**Resilience
Engineering**

A Review

Andy Evans
RAeS EMSG
17 Oct 2006

Resilience Engineering
Concepts and Precepts

Edited by
ERIK HOLLNAGEL
DAVID D. WOODS
NANCY LEVESON
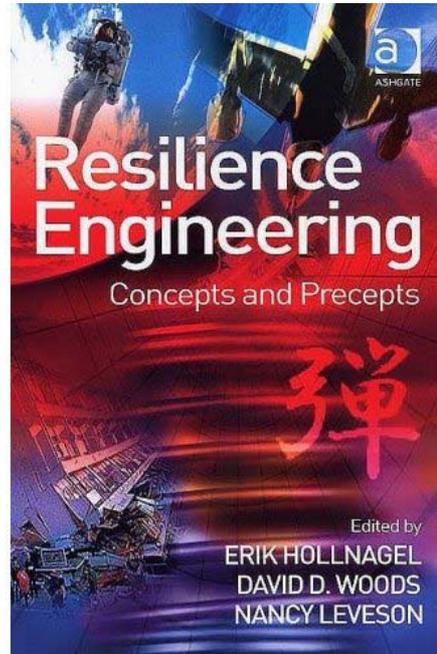
Introduction (1)

- The book consists of 21 papers from a symposium in Sweden in Oct 2004
  - Sponsored by the Swedish CAA (LFV) & Swedish Nuclear Power Inspectorate (SKI)
  - Mostly academics, diverse backgrounds, from mainly US & Europe
  - Now available from Ashgate as:
    - Hardback £55 ISBN 0754646416 (Jan 2006)
    - Paperback £28 ISBN 0754649040 (Sept 2006)
- Focus: organisational / system resilience
  - i.e. robustness to hazards

Introduction (2)

- Prof James Reason is quoted as saying:
  - *This is the most thought provoking collection of papers I've read for a very long time.*
  - *They are written by the best in the field at the top of their form.*
  - *Resilience is a notion whose time has come.*
  - *We cannot realistically expect to eliminate adverse events ... But we can strive to achieve greater robustness...*
- Jane Carthey (Head of R&D at the National Patient Safety Agency) says:
  - This book is the next frontier for improving safety... it emphasises:
    - the importance of learning about the positive side of safety management
    - how frontline staff foresee, adapt & recover from problems.
- The publishers claim the book:
  - *Presents a completely new way forward for safety and risk management*

Introduction (3)

- While *Resilience Engineering* does not really articulate a solution, it does:
  - Integrate independently emerging, *generally* consistent, academic thinking
  - Highlight a philosophy worthy of consideration
    - Particularly on making the consequence of errors less significant
  - Though it considers more that just HF / error
    - SMS in general
- Some key concepts have been extracted here for discussion

Structure of the Book

- Section 1 has seven papers that discuss resilience & the supporting concepts
- Section 2 contains nine papers that examine resilience from a practical perspectives:
  - NASA, railways, healthcare, aviation & business generally
- Section 3 has five papers covering:
  - The design of a safety organisation
  - Safety management systems
  - The need for resilient organisations to be able to change state to accommodate unusual situations

Basic Concept (1)

- Safety is something that a 'organisation' / 'system' <u>does</u> *rather* than a property it <u>has</u>
  - i.e. an aircraft is not itself 'safe' but it may be operated safely
- To be safe, be *resilient:*
  - i.e. able to recover from the inevitable:
    - Irregular variations, disruptions & degradations
    - Note: *these are not just due to HF / errors*
- Understand how to actively ensure:
  - Things do not get out of hand
  - Control is not lost

Basic Concept (2)

- Resilience is a dynamic process
- The better an organisation understands the dynamics of its environment & can adjust, the more resilient it is
- Success depends on their ability to timely anticipate & pre-empt the changing risk
- Failure is simply the absence of that ability - Temporarily or permanently

A Previous Visualisation

Vulnerable (unstable)

Neutral

Resilient (stable)

Prof James Reason
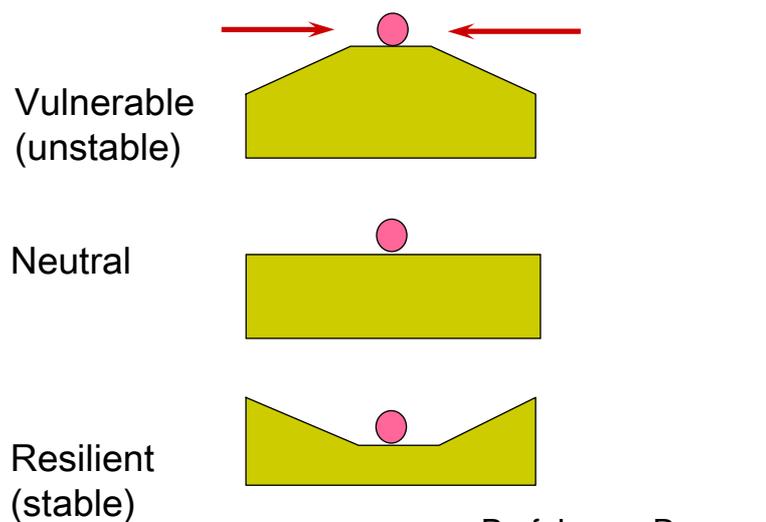
Critical Elements of RE

- Analysing, measuring & monitoring resilience
- Tools and methods to improve resilience
- Techniques to model & predict the effects of changes & decisions on risk

RE View on Human Error (1)

- Error can be approached two ways:
  - Firstly: *erratic people <u>degrade</u> an otherwise safe system*
    - Prevent people from damaging the system, e.g. by:
      - Reporting errors
      - Developing taxonomies of error types
      - Estimating likelihoods of error
      - Training on errors & how they occur
      - Writing more detailed rules etc
  - Secondly: *people are the primary source of resilience and <u>create</u> safety*
    - Albeit while under resource & performance pressures
    - Create means to tolerate or recover from errors

RE View on Human Error (2)

- It is recognised that error management involves *both* reduction & containment (Reason 1997)
- The two approaches to error assume the human is either:
    - The *hazard* – emphasis is on error <u>reduction</u>
    - The *hero* – emphasis is on error <u>containment</u>
        - i.e. tolerance & recovery
- RE puts more emphasis on the latter approach
    - Progress comes from aiding people under this pressure to cope with the complexity
        - Consistent with Dekker's *Field Guide to Understanding Human Error* discussed previously

Thoughts on Relevance to EMSG

- Most current HF initiatives focus on reduction:
    - Reducing <u>probability</u> of error
        - Or probability of violation (i.e. increasing compliance)
    - If humans are seems as a *hazard* so the emphasis is on individuals & conditions that provoke their errors
- RE increases the focus on containment:
    - Accept that errors will occur – plan for tolerance
    - Humans are *heroes* - plan for recovery
    - Primarily reducing the <u>consequences</u>
- RE thus puts a greater emphasis on:
    - Human Centred Design
        - Aircraft (physical design & 'design' of MM & MP)
        - Maintenance / operational process design etc
- The approaches are complimentary
    - Though RE is a more encompassing safety concept