AP1000® Safety Concepts and Robustness to External Hazards

John Giddens, Licensing Manager, Southern Nuclear
Terry Schulz, Consulting Engineer, Westinghouse
Luca Oriani, Engineering Manager, Westinghouse
April 24th, 2012
AP1000 Approach to Safety

• **Passive Safety-Related Systems**
  – Use “passive” processes only, no active pumps, diesels, ….
    – One time alignment of valves
    – No support systems required after actuation
    – Greatly reduced dependency on operator actions

• **Active Defense in Depth-Related Systems**
  – Reliably support normal operation
    – Redundant equipment powered by onsite diesels
  – Minimize challenges to passive safety systems
  – Not necessary to mitigate design basis accidents

**All critical Station Blackout Response Features FAIL SAFE**
AP1000 Mitigates Non-LOCA Events Using Fail Safe, Passive Features

• AP1000 contains features that provide safe shutdown following non-LOCA accidents that are designed to actuate to their “fail safe” state upon loss of power, loss of I&C controls, or loss of instrument air:
  – Reactor shutdown
    – Control rods (insert)
  – Decay heat removal
    – PXS PRHR HX isolation valves (fail open)
  – Containment cooling
    – PCS PCCWST isolation valves (fail open)
  – RCS makeup/boration
    – PXS CMT isolation valves (fail open)
  – Containment isolation valves (fail close)
    – Risk important, normally open containment isolation valves
AP1000 Core / Containment Cooling
Coping Capabilities

* Backup provided through built in plant connections and pre-arranged offsite supply of emergency power and portable pumps.
AP1000 Coping with a Station Black-Out

- No Reliance on AC Power; Long Term Plant Safety Assured without Active Components (Natural Forces Only)
  - For Station Blackout (SBO), AP1000 meets aggressive 72 hours coping time requirements for passive plants using fail safe components

<table>
<thead>
<tr>
<th>NRC Requirement</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing US Plants</td>
<td>4 - 8</td>
</tr>
<tr>
<td>AP1000</td>
<td>168 (7 days)</td>
</tr>
</tbody>
</table>

Hours

0 25 50 75 100 125 150 175
Summary of AP1000 Response to Extreme Events

• AP1000 provides a unique capability to respond to DB and BDB events due to 3 fundamental safety advancements:

1. **AP1000 Self-Actuates.** For station blackouts, critical SSCs will automatically achieve a fail safe configuration without the need for operator action or AC/DC power

2. **AP1000 is Self-Sustained.** AP1000’s passive approach to safety de-emphasizes the importance of AC power and cooling supply.

3. **AP1000 is Self Contained.** Systems, structures, and components (SSCs) critical to placing the reactor in a safe shutdown condition are protected within the steel containment vessel and further surrounded by a substantial “steel concrete” composite shield building.
The AP1000 nuclear power plant was designed to cope with Station Blackout

• The AP1000 nuclear power plant includes safety-related passive systems and equipment that are sufficient to automatically establish and maintain Safe Shutdown Conditions for 72 hours – without operator action and without onsite and offsite AC power sources
  – Fail safe actuation, no ac or dc power required

• The AP1000 plant design includes both onsite equipment and safety-related connections for use with transportable equipment and supplies to provide safety functions for an indefinite time.
Post-72 Hour Passive System Support Provided by Offsite Equipment

• Connections provided in design are safety related (seismic I)
  – Flange is provided for small portable, self-powered, pump for PCS and SFP makeup
    – Pump needs to produce at least 135 gpm with 273 ft of developed head
  – Electrical connection for small portable generator to power post accident monitoring
    – Electrical generator needs to produce at least 80 kW (3 phase 480 VAC) in order to power all of the ancillary loads including PMS I&C and PCS pumps
    – If portable self-powered pumps are used then the electrical generator only needs to produce 15 kW (3 phase 480 VAC)

• Offsite equipment is small enough to be easily transported in a small truck or by a small helicopter
Post-72 Hour Passive System Support
Also Provided by Built-In Equipment

• Built-in Long-term Support is non-safety with some seismic capability
  • 2 small Ancillary Diesels (80 kw) provide AC power for post-72 hour operations.
  • 1 Ancillary Water Storage Tank provides water for containment cooling and the SF pool makeup for 4 additional days.
  • 2 PCS recirculation pumps, powered by ancillary diesels, transfer water to the spent fuel pool and the containment outer surface.
Long-Term Cooling Post Shutdown (7 days and beyond)

- Permanently installed connections for off-site support hook-up of AC power and water supply are provided.
  - Pre-arranged supply covered by written procedures
- With minimal operator actions, core cooling, containment cooling, and spent fuel cooling are maintained indefinitely.
- Post 7 day features may be used earlier if needed.

Service Water CT Basin

Fire Protection Tanks

Condensate Storage Tank

Boric Acid & Demineralized Water Tanks
AP1000 Post-72 Hour Procedures Provide Guidance for Extended SBO Events

• Section 1.9.5.4 of the AP1000 DCD describes the procedures that address actions that would be necessary 72-hours subsequent to a station blackout to maintain safe shutdown conditions for the plant.
APOG Actions to Support Utility Response to Order EA-12-049

Mike Melton, AP1000 Regulatory Interface, Westinghouse
Luca Oriani, Engineering Manager, Westinghouse
April 24th, 2012
AP1000 Proposed Guidance

• Step 1: Establish standard design baseline coping capability considering design basis hazards,
  – SBO is design basis event for AP1000
• Step 2: Apply beyond design basis (BDB) external hazards
  – Perform standard plant design margin assessment
  – Confirm the capability to extend core, containment and spent fuel pool cooling under beyond design basis conditions
• Step 3: Identify any enhancements to baseline capability to address BDB scenarios, if applicable.
Baseline Coping Capability

- **1st Phase:** passive system coping for core, containment, and SFP cooling from 0-72 hours
  - This is covered in the existing licensing basis since SBO is DBA
- **2nd Phase:** Support from the installed ancillary equipment or by offsite equipment from 3-7 days
  - If the ancillary equipment is unavailable, an offsite portable pump and diesel generator are required
- **3rd Phase:** Indefinite coping with offsite assistance which includes diesel fuel oil at a minimum
Storage of FLEX equipment

- AP1000 FLEX equipment can be protected best by locating storage site away from the plant site so that it is not affected by the external hazard that affects the site.
- The AP1000 design supports this approach by:
  - Providing a 72 hour coping time via passive safety systems which provides significant time to transport FLEX equipment to the site.
  - The equipment required to support indefinite coping is minimal:
    - 135 gpm pump, 273’ head; 15 kw/480 volt diesel generator
    - Easy to transport by helicopter if needed
Questions?

“gravity
Sometimes the best ideas are just that simple.”


AP1000 is Safe – But Don’t Just Take Our Word For It

As we have been immensely proud, but not particularly surprised – to see our AP1000 reactor given two highly significant accolades recently by two of the world’s most rigorous and demanding regulatory bodies. In the United States the AP1000 design was awarded Design Certification by the country’s Nuclear Regulatory Commission. Across the Atlantic in the UK, the Office for Nuclear Regulation and the UK Environment Agency have jointly awarded Interim Generic Design Assessment approval to the plant.

These milestones are vital steps towards bringing the Westinghouse AP1000 reactor into commercial operation – delivering not just decades of clean and safe power to future generations, but also thousands of high quality jobs during construction and operation.

Check us out at www.westinghousenuclear.com
• BACKUP
Offsite Equipment Is Easily Transported (Small Equipment)
AP1000 Fail Safe Features
Core Makeup Tanks Isolation Valves (fail open)
AP1000 Fail Safe Features
PRHR HX Isolation Valves (fail open)
AP1000 Fail Safe Features
PCS PCCWST Isolation Valves (fail open)