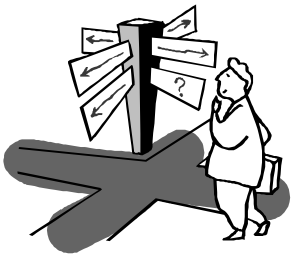
R&S Training Course
CERN, February 2002

Welcome to



Reliability and Safety (R&S)
Training Course

P. Kafka, ESRA, Reconsult

1

R&S Training Course
CERN, February 2002

Content

2

Module 1:
Basic Elements in Reliability Engineering

R&S Training Course
CERN, February 2002

Content:

- Short R&S History
- Some Basic Terms
- A few Definitions and Formalisms
- From Components to Systems
- Important Methods
- Common Cause Failures
- Human Factor Issues
- Types of Uncertainties

3

Module 1:
Short History of R&S as Synonym of Risk

R&S Training Course
CERN, February 2002

- Risk – very old Term (Perikles; 430 v.Chr)
  “the worst thing is to rush into actions before the consequences have been properly debated”, and “the Athenians are capable at the same time of taking Risk and Estimating before-hand”
- „Trial and Error“ Approach (‘00 – ‘40)
- „Worst Case - Safety Case“ Studies (‘40 –)
- Recognition of Stochastic Events (‘40)
- Development of Reliability Theory (’40 -)
- Reliability Studies for Complex Systems (’50 -)
- Comprehensive Risk Studies (’70 -)
- Global Risk Management:
  based on: Goal – Assignment – Proof (’90 -)
- „Risk Informed Decision Making“ (‘95 -)
- Risk Studies for Large Scale Test Facilities just in the beginning (’00 -)

Time Axis

4

Module 1:
Some Basic Terms

R&S Training Course
CERN, February 2002

- Reliability:

  The ability of an item to operate under designated operating conditions for a designated period of time or number of cycles.

  Remark: The ability of an item can be designated through a probability, or can be designated deterministic

- Availability:

  The probability that an item will be operational at a given time

  Remark: Mathematically the Availability of an item is a measure of the fraction of time that the item is in operating conditions in relation to total or calendar time

5

Module 1:
Some Basic Terms

R&S Training Course
CERN, February 2002

- Maintainability:

  The probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources *(IEC 60050)1)*

  Remark: probabilistic definition

- Safety:

  Freedom from unacceptable risk of harm

  Remark: very vague definition

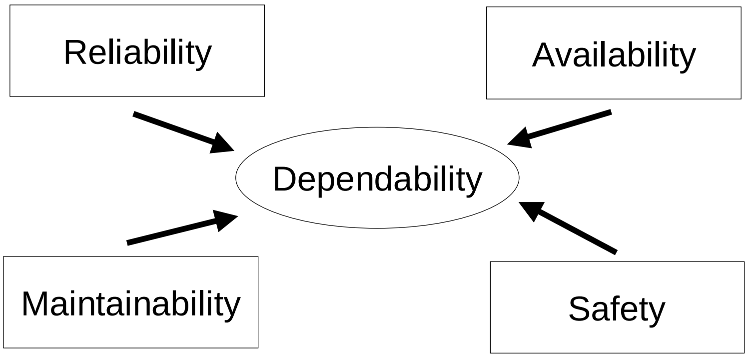
- RAMS: An acronym meaning a combination of Reliability, Availability, Maintainability and Safety

6

Module 1:
Some Basic Terms

R&S Training Course
CERN, February 2002

Today‘s Understanding for Purists



7

Module 1:
Some Basic Terms

R&S Training Course
CERN, February 2002

- Hazard: A physical situation with a potential for human injury, damage to property, damage to the environment or some combination of these
- Individual Risk: The frequency at which an individual may be expected to sustain a given level of harm from the realisation of specified hazards
- Social Risk: The frequency with which a specified number of people in a given population, or population as a whole, sustain a specified level of harm from the realisation of specified hazards

8

Module 1:
A few Definitions and Formalisms

For non-repaired items the reliability function:

$$R(t) = \exp\left[- \int_0^t \lambda(x)dx\right] = \int_t^\infty f(x)dx$$

where

$\lambda(x)$ is the instantaneous failure rate of an item

$f(x)$ is the probability density function of the time to failure of the item

when $\lambda(t) = \lambda$ = constant, i.e. when the (operating) time to failure is exponentially distributed

$R(t) = \exp(-\lambda t)$

Example:

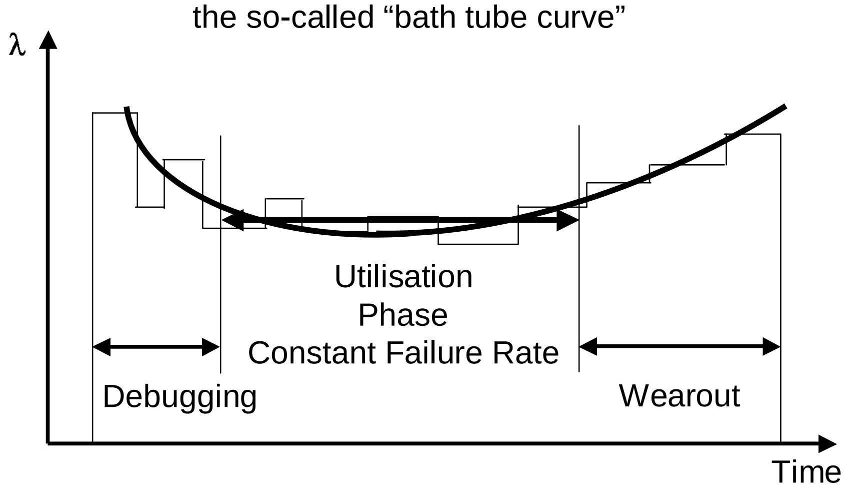
For an item with a constant failure rate of one occurrence per operating year and a required time of operation of six month, the reliability is given by

$R(6m) = \exp(- 1 \times 6/12) = 0{,}6065$

9

Module 1:
A few Definitions and Formalisms

Failure Rate λ follows normally the so-called “bath tube curve”



10

Failure Rate λ are often published in Date Books
A few Examples

- *Offshore Reliability Data*; OREDA Handbook; 2nd Edition; distributed by Det Norska Veritas Industri Norge AS; DNV Technica 1992 ISBN 82 515 0188 1
- *Handbook of Reliability Data for Electronic Components*; RDF 93 English Issue 1993; Copyright France Telecom – CNET 1993
- *Reliability Data of Components in Nordic Nuclear Power Plants*; T-book 3rd Edition; Vattenfall AB; ISBN 91-7186-294-3
- *EUREDATA*; Published by Joint Research Centre (JRC) Ispra, It
- Links for Data Informations see at ESRA Homepage

For non-repaired items:

If observed failure data are available for n non-repaired items with constant failure rate, then the estimated value of λ is given by

$$\lambda = n / \sum_{i=1}^{n} TTF_i$$

where TTF_i is time to failure of item i

Example:
For 10 non-repaired items with a constant failure rate, the observed total operating time to failures of all the items is 2 years. Hence

λ = 10/2 = 5 failures per year

Module 1:
A few Definitions and Formalisms

R&S Training Course
CERN, February 2002

For non-repaired items:

$MTTF = \int_0^\infty R(t)dt$ ………Mean Time To Failure

When time to failure is exponentially distributed,

$MTTF = 1 / \lambda$

Example:
For a non-repaired items with a constant failure rate of two failures per four years of operating time,

MTTF = 1 / 2 / 4 = 2 years = 17.520 h

13

Module 1:
A few Definitions and Formalisms

R&S Training Course
CERN, February 2002

For repaired items with zero time to restoration the reliability function is given

$R(t_1,t_2) = R(t_2) + \int_0^{t1} R(t_2 - t) \cdot z(t)dt$

where
$R(t_2)$, represents the probability of survival to time t_2, and
the second term represents the probability of failing at time $t(t< t_1)$ and, after immediately restoration, surviving to time t_2

z(t) is the instantaneous failure intensity (renewal density) of the item, i.e. z(t)dt is approximately the (unconditional) probability that a failure of the item occurs during $(t, t + \Delta t)$

Example:
For a repaired items with a constant failure rate of one failures per operating year and a required time of operation without failure of six months, the reliability is given by
R(t, t + 6) = exp (-1 x 6/12) = 0,6065

14

Module 1:
A few Definitions and Formalisms

R&S Training Course
CERN, February 2002

For repaired items with zero time to restoration the Mean Time To Failure is given

$$\hat{MTTF} = \int_0^{\infty} R(t)dt$$

When observed operating time to failures of n items are available, then an estimate of MTTF is given by

$$\hat{MTTF} = \text{total operating time} / k_F$$

Example:

For a repaired items with a constant failure rate of 0,5 failures per year

MTTF = 1/0,5/1 = 2 years = 17.520 h

15

Module 1:
A few Definitions and Formalisms

R&S Training Course
CERN, February 2002

Consider:

If a repaired item with zero time to restoration operates continuously, and if the times to failure are exponentially distributed three often use terms are equal

MTTF = MTBF = MUT = $1/\lambda$

MTTF Mean Time To Failure
MTBF Mean Time between Failure
MUT Mean Uptime

16

Repaired items with non-zero time to restoration

The reliability of a repaired item with non-zero time to restoration for the time interval(t_1, t_2) may be written as

$$R(t_1, t_2) = R(t_2) + \int_{0}^{t1} R(t_2 - t)\nu(t)dt$$

where the first term $R(t_2)$ represents the probability of survival to time t_2, and the second term represents the probability of restoration (after a failure) at time $t(t < t_1)$, and surviving to time t_2

$\nu(t)$ is the instantaneous restoration intensity of the item

When the times to failure are exponentially distributed, then

$R(t_1, t_2) = A(t_1)\exp(-\lambda \cdot (t_2 - t_1))$

where $A(t_1)$ is the instantaneous availability at time t_1, and

$\lim_{t \to \infty} R(t, t + x) = [MTTF / (MTTF + MTTR)] \exp(-\lambda t)$

Module 1:
A few Definitions and Formalisms
R&S Training Course
CERN, February 2002

Repaired items with non-zero time to restoration

When times to failure and times to restoration are exponentially distributed, then, using either Markov techniques or the Laplace transformation, the following expression is obtained:

$$R(t_1, t_2) = (\mu_R/(\lambda + \mu_R) + \lambda/(\lambda + \mu_R)\exp[-(\lambda + \mu_R)\, t_1]\exp[-\lambda \cdot (t_1 - t_2)]$$

and

$$\lim_{t \to \infty} R(t, t + x) = \mu_R /(\lambda + \mu_R) \exp(-\lambda \mathbf{x})$$

Example:

For a item with λ = 2 failures per operating year and a restoration rate of μ_R = 10 restorations per (restoration) year, and x = 1/4

$$\lim_{t \to \infty} R(t, t + 1/4) = 10/12 \exp(-2 \text{ x } 1/4) = 0{,}505$$

Repaired items with non-zero time to restoration

We can define a asymptotic mean availability $\bar{A}$ of an item

$$\bar{A} = \lim_{t2 \to \infty} \bar{A}(t_1, t_2) = A = MUT / (MUT + MTTR)$$

where
MTTR… Mean Time to Repair

Example:
For a continuously operating item with a failure rate of λ = 2 failures per operating year and a restoration rate of μ_R = 10 restorations per year
then

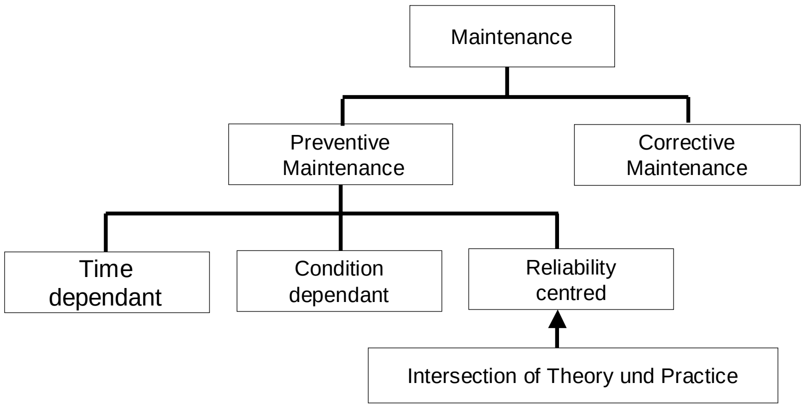
$\bar{A}$ = (0, ¼) = 10/12 + 2/144 {[(exp(-12 x 0) – exp(-12 x ¼)] / ¼ - 0} = 0,886
= (0, 1) = 0,833

Additional Formulas see e.g. in the following Textbooks
(random sample of useful books)

- Birolini, A., *Quality and Reliability of Technical Systems*; Springer 1997 2nd Edition; ISBN 3-540-63310-3
- Hoyland A., & Rausand, M., *System Reliability Theory*; John Wiley & Sons; 1994; ISBN 0-471-59397-4
- Modarres, M., *Reliability and Risk Analysis*; Marcel Dekker, Inc. NY; 1993, ISBN 0-8247-8958-X
- Schrüfer, E., *Zuverlässigkeit von Meß- und Automatisierungseinrich-tungen*; Hanser Verlag, 1984, ISBN 3-446-14190-1
- Knezevic, J., *Systems Maintainability*, Chapman & Hall, 1997, ISBN 0 412 80270 8
- Lipschutz, S., Probability, Schaums Outline Series, McGraw-Hill Book Company, 1965, ISBN 07-037982-3
- IEC 61703, Ed 1: *Mathematical Expressions for Reliability, Availability, Maintainability and Maintenance Support Terms*, 1999 http://www.dke.de

Module 1:
A few Definitions and Formalisms

Types of Maintenance



Module 1:
A few Definitions and Formalisms

R&S Training Course
CERN, February 2002

Maintainability Measures

Probability of Task Completion:

$PTC_{\mathbf{DMT}} = P(DMT \leq T_{\mathbf{st}}) = \int_0^{Tst} m(t)dt$
$T_{\mathbf{st}}$ ….stated time for task completion
m(t)…probability density function of DMT

Mean Duration of Maintenance Task:

$MDMT = E(DMT) = \int_0^{\infty} t \times m(t)dt$
E(DMT)… expectation of the random variable DMT

Module 1: A few Definitions and Formalisms

Maintenance and the Exponential Distribution

$m(t) = (1 / A_m) \cdot \exp - (t / A_m)$, $t > 0$

In case of exponential probability distribution:

$m(t) = P(DMT \leq t) = 1 - \exp - (t / A_m)$

DMT….Duration of Maintenance Task

A_m…….Scale parameter of the exp. distribution = MDMT

Example:

On average it takes 10 days to restore a specific machine; find the chance that less than 5 days will be enough to successfully complete the restoration:

Solution:

$m(t) = (1/10) \cdot \exp - (t / 10)$

and $P(DMT) \leq 5 = M(5) = 1 - \exp - 5/10 = 1 - 0{,}61 = 0{,}39$

Module 1: From Components to Systems

We have to recall some Basic Laws of Probability

A and B are mutually exclusive events than the probability that either of them occurs in a single trial is the sum of their probability

$Pr\{A + B\} = Pr\{A\} + Pr\{B\}$

If two events A and B are general, the probability that at least one of them occurs is:

$Pr\{A + B\} = Pr\{A\} + Pr\{B\} - Pr\{AB\}$

Two events, A & B, are statistically independent if and only if

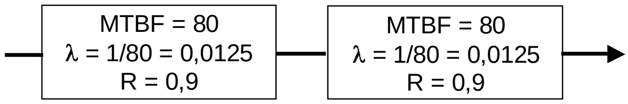
$Pr\{AB\} = Pr\{A\} \cdot Pr\{B\}$

Bayes Theorem

$Pr\{A_i | B\} = PR\{A_i\} \cdot Pr\{B | A_i\} / [\Sigma_i Pr\{B | A_i\} \cdot Pr\{A_i\}]$

More see in e. g. Schaum's Outline Series [Seymour Lipschutz]:
"Theory and Problems of Probability", McGRAW-HILL Book Company

Module 1:
From Components to Systems



$R_S = R_i^{\,n}$

Serial System

We know

$R(t) = e^{-\lambda \cdot t} = 1 – Q(t)$

$Q(t) = 1 – R(t)$ $\quad Q_{av} \sim \lambda \,.\, t / 2$

$\lambda = 1 / MTBF \ [h^{-1}]$

MTBF = Operational Time / Number of Stops

MTTR = Sum of Repair Time / Number of Repairs

For the System we yield:

$\lambda_S = \Sigma\, \lambda = 0{,}0125 + 0{,}0125 = 0{,}025$ 1/h

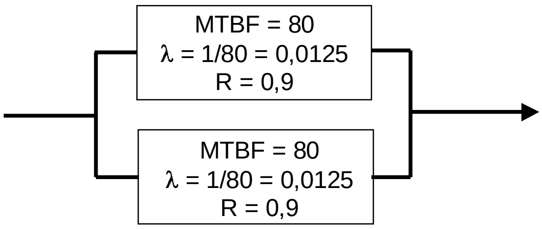
$MTBF_S = 1/(1/MTBF + 1/MTBF) = 1/(1/80 + 1/80) = 40$ h

$R_S = R \times R = 0{,}9 \times 0{,}9 = 0{,}81$

$Q_S = Q + Q – (Q \times Q) = 0{,}1 + 0{,}1 – 0{,}01 = 0{,}19 = 1 - 0{,}81$

Module 1:
From Components to Systems

R&S Training Course
CERN, February 2002



$R_S = 1 - (1 - R_i)^n$

Parallel System

We know

$R(t) = e^{-\lambda \cdot t} = 1 – Q(t)$

$Q(t) = 1 – R(t)$ $\quad Q_{av} \sim \lambda \,.\, t / 2$

$\lambda = 1 / MTBF \ [h^{-1}]$

MTBF = Operational Time / Number of Stops

MTTR = Sum of Repair Time / Number of Repairs

For the System we yield

$\lambda_S = 2\, \lambda / 3 = 0{,}0083$ 1/h

$MTBF_S = 80 + 80 – 1/(1/80 + 1/80) = 120$ h

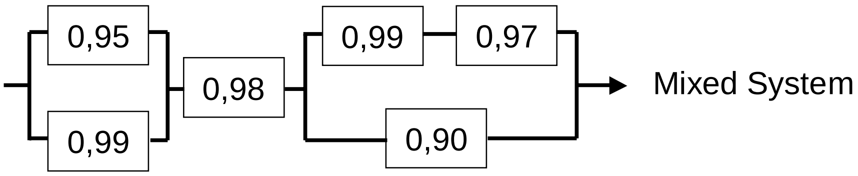
$R_S = 1 - [(1 - R) \times (1 - R)] = 1 – (1 - 0{,}9) \times (1 – 0{,}9) = 0{,}99$

$R_S = R + R – R \times R = 0{,}9 + 0{,}9 – 0{,}9 \times 0{,}9 = 0{,}99$

$Q_S = Q \times Q = 0{,}1 \times 0{,}1 = 0{,}01$

Module 1: From Components to Systems

R&S Training Course
CERN, February 2002



For the System we yield

R_S = 1– [(1– 0,95)(1– 0,99)] x 0,98 x {1– [(1– 0,99) x 0,97 x (1- 0,90)]}

= 0,9995 x 0.98 x 0,99603

R_S = 0,97562 ~ 0,97

The Unreliability

Q_S = 1 – R = 0,02438 ~ 0,03

27

Module 1: From Components to Systems

R&S Training Course
CERN, February 2002

Nowadays we calculate Reliability Characteristics by the means of commercial PC programs like:

- Cafta (USA)
- Care (Israel)
- Item Software (UK)
- Isograph (UK)
- Relex (USA)
- Risk Spectrum (S)
- Saphire (USA)

For further information look for Software presentations at ESREL Conference Sites, e.g. ESREL99; ESREL2001, ESREL2002

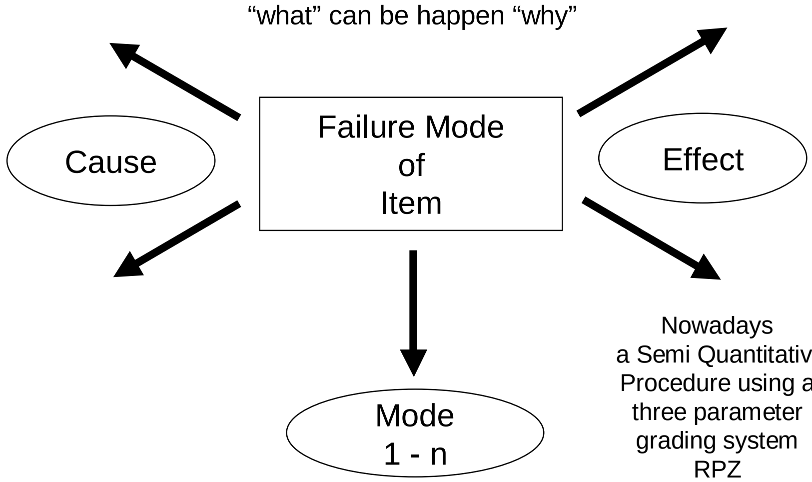
28

Module 1:
Important Methods

R&S Training Course

CERN, February 2002

FMEA Principle:
it represents a qualitative structure
“what” can be happen “why”



Nowadays
a Semi Quantitative
Procedure using a
three parameter
grading system
RPZ

29

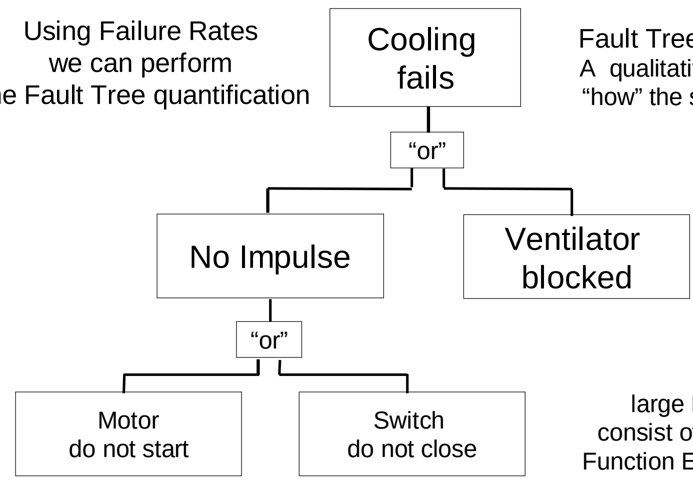
Module 1:
Important Methods

R&S Training Course

CERN, February 2002

Using Failure Rates
we can perform
the Fault Tree quantification

Fault Tree Principle:
A qualitative structure
“how” the system fails



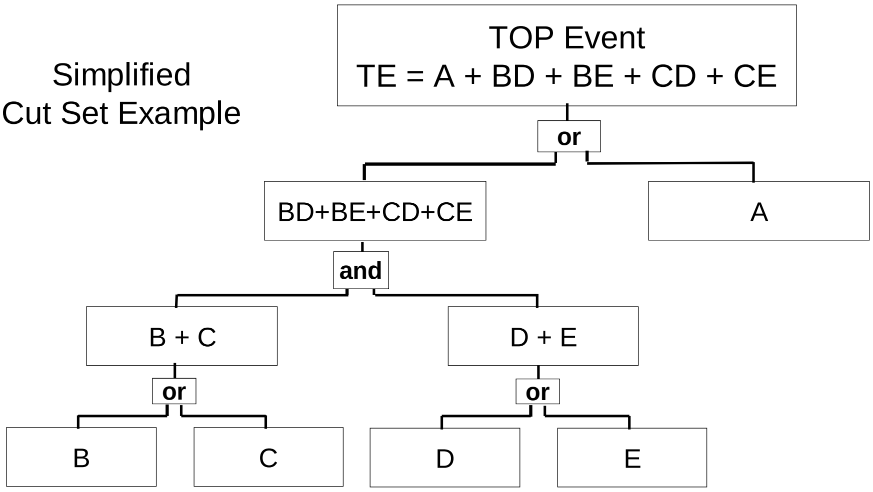
large FTs
consist of 5.000
Function Elements

30

Module 1:
Important Methods

R&S Training Course
CERN, February 2002

Simplified
Cut Set Example



IF A, B, C, D, E = O,1 than TE = 0,045

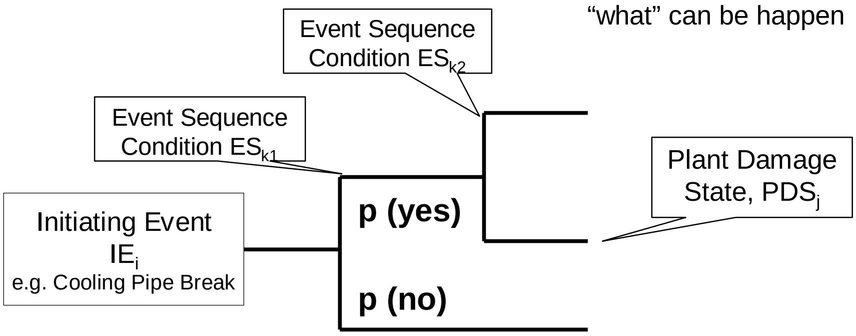
31

Module 1:
Important Methods

R&S Training Course
CERN, February 2002

Using Probabilities
we can perform the
Event Tree Quantification

Event Tree Principle:
it represents a
qualitative structure
“what” can be happen

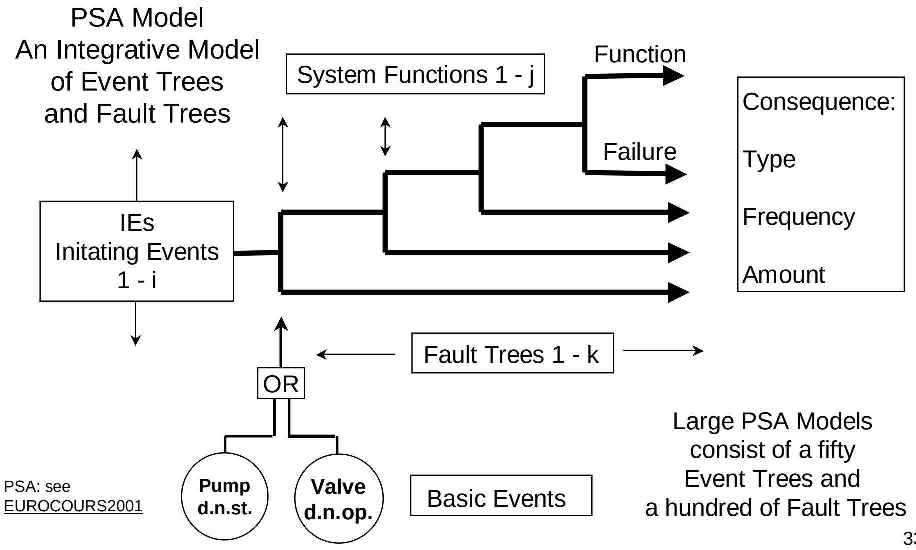


Large Event Trees
consist of dozen‘s
of branches

32

Module 1:
Important Methods

R&S Training Course
CERN, February 2002



33

Module 1:
Important Methods

R&S Training Course
CERN, February 2002

Markov Modelling / Chains

Three Types:
- Homogeneous Continuous Time Markov Chain
- Non-Homogeneous Continuous Time Markov Chain
- Semi-Markov Models

Pros
- very flexible capability
- good for repair
- good for standby spares
- good for sequence dependencies
- Good for different type of fault coverage, error handling and recovery

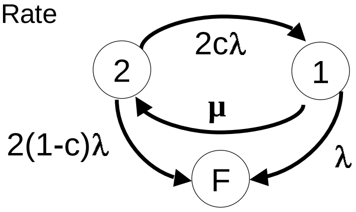
Cons
- can require large number of states
- modelling is relative complex model often different from physical or logical organisation of the system

34

Markov Modelling / Chains

Simple Example

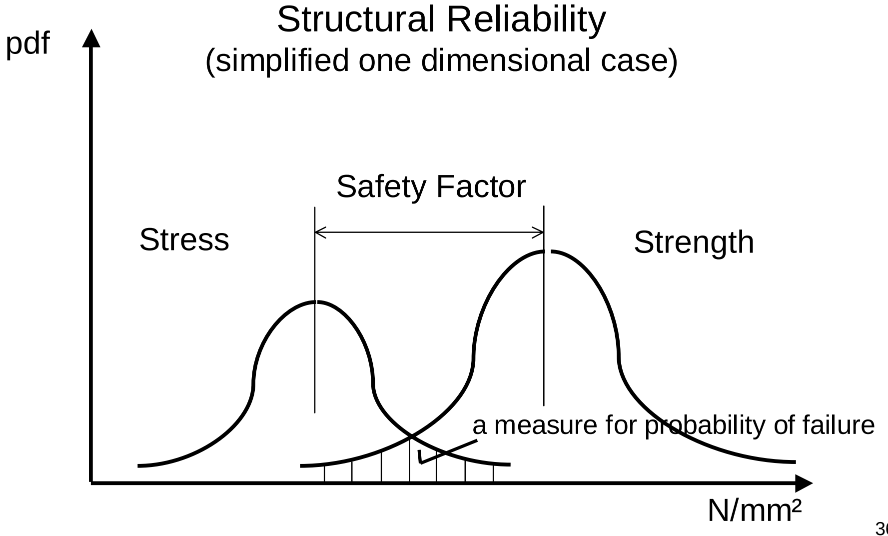
- Control System
- Two processors; 1 active, 1 hot backup
- Fault coverage may be imperfect
- c = pr {fault detected and recovery is successful given processor fault occurs}
- 1 – c = pr {fault is not detected or recovery is unsuccessful given processor fault occurs}
- λ = Failure Rate
- **μ** = Repair Rate



Module 1:
Important Methods

R&S Training Course
CERN, February 2002

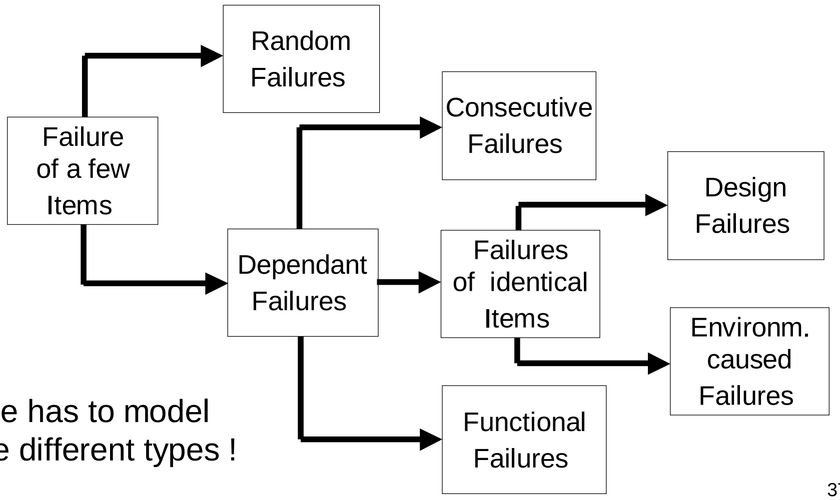
Structural Reliability
(simplified one dimensional case)



Module 1:
Common Cause Failures

R&S Training Course
CERN, February 2002

Type of Failures of Items



One has to model these different types !

37

Module 1:
Common Cause Failures

R&S Training Course
CERN, February 2002

The Boolean representation of a three component system considering Common Cause Failures (CCF) shows as following:

$A_T = A_i + C_{AB} + C_{AC} + C_{ABC}$

A_T….total failure of component A

A_i…..failure of component A from independent causes

C_{AB}..failure of component A and B (and not C) from common cause

C_{AC}..equivalent

38

Module 1:
Common Cause Failures

R&S Training Course
CERN, February 2002

The simple single parameter model called β factor model looks like

$$Q_{\mathbf{m}} = \beta \cdot Q_t$$

β= e.g. 0,1 that means in other words
10% of the unavailability of a system would be caused by common cause failures

Some other models are shown in the next copy

39

Module 1:
Common Cause Failures

R&S Training Course
CERN, February 2002

Estimation Approach			Model	Model Parameters	General Formula for Multiple Component Failure Probability
Nonshock Models	Direct		Basic Parameter	$Q_1, Q_2, \ldots, Q_m$	$Q_k = Q_k$ k=1, 2, …, m
Nonshock Models	Indirect	Single Parameter	Beta Factor	Q_t, β	$Q_k = \begin{cases} (1-\beta)Q_t & k=1 \\ 0 & 1<k<m \\ \beta Q_t & k=m \end{cases}$
Nonshock Models	Indirect	Multiparameter	Multiple Greek Letters	$Q_t, \beta, \gamma, \delta, \ldots$ m - 1 parameters	$Q_k = \frac{1}{\binom{m-1}{k-2}}\left(\prod_{i=1}^{k}\rho_i\right)(1-\rho_{k+1})Q_t$ $\rho_1 = 1, \rho_2 = \beta, \rho_3 = \gamma, \ldots, \rho_{m+1} = 0$
Nonshock Models	Indirect	Multiparameter	Alpha Factor	$Q_t, \alpha_1, \alpha_2, \ldots \alpha_m$	$Q_k = \frac{k}{\binom{m-1}{k-1}}\frac{\alpha_k}{\alpha_t}Q_t$ k = 1, …, m $\alpha_t = \sum_{k=1}^{m} k\alpha_k$
Shock Models			Binomial Failure Rate	Q_I, μ, ρ, w	$Q_k = \begin{cases} \mu\rho^k(1-\rho)^{m-k} & k \neq m \\ \mu\rho^m + w & k = m \end{cases}$

Table 3.3 Summary Description of Parametric Common Cause Failure Models

Module 1:
Human Factor Issues

R&S Training Course
CERN, February 2002

Human Factor Issues are massive involved in the R&S Technology

- Human Operator Reliability in control rooms
- Human Reliability in maintenance work
- Human Reliability in abnormal, accidental and emergency conditions
- Man – Machine Effectiveness
- Human Operators in control loop systems
- Ergonomics for control, supervision and maintenance of systems

41

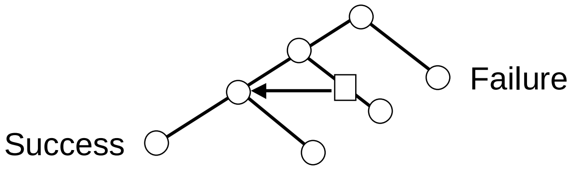
Module 1:
Human Factor Issues

R&S Training Course
CERN, February 2002

HR Models of the first generation

- THERP (Techniques for Human Error Program)
- HCR (Human Cognitive Reliability Model)
- PHRA (Probabilistic Human Reliability Analysis)
- SLIM (Success Likelihood Index Method)

Within THERP the so called HRA Action Tree represents the procedure used for estimating probabilities



$P_{\mathbf{tot}}$ =
A + (a×B)
+ (a×b×C×D)
+ (a×b×C×d×E)
+(a×b×c×E)

42

Module 1:
Human Factor Issues

R&S Training Course
CERN, February 2002

HR Models of the second generation

- ATHENA (NRC)
- CREAM (Halden)
- MERMOS (EDF)
- FACE (VTT)

and many others. These models are more cognitive oriented as the first generation models

The challenge nowadays is the estimation of HEPs for “Errors of Commission”

For “Errors of Omission” a soundly based tool box and validated data are available

43

Module 1:
Software Issues

R&S Training Course
CERN, February 2002

Why Software Reliability Prediction (SRP) is needed?

- Amount & Importance of software is increasing
- Software accounts for approximately 80 % of switch failures
- Software reliability is not improving fast
- Software is costly to fix
- Motivation, pressure and number of experts for doing SRP is limited

Basic Questions in SRP:

- At what rate do failures occur ?
- What is the impact of these failures ?
- When will faults be corrected ?

44

Important Definition

Failure…. An event in which the execution of a software system produces behaviour which does not meet costumer expectation (functional performance)

Fault……The part of the software system which must be repaired to prevent a failure.

Module 1:
Software Issues

R&S Training Course
CERN, February 2002

If we have an observed data example we can calculate $\lambda(t)$ (failure intensity/rate)

if a Logarithmic Poisson Distribution is suitable:

$\lambda(t) = a / (b \cdot t + 1)$

The parameters to be estimated are a and b

For that we need the likelihood function or

the probability that the observed data occur:

$L(\text{data}) = \Pi_j \Pr\{y_j \text{ failure in period } j\}$

Example:

Period j	System Month t_j	Number of Failures y_j
1	23	55
2	52	62
3	89	47
4	137	52
5	199	56
6	279	42
7	380	47
8	511	49

Example:

Parameter estimates: a = 2,93; b = 0,016

$\lambda(t)$ = 2,93 / (0,016 · t + 1)

Thus:

Estimates of failure intensity at 1.000 system month:

$\lambda(t)$ = 2,93 / (0,016 x 1000 + 1) = 0,17 failures per system month

Estimate the mean cumulative number of failures at 5.000 system month:

2,93 / 0,016) · ln (0,016 · t +1) =

2,93 / 0,016) · ln (0,016 x 5.000 +1) = 805 failures

Today's References [IEC 61508; Belcore Publications plus Handout]

Module 1: Types of Uncertainties

R&S Training Course
CERN, February 2002

Within the process of R&S we have to be aware about - at least - three type of uncertainties

- Parameter uncertainties (aleatory uncertainties)
- Model uncertainties (epistemic uncertainties)
- Degree of completeness

Problems and unresolved issues performing an uncertainty assessment increases as this sequence

But
"some information about uncertainties is better than nothing"

49

Module 1: Some Standards

R&S Training Course
CERN, February 2002

IEC 300	Dependability Management
IEC 605	Equipment Reliability Testing
IEC 706	Guide to the Maintainability of Equipments
IEC 50(191)	Procedure for Failure Mode and Effect Analysis (FMEA)
IEC 1014	Programmes for Reliability Growth
IEC 1025	Fault Tree Analysis (FTA)
IEC 1070	Compliance Test Procedure for Steady State Availability
IEC 1078	Reliability Block Diagrams
IEC 1123	Reliability Testing
IEC 1160	Formal Design Review
IEC 1146	Reliability Growth Models and Estimation Methods
IEC 1165	Application of Markov Methods
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety related systems

Others for Reliability Issues: CENELEC, IEEE, ISO, MIL, ASME, etc.

50

Module 2:
Systems Reliability towards Risk Informed Approach

R&S Training Course
CERN, February 2002

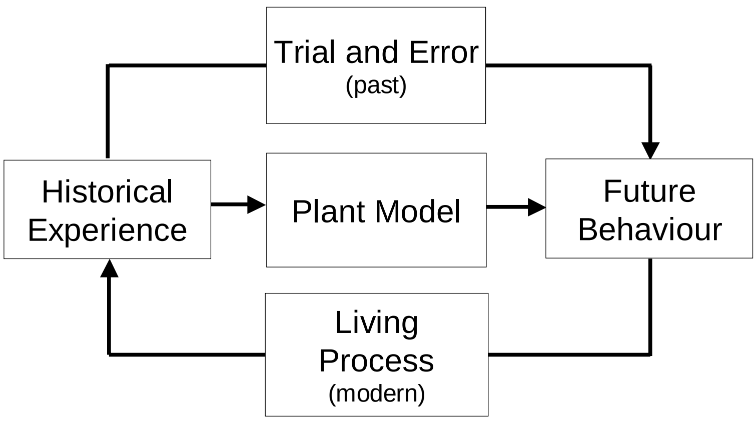
Content:

- Systems Reliability towards Risk Informed Approach
- Anatomy of Risk
- Some Definitions
- Living Models
- Reliability Growth Management
- Risk Monitoring
- How Safe is Safe Enough?

51

Module 2:
Systems Reliability towards Risk Informed Approach

R&S Training Course
CERN, February 2002



52

Deterministic in System Reliability

- Design Process:
  based on pre-defined rules and criterions derived from experiences
- Calculation Process:
  based on determined laws and formulas, calculating point values
- Review Process:
  check of the compliance with rules and standards
- Decision Making Process:
  yes / no - go / no go answers based on rule compliance

Probabilistic in System Reliability

- Design Process:
  based on pre-defined rules and criterions based on experiences
  plus probabilistic goals and targets
- Calculation Process:
  based on determined laws and formulas *plus* uncertainties and random variables, calculating distribution functions
- Review Process:
  check of the compliance with rules and standards
  plus check of the compliance with the goals and targets
- Decision Making Process:
  yes / no - go / no go answers based on risk insights

Module 2:
Systems Reliability towards Risk Informed Approach

R&S Training Course
CERN, February 2002

- In the Deterministic Approach we use formalisms derived from best practice and fitted with single point values as a first guess
- The „Real World“ do not follow that formalisms based on single point values. Practical all values required show spreads (uncertainties) and / or a stochastic behaviour

Therefore exists a challenge for modern analysis techniques and numerical solutions (e.g. Simulations)

I advocate for the extension from deterministic approach towards probabilistic models to consider the stochastic behaviour and the uncertainties

55

Module 2:
Systems Reliability towards Risk Informed Approach

R&S Training Course
CERN, February 2002

Probabilistic towards Risk Informed Approach

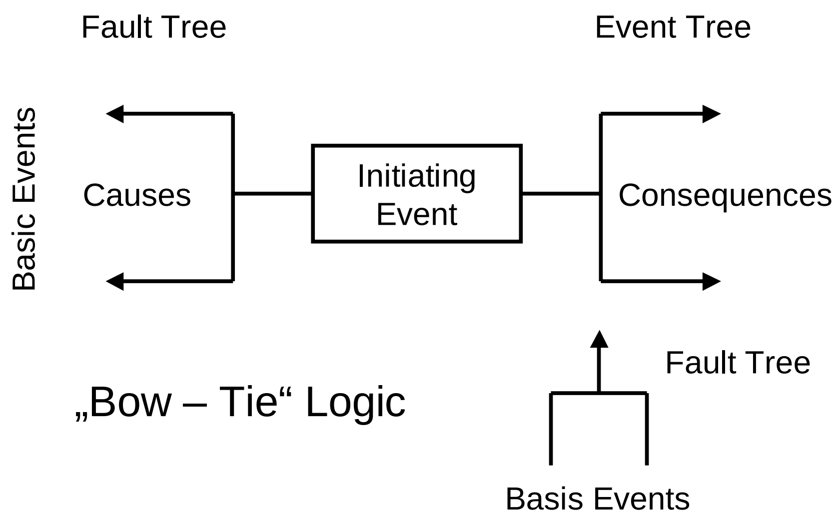
PROS
- it is an extension of the deterministic basis
- it is supported quantitatively by historical experiences
- it models determined, random and uncertain elements
- it is quantitative and therefore appropriate for sensitivity, importance and optimisation studies
- it integrates design, manufacturing and operational aspects
- it integrates various safety issues and allows rankings
- it shows explicit vagueness and uncertainties

CONS
- relatively new, more complex, and not well understood
- larger projects, harder to get financial support
- harder transformation of results into “yes or no” decisions

56

Module 2:
Systems Reliability towards Risk Informed Approach

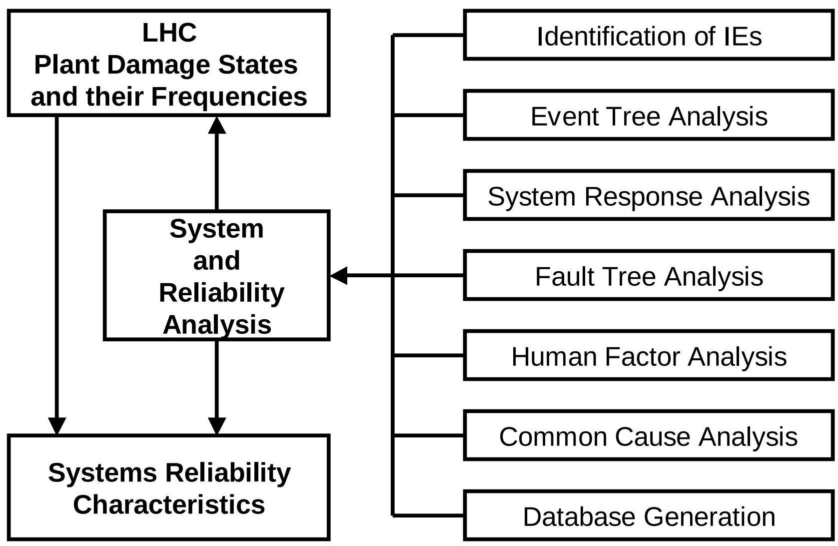
R&S Training Course
CERN, February 2002



57

Module 2:
Systems Reliability towards Risk Informed Approach

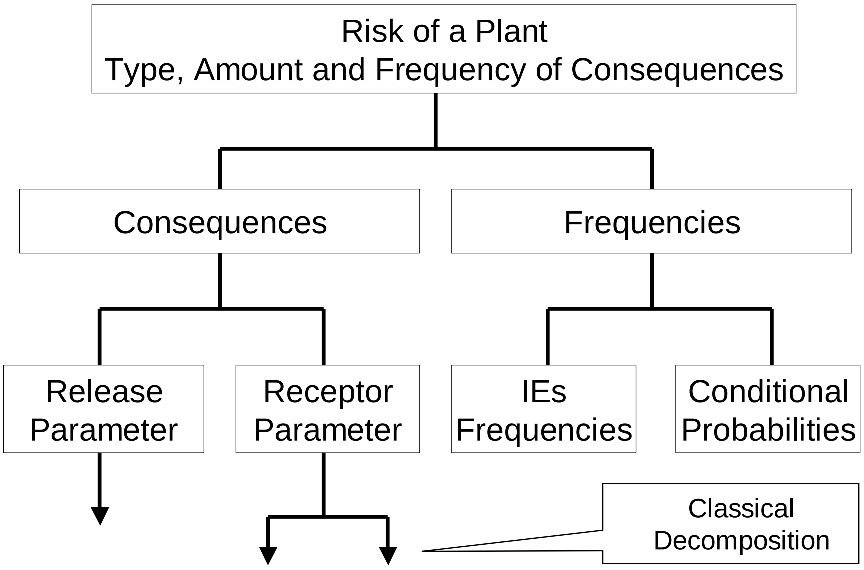
R&S Training Course
CERN, February 2002



58

Module 2:
Anatomy of Risk

R&S Training Course
CERN, February 2002



59

Module 2:
Some Definitions

R&S Training Course
CERN, February 2002

Reliability Insights generated by Importance Measures

- Fussel-Vesely = [PR{top} – Pr{top|A = 0}] / Pr{top}
  Weighted fraction of cut sets that contain the basic event
- Birnbaum = Pr{top|A = 1} – Pr{top|A = 0}
  Maximum increase in risk Associated with component A is failed to component A is perfect
- Risk Achievement worth = Pr{top|A = 1} / Pr{top}
  The factor by which the top probability (or risk) would increase if component A is not available (not installed)
- Risk Reduction Worth = Pr{top} / Pr{top|A = 0}
  The factor by which the risk would be reduced if the component A were made perfect

60

Module 2:
Living Models

R&S Training Course
CERN, February 2002

In R&S we have to learn permanently from the past; that means it is an ongoing, never ending process, we call it Living Process

It is strongly recommended to establish and to store all the models and data with the means of computerised tools

This helps to manage in a more efficient way three important issues

- System Changes
- Personal Changes
- Increasing State of Knowledge

61

Module 2:
Reliability Growth Management

R&S Training Course
CERN, February 2002

Basic Structure

- Management
- Testing
- Failure Reporting, Analysis and Corrective Action System (FRACAS)

During Test we observe

- Type A modes (not fixed)
- Type B modes (fixed)

At beginning of the test operation

$$\lambda_i = \lambda_A + \lambda_B$$

Effectiveness Factor EF

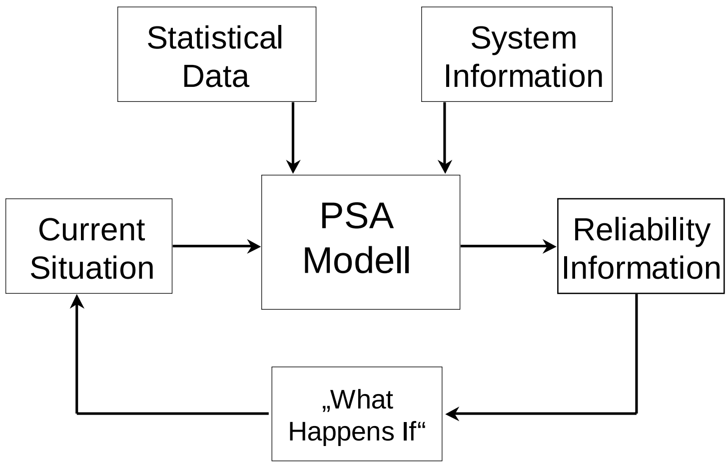
$$\lambda_{inh} = \lambda_A + (1 - EF)\ \lambda_A$$

(more details for growth models see MIL-HDBK-189)

62

Module 2:
Risk Monitoring

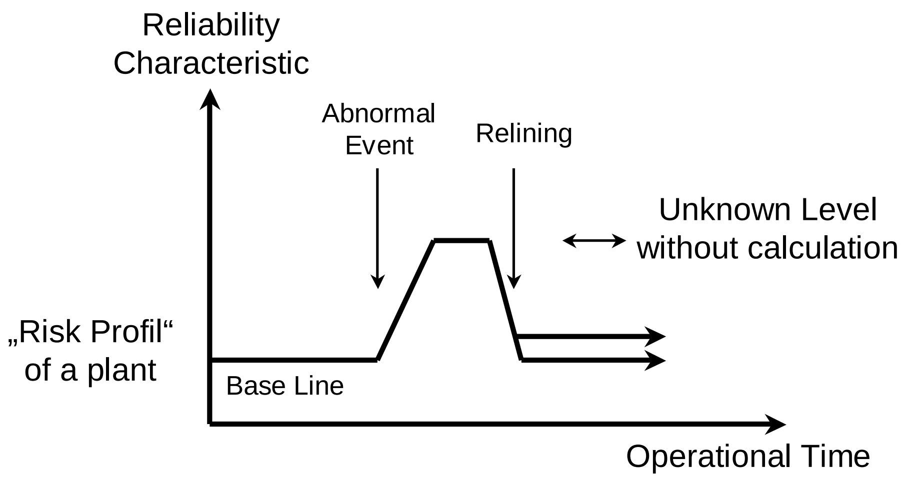
R&S Training Course
CERN, February 2002



63

Module 2:
Risk Monitoring

R&S Training Course
CERN, February 2002

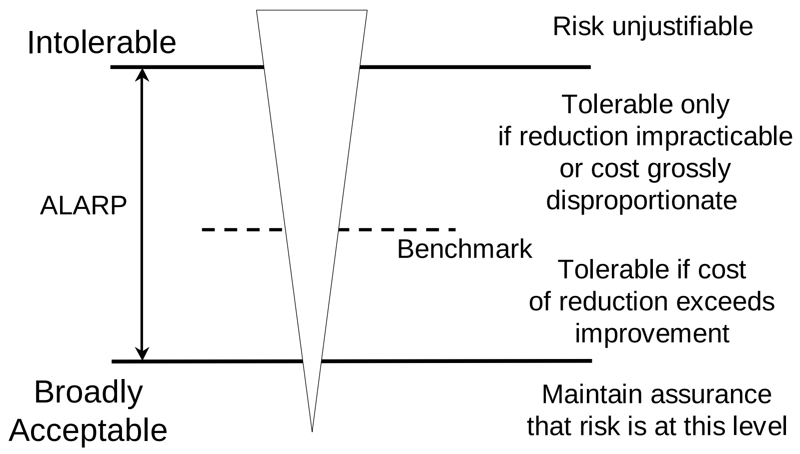


64

Module 2:
How Safe is Safe Enough?

R&S Training Course
CERN, February 2002

Typical way of Thinking



65

Module 2:
How Safe is Safe Enough?

R&S Training Course
CERN, February 2002

List of important qualitative Risk Characteristics related to Tolerability of Risk

Qualitative Characteristics	Direction of Influence
✧ Personal Control	Increase Risk Tolerance
✧ Institutional Control	Depends on Confidence
✧ Voluntariness	Increase Risk Tolerance
✧ Familiarity	Increase Risk Tolerance
✧ Dread	Decrease Risk Tolerance
✧ Inequitable Distribution	Depends on Individual Utility
✧ Artificiality of Risk Source	Amplifies Risk Awareness
✧ Blame	Increase Quest for Social and Political Response

66

Module 2:
How Safe is Safe Enough?

R&S Training Course
CERN, February 2002

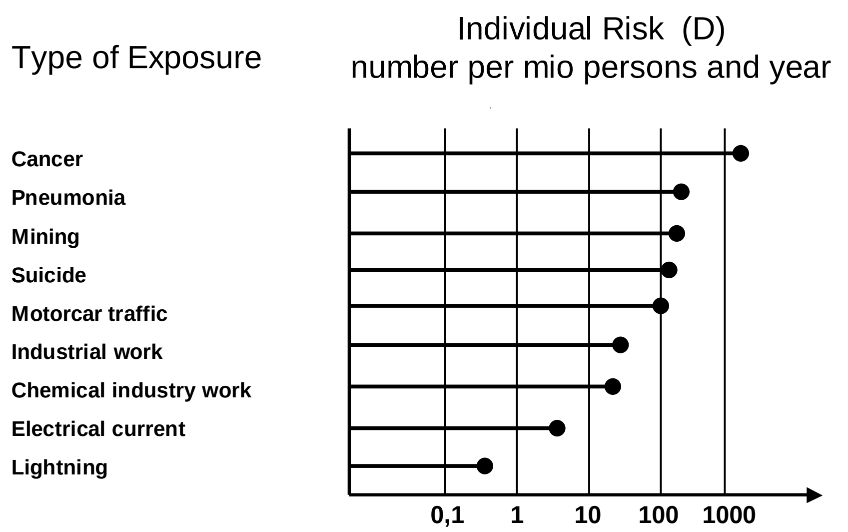
Z	**The Netherlands** (new establishments)	Z	**Canada**	Z	**UK**
1	IR < 10^{-6} Housing, schools, hospitals allowed	i	IR < 10^{-6} Every activity allowed	A	PED < 10^{-6} Insignificant risk area
2	10^{-6} < IR < 10^{-5} Offices, stores, restaurants allowed	ii	10^{-6} < IR < 10^{-5} Commercial activity only	B	10^{-6} < PED < 10^{-5} Risk assessment required
3	IR > 10^{-5} Only by exemption	iii	10^{-5} < IR < 10^{-4} Only adjacent activity	C	PED > 10^{-5} High risk area
		iv	IR > 10^{-4} Forbidden area		

Risk Contours in Land Use Planning (z-Zone) [Okstad; ESREL01]

67

Module 2:
How Safe is Safe Enough?

R&S Training Course
CERN, February 2002



68

Module 3:
The ideal R&M Process for Large Scale Sys

R&S Training Course
CERN, February 2002

Content:

- The ideal Process
- Anatomy of Risk
- From R&S Goals via the Implementation into the System to the Proof of the Compliance
- Constraints and Problems Implementing an ideal Process

69

Module 3:
The ideal Process

R&S Training Course
CERN, February 2002

The ideal R&S process consists (simplified) of

four main elements:

- Establishment of the Risk Policy
- Evaluation and Assessment of the Risk Concerns
- Performing Risk Control
- To do Decision Making

The process is highly intermeshed and iterative!

and multi-disciplinary

70

Module 3:
The ideal Process

- To make this ideal process useful for application we need quantitative Safety Risk / Goal which is tolerable by the society.
- There is trend to use as orientation for this Goal the so called Minimal Endogen Mortality (MEM Value) which is the individual risk for young people to die per year
- This MEM value is given in most of the countries at al level of 2×10^{-4} per person year
- Based on this number some experts advocate for a Global Individual Risk Goal for Hazardous Installations at a level of 10^{-5} per person year.

Module 3:
The ideal Process

List of important qualitative Risk Characteristics related to the Tolerability of Risk

Qualitative Characteristics	Direction of Influence
✲ Personal Control	Increase Risk Tolerance
✲ Institutional Control	Depends on Confidence
✲ Voluntaries	Increase Risk Tolerance
✲ Familiarity	Increase Risk Tolerance
✲ Dread	Decrease Risk Tolerance
✲ Inequitable Distribution	Depends on Individual Utility
✲ Artificiality of Risk Source	Amplifies Risk Awareness
✲ Blame	Increase Quest for Social and Political Response

Module 3:
The ideal Process

R&S Training Course
CERN, February 2002

The ideal process integrates design, construction, and operational parameters from the system, the operator and the environment.

The process is plant wide and comprehensive

As a consequence we need for at least the analysis of hardware, software, paperware and the operator behavior

- The analysis of hardware is reasonably established
- The analysis of operator behavior is reasonably established
- The analysis of paperware is reasonably established
- The analysis of software is not well established

73

Module 3:
Anatomy of Risk

R&S Training Course
CERN, February 2002

- Three main Elements (Anatomy) of Risk:
  - what can go wrong ?
  - how frequent is it ?
  - what are the consequences ?
- Consensus across Technologies
  - these elements describe in a most complete form the “real world”
  - the larger the consequences the smaller the frequencies should be
- Unresolved issue across Technologies
  - how safe is safe enough - tolerability of risk

74

Module 3:

From Goals towards Compliance

R&S Training Course

CERN, February 2002

75

Module 3:

From Goals towards Compliance

R&S Training Course

CERN, February 2002

The allocation of local targets derived from a global goal for LSS is analytically not possible. It is multi parameter problem.

Therefore some simplifications of the problem were developed. One of them is the so-called AGREE Allocation [US MIL HDBK-338]. It works primarily for serial systems

$\lambda_j = n_j \cdot [- \log(R\cdot(T))] / (E_j \cdot t_j \cdot N)$ $\quad R(t_j) = 1 - \{1 - [R\cdot(T)]^{nj/N}\} / E_j$

with

$R\cdot(T)$ system reliability requirement

n_j, N number of modules in (unit j, system)

T time that the system is required to operate

t_j time that unit j is required during T

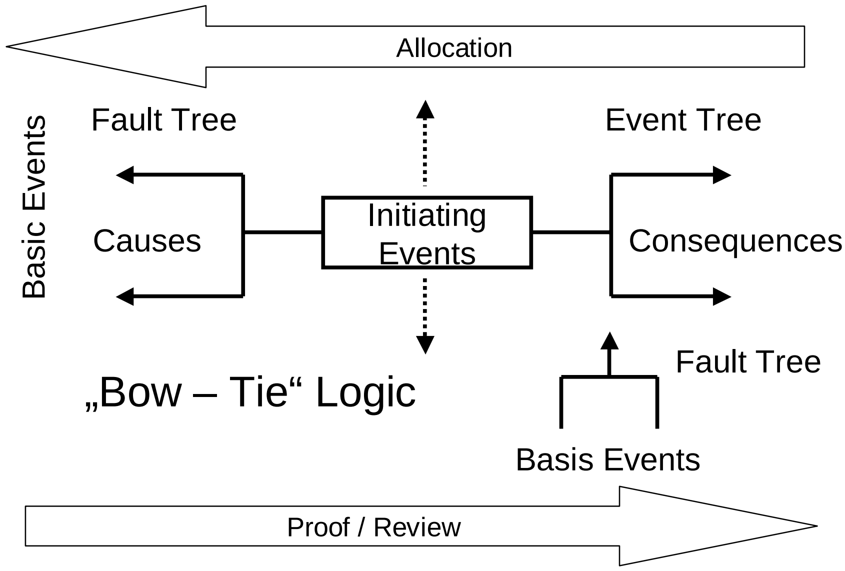
76

Module 3:

From Goals towards Compliance

R&S Training Course

CERN, February 2002



77

Module 3:

From Goals towards Compliance

R&S Training Course

CERN, February 2002

- For the allocation of local targets a linear partition to all the considered initiating events (IEs) should be used as a first approximation

- The allocated targets to the IEs should be subdivided also linear for all the system function modules relevant for that IE

- This liner allocation could be realised by spread sheet programming

- Commercial programs use a Simulation procedure applied to the system topology

78

- For the proof of the global target all the frequencies calculated for similar consequences have to be summed up
- Commercial programs realise fault tree linking based on the identified event trees to do these summation process computerised

Allocation of MTTR [British Standard 6548] for New Designs

$MTTR_{\mathbf{i}} = (MTTR_{\mathbf{s}} \times \Sigma_1^k n_{\mathbf{i}} \bullet \lambda_{\mathbf{i}}) / kn_{\mathbf{i}} \bullet \lambda_{\mathbf{i}}$

where $MTTR_i$ is the target mean active corrective maintenance time (or mean time to repair) for the a system with k consisting items

The Linear Programming Method proposed by Hunt (92, 93) using different constraints produces more realistic MTTRs. The method permits better system modelling, different repair scenarios, trade offs, data updating. etc.

Module 3:

From Goals towards Compliance

R&S Training Course

CERN, February 2002

Allocation of MTTR [British Standard 6548] for New Designs
Example: MTTR based on BS 6584 versus
LP (MTTRs 30min; MTTRmin 5 min; MTTRmax 120 on average)

Item	n	λ (10^{-3})	n x λ	MTTR	MTTR
Unit A	1	0,3430	0,3430	10,93	17,63
B	1	0,2032	0,2032	18,45	29,76
C	1	0,1112	0,1112	33,72	54,38
D	1	0,2956	0,2956	12,69	20,46
E	1	0,0439	0,0439	85,42	123,95
F	1	0,0014	0,0014	2.678,57	120,00
G	1	0,0001	0,0001	37.500,00	120,00
H	1	0,0016	0,0016	2343,75	120,00

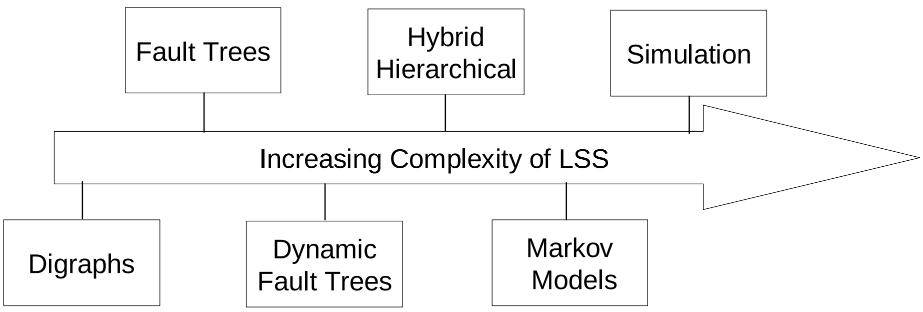
81

Module 3:

P&Cs Performing the ideal Process

R&S Training Course

CERN, February 2002



Trade-off for selecting methods:
Simplicity versus Flexibility

The Place of Various Modelling Techniques for LSSs

82

Module 4:
Some Applications of R&S on LHC

Content:

Module 4:
Where We Are

ACCELERATOR SYSTEMS RELIABILITY ISSUES

Burgazzi Luciano
ENEA, Bologna
Via Martin di Monte Sole, 4
40129 Bologna
Tel. 051 6098556 Fax 051 6098279
Email: burgazzi~bologna.enea.it

ABSTRACT

In the lastyears It has been recognized the needfor investigation into the reliability of accelerator systems. This requirement results ftom new applications of accelerators (e.g. High Power Proton Accelerators for Accelerator Production of Tritium and Accelerator Transmutation of Wastes, International Fusion Materials Irradiation Facility) demanding high availability and reliability.

Atpresent, although a sign~ficant history ofaccelerator operation has been accumulated over the past 50 or so years, there is a deficiency in re/iability estimates of accelerator systems due to thefact that the reliability is not a major topic asfar as most existing acceleratorsfor scient~fic experiments, in thefield ofhigh energy physics, are concerned.

At the moment, despite the fact that standard reliability tools are suitable for accelerator reliability mode/, no formal reliability database for major accelerator components (such as Ion source, RE systems, etc.) 15 available, being evident that the only available data (in terms ofmean time between failures and mean time between repairs) may be inferred by the analysis of existing facilities operational experience information, leading consequently to a large uncertainty in the results (i.e. high EE, iflognormal distributions are assumed).

Therefore an activity aimed at continued data collection, continued statistical inference analysis and development of mode/ing approaches for accelerators is envisaged in the next future.

The present paper intends to highlight the main issues concerning the reliability assessment of accelerator machin es, focusing on the state of the art in this area and suggesting future directions for addressing the issues. In particular the topic is discussed referring mainly to Acce/erator-Driven Reactor System concept, on which the effort ofseveral research organization isfocused aiming at its development.

Continued research and methodology development are necessary to achieve the future accelerator system design with characteristics satisfring the desired requirements, in terms of availability and safety.

Module 4:
Where We Are

R&S Training Course
CERN, February 2002

REFERENCES

[1] F. E. Dunn, DC. Wade "Estimation of thermal fatigue due to beam interruptions for an ALMR-type ATW" OFCD-NEA Workshop on Utilization and Reliability of High Power Proton Accelerators, Aix-en-Provence, France, Nov.22-24, 1999

[2] L.C. Cadwallader, T. Pinna Progress Towards a Component Failure Rate Data Bank for Magnetic Fusion Safety International Topical Meeting on Probabilistic Safety Assessment PSA 99, Washington DC (USA), August 22-26 1999

[3] C. Piaszczyck, M. Remiich, "Reliability Survey of Accelerator Facilities", Maintenance and Reliability Conference Proceedings, Knoxville (USA), May 12-14 1998

[4] C. Piaszczyck, 'Operational Experience at Existing Accelerator Facilities", NEA Workshop **011** Utilization and Reliability of High Power Accelerator, Mito (Japan), October 1998

[5] VI. Martone, "IFMIF Conceptual Design Activity" Final Report, Report ENEA RT-ERG-FUS-96-1 1(1996)

[6] C. Piaszczyck, M. Rennieh "Reliability Analysis of IFMIF" 2nd International Topical Meeting on Nuctear Applications of Aceelerator Technology , ACCAPP '98, Gatlinburg (USA), September 20-23 1998

[7] L. Burgazzi, "Safety Assessment of the IFMIF Facility", doc. ENEA-CT-SBA-00006 (1999)

[81 C. Piaszczyck, M. Eriksson "Reliability Assessment of the LANSCE Accelerator System" 2'd International Topical Meeting on Nuelear Applications of Accelerator Technology , ACCAPP '98, Gatlinburg (USA), September 20-23 1998

[9] L. Burgazzi,"Uncertainty and Sensitivity Analysis on Probabilistic safety Assessment of an Experimental Facility" 5th International Conference on Probabilistic safety assessment and Management" Osaka (Japan) Nov. 27-Dec 1,2000.

85

Module 4:
Where We Are

R&S Training Course
CERN, February 2002

Component [from Burgazzi, ESREL2001]	
Ion Source rf Antenna	6,0 E-3
Ion Source Extractor	1,0 E-5
Ion Source Turbomech Vac Pump	5,0 E-5
LEPT Focussing Magnet	2,0 E-6
LEBT Steering Magnet	2,0 E-6
DTL Quadrupole Magnet	1,0 E-6
DTL Support Structure	2,0 E-7
DTL Drive Loop	5,0 E-5
DTL Cavity Structure	2,0 E-7
High Power rf Tetrode	1,0 E-4
Circulator	1,0 E-6
Rf Transport	1,0 E-6
Directional Coupler	1,0 E-6
Reflectometer	1,0 E-6
Resonance Control	1,0 E-5
Solid State Driver Amplifier	2,0 E-5

86

Module 4:
Where We Are

R&S Training Course
CERN, February 2002

Results of Reliability Studies at LANSCE Accelerator
[from Burgazzi, ESREL2001]

Main System	Subsystem	MDT [h:min]	MTBF [h:min]
805 RF	Klystron Assembly	0:44	11560
	High Voltage System	0:18	960
Magnet Focusing	DC Magnet	0:53	232280
	Magnet	0:50	8445
	Supplies		
Pulse Power	Harmonic Puncher	0:09	44
	Chopper Magnet	0:08	291
	Deflector Magnet	0:10	684
	Kicker Magnet	1:58	557
Water System	Water Pump	0:29	29506
Vacuum System	Ion Pump	0:29	25308

87

Module 4:
Similarities and Differences in R&S

R&S Training Course
CERN, February 2002

It makes a difference analysing for „Reliability“ of LHC or for „Safety“. But many elements and parts of analysis are common

For “R” we look mainly for failures in operational systems
For “S” we look after occurring an initiating event for failures in stand-by (safety) systems

In other words:
R….what is the probability of loss of function of LHC
S….what is the probability of a given damage (consequence) at the LHC

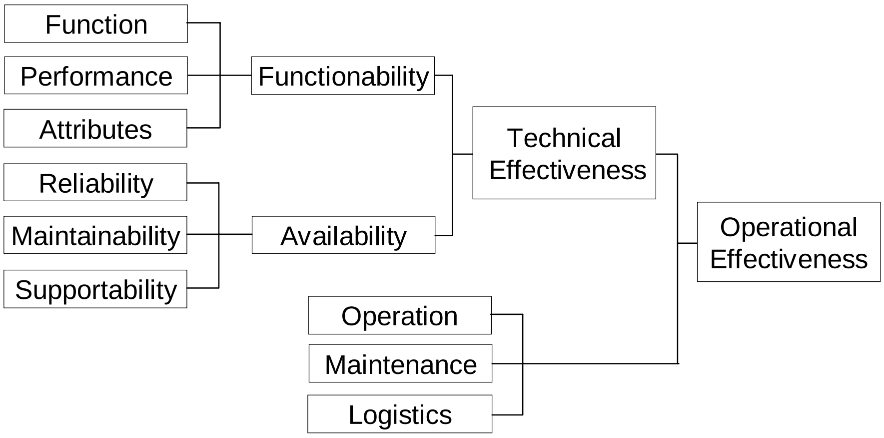
88

Module 4: Similarities and Differences in R&S

R&S Training Course

CERN, February 2002

R for Reliability of LHC is mainly involved in Systems Operational Effectiveness

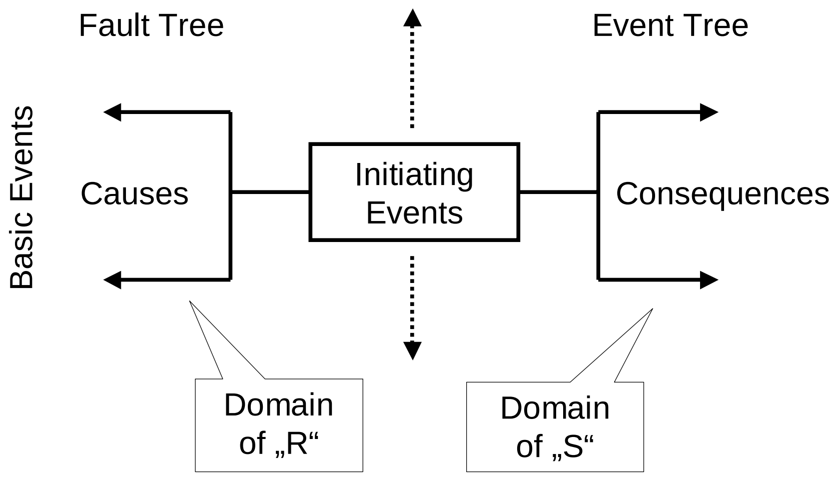


89

Module 4: Similarities and Differences in R&S

R&S Training Course

CERN, February 2002



90

Module 4: Master Logic

R&S Training Course
CERN, February 2002

Analysing R we have to look first which system functions are needed for the function of the entire LHC

The opposite of the function R answers for the malfunction Q (unavailability Q = 1 - R) of the LHC

To answer the question:
“which system functions are needed”
the so-called Master Logic is an appropriate tool and a way of thinking

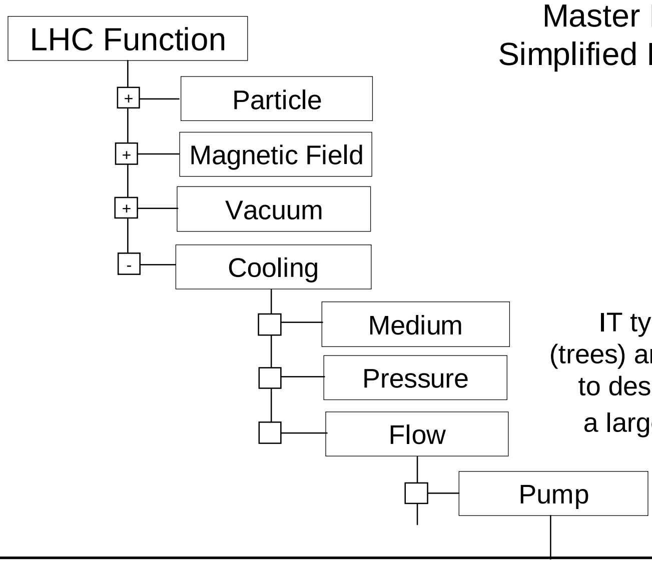
In the next slide a simplified example, but for training we should expand it using an excel sheet

91

Module 4: Master Logic

R&S Training Course
CERN, February 2002

Master Logic
Simplified Principle



IT type of graphics (trees) are very convenient to design and to show a large Master Logic

92

Module 4: Anatomy of Risk

R&S Training Course
CERN, February 2002

Analysing S we have to look first which Type of Risks we have to evaluate. This is strongly dependent from the so-called hazard potential

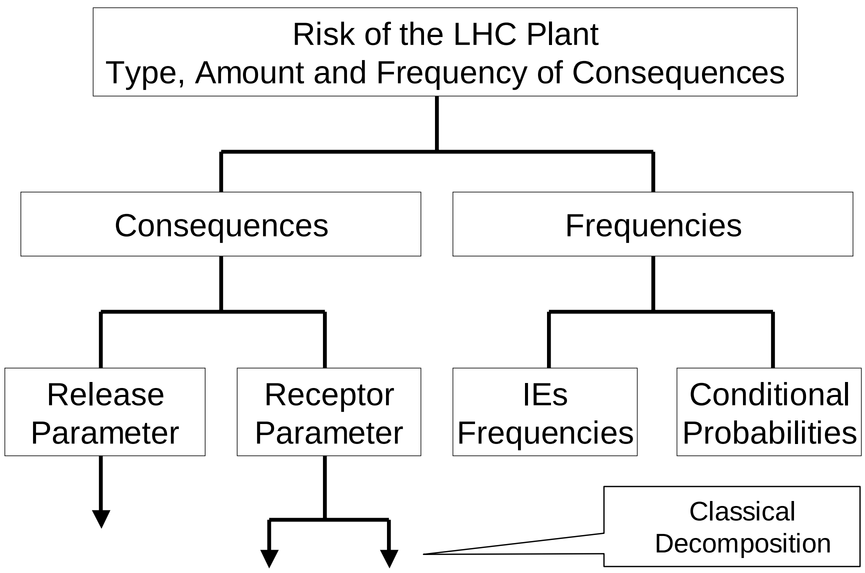
To answer the question:
“which type of risks we have to evaluate”
the so-called Anatomy of Risk is an appropriate tool and a way of thinking

In the next slide a simplified example, but for training we should expand it using an excel sheet

93

Module 4: Anatomy of Risk

R&S Training Course
CERN, February 2002

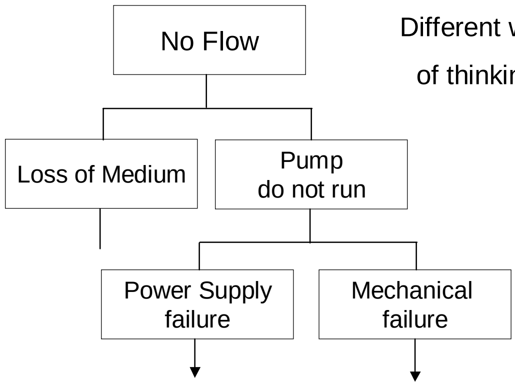


94

R&S Training Course
CERN, February 2002

Module 4:
Decomposition and Aggregation of the System

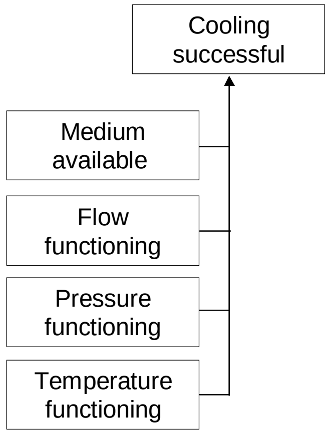
Decomposition
Down to Component Level



Different way

of thinking

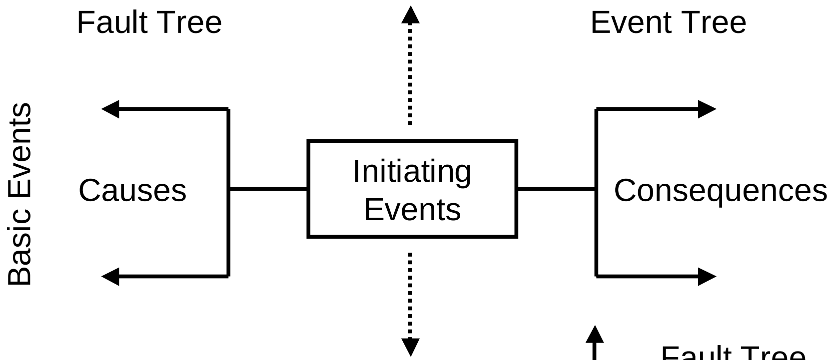
Aggregation
Up to System Function Level

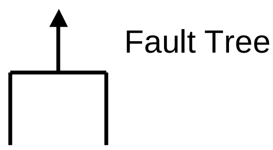


95

R&S Training Course
CERN, February 2002

Module 4:
Cause – Consequence Diagram





„Bow – Tie“ Logic
is appropriate for S

96

Module 4: Identification of IEs

R&S Training Course

CERN, February 2002

Task:

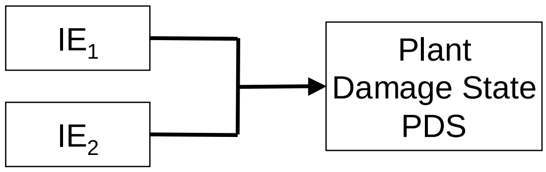
- Identification of Initiating Events (IEs), which can lead at the end of an event sequence to a plant damage state.

Method:

- Master Logic Diagram
- Operational Experience

Analysis Logic:

Master Logic Diagram



97

Module 4: Event Sequence Analysis

R&S Training Course

CERN, February 2002

Task:

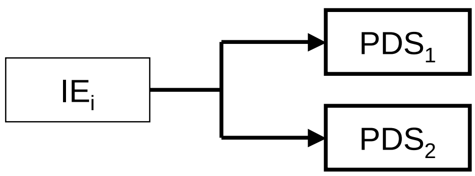
- Identification of Event Scenarios and the related techn/physical parameters which can lead at the end of the event sequences to a plant damage state.

Method:

- Event Tree, System Response Analysis
- Operational Experience

Analysis Logic:

Event Tree Diagram



98

Module 4:
PDS Frequencies

R&S Training Course
CERN, February 2002

Task:

- Evaluation of the plant damage states frequencies at the end of all the different event sequences

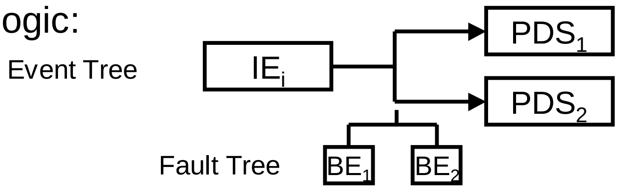
Method:

- Event Sequence Analysis, Fault Tree Analysis
- Operational Experience and Data Generation

Formalism:

f(PDS) = f(IE) . p(IE --> PDS)

Analysis Logic:



99

Module 4:
Source Term Analyse

R&S Training Course
CERN, February 2002

Task:

- Evaluation of type, amount and frequency of possible releases of harmful material and classification into release categories (STGs)

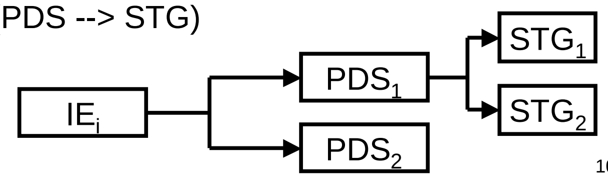
Method:

- Event Sequence Analysis, Fault Tree Analysis
- System Response Analyse
- Operational Experience and Data Generation

Formalism:

f(STG) = f(PDS) . p(PDS --> STG)

Analysis Logic:



100

Module 4:
Consequence Model

R&S Training Course
CERN, February 2002

Task:

- Evaluation of type, amount and frequency of the various possible consequences around a plant

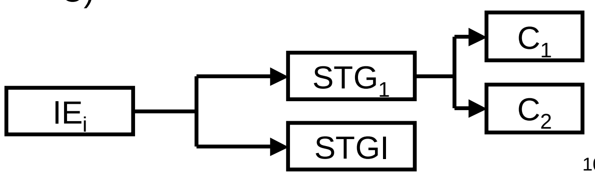
Method:

- Event Sequence Analysis, Fault tree Analysis, Source Term Analysis, Dispersion Modelling
- Operational Experience and Data Generation

Formalism:

f(C) = f(STG) . p(STG --> C)

Analysis Logic:



101

Module 4:
Risk Model

R&S Training Course
CERN, February 2002

Task:

- Evaluation of the Risk Parameters for the involved Persons

Method:

- Dose Response Modelling, Population Modelling
- Data Analysis

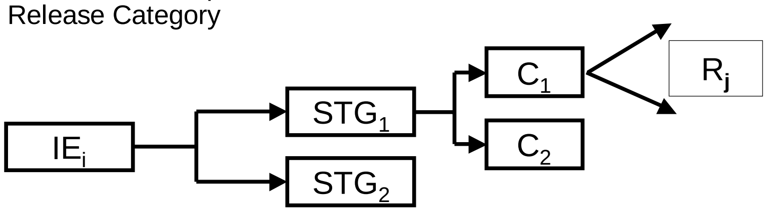
Formalism:

R(C) = f(STG) . C(STG)

R(C)……Vector of the Risk Parameters per Year

f(STG)…Vector of the Frequency of a Source Term

C(STG)..Matrix of Consequence Parameter under the Condition of a Release Category



102

Module 5:
Lessons Learned from Various Technologies

Content:

- Success Stories and Pitfalls
- Constraints in Data and Methods
- Limitations per se
- Technologies such as Aviation, Space, Process, Nuclear, Offshore, Transport

Module 5:
Success Stories and Pitfalls

There is a consensus across technologies that we should know the main elements (Anatomy) of Risk:

- ➤ what can go wrong ?
- ➤ how frequent is it ?
- ➤ what are the consequences ?

and we should consider:

the larger the consequences the smaller the frequencies should be

These elements describe in a most complete form the "real world"

It exist the unresolved issue across technologies

"how safe is safe enough ?" – the tolerability of risk

Module 5: Constraints in Data and Methods

R&S Training Course
CERN, February 2002

- To model the Real World we have the transform the historical experience via methods and data into a prognosis for the future
- The data base is often sparse and limited
- We have to start with generic data, statistically improved by Bayesian technique, if more and more plant specific data will be available
- Methods should be tested by Benchmarks between independent expert teams
- Formal Expert Judgement procedures should be used if the evidence from the past related to the methods and the data is very limited
- Remember: as longer you would search in potential date bases as more reliable date you would identify

105

Module 5: Limitations per se

R&S Training Course
CERN, February 2002

Within the R&S process we have to be aware about
- at least - three type of uncertainties

- Parameter uncertainties (aleatory uncertainties)
- Model uncertainties (epistemic uncertainties)
- Degree of completeness

Problems and unresolved issues performing an uncertainty assessment increases with this sequence

But

“some information about uncertainties is better than nothing”

Remember: in the Deterministic Approach we generate point values only

106

Module 5: Situation in different Technologies

- Process Industry: large differences; from "yes" or "no" to risk based
- Offshore Industry: small differences; primarily risk-based
- Marine Structures: small differences; primarily risk-based
- Aviation: small differences; primarily risk-based
- Civil Engineering: differences; for specific structures risk-based
- Nuclear Industry: differences; tendency towards risk-based
- Transport: differences: tendency towards risk-based
- Motor Car Industry: differences; tendency towards risk-based
- Space Industry: strong tendency towards risk-based

Module 5: Examples from different Technologies

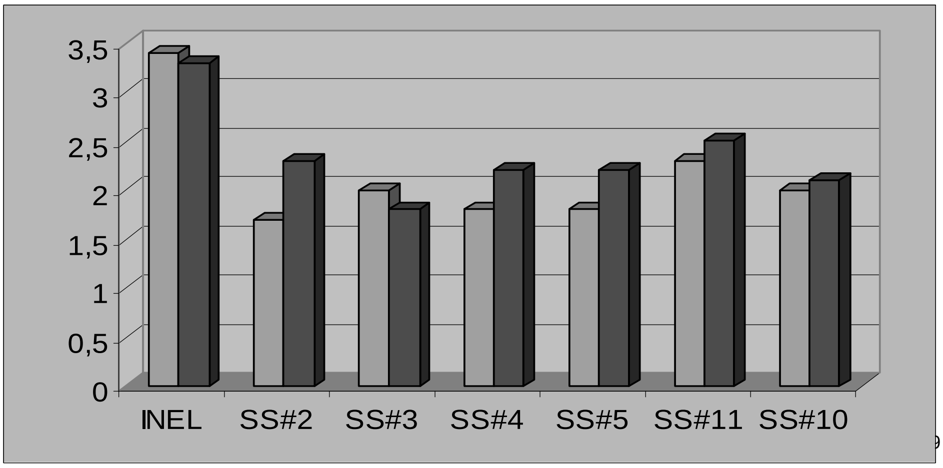
Why Events Occur (in 352 LERs, NPP; USA)

Human Variability	50 [%]
Work Place Ergonomics	25
Procedure not Following	28
Training	10
Task Complexity	5
Procedures	7
Communication	5
Changed Organisation	8
Work Organisation	28
Work schedule	10
Work Environment	8

Module 5:
Examples from different Technologies

R&S Training Course
CERN, February 2002

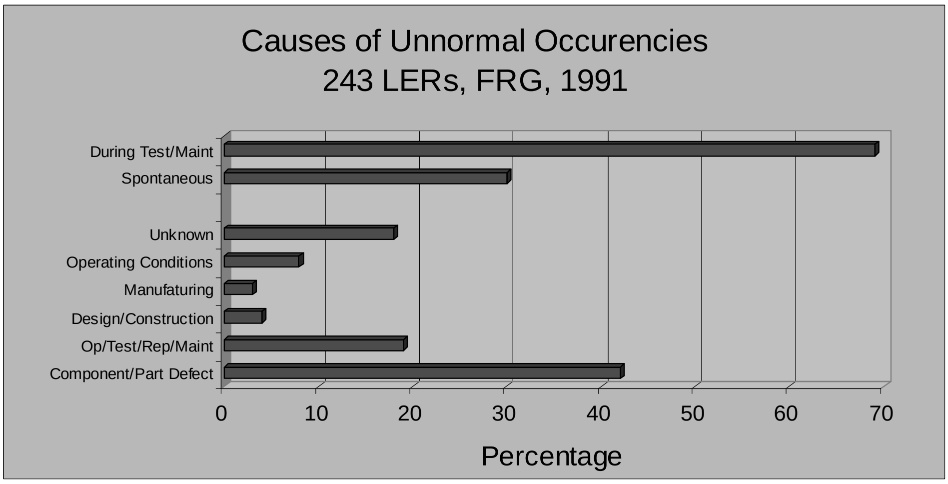
System Model versus Historical Experience (INEL; USA)
Outage Frequency per Year for different Grid Systems



Module 5:
Examples from different Technologies

R&S Training Course
CERN, February 2002

Informations related to the split of different causes of failures and their identification are useful

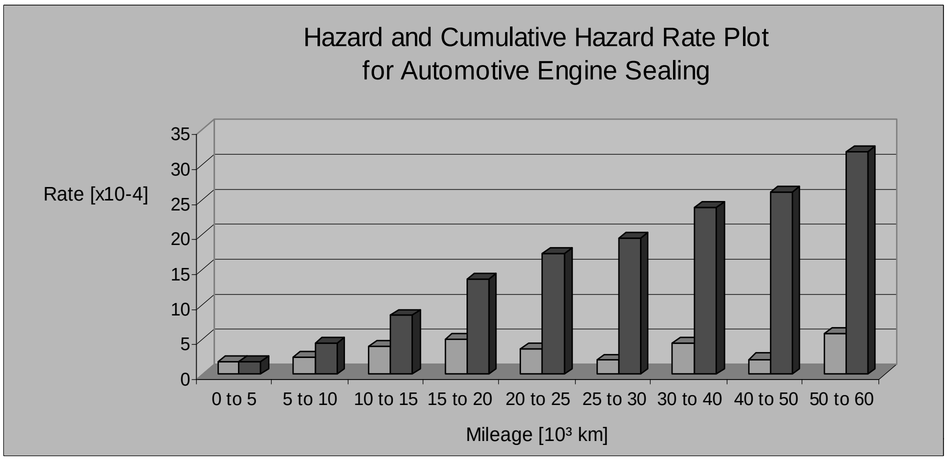


Module 5: Examples from different Technologies

R&S Training Course
CERN, February 2002

Hazard Rate from Test Runs [Campean, ESREL01]

h_j = Number of failures in current mileage band / mileage accumulated by all vehicles in current mileage band



Module 5: Examples from different Technologies

R&S Training Course
CERN, February 2002

The Volume and Importance of Maintenance in the Life Cycle of a System, e. g. Boeing 747; N747PA

[Knezevic: Systems Maintainability, ISBN 0 412 80270 8; 1997]

Been airborne	80.000 hours
Flown	60,000.000 km
Carried	4,000.000 passengers
Made	40.000 take-off and landings
Consumed	1.220.000.000 litres of fuel
Gone through	2.100 tyres
Used	350 break systems
Been fitted with	125 engines
Had the passenger comp. replaced	4 times
Had structural inspections	9.800 X-ray frames of films
Had the metal skin replaced	5 times
Total maintenance tasks during 22 y	806.000 manhours

The Volume and Importance of Maintenance in the Life Cycle of a System, e. g. Civil Aviation

[Knezevic: Systems Maintainability, ISBN 0 412 80270 8; 1997]

Between 1981 and 1985
19 maintenance-related failures claimed 923 lives

Between 1986 and 1990
27 maintenance-related failures claimed 190 lives

Example Civil Aviation

[Knezevic: Systems Maintainability, ISBN 0 412 80270 8; 1997]

Safety demands expressed through the achieved hazard rates (1982 – 1991) for propulsion systems required by CAAM

Hazard	Hazard Rate
High energy non-containment	3,6 x 10^{-8} per engine hour
Uncontrolled fire	0,3 x 10^{-8} per engine hour
Engine separation	0,2 x 10^{-8} per engine hour
Major loss of trust control	5,6 x 10^{-8} per engine hour

If we have good (hard) statistical data then we should use it

- e.g. for traffic accidents normally exist good statistics. Thus, for RIDM we should use these data base [bast Heft M95; Risikoanalyse des GGT für den Zeitraum 87-91 für den Straßengüternahverkehr (GVK) und für den Benzintransport", D]

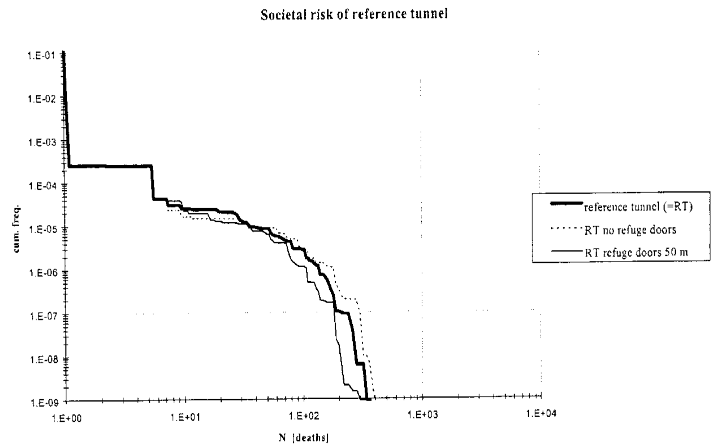
Accidents (GVK)	Number	89
Driving Performance (GVK)	mio.Vehiclekm	416,2
Accident Rate(GVK)	Accidents/ mio.Vehiclekm	0,214
Accident Rate (GVK)	Accidents / mio.Vehiclekm	214 x 10-9
Gasoline Transport		
Accident Rate 0 -100 l	Accidents / mio.Vehiclekm	72,76 x 10-9
Accident Rate 110 – 10.000 l	Accidents / mio.Vehiclekm	109,14 x 10-9
Accident Rate >10.000 l	Accidents / mio.Vehiclekm	32,10 x 10-9

If we have good (hard) statistical data in Handbooks then we should use it (see also [Birolini; Springer 1997, ISBN 3-540-63310-3])

- MIL-HDBK-217F, USA
- CNET RDF93, F
- SN 29500, DIN 40039 (Siemens, D)
- IEC 1709, International
- EUREDA Handbook, JRC Ispra, I
- Bellcore TR-332, International
- RAC, NONOP, NPRD; USA
- NTT Nippon Telephone, Tokyo, JP
- IEC 1709, International
- T-Book (NPP Sweden)
- OREDA Data Book (Offshore Industry)
- ZEDB (NPP Germany)

Module 5: Examples from different Technologies

R&S Training Course
CERN, February 2002



Societal Risk of reference tunnel; RT, RT no ref.doors, RT ref. doors 50m from [D.de.Weger, et al, ESREL2001, Turin]

117

Module 5: Examples from different Technologies

R&S Training Course
CERN, February 2002

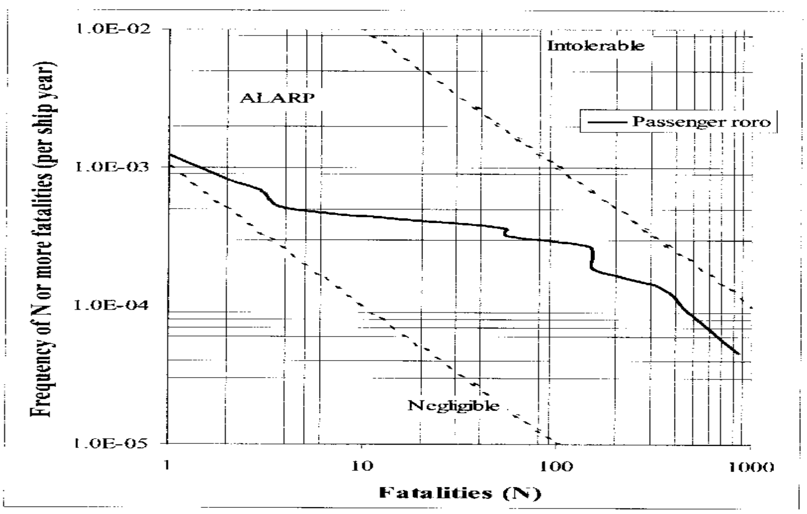


Figure 4: ***FN acceptance criterion and historic risk levels for crew and passengers on passenger Ro/Ro ferries.***

Module 5:
Examples from different Technologies

R&S Training Course
CERN, February 2002

There is a consensus across technologies that we should know the main elements (Anatomy) of Reliability:

- what can go wrong ?
- how frequent is it ?
- what are the consequences ?

and we should consider:

the larger the consequences (e.g. costs) the smaller the frequencies should be

These elements describe in a most complete form the “real world”

It exist the unresolved issue across technologies

“how reliable is reliable enough ?” – what is the most beneficial plant over time?

119

Module 5:
Examples from different Technologies

R&S Training Course
CERN, February 2002

- R&S has a long and successful story in industrial application
- The Deterministic Approach is a good basis for Safety Cases
- Nowadays new need an extension towards the Probabilistic Approach to model the ‘”Real World” in a more realistic manner
- A Risk Informed Decision Making Process (RIDM) should take place for all the safety concerns in the society
- Matured methods, tools and experienced experts, working since years in this field, are available and willing to help for dissemination of this RIDM process into practice
- The RIDM process can be used for all type of facilities

120

In the following Periodicals examples are published from different technologies

- *Reliability Engineering & System Safety* (RESS)
  Elsevier; http://www.elsevier.com/locate/ress
- *IEEE Transactions on Reliability*, published by IEEE Reliability Society ISSN 0018-9528
- *Qualität und Zuverlässigkeit*; published by DGQ, Germany
  Carl Hanser Verlag; http://hanser.de

At the following Conference Series you would get plenty R&S Informations

- ESREL Annual Conference Series
- PSAM Conference Series (every two years)
- RAMS Annual Conference Series
- SRA Annual Conference Series
- ICOSSAR Conference Series (every 4 years)
- OMEA Conference Series
- NASA & ESA Conferences on Risk and Reliability

Plus specific Human Factor and Software Reliability Conferences, e.g. IFAC and ENCRESS

Some Key Words

R&S Training Course
CERN, February 2002

Availability	Verfügbarkeit
Case	Fall
Cause	Ursaache
Consequence	Auswirkung
Event	Ereignis
Event Tree	Ereignisbaum
Example	Beispiel
Failure Mode	Fehlerart
Failure Rate	Ausfallrate
Fault Tree	Fehlerbaum
FMEA	Fehler-Möglichkeits- und Auswirkungsanalyse
Initiating Event	Auslösendes Ereignis
Maintainability	Instandhaltbarkeit
Maintenance	Instadhaltung
Minimal Cut Set	Minimale Schnittmenge
Probability	Wahrscheinlichkeit
Reliability	Zuverlässigkeit
Result	Ergebnis
Risk	Risko
Safety	Sicherheit
Solution	Lösung
Time	Zeit

123

Used Abbreviations

R&S Training Course
CERN, February 2002

A	Availability
ALARP	As Low As Reasonably Achievable
ETA	Event Tree Analysis
ESRA	European Safety And Reliability Association
ESREL	European Safety And Reliability Conference Series
IE	Initiating Event
f	Frequency
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
MTBF	Mean Time Between Failure
MUT	Mean Up Time
p	Probability
PSA	Probabilistic Safety Assessment
Q	Unreliability
QRA	Quantitative Risk Assessment
R	Reliability
RAMS	Reliability, Availability, Maintainability, Safety
t	Time
λ	Failure Rate
μ	Repair Rate

124

That’s All

R&S Training Course
CERN, February 2002

Thank you very much for your attention and the patience to follow all my presented issues

125