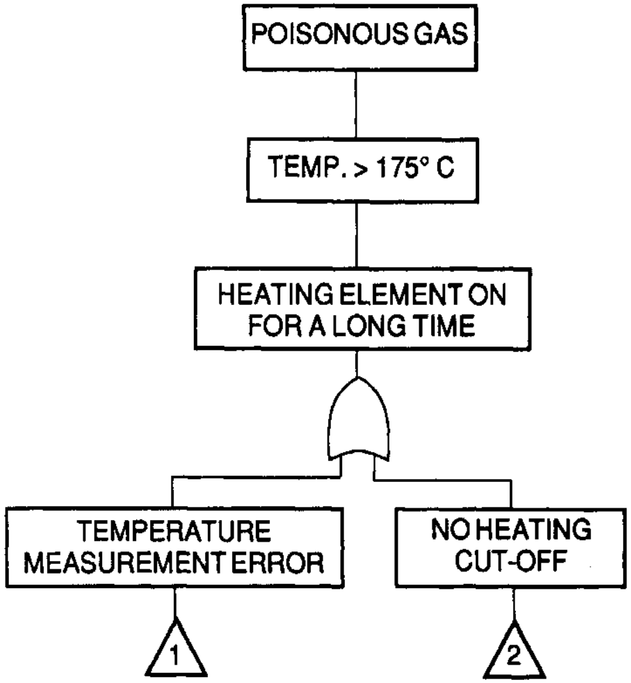


Safety Analysis (cont.)

An Example for fault tree analysis (cont.)

Identification of the top-event:

Emission of poisonous gas is the top event

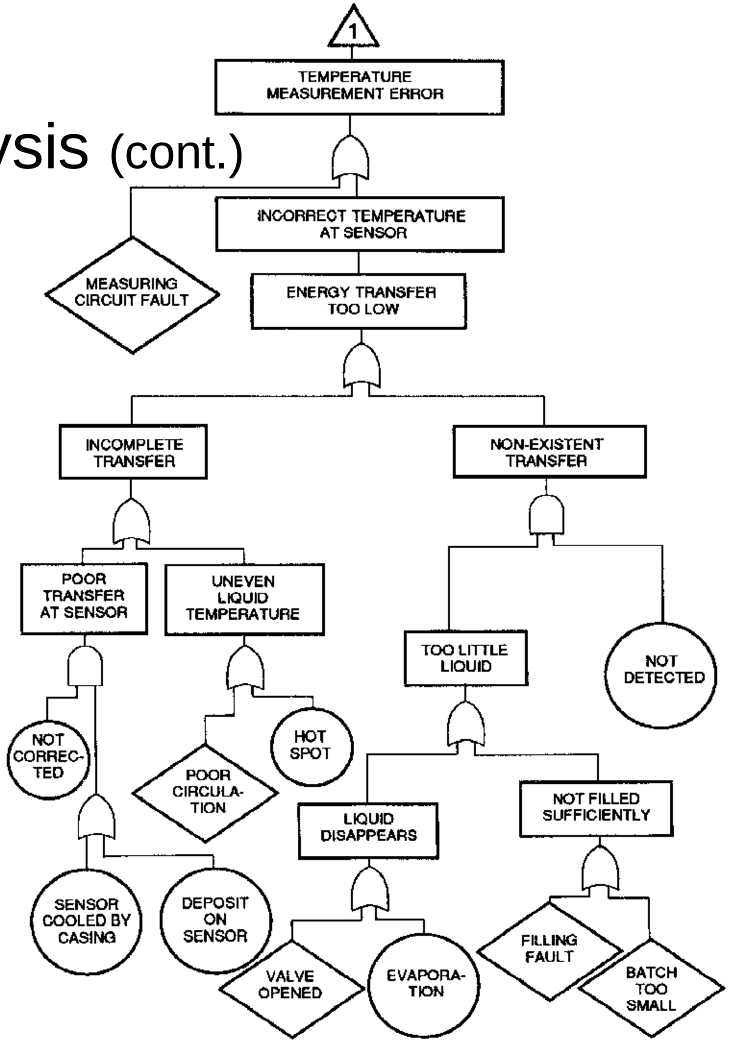

POISONOUS GAS
TEMP. > 175° C
HEATING ELEMENT ON FOR A LONG TIME
TEMPERATURE MEASUREMENT ERROR
NO HEATING CUT-OFF
1
2

The upper part of the fault tree

Safety Analysis (cont.)

An Example for fault tree analysis (cont.)

Subtree for temperature measurement failure

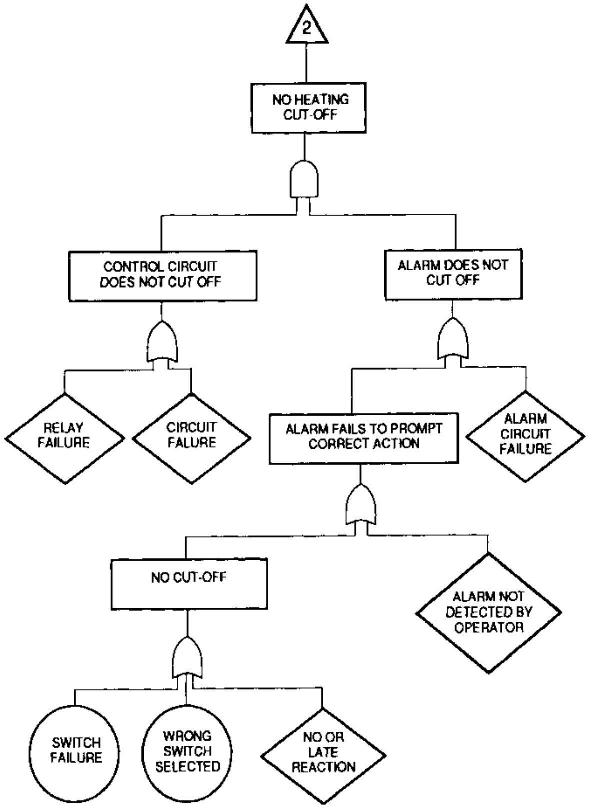


Safety Analysis (cont.)

An Example for fault tree analysis (cont.)

Subtree for heating

cut off failure



Safety Analysis (cont.)

Event Tree Analysis (ETA)

Models the potential consequences of faults which are considered as events. Can be used as a quantitative method.

- identification of basic events
- start with basic events and describe possible consequences of this event
- binary decision for consequences of events
- opposite of FTA which starts with top events

Safety Analysis (cont.)

Failure Modes and Effect Analysis (FMEA)

A common method where the designer in a systematical way has to answer the questions “How can the component fail?” and “What happens then?”.

- the system is dived up into different components in the form of a block diagram
- failure modes are identified for all components
- causes, consequences and the significance of failures are assessed for each failure mode

Safety Analysis (cont.)

Failure Modes and Effect Analysis (FMEA) (cont.)

- an investigation is made into how the failure can be detected
- if necessary, recommendations for suitable control measures are made
- analysis is supported by tabular sheets (e.g. IEC standard 1985)
- failure mode, effects and criticality analysis (FMECA) puts special emphasis on the criticality aspect

Safety Analysis (cont.)

An example FMEA hazard assessment

Severity of consequence		*Probability of occurrence*			*Probability of detection*	
10	Very severe System operation has to be abandoned or even a safety critical state may be reached	10	High It is almost certain that the failure will occure with high probability	$500\ 10^{-6}$	10	Unprobable It is impossible or at very improbable that the failure can be detected
9		9			9	Very low It is possible to detect the fault before the system fails
8	Severe Failure causes disturbance of end user (no safety critical failures or violations of regulations)	8	Moderate The component is similiar to component designs which already have caused problems in the past	$50\ 10^{-6}$	8	Small
7		7			7	
6	Moderate Failure causes inconvenience of the end user, restricted system operation will be perceived by the customer	6	Small The component is similiar to component designs which have caused problems in the past, but the extend of problems was relatively low	$5\ 10^{-6}$	6	
5		5			5	Moderate
4		4			4	
3	Minor Failure causes only minor inconvenience of the end user, only minor restrictions of the system operation are perceiveable	3	Very small The component is similiar to component designs which had very low failure rates in the past	$100\ 10^{-9}$	3	
2					2	High
1	Improbable It very improbable that the failure will be perceived by the end user	1	Improbable It is very improbable that a failure ocurrs	$1\ 10^{-9}$	1	Very High It is certain that the faults gets detected before the system fails

Safety Analysis (cont.)

An example FMEA hazard assessment (cont.)

Function	*Failure Mode*	*Cause*	*Effect*	*Controls*	***Severity***	***Probability***	***Dedection***	***Product***
speed sensor	open	connector or harness	no operation possible	supplier quality control and end of line testing	9	4	3	108
		computer	no operation possible	computer supplier quality control and end of line testing	9	3	3	81
		sensor	no operation possible	sensor supplier quality control, module and end of line testing	9	4	3	108
	short to supply	connector or harness	no operation possible	supplier quality control and end of line testing	9	2	3	54
		computer	no operation possible	computer supplier quality control and end of line testing	9	2	3	54
		sensor	no operation possible	sensor supplier quality control, module and end of line testing	9	2	3	54
	short to ground	connector or harness	no operation possible	supplier quality control and end of line testing	9	1	3	27
		computer	no operation possible	computer supplier quality control and end of line testing	9	1	3	27
		sensor	no operation possible	sensor supplier quality control, module and end of line testing	9	1	3	27

Safety Analysis (cont.)

Cause-consequence analysis

Combination of fault tree analysis and event tree analysis

- starts at a critical event
- works forward by using event tree analysis (consequences)
- works backward by using fault tree analysis (causes)
- very flexible
- well documented method

Comparison of Safety Analysis Methods

Comparison of Safety Analysis Methods

Method	Advantages	Restrictions and deficiencies
Preliminary hazards analysis	A required first step.	None.
Hazards and operability study	Suitable for large chemical plants. Results in a list of actions, design changes and cases identified for more detailed study. Enhances the information exchange between system designers, process designers and operating personnel.	Technique is not well standardized and described in the literature. Most often applied to continuos processes.
Action error analysis	Gives the computer system designer proposals for proper interface design. Helps the personnel or users to monitor the process during operation and helps to prevent operator mistakes.	AEA is an analysis of the technical system, and does not analyze the behavior of operators. The thoughts and intentions of human beings, i.e. the reasons for mistakes, are not considered.

Comparison of Safety Analysis Methods (cont.)

Method	Advantages	Restrictions and deficiencies
Fault tree analysis	Well accepted technique. Very good for finding failure relationships. A fault oriented technique which looks for the ways a system can fail. Makes it possible to verify requirements, which are expressed as quantitative risk values.	Large fault trees are difficult to understand, bear no resemblance to system flow charts, and are mathematically not unique. It assumes that all failures are of binary nature, i.e. a component completes successfully or fails completely.
Event tree analysis	Can identify effect sequences and alternative consequences of failures. Allows analysis of systems with stable sequences of events and independent events.	Fails in case of parallel sequences. Not suitable for detailed analysis due to combinatorial explosion. Pays no attention to extraneous, incomplete, early or late actions.

Comparison of Safety Analysis Methods (cont.)

Method	Advantages	Restrictions and deficiencies
Failure modes and effects analysis	Easily understood, well accepted, standardized technique. Non-controversial, non-mathematical. Studies potential failures and their effects on the function of the system.	Examines non-dangerous failures and is therefore time consuming. Often combinations of failures and human factors not considered. It is difficult to consider multiple and simultaneous failures.
Cause-consequence analysis	Extremely flexible and all-encompassing methodology. Well documented. Sequential paths for critical events are clearly shown.	Cause-consequence diagrams become too large very quickly (as FTA, ETA). They have many of the disadvantages of fault tree analysis.

Problems with software safety analysis

- relatively new field
- lack of systematic engineering discipline
- no agreed or proven methodologies
- time and cost
- complexity
  (understanding of the problem domain, separation of knowledge)
- discrete nature of software
  (difficulties with large discrete state spaces)
- real-time aspects
  (concurrency and synchronization)
- (partially) invalid assumption of independent failures