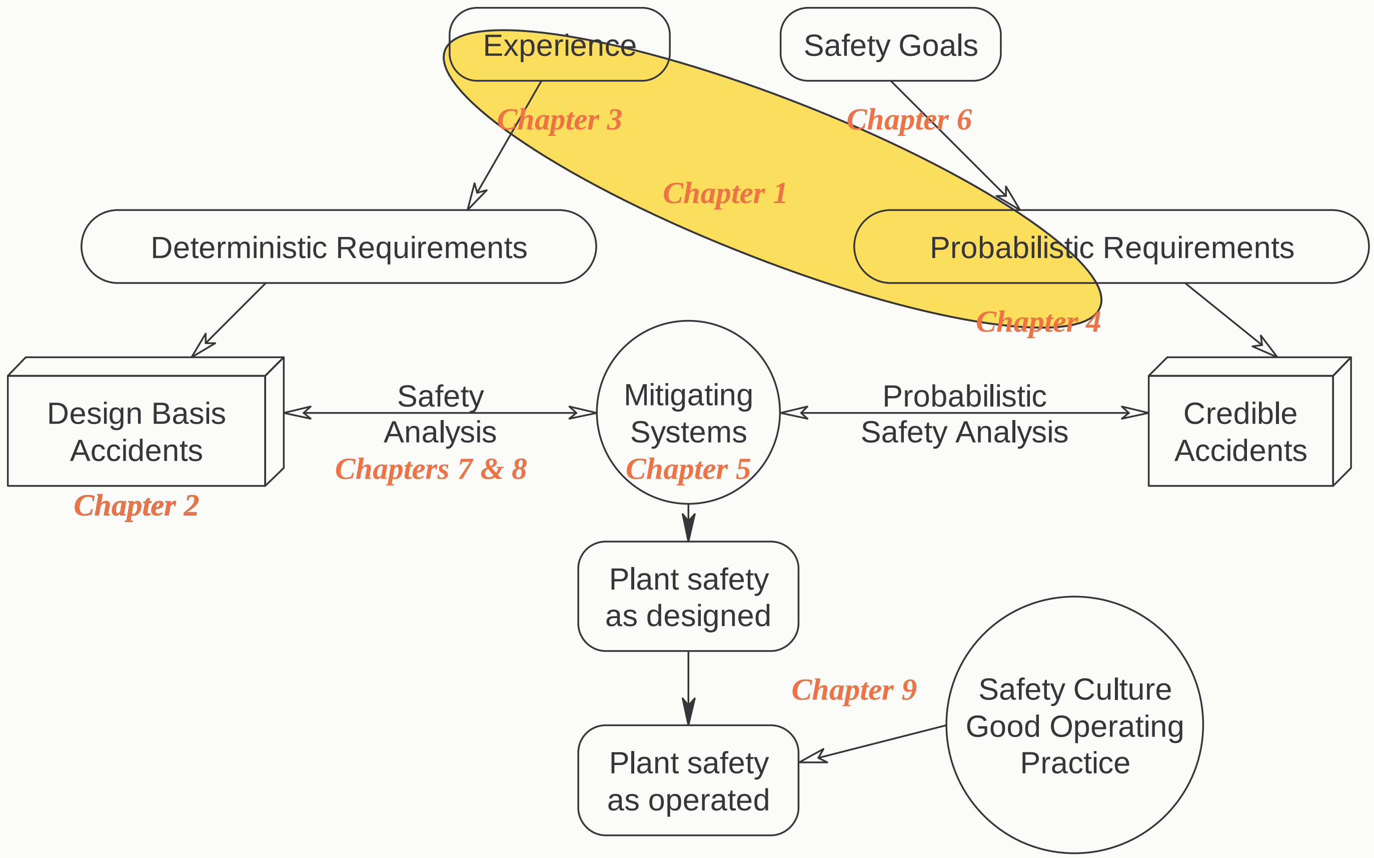
Lecture 4 – Case Studies (cont’d)

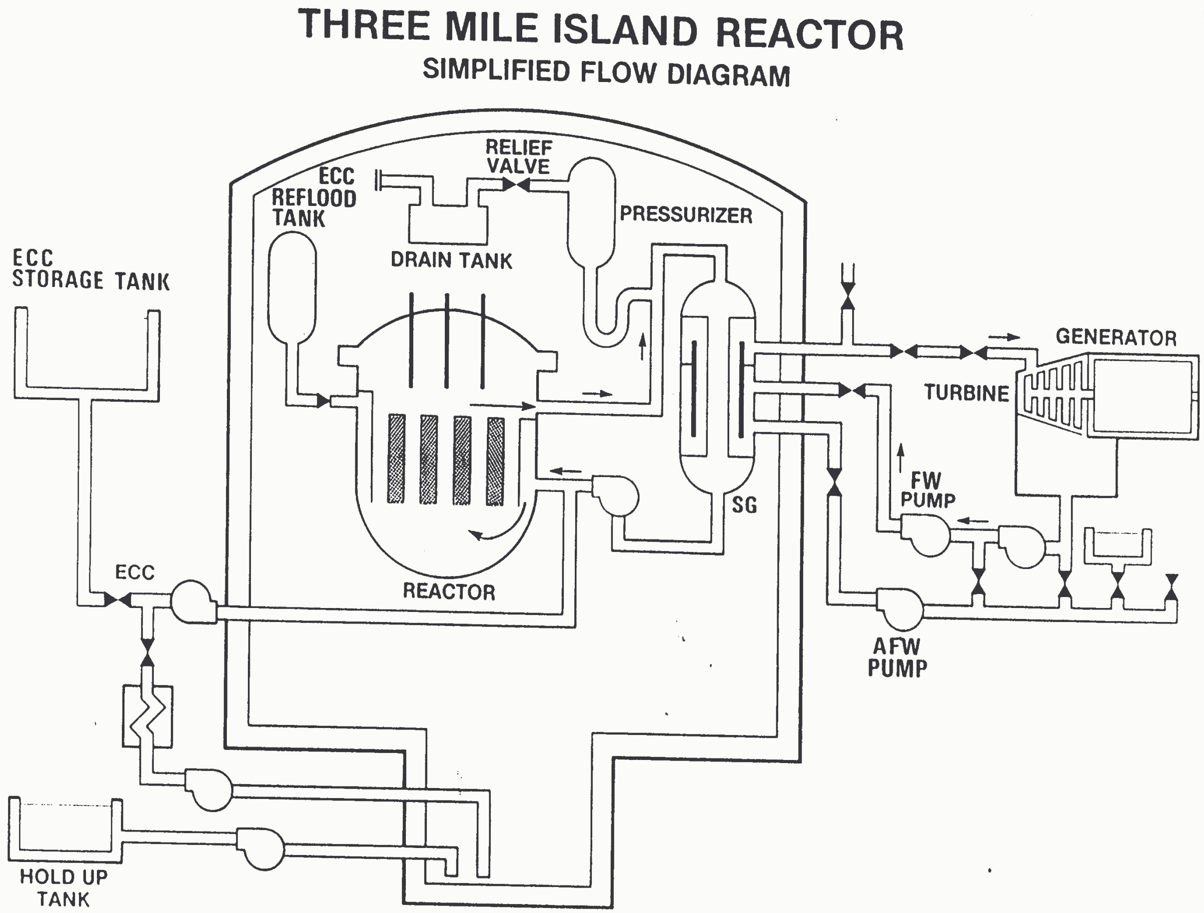
Dr. V.G. Snell

(With thanks to D. Meneley for some material)

Where We Are


Experience
Safety Goals
Chapter 3
Chapter 6
Chapter 1
Deterministic Requirements
Probabilistic Requirements
Chapter 4
Design Basis Accidents
Safety Analysis
Chapters 7 & 8
Mitigating Systems
Chapter 5
Probabilistic Safety Analysis
Credible Accidents
Chapter 2
Plant safety as designed
Chapter 9
Safety Culture Good Operating Practice
Plant safety as operated

Three Mile Island



Event Sequence
(from Brooks & Siddall)

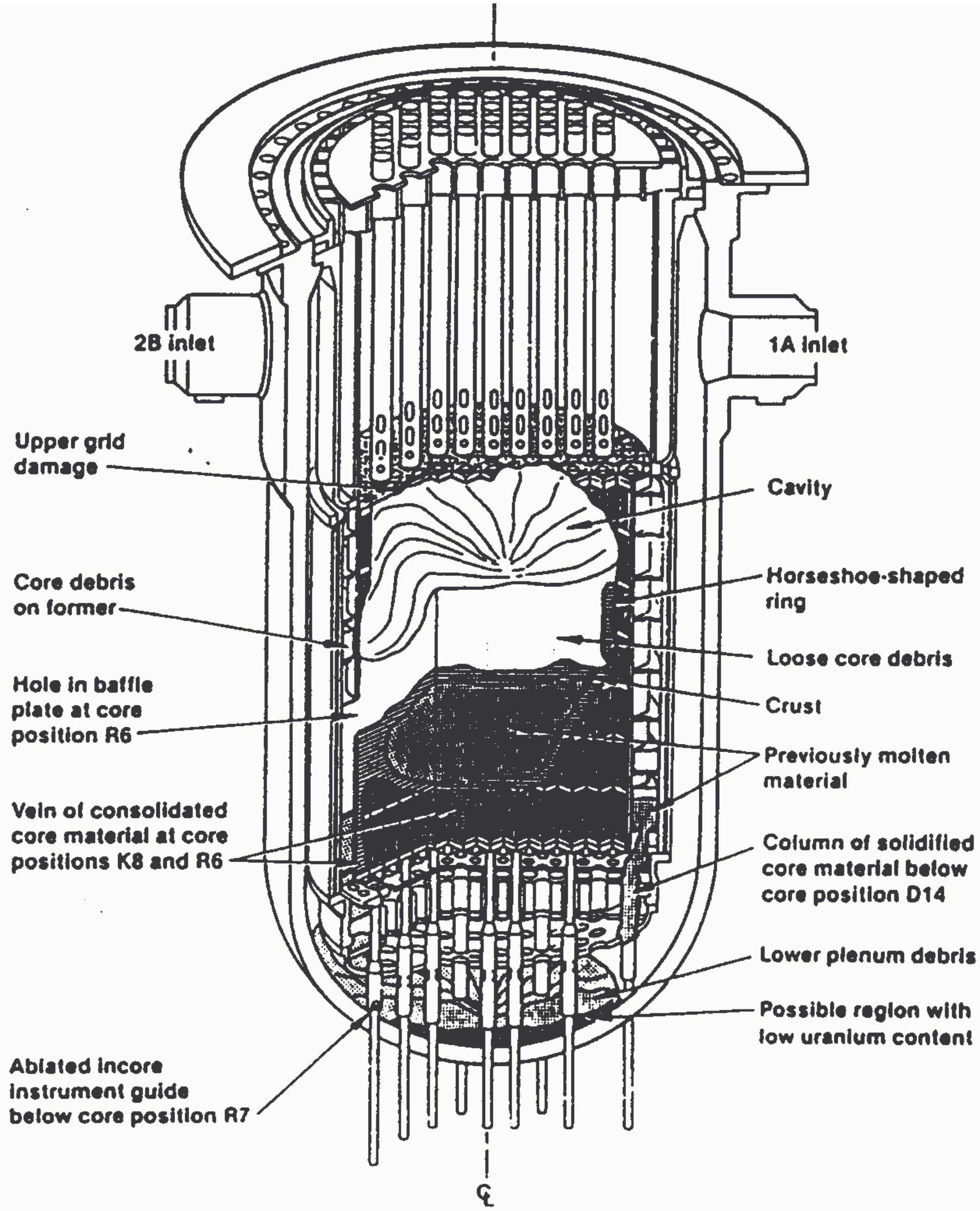
Logic	#	Event
		PHASE A - INITIATING SEQUENCE (A Mishap Within the Normal Range of Viable Operation) (First Minute)
START	1	Wrong detailed design of polisher resin transfer system leading to resin blockage in transfer line.
AND	2	Wrong action by operators in connecting service instrumentation air system to higher pressure water system in trying to clear resin blockage.
RESULT	3	Water in air system caused sudden loss of normal feedwater supply. Turbine tripped. Pilot operated relief valve (PORV) opened correctly..
AND	4	PORV stuck in open position

Logic	#	Event
		PHASE B - SEQUENCE LEADING INTO MAIN ACCIDENT (A Very Important Safety Related Event) (First 50 Mins. After Start)
AND	5	PORV position lights in control room worked from signal and not from valve plug.
AND	6	Previous occasion when 4 had occurred at this same unit (TMI 2) (although for different reasons) had not come to these operators' attention
AND	7	Operators forgot or did not know about 5 and failed to recognize significance of sustained high PORV discharge temperature
RESULT	8	The operators did not realize that the PORV was stuck open.
AND	9	Design engineers and regulatory agency were excessively concerned about avoiding solid (i.e. all liquid) system operation.
AND	10	Operating manuals placed undue emphasis on avoiding solid system arising from 9.
RESULT	11	The operators concentrated on establishing a vapour space in the pressurizer by cutting back emergency injection and maximizing letdown flow despite the fact that the primary coolant was boiling away.

Logic	#	Event
		PHASE C - THE MAIN ACCIDENT **(Failure to Take the Last Clear Chance to Avoid the Accident)** **(From 50 Mins. To 2 Hours after Start)**
AND	12	The operating manuals and the operators' training did not deal with the case of a loss of coolant accident resulting from a small leak at the top of the pressurizer, which is what this was. The operators had no guidance or instructions for this contingency.
AND	13	During a period of more than an hour, 2 senior operators, 2 control room operators and the Superintendent of Technical Support all failed to recognize from basic principles that the primary coolant was boiling away, despite clear instrument indications of high primary coolant temperature, low primary coolant pressure, low primary pump flow, high primary pump vibration, and reactivity disturbances.
AND	14	There had been a failure to communicate to the operators or to incorporate in Operating manuals or training the lessons of at least two previous events (Beznau and Davis-Besse) which had given warning of many of the problems here encountered.
RESULT	15	Two hours after the start, much of the primary coolant had boiled away and serious fuel damage started. Despite partial recovery by the operators and other management and engineers who arrived later, the damage continued and adequate cooling was not permanently restored until nearly 16 hours after the start.

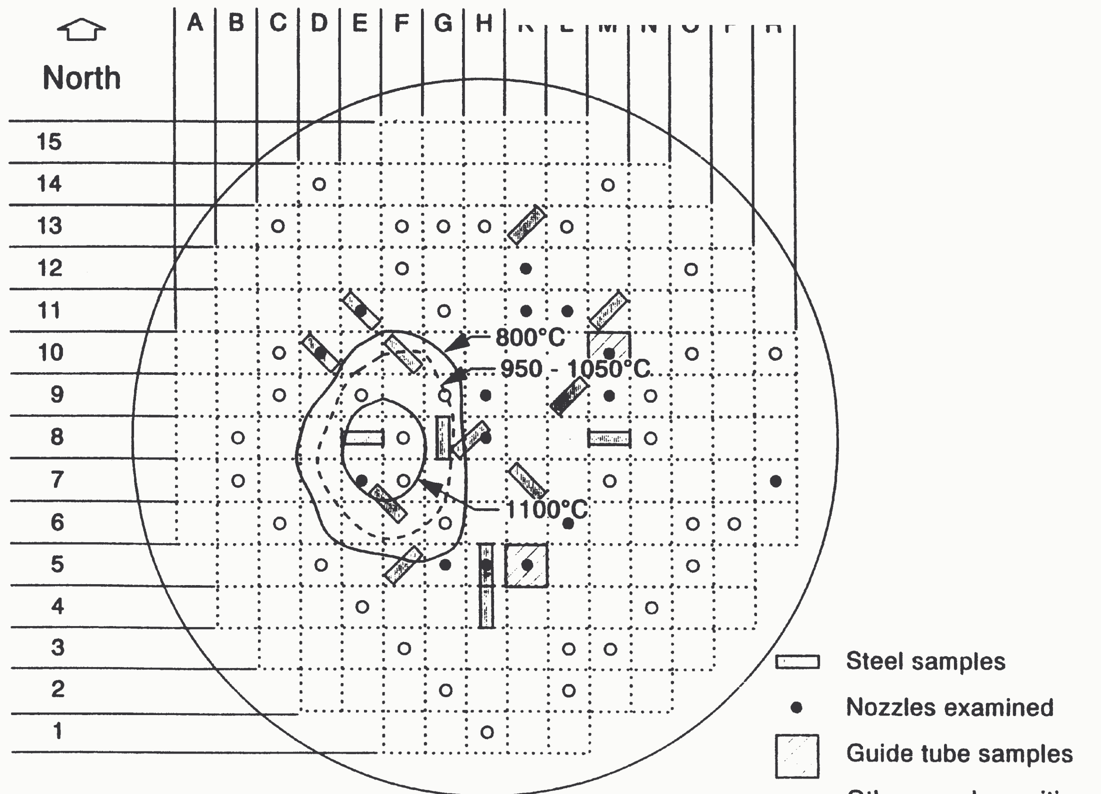
Logic	#	Event
		PHASE D - LATER STAGES (A Warning Event for the Future) (during 15 Hours after Start)
AND	16	Primary coolant liquid and vapour, hydrogen and fission product gas and vapour escaped through the open PORV to the reactor coolant (RC) drain tank and then into the containment building.
AND	17	Containment system was wrongly designed for small leaks in primary system. Operators could not isolate (i.e. close off) the containment building without loss of primary coolant pump seal cooling because of the inflexible design of the isolation system. Automatic isolation was even less helpful and was in fact overridden by the operators.
AND	18	Gases and vapour were pumped from the RC drain tank into the waste gas header which had leaks and pressure relief devices - so that gases and vapour escaped to the atmosphere.
RESULT	19	Much of the noble gas fission products and a small amount of radioactive iodine escaped to the atmosphere and caused limited radiation exposure of the public. Much of the radioactive iodine was trapped in water in the auxiliary building and the containment building. Hydrogen, formed from overheated fuel sheaths in contact with steam, burned in the reactor building.

End State



TMI-2 end-state configuration

TMI Bottom Head Peak Temperature Estimates



Some Lessons Learned

- Design of valve position indicators
- Operator training / aids
- Hydrogen control
- Primary Coolant Pumps
- Revise prescriptive approach
- Severe Accidents – PSA
- Wetter is better $CsI \longrightarrow Cs^{+} + I^{-}$

Another Point of View - 1
James Reason, "Human Error"

Maintenance crew introduces water into the instrument air system.	Although this error had occurred on two previous occasions, the operating company had not taken the steps to prevent its recurrence. *(Management failure)*
Turbine tripped. F/W pumps shut down. Emergency F/W Pumps come on automatically, but flow blocked by two closed valves.	The two block valves had been erroneously left in the closed position during maintenance, probably carried out on two days prior to the accident sequence. On of the warning lights showing that valves were closed was obscured by a maintenance tag. *(Maintenance failures)*

Another Point of View -2 James Reason, "Human Error"

Rapid rise in core temperature and pressure, causing the reactor to trip. Relief valve (PORV) opens automatically, but then sticks in the open position. The scene is now set for a loss of coolant accident (LOCA) 13 seconds into the emergency.	During an incident at the Davis-Besse plant (another Babcock & Wilcox PWR) in September 1977, the PORV also stuck open. The incident was investigated by Babcock & Wilcox and the US Nuclear Regulatory Commission. However, these analyses were not collated, and the information obtained regarding appropriate operator action was not communicated to the industry at large. *(Regulatory failure)*

Another Point of View - 3
James Reason, "Human Error"

Operators fail to recognize that the relief valve is stuck open. Primary cooling system now has a hole in it through which radioactive water, under high pressure, pours into the containment area, and thence down into basement.	1. Operators were misled by control panel indications. Following an incident 1 year earlier, an indicator light had been installed. But this merely showed whether or not the valve had been commanded shut: it did not directly reveal valve status. *(Design and management failures)* 2. Operators wrongly assumed that high temperature at the PORV drain pipe was due to a chronically leaking valve. The pipe temperature normally registered high. *(Management / procedural failure)*

Another Point of View - 4 James Reason, "Human Error"

Operators failed to diagnose stuck – open PORV for more than 2 hours. The resulting water loss caused significant damage to the reactor.	1. The control panel was poorly designed with hundreds of alarms that were not organized in logical fashion. Many key indicators were sited on the back wall of the control room. More than 100 alarms were activated with no means of suppressing unimportant ones. Several instruments went off – scale, and the computer printer ran more than 2 hours behind events. *(Design and management failures)* 2. Operator training, consisting largely of lectures and work in the reactor simulator, provided an inadequate basis for coping with real emergencies. Little feedback given to the students, and training program was insufficiently evaluated. *(Training and management failures)*

Another Point of View - 5 James Reason, "Human Error"

The crew cut back the high pressure injection (HPI) of the water into the reactor coolant system, thus reducing the net flow rate from around 1000 gallons/min to about 25 gallons/min. This 'throttling' caused serious core damage.	1. Training emphasized the dangers of flooding the core. But this took no account of the possibility of a concurrent LOCA. *(Training and management failures)* 2. Following the 1977 Davis-Besse incident, the Nuclear Regulatory Commission issued a publication that made no mention of the fact that these operators had interrupted the HPI. The incident appeared under the heading of "valve malfunction" not "operator error". *(Regulatory failure)*

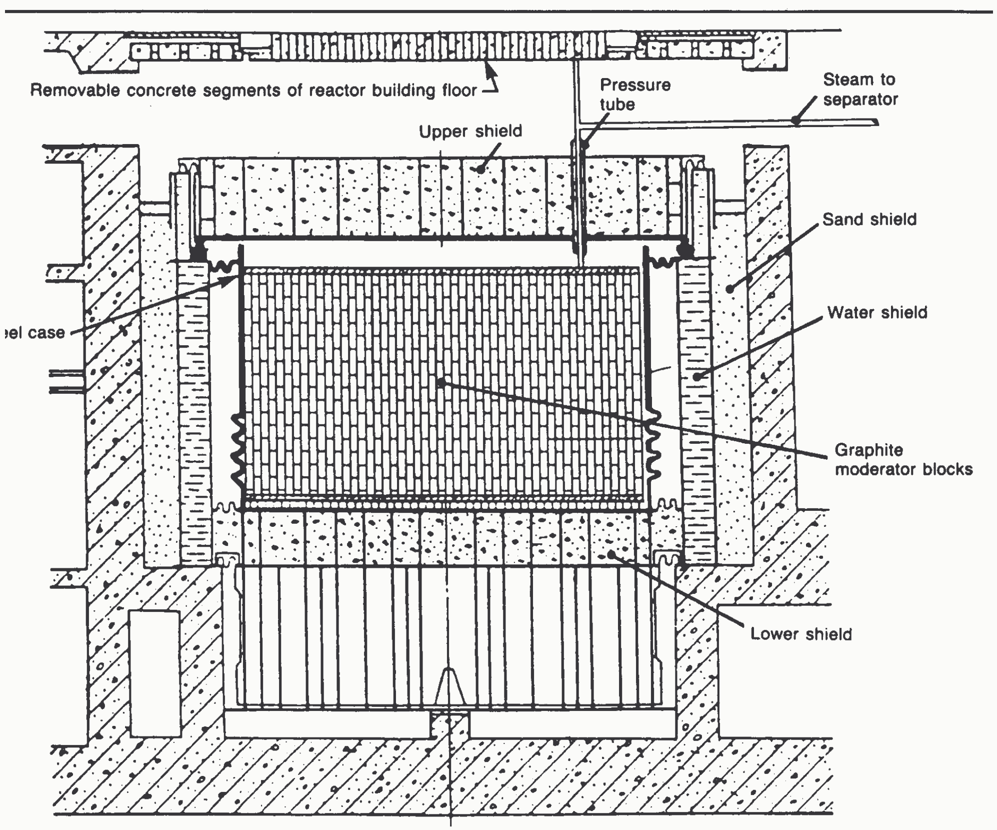
Some More TMI Lessons

- "A Review of Recommendations Arising from the Three Mile Island Accident", TMI Task Group, Ontario Hydro, August 1980 (3 volumes)
- "Fact Sheet on the Accident at Three Mile Island", US Nuclear Regulatory Commission, ~1993

  www.nrc.gov/reading-rm/doc-collections/fact-sheets/
- "Human Error", James Reason, Cambridge University Press, 1990, ISBN 0-521-30669-8 p. 251
- General info: "Managing the Unexpected - Assuring High Performance in an Age of Complexity", K.E. Weick & K.M. Sutcliffe, Jossey-Bass, 2001

Chernobyl - Core

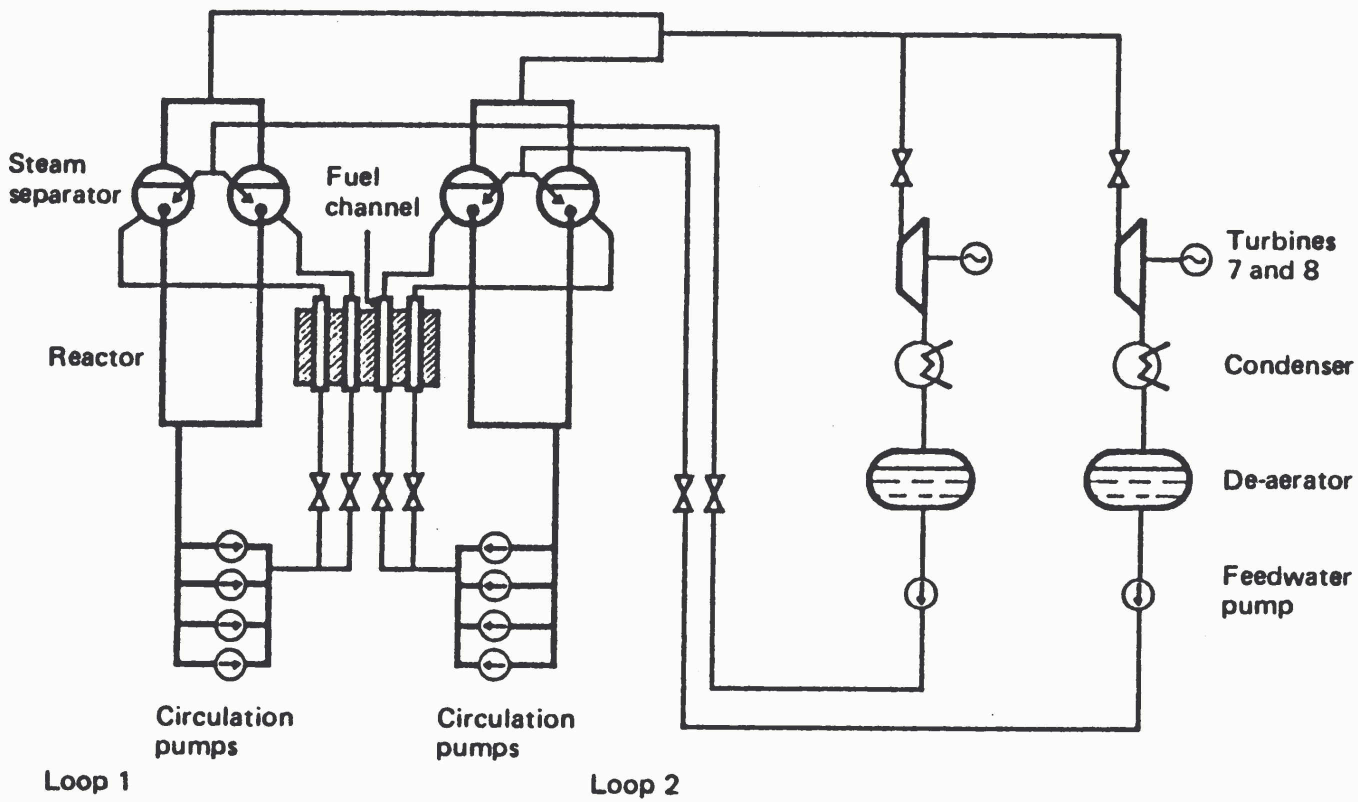
- Light-water cooled
- Direct cycle
- Vertical pressure tubes
- Graphite moderator
- Positive void coefficient which depended on reactor state



Control System

- (24) Shortened absorbing rods
- (24) Auto control rods
  - (12) Local auto control (LAC)
    -- 12 control zones
  - (12) Average power control
    -- 3 banks of 4 rods each
- (139) Manual rods
- (24) Emergency rods
  - (Manual rods and Emergency rods together:)
  - (24) Emergency control
    -- uniformly selected
  - (24) Local emergency protection
    -- 2 rods per zone
  - (115) Manual control

Steam and Feedwater System



Accident Sequence

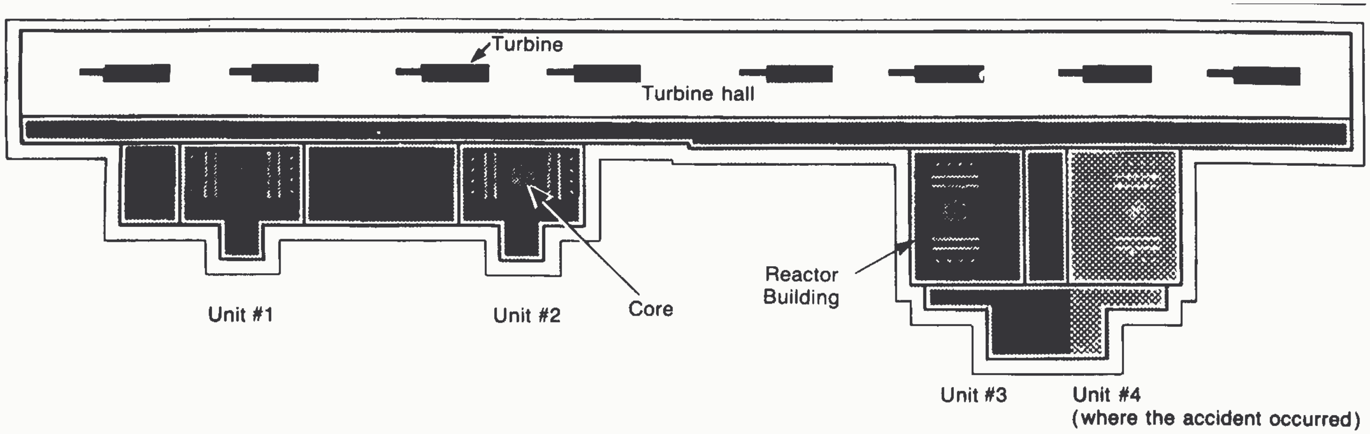
- Test to show that a running-down turbine could power main pumps
- Reactor & pump trip at low power with core near saturation
- Power rise due to positive void
- Accelerated by reverse action of shutoff rods
- Fuel vaporization, steam explosion
- Ejection of core lid

Reactivity History

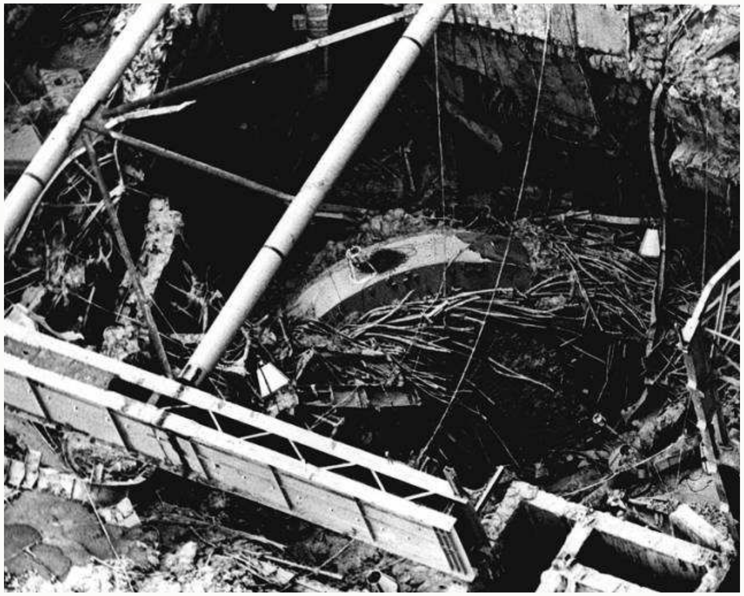
Time	Net Reactivity (%)
01:23:30	0.00
01:23:31	0.08
01:23:40	0.15
01:23:41	0.30
01:23:42	0.50
01.23:43	0.80
01:23:43.4	1.00
01:23:44	0.30
01:23:44.7	-0.15
01:24:44.9	1.40
01:24:45.3	1.00
01:24:45.5	0.00
01:24:46.9	-1.00

Accident Sequence - 2

- Massive core destruction / dispersal – subcritical
- Graphite fire for several days
- Core melted and ‘lava’ flowed into rooms below reactor; core area empty



Chernobyl core damage



Remediation

- Extinguish roof fire
- Boron to ensure subcriticality
- Dolomite-lead-sand-clay to cover core, then nitrogen to stop fire
- Concrete sarcophagus around reactor
- Reduced void reactivity, improved SORs?

Core inventory on 26 April 1986			Total release during the accident	
Nuclide	Half-life	Activity (PBq)	Percent of inventory	Activity (PBq)
33Xe	5.3 d	6 500	100	6500
131I	8.0 d	3 200	50 - 60	~1760
134Cs	2.0 y	180	20 - 40	~54
137Cs	30.0 y	280	20 - 40	~85
132Te	78.0 h	2 700	25 - 60	~1150
89Sr	52.0 d	2 300	4 - 6	~115
90Sr	28.0 y	200	4 - 6	~10
140Ba	12.8 d	4 800	4 - 6	~240
95Zr	1.4 h	5 600	3.5	196
99Mo	67.0 h	4 800	>3.5	>168
103Ru	39.6 d	4 800	>3.5	>168
106Ru	1.0 y	2 100	>3.5	>73
141Ce	33.0 d	5 600	3.5	196
144Ce	285.0 d	3 300	3.5	~116
239Np	2.4 d	27 000	3.5	~95
238Pu	86.0 y	1	3.5	0.035
239Pu	24 400.0 y	0.85	3.5	0.03
240Pu	6 580.0 y	1.2	3.5	0.042
241Pu	13.2 y	170	3.5	~6
242Cm	163.0 d	26	3.5	~0.9

Consequences

- 31 prompt deaths among cleanup crew
- Delayed cancer fatalities:
  - Several thousand if linear hypothesis is true at small doses – hard to observe
  - Few thousand excess thyroid cancers observed in children
  - Some increase in leukaemia among cleanup crew
  - No other cancers observed in population

Root Causes - Design

- Void reactivity strongly dependent on operating state (30 mk. just before accident)
- Shutdown slow, shared with control system and dependent on operating state
- Shutoff rods worked in reverse if fully withdrawn

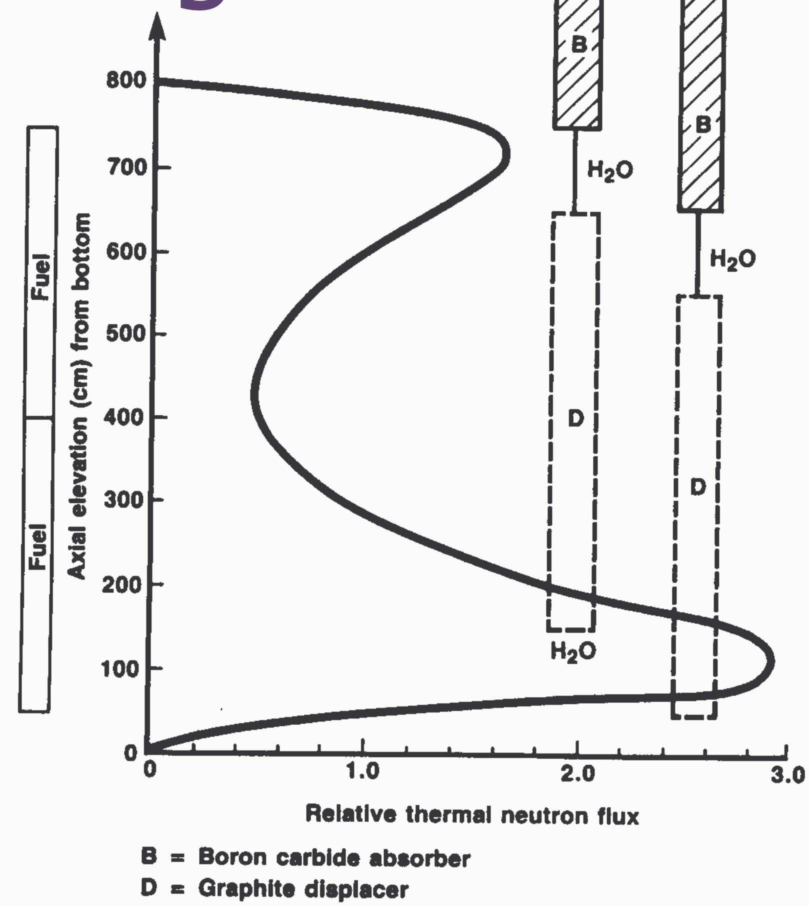


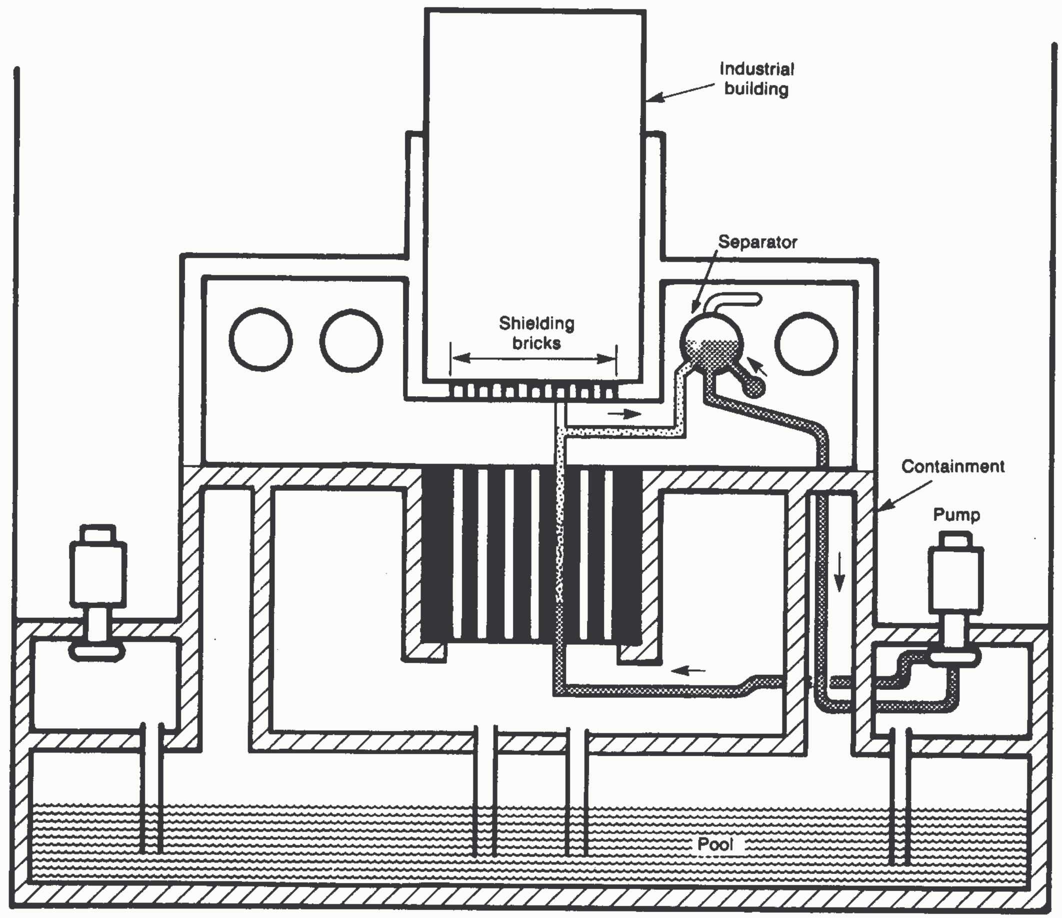
Figure 5 Axial flux distribution preceding accident.

Root Causes - Operation

- Test procedure subject to ad hoc alteration
- Operators did not follow procedures and/or
- Safety culture was not conducive to prudent operation

Contributing cause

- Containment bypassed (but not normally designed for reactor explosion)



Chernobyl - Some Lessons From 75-INSAG-1, IAEA 1986

- Root cause of the Chernobyl accident was the human element
  - Training, with emphasis on severe accident sequences
  - Auditing, (internal and external) especially to prevent complacency
  - Sustaining awareness of potential safety implication of mal-operation
  - CONCLUSION: place complete authority and responsibility for safety on a senior member of the operating staff of the plant. Create safety culture.
- Implement defence in depth concept in reactor design
  - Look for inherent stability of the chain reaction of the reactor
  - Automatic safety systems to act as soon as safety of the plant is threatened
  - Ultimate passive barrier (containment) to dispersion, in case all else fails
- If no feasible containment can be designed, special attention should be given to protect against the consequences of a reactivity excursion

Chernobyl - Some More Lessons From 75-INSAG-1, IAEA 1986

- A satisfactory man-machine interface is very important
  - Recognize that competent operators provide the first and best defence.
  - Ensure clear display of data vital to safety, including diagnostic capability
  - As backup to operators, install reliable safety backup to ensure that plant is within the safe operating envelope at all respects. This backup must be so designed as to be difficult to bypass, and so that normal or planned operation raises no temptation to bypass it.

A Close Call -- Davis-Besse

- PWR, 873 MWe, started up in 1977
- Boric acid clogged containment air cooler in 1999
- Containment radiation monitor showed contamination and clogging in May 1999
- Significant head corrosion began in 1998 or earlier
- Five control rod penetration nozzles were cracked, 3 penetrated nozzle wall
- Large cavity in vessel wall, sealed only by vessel liner
- NRC placed 27 PWR plants in the ‘high risk’ category for vessel corrosion - some in vessel bottom penetrations

Davis-Besse Head Corrosion Location

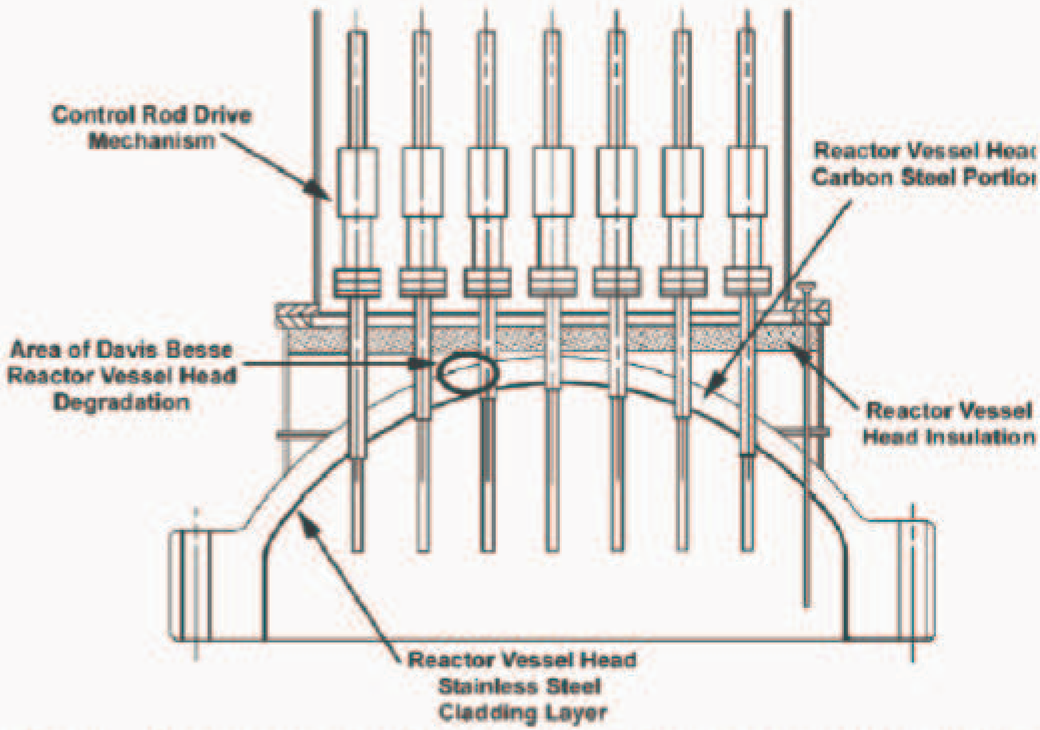
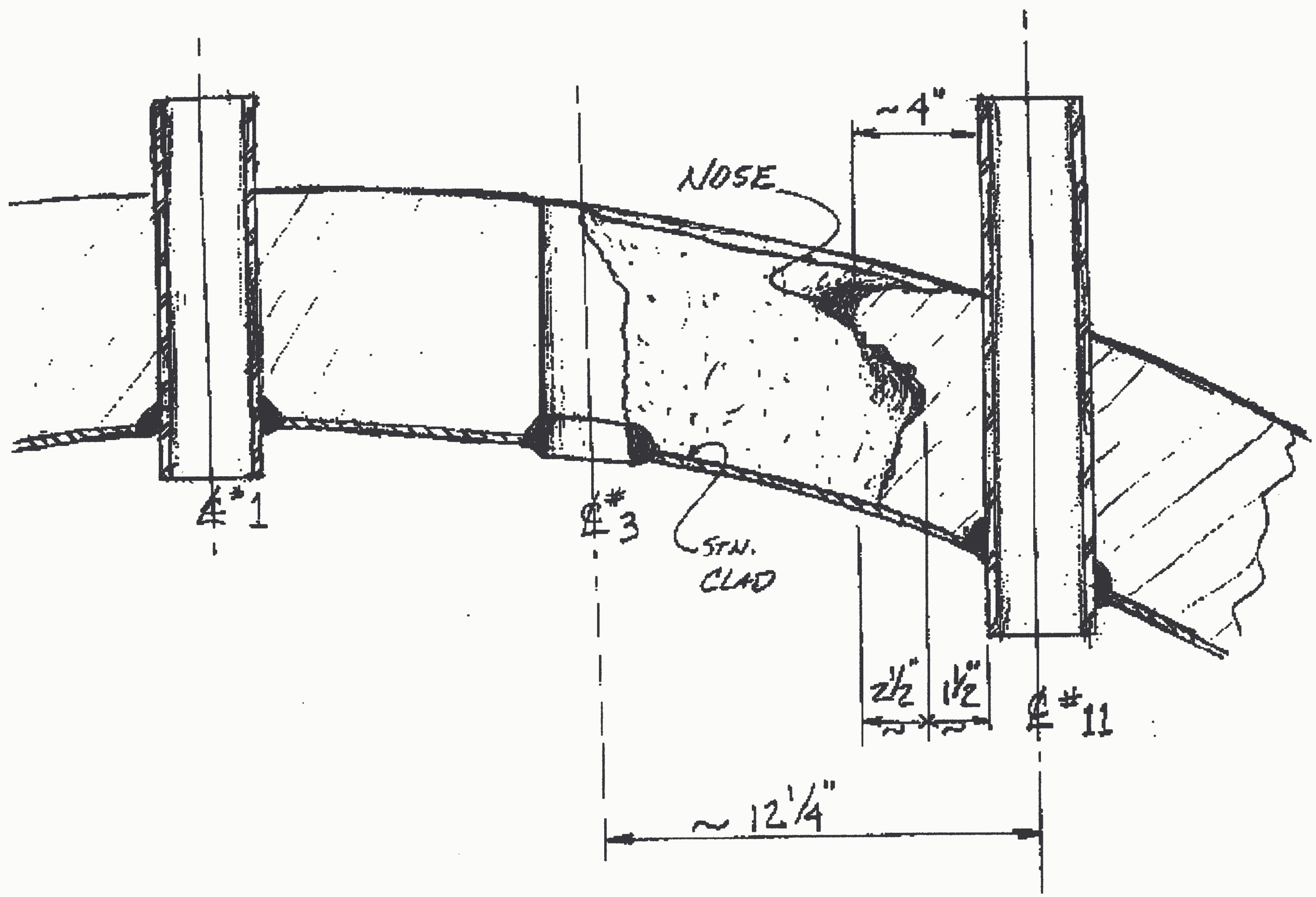


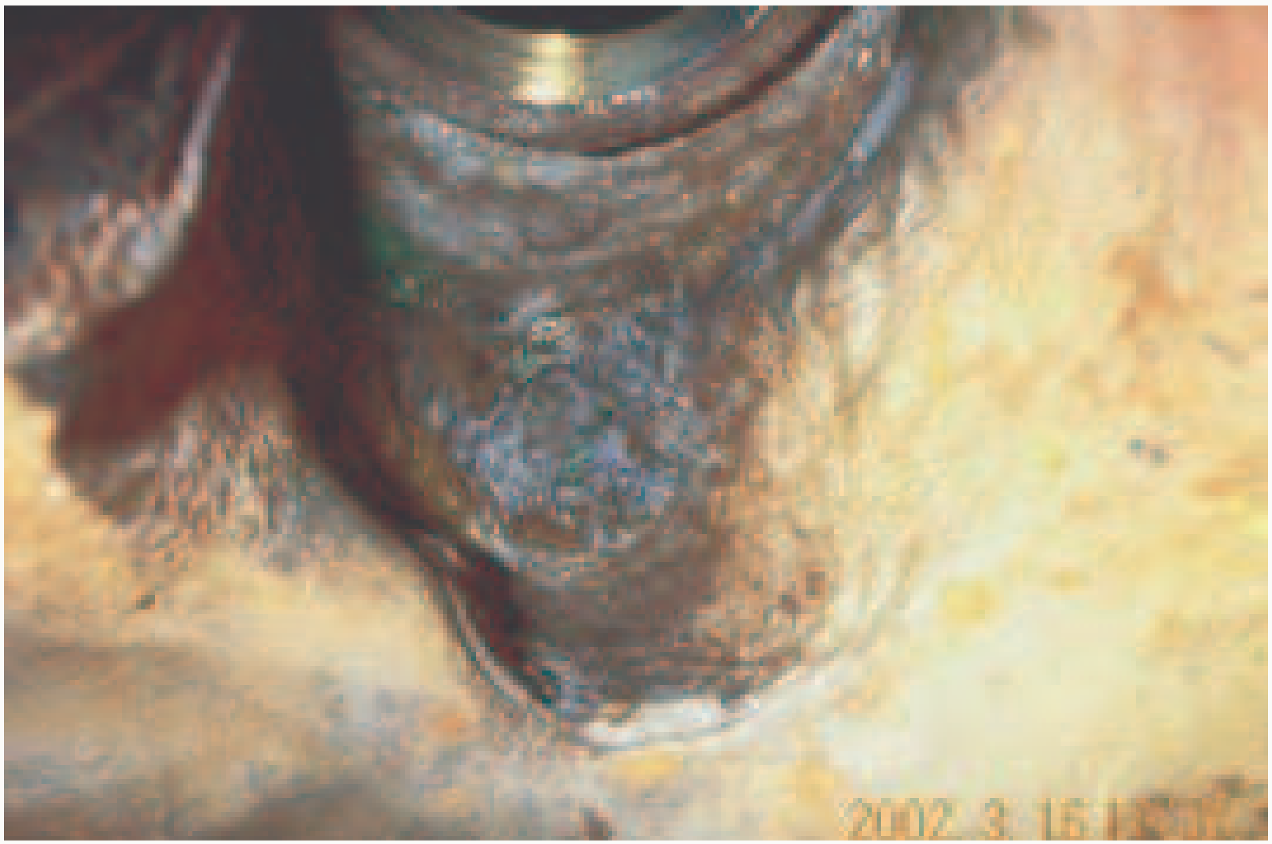
Figure 1. Reactor pressure vessel head at the Davis-Besse nuclear generating station.

Davis-Besse Head Cross-Section Showing Damage



DB - A Hole in the Head
Stainless steel liner bulged, but did not fail

Close-up of Hole, from Top



Lessons to be Learned

?