Lessons from the Nuclear Risk-Informed Assessments

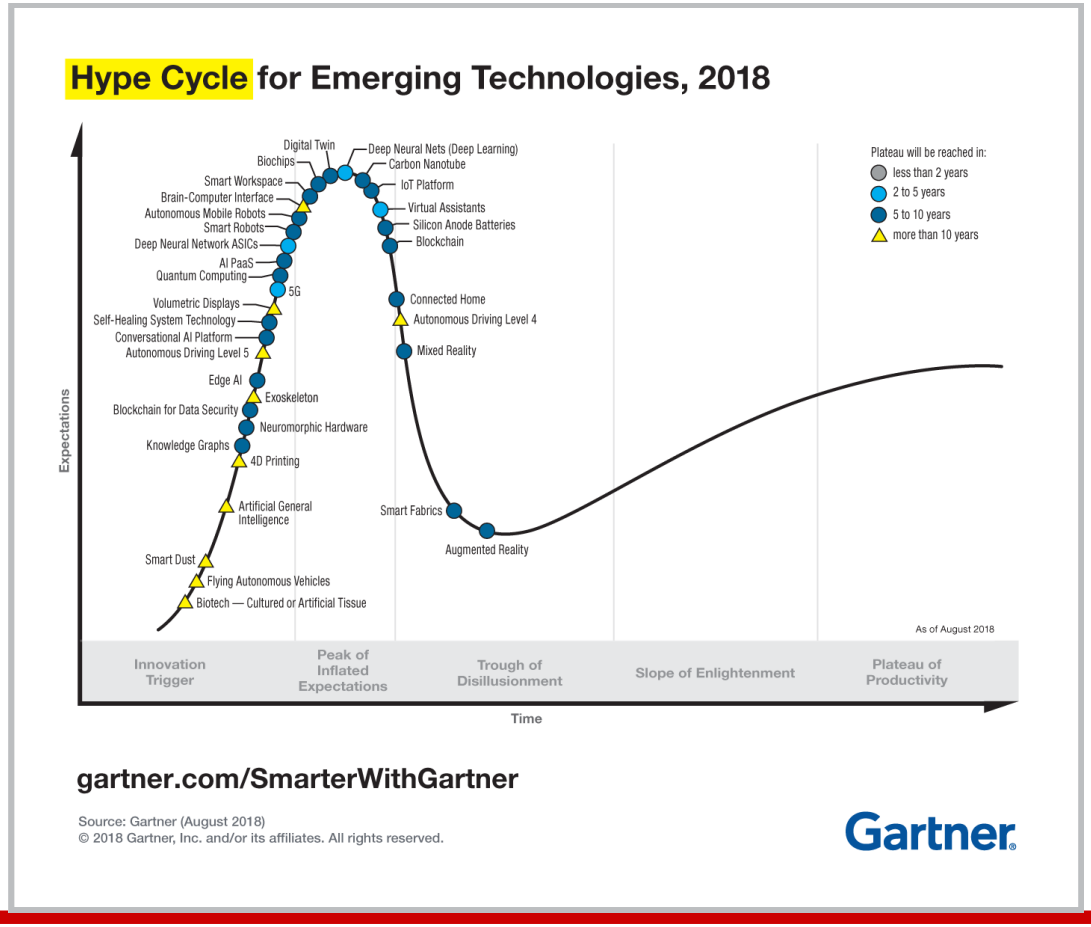
Mohammad Modarres
Center for Risk and Reliability
University of Maryland

Topics

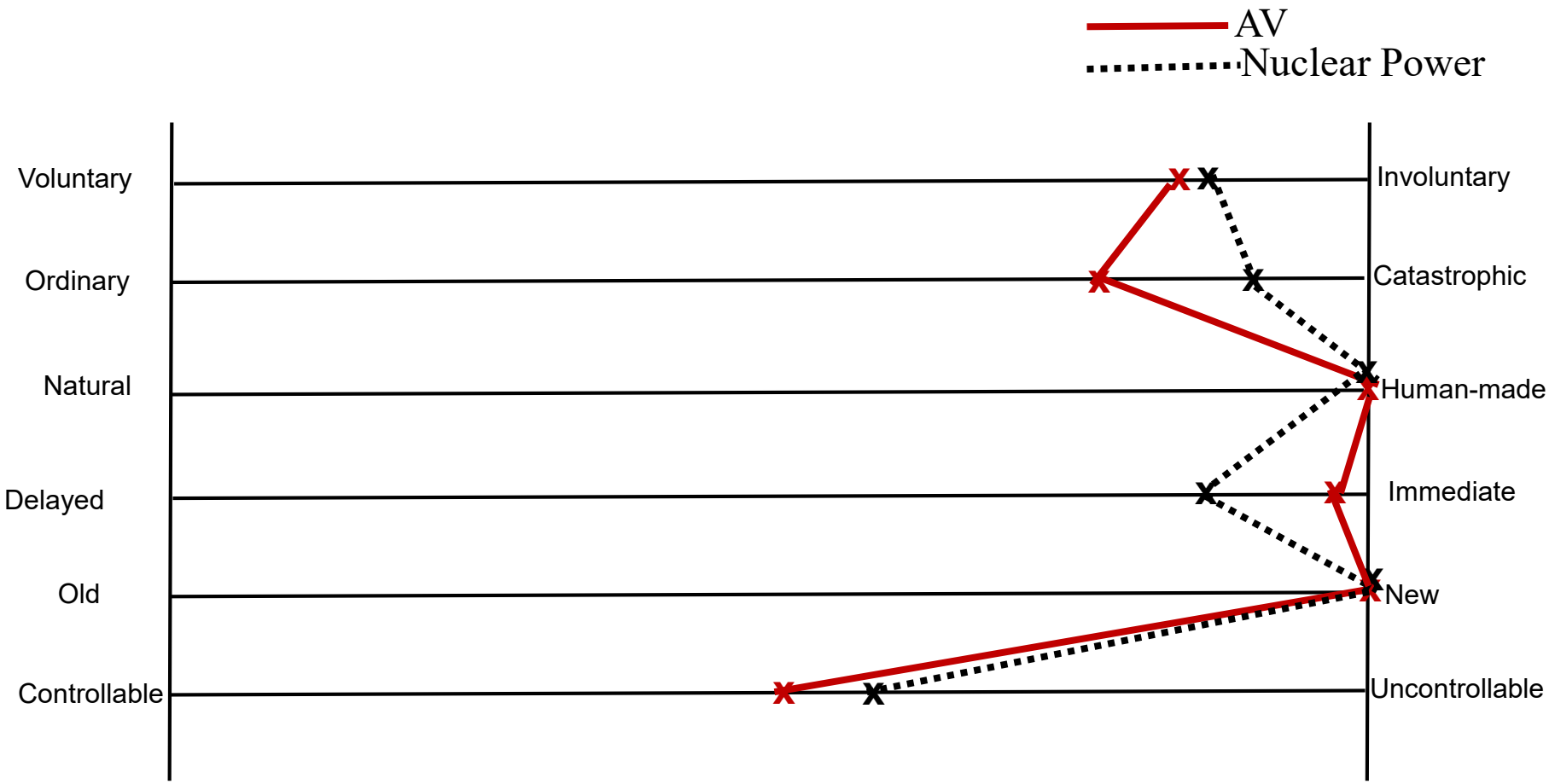
- Similarities and differences of safety and risk characteristics of AVs vs. nuclear technologies
- A quick history of safety considerations in the nuclear industry
- Emergence of "risk-informed" safety assessment
- What can we learn from nuclear safety experience
- Conclusions

Hype Cycle

- New technologies AVs and Nuclear included experience the so-called "Hype Cycle"



A Psychometric Risk Profile Comparison of Risks from AVs and Nuclear Power



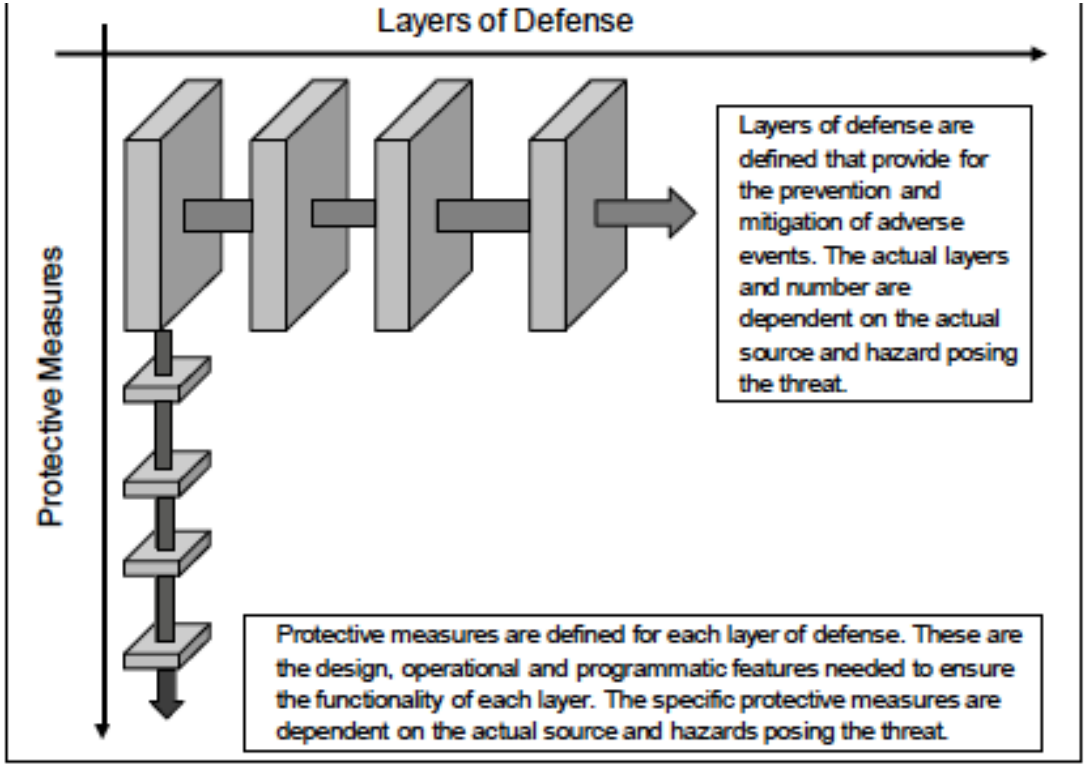
Some Nuclear Safety History

- U.S. Atomic Energy Act of 1946 rested atomic technology and military applications with Government

- U.S. Atomic Act of 1954 ended the government's monopoly and allowed peaceful uses provided that: " . . . a *reasonable assurance* exists that such uses would not result in undue risks to the health and safety of the public"

Defense-in-Depth (DiD) Became A Safety Design Principle

DiD evolved into a collection of design and operating reqirements to overcome lack of precise knowledge



NEI, Modernization of Technical Requirements, Draft 9/2018

Defense-in-Depth (Cont.)

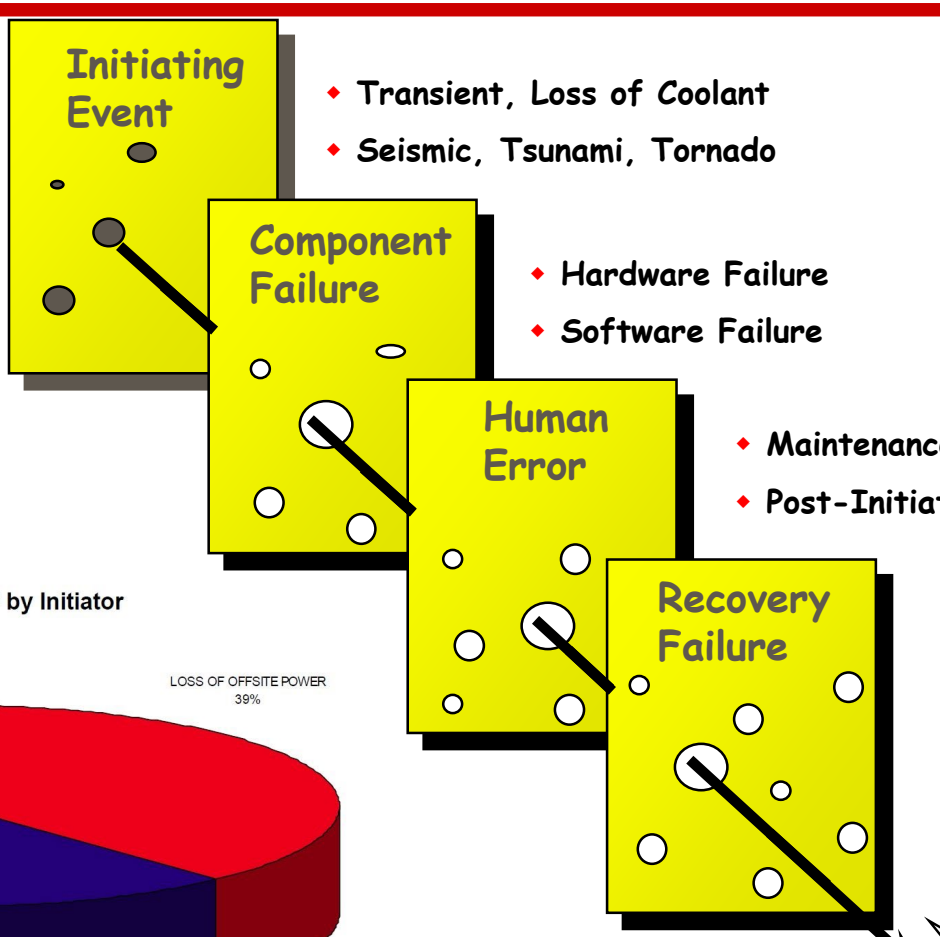
Acceptance criteria needed to measure adequacy of DiD

- Withstand a fixed set of accident scenarios *judged* by experts as most significant adverse events or the so-called "Design Basis Accidents (DBAs)"
- Assumed a plant that could handle the DBAs, it will handle any other accident
- Reasonable assurance was interpreted as conformance to the body of regulations on the basis of DiD.
- Acceptances criteria measured deterministically with conservative methods, tools and bounds

Emergence of Probabilistic Risk Assessment (PRA)

- In the mid-1960s, concerns such as containment integrity under loss of reactor coolant paved the way for use of PRA to address the shortcomings of the DBAs
- PRA was to model more realistic accident scenarios
- PRA was meant to answer: What can go wrong?, How likely is it? What are its consequences?
- The landmark WASH-1400 study commissioned by the AEC (later NRC) in 1972-1975, developed the concept, practice and realistic examples of PRA

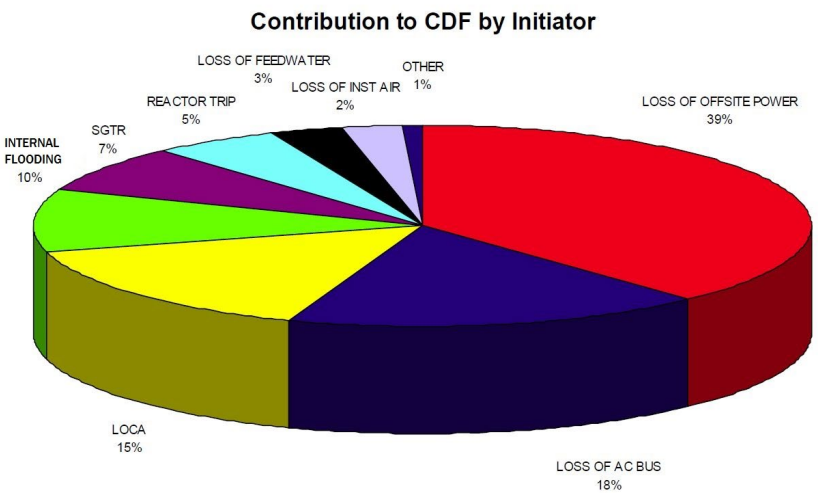
Key Elements of a PRA



- Transient, Loss of Coolant
- Seismic, Tsunami, Tornado

- Hardware Failure
- Software Failure

- Maintenance/Design Errors
- Post-Initiator Errors



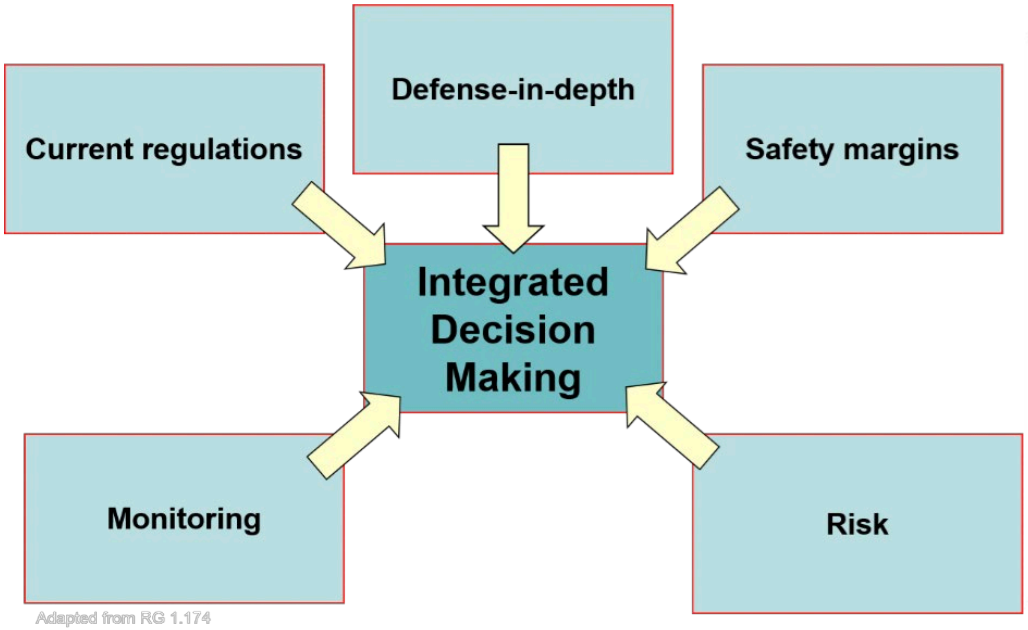
Source: Nuclear Regulatory Commission

Pre- & Post-WASH1400

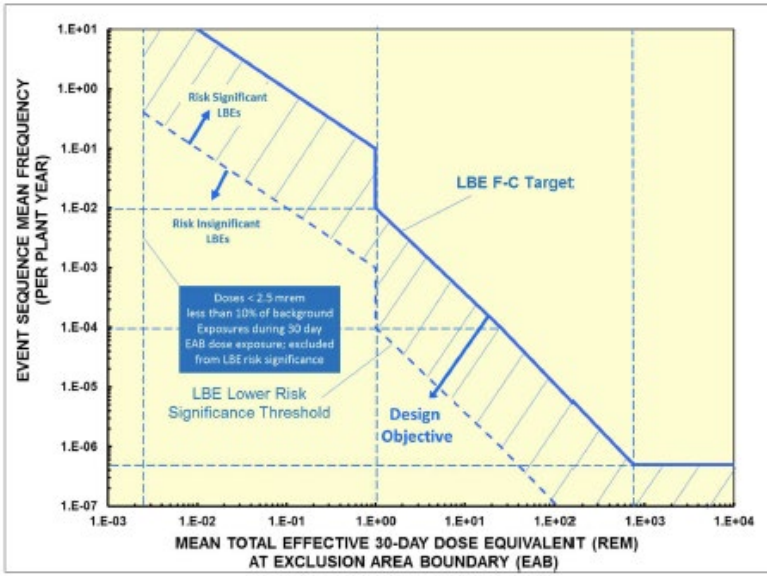
- Pre:
  - Protect again large loss of coolant
  - Core damage is unlikely < 10^{-8} per year
  - Consequences are disastrous
- Post:
  - Small loss of coolant and transients are more important
  - Core damage is more likely than believed ~5×10^{-5}
  - Consequences are significantly smaller
  - Support systems and human actions are very important
- Based on political and technical factors NRC in late 1978 withdrew its support of PRA
- TMI accident a few month later in March 1979 was consistent with WASH1400 conclusions

Risk-Informed Regulation

- NRC developed a set of qualitative safety goals and qualitative (probabilistic) safety objectives
- NRC developed a PRA Policy Statement and reformed its safety regulation to "risk-informed"



Adapted from RG 1.174



Lessons of Risk-Informed Approach that Applies to AV Safety?

- Formal PRA models can provide important realistic static and dynamic scenarios and contributors to accident risks in design and operation of AVs
- The PRA models can be updated through streams of sensor data, weather and road conditions, state of the vehicle and the entire fleet of related vehicles
- PRAs may serve in support of risk management and policy decision making to predict, avoid and mitigate road accidents
- PRA can learn by updating its risk models with near-miss events and specialize itself to a specific car, driver and region
- Data on significant near miss events can be shared among manufactures

Risk-Informed Autonomous Action

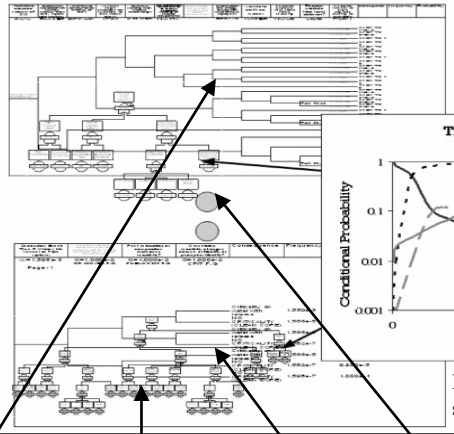
Decision Module

Dynamic Probabilistic Scenario Generator/Simulator

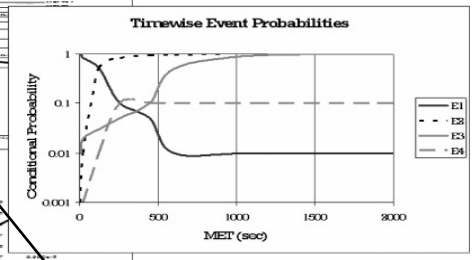
Risk-Informed Assessment Module

Policy/ Insurance Decisions

Operator Behavior Module



Probabilities change as a function of time



From: Mike Franke: quasi-dynamic PRA structure for space reactor

Analytics and Deep Learning Module

Data Processing/Filtering Module

Conclusions

- Old methods of safety analysis may be insufficient for complex technologies such as AVs
- Major accidents could prove disastrous to the vitality of the industry
- Risk-informed performance-based approaches could characterize all uncertainties including engineering ones into the operation, policy and regulation of AVs
- Risk-informed methods empower innovation and lead to better design, adequate safety features and sound policy

Thank you!

Questions?