Discussion on Risk in Complex Operational Settings

International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth – Advances and Challenges for Nuclear Installation Safety

Ken Ellis
WANO Managing Director
23 October 2013
(a) Product of unreliable system components (Complicated)

(b) Product of improperly aligned, or poorly integrated activities (Interactions, relations) (Complex)
Complicated Systems

Designed based on a defined set of rules

Collection of inter-related individual components

Reliable: Designed such that functioning whole is dependent on collection of parts
- MTBF
- FMEA
- SPV

Complicated: can disassemble it, put it back together and it still works

\[ Risk = \sum_{i=1}^{k} c_i p_i \]
Complicated Systems (continued)

- Fault Tree Analysis
- Add redundancies
- Lower Risk
- Reduce variability
  - Get rid of people
  - More training
  - PM
  - PdM
  - FMEA
  - SPV
  - Better operating procedures
  - Lower Risk
  - Get rid of people
  - More training
  - PM
  - PdM
  - FMEA
  - SPV
  - Better operating procedures
(a) Product of unreliable system components
(Complicated)

(b) Product of improperly aligned, or poorly integrated activities
(Interaction, relations)
(Complex)
The complicated aircraft is now suddenly a complex system.
Complex Systems (continued)

Almost an organic process

Fundamental understanding of wholistic system >> one person's knowledge

Things not hardwired but loosely coupled

Diversity of inputs

Perception and perspective can vary widely

Interdependencies versus dependencies

Collection of inter-related individual components with specific design rules does NOT apply

No SPV

Inter-relationships unclear

Large variability of actions that no longer have a direct link from stimulus to output

Risk
Complex Systems (continued)

Normalisation of deviations (reduced safety merging)

Technical depth (or lack thereof) of staff at given moment

Results are path and time dependent

Risk Tolerance / Risk Rationalisation by individual staff

Risk appetite of organisation (senior managers, supervisors)

Culture feeds off historical normal

Results are path and time dependent
Reactive decision making is risky business

Problem: Where is acceptable risk? (and by whom)
Answer: You only really know where the boundary is when you cross it.
Man’s ability to conceptualise, design and construct a technology often outstrips mankind’s ability to operate it

**Event → Accident investigation → Reconstruct**
The event puzzle using Newtonian cause/effect → distill down to the root cause (often human error) → building in future defences

Has served us well over the years, and is powerful
How to deal with complex systems:

- The more exotic the system, the more exotic the problems, and the need for exotic solutions....
- Some ideas to get a foothold:
  1. Talk about risk frequently
  2. Carry out gap analysis between expectations and behaviours in the field “you get what you inspect, not expect”
  3. Actively solicit diverging opinion to (avoids intentional blindness)
  4. Debate “acceptable boundaries”
  5. Discuss antecedents for people’s behaviours including the ‘unofficial messages’
  6. Never allow doubt and uncertainty to go unchallenged
How to deal with complex systems (continued)

7. Demand proof it is safe to operate, not unsafe to operate
8. Demand Operational Decision Making (ODM) forums discuss the above when debating a new issue
9. Create a Nuclear Safety Culture Monitoring Panel (NSCMP) to meet quarterly to:
   a) Discuss the above
   b) Construct the puzzle without first knowing the final picture, ie: avoid the event instead of reacting to it