Level 1 PRA

Hymie S. Shapiro, Principal Engineer - PSA

Presentation to US Nuclear Regulatory Commission

Washington DC

May 8, 2003

AECL
TECHNOLOGIES INC.

PRA Applications

- Design Assist Role:
  - Confirm adequacy of safety design
  - Redundancy & functional separation of mitigating system
  - System interface & capability requirements
  - Assessment of potential design options for risk reduction
  - Recommend design changes based on cost benefit assessment
- Provide input to Environmental Qualification program; identify equipment requiring protection against:
  - Steam, radiation, pipe whip
- Risk Evaluation - Estimate of severe core damage frequency

PRA Applications….

- **PRA Role in Operations:**
  - Provide input to test and maintenance programs, so that these can be optimized in terms of cost and safety
  - Identify maintenance restrictions
  - Outage planning
  - Risk impact of changes in plant configuration, test frequencies, on line series/parallel equipment maintenance
  - Input to Technical Specifications (e.g., impairment levels for Special Safety Systems)
  - Identify safety critical components

PRA Applications….

- Develop understanding of integrated plant response to accidents
- Identify operator actions, alarms and annunciations and thus input to control centre designs and Emergency Operating Procedures (EOPs) for accident mitigation
- Licensing role
  - Establish a comprehensive list of initiating events for safety analysis
  - Risk informed regulation
  - Ranking of safety critical systems
- Assessment of containment performance for severe core damage accidents
- Assessment of severe accident mitigation design accidents (SAMDA)

Early (1970-1980) PRA Input to CANDU 6 Design

- Gravity fed cooling from reserve feedwater tank for feedwater pumps and air compressors
- Second automatic auxiliary boiler feedwater pump (or auto depressurization of steam generators (SGs) and gravity feed from dousing tank to SGs) to cater to station blackout
- Automated source of make-up to recirculated cooling water (up to 1" pipe break)
- Local air tanks for aux feedwater control valves
- Hardwired boiler level control feature to cater to loss of computers, instrument air
- Second source of bearing cooling water for raw service water pumps
- Hardwired windows annunciations on Reactor Inlet Header (RIH) high temperature - complements other indications of degradation of boiler heat sink, e.g. boiler low level, low boiler feed line pressure etc.

Design Changes

Station Design Change Requests (DCRs) from Early PRA Studies

STATION	DESIGN CHANGES
Gentilly-2* – (Oct. ‘83)**	92
Point Lepreau* – (Feb. ‘83)**	66
Wolsong Unit 1* – (Apr. ‘83)**	37
Pickering “B” – 4 units (May ‘83, Feb. ‘84, Jan. ‘85, Feb. ‘86)**	22
Bruce “B” – 4 units (Mar. ‘85, Sep. ‘84, Apr. ‘86, May ‘87)**	17

Approximately 80% of the approved design changes were with the balance of plant and service systems (non-nuclear portion)

* CANDU 6 Station
** In-Service Date

PRA Based Design Proposed Changes for Recent (Wolsong, Qinshan) CANDU 6 Designs

- Shutdown cooling (SDC) pump gas locking during drained state: design changes and procedures to avoid and/or cope with gas locking of SDC pumps - e.g., low motor amp alarms, maximize difference between SDC take-off line and drained state level
- Emergency Power Supply/Emergency Water Supply (EPS/EWS) for Local Air Coolers for containment integrity
- Design simplification and/or procedures to facilitate monthly testing of the SDC
- Duplicate EWS Valves to Steam Generators - reduction in loss of heat sink frequency

PRA Based Design Proposed Changes for Recent (Wolsong, Qinshan) CANDU 6 Designs

- Lessons from Wolsong 2/3/4 PRA - e.g., EWS building bracing, additional lateral restraints for battery racks, anchorage of Motor Control Centres and transformers
- Field start capability of auxiliary feedwater pump to cope with main control room fires
- Moderator make-up for postulated feeder stagnation break and end fitting ejection
- 24 Hour Main Steam Safety Valve Capacity after Loss of Instrument Air thus eliminating operator dependence to gag open the valves
- Confirmation of feedwater supply by gravity feed from deaerator to depressurized boilers
- Protection of Class IV (offsite power) switchgear, feedwater, recirculated cooling water and instrument air from main steam line break inside the turbine building

ACR PRA Status

- PRA is further used in an up-front design assist role of ACR
  - RSW/RCW division concept
  - 2 phase versus 3 phase transformers
  - Setting reliability targets for frontline and support systems
  - Steam generator as a heat sink reliability
  - Compressed air design concept
- ACR PRA Scope
  - Internal Events – includes full power and shutdown state
  - External Events – PRA based seismic margin, internal fire and floods
  - Level 1 and Level 2 PRA
- ACR PRA program is consistent with international practice. The same PRA methodology is applied to the Pt. Lepreau Refurbishment

ACR PRA Status (Cont'd)

- Initiating Events
  - Systematic plant review for initiating events identification
  - Frequencies based on CANDU or International NPP operating experience
- Event Trees
  - Event Trees with post-IE operator explicitly modeled
- Fault Trees
  - Reliability data
    - components based on Darlington A Risk Assessment (DARA)
    - Human data based on ASEP of USA
    - Common Cause Failure - Unified Partial Method, CCF-UPM, (partial beta) model

Current Level 1 PRA Tools (Data Systems and Solutions)

- CAFTA For Windows
  - Event Tree editor
  - Fault Tree Analysis
  - Building, Editing & Plotting the Fault Trees
  - Building of the Reliability Database
  - Cutsets editor
- CSRAM: allows solution of initiating event frequency fault tree
- GTPROB: companion code with CAFTA for intermediate gate probability calculation
- PRAQUANT: accident sequence quantification
- UNCERT: uncertainty analysis

Initiating Event Identification

- Include pertinent events from CNSC's Document C6, and
- Perform Systematic Review of Plant Design - Master Logic Diagram, and
  - Identify main systems containing radionuclides
  - Systematically examine potential ways of displacement of radioactive material from their normal location
  - Group events of logic diagram based on similarity of plant response
- Plant operating experience - significant event report review, and
- Design Reviews

Initiating Event Frequency Estimates

- Base case analysis - best estimate (mean) values,
- Base case event frequency estimate:
  - > 10 occurrences, use average
  - 1 – 10 occurrences, use chi square distribution for 50% confidence limit
  - 0 occurrences – variety of methods (e.g., LWR experience review, etc.)
  - For certain events, event frequency is estimated by fault tree analysis
- Uncertainty is ratio of 95% confidence to 50% confidence level values (called error factor ranges from 2 to 10)

Common Cause Failure (CCF) Analysis

- **CCFs are dependent failures which compromise the purpose of diversity and redundancies, e.g.:**
  - defective manufacturing process
  - component design errors
  - harsh environment (smoke, high temperature, humidity)
  - inadequate test, operating or maintenance procedures
  - human errors
  - external hazards (RFI/EMI)
- **For CANDU 6 PRA, UPM approach (partial beta model is being used)**
  - allows β factors to be assigned based on design assessment
  - Developed by Safety Reliability Directorate (SRD - UK)
  - quantitative aspects from historical data of PWRs in US and Europe

CCF Analysis – Evaluation Criteria

- **8 evaluation criteria:**
  - redundancy and diversity
  - separation
  - level of understanding (years of operation, complexity, etc.)
  - prior analysis of system (fault tree)
  - man-machine interface
  - safety culture
  - control of operating environment
  - environmental testing

CCF Example - Separation

Components in same room

Components separated by barrier

Components in adjacent rooms

Components in non-adjacent rooms

Components in separate buildings

Decreasing partial beta-factor

Typical CCF Analysis Results from Earlier PRAs

FAULT TREE DESCRIPTION	UNAVAIL WITHOUT CCF	UNAVAIL WITH CCF
EWS: manually initiated dousing tank flow to SGs	1.44e-3	2.10e-3
EWS: manually initiated pumped flow to SGs	1.72e-2	1.85e-2
EWS: auto initiated dousing tank flow to SGs	1.37e-2	1.5e-2
EWS: manually pumped and dousing tank flow to SGs	1.44e-3	1.76e-3
EPS to ODD 4.16 kV bus	1.65e-2	2.12e-2

CCF Analysis – UPM Methodology

- **Unified Partial Method (UPM)**
  - **UPM criteria fulfills a design audit role, providing designers with an indication of best practices and their quantitative impact**

    (AECL has applied this methodology on CANDU 9 and Generic PRA; it is being used for the Pt. Lepreau Refurbishment PRA)

Human Reliability Analysis

- HRA approach is based primarily on ASEP (NUREG 4772)
- Pre Accident
  - Calibration, test, maintenance errors
  - Dependency effects
- Post Accident Errors:
  - Errors of diagnosis + execution
- Risk Dominant Sequences – (Use THERP- Handbook)

Human Reliability Analysis

- AECL HRA approach is based primarily on ASEP (NUREG 4772)
- Pre-Accident (e.g., calibration, test, maintenance) errors:
  - Basic HEP for any task is 3×10^{-2}
  - Apply Recovery Factors ranging from 10^{-4} to 10^{-1} e.g.:
    - for a compelling signal like a window alarm, RF = 10^{-4}
    - for task verification by a second person, RF = 10^{-1}
  - For actions performed on redundant components, dependency effects are considered
- Post Accident Errors:
  - Errors of diagnosis as well as execution are modeled

Post Accident HRA

	HEPs for Errors of Diagnosis	
Diagnosis Time (minutes)	Joint HEP (Entire MCR Room Team)	Error Factor (EF)
0-15	1.0	----
16-20	1E-01	1.0
21-30	1E-02	1.0
31-60	1E-03	1.0
61-240	1E-04	3.0
241-480	1E-05	3.0

Post Accident HRA ...

Post Accident Execution Errors								
Post-Diagnosis Actions (Execution)	Step-by-Step Task Moderate Stress		Step-by-Step Task Extreme Stress		Dynamic Task Moderate Stress		Dynamic Task Extreme Stress	
Operator	HEP	EF	HEP	EF	HEP	EF	HEP	EF
Original Performer	2E-2	5	5E-2	5	5E-2	5	2.5E-1	5
Second/Third Operator - Credit only if > 30 min and > 60 min available	2E-1	5	5E-1	5	5E-1	5	5E-1	5
For Seismic, apply a PSF of 5 to 10								

Recovery Analysis

- **Overview:**
  - Application of post-accident operator actions at the cutset level following accident sequence quantification
  - At cutset level, it is possible to identify the nature of the mitigating system failure (e.g., dormant failure or failure during mission)
  - Depending on the timing of the failure during mission, recovery actions can be credited

Recovery Analysis…

- **Type of Recovery Actions:**
  - **Class IV power restoration (from 30 min to 12 hours)**
  - **Restore System Service Transformer within 12 hours**
  - **Transfer of SDC mode to main coolant pump mode after 1 hour**
  - **Connect Nitrogen bottles to boiler feedwater and condensate supply regulating valves**
  - **Trip main coolant pumps 1 hour after LOCA (from switchgear room)**

Shutdown State PRA

- A shutdown state PRA addresses additional concerns such as:
  - simultaneous system unavailability during different configurations of outage (e.g., reactor coolant system full, drained)
  - importance of operator actions to restore functions
  - maintenance restrictions to various mitigating and safety systems while the plant is in a specified shutdown state

Main Elements of Shutdown State PRA

- Systematically identify low power and planned outage configurations
- In consultations with Operations group, identify/establish maintenance restrictions
- Modify system fault trees to account for system/equipment outage
- Detailed HRA since most mitigation actions need operator action
- Event tree analysis for the postulated events
- Recovery analysis
- Uncertainty and sensitivity analysis

Lessons Learned from Severe Core Damage Accident Analysis from CANDU GPSA

- **CANDU design is inherently robust by having lots of water inventory in the moderator and calandria vault, allowing time for severe core damage accident management before the containment fails**
- **Separation philosophy helps to ensure low severe core damage frequency**

Lessons Learned (Cont'd)

Insights from Wolsong 2/3/4 Design

- Fragility analyses of structures and components provide confidence there is no cliff edge when seismic event is greater that DBE (e.g., EWS pump house)
- Bolting materials for component supports important
- Masonry block walls in electrical switchgear rooms need reinforcement
- Battery racks need support to ensure integrity for mild earthquake
- Increased drain size and automatic RSW pump trip to cope for RSW expansion joint failure in RSW/RCW heat exchanger pit area (implemented on Qinshan CANDU)
- Walk downs have been performed in support of fire, seismic and flood PRA for Pt. Lepreau Refurbishment. Feedback from these walkdowns is applied to ACR

Initial Training for External Events PRA

- External Events considered:
  - Seismic
  - Internal fires
  - Internal floods
- Initial training provided by EQE & PLG (U.S. Consultants)
- Training during Analysis Phase by KOPEC (1.5 years)
- Completed seismic and fire walkdown training at Pt Lepreau with EQE, PLG and NB Power in 1998
- Second seismic and fire walkdown training at Pt Lepreau with senior AECL and NB Power staff in 2002

Elements of Seismic Walkdown

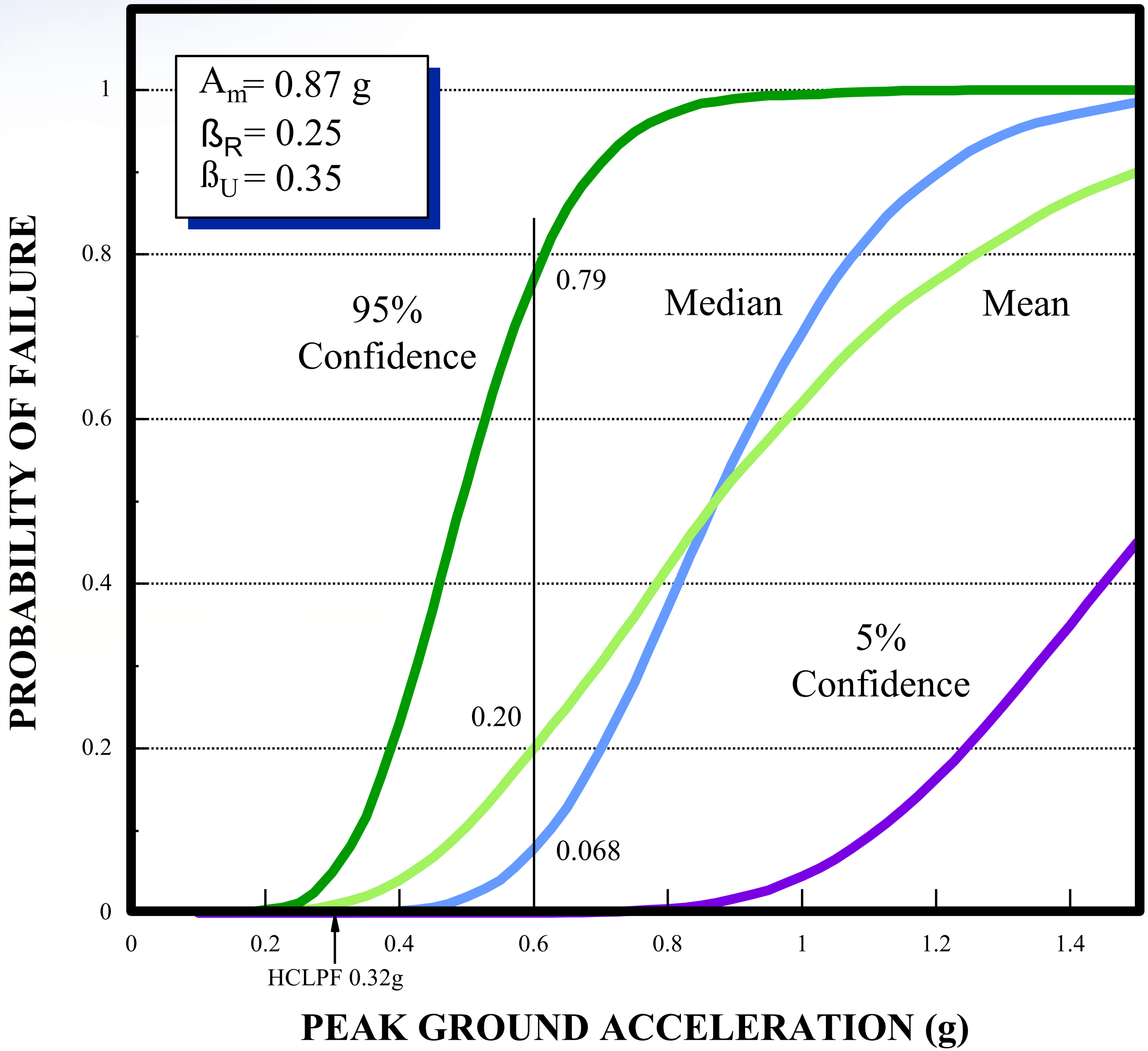
- **Seismic Walkdown**
  - Identify all equipment items that are expected to have sufficiently high seismic capacities to be screened out
  - Define failure modes for components not expected to have high seismic capacities
  - Gather detailed information on equipment and structures for performing seismic fragility evaluations
  - Observe and record any deficiencies
  - Identify spatial interactions
  - Identify areas for potential seismic induced fires (storage of flammable liquids or gases)

Steps of PRA-Based Seismic Margin Assessment

- **Select structures/components for seismic capacity analysis**
- **Review Internal Events PRA Model and Results**
- **Perform seismic capacity analysis**
- **Identify seismically induced Initiating Events. Develop seismic event trees for these initiating events**
- **Develop seismic Fault Trees (FTs) (based on internal event FTs)**
- **Generate Minimal Cutsets for Seismic-Induced Severe Core Damage Sequences**
- **Calculate the HCLPF value for each seismic severe core damage sequences**

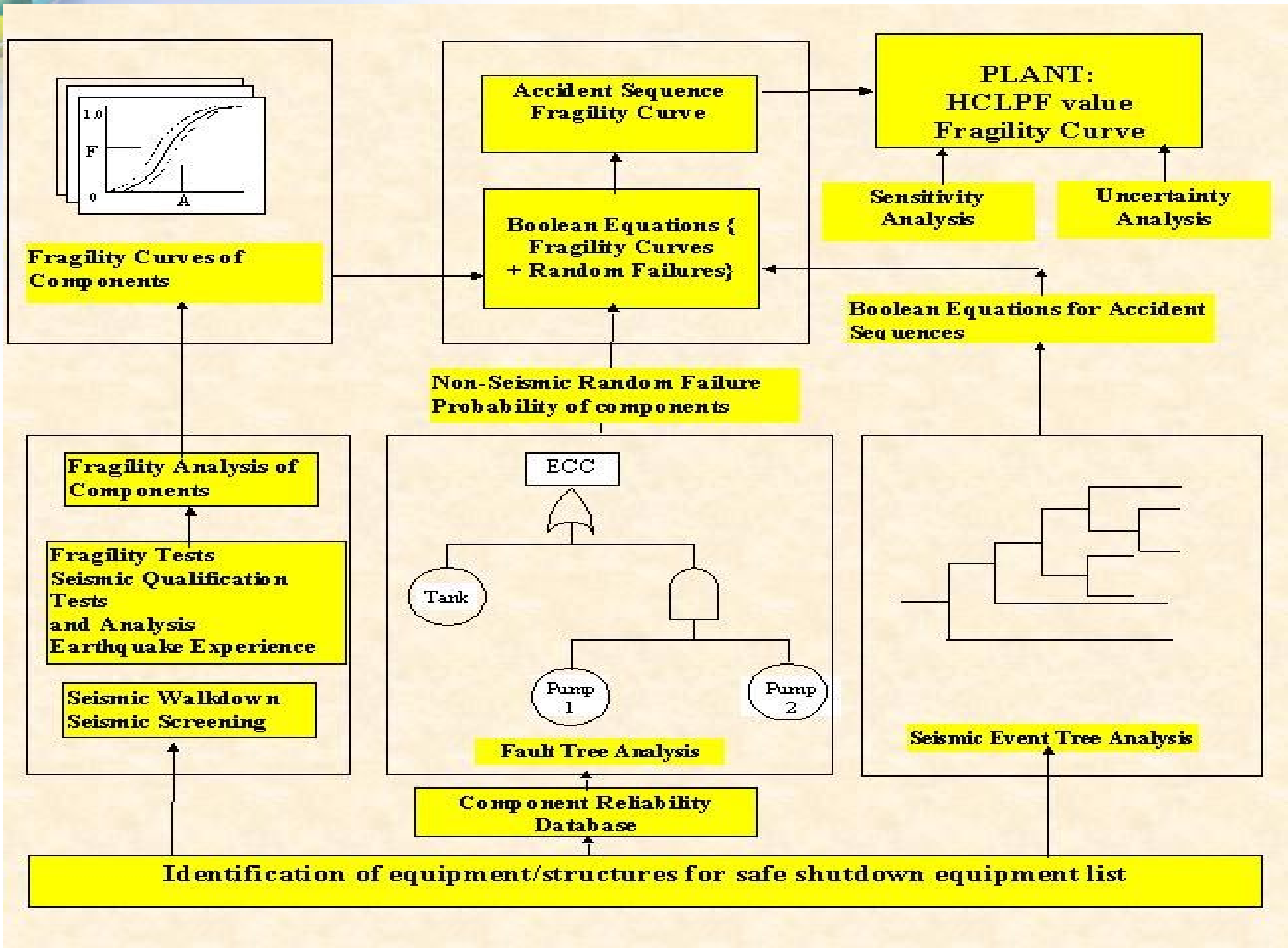
<u>The plant HCLPF is the lowest sequence HCLPF</u>

Seismic Fragility Curves



Acceptance of Seismic Margin Assessment (SMA)

- Our understanding is that:
  - 62 IPEEEs submittals to NRC are SMA
  - 41 IPEEEs are PRAs
- PRA based SMA performed for new (ALWR type) designs:
  - KNGR, AP600, EUR
- Recommendation for adopting PRA based SMA is based on (SECY 93-87)
  - Does not convolute fragility with hazard curves
  - Provides all the benefits of PRA without having to account for large uncertainties in hazard curves
  - Aim to have a plant HCPLF of 0.5g (1.67 times of the DBE)


1.0
F
0
A
Fragility Curves of Components
Accident Sequence Fragility Curve
PLANT: HCLPF value Fragility Curve
Boolean Equations { Fragility Curves + Random Failures}
Sensitivity Analysis
Uncertainty Analysis
Boolean Equations for Accident Sequences
Non-Seismic Random Failure Probability of components
Fragility Analysis of Components
Fragility Tests
Seismic Qualification Tests
and Analysis
Earthquake Experience
Seismic Walkdown
Seismic Screening
ECC
Tank
Pump 1
Pump 2
Fault Tree Analysis
Seismic Event Tree Analysis
Component Reliability Database
Identification of equipment/structures for safe shutdown equipment list

Fire PRA Approach

- Identify Ignition Sources: Fire Hazard Assessment for ACR and/or CANDU 6 Equipment Data Base where applicable
- Estimate Fire Frequency: CANDU Fire Data Base
- Identify PRA-Credited Equipment: CANDU 6 Equipment Data Base and Train/Channel Based Assumption for the Cables
- Perform screening analysis to identify Potential Significant Fire Areas
- Evaluate Fire Growth and Propagation: COMPBRN IIIe or hand calculation
- Develop Fire Scenarios Including Fire Detection and Suppression Probability
- Estimate conditional core damage probability (CCDP) for Each Fire Scenario
- Estimate Severe Core Damage Frequency (SCDF) combining the Fire Scenario Frequency and CCDP
- Sensitivity Analysis and Insights for Risk Management

Fire Frequencies for the Categories of Fire Event Sources

Category ID	Category Name	Mean Frequency (events / plant / year)
1	Battery	1.29E-03
2	Battery charger	2.35E-03
3	Inverters	1.01E-03
4	Main control room	3.06E-03
5	Digital control computers	4.15E-03
6	Diesel generator sets	2.25E-02
7	HVAC equipment	3.26E-03
8	Dryers	5.27E-03
9	Hydrogen fires	7.50E-03
10	Logic and protection cabinets	1.82E-02
11	PHTS pumps	3.88E-03
12	Pumps	1.17E-02
13	Motor control center	6.38E-03
14	Motors	1.06E-02
15	Motor generator sets	1.34E-03
16	Power and control cables	1.26E-02
17	Low voltage switchgear	7.40E-03
18	High voltage switchgear	1.21E-02
19	Standby generators	1.29E-02
20	Turbine-generator	2.57E-02
21	Main unit transformer	1.15E-02
22	Transformers	1.23E-02
23	Human error	1.89E-02
24	Cable fires by welding/cutting	1.71E-03
25	Transient fires by welding/cutting	2.92E-02

Design Insights from GPSA - Fire PRA

- **The following design features go a long way in reducing fire induced SCDF**
  - **Gravity feed from deaerator storage tank**
  - **IEEE-383 fire retardant cables**
  - **Automatic fire suppression in Reactor Building**

Flooding PRA Approach

- Identify flooding sources in each flooding area
- Identify PRA-Credited Equipment in the Areas of Concern
- Perform screening analysis to identify potential significant flooding areas
- Estimate Flooding Frequencies
- Evaluate Flood Growth and Flood Propagation: Flood Flow Rate, Floodable Volume, Flood Barrier, etc.
- Develop Flood Scenarios Considering Flood Protection Design Features and Operator Intervention
- Estimate CCDP for Each Flood Scenarios
- Estimate CDF Combining the Flood Scenario Frequency and CCDP
- Sensitivity Analysis and Insights for Risk Management

Design Insights from GPSA - Flooding PRA

- **Low core damage frequency expected**
  - **Automatic CCW pump trip on T/B basement high level**
  - **Automatic trip of RSW pumps on RCW HX pit high level**
  - **Flood/Steam barriers in RCW HX room and feedwater pump room**
  - **Fewer unlimited flooding sources due to air-cooled standby Diesel Generators and RCW cooling of spent fuel pool cooling heat exchanger**

Plant Damage States

- PDS0 - Failure to shutdown
- PDS1- Late loss of core structural integrity with high RCS pressure
- PDS2 - Late loss of core structural integrity with low RCS pressure
- PDS3 - Loss of core cooling with moderator required early as sustained heat sink
- PDS4 - Loss of core cooling with moderator required late as sustained heat sink
- PDS5 - Loss of cooling/inadequate cooling following a LOCA with successful initiation of ECC
- PDS6 - Power cooling mismatch with late ECC injection due to channel failure

Plant Damage States (Cont'd)

- **PDS7- Power cooling mismatch in a single channel with containment overpressure**
- **PDS8 - Power cooling mismatch in a single channel with no containment overpressure**
- **PDS9 - Tritium release**
- **PDS10 - Fueling machine failures**

Uncertainty Analysis

- Primarily deals with assessment of uncertainty in the failure rate database
- Uncertainty (error factor, K):
  - K (error factor) = $\lambda_{95\%} / \lambda_{50\%}$
- UNCERT code is used for quantification of uncertainty
- Required inputs are:
  - K (error factor, range 2 to 10)
  - probability distribution
- In addition to component failure uncertainties, Human Error Probability (HEP) uncertainties are also addressed

Sensitivity Analysis

- **Two objectives:**
  - to test the sensitivity of PRA results to changes in key input assumptions
  - to optimize design by highlighting systems or subsystem which are especially large/small risk contributors - prioritizing plant improvements
- **Typical sensitivity variables in recent PRAs:**
  - mission time for mitigating systems (e.g., 24 hours to 3 months)
  - post accident recovery actions
  - changes in test intervals
  - various maintenance configurations
  - frequency of initiating events and component failure rates

Conclusion

- **AECL has extensive experience in applying PRA as a design audit tool in improving the design of CANDU**
- **The PRA insights from previous CANDUs are being factored into the ACR design**
- **Performing Level 1 and Level 2 PRA will further confirm that the high risk contributors are identified**

AECL

TECHNOLOGIES INC.