



Design. Analyze. Optimize.

ELMAS – RAMS, Risk Assessment and Use Cases



EuCARD2 WP4 – CERN (Geneva) 22-23.6.2015

Reliability of Accelerators for Accelerator Driven Systems (ADS)

Ramentor Oy
Hermiankatu 8 D
FI-33720 Tampere

Tel. +358 (0) 40 746 6585
info@ramentor.com
www.ramentor.com

Jussi-Pekka Penttinen

Outline

1. Brief introduction
 - Ramentor, ELMAS, RAMS, Risk assessment process
2. Concrete use cases
 - a) Availability and radiation safety of encapsulation plant
 - b) Life Cycle Profit Management (LCPM) of process critical molding cranes – Modernization and improvement scenario analysis
 - c) Analysis of Alternative Bypass Lines of Mineral Processing Line
 - d) Infrastructure Availability – Design-Phase Data Center
 - e) Nuclear Power Plant (NPP) – Sustaining and developing safety, availability and performance factors

Ramentor Inc.

- Founded in 2006 and based in Tampere, Finland
 - Personnel ~10 (Dr. & M.Sc. – Mech. & aut. eng. / Applied math. / Software dev.)
 - Privately owned and independent software and expertise company
- Background: Tampere University of Technology (TUT)
 - Finnish Technology Agency (TEKES) Competitive Reliability Programme 1996-2000
 - Probabilistic approach in reliability and maintenance management 2001-2003
 - RAM Products 2003-2005, RAM Solutions 2006-2008, RAM Efficiency 2008-2010
- Please visit for more information: www.ramentor.com

Our goal is to become the leading expert and a partner in the field of Risk Management and RAMS methods and tools

Ramentor – Experience in Industry Sectors

- Energy Industry:
 - Nuclear Power Plants, District Cooling, ...
- Process Industry :
 - Pulp & Paper Mills, Steel Industry, Mineral Processing, Medical, ...
- IT Industry:
 - Data Centers, Telecommunication, Broadband connections, ...
- Equipment Manufacturers:
 - Cranes, Elevators, Thruster Units, ...
- Education and Research Organizations:
 - Universities (technology / applied sciences), CERN, ...

Ramentor – ELMAS Users / Co-developers

Industry Service	Design for Reliability	Quality & Risk mgmt
      	     	        
Operation & Maintenance	After Sales Support Service & Warranty	Research & Education
       	      	        

ELMAS – An Acronym

Event

- Time to Failure, Distribution
- Time to Repair, Distribution
- Maintenance actions
- Break and downtime loss
- Repair Costs
- Hazards
- Usage and stress profile
- External events

Logic

- OR
- AND
- K/N-Voting
- XOR-Exclusive
- Limits
- Conditional probability
- Delays
- Throughput, fuzzy logic
- Dynamic coding

Modeling

- Fault tree
- Event tree
- Cause-consequence-tree
- Reliability block diagram
- Process diagram
- Waiting and redundancy
- Buffers
- Failure modes, RCA

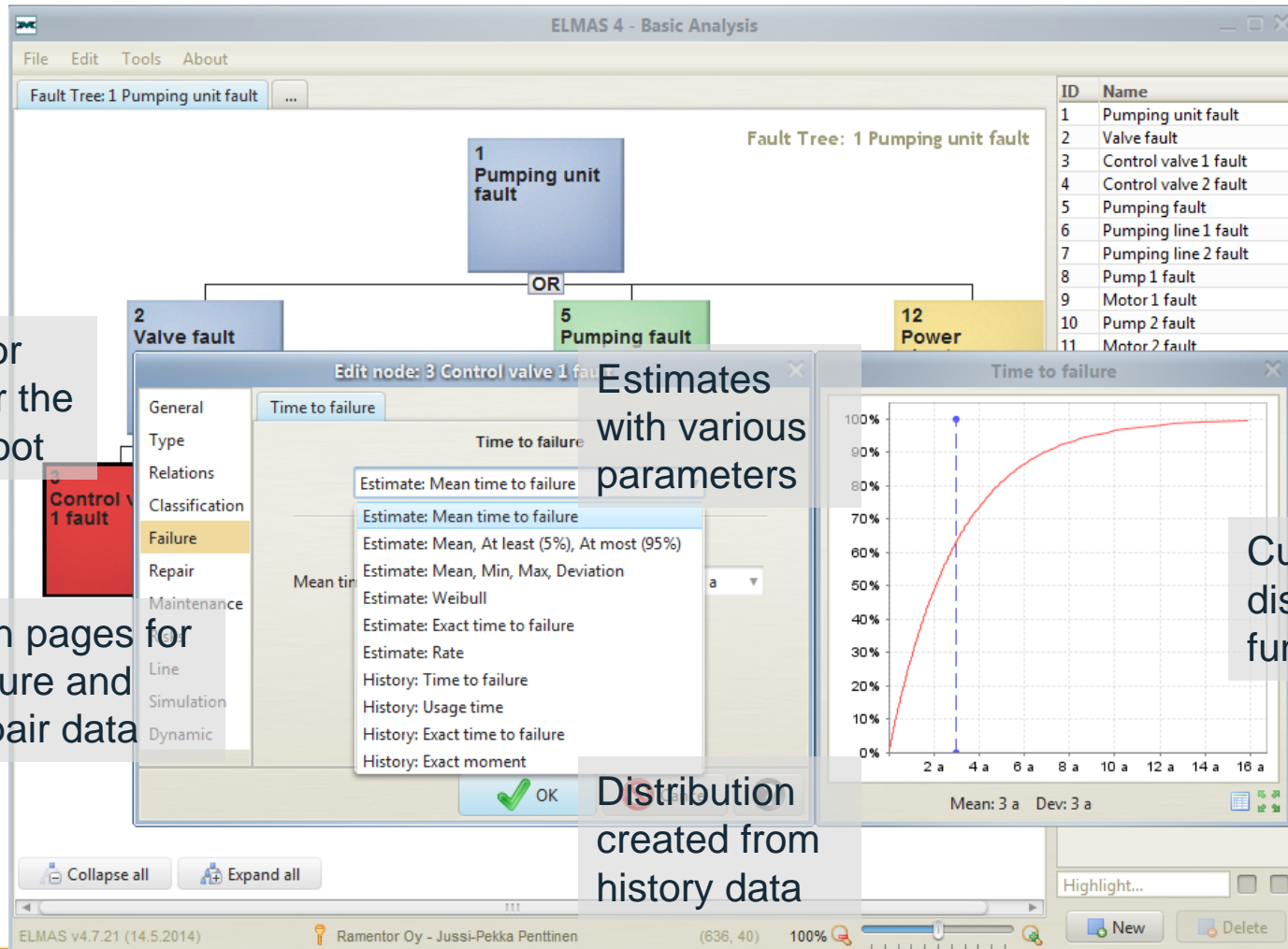
Analysis

- Simulation
- Reliability, Availability
- Risk Analysis
- Importance measures
- Conditional probabilities
- Spare part consumption
- Resources
- FMEA, Classification, RCM, Decision tree, Criticality

Software

- Graphical user interface
- Excel export and import
- HTML report
- Table summary
- ERP interface
- Project versioning
- Template library
- Search
- Web start

ELMAS – Root: Failure/Repair Distribution



ELMAS 4 - Basic Analysis

File Edit Tools About

Fault Tree: 1 Pumping unit fault

1 Pumping unit fault

OR

2 Valve fault **5 Pumping fault** **12 Power**

ID	Name
1	Pumping unit fault
2	Valve fault
3	Control valve 1 fault
4	Control valve 2 fault
5	Pumping fault
6	Pumping line 1 fault
7	Pumping line 2 fault
8	Pump 1 fault
9	Motor 1 fault
10	Pump 2 fault
11	Motor 2 fault

Node editor opened for the selected root

Estimates with various parameters

Cumulative distribution function shown

Own pages for Failure and Repair data

Distribution created from history data

Estimate: Mean time to failure
Estimate: Mean time to failure
Estimate: Mean, At least (5%), At most (95%)
Estimate: Mean, Min, Max, Deviation
Estimate: Weibull
Estimate: Exact time to failure
Estimate: Rate
History: Time to failure
History: Usage time
History: Exact time to failure
History: Exact moment

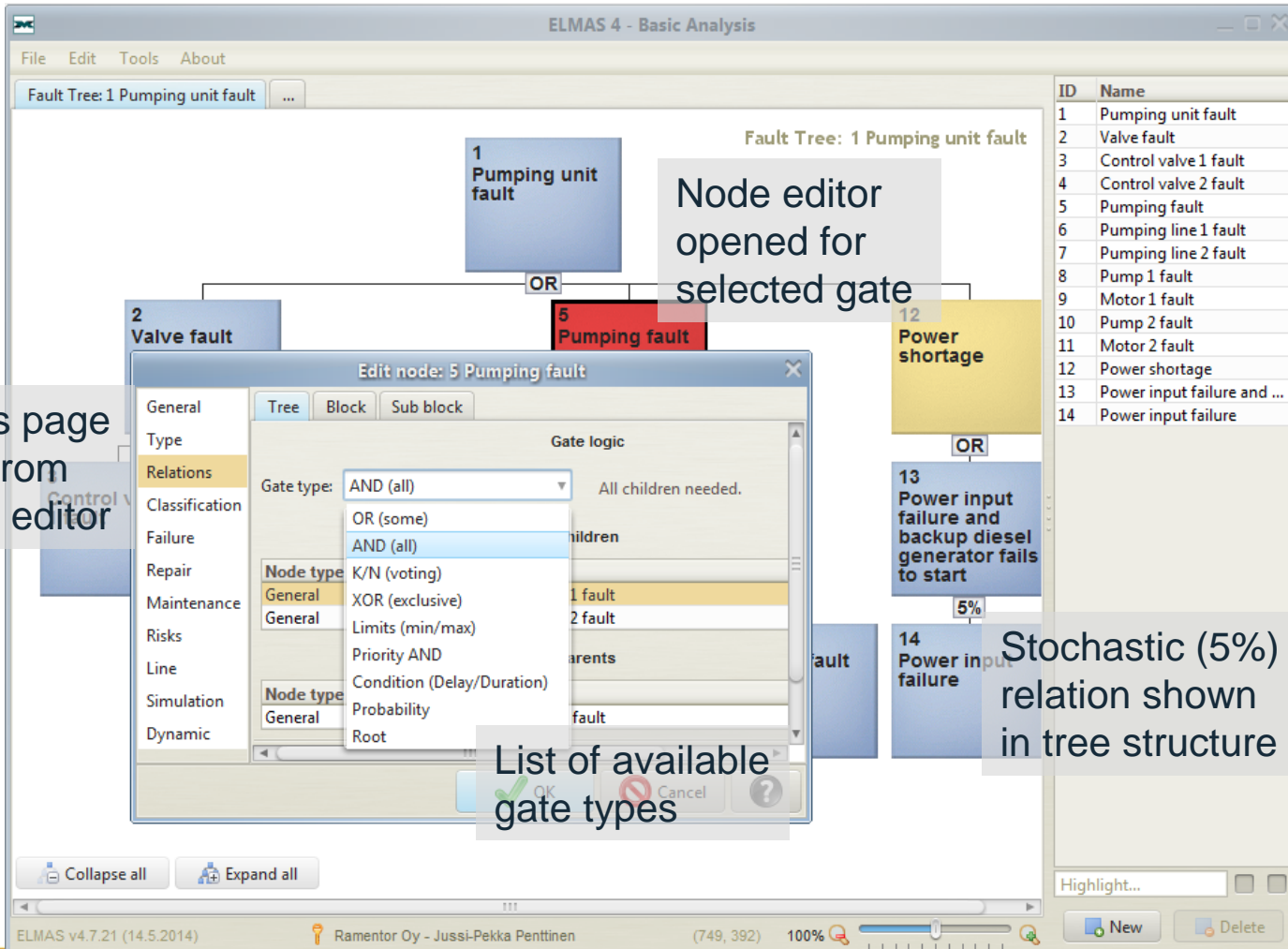
Time to failure

Mean: 3 a Dev: 3 a

ELMAS v4.7.21 (14.5.2014) Ramentor Oy - Jussi-Pekka Penttinen (636, 40) 100%

www.ramentor.com

ELMAS – Gate: Logic/Stochastic/Delay



The screenshot displays the ELMAS 4 - Basic Analysis software interface. The main window shows a fault tree diagram for 'Fault Tree: 1 Pumping unit fault'. The tree structure includes nodes such as '1 Pumping unit fault', '2 Valve fault', '5 Pumping fault', '12 Power shortage', '13 Power input failure and backup diesel generator fails to start', and '14 Power input failure'. A 'Node editor' is open for the selected '5 Pumping fault' node, showing the 'Relations' page. The 'Gate logic' section of the editor displays a dropdown menu for 'Gate type' with options: AND (all), OR (some), AND (all), K/N (voting), XOR (exclusive), Limits (min/max), Priority AND, Condition (Delay/Duration), Probability, and Root. A callout points to the '5%' value associated with node 14, indicating a stochastic relation.

Node editor opened for selected gate

Relations page opened from the node editor

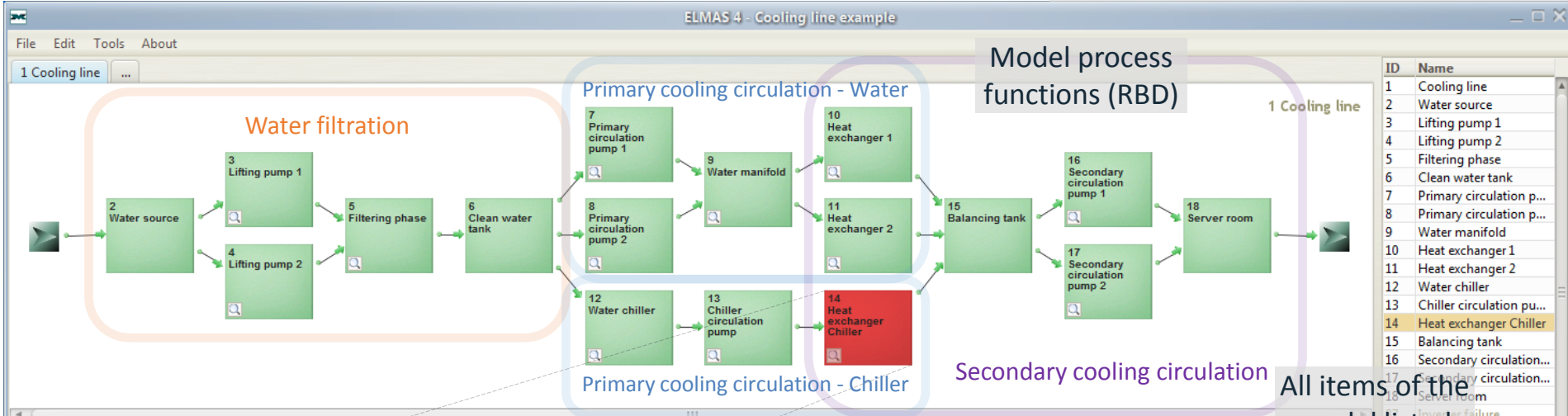
List of available gate types

Stochastic (5%) relation shown in tree structure

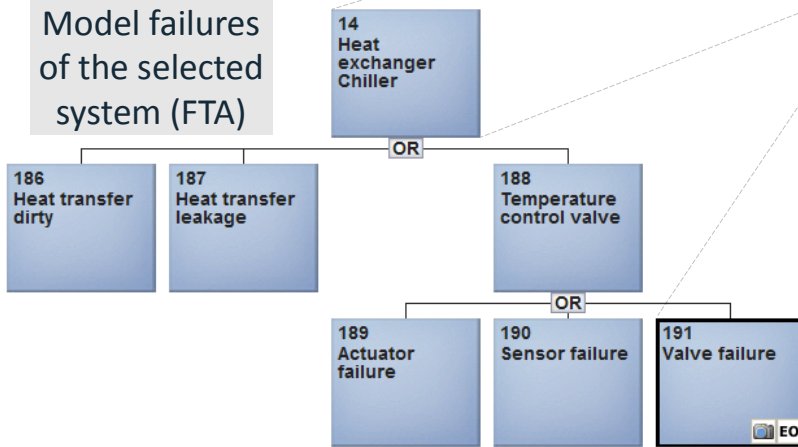
ID	Name
1	Pumping unit fault
2	Valve fault
3	Control valve 1 fault
4	Control valve 2 fault
5	Pumping fault
6	Pumping line 1 fault
7	Pumping line 2 fault
8	Pump 1 fault
9	Motor 1 fault
10	Pump 2 fault
11	Motor 2 fault
12	Power shortage
13	Power input failure and ...
14	Power input failure

ELMAS 4.7

<http://www.ramentor.com/products/elmas/>



Model failures of the selected system (FTA)



Edit node: 191 Valve failure

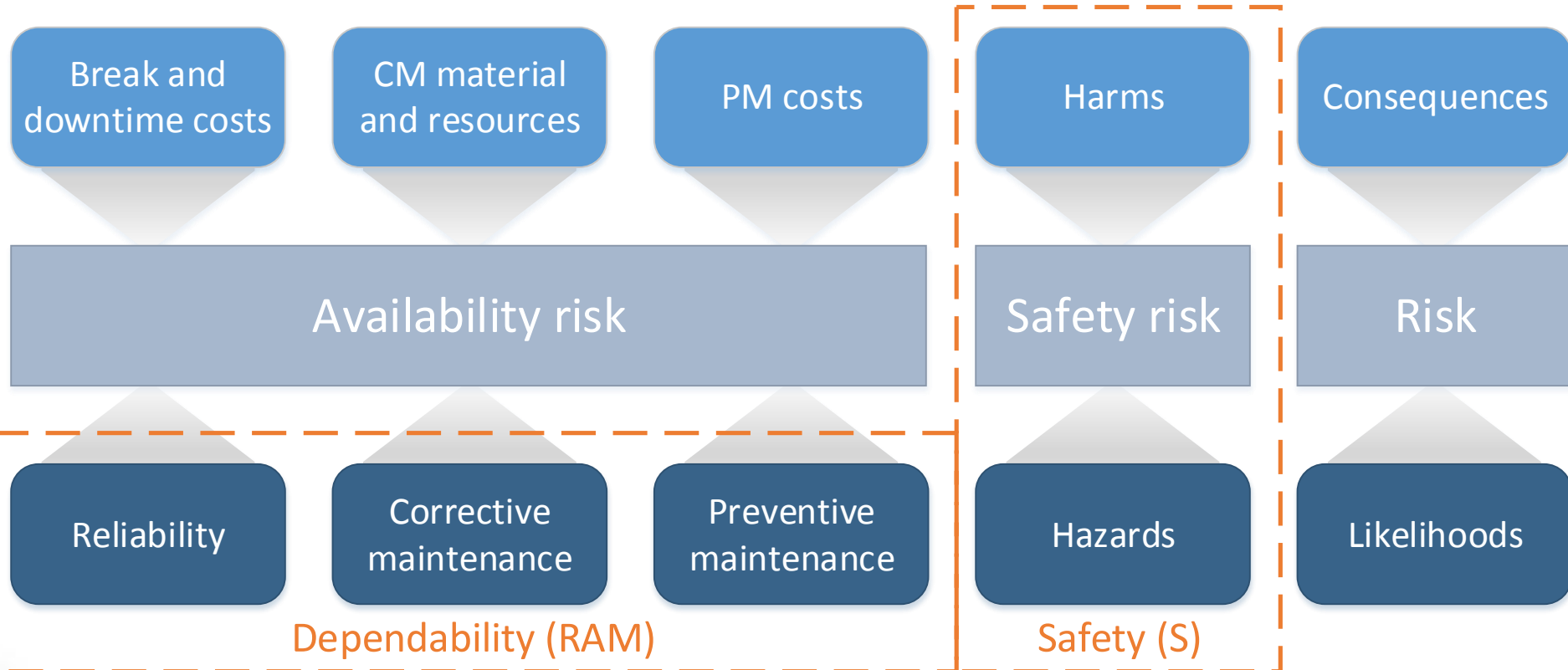
General	Restoration	Replacement	Finding	Redesign	RTF	
Type	Maint. LTA		Preventive	Inspection		
Relations	Inspections					
Classification	Generally it is reasonable to carry out the scheduled condition monitoring actions, if 1) it is possible to define and detect the symptoms of the failure early enough, 2) P-F-period (Point Failure) is moderately solid and 3) it is practical to control the object in shorter time periods than the P-F-period.					
Failure						
Repair						
Maintenance						
Risks	Active	Name	Interval	Cost (€)	Symptom ti...	Probability
Line	<input checked="" type="checkbox"/>	Valve check	30.0 d	20.0	30.0 d	0.9
Simulation	<input type="button" value="Add inspection"/> <input type="button" value="Remove selected rows"/>					
Add cost from all overlapping (even only first is handled): <input type="checkbox"/>						
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>						

Input data for the selected component

All items of the model listed

- 19 Inverter failure
- 20 Motor failure
- 21 Inverter failure
- 22 Inverter failure
- 23 Inverter failure
- 24 Chiller stopping main
- 25 Chiller stopping main
- 26 Chiller stopping main
- 27 Chiller stopping main
- 28 Chiller stopping main
- 29 Chiller stopping main
- 30 Chiller stopping main
- 31 Chiller stopping main
- 32 Chiller stopping main
- 33 Chiller stopping main
- 34 Chiller stopping main
- 35 Chiller stopping main
- 36 Chiller stopping main
- 37 Chiller stopping main
- 38 Chiller stopping main
- 39 Chiller stopping main
- 40 Chiller stopping main
- 41 Chiller stopping main
- 42 Chiller stopping main
- 43 Chiller stopping main
- 44 Chiller stopping main
- 45 Chiller stopping main
- 46 Chiller stopping main
- 47 Chiller stopping main
- 48 Chiller stopping main
- 49 Chiller stopping main
- 50 Chiller stopping main
- 51 Chiller stopping main
- 52 Chiller stopping main
- 53 Chiller stopping main
- 54 Chiller stopping main
- 55 Chiller stopping main
- 56 Chiller stopping main
- 57 Chiller stopping main
- 58 Chiller stopping main
- 59 Chiller stopping main
- 60 Chiller stopping main
- 61 Chiller stopping main
- 62 Chiller stopping main
- 63 Chiller stopping main
- 64 Chiller stopping main
- 65 Chiller stopping main
- 66 Chiller stopping main
- 67 Chiller stopping main
- 68 Chiller stopping main
- 69 Chiller stopping main
- 70 Chiller stopping main
- 71 Chiller stopping main
- 72 Chiller stopping main
- 73 Chiller stopping main
- 74 Chiller stopping main
- 75 Chiller stopping main
- 76 Chiller stopping main
- 77 Chiller stopping main
- 78 Chiller stopping main
- 79 Chiller stopping main
- 80 Chiller stopping main
- 81 Chiller stopping main
- 82 Chiller stopping main
- 83 Chiller stopping main
- 84 Chiller stopping main
- 85 Chiller stopping main
- 86 Chiller stopping main
- 87 Chiller stopping main
- 88 Chiller stopping main
- 89 Pressure sensor failure
- 90 Pump failure
- 91 Inverter failure
- 92 Motor failure
- 93 Pressure sensor failure
- 94 Pump failure
- 95 Filters fail
- 96 Filter 1
- 97 Inverter failure
- 98 Motor failure
- 99 Gearbox failure
- 100 Gaskets
- 101 Filter 2
- 102 Inverter failure
- 103 Motor failure
- 104 Gearbox failure
- 105 Gaskets
- 106 Filter 3
- 107 Inverter failure
- 108 Motor failure
- 109 Gearbox failure
- 110 Gaskets
- 113 Chiller stopping failure
- 173 Chiller stopping failure
- 204 Chiller stopping main

ELMAS – RAMS and Risk



ELMAS – Risk Assessment and RAMS

Risk Assessment

Likelihoods/Events

Consequences/Costs

Failures

Repair durations

Maintenance effects

External / Conseq. events

Break and Downtime costs

Repair costs

Maintenance costs

Env., Human, etc hazards

RAMS

ELMAS

ELMAS – Risk Assessment Process (ISO GUIDE 73)

1) Risk identification

- Find, recognize and describe risks
- ELMAS: Collect available information to comprehensive model

2) Risk analysis

- Comprehend the nature and determine the level of risk
- ELMAS: Stochastic discrete event simulation of the model

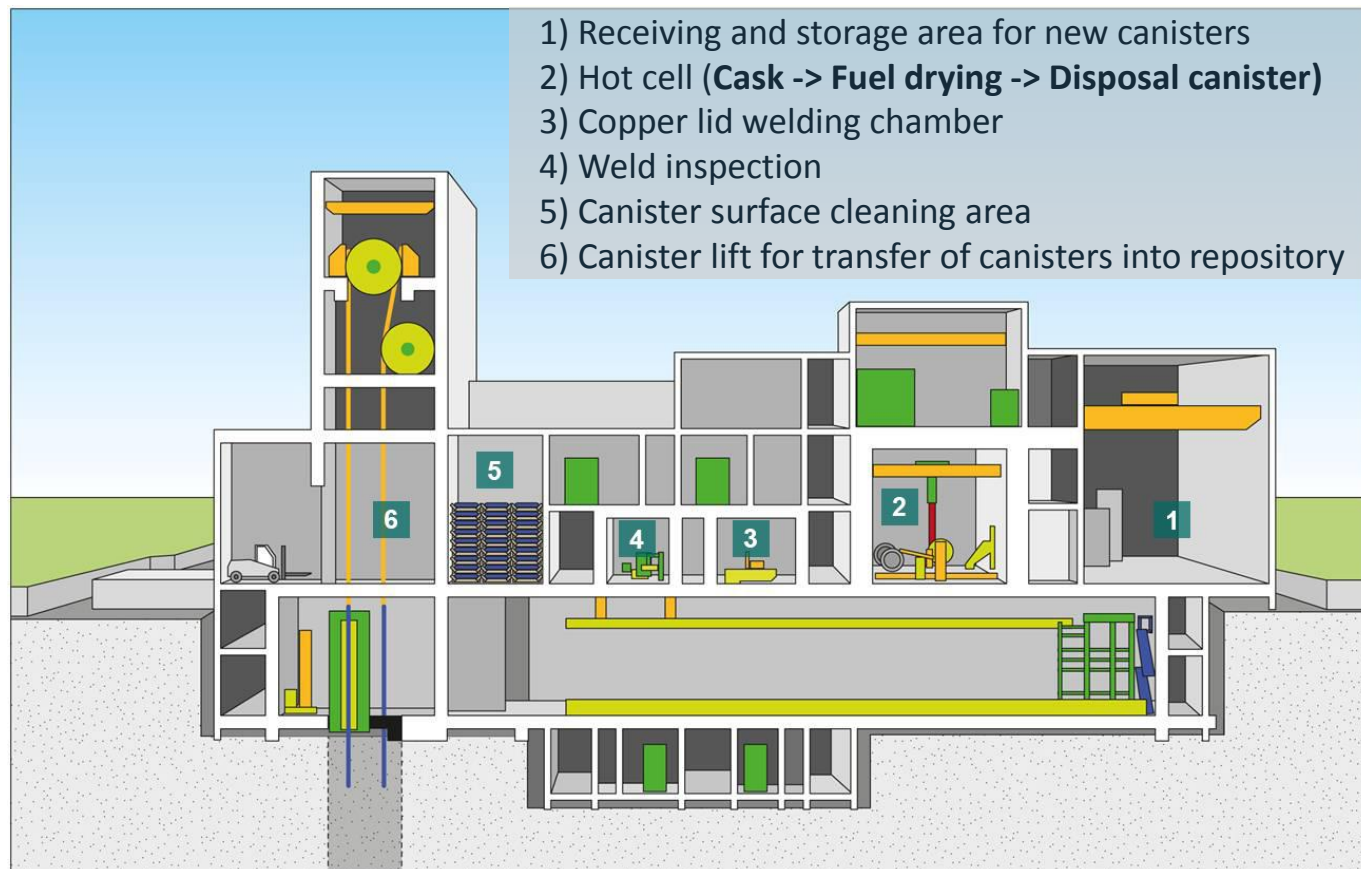
3) Risk evaluation

- Compare analysis results with risk criteria to determine whether the risk and its magnitude is acceptable or tolerable
- ELMAS: Report explicit results, compare scenarios, ...

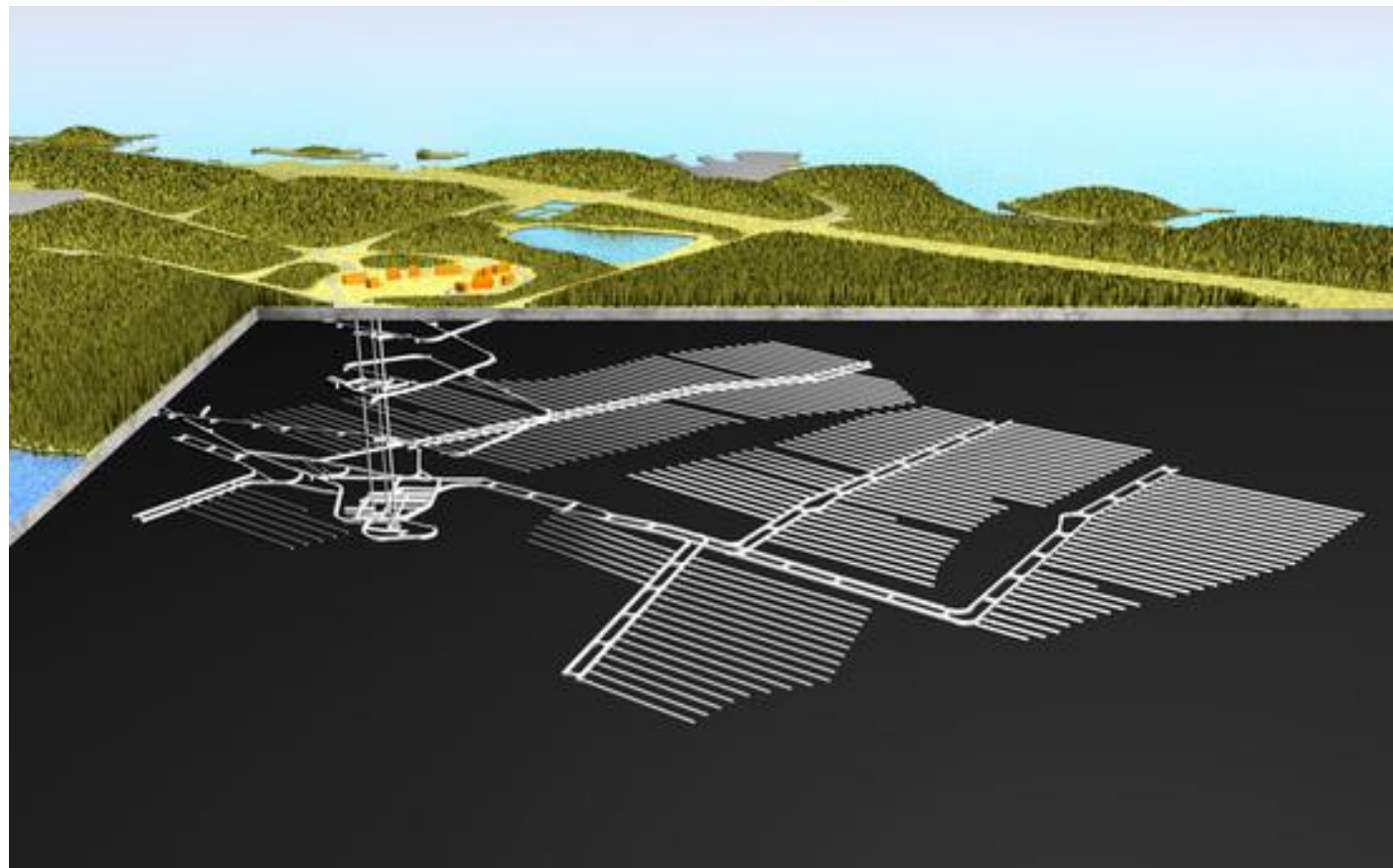
Case A) – Final Disposal Facility (FDF)

- The purpose of the FDF is to take care of packing the spent nuclear fuel assemblies in canisters and to dispose them permanently into the bedrock
- Aboveground encapsulation plant
 - Spent nuclear fuel is received, dried and packed into final disposal canisters
- Repository (ONKALO)
 - Located deep inside the bedrock, in which the most important section are the tunnels where the encapsulated spent nuclear fuel is disposed of

Case A) – Final Disposal Facility (FDF): Aboveground Encapsulation Plant



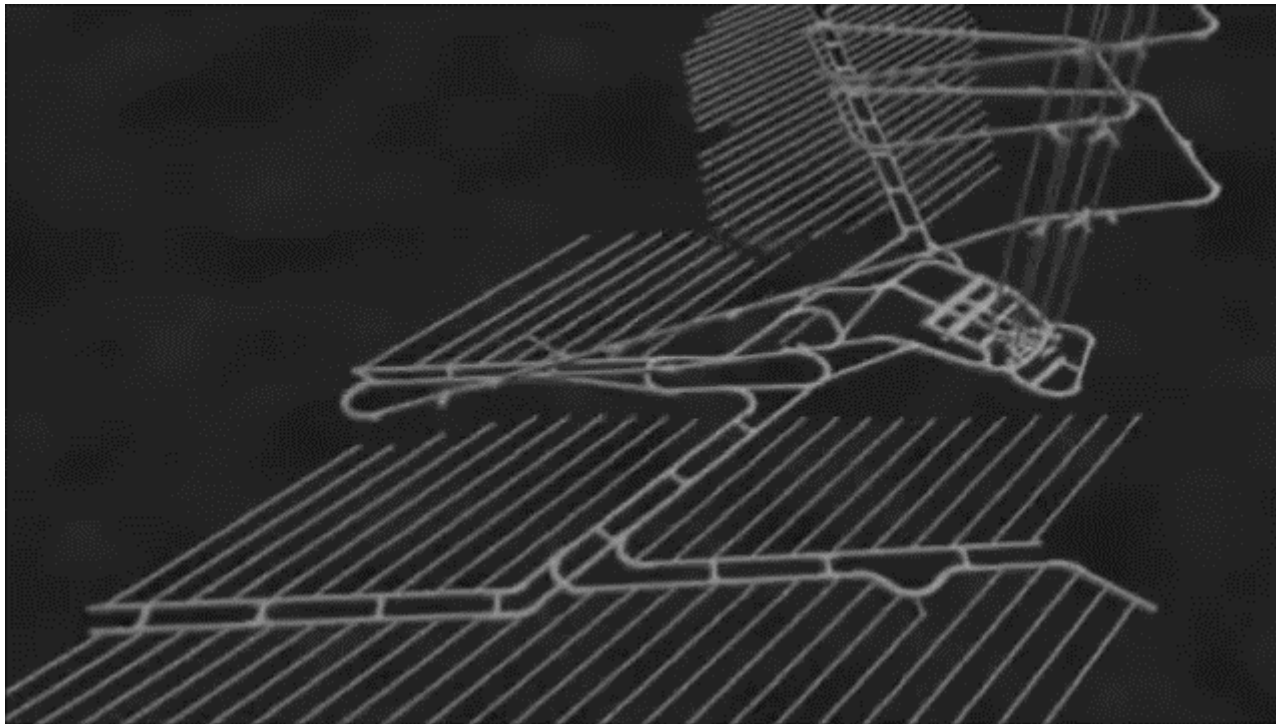
Case A) – Final Disposal Facility (FDF): Repository (ONKALO)



Case A) – Final Disposal Facility (FDF): Encapsulation Plant Case Description

- ELMAS analyses were made by Pöyry for Posiva
 - Availability and radiation safety of encapsulation plant
- **Transportation cask -> Fuel drying -> Disposal canister**
 - Availability models: Docking, Lifting, Moving (AGV), Welding, ...
- Design review and management of required changes
 - PSAM12 publication: Virtanen, Penttinen, Kiiski, Jokinen
- Safety models and reports
 - Ventilation system: Cooling, heating, filtering, low pressure
 - STUK (The Radiation and Nuclear Safety Authority in Finland)

Case A) – Final Disposal Facility (FDF): Fuel Handling Cell Equipment Example (1/5)



Full video: <https://youtu.be/hZI3AYI85n8>

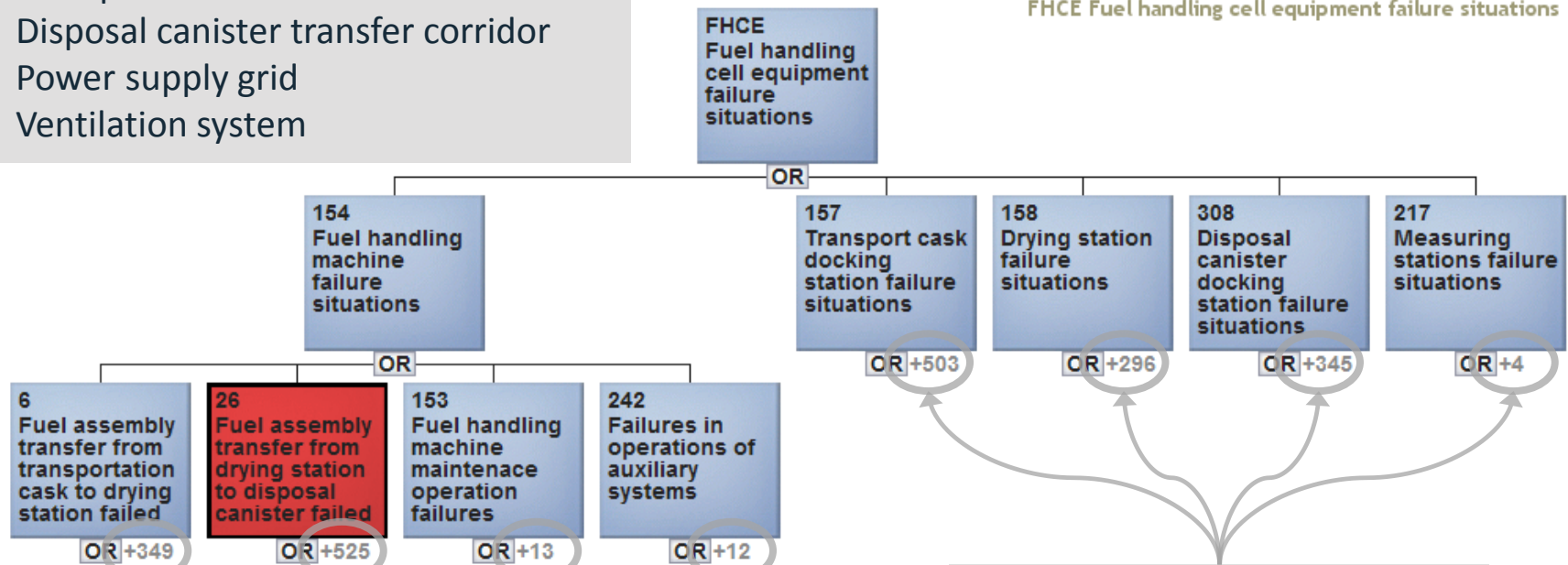
Case A) – Final Disposal Facility (FDF): Fuel Handling Cell Equipment Example (2/5)

Similar availability models also for:

- Receiving and storage area
- Transportation cask transfer corridor
- Disposal canister transfer corridor
- Power supply grid
- Ventilation system

Small part of the full
FDF availability model

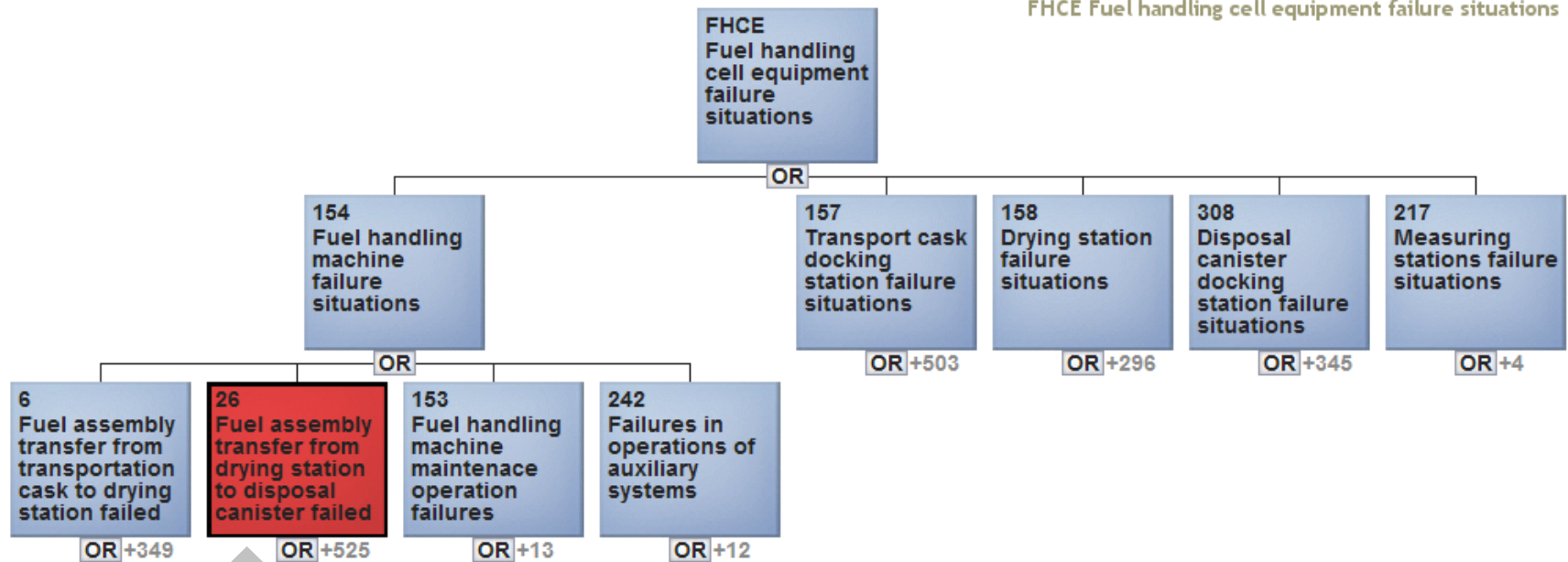
FHCE Fuel handling cell equipment failure situations



Subtrees of different failure situations are hidden

Case A) – Final Disposal Facility (FDF): Fuel Handling Cell Equipment Example (3/5)

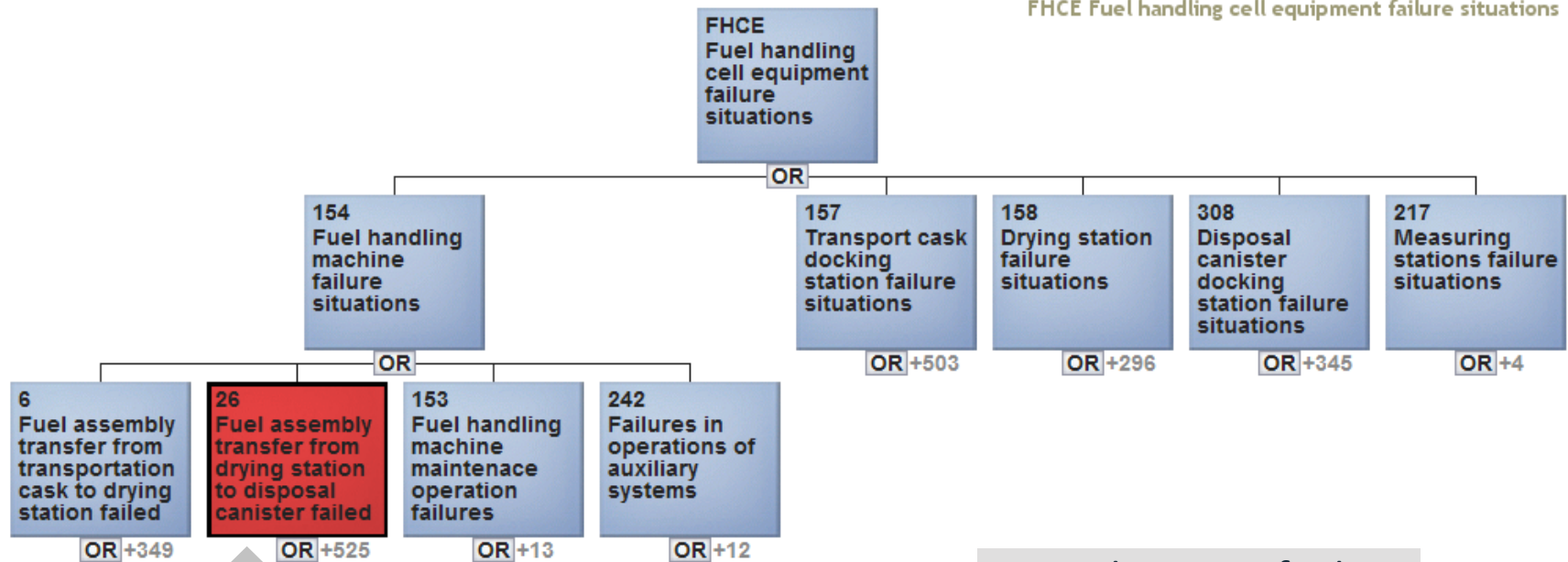
FHCE Fuel handling cell equipment failure situations



More detailed causes
for availability risk

Case A) – Final Disposal Facility (FDF): Fuel Handling Cell Equipment Example (4/5)

FHCE Fuel handling cell equipment failure situations



Remove failed, Move failed, Add failed, ...

Fuel assembly is curved, ...

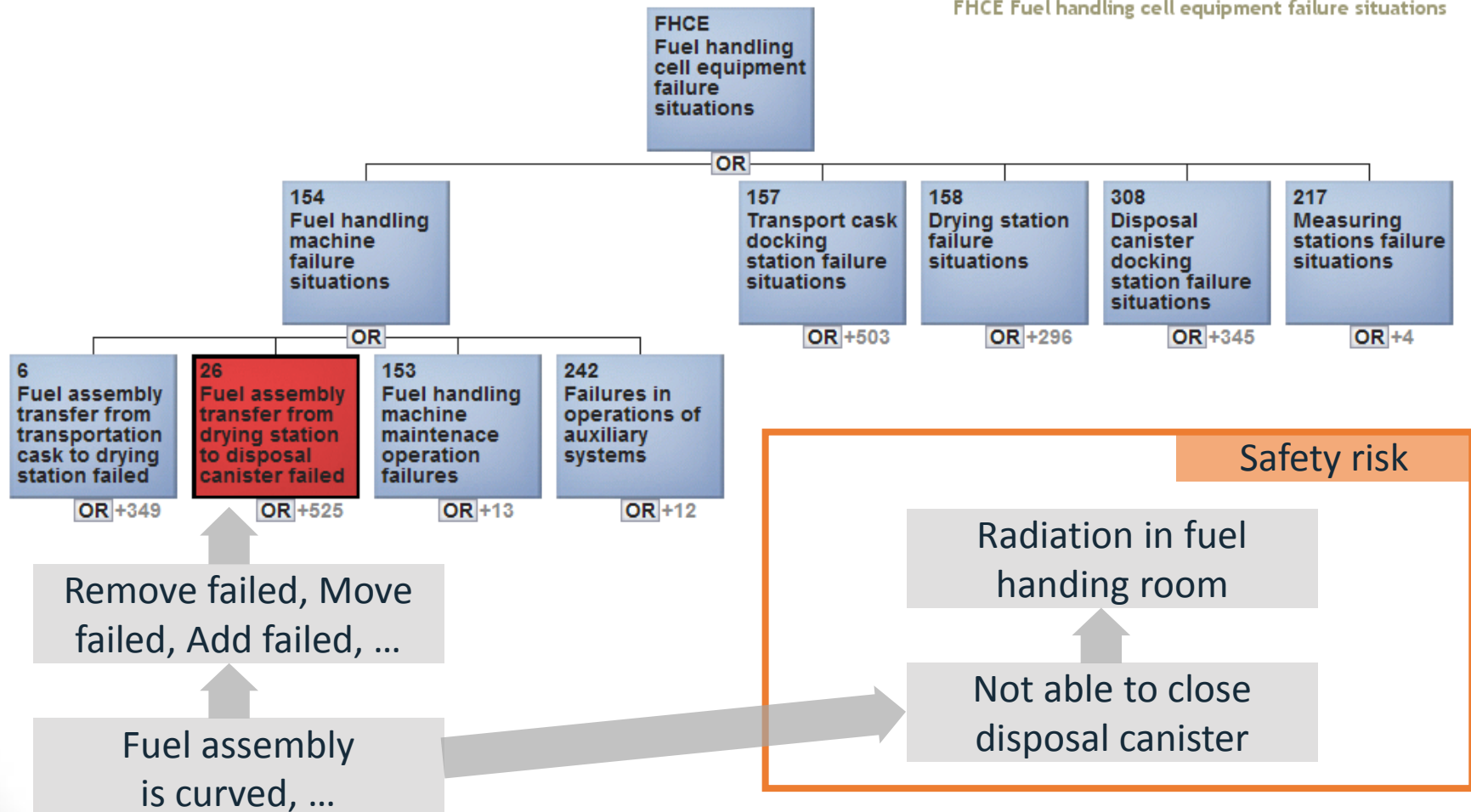
A cause can have other consequences

Radiation in fuel handling room

Not able to close disposal canister

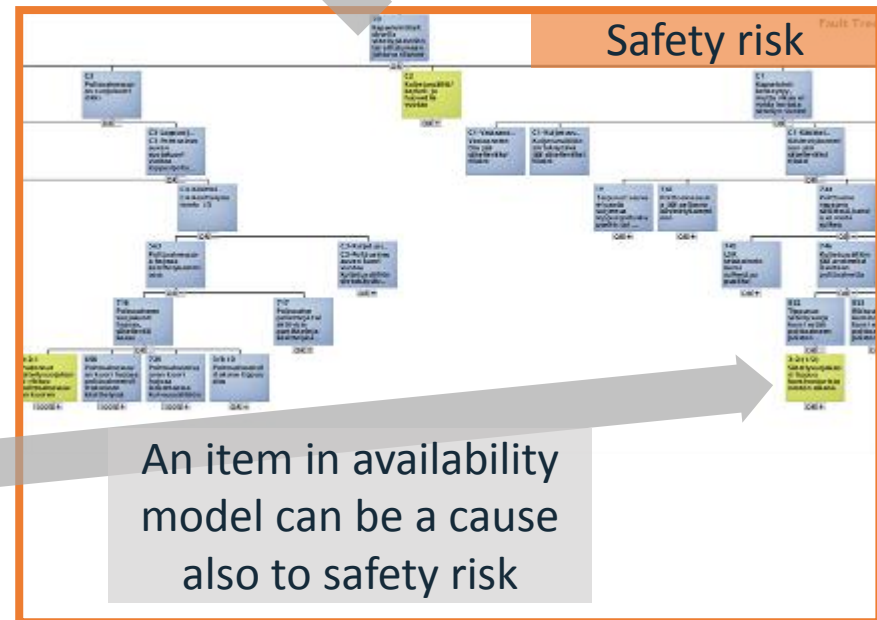
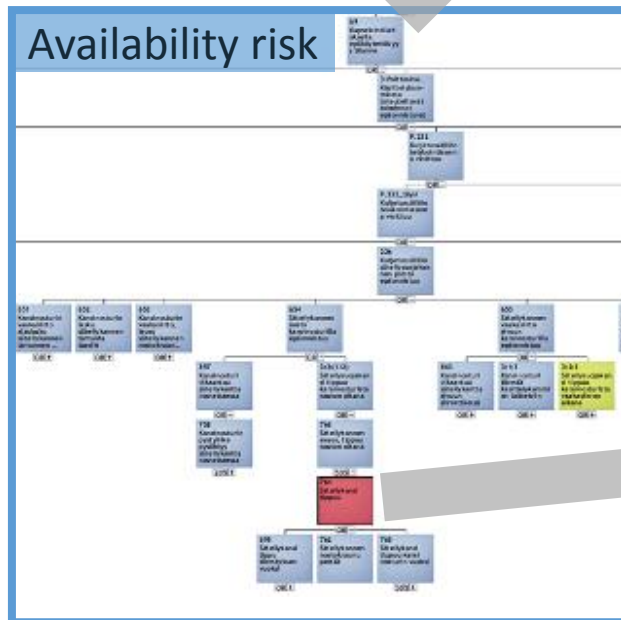
Case A) – Final Disposal Facility (FDF): Fuel Handling Cell Equipment Example (5/5)

FHCE Fuel handling cell equipment failure situations



Case A) – Final Disposal Facility (FDF): Combined Risk Model – Availability/Safety

All items and their causalities related to availability and safety risks are collected to a comprehensive model:
Availability and Radiation Safety of Encapsulation Plant

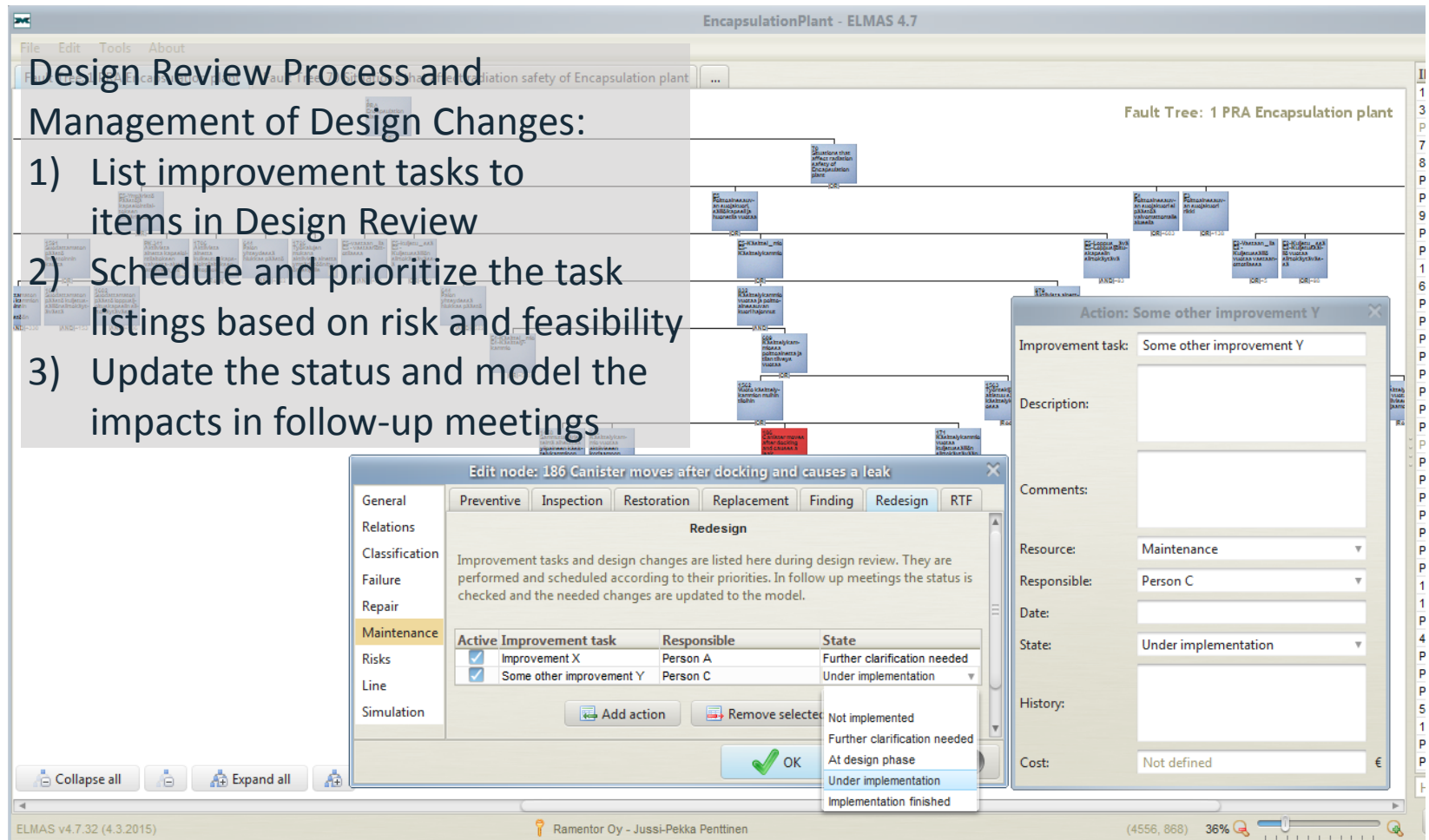


An item in availability model can be a cause also to safety risk

Case A) – Final Disposal Facility (FDF): Design Review / Change Management

Design Review Process and Management of Design Changes:

- 1) List improvement tasks to items in Design Review
- 2) Schedule and prioritize the task listings based on risk and feasibility
- 3) Update the status and model the impacts in follow-up meetings



The screenshot displays the ELMAS 4.7 software interface. The main window shows a fault tree diagram titled "Fault Tree: 1 PRA Encapsulation plant". The diagram consists of several rectangular nodes connected by lines, representing a hierarchical structure of failure events and causes. The nodes contain text in Finnish, such as "Suoritusvirheen vaikutus radionuclidien läpikulkuun" and "Käytännön ongelma".

Two dialog boxes are overlaid on the main window:

- Edit node: 186 Canister moves after docking and causes a leak**: This dialog has tabs for "Preventive", "Inspection", "Restoration", "Replacement", "Finding", "Redesign", and "RTF". The "Redesign" tab is active, showing a table of improvement tasks.

Active Improvement task	Responsible	State
<input checked="" type="checkbox"/> Improvement X	Person A	Further clarification needed
<input checked="" type="checkbox"/> Some other improvement Y	Person C	Under implementation

 Below the table are buttons for "Add action" and "Remove selected". A dropdown menu is open over the "Under implementation" state, showing options: "Not implemented", "Further clarification needed", "At design phase", "Under implementation" (highlighted), and "Implementation finished".
- Action: Some other improvement Y**: This dialog contains fields for "Improvement task" (Some other improvement Y), "Description", "Comments", "Resource" (Maintenance), "Responsible" (Person C), "Date", "State" (Under implementation), "History", and "Cost" (Not defined). It also has an "OK" button.

The bottom status bar shows "ELMAS v4.7.32 (4.3.2015)", "Ramentor Oy - Jussi-Pekka Penttinen", and "(4556, 868) 36%".

Case A) – Final Disposal Facility (FDF): Key Findings and Improvements

- Comprehensive availability and safety model created
- Several changes were made based on design reviews
 - Improved identification of unexpected impacts of the design changes on all related systems and to risks
 - Early stage identification of the problem areas became possible
- STUK statement 12/02/2015 (construction license):
 - Nuclear waste facility can be built to be safe
- Failure tolerance analysis can utilize the created models
 - Required for STUK later (operating license)
 - Common cause failures, Defense in depth levels, ...

Case B) – Life Cycle Profit Management (LCPM)

- Aims to **maximize the life cycle profit of an investment**
- Guides development work and investment decisions to **focus on overall costs** (not just investment costs)
 - All relevant cost factors from specification to decommission
- Emphasizes to take unavailability into consideration
 - Production loss
 - Break costs
 - Overtime work costs

Case B) – Life Cycle Profit Management (LCPM): Molding Crane



Case B) – Life Cycle Profit Management (LCPM): Molding Cranes Case Description

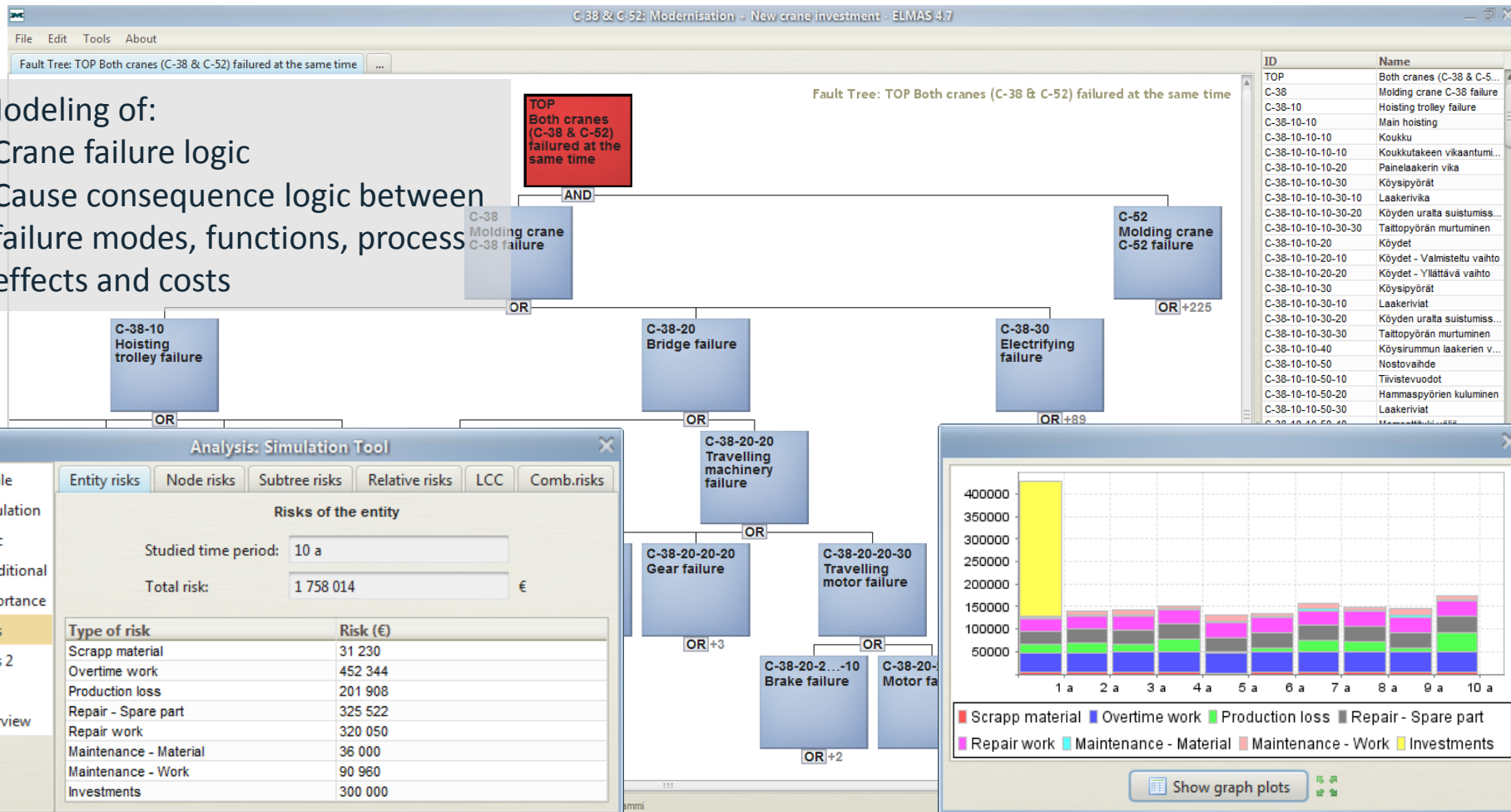
- Scenario analysis of two process critical molding cranes
 - Work rhythm 3 shifts/day and 5 days/week
 - One crane can handle 75% of the process flow
 - Overtime works can be used at weekends if necessary
- Comparison of 3 scenarios:
 1. Current situation
 2. Modernization of auxiliary hoisting & corrective action planning based on improvements potentials
 3. Modernization of auxiliary hoisting & renewal of older crane

Case B) – Life Cycle Profit Management (LCPM): Modeling, Simulation and Analysis

Figures are
fictional

Modeling of:

- Crane failure logic
- Cause consequence logic between failure modes, functions, process effects and costs



Case B) – Life Cycle Profit Management (LCPM): Comparison of Scenarios

Figures are
fictional

C-38 & C-52 Scenario analysis (10 a)	Scenario 1: Current situation	Scenario 2: C-38 modernisation & C-52 corrective actions	Scenario 3: C-38 modernisation & C-52 renewal
			Change
C-38 & C-52 failures	27.6	20.0	27.5 %
C-38 & C-52 failure time	4 d 16 h	3 d 14 h	1 d 2 h
C-38 & C-52 unplanned unavailability	~ 0.128 %	~ 0.098 %	23.4 %
C-38 failures	375.3	305.9	18.5 %
C-38 failure time	97 d 23 h	75 d 4 h	22 d 19 h
C-38 unplanned unavailability	~ 2.68 %	~ 2.06 %	23.1 %
C-52 failures	365.7	359.0	1.8 %
C-52 failure time	115 d	91 d 4 h	23 d 20 h
C-52 unplanned unavailability	~ 3.15 %	~ 2.50 %	20.6 %
Costs			
Scrapp material	45 870	33 510	26.9 %
Overtime work	636 214	496 953	21.9 %
Production loss	199 243	150 539	24.4 %
Repair - Spare part	411 001	368 415	10.4 %
Repair - Work	375 465	358 243	4.6 %
Maintenance - Material	36 600	36 600	0.0 %
Maintenance - Work	94 320	94 320	0.0 %
Replacement costs	0	8 081	
Unavailability costs	1 798 713	1 546 661	14.0 %
Investment costs	0	60 000	
Overall costs	1 798 713	1 606 661	10.7 %

Case B) – Life Cycle Profit Management (LCPM): Comparison of Scenarios

Figures are
fictional

C-38 & C-52 Scenario analysis (10 a)	Scenario 1: Current situation		Scenario 2: C-38 modernisation & C-52 corrective actions		Scenario 3: C-38 modernisation & C-52 renewal	
				Change		Change
C-38 & C-52 failures	27.6	20.0	27.5 %		16.8	39.1 %
C-38 & C-52 failure time	4 d 16 h	3 d 14 h	1 d 2 h		3d 5h	1 d 11 h
C-38 & C-52 unplanned unavailability	~ 0.128 %	~ 0.098 %	23.4 %		~ 0.088 %	31.3 %
C-38 failures	375.3	305.9	18.5 %		306.3	18.4 %
C-38 failure time	97 d 23 h	75 d 4 h	22 d 19 h		75 d 3 h	22 d 21 h
C-38 unplanned unavailability	~ 2.68 %	~ 2.06 %	23.1 %		~ 2.04 %	23.9 %
C-52 failures	365.7	359.0	1.8 %		226.6	38.0 %
C-52 failure time	115 d	91 d 4 h	23 d 20 h		58 d 23 h	12d 12h
C-52 unplanned unavailability	~ 3.15 %	~ 2.50 %	20.6 %		~ 1.54 %	51.1 %
Costs						
Scrapp material	45 870	33 510	27.9 %		49 530	8.5 %
Overtime work	636 214	496 953	21.9 %		890 530	39.5 %
Production loss	199 243	150 539	24.4 %		112 072	43.5 %
Repair - Spare part	411 001	368 415	10.4 %		202 030	31.2 %
Repair - Work	375 465	358 243	4.6 %		275 830	26.5 %
Maintenance - Material	36 600	36 600	0.0 %		36 000	1.6 %
Maintenance - Work	94 320	94 320	0.0 %		90 960	3.6 %
Replacement costs	0	8 081			0	
Unavailability costs	1 798 713	1 546 661	14.0 %		1 214 671	32.5 %
Investment costs	0	60 000			300 000	
Overall costs	1 798 713	1 606 661	10.7 %		1 514 671	15.8 %

Scenario 3 has the largest investment costs but the lowest overall costs due to residual unavailability

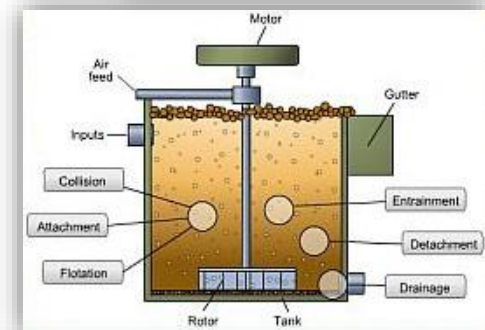
Case B) – Life Cycle Profit Management (LCPM): Key Findings and Improvements

*Figures are
fictional*

- Based on LCPM analysis, scenario 3, modernisation of auxiliary hoisting & renewal of older crane, improves the life cycle profit:
 - **Production loss reduced ~43 %**
 - **Overtime work costs reduced ~39 %**
 - **Simultaneous failures reduced ~39 %** and unavailability ~31 %
 - Total cost risk (including investments) reduced by ~16 % and 280 000 € during the 10 years period
 - Investment payback time ~5 years

Case C) – Mineral Processing Line

- Flotation process
 - Six processing tanks
 - Installed in series
 - Forming three tank pair units
- Goal of process
 - Recover metal particles from the slurry flowing through the tanks
 - with the help of rising air bubbles from the bottom of the processing tank

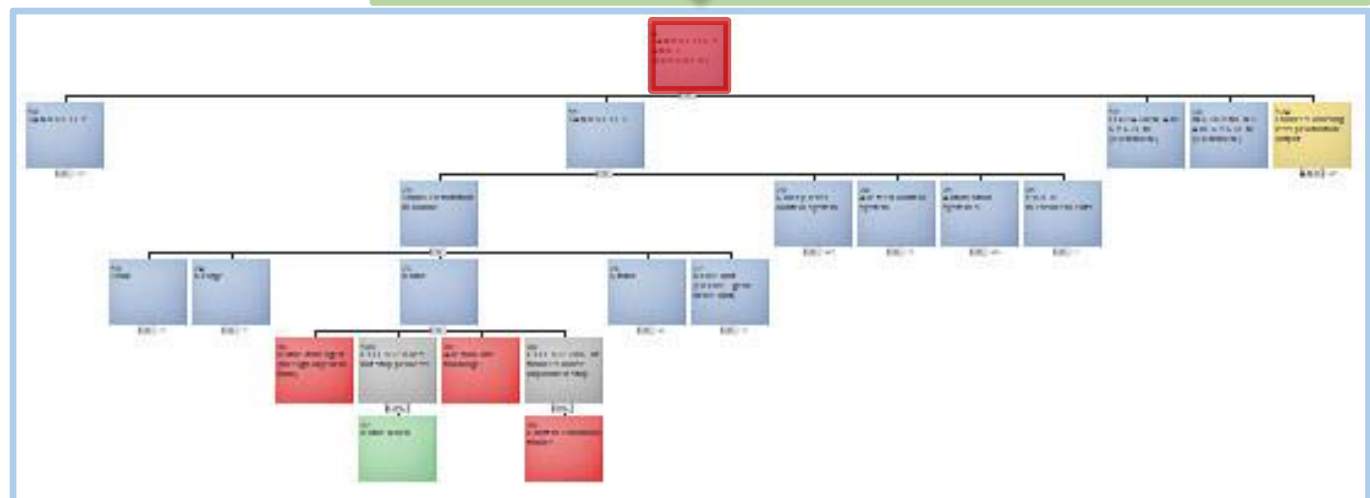


Case C) – Mineral Processing Line (MPL): Case Description

- The main goals of the project were:
 - 1) **Determine the availability and OEE** of the analyzed process line
 - 2) **Locate critical failure modes** for the line operation
 - 3) **Create methods for increasing the OEE value** of the process
- Project team (Experts from Ramentor and client) created a model
 - All mechanical and automation components included
 - Components of processing tanks and supporting systems included
 - Also process and user-related faults included
- Overall equipment effectiveness (OEE)
 - In addition to availability also performance (and quality) included

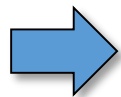
Case C) – Mineral Processing Line (MPL): ELMAS Project Model

- The **flow characteristics** model of the flotation process was combined with extensive **fault tree analytics**
- 600 nodes
- 200 failure modes



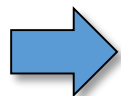
Case C) – Mineral Processing Line (MPL): Key Findings

- 1) The failure events slowing down the production had a major effect on the line OEE value (High availability, Low OEE)
 - Failures stopping the production caused **30%** of the total loss
 - Failures slowing down the process **70%** of the total loss



Focus on the situations slowing down the process

- 2) About **10%** of the failure modes caused over **83%** of the total lost production

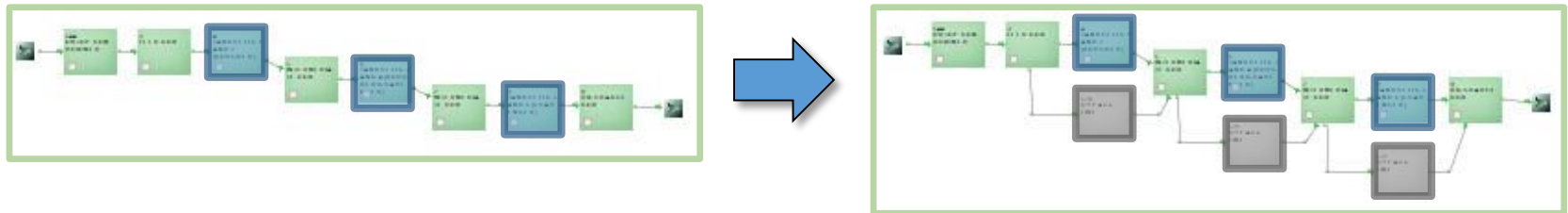


Focus on the highest impact failure modes

Case C) – Mineral Processing Line (MPL): Improvement – Maintenance bypass lines

- The effect of maintenance bypass lines installation shown
 - Direct the process flow around when a tank pair on repair
 - Only minor slowing down for the process during bypass

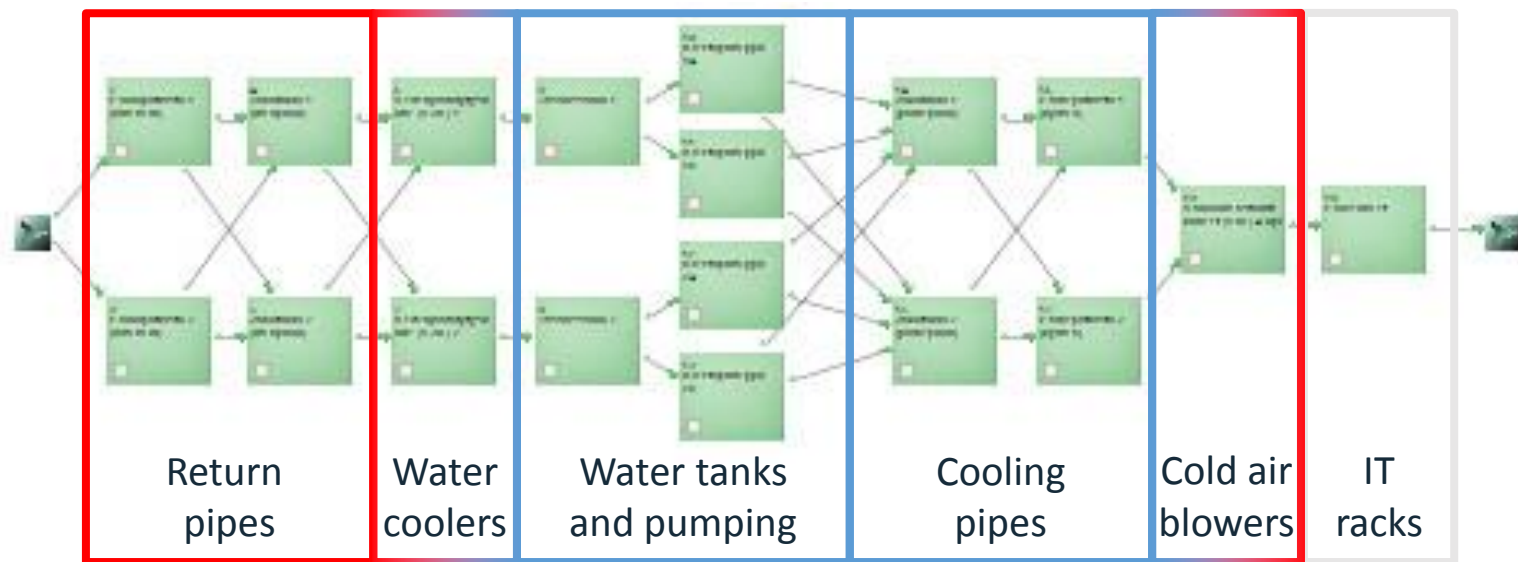
Tank pairs  Maintenance bypass lines 



- MPL manufacturer can justify the investment to customer
 - Lost production decreases by millions of euros during 10 years
 - The installation is quite inexpensive -> Very good investment!

Case D) – Infrastructure Availability: Design-Phase Data Center

- Availability study of a Data Center infrastructure
 - Including: Cooling system, Power input for the cooling, IT racks



+ Power input system (National grid inputs, Internal grid, UPS) for equipment and IT racks

Case D) – Infrastructure Availability: Case Description

- The main goals of the project were:
 - 1) Calculate the infrastructure availability
 - 2) Modifying the design structure to meet the highest Tier level 4 i.e. 99.995% availability (standard TIA-942)

Tier Level	Requirements
1	<ul style="list-style-type: none"> • Single non-redundant distribution path serving the IT equipment • Non-redundant capacity components • Basic site infrastructure with expected availability of 99.671%
2	<ul style="list-style-type: none"> • Meets or exceeds all Tier 1 requirements • Redundant site infrastructure capacity components with expected availability of 99.741%
3	<ul style="list-style-type: none"> • Meets or exceeds all Tier 1 and Tier 2 requirements • Multiple independent distribution paths serving the IT equipment • All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture • Concurrently maintainable site infrastructure with expected availability of 99.982%
4	<ul style="list-style-type: none"> • Meets or exceeds all Tier 1, Tier 2 and Tier 3 requirements • All cooling equipment is independently dual-powered, including chillers and heating, ventilating and air-conditioning (HVAC) systems • Fault-tolerant site infrastructure with electrical power storage and distribution facilities with expected availability of 99.995%

Case D) – Infrastructure Availability: Key Findings

- 1) The availability of the original design was at Tier level 3
 - The required highest Tier level 4 was not met
- 2) 8 hand valves were the source of highest availability risk
 - Minimum cooling power for operation is 75%
 - Repair of any of these 8 critical hand valves causes drop to 50% cooling power
- 3) The power input line was extremely reliable even without the backup generator
 - Discussions started considering the need of a backup generator

Case D) – Infrastructure Availability: Improvement – Eight new hand valves

- Effect of installing eight new hand valves shown
 - Now also the original eight critical hand valves can be isolated
 - Possible to repair/change any valve on the cooling line without lowering the cooling power below the required 75%
- Tier level 4 was met

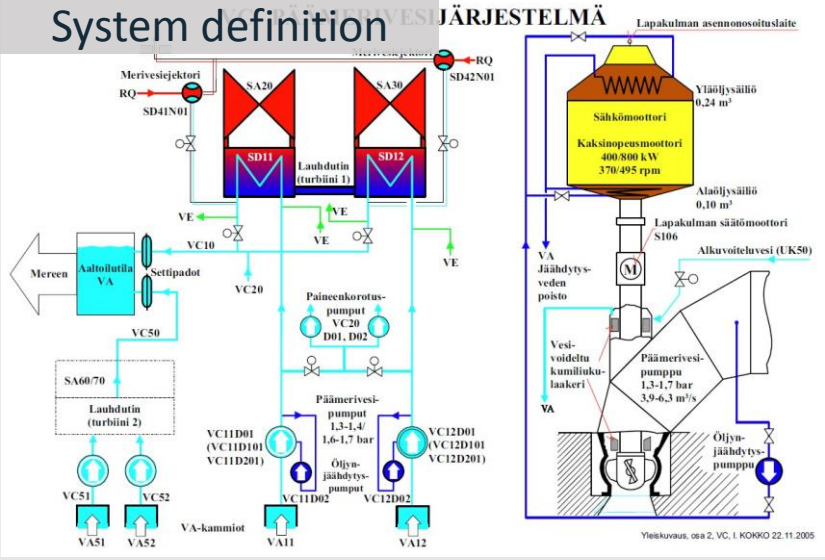


Case E) – Nuclear Power Plant (NPP): Project Scope

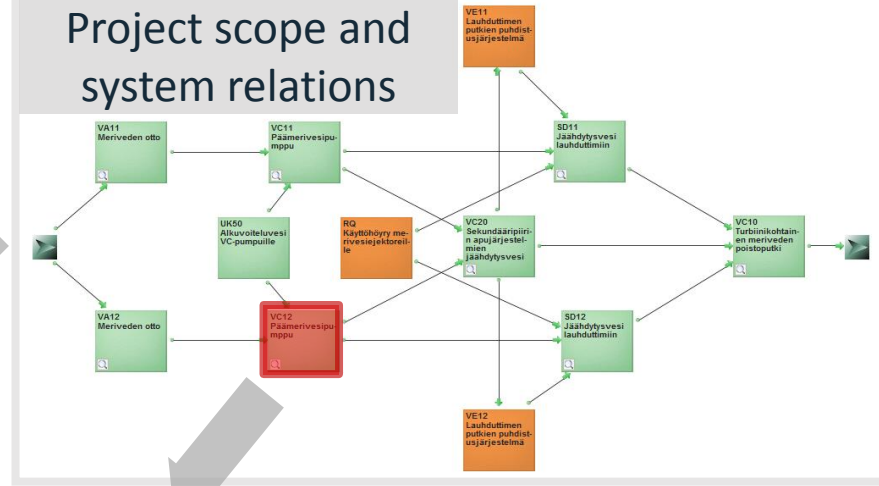
- RCM analysis of Main Cooling Water Pumping System
 - 1) Main function: Cooling of turbine condensers
 - 2) Secondary function: Cooling of auxiliary systems of secondary cooling circuit
- The Main Cooling Water Pumping System Includes:
 - 1) Sea water input, output and filtering system
 - 2) Main sea water system (pumps, motors, tubes, sea water ejectors etc.)
 - 3) Initial lubrication water system
 - 4) Cleaning system of condenser tubes

Case E) – Nuclear Power Plant (NPP): ELMAS Project Model

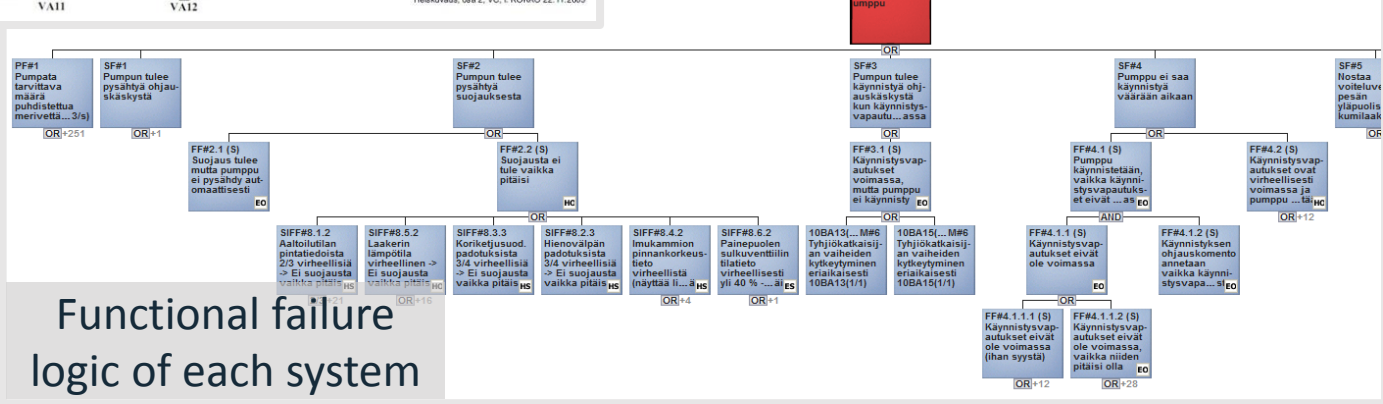
System definition



Project scope and system relations



Function hierarchy: VC11 Päämerivesipumppu



Functional failure logic of each system

Case E) – Nuclear Power Plant (NPP): Customer Demands

1. RCM analysis must include
 - All functions and functional failures
 - Safety, reliability, availability and maintainability aspect
 - All necessary cost types for comprehensive risk analysis
 - Maintenance action planning and optimization for critical equipment
2. RCM/ELMAS methodology training during the project

Case E) – Nuclear Power Plant (NPP): Key Findings & Value Added

- **Reduced preventive maintenance costs** by ~20%
- **Reduced overall cost risks** by ~10%
- Advanced criticality classification for equipment
- **List of critical spare parts**
 - Recommendations for spare part policy
- Motivation for improvements in use of operative IT-systems
- Scenarios for risks & equipment life cycle management

Summary – Applied ELMAS Features

- Cause-consequence relations model applied in each case
 - Fault tree applied in each case (Logic and stochastic relations)
 - Block diagram applied in two cases (Production flow)
 - Fuzzy relation in one case (75% operation with one crane)
 - Dynamic relations applied in one case (Change logic of backup)
- Failure and repair time definition for items in each case
 - Cumulative distribution function (parameter estimation / history data)
- Stochastic discrete event simulation made in each case
 - Different analysis results (risks, availability, ...) and reports
- Management of improvement tasks of items in one case
 - List tasks -> Prioritize and schedule -> Update model



Ramentor Inc.



Risk management, Risk assessment, Dependability – Standards and Theory

ISO GUIDE 73:2009 (1/2)

Risk management. Vocabulary

- **Risk:**
 - Effect of uncertainty on objectives
 - Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
- **Risk management:**
 - Coordinated activities to direct and control an organization with regard to **risk**

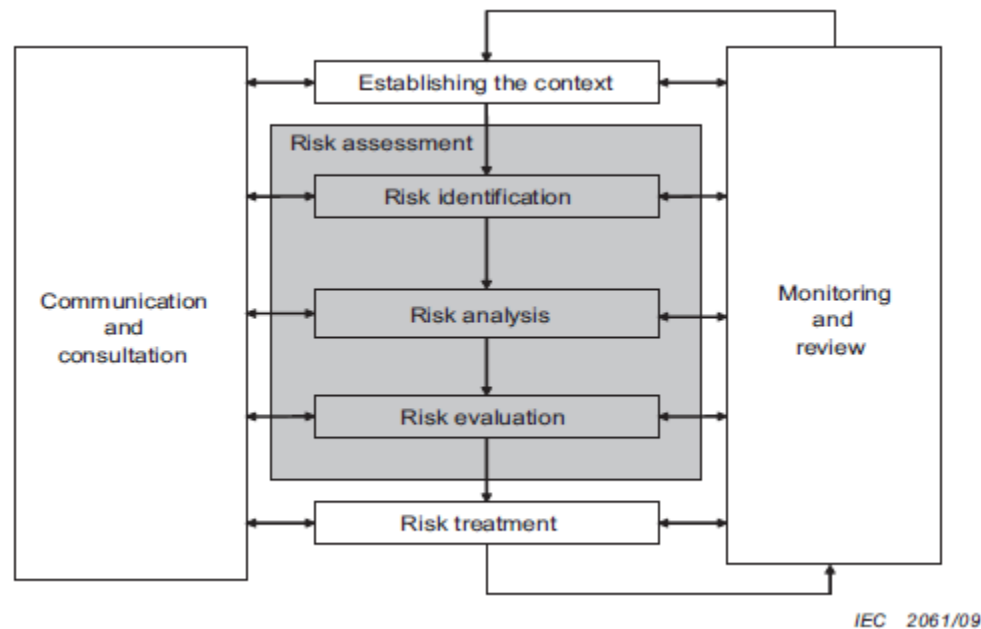
ISO GUIDE 73:2009 (2/2)

Risk management. Vocabulary

- **Risk assessment:**
 - Overall process of **risk identification**, **risk analysis** and **risk evaluation**
- **Risk identification:** Process of finding, recognizing and describing **risks**
- **Risk analysis:** Process to comprehend the nature of **risk** and to determine the **level of risk**
- **Risk evaluation:** Process of comparing the results of **risk analysis**, with **risk criteria** to determine whether the **risk** and/or its magnitude is acceptable or tolerable

EN 31010:2010

Risk management. Risk assessment techniques

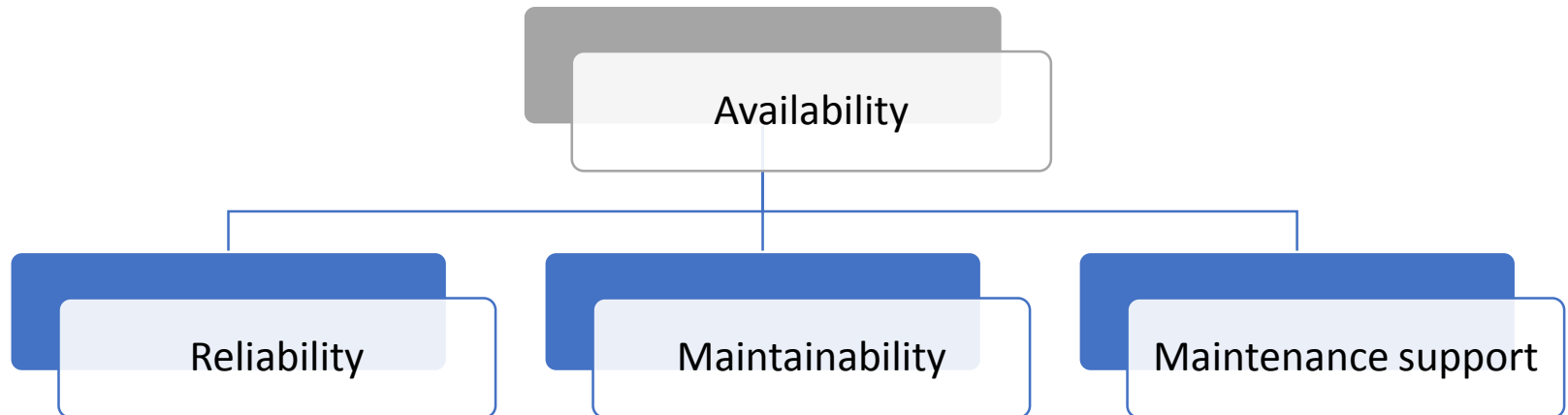


Contribution of risk assessment to the risk management process

IEC 50(191):1990

Electrotechnical vocabulary. Dependability and quality of service

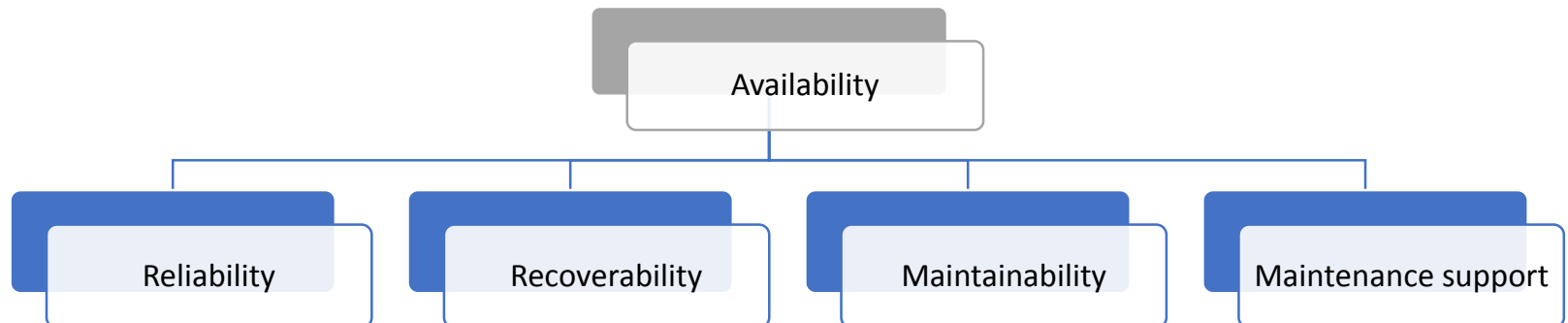
- **Dependability:**
 - The collective term used to describe the **availability** performance and its influencing factors: **reliability** performance, **maintainability** performance and **maintenance support** performance.



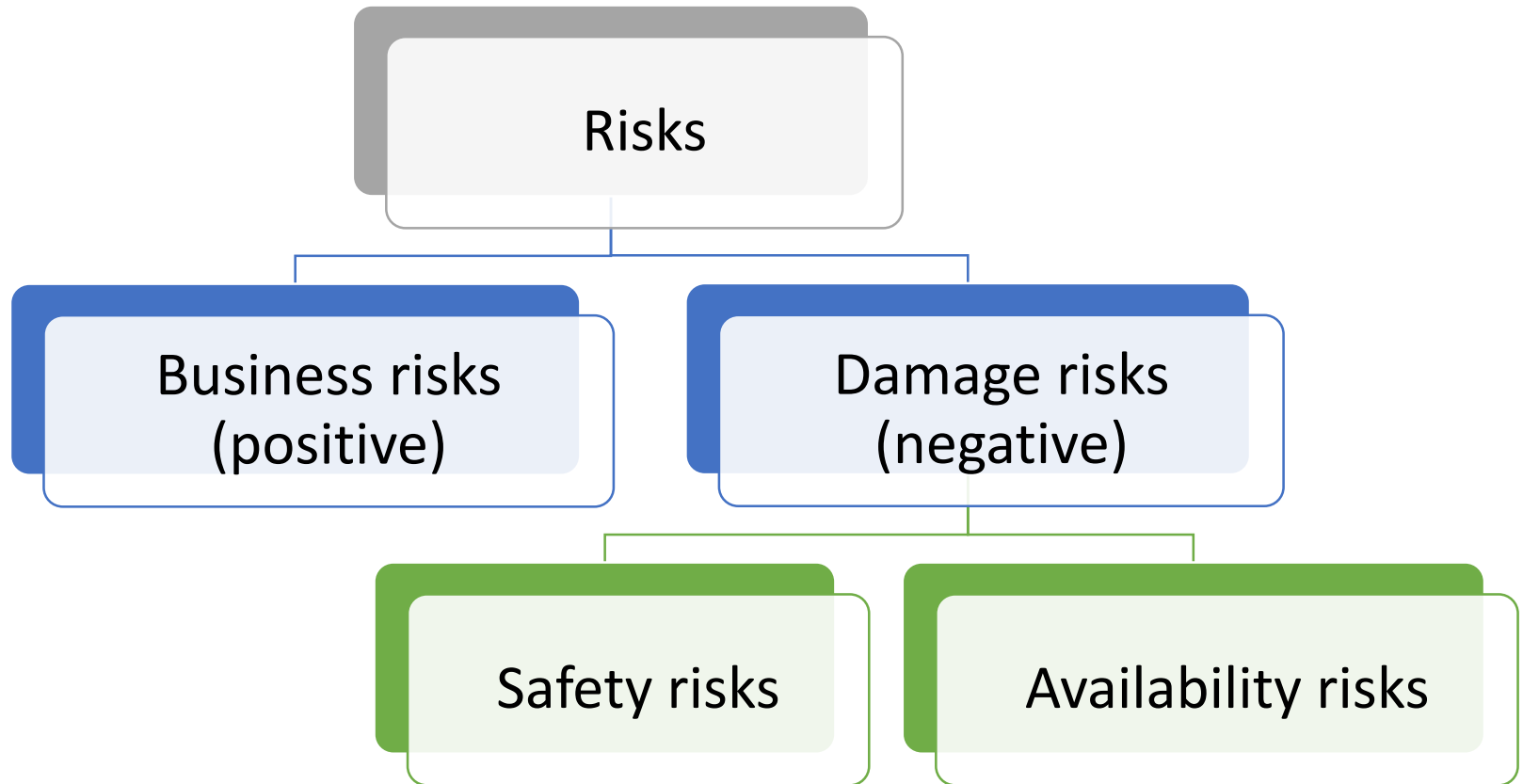
EN 13306:2010

Maintenance. Maintenance terminology

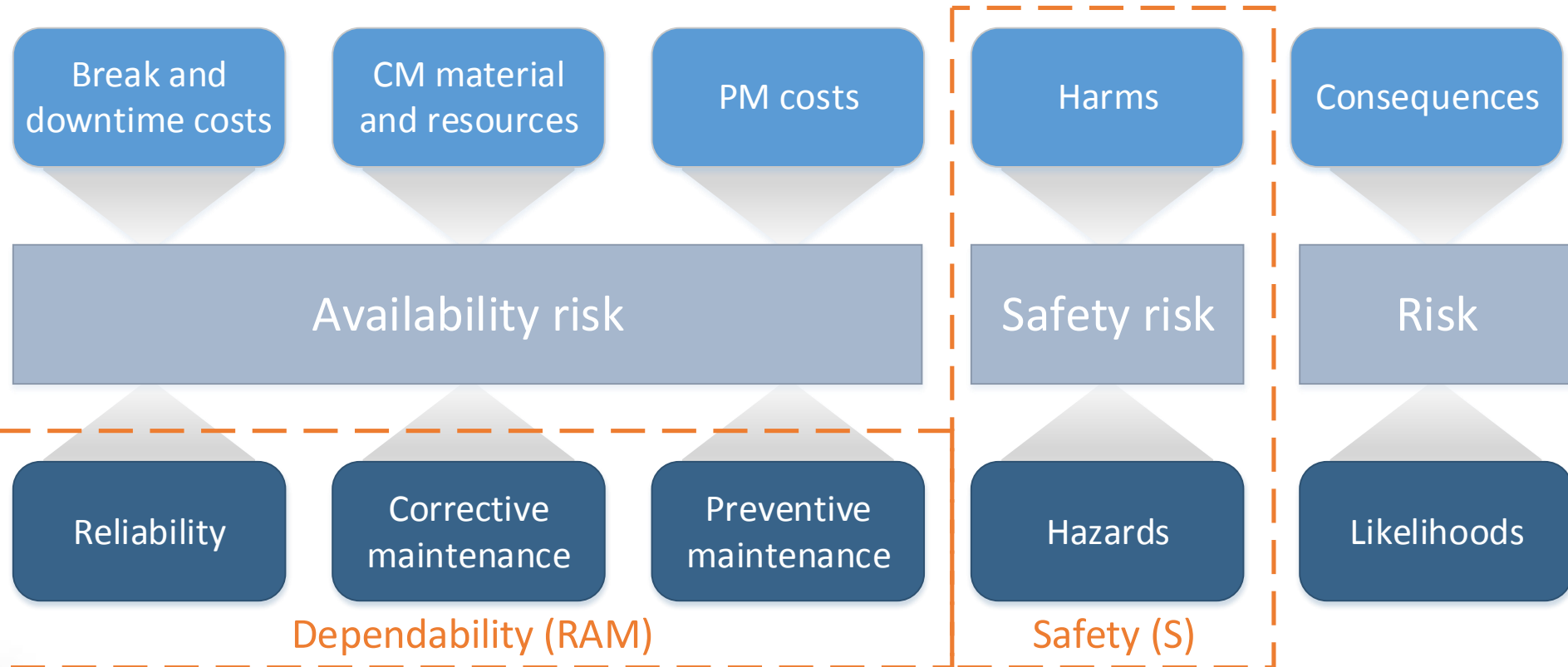
- **Dependability:**
 - Ability to perform as and when required
 - Dependability characteristics include availability and its influencing factors (reliability, recoverability, maintainability, maintenance support performance) and, in some cases, durability, economics, integrity, safety, security and conditions of use.



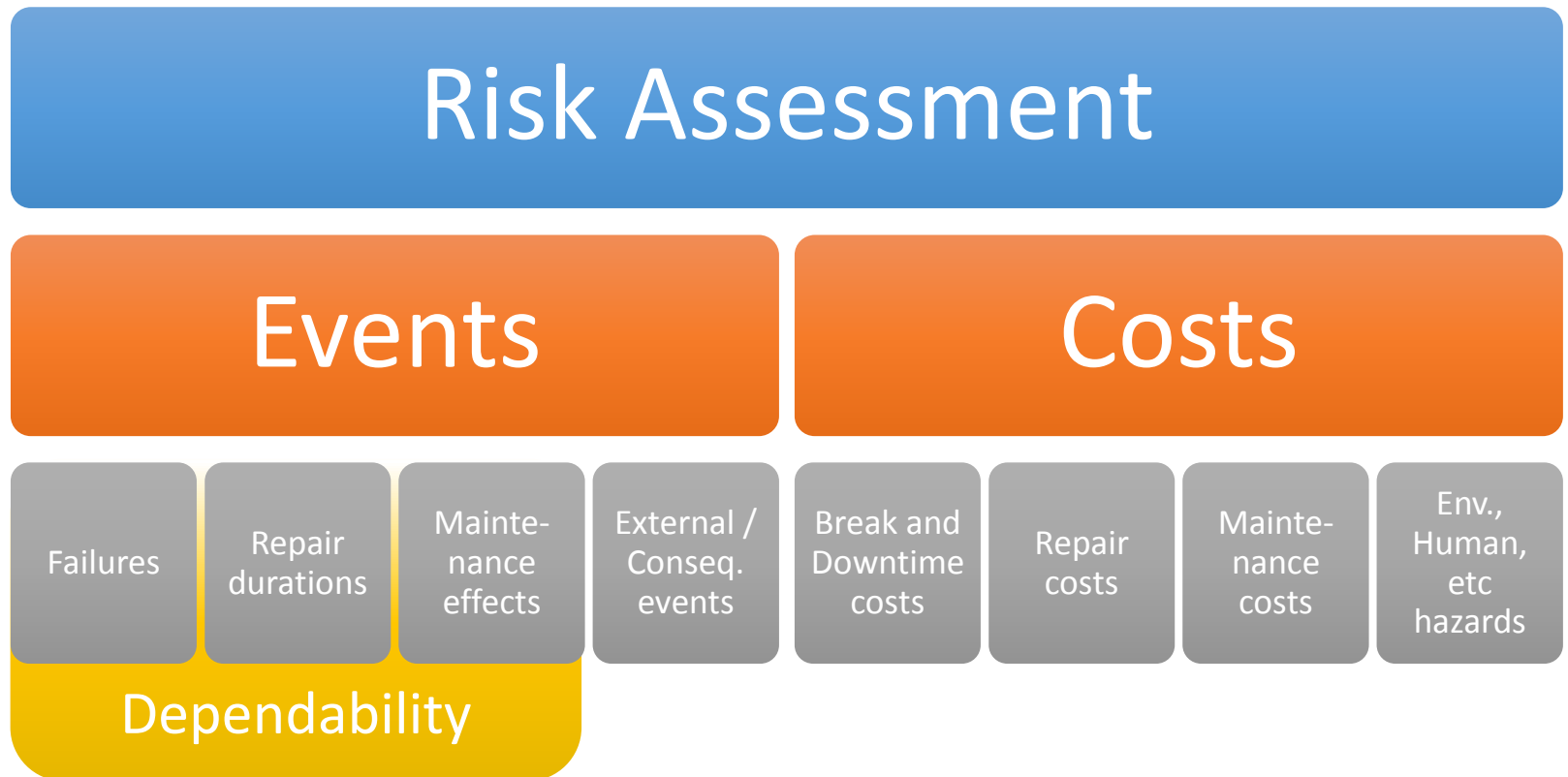
Risks – 1/2



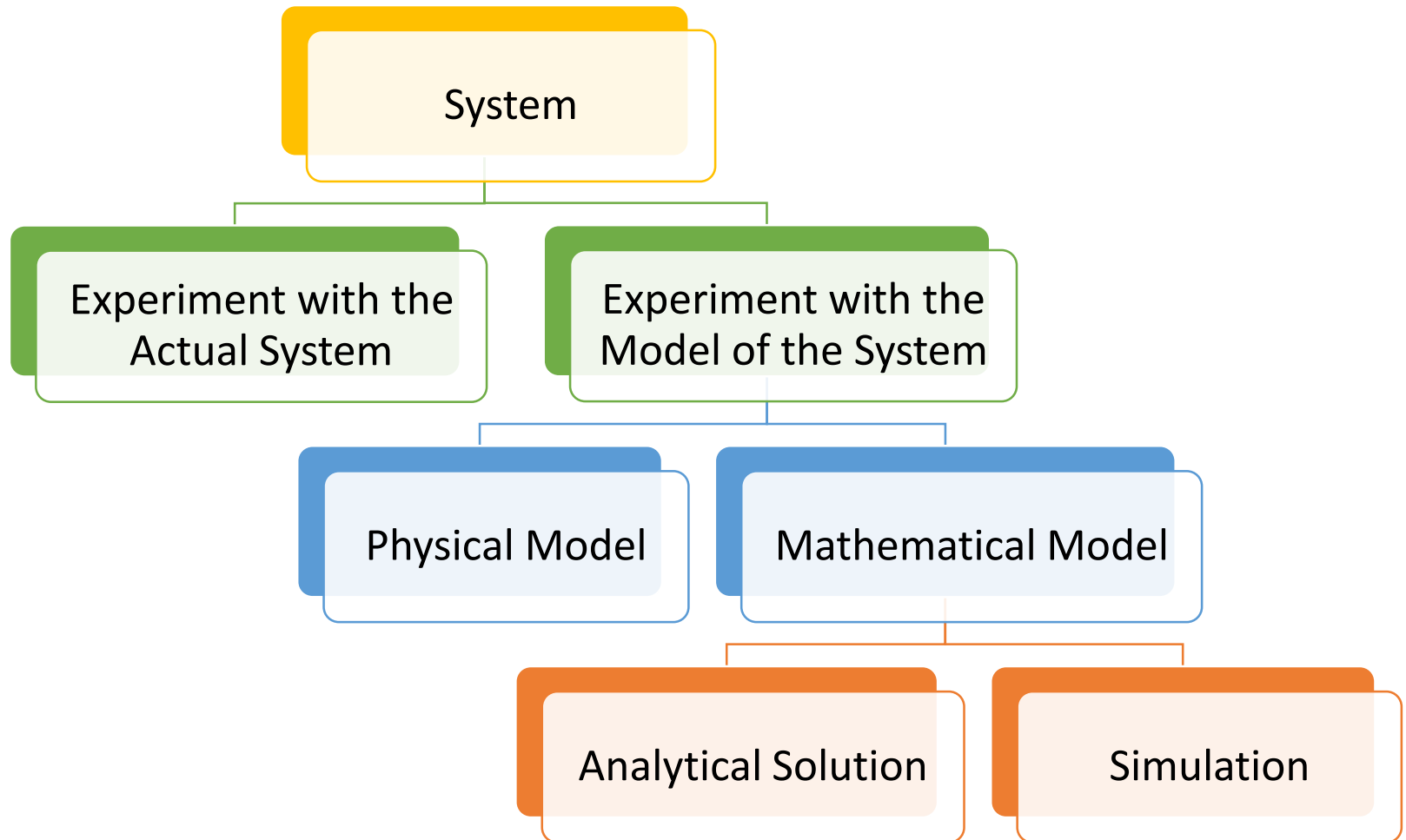
Risks – 2/2



Risk Assessment and Dependability



Ways to Study a System





Methods: Tools and Techniques

- EN 31010:2010 Risk management. Risk assessment techniques

Qualitative tools and techniques

- Failure modes and effects analysis (FMEA)
 - Identify the ways in which components, systems or processes can fail to fulfil their design intent. Identifies all potential failure modes of the various parts of a system, the effects these failures may have on the system, the mechanisms of failure and how to avoid the failures, and/or mitigate the effects of the failures on the system.
- Reliability centered maintenance (RCM)
 - Identify the policies that should be implemented to manage failures so as to efficiently and effectively achieve the required safety, availability and economy of operation for all types of equipment.
- Root cause analysis (RCA), 5 times “Why?”
 - Identify the root or original causes instead of dealing only with the immediately obvious symptoms.
- Hazard and operability studies (HAZOP)
 - Identify risks to people, equipment, environment and/or organizational objectives.
- Check-lists
 - Lists of hazards, risks or control failures that have been developed usually from experience, either as a result of a previous risk assessment or as a result of past failures.

Quantitative tools and techniques

- **Fault tree analysis (FTA)**
 - A technique which starts with the undesired event (top event) and determines all the ways in which it could occur. These are displayed graphically in a logical tree diagram. Once the fault tree has been developed, consideration should be given to ways of reducing or eliminating potential causes/sources.
- **Event tree analysis (ETA)**
 - Using inductive reasoning to translate probabilities of different initiating events into possible outcomes.
- **Monte Carlo simulation**
 - For systems that are too complex for the effects of uncertainty on them to be modelled using analytical techniques
- **Cause and consequence analysis**
 - A combination of fault and event tree analysis that allows inclusion of time delays. Both causes and consequences of an initiating event are considered.
- **Failure modes and effects and criticality analysis (FMECA)**
 - FMECA extends an FMEA so that each fault mode identified is ranked according to its importance or criticality.



Event Logic Modelling and Analysis Software – ELMAS Overview

ELMAS – Risk Assessment and RAMS

Risk Assessment

Likelihoods/Events

Consequences/Costs

Failures

Repair durations

Maintenance effects

External / Conseq. events

Break and Downtime costs

Repair costs

Maintenance costs

Env., Human, etc hazards

RAMS

ELMAS

ELMAS

Event

- Time to Failure, Distribution
- Time to Repair, Distribution
- Maintenance actions
- Break and downtime loss
- Repair Costs
- Hazards
- Usage and stress profile
- External events

Logic

- OR
- AND
- K/N-Voting
- XOR-Exclusive
- Limits
- Conditional probability
- Delays
- Throughput, fuzzy logic
- Dynamic coding

Modeling

- Fault tree
- Event tree
- Cause-consequence-tree
- Reliability block diagram
- Process diagram
- Waiting and redundancy
- Buffers
- Failure modes, RCA

Analysis

- Simulation
- Reliability, Availability
- Risk Analysis
- Importance measures
- Conditional probabilities
- Spare part consumption
- Resources
- FMEA, Classification, RCM, Decision tree, Criticality

Software

- Graphical user interface
- Excel export and import
- HTML report
- Table summary
- ERP interface
- Project versioning
- Template library
- Search
- Web start

ELMAS 4.7

<http://www.ramentor.com/products/elmas/>

ELMAS 4 - Cooling line example

File Edit Tools About

1 Cooling line

Model process functions (RBD)

Water filtration

Primary cooling circulation - Water

Primary cooling circulation - Chiller

Secondary cooling circulation

All items of the model listed

ID	Name
1	Cooling line
2	Water source
3	Lifting pump 1
4	Lifting pump 2
5	Filtering phase
6	Clean water tank
7	Primary circulation p...
8	Primary circulation p...
9	Water manifold
10	Heat exchanger 1
11	Heat exchanger 2
12	Water chiller
13	Chiller circulation pu...
14	Heat exchanger Chiller
15	Balancing tank
16	Secondary circulation...
17	Secondary circulation...
18	Server room
19	Server room
20	Inverter failure
21	Motor failure
22	Pressure sensor failure
23	Pump failure
24	Inverter failure
25	Motor failure
26	Pressure sensor failure
27	Pump failure
28	Filters fail
29	Filter 1
30	Inverter failure
31	Motor failure
32	Gearbox failure
33	Gaskets
34	Filter 2
35	Inverter failure
36	Motor failure
37	Gearbox failure
38	Gaskets
39	Filter 3
40	Inverter failure
41	Motor failure
42	Gearbox failure
43	Gaskets
44	Chiller stopping failure
45	Chiller stopping main

Model failures of the selected system (FTA)

14 Heat exchanger Chiller

OR

186 Heat transfer dirty

187 Heat transfer leakage

OR

188 Temperature control valve

OR

189 Actuator failure

190 Sensor failure

191 Valve failure

Input data for the selected component

14 Heat exchanger Chiller

Edit node: 191 Valve failure

General Restoration Replacement Finding Redesign RTF

Type Maint. LTA Preventive Inspection

Relations

Classification

Failure Generally it is reasonable to carry out the scheduled condition monitoring actions, if 1) it is possible to define and detect the symptoms of the failure early enough, 2) P-F-period (Point Failure) is moderately solid and 3) it is practical to control the object in shorter time periods than the P-F-period.

Repair

Maintenance

Active	Name	Interval	Cost (€)	Symptom ti...	Probability
<input checked="" type="checkbox"/>	Valve check	30.0 d	20.0	30.0 d	0.9

Add cost from all overlapping (even only first is handled):

Add inspection Remove selected rows

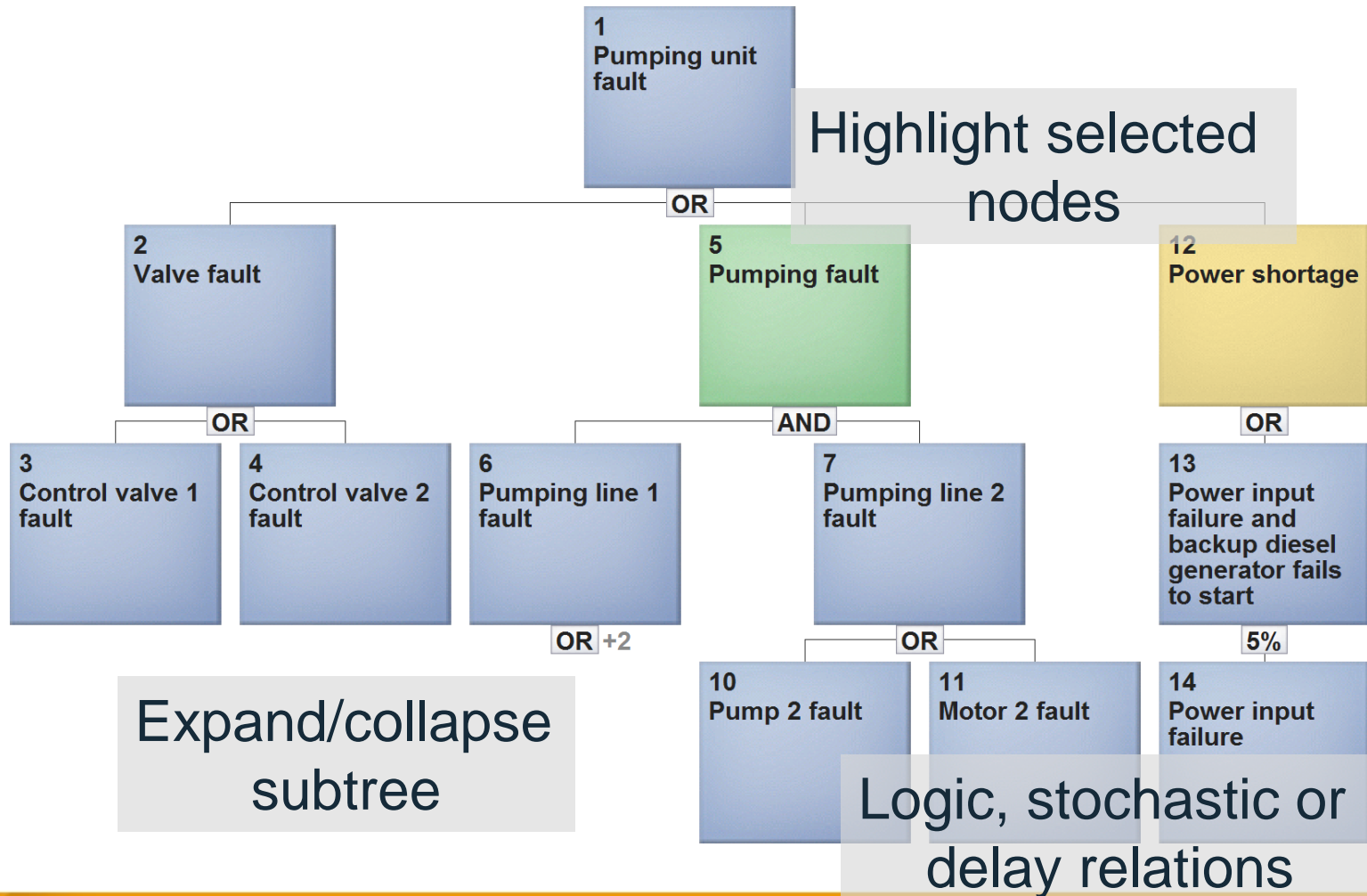
OK Cancel ?

Hide level Collapse all Expand all

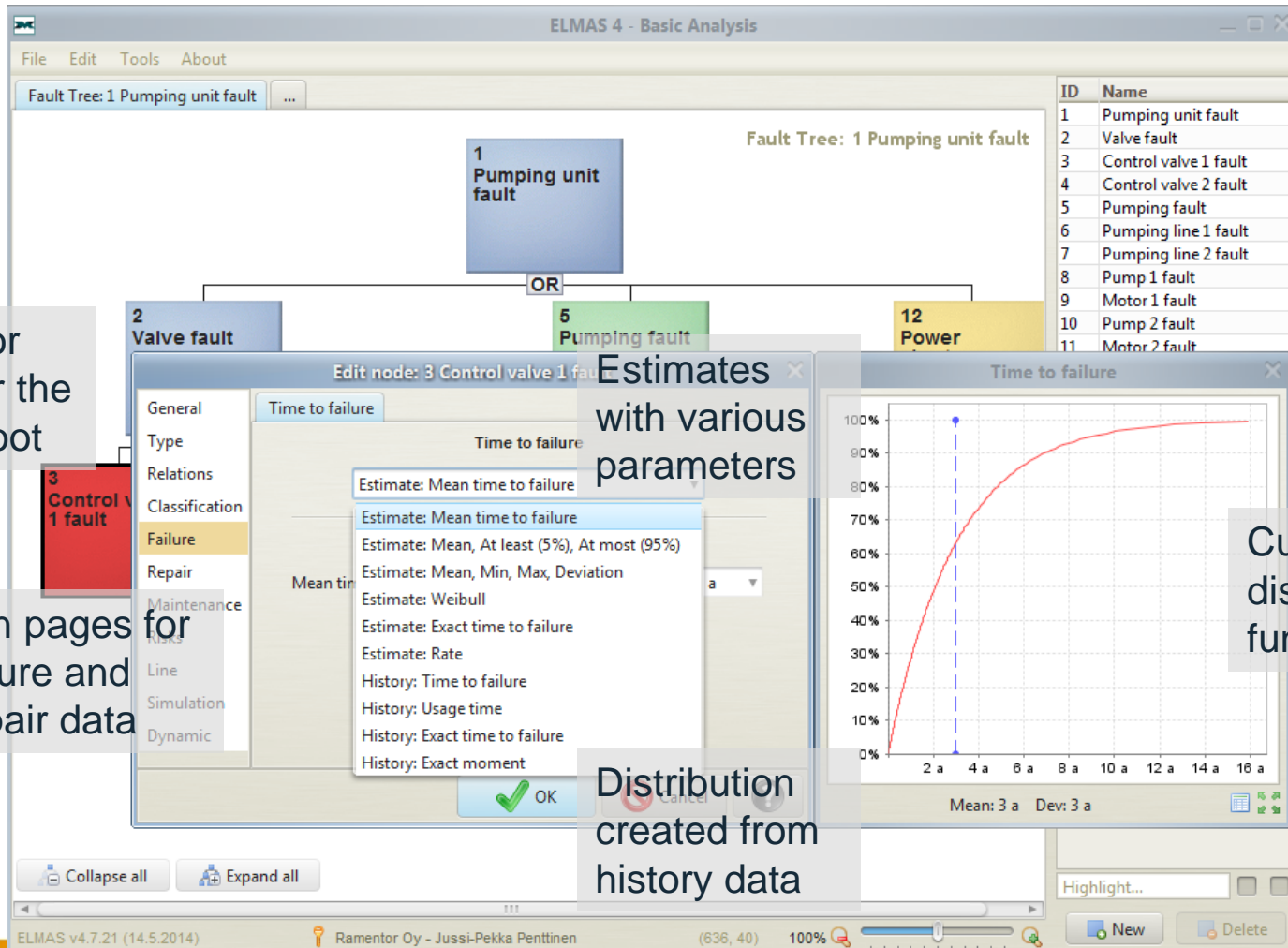
ELMAS v4.7.22 (3.6.2014) Ramentor Oy - Jussi-Pekka Penttinen (912, -28) 100%

www.ramentor.com

Modelling of a Fault tree structure



Failure and Repair distribution for root



File Edit Tools About

Fault Tree: 1 Pumping unit fault

ID	Name
1	Pumping unit fault
2	Valve fault
3	Control valve 1 fault
4	Control valve 2 fault
5	Pumping fault
6	Pumping line 1 fault
7	Pumping line 2 fault
8	Pump 1 fault
9	Motor 1 fault
10	Pump 2 fault
11	Motor 2 fault

1 Pumping unit fault

OR

2 Valve fault

5 Pumping fault

12 Power

3 Control valve 1 fault

Estimates with various parameters

Time to failure

Estimate: Mean time to failure

Estimate: Mean, At least (5%), At most (95%)

Estimate: Mean, Min, Max, Deviation

Estimate: Weibull

Estimate: Exact time to failure

Estimate: Rate

History: Time to failure

History: Usage time

History: Exact time to failure

History: Exact moment

OK

Time to failure

100%

90%

80%

70%

60%

50%

40%

30%

20%

10%

0%

2 a

4 a

6 a

8 a

10 a

12 a

14 a

16 a

Mean: 3 a Dev: 3 a

Cumulative distribution function shown

Own pages for Failure and Repair data

Distribution created from history data

ELMAS v4.7.21 (14.5.2014)

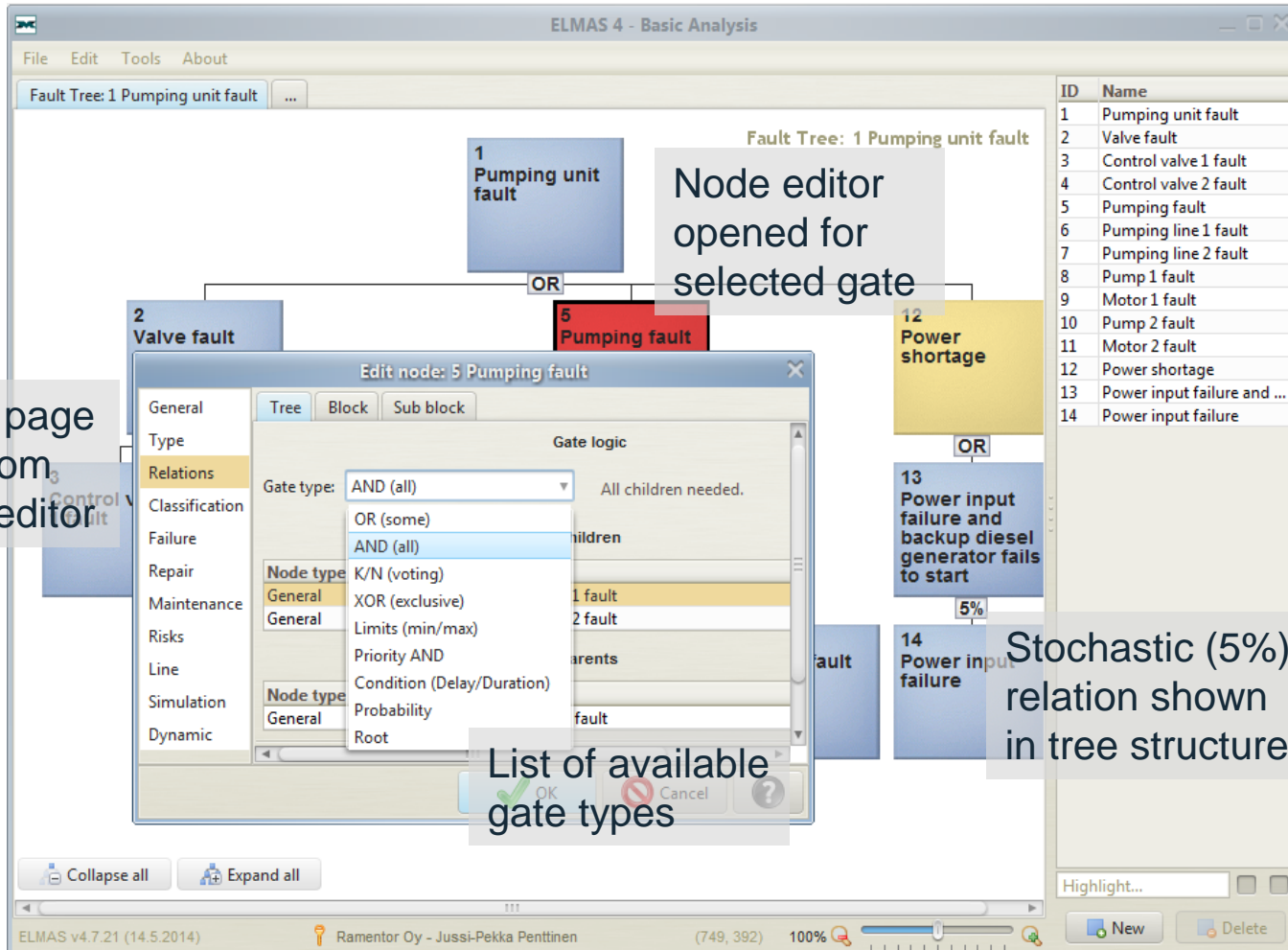
Ramentor Oy - Jussi-Pekka Penttinen (636, 40) 100%

New Delete

Highlight...

www.ramentor.com

Logic, Stochastic and Delay gates



ELMAS 4 - Basic Analysis

File Edit Tools About

Fault Tree: 1 Pumping unit fault

1 Pumping unit fault

2 Valve fault

5 Pumping fault

12 Power shortage

13 Power input failure and backup diesel generator fails to start

14 Power input failure

Node editor opened for selected gate

Relations page opened from the node editor

Stochastic (5%) relation shown in tree structure

List of available gate types

ID	Name
1	Pumping unit fault
2	Valve fault
3	Control valve 1 fault
4	Control valve 2 fault
5	Pumping fault
6	Pumping line 1 fault
7	Pumping line 2 fault
8	Pump 1 fault
9	Motor 1 fault
10	Pump 2 fault
11	Motor 2 fault
12	Power shortage
13	Power input failure and ...
14	Power input failure

ELMAS v4.7.21 (14.5.2014) Ramentor Oy - Jussi-Pekka Penttinen (749, 392) 100%

www.ramentor.com

Dynamic parameters and Coding

Edit node: 21 Backup diesel generator 1 running failure

General | Shortcuts | Constants | Parameters | Lists | Basic code | **Event Code**

Type: Event simulation code

```
//START RUNNING
//If backup diesel generator is needed
if (GET_NODE("14").getState() != GET_NODE("14").getPreviousState() &&
GET_NODE("14").getState() == STATE_FAILED) {

    //And start is successful
    if (GET_NODE("13").getState() == STATE_OK) {
        THIS_NODE.startOperation();
    }
}

//STOP RUNNING
//If backup diesel generator is NOT needed
if (GET_NODE("14").getState() != GET_NODE("14").getPreviousState() &&
GET_NODE("14").getState() == STATE_OK) {
    THIS_NODE.setSleep();
}
}
```

Dynamic coding page opened from the node editor

OK Cancel ?

Own tabs to define used parameters and codes of different situations

Freely defined Java code with links to simulation states

Dynamic coding page opened from the node editor

Other node properties

- Maintenance actions, intervals, costs and resources
 - Preventive, Inspection, Restoration, Replacement, Failure finding
- Expenses related to risk analysis (static or stochastic)
 - Break and downtime loss, repair and resource costs, spare parts
- Throughput of a production line
 - Fuzzy logic operations
- Node classification based on selected criteria
 - FMEA, Criticality

Stochastic simulation and results

Studied period tab from basic results page opened

Analysis: Simulation Tool

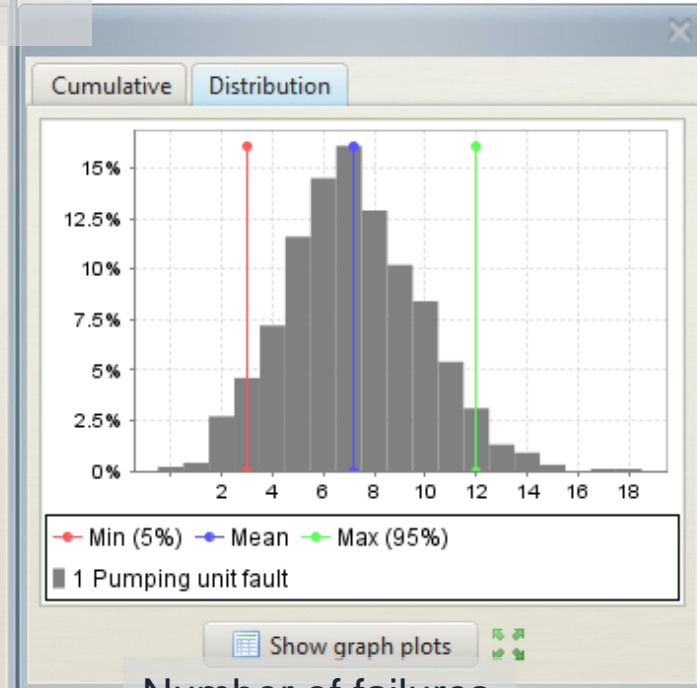
Profile Availability Unreliability Mean times Studied period

Simulation Failures during studied period

Basic Studied time period: 10 a

ID	Name	Failed time	Failures
1	Pumping unit fault	3 d 6 h	7.192
2	Valve fault	2 d 6 h	6.724
5	Pumping fault	43.1 s	0.006
12	Power shortage	1 d 21 min	0.465
3	Control valve 1 fault	1 d 3 h	3.351
4	Control valve 2 fault	1 d 3 h	3.376
6	Pumping line 1 fault	2 d 23 h	6.373
7	Pumping line 2 fault	3 d 2 h	6.624
13	Power input failure and backup di...	1 d 21 min	0.465
8	Pump 1 fault	1 d 23 h	3.967
9	Motor 1 fault	23 h 36 min	2.409
10	Pump 2 fault	2 d 28 min	4.09
11	Motor 2 fault	1 d 1 h	2.537
14	Power input failure	22 d 18 h	9.722

Results for each simulated node shown in table



Number of failures distribution shown for selected node

Risk analysis

Analysis: Simulation Tool

Entity risks Node risks Subtree risks **Relative risks** LCC Comb.risks

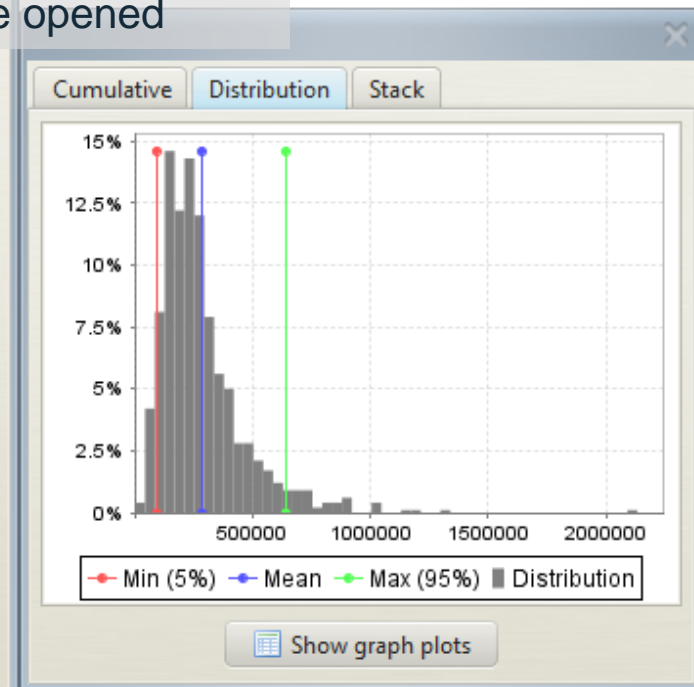
Relative risks

Studied time period: 10 a

Show lines with zero risk:

ID	Name	Downtime (€)	Spare parts (€)	Relative risk...
1	Pumping unit fault	234 475	49 310	283 784
2	Valve fault	161 399	13 454	174 853
3	Control valve 1 fault	80 923	6 702	87 625
4	Control valve 2 fault	80 489	6 752	87 241
12	Power shortage	73 079	2 431	75 510
13	Power input failure and backu...	73 079	2 431	75 510
14	Power input failure	73 079	2 431	75 510
5	Pumping fault	36	33 425	33 461
7	Pumping line 2 fault	36	17 060	17 095
6	Pumping line 1 fault	36	16 366	16 401
11	Motor 2 fault	13	8 880	8 893
9	Motor 1 fault	13	8 432	8 444
10	Pump 2 fault	23	8 180	8 203
8	Pump 1 fault	23	7 934	7 957

Relative risks tab from Risk results page opened



Relative risk = the risk of the node itself + the risk the node causes through other nodes

Distribution of risks with min and max estimate shown for selected node

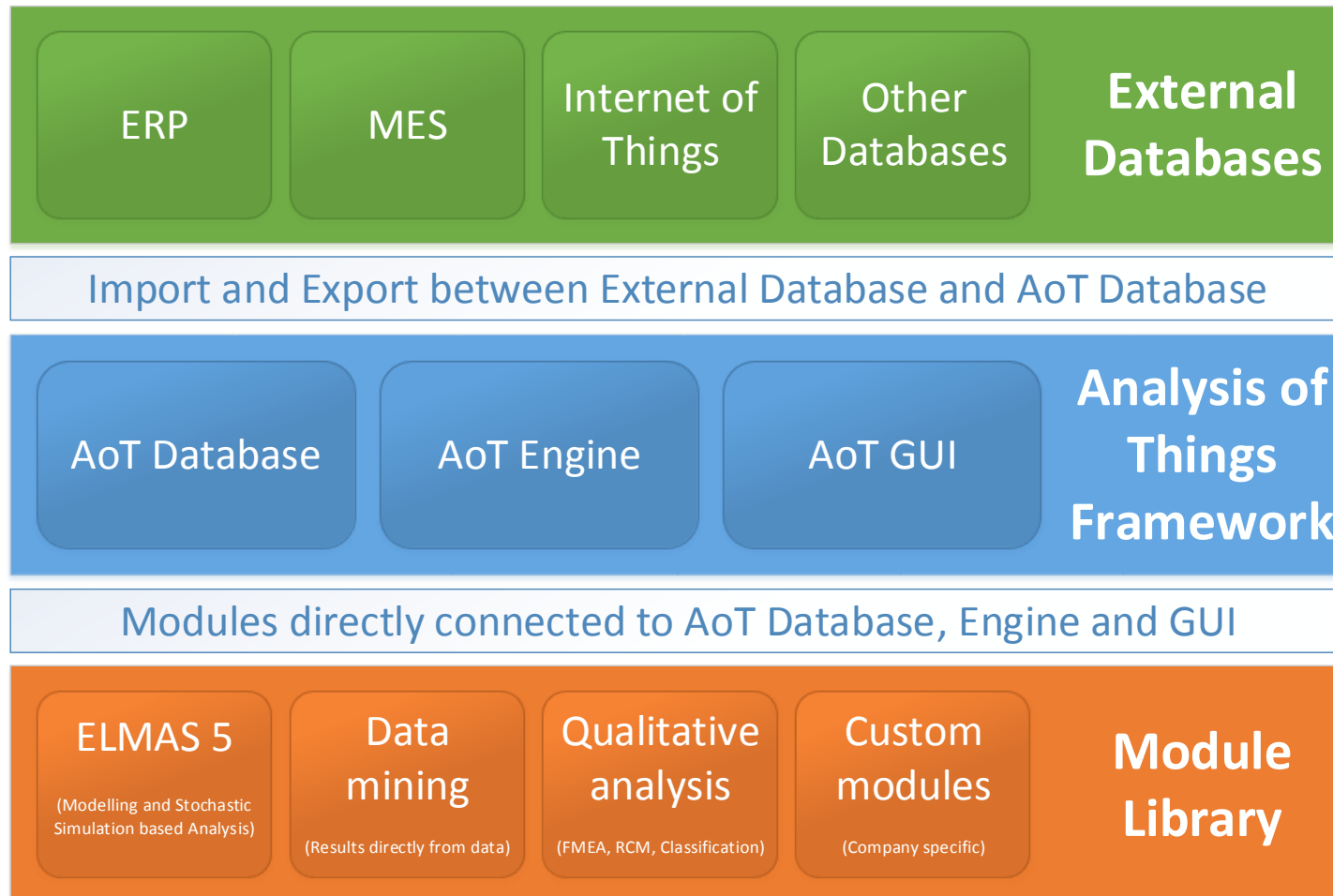
Other properties

- Import data through Excel tables
- Export HTML or Excel reports
- FMEA, RCM and RCA tools
- Combined Block diagrams, Fault trees and Event trees
- Usage, stress and production profile in simulation
- Conditional and importance results from simulation
- History report simulation
- Show only needed tools and hide unused tools
- Change terms and texts used in the software for each case

Some future plans

- Analysis of Things (AoT) framework with modules for different usages:
 - ELMAS 5, Data mining, Qualitative analyses, Company specific...
- Direct data import/export with external databases
 - ERP, MES, Internet of Things, Company database...
- More possibilities (than change of terms and hide analyses) to tailor GUI and simulation for each case
 - Efficiency for large and complex model simulations (Nuclear)
 - Straightforward simple analyses (PERT, basic fault tree)
- Online module library for different usages/analyses

Analysis of Things (AoT) Framework



Levels with Fleet Model included

Model creation (Experts), Data collection (MES, ERP)

Failure/Repair distribution

Maintenance, Diagnostics

Expert knowledge

Device hierarchy

Usage profile data

Customer needs

Costs data

Hazards

Risk Model (and Consequence Model)

Fleet Model

System Model

Component / Device Model

Causality Logic

Fleet logic Usage profile

Chains of consequences

Costs: Repair, Maintenance, Downtime, ...

Simulation, Analysis, Optimization

Component reliability

Maintenance strategy

System availability

Component importance

Fleet performance

Customer satisfaction

Risks, Safety

Warranty

Reporting, Decision Making, Life Cycle Management

Ramentor Oy