Westinghouse Passive Plants Meet Power Company Needs

- **Satisfies all U.S. Utility Requirements (ALWR URD)**
  - Cost, construction, operations advantages demonstrated

- **Major Simplifications Achieved**
  - Construction, design, maintenance & operations

- **Provides New Standard in Safety**
  - Improved safety and risk performance, margins verified

- **Licensing Certainty**
  - Rigorous NRC review & comprehensive test program
  - Assures licensibility for domestic & international sites
Design Bounded By:

- Make it safe
- Meet US regulatory requirements
- Satisfy utility requirements
- Make it simple
- Use proven technology
- Make safety systems passive
- Make it affordable
Naturally Occurring Physical Phenomena Used in Operation of Safety Systems

- Natural circulation of air, water, and steam
- Gravity and gas pressure drive flow of cooling water.
- Natural heat transfer through conduction, convection, and evaporation
- Flow and cooling occur in accordance with nature’s laws - No support systems
- One time alignment of active valves (dc battery actuated)
  - No dc actuation power after 24 hours
- Greatly reduced operator dependency
AP1000 Approach to Safety

- **Passive Safety Systems**
  - Use “passive” process only, no active pumps, diesels, ....
    - One time alignment of valves
    - No support systems required after actuation
  - Reduced dependency on operator actions
  - Mitigate design basis accidents without nonsafety systems
  - Meet NRC safety goals without use of nonsafety systems

- **Active Nonsafety Systems**
  - Reliably support normal operation
    - Redundant equipment powered by onsite diesels
  - Minimize challenges to passive safety systems
  - Not required to mitigate design basis accidents
Major Safety Advancements

- No Reliance on AC Power
- No Operator Action Required to Assure Safety
- Long Term Plant Safety Assured without Active Components (Natural Forces Only)
- Containment is Not Breached for Postulated Design Basis Events
- In Severe Accidents, Reactor Vessel Cooling Keeps Core in Vessel
- Large Margin to Safety Limits
- Defense in Depth - Active Systems Provide ADDITIONAL first line of defense
AP1000 Design Features

- Integrated Power Plant Design
- Simplified RCS Loops with Canned Motor Pumps
- Simplified Passive Safety Systems
- Microprocessor, Digital Technology Based I&C
- No Requirement for Safety AC Power
- Compact Control Room, Electronic Operator Interface
- Optimized Plant Arrangement
  - Construction, Operation, Maintenance, Safety, Cost
- Extensive Use of Modular Construction
Approach to Safety: Defense-in-Depth

- **Simple Passive Safety Systems**
  - Dedicated safety systems - not required for normal operation
  - Use “natural” driving forces - no active pumps, diesels
  - One-time alignment of active valves
  - No support systems after actuation
  - Reduced operator dependency
  - Mitigate design basis accidents without nonsafety systems

- **Simple Active Non-Safety Systems**
  - Reliable active equipment for normal operation
  - Redundant active equipment powered by nonsafety diesels
  - Minimize unnecessary use of passive safety systems
  - Reduce risk to utility & public
Simplicity Applies to Every Element of the AP1000/AP600

- **Simplicity in Design** through reduced number of components and bulk commodities
- **Simplicity in Safety** through use of passive safety systems
- **Simplicity in Procurement** through standardization of components
- **Simplicity in Operation and Maintenance** through use of proven systems and components and man-machine interface advancements
Passive Safety Features: Eliminate the Need for Safety AC Electric Power

- **Passive Decay Heat Removal**
  - Natural circulation heat exchanger connected to Reactor Coolant System (RCS)

- **Passive Safety Injection**
  - Gravity drain core makeup tanks (RCS pressure)
  - $\text{N}_2$ pressurized accumulators
  - Gravity drain refueling water storage tank (containment pressure)
  - Automatic RCS depressurization

- **Passive Containment Cooling**
  - Steel containment shell transfers heat to natural circulation of air and evaporation of water drained by gravity

- **Passive Heating Ventilation Air Conditioning**
  - Compressed air for habitability of main control room (MCR)
  - Concrete walls for heat sink (MCR and C&I rooms)
Passive Containment Cooling
AP1000 Passive Core Cooling System

- **AP600 System Configuration Retained**
- **Capacities Increased to Accommodate Higher Power**
  - Core 1933 MW > 3400 MW or 76%
  - PRHR HX Capacity Increased 72%
  - CMT Volume & Flow Increased 25%
  - ADS 4 Flow Increased 93%
  - IRWST Injection Increased 89%
  - Cont. Recirc. Increased 139%
- **System Performance Maintained**
  - No core uncovery for SBLOCA
    - < DVI line break
    - Large margin to PCT limit
  - No operator actions required for SGTR
AP1000 EHVAC MCR

- Compressed air provides breathable air for operators
  - 72 hours of operation
  - 65 SCFM air flow pressurizes MCF 1/8 in water

- Thermal mass of concrete provides temperature control
Approach to Safety: Defense-in-Depth

- **Simple Passive Safety Systems**
  - Dedicated safety systems - not required for normal operation
  - Use “natural” driving forces - no active pumps, diesels
  - One-time alignment of active valves
  - No support systems after actuation
  - Reduced operator dependency
  - Mitigate design basis accidents without nonsafety systems

- **Simple Active Non-Safety Systems**
  - Reliable active equipment for normal operation
  - Redundant active equipment powered by nonsafety diesels
  - Minimize unnecessary use of passive safety systems
  - Reduce risk to utility & public
Active Nonsafety Systems

- **Active Nonsafety System Functions**
  - Reliably support normal operation
  - Minimize challenge to passive safety systems
  - Not required to mitigate design basis accidents
  - Not required to meet NRC safety goals

- **Active Nonsafety System Design Features**
  - Redundancy to minimize failures effects
  - Automatic actuation with power from onsite diesels

- **Active Nonsafety System Equipment Design**
  - Reliable industrial grade equipment
  - Non-ASME, non-seismic, limited fire / flood / wind protection
  - Availability controlled by procedures, no shutdown requirements
  - Reliability controlled by maintenance program (not maintenance rule)
System Defense In Depth

- AP1000 Provides Multiple Levels of Defense
  - First feature is usually nonsafety active feature
    - High quality industrial grade equipment
  - One feature is safety passive feature
    - Provides safety case for DCD
    - Highest quality nuclear grade equipment
  - Other passive features provide additional defense-in-depth
    - Example; passive feed/bleed backs up PRHR HX
  - Available for all shutdown conditions as well as at power
  - More likely events have more levels of defense
Passive Safety Systems

- **Passive Safety System Functions**
  - Dedicated safety systems, not used for normal operation
  - Mitigate design basis accidents without nonsafety systems
  - Meet NRC safety goals without use of nonsafety systems

- **Passive Safety System Design Features**
  - Only passive processes; no active pumps, diesels, fans, …
  - DBA considerations; margin, single failure
  - PRA considerations; reliability, common mode failures
  - Reduced dependency on operator actions

- **Passive Safety System Equipment Design**
  - Reliable, experienced based, nuclear grade equipment
  - ASME, seismic I, full fire / flood / wind protection
  - Availability controlled by Tech Spec with shutdown requirements
  - Reliability controlled by ISI / IST and maintenance program
Active Nonsafety Systems

- **Active Nonsafety System Functions**
  - Reliably support normal operation
  - Minimize challenge to passive safety systems
  - Not required to mitigate design basis accidents
  - Not required to meet NRC safety goals

- **Active Nonsafety System Design Features**
  - Simplified designs (fewer components, separation not required)
  - Redundancy for more probable failures
  - Automatic actuation with power from onsite diesels

- **Active Nonsafety System Equipment Design**
  - Reliable, experienced based, industrial grade equipment
  - Non-ASME, non-seismic, limited fire / flood / wind protection
  - Availability controlled by procedures, no shutdown requirements
  - Reliability controlled by maintenance program
  - Quality Class D used for components that minimize challenges to passive systems
AP1000 Electrical Systems

- **Class 1E DC and UPS System (IDS)**
  - Provides electrical power to safety components

- **Non-Class 1E DC and UPS System (EDS)**
  - Provides electrical power to non-safety components requiring highly-reliable power

- **Main AC Power System (ECS)**
  - Provides bulk electrical power

- **Onsite Standby Power System (ZOS)**
  - Provides electrical power to defense-in-depth and investment protection loads when offsite power is lost
AP1000 Class 1E DC & UPS System (IDS)

- 125 Vdc
- 120/208Vac 60 Hz (uninterruptible)
- Four Divisions
  - Divisions A and D each have one 24-hour battery for actuation
  - Divisions B and C each have one 24-hour battery and one 72-hour battery for post-accident monitoring
  - 72-hour battery is for monitoring only
  - Spare battery
    - Can be manually connected to replace any of the 6 primary batteries
AP1000 Class 1E DC & UPS System (IDS)

- Provides electrical power to safety components
  - Primary Protection System
  - MCR lighting
  - Valve actuators
  - Reactor trip, RCP trip

- Class 1E
  - Meets IEEE 308, 323, 344, 379, 384, 603, etc.
AP1000 Non-Class 1E DC & UPS System (EDS)

- 125 Vdc
- 120/208Vac 60 Hz (uninterruptible)
- Two load groups
  - Each group has two 2-hour batteries
  - The IDS spare battery can be used to replace any of the 4 primary nonsafety batteries
AP1000 Non-Class 1E DC & UPS System (EDS)

- Provides electrical power to non-safety components requiring highly-reliable power
  - Plant Control System
  - Data Display System
  - Diverse Actuation System
  - Other control systems
  - Communications
  - Hydrogen igniters

- Non-Class 1E
  - Quality Class D
  - RTNSS Important (portions)
AP1000 Main AC Power System (ECS)

- Provides bulk electrical power
  - 6.9 kV, 480 V, 120/208 V, 60 Hz
- Normal power supply from main generator
- Preferred power supply is offsite source through main and auxiliary transformers
- Maintenance power supply is through reserve auxiliary transformer
- Standby power source is two diesel generators
- Two load groups
  - Each group is connected to one standby diesel generator, one auxiliary transformer and the reserve auxiliary transformer
AP1000 Main AC Power System (ECS)

- Includes two ancillary diesel generators (35 kW each) for post-72-hour coping
  - Post-accident monitoring instrumentation
  - Control room lighting
  - Passive containment cooling tank refill
  - Spent fuel pool refill

- **Non-Class 1E**
  - Equipment Class D (portions)
  - RTNSS Important (portions)
Onsite Standby Power System (ZOS)

- Two diesel generators (4000 kW each)
- Provides electrical power to defense-in-depth and investment protection loads when offsite power is lost
- Non-Class 1E
  - Quality Class D
  - RTNSS Important
AP1000 I&C Systems

- **Primary Protection System (PMS)**
  - Plant wide system for all safety displays & controls
  - Microprocessor / software based

- **Diverse System (DAS)**
  - Limited scope system, PRA based displays & controls
  - Backs up PMS where common mode failure is risk important
  - Different hardware & software than PMS

- **Plant Control System (PLS/DDS)**
  - Plant wide system for all normal displays & controls
  - Microprocessor / software based

- **Special Purpose Systems (Seismic Monitoring, Radiation Monitoring, Incore Instrumentation, etc.)**
I&C systems are included in Certified Design.

I&C system designs were not reviewed by the NRC.

Functional requirements consistent with the safety analyses and PRA were established.

A design process was defined.

Test and acceptance criteria were established.

A conceptual design was developed.

A detailed I&C design will be developed based on the functional requirements, using the certified design process, and meeting the certified acceptance requirements after a plant is ordered.
AP1000 Protection System (PMS)

- Plant-wide Class 1E system for all safety displays & controls
- Originally expected to be ‘Eagle’, now expected to be ‘Common Q’
- Detects off-nominal conditions and actuates safety functions
- Provides post-accident monitoring functions
  - Regulatory Guide 1.97 Category 1 and some Category 2 variables
- Microprocessor / software based
- Multiplexed communications
- Class 1E
  - Meets IEEE-603, 7-4.3.2, 323, 344, 379, 384, etc.
AP1000 Protection System (PMS)

- **Redundant Trains**
  - 4 divisions, physically separated with electrical isolation (fiber-optic)
    - Each with own independent battery-backed power supply
    - 24-hour batteries for actuation, 72-hour batteries for monitoring
    - Improved HVAC separation/fire protection (2 separate HVAC systems)
  - 2-out-of-4 bypass logic, fail safe when appropriate
  - Different plant parameters provide functional diversity

- **Verification and Validation**

- **Equipment Qualification**
  - Environmental, seismic, EMC

- **Improved In-Plant Testing**
  - Built-in continuous self-testing and manual periodic testing

- **Westinghouse Extensive Experience with Digital I&C Designs**
  - Operating plant upgrades and new plants (Sizewell, Temelin)
AP1000 Diverse Actuation System (DAS)

- **Limited scope system**
  - PRA-based displays & controls
  - Backs up PMS where common mode failure is risk important
- **Microprocessor / software based**
- **Different architecture, hardware & software than PMS**
- **No multiplexing**
- **Manual controls and indications use no software**
  - Direct wiring to actuation devices
  - Compliance with USNRC Branch Technical Position HICB-19, Position 4
- **Separate sensors from PMS and PLS**
AP1000 Diverse Actuation System (DAS)

- DAS shares some actuated equipment (e.g., valves) with PMS
  - DAS signals isolated from PMS
  - Separate actuation devices
    - Solenoid valves on AOVs
    - Igniters on squib valves
    - Relays in MCCs controlling AOVs

- Non-Class 1E
  - Equipment Class D
  - RTNSS Important
AP1000 Control System (PLS / DDS)

- Plant-wide system for all normal displays & controls
- Microprocessor / software based
- Highly redundant
- Continuously used
- Multiplexed communications
- Includes plant computer functions
- Non-Class 1E
  - Equipment Class D
AP1000 Advanced Control Room

- **Compact Control Room**
  - Designed for 1 Reactor Operator and 1 Supervisor

- **Displays**
  - Plant status / overview via wall panel (DDS, non 1E)
  - Detail display via workstation video displays (DDS, non 1E)
  - Small number of dedicated displays; safety (PMS, 1E) & diverse (DAS, non 1E)

- **Controls**
  - Soft controls (DDS, non 1E)
  - Small number of dedicated switches; safety (PMS, 1E) & diverse (DAS, non 1E)

- **Advanced Alarm Management**

- **Computer Based Procedures**
  - Paper backup
AP1000 is Different

- Safety systems are not used for normal operation.
  - Multiple, diverse levels of defense
  - Signals from safety sensors are provided to nonsafety system.
- No safety source of electrical power.
  - Batteries provided for I&C and lighting.
- No safety actuation power after 24 hours without ac power.
  - Planned safety actuations are one-time-only.
- Batteries provided for monitoring are sized for 72 hours.
  - Small non-safety diesels provided for post-72 hour monitoring and water.
- No safety air conditioning.
- Safety motors are limited to MOV operators.
- Compact control room.
  - Limited number of discrete controls