Fukushima Daiichi Nuclear Accident

A system-level examination of layered protection and common vulnerability

Source Material: IAEA Director General's Report (2015)
Analysis: Systems Engineering & Reliability Perspective

Source Material: I1 Director General's Report (2015)
Analysis: Systems Engineering & Reliability Perspective

System Overview and Boundaries

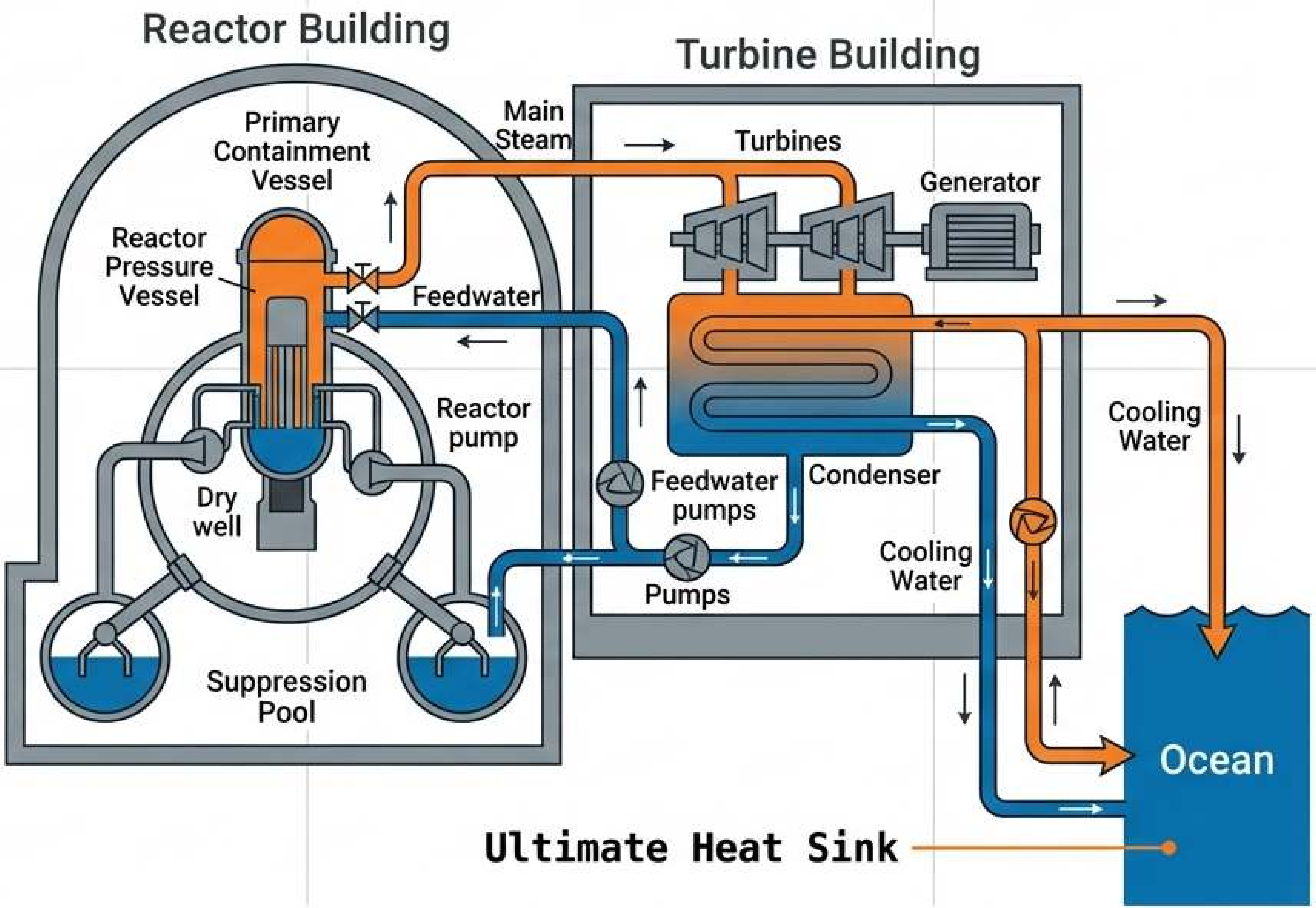
Configuration
Six Boiling Water Reactor (BWR) units on a coastal site.

Status (March 11)
Units 1–3 operating at full power; Units 4–6 in outage.

Thermodynamics
Utilized the Pacific Ocean as the infinite heat sink for ultimate heat removal.

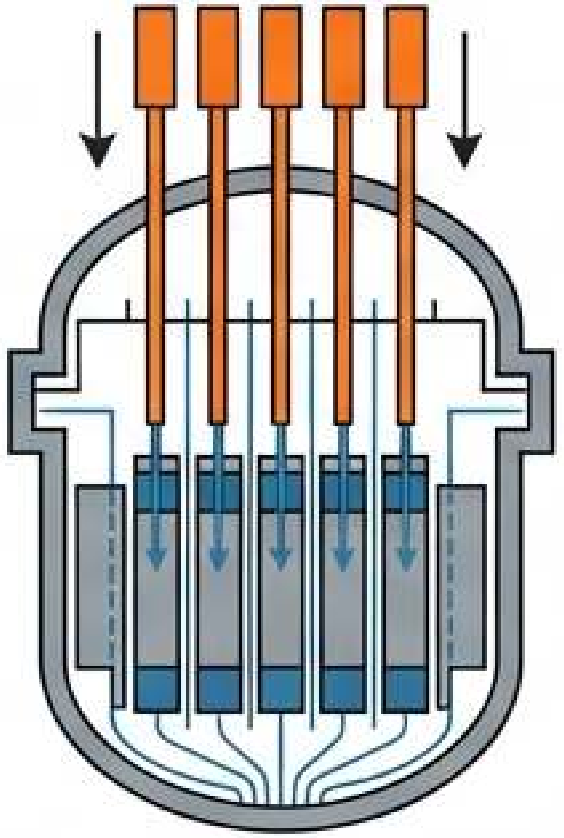
Dependency
Active safety systems required electrical power (AC/DC) to drive pumps, valves, and instrumentation.

System Boundary
Physical plant perimeter and connection to the offsite electrical grid.



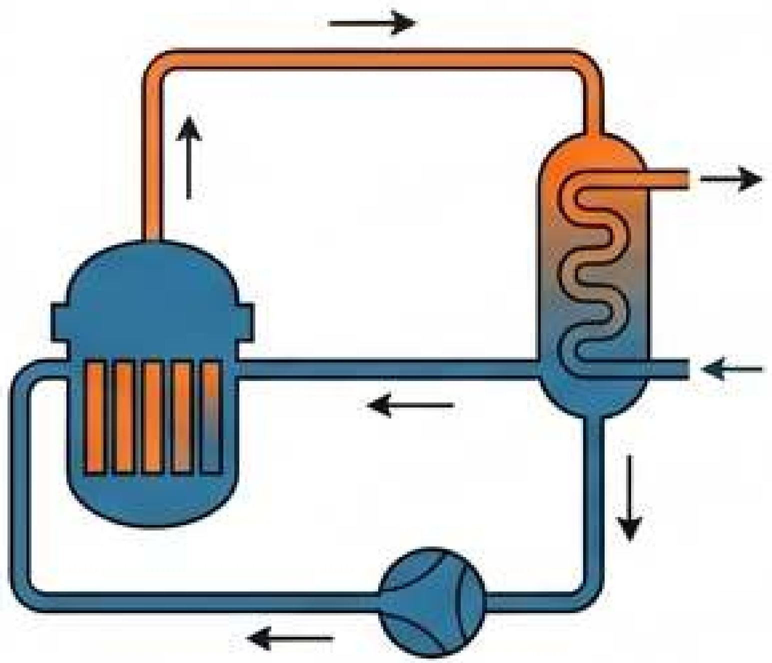
Intended System Function: The Three Fundamental Safety Functions

1. Control Reactivity



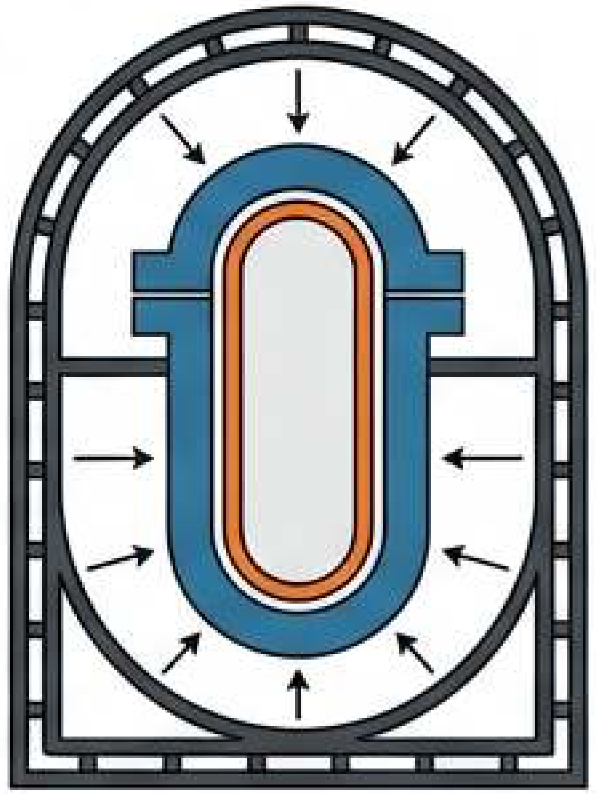
Capability to immediately terminate the fission reaction (SCRAM).

2. Remove Heat



Continuous removal of decay heat from the reactor core and spent fuel pools.

3. Confine Radioactive Material



Maintenance of physical barriers (fuel cladding, RPV, primary containment).

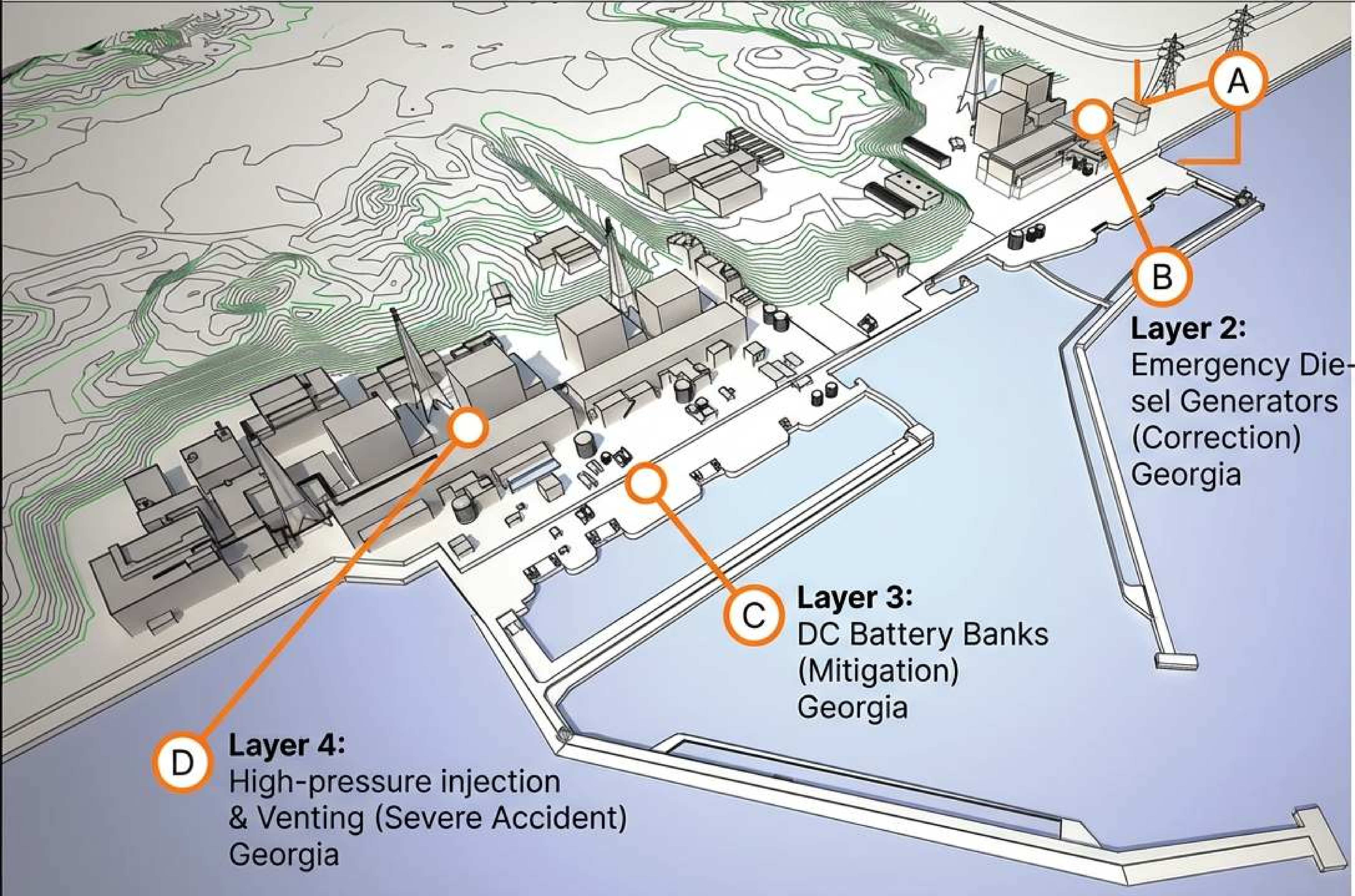
Dependent on Function 2.

Box 2.6. Fundamental safety functions

The three fundamental safety functions are: (1) Control of the reactivity; (2) Heat removal; (3) Confinement of Confinement of radioactive material.

Source Note
in `JetBrains Mono`

Layered Protection Architecture (Defense in Depth)



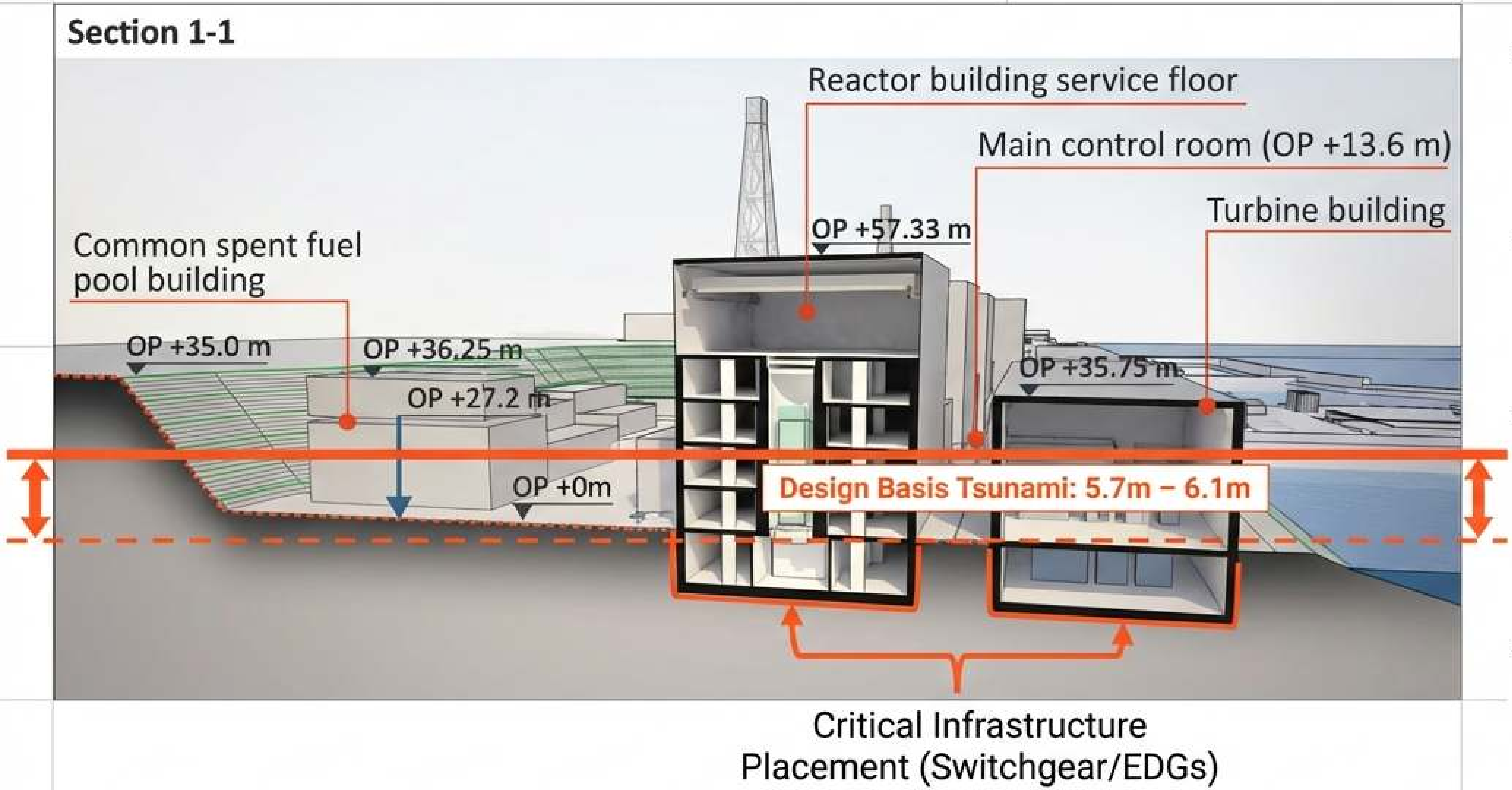
Design Philosophy: Independence and redundancy intended to prevent single-point failure propagation.

Assumed simultaneous failure of multiple layers was impossible.

JetBrains Mono

Source Note: Based on Site Perspective and Technical Specifications.

Design Basis Assumptions and Constraints



- **Seismic:** Designed for high-g ground motion based on historical regional data.
- **Tsunami:** Design basis assumed maximum wave height of ~5.7m–6.1m.
- **Placement:** Critical power infrastructure located in basements based on flood assumptions.
- **Station Blackout (SBO):** Assumed short duration; batteries sized for ~8 hours coping time.

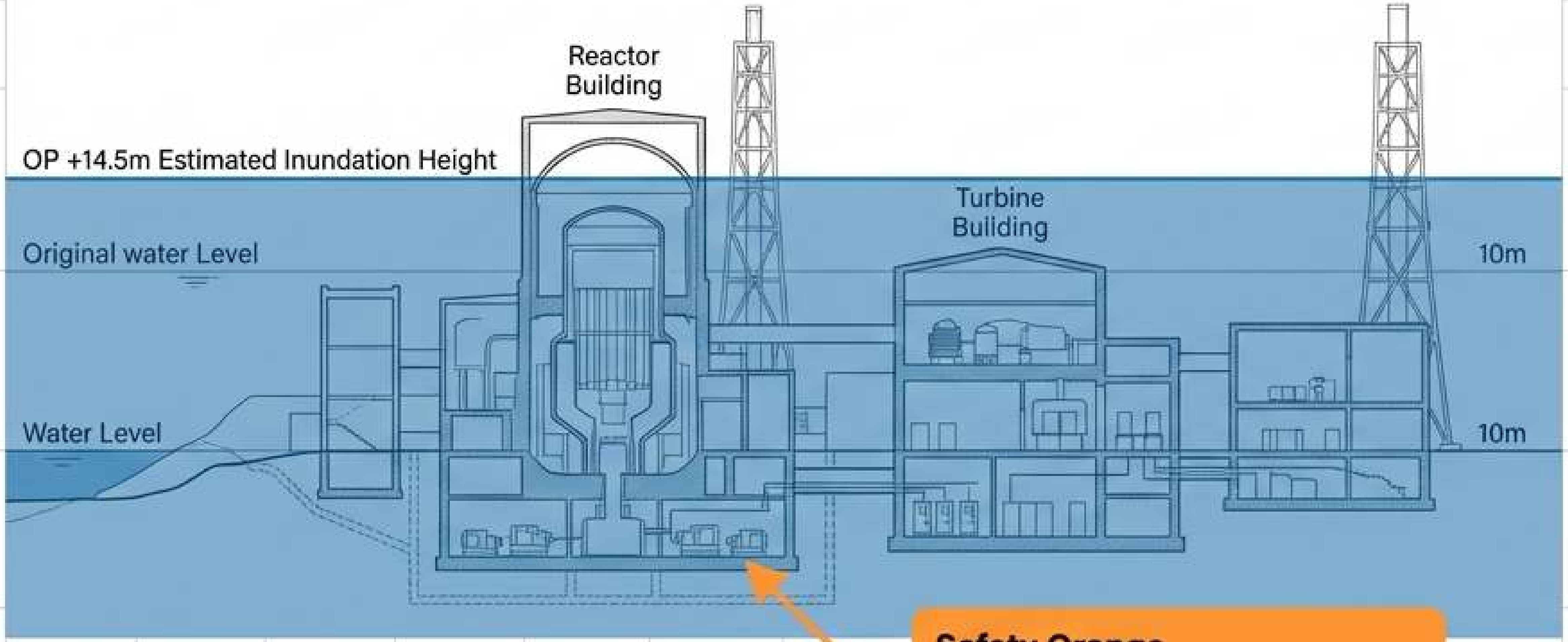
KEY INSIGHT: *System was robust* inside *the design envelope; brittle* outside *it*

14:46: Loss of Offsite Power (Layer 1)

Status Board			
Seismic Event	Magnitude 9.0		**Georgia:** Exceeded design basis, but but containment maintained.
Function 1: Reactivity Control	Automatic SCRAM	OK	**Georgia:** Control rods inserted. Fission terminated.
Offsite Power (Layer 1)	Grid Connection	FAIL LOST	**Georgia:** Seismic damage to switchyards/transmission towers. Total Loss of Offsite Power (LOOP).
Emergency Response (Layer 2)	**Emergency Diesel Generators (EDGs)**	ACTIVE	**Georgia:** Started automatically. Safety functions maintained.

Source Note: Based on Plant Data Logs and Regulatory Accident Investigation Report Appendix III.

15:37: Loss of Emergency Power (Layers 2 & 3)

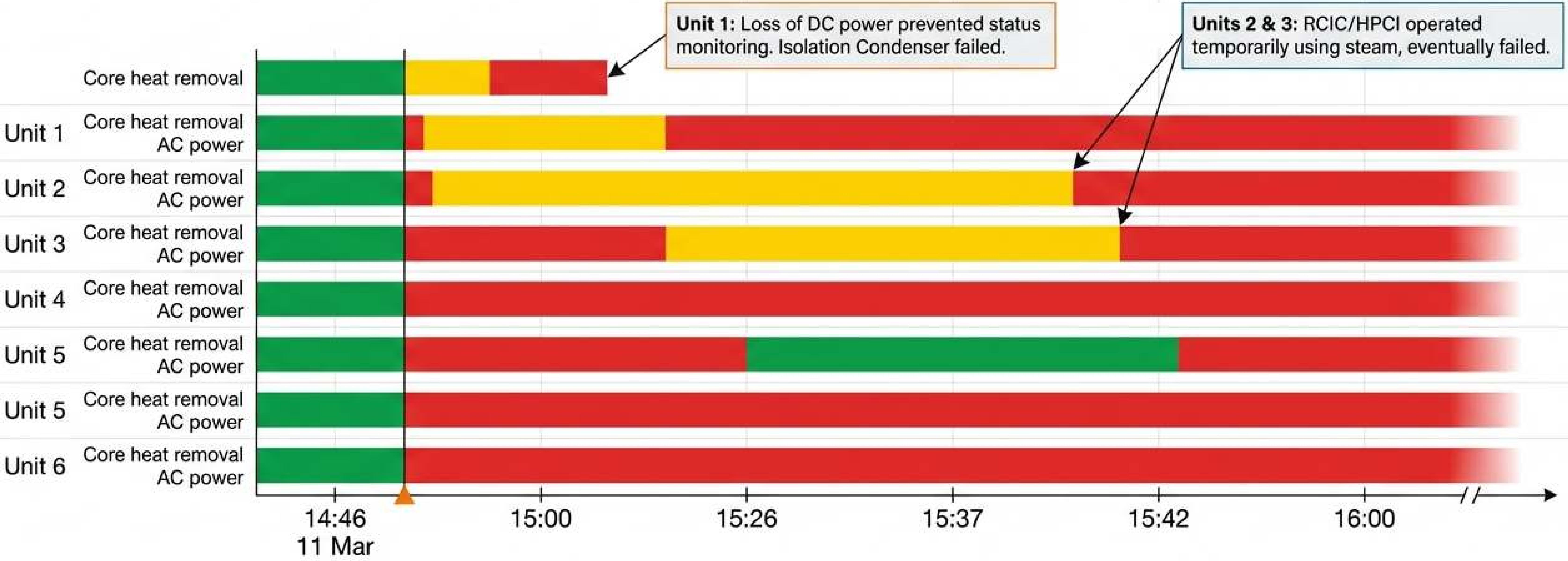


Safety Orange
COMMON CAUSE FAILURE:
Floodwaters submerged EDGs, AC switchgear, and DC distribution panels.

- Tsunami Runup: 14–15m (Exceeded 10m site elevation).
- Mechanism: Direct submersion of electrical infrastructure and loss of seawater pumps (ultimate heat sink).
- Result: Station Blackout (SBO) across Units 1–5.
- Exception: Unit 6 air-cooled EDG (located higher) survived.

Source Note: Based on Plant Data Logs and Regulatory Accident Investigation Report Appendix III.

Progressive Loss of Cooling Capabilities

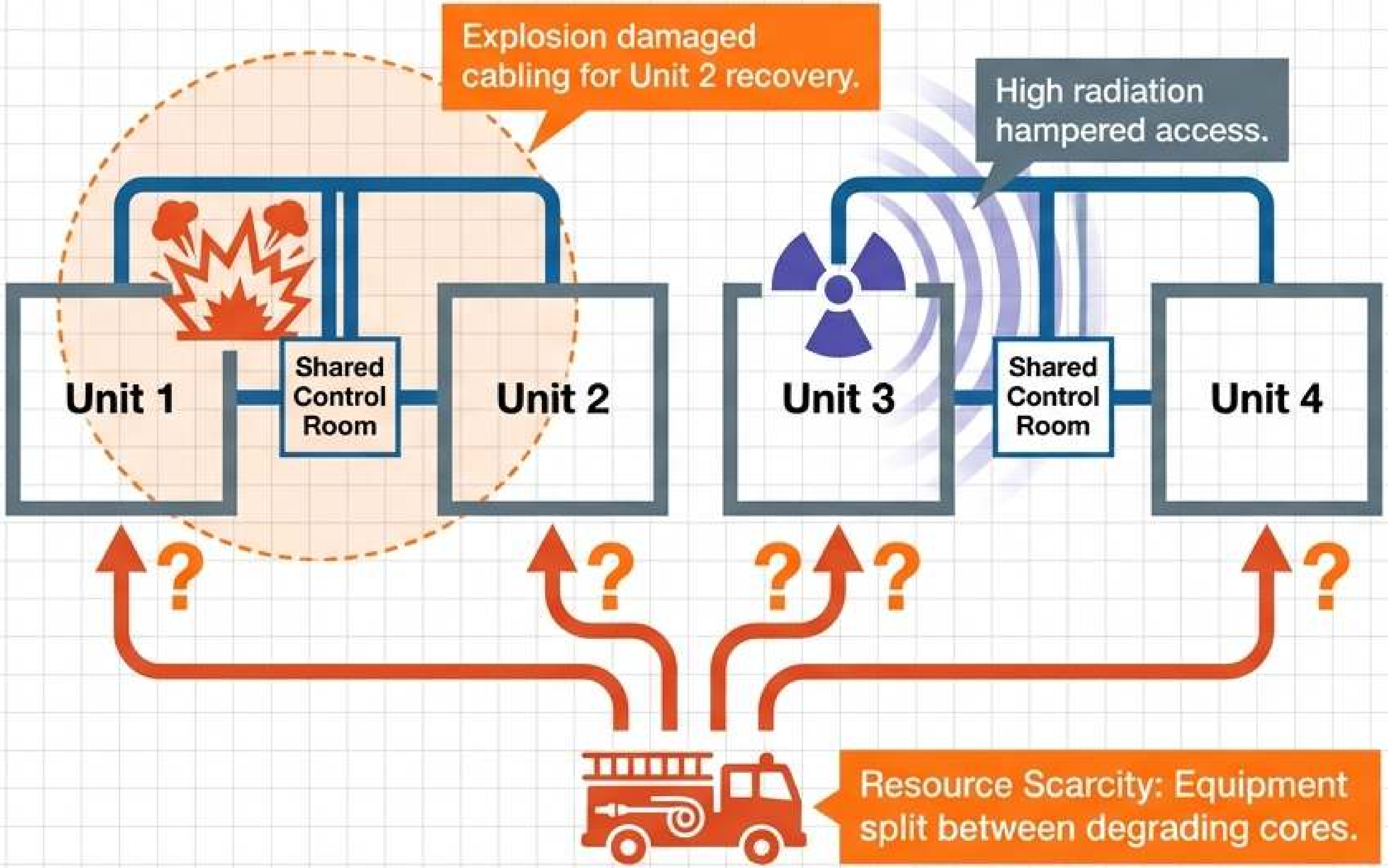


Thermodynamic Reality: Decay heat generation > Heat removal capacity.

Consequence: Reactor Pressure Vessel (RPV) water levels dropped; fuel uncovered; hydrogen generation began.

Technical Forensic Report

Multi-Unit Coupling and Resource Contention



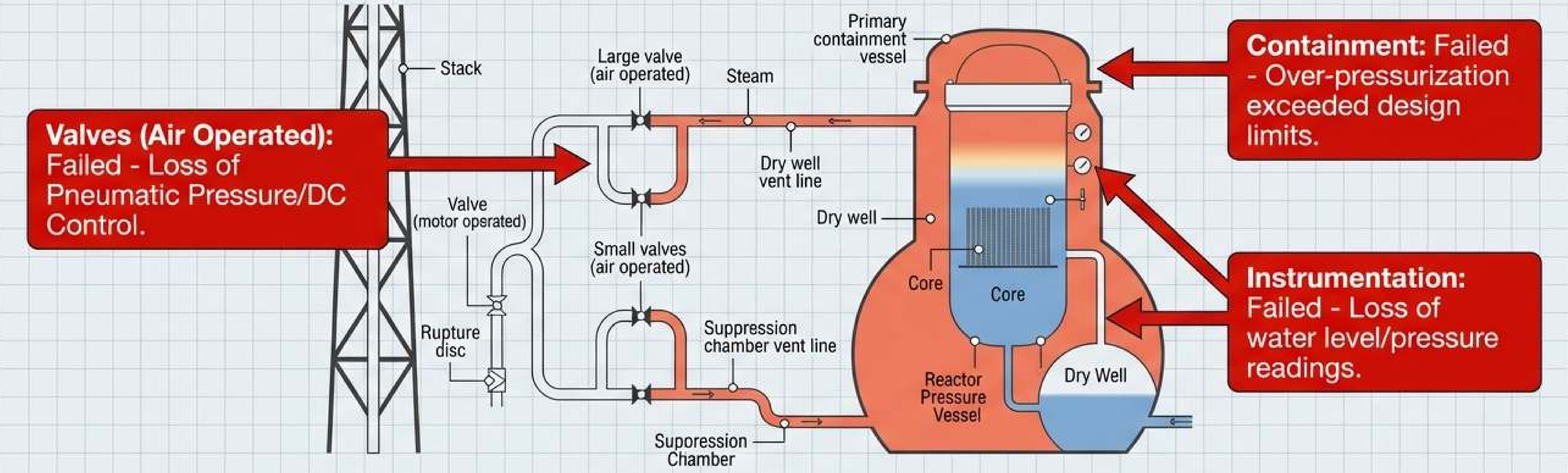
Key Findings

- Simultaneous emergencies at Units 1–4 exhausted site resources.
- Shared main control rooms complicated situational awareness.
- Interdependence became a liability: Independent units became interdependent under stress.

Source Note: Based on Plant Data Logs and Regulatory Accident Investigation Report Appendix III.

Functional Failure Analysis

Venting System Schematic



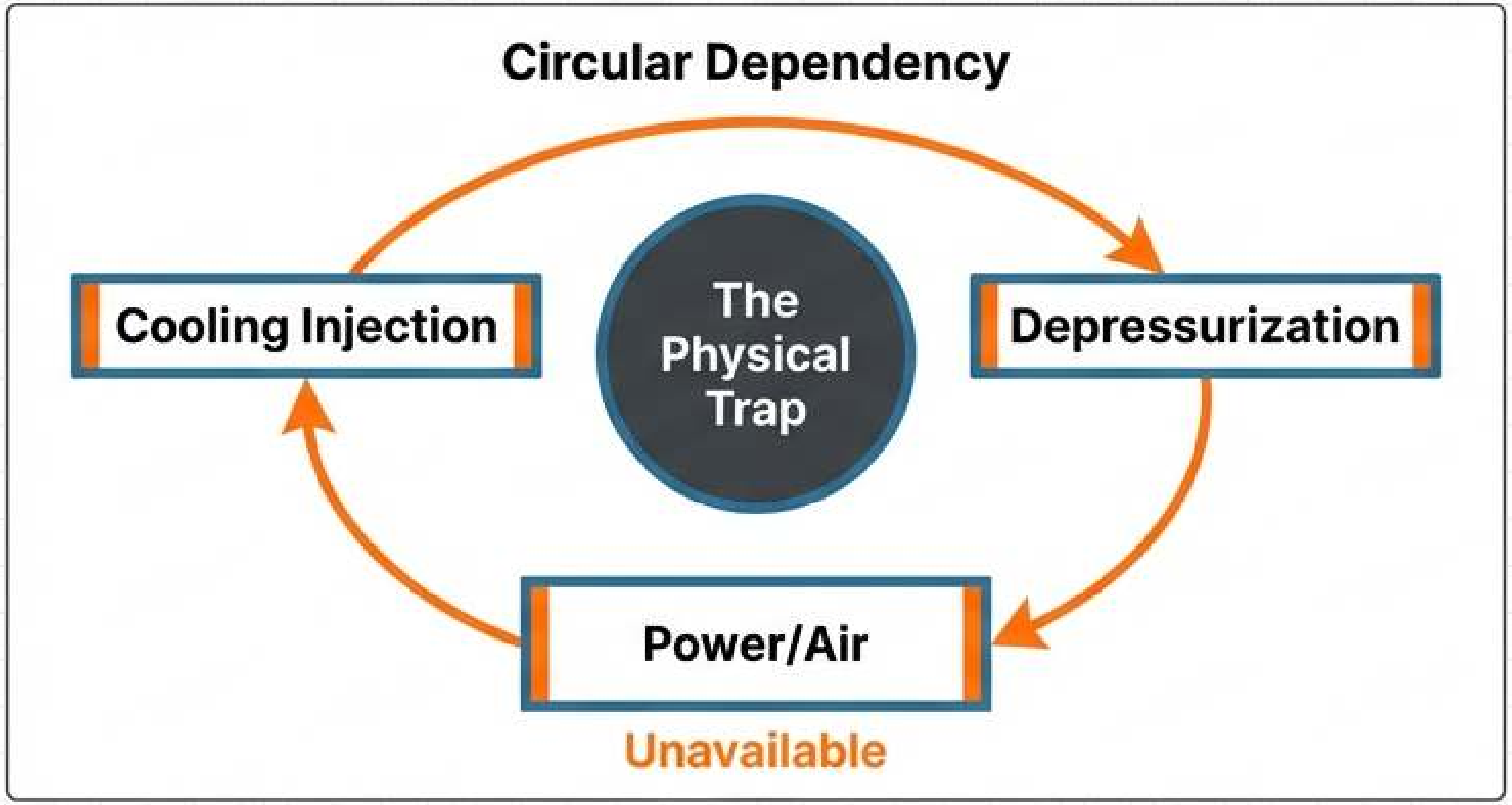
Key Findings

- **Heat Removal**: Loss of ultimate heat sink; inability to inject against high pressure.
- **Confinement:** Venting required AC power and air pressure—both were lost.
- **Result:** Containment vessels failed or leaked; hydrogen migrated to reactor buildings.

Source Note: Based on Regulatory Accident Investigation Report Appendix IV.

Technical Forensic Report

Why Escalation Became Unavoidable



Key Findings

- **The Keystone Dependency:** Electrical power was required for cooling, venting, *and* monitoring.
- **The Physics Limit:** Without power, decay heat pressurized the vessel, locking out low-pressure injection (fire trucks).
- **The Physics Limit:** Without power, decay heat pressurized the vessel, locking out low-pressure injection (fire trucks).
- **Exhausted Margins:** Once core damage began, high radiation precluded manual onsite intervention.

Source Note: Based on Plant Data Logs and Regulatory Accident Investigation Report Appendix IV.

Transferable System Insights

Design Basis Fallacy

Historical data provided a false ceiling for risk. Future extreme events are not bound by past records.

Illusion of Redundancy

Identical systems (Train A/B) sharing an environment (basement) are not truly independent.

Cliff-Edge Effects

Systems optimized for efficiency often lack margins for 'beyond design basis' recovery.

Coupling & Dependency

Critical infrastructure has hidden circular dependencies (e.g., cooling needs power; power needs cooling).

Source Note: Based on Regulatory Accident Investigation Report Appendix IV.

Reflection

The Fukushima Daiichi accident demonstrated that extreme natural hazards have the potential to invalidate multiple levels of defence in depth simultaneously.

Which of our protection layers are truly independent — and which share the same hidden vulnerabilty?

Source Note: Based on Regulatory Accident Investigation Report Appendix IV.