



The Precautionary Principle and Defense in Depth

George E. Apostolakis
Massachusetts Institute of Technology
apostola@mit.edu

Presented at the Second ILK Symposium
Munich, October 28, 2003

MIT Department of Nuclear Engineering

1



The Precautionary Principle

- **Its scope covers “those specific circumstances where scientific evidence is insufficient, inconclusive or uncertain and there are indications through preliminary objective scientific evaluation that there are reasonable grounds for concern that the potentially dangerous effects on the environment, human, animal or plant health may be inconsistent with the chosen level of protection.”**

[Communication from the Commission of the European Communities, COM (2000) 1, 2/2/00]

MIT Department of Nuclear Engineering

2



What is it?

- **“A prudent and sound choice of response in the face of uncertainty.”** [Precau-Pri Project, Renn et al, 2003]
- **It applies when there is no sufficient probability of future harm, yet there is reason to believe that such harm may occur.**
- **It is a form of risk management.**
- **“It is a rhetorical statement that provides government a public welfare masquerade for an indefinite deferment of a long-term policy response.”** [Starr, 2003]



The Nuclear Power Example

- **The history of nuclear reactor safety may provide insights regarding the value of caution and risk assessment.**
- **The landmark event is the publication of the Reactor Safety Study (WASH-1400) in 1975.**



Pre-PSA Era (before 1975)

- Probabilities of accidents were not quantified at the time.
- The core damage frequency (CDF) was thought to be very low.
- The accident consequences were thought to be disastrous.
- **Precautionary attitude prevailed leading to:**
 - Conservative design and operations
 - Defense-in-depth
 - Large safety margins



Defense in Depth

“Defense-in-Depth is an element of the Nuclear Regulatory Commission’s safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility.”

[Commission’s White Paper, USNRC, 1999]



Post-PSA Era (after 1975)

- **The system is analyzed as a socio-technical system.**
- **Some uncertainties are quantified.**
- **Previously unknown contributors to risk are identified (e.g., ISLOCA).**
- **CDF estimates higher than previously believed.**
- **Accident consequences significantly smaller.**



Lessons Learned

- **Beliefs without a risk assessment can be wrong.**
- **Precautionary measures are not always conservative – some important failure modes were missed.**
- **In some instances, unnecessary regulatory burden is imposed wasting valuable resources.**



Evolution of PSA Use

Phase 1

- **The value of the methodology is questioned by safety experts who are uncomfortable with the explicit quantification of judgment.**

Phase 2

- **Vulnerabilities identified by PSA are dealt with.**

Phase 3

- **Unnecessary safety requirements (“regulatory burden”) are removed.**



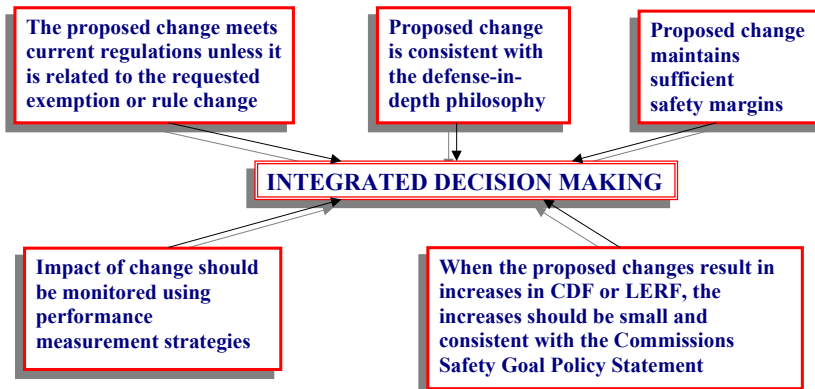
Caution Prevails

“The use of PRA technology should be increased in all regulatory matters to the extent supported by the state of the art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.”

[Commission's Policy Statement, USNRC, 1995]



The Decision-Making Process of Regulatory Guide 1.174



Preserving the DiD Philosophy

- A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation.
- Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided.
- Defenses against CCFs are preserved.
- Independence of barriers is not degraded.
- Defenses against human errors are preserved.



ACRS Interpretations of DiD

- **Structuralist:** DiD is embodied in the structure of regulations and in the design of the facilities built to comply with those regulations. “What if this barrier or safety feature fails?” (**Precautionary attitude**)
- **Rationalist:** DiD is the aggregate of provisions made to compensate for uncertainty in our knowledge of accident initiation and progression.



The Concerns

- Arbitrary appeals to the structuralist interpretation of defense-in-depth might diminish the benefits of risk-informed regulation.
- Strict implementation of risk-based regulation (the rationalist interpretation of defense-in-depth) without appropriate consideration of the structuralist defense-in-depth could undermine the historical benefits.



We continue to be surprised

- **Recent events have shaken our confidence in our assumptions.**
 - “The NRC and DBNPS failed to adequately review, assess, and followup on relevant operating experience.”
 - “DBNPS failed to assure that plant safety issues would receive appropriate attention.”
 - “The NRC failed to integrate known or available information into its assessments of DBNPS’s safety performance.”

[Davis Besse NPS Lessons-Learned Report, USNRC, September 30, 2002]



The ACRS Pragmatic Approach

- **Apply defense-in-depth (the structuralist approach) at a high level, e.g., the ROP cornerstones (e.g., IEs, Safety Functions).**
- **Implement the rationalist approach at lower levels, except when PSA models are incomplete. Revert to the structuralist approach in these cases.**



Conclusions

- **Responsible decision making bodies have been conservative in the face of large and unquantified uncertainties.**
- **Conservative approaches turn out to be not so conservative in some cases.**
- **Risk assessment is the rational way for us to identify what we know and what we don't know.**
- **The need for a precautionary principle is questionable.**



Selected References

- G. E. Apostolakis, "How Useful Is Quantitative Risk Assessment?" *Risk Analysis*, to appear.
- E. S. Beckjord, M. C. Cunningham, and J. A. Murphy, "Probabilistic Safety Assessment Development in the United States 1972-1990," *Reliability Engineering and System Safety*, 39 (1993) 159-170.
- O. Renn et al, "The Application of the Precautionary Principle in the European Union," Center for Technology Assessment, Stuttgart, Germany, April 2003.
- J. N. Sorensen, G.E. Apostolakis, T.S. Kress, and D.A. Powers,, "On the Role of Defense in Depth in Risk-Informed Regulation," *Proceedings of PSA '99, International Topical Meeting on Probabilistic Safety Assessment*, pp. 408-413, Washington, DC, August 22 - 26, 1999, American Nuclear Society, La Grange Park, Illinois.
- C. Starr, "The Precautionary Principle versus Risk Analysis," *Risk Analysis*, 23 (2003) 1-3.
- U. S. Nuclear Regulatory Commission, WASH-1400, *Reactor Safety Study, An Assessment of Accident Risks in U. S. Nuclear Power Plants*, (NUREG-75/014), 1975.
- U.S. Nuclear Regulatory Commission, "Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement," *Federal Register*, Vol. 60, p. 42622, August 16, 1995.
- U. S. Nuclear Regulatory Commission, Regulatory Guide 1.174, *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis*, June 1998.