Value of Failure

Students Course

Module 5: How to detect failure

Module 5: How to detect failure

Content

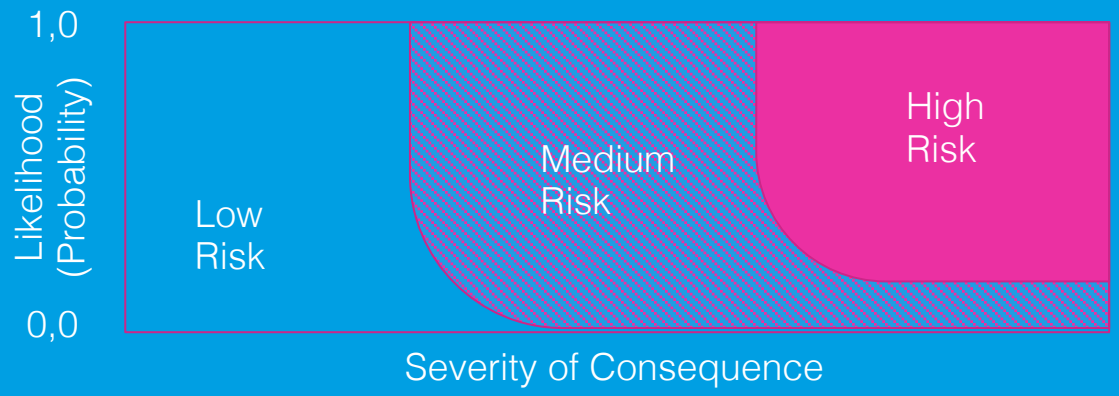
1. Risk assessment
2. Methods of hazard identification

Module 5: How to detect failure

1. Risk assessment

- Risk assessment: Not all risks are equal

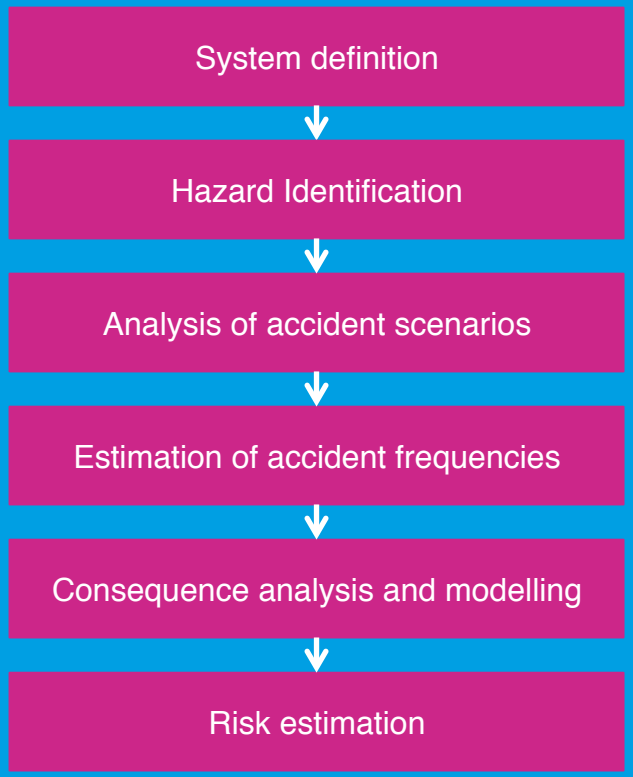
  - Risks are assessed by characterizing the probability that a project will experience an undesired event and the consequences, impact or severity of the undesired event, were it to occur
  - Risks can be compared on iso-curves consisting of a likelihood measure and a consequence measure
  - Since the assessment of the likelihood and consequence of a risk is both subjective and has significant uncertainty the characterization of risk either qualitative (low medium or high) or semi-quantitative (risk are captured on a matrix)



Module 5: How to detect failure

1. Risk assessment

- Risk assessment: Process of risk assessment
  - Scheme for qualitative and quantitative assessments
  - At all steps risk reducing measures need to be considered



Source: Regional Environmental Center for Central and Eastern Europe

Module 5: How to detect failure

1. Risk assessment

- Risk assessment: An example from NASA of some semi-quantitative definitions to enable a project to compare and rank risks

Probability of Occurrence	
Scale	Measure
5	Near certain to occur (80-100%).
4	Highly likely to occur (60-80%).
3	Likely to occur (40-60%).
2	Unlikely to occur (20-40%).
1	Not likely; Improbable (0-20%).

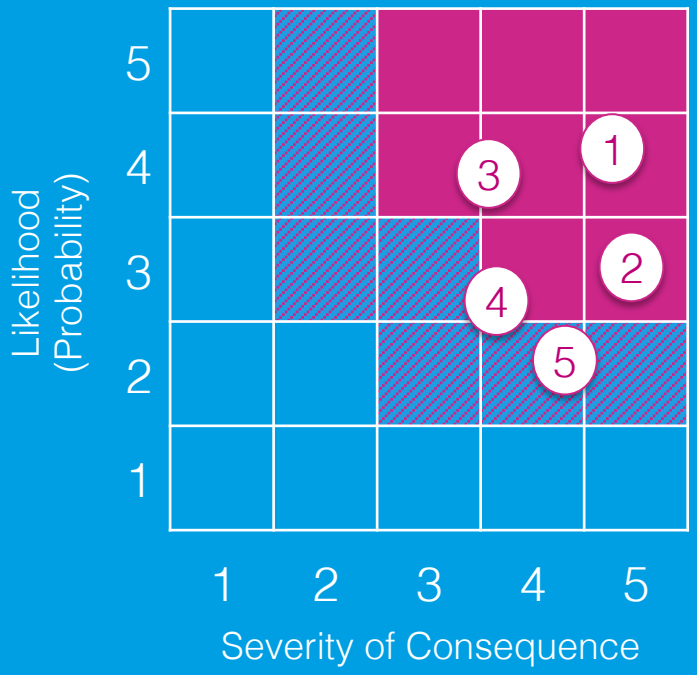
Impact of Consequences			
Class	Technical	Schedule	Cost
Class I Catastrophic (Scale 5)	A condition that may cause death or permanently disabling injury, facility destruction on the ground, or loss of crew, major systems, or vehicle during the mission	launch window to be missed	cost overrun > 50 % of planned cost
Class II Critical (Scale 4)	A condition that may cause severe injury or occupational illness, or major property damage to facilities, systems, equipment, or flight hardware	schedule slippage causing launch date to be missed	cost overrun 15 % to 50 % of planned cost
Class III Moderate (Scale 3)	A condition that may cause minor injury or occupational illness, or minor property damage to facilities, systems, equipment, or flight hardware	internal schedule slip that does not impact launch date	cost overrun 2 % to 15 % of planned cost
Class IV Negligible (Scale 2)	A condition that could cause the need for minor first aid treatment but would not adversely affect personal safety or health; damage to facilities, equipment, or flight hardware more than normal wear and tear level	internal schedule slip that does not impact internal development milestones	cost overrun < 2 % of planned cost

Source: Lisa Guerra of NASA's Exploration Systems Mission Directorate

Module 5: How to detect failure

1. Risk assessment

- Risk assessment: Not all risks require the same attendance and action
  - A 5x5 risk matrix provides a quick visual comparison of all project risks



Rank & Trend	Risk ID	Approach	Risk Title
1	DFRC-34	R	Landing gear door system failure
2	DFRC-12	M	Cost growth for engine components
3	DFRC-07	W	Quality control resources insufficient
4	DFRC-24	A	Avionics software behind schedule
5	DFRC-01	W	Limited flight envelope, due to technical issues

Risk Level		Risk Trend		Risk Approach	
	High risk		Decreasing (Improving)	M	Mitigate
	Medium risk		Increasing (Worsening)	W	Watch
	Low risk		Unchanged	A	Accept
			New since last period	R	Research

Source: Lisa Guerra of NASA's Exploration Systems Mission Directorate

Module 5: How to detect failure

Content

1. Risk assessment
2. Methods of hazard identification

Module 5: How to detect failure

2. Methods of hazard identification

- Methods of hazard identification: Some of the methods available:
  - HAZOP Analysis
  - Index-based methods
  - Fault tree analysis

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: Definition & Objectives
  - HAZOP Analysis:
    - a systematic technique for identifying HAZards and OPerability problems throughout an entire project
    - a formal systematic rigorous examination to the process and engineering facets of a production facility
    - a qualitative technique based on “guide-words” to help provoke thoughts about the way deviations from the intended operating conditions can lead to hazardous situations or operability problems
    - Originally developed by Lawley for Chemical industries and engineering → needs adoption for other purposes
  - Use:
    - to identify unwanted hazards due to lack of information or due to changes in process conditions or operating procedures
  - Objectives:
    - to detect any predictable deviation (undesirable event) in a process or a system. This purpose is achieved by a systematic study of the operations in each process phase

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: How and why HAZOP is used
  - Objectives and use:
    - HAZOP identifies potential hazards, failures and operability problems
    - Its use proven for over 40 years
    - It is most effective as a team effort combining all relevant experts
    - It encourages creativity in design concept evaluation
    - Its use results in fewer commissioning and operational problems
    - It results in better informed personnel,
    - It results in overall cost effectiveness improvement

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: How and why HAZOP is used (continued)
  - Objectives and use:
    - The analytical procedure suggests necessary changes to a project or system and eliminates or reduces the probability of operating deviations
    - It is a management tool but also helps to show insurers or official inspectors evidence of comprehensive thoroughness
    - HAZOP reports are an integral part of plant and safety records and are also applicable to design changes and plant modifications, thereby containing accountability for equipment and its associated human interface throughout the operating lifetime

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: How and why HAZOP is used (continued)
  - What HAZOP can do – and what it cannot do:
    - It emphasizes upon the operating integrity of a system, thereby leading methodically to most potential and detectable deviations which could conceivably arise in the course of normal operating routine
      - including "start-up " and "shut-down" procedures
      - as well as steady-state operations
    - It is important to remember at all times that HAZOP is an identifying technique and not intended as a means of solving problems nor is the method intended to be used solely as an undisciplined means of searching for hazardous scenarios

Module 5: How to detect failure

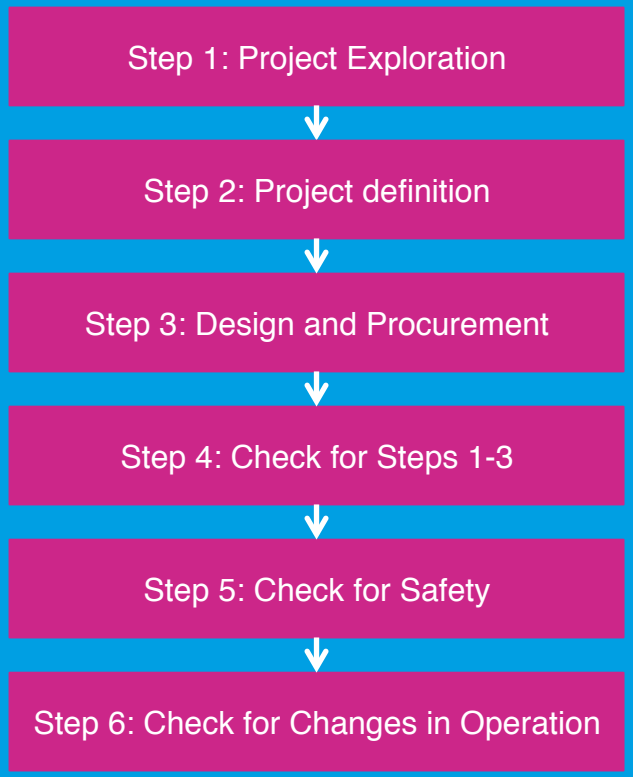
2. Methods of hazard identification

- HAZOP Analysis: How and why HAZOP is used (continued)
  - Where HAZOP is normally used:
    - HAZOP is used by most major companies handling and processing hazardous material:
      - oil and gas production
      - flammable and toxic chemicals
      - pharmaceuticals etc.

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: Six basic steps



No standard - different projects require different routines

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: Step 1 – Project exploration
  - Project exploration / preliminary project assessment
    - to identify inherent hazards of the project (process, facility, suitability and probable environmental impact)

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: Step 2 – Project definition

  - Project definition
    - to identify and reduce significant hazards associated with items and areas, check conformity with relevant standards and codes of practices

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: Step 3 – Design and procurement

  - Design and procurement
    - to examine the design in detail for identification of deviations capable of causing operability problems or hazards

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: Step 4 – Check for Steps 1-3

  - Check for Steps 1-3
    - During final stages of project completion:
      - check that all recommended and accepted actions recorded in steps 1-3 are implemented

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: Step 5 – Check for Safety

  - Check for Safety:
    - During finishing the project: check that all relevant statutory requirements have been acknowledges and all installed safety systems are reliably operable

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: Step 6 – Check for Changes in Operation

  - Check for Changes in Operation:
    - During normal operation, some time after finishing the project (especially if any modifications been made): check if changes in operation has not invalidated the HAZOP report of step 1-3 by introducing new hazards

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: Guide Questions and HAZOP Matrix

  - Guide Questions
    - Risks are identified and measured through guide questions and guide words and possible characteristics of the risks are captured in a matrix

    - Example: Pipe and Pump System

		Guide words						
		No	Low	High	Part of	Also	Other than	Reverse
Process variable	Flow	No flow	Low flow	High flow	Missing ingredience	Impurties	Wrong material	Reverse flow
	Level	Empty	Low level	High level	Low interface	High interface	-	-
	Pressure	Open to atmosphere	Low pressure	High pressure	.-	-	-	Vacuum
	Temperature	Freezing	Low temp.	High temp.	-	-	-	-

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: Example of a Study Flow Chart

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: Criticality analysis

  - Criticality:
    - Criticality: combination of severity of an effect and the probability or expected frequency of occurrence
    - Quantify the relative importance of each failure effect, so that priorities to reduce the probability or to mitigate the severity can be taken.

    - Example formula for criticality:

      $Cr = P \times B \times S$

      Cr: criticality number
      P: probability of occurrence in an year
      B: conditional probability that the severest consequence will occur
      S: severity of the severest consequence

Source: Regional Environmental Center for Central and Eastern Europe

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: Criticality analysis

  - The criticality number
    - used to rank the identified deviations in a HAZOP or FMEA study
    - cannot be used as a risk measure
    - product of three rough estimates

    - Before a criticality analysis can be performed guidelines have to be developed on how to determine P, B and S. There are no generally accepted criteria for criticality applicable to a system.

Source: Regional Environmental Center for Central and Eastern Europe

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: Criticality analysis

Categories					
Probability P		Conditional Probability B		Severity S	
Very rare	1	Very low	1	Low	1
Rare	2	Low	2	Significant	2
Likely	3	Significant	3	High	3
Frequent	4	High	4	Very high	4

Source: Regional Environmental Center for Central and Eastern Europe

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: Interpretation of values
  - Probability (P)
    - very rare - less than once in 100 years
    - rare - between once in 10 y. and once in 100 y.
    - likely - between once a year and once in 10 years
    - frequent - more frequent than once a year
  - Conditional probability (B)
    - very low - less than once every 1000 occurrences of the cause
    - low - less than once every 100 occurrences of the cause
    - significant - less than once every 10 occurrences of the cause
    - high - more than once every 10 occurrences of the cause
  - Severity (S)
    - low - no or minor economical loss/small, transient environmental damage
    - significant - considerable economic losses/considerable transient environmental damage/slight non-permanent injury
    - high - major economic loss/considerable release of hazardous material/serious temporary injury
    - very high - major release of hazardous material/permanent injury or fatality

Source: Regional Environmental Center for Central and Eastern Europe

Module 5: How to detect failure

2. Methods of hazard identification

- HAZOP Analysis: Decision making
  - Definitions
    - Definition of X and Y by decision maker
    - It might be necessary to formulate some additional criteria
      - for instance: every deviation for which the severity is classified as “very high severity” shall be evaluated to investigate the possibilities of reducing the undesired consequences

Criticality	Judgment	Meaning
Cr < X	Acceptable	No action required
X < Cr < Y	Consider modification	Should be mitigated within a reasonable time period unless costs demonstrably outweigh benefits
Cr > Y	Not acceptable	Should be mitigated as soon as possible

Source: Regional Environmental Center for Central and Eastern Europe

Module 5: How to detect failure

2. Methods of hazard identification

- Methods of hazard identification: Some of the methods available:
  - HAZOP Analysis
  - Index-based methods
  - Fault tree analysis

Module 5: How to detect failure

2. Methods of hazard identification

- Usage of an index for Risk assessment:
  - Indexes can be used for risk ranking
  - Process units can be assigned a score or index based on
    - Type of substance (flammable, explosive and/or toxic properties)
    - Type of process (pressure, temperature, chemical reactions)
    - Quantity
  - Ranking of the hazards
  - Focus attention on hazard analysis for the most hazardous units

Source: Regional Environmental Center for Central and Eastern Europe

Module 5: How to detect failure

2. Methods of hazard identification

- Examples of substance indexes:
  - In some areas existing indexes (e.g. material indexes) can be used. For other projects new indexes have to be developed
  - Substance Hazard Index (SHI): Proposed by the Organization of Resources Counsellors (ORC) to OSHA.
    - Based on a ratio of the equilibrium vapour pressure (EVP) at 20 ^{o}C divided by the toxicity concentration
  - Material Hazard Index (MHI): Used by the state of California to determine threshold quantities of acutely hazardous materials for which risk management and prevention programs must be developed

Source: Regional Environmental Center for Central and Eastern Europe

Module 5: How to detect failure

2. Methods of hazard identification

- Examples of substance indexes:
  - Dow Fire and Explosion Index (F&EI): Evaluates fire and explosion hazards associated with discrete process units
  - Mond Fire and Explosion Index: Developed by ICI's Mond Division, an extension of the Dow F&EI
  - These indexes focus on fire and explosion hazards, e.g. Butane has a Dow Material Index of 21, and Ammonia 4

Source: Regional Environmental Center for Central and Eastern Europe

Module 5: How to detect failure

2. Methods of hazard identification

- Methods of hazard identification: Some of the methods available:
  - HAZOP Analysis
  - Index-based methods
  - Fault tree analysis

Module 5: How to detect failure

2. Methods of hazard identification

- Fault tree analysis: Basics
  - Fault tree:
    - Graphical representation of the logical structure displaying the relationship between an undesired potential event (top event) and all its probable causes
      - top-down approach to failure analysis
      - starting with a potential undesirable event (top event)
      - determining all the ways in which it can occur
      - mitigation measures can be developed to minimize the probability of the undesired event
    - Fault trees can help to:
      - Quantifying probability of top event occurrence
      - Evaluating proposed system architecture attributes
      - Assessing design modifications and identify areas requiring attention
      - Complying with qualitative and quantitative safety/reliability objectives
      - Qualitatively illustrate failure condition classification of a top-level event
      - Establishing maintenance tasks and intervals from safety/reliability assessments

Source: Regional Environmental Center for Central and Eastern Europe

Module 5: How to detect failure

2. Methods of hazard identification

- Fault tree analysis: Basics
  - Fault tree construction:

Name	Look	Description
AND gate		To show that the output event occurs only if all the input events occur
OR gate		To show that the output event occurs only if one or more of the input events occurs
Basic event		A basic event requires no further development because the appropriate limit of resolution has been reached
Intermediate event		An intermediate event occurs because of one or more antecedent causes acting through logic gates
Transfer		A triangle indicates that the tree is developed further at the occurrence of the corresponding transfer symbol
Underdeveloped event		A diamond is used to define an event which is not further developed either because it is of insufficient consequence or because of insufficient information

Source: Regional Environmental Center for Central and Eastern Europe

Module 5: How to detect failure

2. Methods of hazard identification

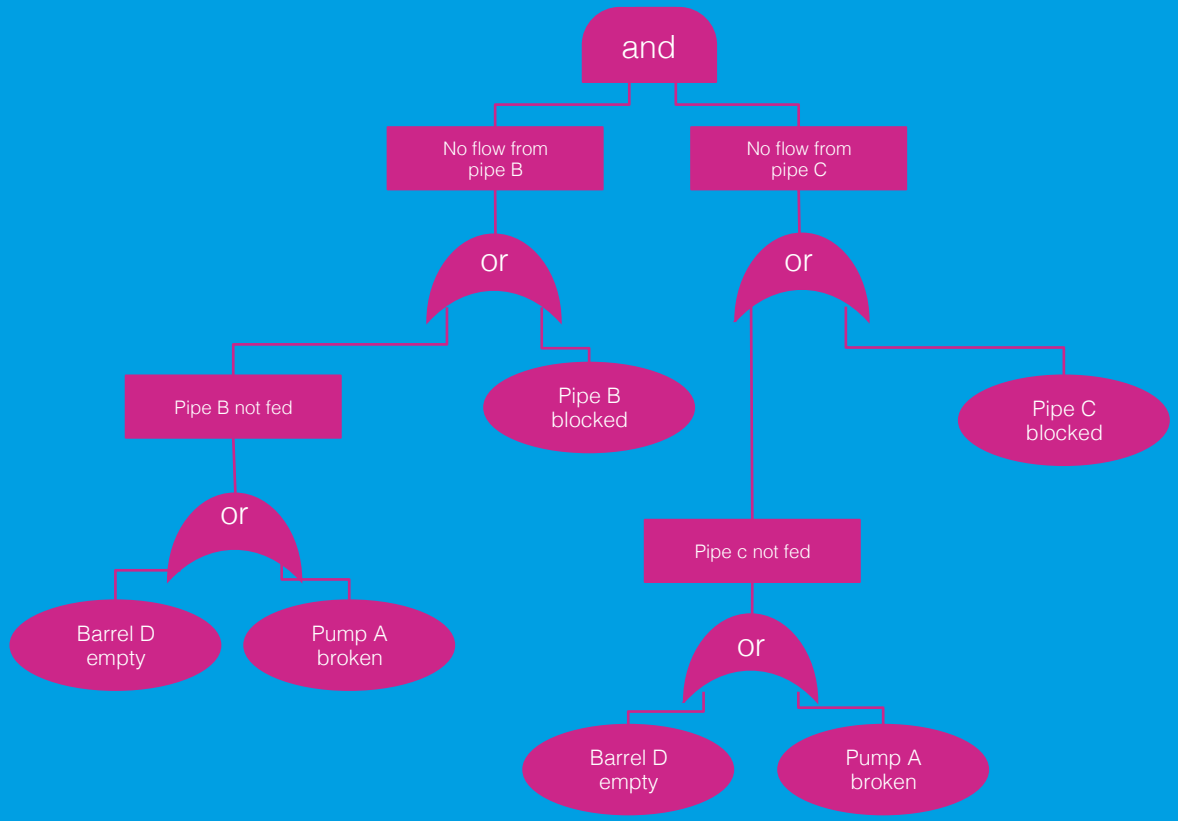
- Fault tree analysis: Guidelines to develop a fault tree
  - Guidelines:
    - Be as specific as possible
      - Replace abstract events by less abstract events
    - Use classifications
      - Classify an event into more elementary events
    - Identify distinct causes for an event
    - Couple trigger events with “no protective action”
    - Find co-operative causes for an event
    - Pinpoint a component failure event

Source: Regional Environmental Center for Central and Eastern Europe

Module 5: How to detect failure

2. Methods of hazard identification

- Fault tree analysis: Visual presentation of a fault tree
  - Example: Top event: No flow into barrel E



Source: Regional Environmental Center for Central and Eastern Europe

Module 5: How to detect failure
Learned

- What we discussed today
  - Basics of risk assessment
  - Methods of hazard identification
    - HAZOP Analysis
    - Index-based methods
    - Fault tree analysis

- Thank you for your attention

The Value of Failure Project has been funded with support from the European Commission. The author is solely responsible for this publication (communication) and the Commission accepts no responsibility for any use may be made of the information contained therein.

Erasmus+

Editor: © 2015
The Visonworks
Rannische Str. 17
D-06108 Halle (Saale)

Graphics & Layout:
The Visonworks
Rannische Str. 17
D-06108 Halle (Saale)

Project Partners:

Uniwersytet Szczeciński, canice consulting, thevisionworks, Enterprise Northern Ireland, Creo mind

Funded by:

Erasmus+

www.valueoffailure.com