Latent Weaknesses and Root Causes in the Feedback of Operating Experience Programmes

Milorad Dusic, Nuccon GmbH

m.dusic@nuccon.eu

Latent weaknesses and root causes

- Incidents are inevitable part of operational life of any complex industrial facility
- It is hard to predict the way that various contributing factors combine to cause the undesired outcome
- But it should be possible to detect the existence of latent conditions that together with the triggering failure(s) result in abnormal events

Latent weaknesses and root causes

- Such latent conditions are: poor design, gaps in supervision, maintenance faults, inadequate procedures, shortfalls in training, etc.
- We must try to detect as many as possible
- Good surveillance is the key to their identification and elimination
- Root causes should be looked for in the management of surveillance programmes
- Cases of large industrial accidents, well described in open literature can be used to demonstrate such pre-existing latent weaknesses:

Davis Besse event

- In 2002, inspection of CRDM nozzle cracking on the head of RPV (NRC Bull 2001-01)
- After nozzle crack repair (welding), nozzle observed to tip sideways
- After CRDM nozzle and deposited boric acid removed – large cavity discovered
- Ultrasonic testing measured 3/8 inch remaining thickness of the RPV head – stainless steel cladding
- 1987 Turkey Point and Salem

  1988 NRC Generic Letter 88-05 – addresses corrosive effects of boric acid

  1996 onwards, boric acid deposits on top of RPV head at Davis-Besse
- Utility believed that it was due to the leakage through CRDM flange and that elevated temp. at that location would prevent corrosion
- For several years warning signs ignored; industry reports, coolant leakage, rust, boron on filters, amount of dry boric acid on RPV head – poor safety culture.

Davis Besse event

Analyses methods

- Not all events are alike and therefore different techniques are required for their investigation and analysis
- Some basic information :
  - Root Cause Analyses – TECDOC-1756
  - Probabilistic Precursor Analyses – TECDOC-1417
  - Deterministic Transient Analyses – TECDOC-1550
- To be used by NPPs, RBs and TSOs

I. Root Cause Analysis

- Most commonly used
- Several techniques exist
- Prime objective to find the Root Cause defined as the underlying cause that if properly addressed would prevent recurrence

Root Causes are directly correctable, i.e. are within the influence of the organisation

Root Cause Analysis

Many different techniques in use:

- Task Analysis
- Change Analysis
- Barrier Analysis
- Event and Casual Factor Charting (ECFC)
- ASSET/PROSPER
- HPES – Human Performance Enhancement System
- MTO – Man, Technology, Organization
- AEB – Accident Evolution and Barrier Function Analysis
- MORT – Management Oversight and Risk Tree Analysis
- HPIP – Human Performance Investigation Process

Event and Causal Factor Charting (ECFC)

Description

An ECFC is a graphically displayed flowchart of an entire event plotted on a time line.

As an event line is established, additional features such as related conditions, secondary events and presumptions are added.

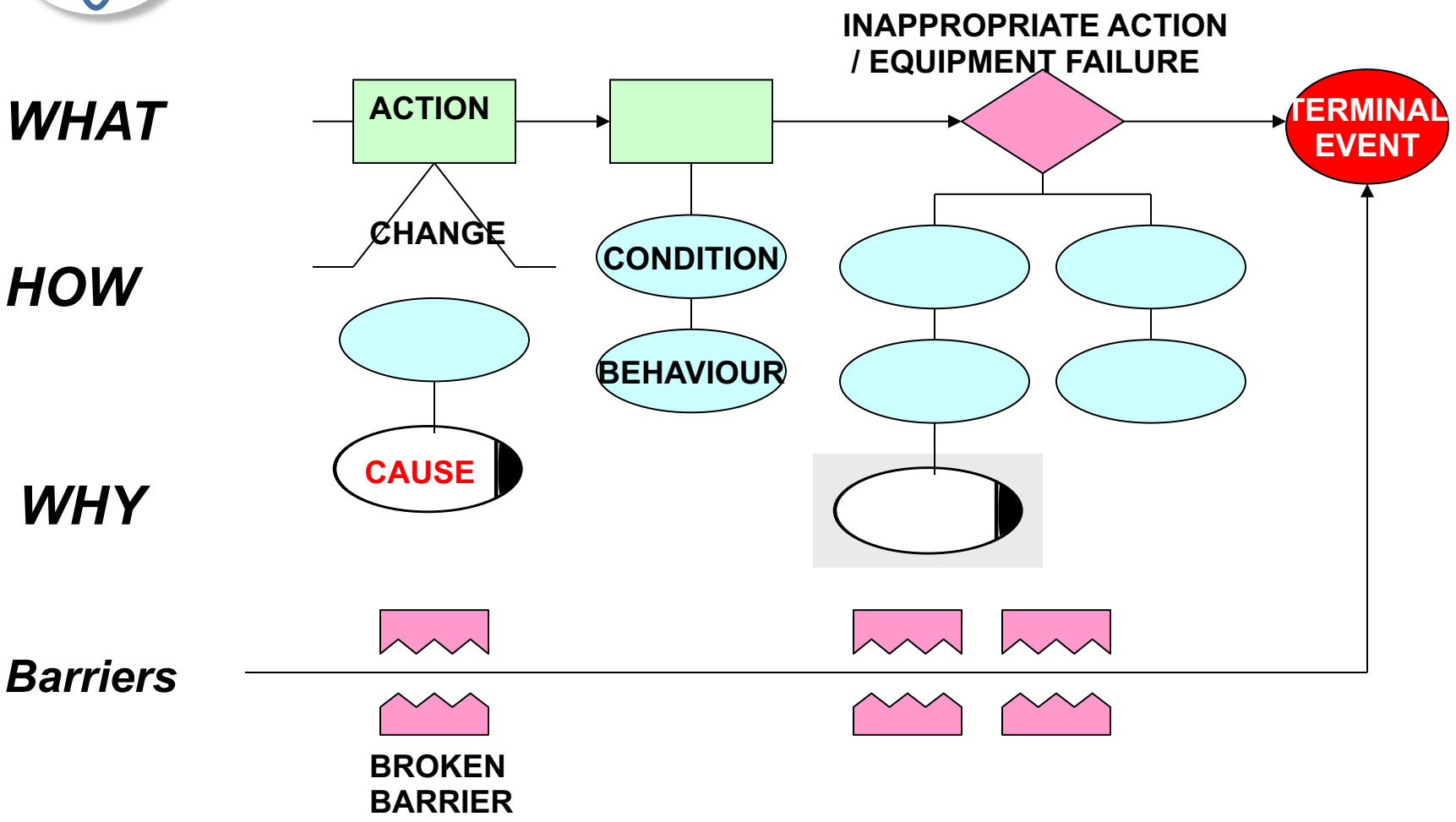
Strengths

- An excellent opportunity to graphically display barriers, changes, causes and effects and human performance interactions
- Organizes data and provides a broad picture
- Easy to understand and communicate with those not familiar with the techniques (management, operators)

Limitations

- Can be time consuming
- Rarely stands alone and greatly enhanced by superimposed barrier and change analyses

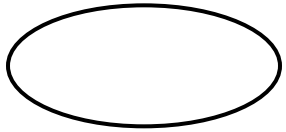
Event & Causal Factor Chart



Events & Causal Factors Chart Symbols:

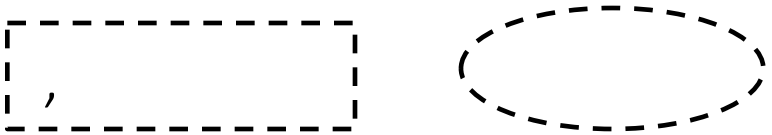
- Events: who did, what, where, when

- Conditions: background factors, influences, environment



- Relationships of parts - lines: ,

- Assumptions:



ASSET/PROSPER

Description

The root cause methodology developed to support the IAEA ASSET/PROSPER Services.

Root causes are clearly defined as the answer to the question : why was it not prevented?

Strengths

- Freely available to use
- Used numerous times on ASSET/PROSPER Missions
- Output is directed at NPP management
- Training available by the IAEA

Limitations

- Has a different definition of root cause as other techniques
- Identifies deficiencies in management and policy, therefore requires knowledgeable senior staff to do the analyses

HPES – Human Performance Enhancement System

Description

The techniques encompassed within the HPES package include:

- Task analysis, Change analysis, Barrier analysis, Event and Causal Factor Charting-ECFC
- Behavioral analysis, Situational analysis
- Interviewing techniques

Strengths

- Provides a toolbox of techniques
- Proven methodology used worldwide
- Training courses and handbooks available

Limitations

- Requires experience and training to apply effectively
- The process does not specifically identify organizational issues

MORT – Management Oversight and Risk Tree

Description

The method consists of a Fault Tree together with a long series of interrelated questions

Strengthen

- Comprehensive Manual and Training available
- Uses detailed Fault Trees
- Flexible (can use parts of Fault Tree for small events)
- Uses Barrier analysis
- Computerized version is available

Limitations

- Requires experience to use
- Time consuming due to extensive task analysis

II. Precursor Analysis

- Quantitative estimation of safety significance
- Uses the concept of CCDP to determine safety significance of events
- A measure, in the PSA model, how far is the event which is being analysed from the core damage scenario
- Much more detailed than INES

Conditional Core Damage Probability - CCDP

CCDP = Probability of Core Damage given something* has happened in the plant

***) something means:**

- **an initiating event has actually happened, or**
- **safety related equipment was out of service during a certain time or both together.**

Two types of Precursor Events:

- **A transient which interrupts normal operation**
  - Real effect on plant operation
  - Easily related to an IE in the PSA
  - Scenarios affected by precursor are all those developing from this IE
- **Unavailability or a degradation of equipment/systems for a longer time period**
  - No immediate impact on plant operation
  - Precursor affects one or more safety functions
  - All IE which require the affected safety function must be identified

Process

1. Precursor review and analysis
   - ❑ Understanding the event
2. Mapping of the Precursor on the PSA
   - ❑ Relate the event and its implications on the PSA model
   - ❑ Are PSA models adequate?
   - ❑ Revise, extend if necessary
3. Quantification
   - ❑ Estimate failure probabilities
   - ❑ Adopt PSA reliability models
4. Initial evaluation
   - ❑ Recalculate CCDPs for all affected sequences

Process – cont.

5. Recovery actions
   - ❑ Determine potential recovery actions
   - ❑ Model recoveries
6. Evaluation
   - ❑ Calculate new importance measures
   - ❑ Perform uncertainty and sensitivity analysis
7. Extension
   - ❑ What would happen if under different conditions
8. Interpretation, conclusions, insights, corrective measures

Precursor Terminology

CCDP < 1.E-6	Not a Precursor
1.E-4 > CCDP > 1.E – 6	Precursors
1.E-3 > CCDP > 1.E – 4	Important Precursors
CCDP > 1.E – 3	Significant Precursors

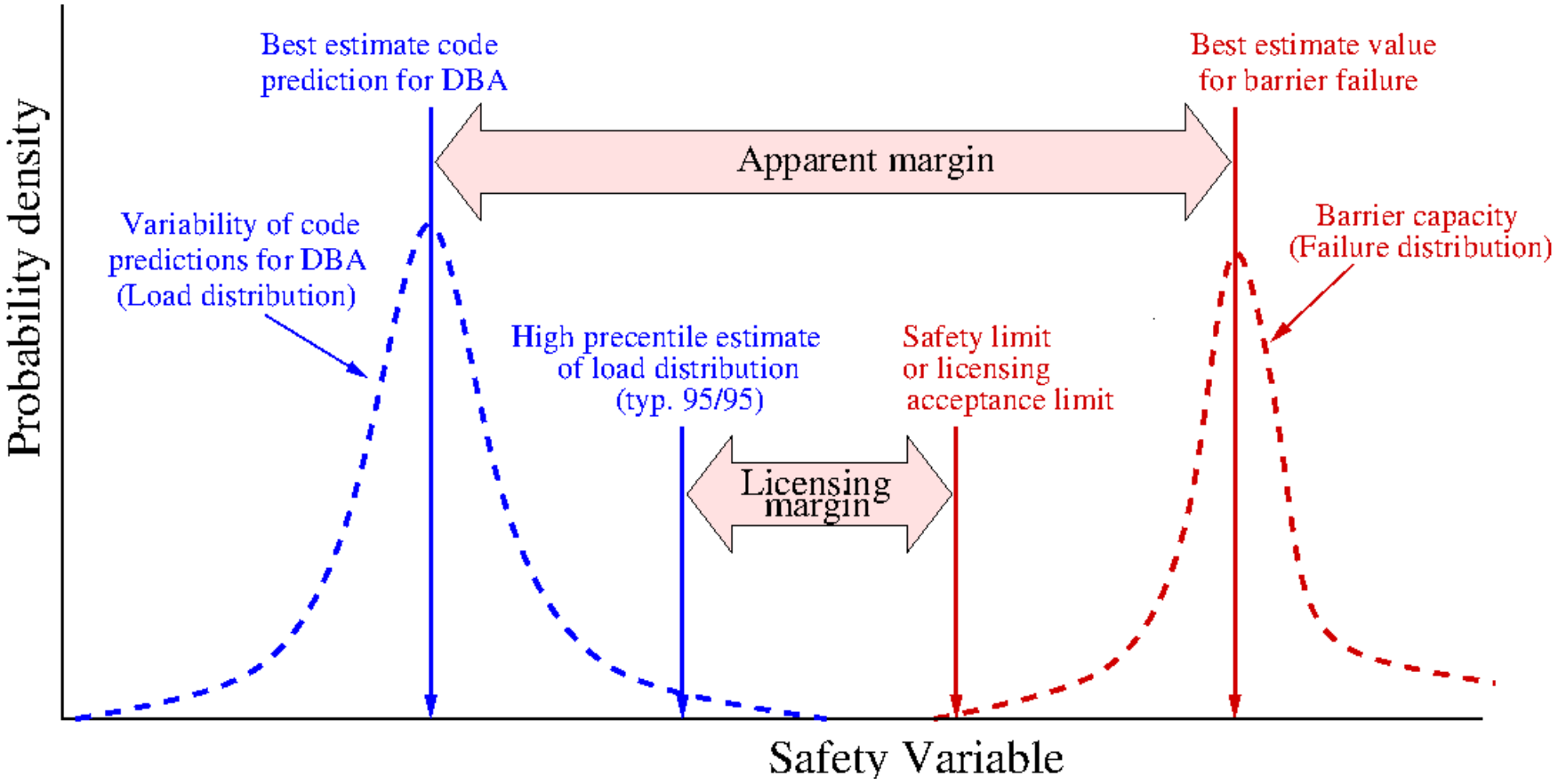
III. Deterministic Transient Analysis

- Used mostly for events with fast development
- Better understanding of the phenomena, occurring during a specific event
- Identification of the impact of different contributing factors and conditions (operator vs. automated action).
- Evaluation of the plant safety margins during the event
- Improvements in operator training and operating procedures

Load and Barrier Probability Distributions

- Distribution of code predictions/results is a consequence of uncertainties in I&B conditions data as well as in computer model
- Distribution of failures i.e. values where the barrier fails is a consequence of our limited knowledge of the precise phenomenon that causes failure

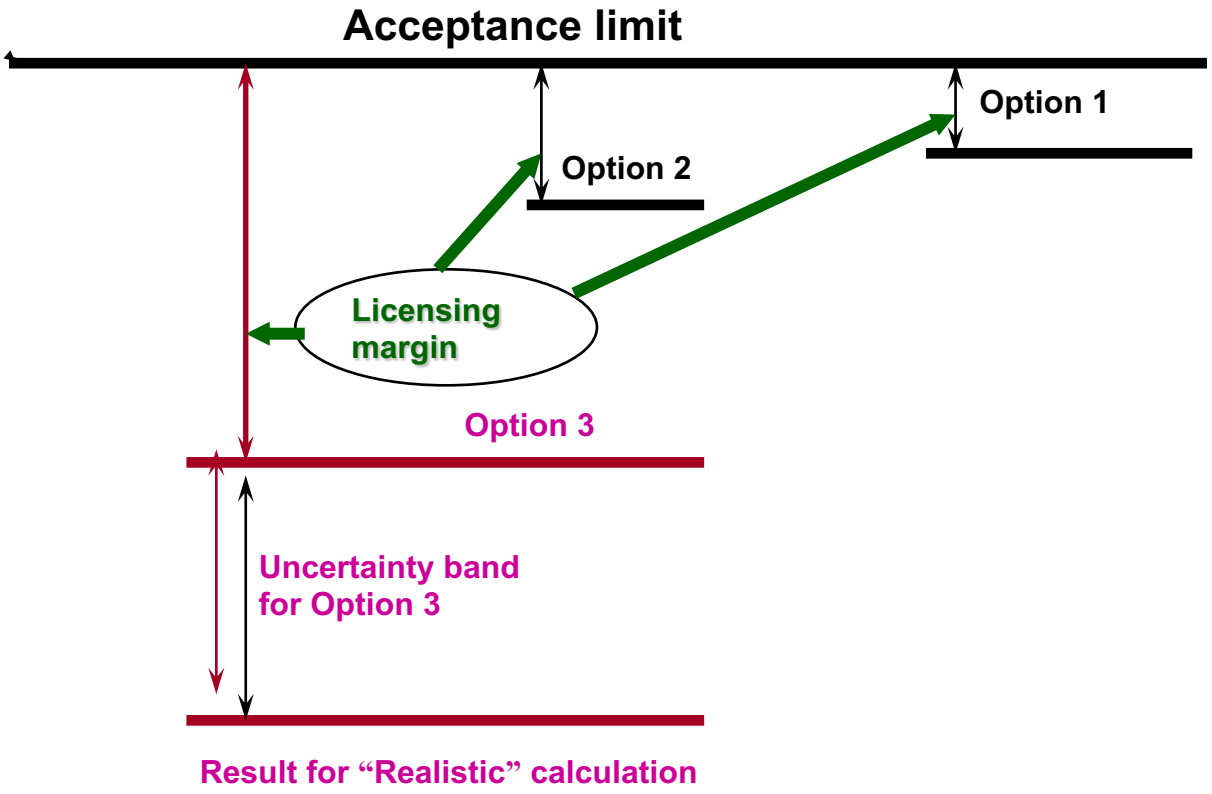
Load and Barrier Probability Distributions



Options for DSA

- Option 1: Conservative
- Option 2: Best Estimate (BE)
- Option 3: Best Estimate plus Uncertainty (BEPU)
- Option 4: Extended BEPU (E-BEPU)

Licensing Margins under Options 1, 2, 3



Conclusions

- RCA remains to be most important techniques for incident evaluation – provides Root Causes
- Precursor analysis provide the best method for determination of safety significance of events
- Transient analysis are the best suited for events with rapid development of occurrences
- All three methods complement each other
- Not all events are alike and a careful consideration should be given which method to use for evaluation of a particular event.

Thank you for your attention

m.dusic@nuccon.eu