International Atomic Energy Agency

P4: Experience in PSA Applications

P. Hlavac
hlavac@relko.sk

Application of Level 1 Probabilistic Safety Assessment

Bangkok, Thailand
5 – 9 September, 2022

Contents

- Living PSA
- Risk monitors
- Optimization of allowed outage times (AOT)
- Risk-Informed In-service Inspection
- Significance Determination Process (SDP)
- Mitigating Systems Performance Index (MSPI)

Living PSA

Living PSA

IAEA definition (IAEA-TECDOC-1101, Framework for a Quality Assurance Programme for PSA, 1999):

“A PSA of the plant, which is updated as necessary to reflect the current design and operational features, and is documented in such a way that each aspect of the model can be directly related to existing plant information, plant documentation or the analysts' assumptions in the absence of such information. The LPSA would be used by designers, utility and regulatory personnel for a variety of purposes according to their needs, such as design verification, assessment of potential changes to the plant design or operation, design of training programmes and assessment of changes to the plant licensing basis“

Living PSA

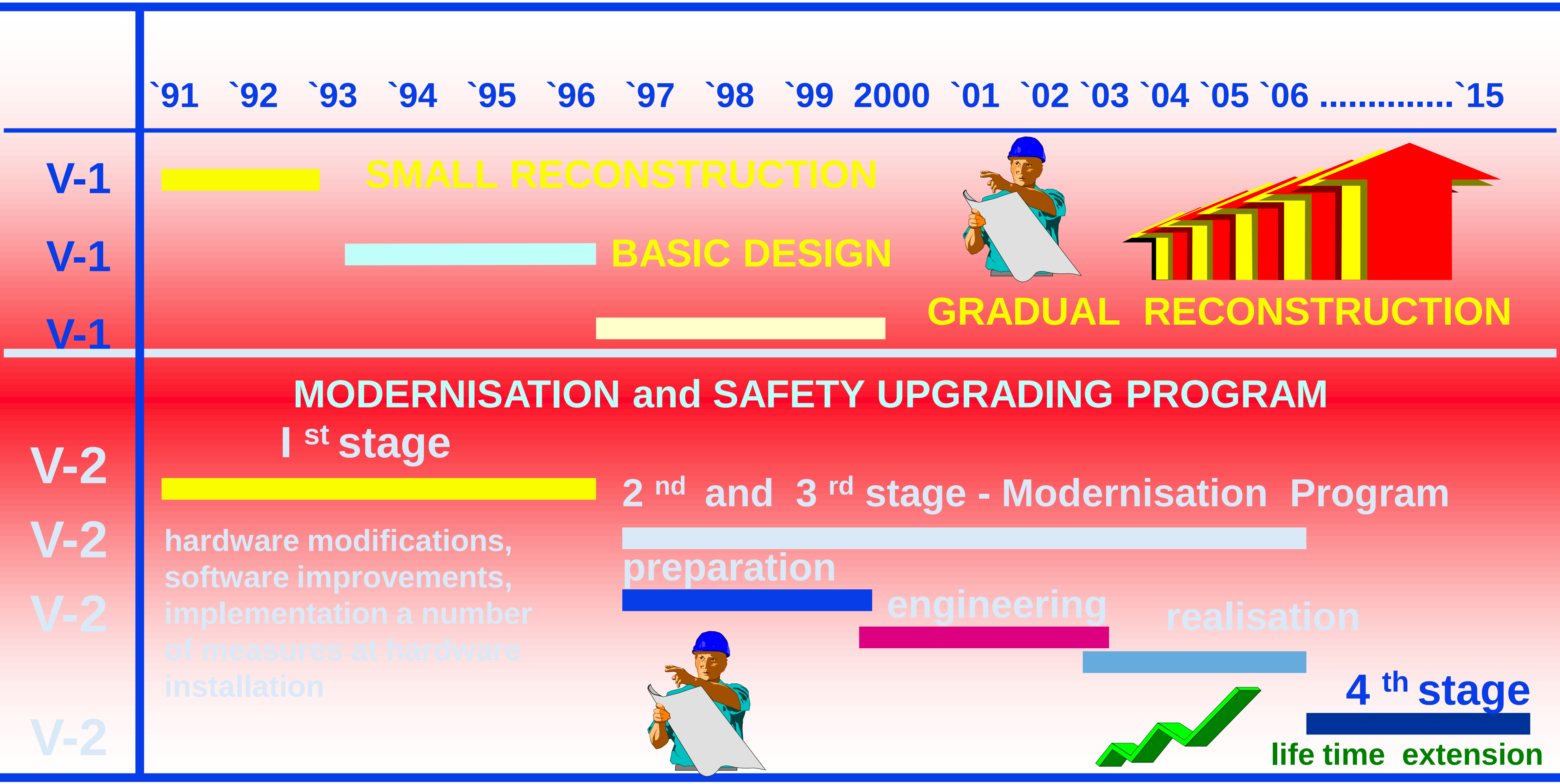
- The LPSA meets two basic requirements:

  1) PSA is updated if changes are made to plant design and operation, feedback is obtained from internal and external operational experience, the understanding of thermal–hydraulic performance or accident progression is improved, and advances are made in modeling techniques;

  2) the PSA model is comprehensively documented so that each aspect of the model is directly related to existing plant information or to the analysts’ assumptions of how the plant and the operating staff behave.

LPSA in Slovakia

BOHUNICE NPPs Upgrading Program Schedule



`91 `92 `93 `94 `95 `96 `97 `98 `99 2000 `01 `02 `03 `04 `05 `06 ............. `15

V-1 SMALL RECONSTRUCTION

V-1 BASIC DESIGN

V-1 GRADUAL RECONSTRUCTION

MODERNISATION and SAFETY UPGRADING PROGRAM

V-2 I st stage

V-2 2 nd and 3 rd stage - Modernisation Program

V-2 hardware modifications, software improvements, implementation a number of measures at hardware installation

preparation

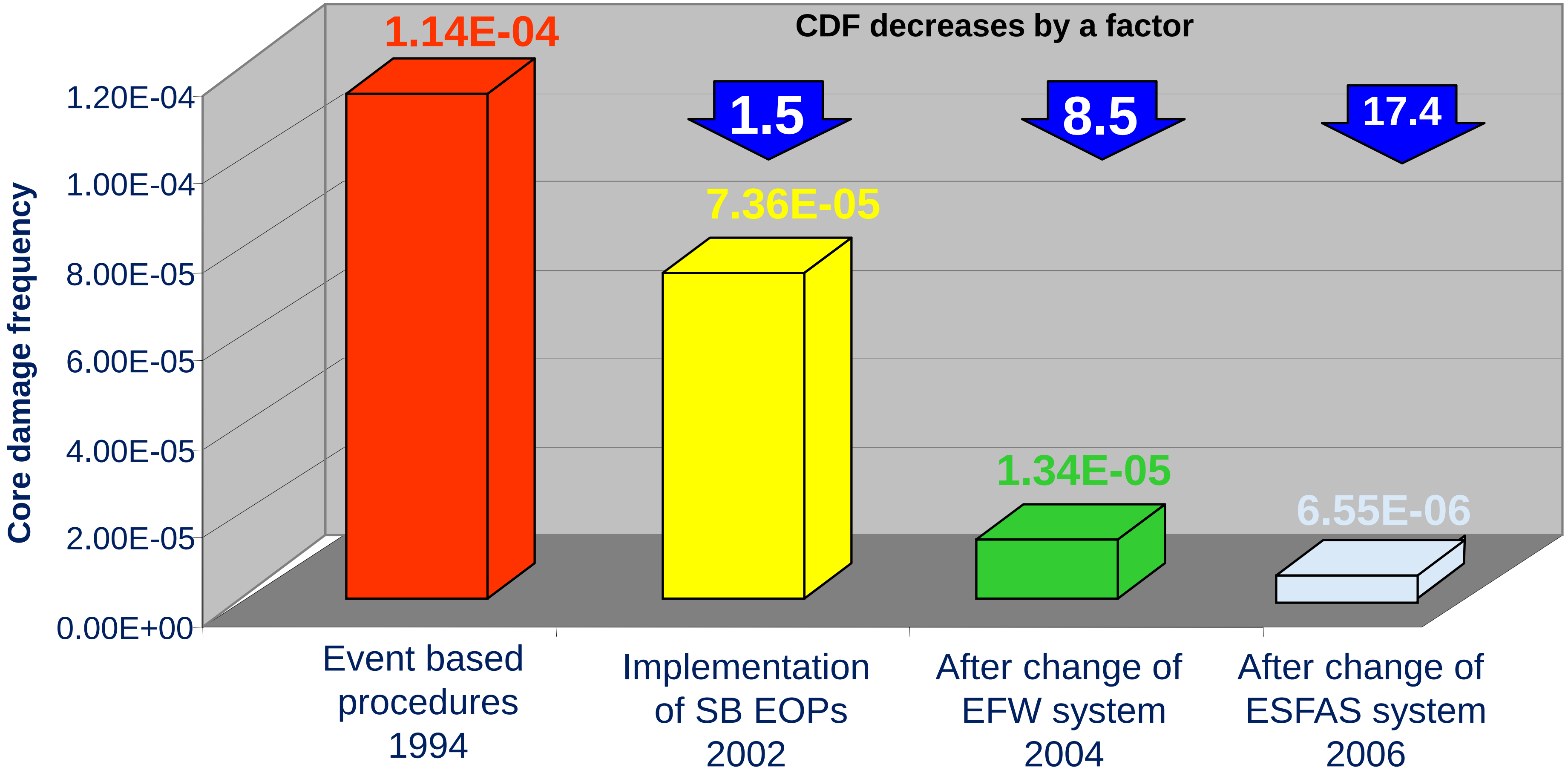
engineering

realisation

V-2 4 th stage

life time extension

LPSA in Slovakia



Risk monitors

Risk Monitor

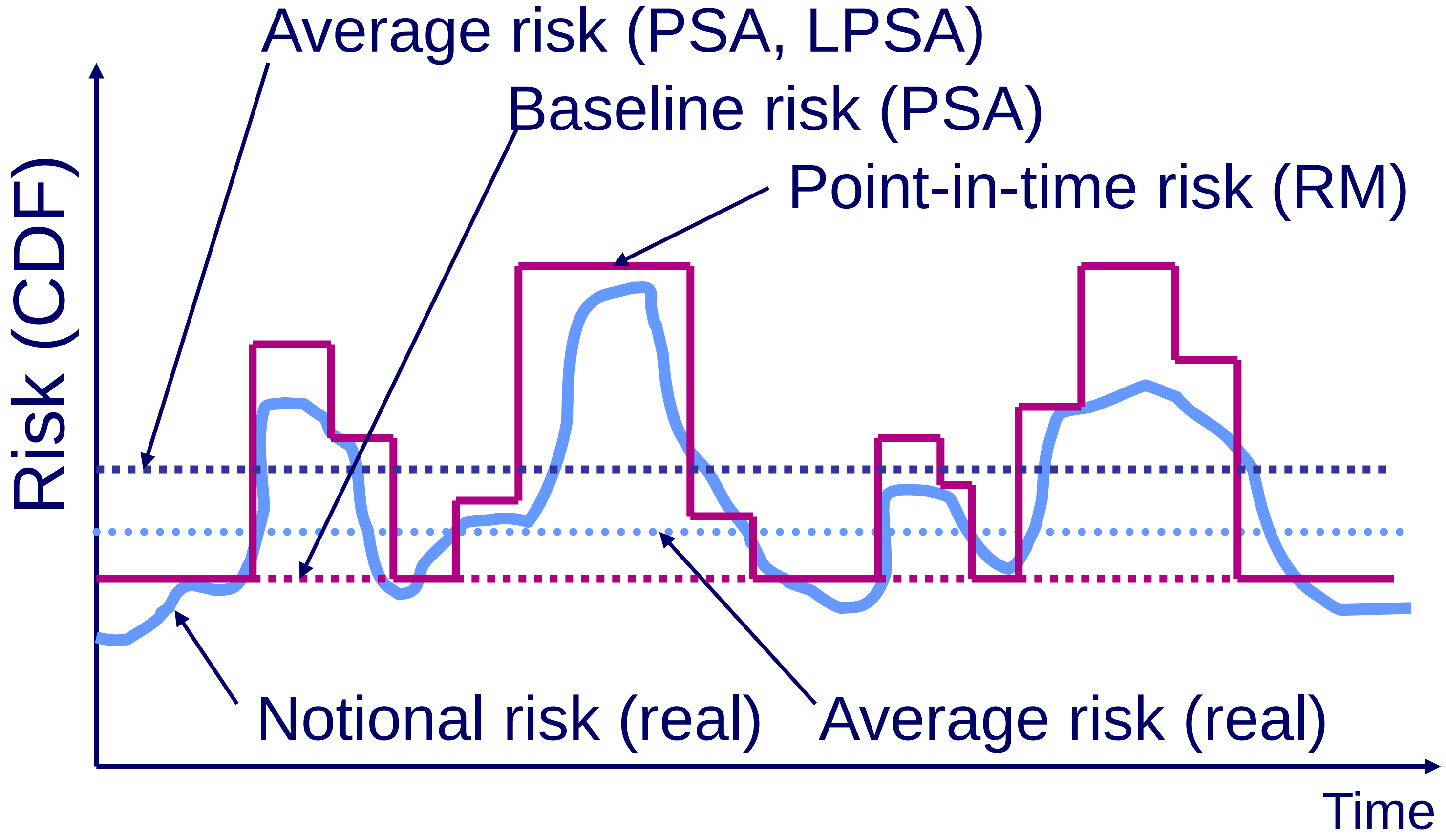
IAEA definition (IAEA-TECDOC-1101):

"A plant specific real-time analysis tool used to determine the instantaneous risk based on the actual status of the systems and components. At any given time, the Risk Monitor reflects the current plant configuration in terms of the known status of the various systems and/or components – for example, whether there are any components out of service for maintenance or tests. The Risk Monitor model is based on, and is consistent with, the LPSA. It is updated with the same frequency as the LPSA. The Risk Monitor is used by the plant staff in support of operational decisions"

Differences between LPSA and RM

Living PSA	Risk Monitor
Used off-line	Used on-line and off-line
Used by PSA specialists	Useable by all plant staff
Calculates average risk	Calculates point-in-time risk
Averages risk over all plant configurations	Calculates risk for an actual plant configuration

Plant risk

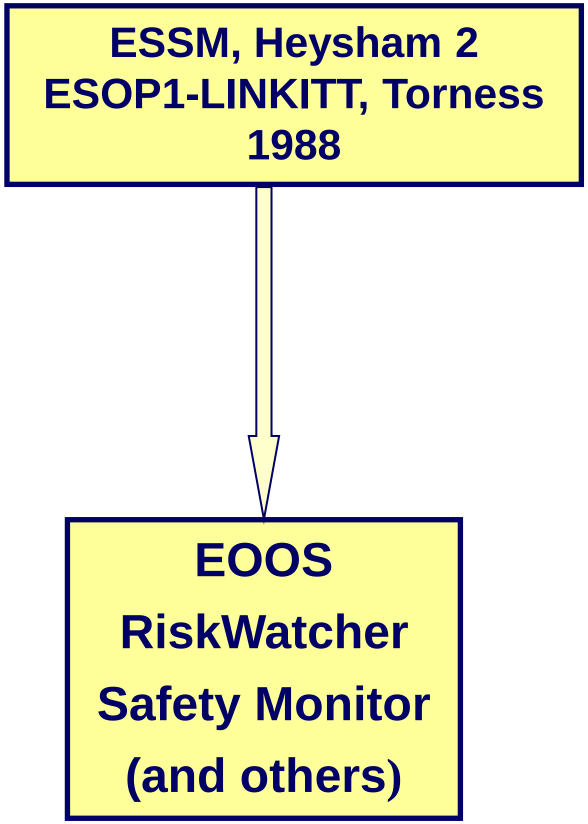

Average risk (PSA, LPSA)
Baseline risk (PSA)
Point-in-time risk (RM)
Risk (CDF)
Notional risk (real)
Average risk (real)
Time

Development of Risk Monitor PSA Model

- **LPSA is not useable directly for a Risk Monitor application**
- **Changes required to LPSA**
  - removal of asymmetries
  - model system alignments; running/ standby trains
  - review screening in LPSA
- **Enhancements often made to the PSA**
  - better common cause failure model
  - revised human error probabilities
- **Required to verify that the Risk Monitor results are consistent with LPSA**
  - produces equivalent cut-sets
  - results for new features are correct (to cover the CCF model, HEPs, dynamic events, alignments not included in LPSA, etc. as appropriate)

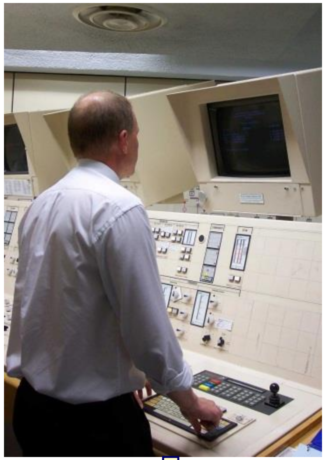
Risk Monitor Development

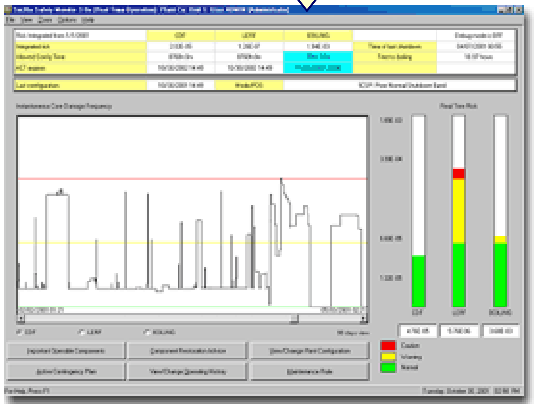
The first Risk Monitor:



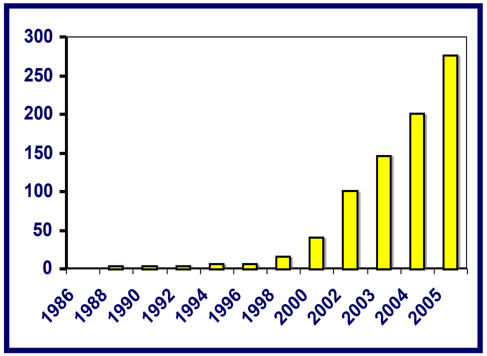
ESSM, Heysham 2
ESOP1-LINKITT, Torness
1988

EOOS
RiskWatcher
Safety Monitor
(and others)





Large number of Risk Monitors now in service



Most influential application of PSA

Typical Reasons for Using a Risk Monitor

- Apply a risk-informed approach to managing plant operational safety
- Schedule maintenance to avoid peaks in the risk
- Achieve greater flexibility in plant operation
- Provide justification for carrying out more maintenance on-line
- Get information on component restoration/ importance during maintenance
- Address US NRC Maintenance Rule

US NRC - Maintenance Rule (a)(4)

- **10CFR50.65 (a)(4) says:**

  “Before performing maintenance activities (including but not limited to surveillance, post-maintenance testing, and corrective and preventive maintenance), the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities. The scope of the assessment may be limited to structures, systems, and components that a risk-informed evaluation process has shown to be significant to public health and safety.”

Optimization of allowed outage times

(AOT)

Optimization of allowed outages times

- The allowed outage time (AOT) is the time the component is allowed to be out of service during power operation or shutdown operating mode of the plant.

- If the component is not restored during this time, the plant in operation must be shut down or the plant in a given shutdown mode has to go to safer shutdown mode.

Nomenclature

- The *Allowed Outage Time* (AOT) has been replaced in many references (mainly US) with *Allowed Configuration Time* (ACT) or *Completion Time* (CT)
- The meaning is the same and refers to the time allowed for corrective measures before a mode change (shutdown) is required

AOT = ACT = CT

Optimization of allowed outages times

Nomenclature

- CDF, ΔCDF, CCDP and ICDP
  - ✓ *Core Damage Frequency* (CDF) = number of core melt events per year
  - ✓ *Conditional Core Damage Probability* (CCDP) = probability of core melt (dimensionless), given an initial condition
  - ✓ ΔCDF = increase above baseline CDF
  - ✓ Δt = exposure time (years, or fraction thereof)
  - ✓ *Incremental Core Damage Probability* (ICDP)

    ICDP = ΔCDF * Δt

Optimization of allowed outages times

- Quantitative Thresholds
  - NUMARC 93-01 (NEI - Industry Guideline For Monitoring The Effectiveness Of Maintenance At Nuclear Power Plant) provides the following thresholds for when risk management actions are required:

ICDP	Actions
$>10^{-5}$	Configuration should not normally be entered voluntarily
10^{-6} to $>10^{-5}$	Establish risk management actions
$<10^{-6}$	Normal work controls

Optimization of allowed outages times

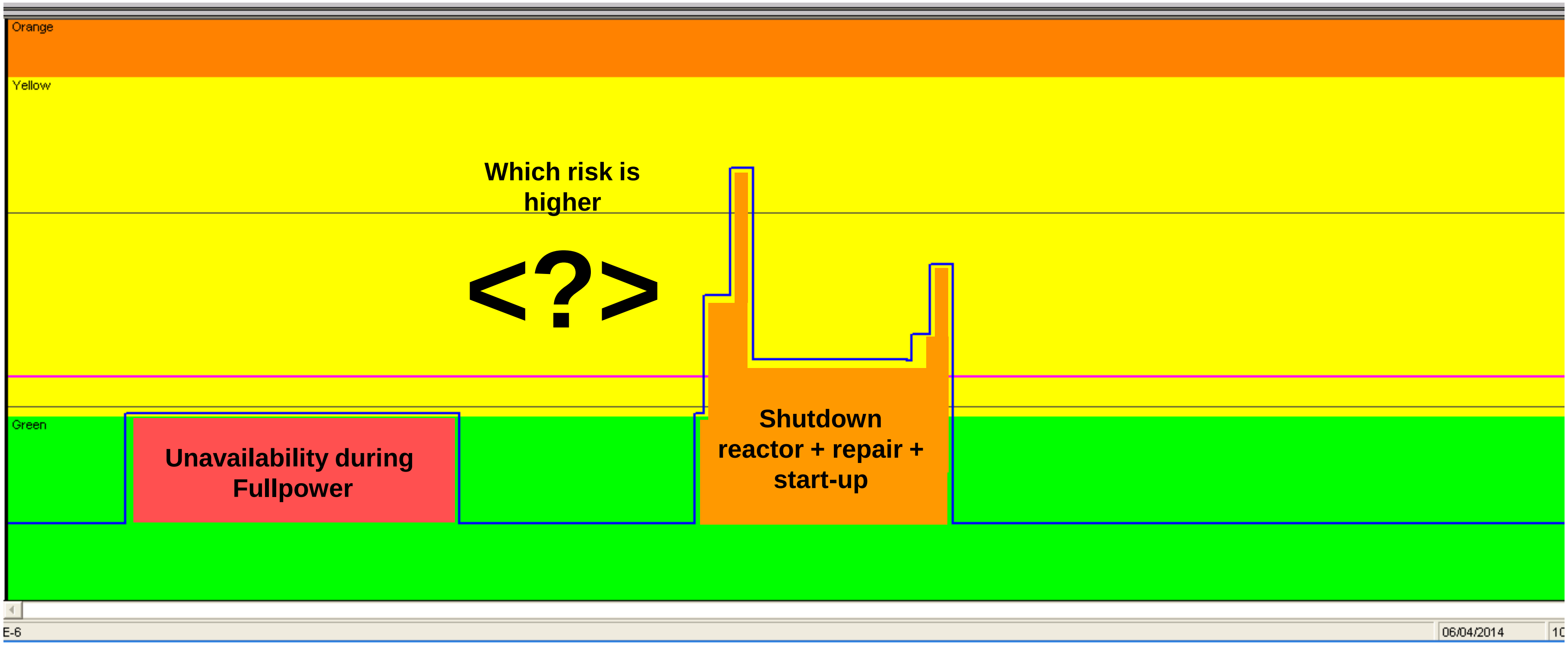
- Another Quantitative Threshold often referenced - 5.0E-7
  - The ICDP acceptance guideline of 5.0E-7 is based upon the hypothetical situation in which the subject equipment at a representative plant is out for five hours, causing the CDF of the plant, with an assumed baseline CDF of 1.0E-4 per reactor year, to conditionally increase to 1.0E-3 per reactor year (or one order-of-magnitude above the Safety Goal).
  - This basis assumes that the majority of repairs can be made in five hours or less and that the regulatory authority (NRC) has accepted this level of risk for existing operating plants. On the basis of these arguments and assumptions, the USNRC acceptance guideline for ICDP is calculated as 5.0E-7 ((1.0E-3-1.0E-4) * 5 hrs / 8760 hrs per year).

Optimization of allowed outages times

- When deciding on the optimum strategy, the risk exposure for the current operating mode and the new operating mode should be compared. Such comparison can be made for all components involved in the limiting conditions of operation (LCO) using the full power and shutdown PSA model (approach used in Slovakia).

Optimization of allowed outages times

AOT calculation using full power and shutdown PSA model



Which risk is higher

<?>

Orange
Yellow
Green
Unavailability during Fullpower
Shutdown reactor + repair + start-up
E-6
06/04/2014
10

Risk-informed In-Service Inspection (ISI)

Why do we perform In-service Inspections?

- Over the operating lifetime of a NPP, components such as pipework, may be exposed to influences such as stress, high temperature, irradiation, hydrogen absorption, corrosive attack, vibration and fretting, and all of their effects depending on time and operating history.
- These influences may result in
  - changes of material properties due for example to irradiation, thermal embrittlement or corrosion fatigue and
  - the initiation and growth of flaws.
- In Service Inspection programmes are intended to address all systems and components that are subject to such degradation and to propose remedial measures.

Why Risk Informed – In-service Inspection?

- Thus the objective of In-service Inspection (ISI) is to identify conditions, such as cracks, material flaws, etc. that are precursors to leaks and ruptures
  - Traditionally used code classification and expert judgment in developing inspection scope and tests

- RI-ISI is an alternative method for classifying piping into safety significant groups using risk related information:
  - Reduced Inspections, reduced dose to staff
  - Concentrate on important inspections

Basic Concept of RI-ISI

- Develop an efficient inspection programme
- Develop a programme that is consistent with other risk informed processes (i.e. Integrated Decision-Making Process)
- Concentrate resources on higher risk components/piping

- Guidance given in:
  IAEA Nuclear Energy Series (NP-T-3.1)
  'Risk-informed In-service Inspection of Piping Systems of Nuclear Power Plants: Process, Status, Issues And Development', Vienna, 2010

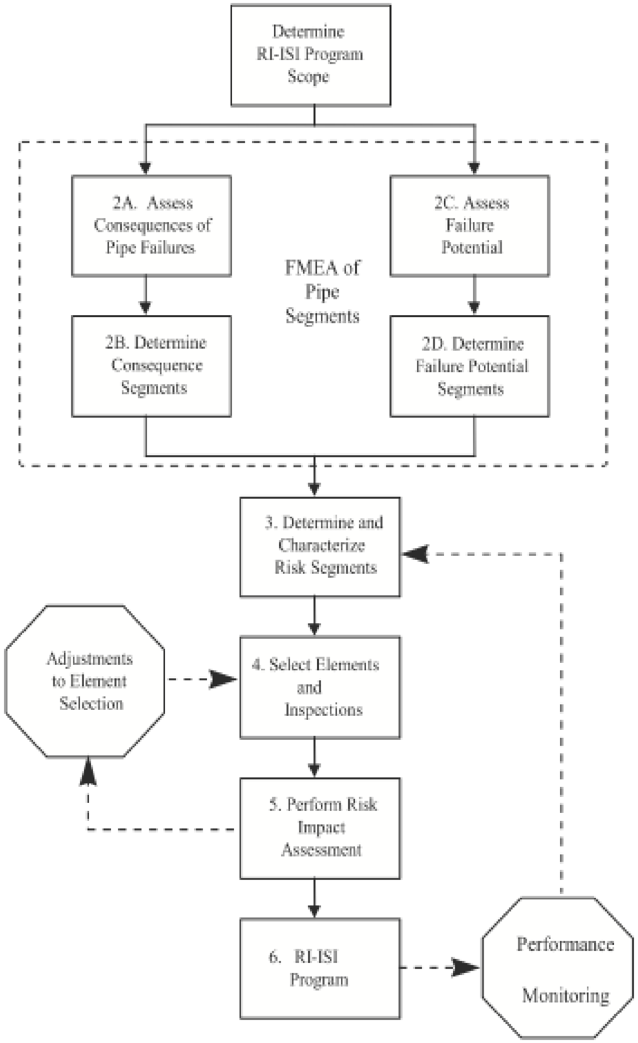
How to achieve the RI-ISI

- **Traditional**
  - Treat every component the same
  - If practicable, inspect quarterly
  - Otherwise:
    - Inspect at cold shutdown, or
    - Inspect at refueling (based on practicability)

- **Risk-informed**
  - Understand component relative risk
  - Understand component performance
  - Understand component failure modes
  - Assess inspection needs relative to failure modes
  - Based on understanding, determine inspection interval

Typical RI-ISI methodology

1. Scope and Segment Definition - Includes PSA identification and ASME Section XI Segments
2. Consequence Evaluation - consider direct and indirect consequences
3. Failure Probability Assessment - estimate the likelihood of the piping failure
4. Risk Evaluation - combine 2, 3 above for CDF and LERF Estimates. Use RRW importance
5. Expert Panel Categorization - Blend of PSA and Deterministic insights
6. Element NDE Selection - Choosing which welds are inspected using NDE
7. Implement Programme - Revise present ISI programme, procedures and documents
8. Feedback Loop - Monitor the effectiveness of the programme and evaluate plant changes, industry experience, PSA model changes, etc.


Determine RI-ISI Program Scope
2A. Assess Consequences of Pipe Failures
2C. Assess Failure Potential
FMEA of Pipe Segments
2B. Determine Consequence Segments
2D. Determine Failure Potential Segments
3. Determine and Characterize Risk Segments
Adjustments to Element Selection
4. Select Elements and Inspections
5. Perform Risk Impact Assessment
6. RI-ISI Program
Performance Monitoring

RI-ISI - Two Methods

- Two general methods being supported:
  - WROG RI-ISI Methodology - Westinghouse approach, which uses a more quantitative PSA approach
  - EPRI Approach, which is initially less reliant on PSA results

Significance Determination Process - SDP

What is the *Significance Determination Process*?

- NRC method for classifying event significance
- Allows numerical assessment of licensee events
- Designed to remove subjective element from licensee assessment

MD 8.3 and SDP

- NRC Management Directive 8.3
  - Used by the NRC to determine the size of an inspection team following an “unusual event”
- *Significance Determination Process*
  - Used by the NRC to assess the severity of an “unusual event”
  - The NRC may send a designated team, following an “incident,” to investigate the associated risk significance, complexity and generic safety implications

Levels of Significance

- GREEN: <1E-6 CDP and <1E-7 LERP; least severe
- WHITE: up to 1E-5 CDP and 1E-6 LERP
- YELLOW: up to 1E-4 CDP and 1E-5 LERP
- RED: ≥1E-4 CDP or ≥1E-5 LERP; highest level of severity

Mitigating Systems Performance Index (MSPI)

Background
Regulations / Requirements

- **RG 1.174 RG 1.174 ,**
  Regulatory Guide 1.174 - An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis

- **RG 1.177 RG 1.177**
  An Approach for Plant-specific, Risk-informed Decision Making: Technical Specifications

Mitigating Systems Performance Index

- Focus on monitored systems/components:

- Monitored Component: A component whose failure to change state or remain running renders the train incapable of performing its monitored functions. In addition, all pumps and diesels in the monitored systems are included as monitored components.

Mitigating Systems Performance Index

- MSPI monitors risk due to:
  - Unavailability at the train level
  - Unreliability at the component level

- MSPI = UAI + URI
  - UAI – Unavailability Index
  - URI – Unreliability Index

Input to MSPI

- MSPI = UAI + URI

- MSPI
  - Accumulated plant data
    - Unavailability – maintenance hours - UAI
    - Unreliability   – failures - URI

- Input to MSPI
  - PSA Model
    - CDF
    - Fussel-Veselys and Birnbaums

MSPI - Unreliability

$$URI = \sum_{i=1}^{n-components} W_i (UR_{Bci} - UR_{BLci})$$

UR_{Bci} - is the actual Unreliability of component *i*

UR_{BLci} - is the Baseline Unreliability of component *i*

W_i - is the risk weight for component *i*

MSPI - Unavailability

$$UAI = \sum_{i=1}^{n-trains} W_i (UA_{ti} - UA_{BLti})$$

UA_{ti} - is the actual Unavailability of train *i*

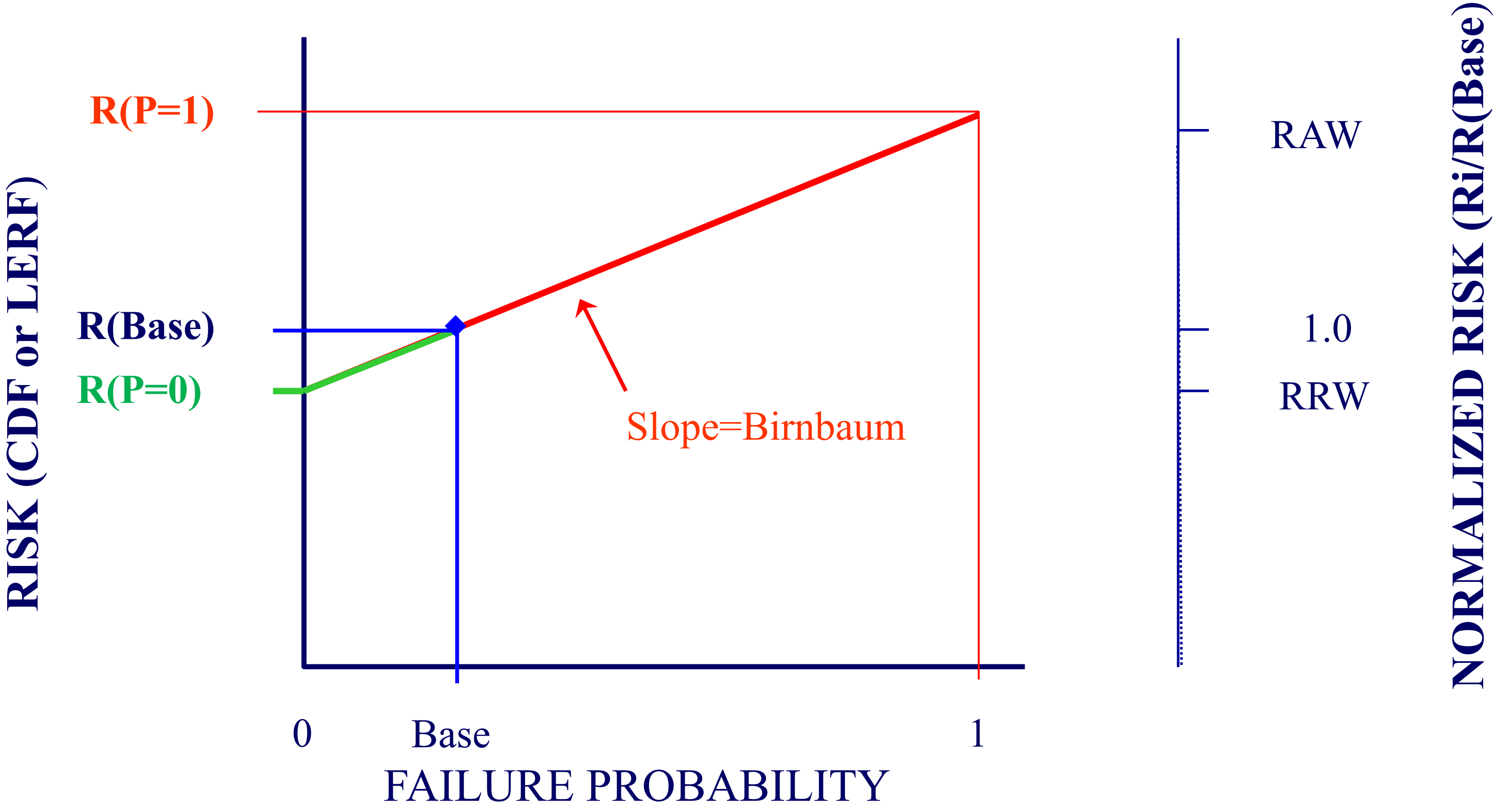
UA_{BLti} - is the Baseline Unavailability of train *i*

W_i - is the risk weight for train *i*

Input to MSPI products

- Fussell –Vesely
  - $Fv_i = \Sigma$ all cutsets with Be_i / CDF
- Birnbaum
  - Bi = Fv_i /($Prob_i$ of Bei) x CDF
  - $B_i = \Sigma$ cutsets with Be_i / (Prob of Be_i)

Importance Measures (Graphical Depiction)



Birnbaum is a measure of slope of the line from RAW to RRW

Mitigating Systems Performance Index – As Implemented

- MSPI is calculated for a system and compared to risk thresholds

$MSPI \leq 1\times10^{-6}$	▪ THEN performance is GREEN
$1\times10^{-6} < MSPI \leq 1\times10^{-5}$	▪ THEN performance is WHITE
$1\times10^{-5} < MSPI \leq 1\times10^{-4}$	▪ THEN performance is YELLOW
$1\times10^{-4} < MSPI$	▪ THEN performance is RED

MSPI Monitored Systems

BWRs	PWRs
High pressure coolant injection/core spray (HPCIC)	HPSI (high pressure safety injection)
Reactor Core Isolation Cooling (RCIC) or isolation condenser	AFW (auxiliary or emergency feedwater)
RHR (residual heat removal)	RHR (may include containment spray)
EAC (emergency AC power)	EAC
Cooling Water Support Systems	Cooling Water Support Systems

References

- **NEI 99-02 rev. 6, Section 2.2 and Appendices F & G**
  - **F. Methodologies for Computing the Unavailability Index, the Unreliability Index and Component Performance Limits**
  - **G. MSPI Basis Document Development**

THANK YOU FOR YOUR ATTENTION