CANDU Safety
#22 - Regulatory Requirements for Design

Dr. V.G. Snell
Director
Safety & Licensing

Differences from LWR Approach

- there are very few regulatory documents on system design
- the documents focus on the special safety systems
  - shutdown systems, ECC, containment
  - overpressure protection
- the requirements are goal-oriented, not detailed
- the regulator audits the results
- benefits:
  - flexibility for new ideas
  - clear responsibility
- disadvantages
  - sometimes no clear rules, judgement required

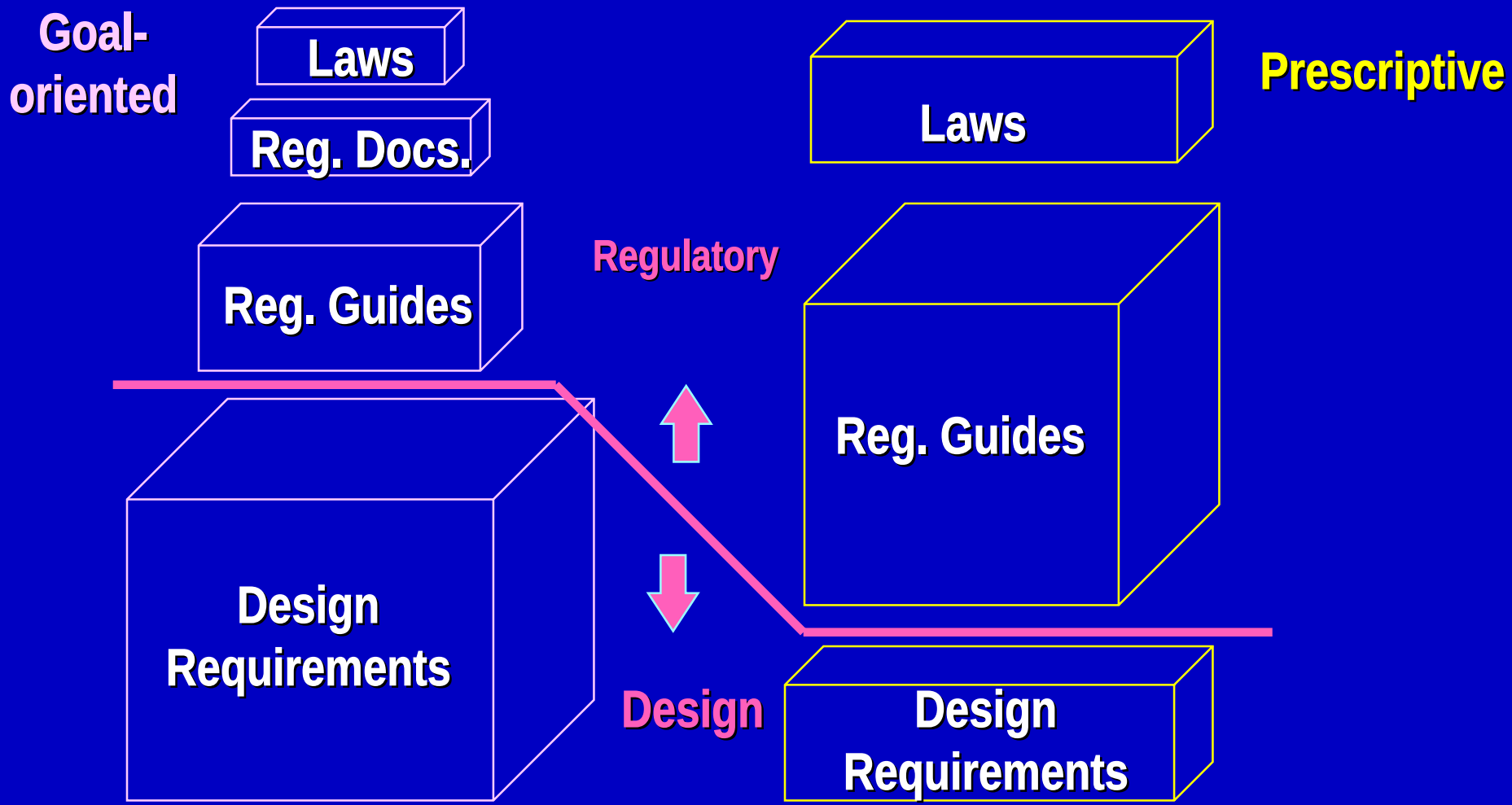
Other Sources of Requirements

- national standards cover many design aspects
  - Canadian Standards Association (CSA)
  - other recognized standards - ANSI, ISO, IEEE
- AECB participates in CSA Committees
- designer sets the detailed requirements
  - submitted to AECB and audited
- some must be formally accepted and need approval if changed
  - Safety Design Guides

Safety Design Requirements Documents

- Licensing Basis
- QA Programme
- Safety Design Guides
- Safety Critical Software Standards and Procedures
- Compliance with Regulatory Documents
- Human Factors Engineering Programme Plan
- Safety Analysis Initial Conditions and Standard Assumptions
- Probabilistic Safety Analysis Methodology
- Design Requirements for Safety-Related Systems
- Disposition of Generic Licensing Issues
- Severe Accident Programme, etc.

Comparison of Requirements Documents



AECB Key Documents for Safety Systems

- R-7: Requirements for Containment Systems
- R-8: Requirements for Shutdown Systems
- R-9: Requirements for Emergency Core Cooling Systems
- R-10: The Use of Two Shutdown Systems in Reactors

Common Elements - 1

- minimum allowable performance standards (MAPS)
- public dose limits for accidents
- environmental qualification
  - for those portions required for accident mitigation
- system unavailability < 10^{-3} years / year
- support system unavailability to meet system unavailability
- long-term post accident availability
- single component failure criterion
  - not required for components which do not change state and which do not depend on safety support equipment
- fail-safe where practicable

Common Elements - 2

- known failed component can be put in safe state
- all automatic actions can also be manually initiated from control room
- physical and operational independence from other safety systems, no shared equipment
- independence from process systems
- separation of redundant instrument channels
- justification of independent subsystems
- call-up of specific CSA Standards
- seismic qualification of portions that are credited in safety analysis after DBE

Common Elements - 3

- no operator action credited until 15 minutes after clear signal
- in-service component testing to demonstrate availability
- testing does not impair system
- safety function cannot depend on Class IV power supply
- periodic but infrequent integrated system tests, for shutdown & containment
- safety systems cannot be intentionally made unavailable (except under specific conditions - e.g., guaranteed shutdown, backup heat sinks available)

Example of Goal-Oriented Requirement

"Design principles for separation of redundant instrument channels…shall be prepared and shall require approval by the AECB prior to the issuance of a construction approval"

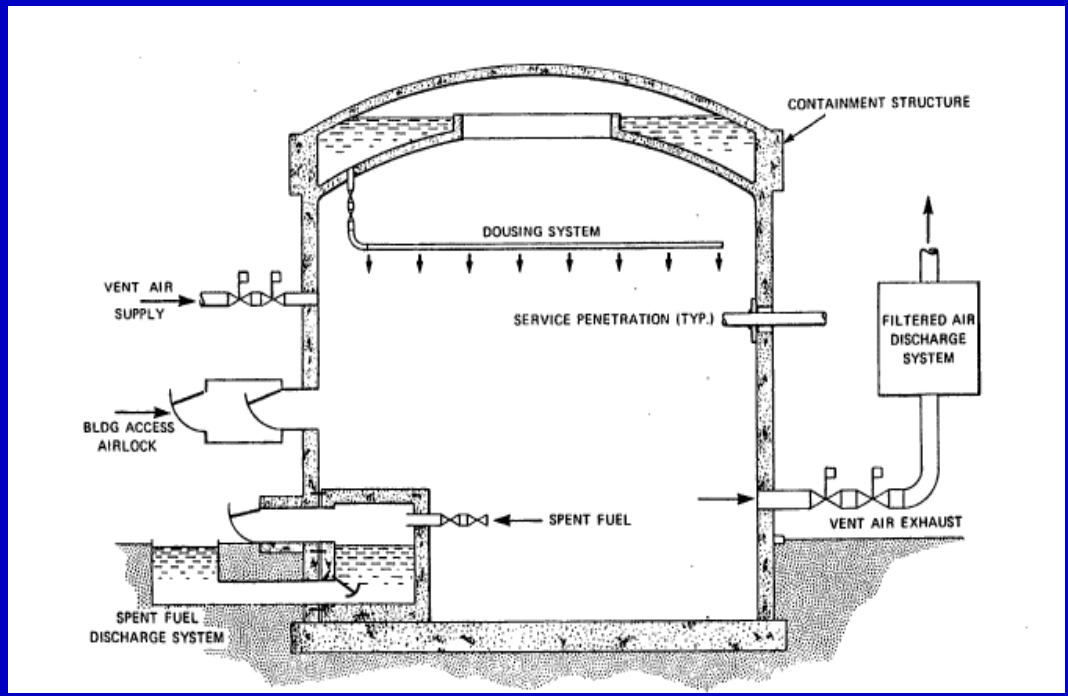
- no numbers or acceptance criteria given
- designer prepares Safety Design Guide stating specific separation requirements
- Safety Design Guide approved by AECB
- major exceptions or changes to Safety Design Guide require approval of AECB

Specific Containment Requirements - 1

- design pressure set only by accidents which release radioactivity (LOCA)
- must assume failure of dousing in setting design pressure
- for primary and secondary side failures, with or without dousing, cannot impair structure so that damage to reactor systems occurs
- for primary side failures with or without dousing, and secondary side failures with dousing, no damage to containment structure
- maximum leakage rate set by value used in safety analysis

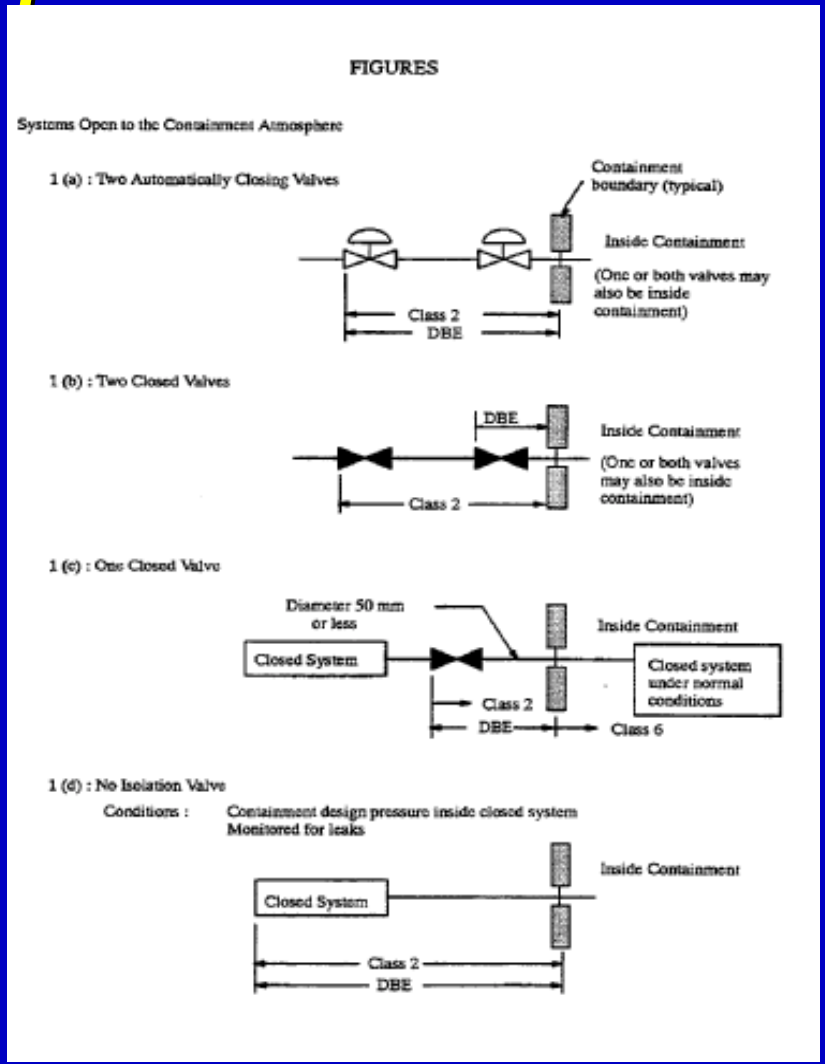
Specific Containment Requirements - 2

- pressure control following an accident
- control of hydrogen / oxygen after an accident unless no possibility of explosion or deflagration
- isolation of compressed air
- proof testing at >1.15 design pressure prior to operation



Specific Containment Requirements - 3

- tests of penetration and isolating devices (no method specified)
- appendix giving detailed requirements for metal extensions of the containment envelope

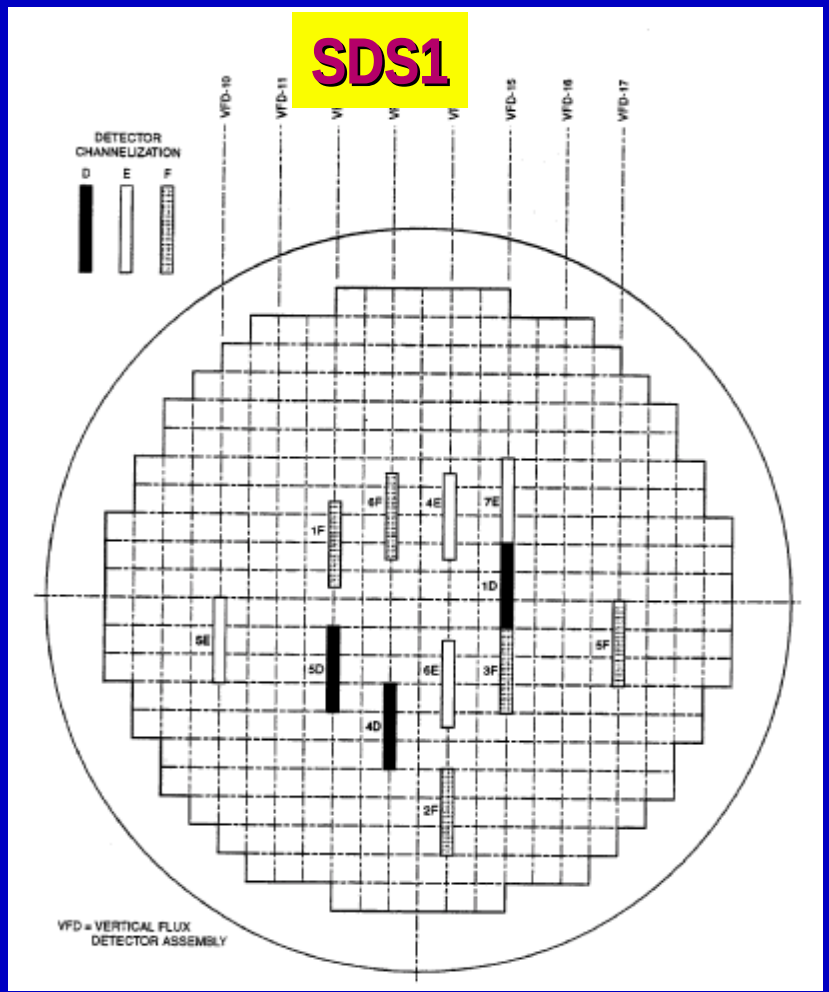


Specific Shutdown System Requirements

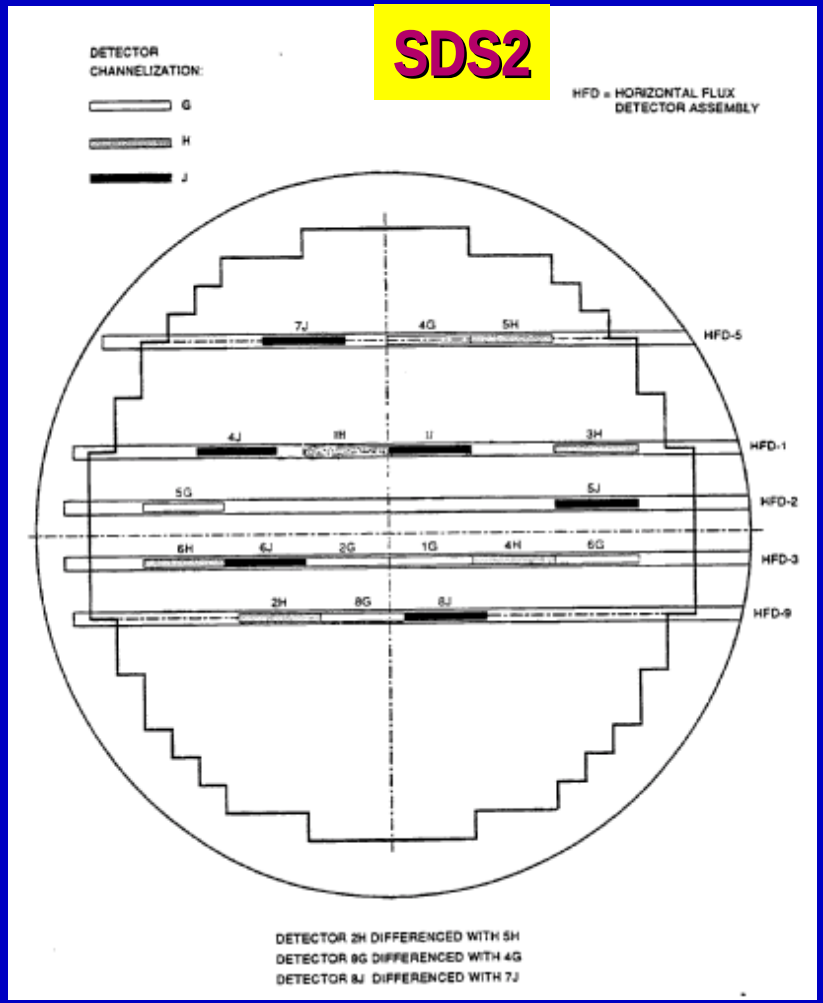
- provision of 2 independent shutdown systems
- prevent loss of heat transport system integrity
- manual operation from main control room and remote location
- diverse designs
- normal process system action, or inaction, cannot reduce effectiveness
- two diverse trip parameters on each shutdown system for each accident (unless impracticable or detrimental to safety)
- re-poising of shutdown systems after trip
- procedures for guaranteed shutdown but at least one shutdown system must be available even then

Diversity & Separation of Flux Detectors

SDS1



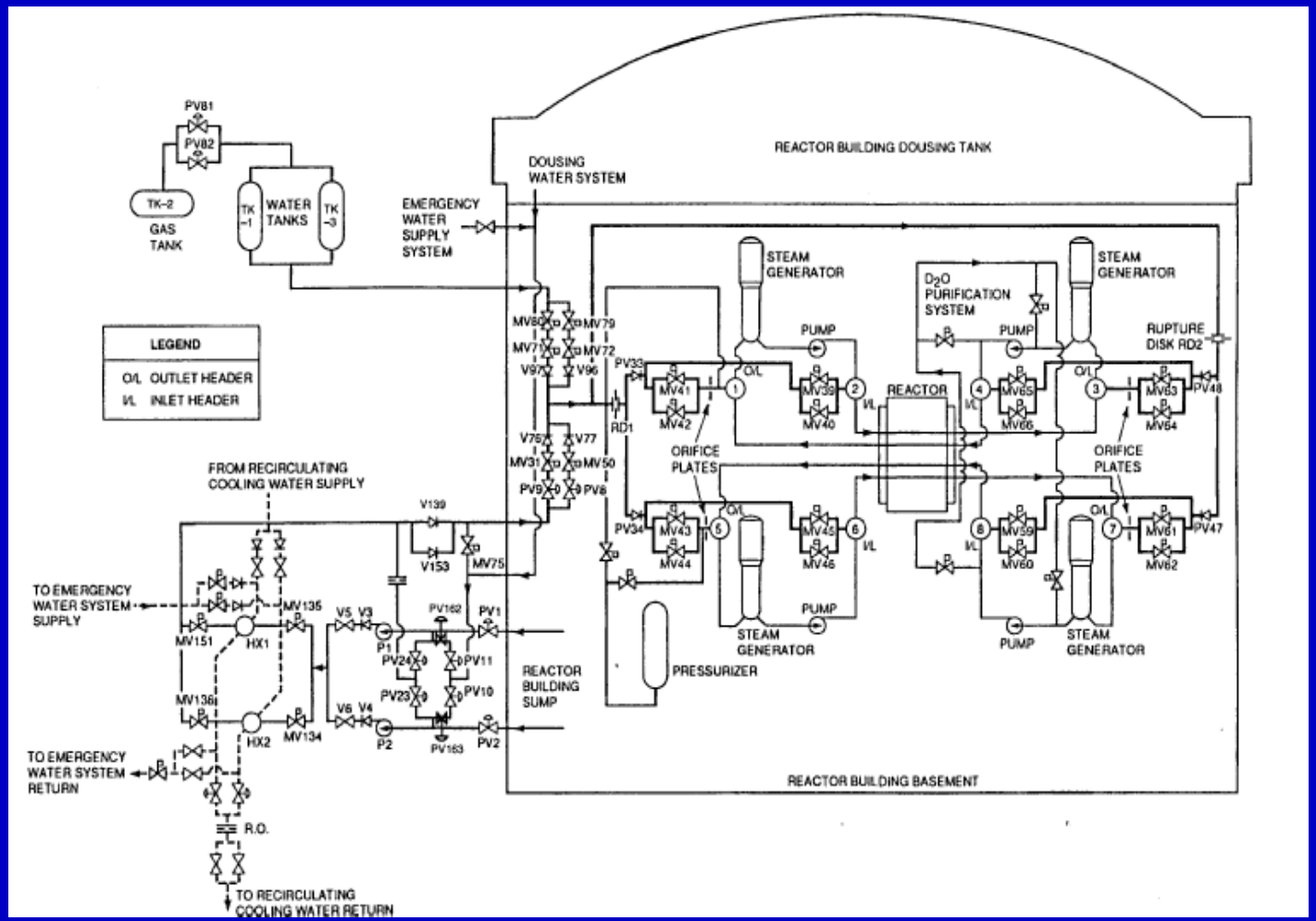
SDS2



Specific Emergency Core Cooling System Requirements

- fuel failures prevented for small LOCA and secondary side breaks
- coolable geometry in fuel channels for all LOCAs
- no further fuel damage after ECC has re-established cooling
- long-term reliability targets required, defined by designer (typically unavailability in long term < 10^{-2} years/year)
- leakage collection and control for ECC components outside containment
- no detrimental safety affect due to inadvertent operation

ECC Schematic



Conclusions

- regulatory requirements on design are goal-oriented
- detailed requirements set by designer & approved by regulator
- emphasis on reliability, separation, testability
- strong tie to accident analysis through MAPS
- qualification where required