Writing software to control Sizewell B Nuclear Power Station

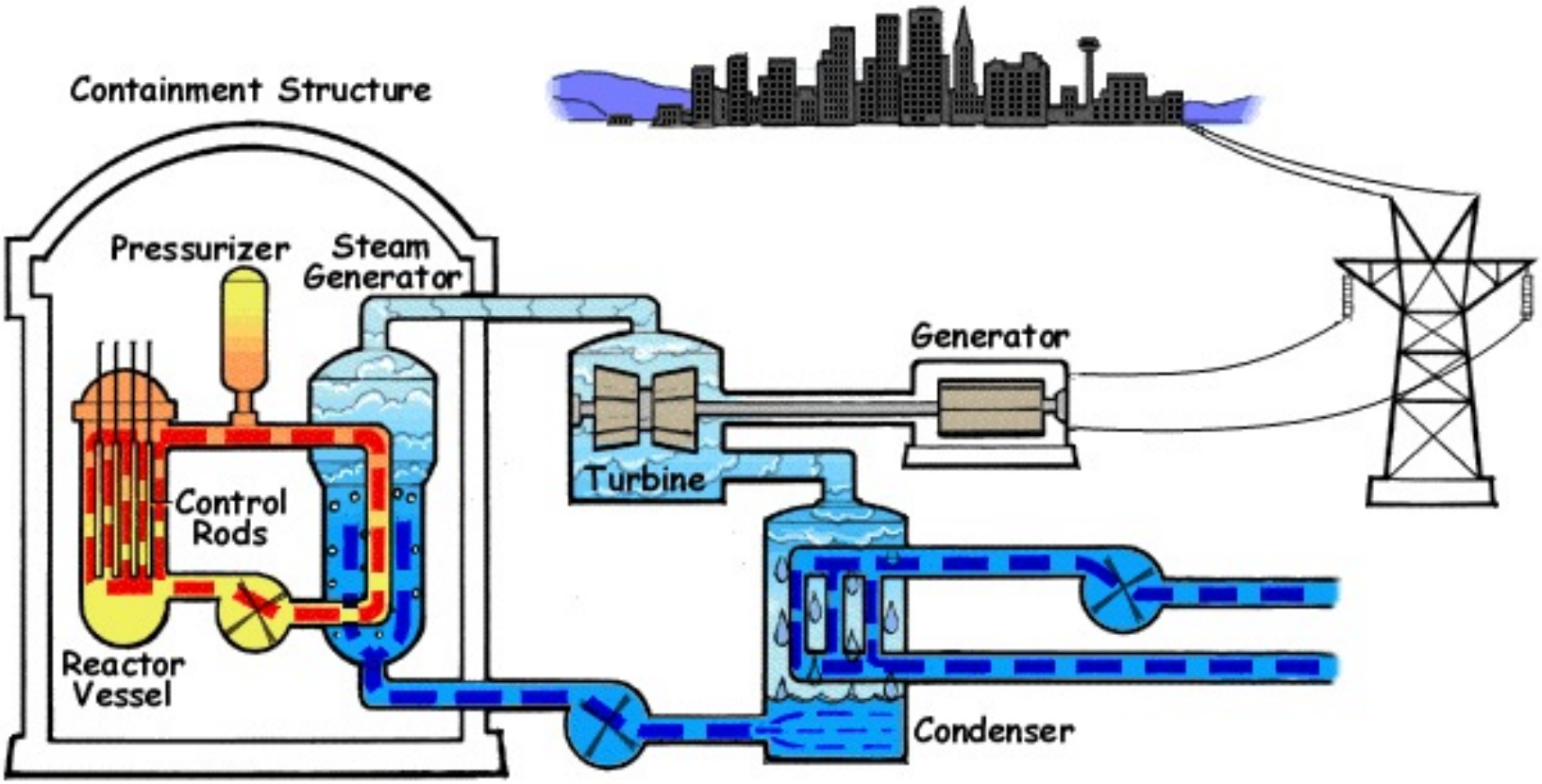
Dr Robin Wilson

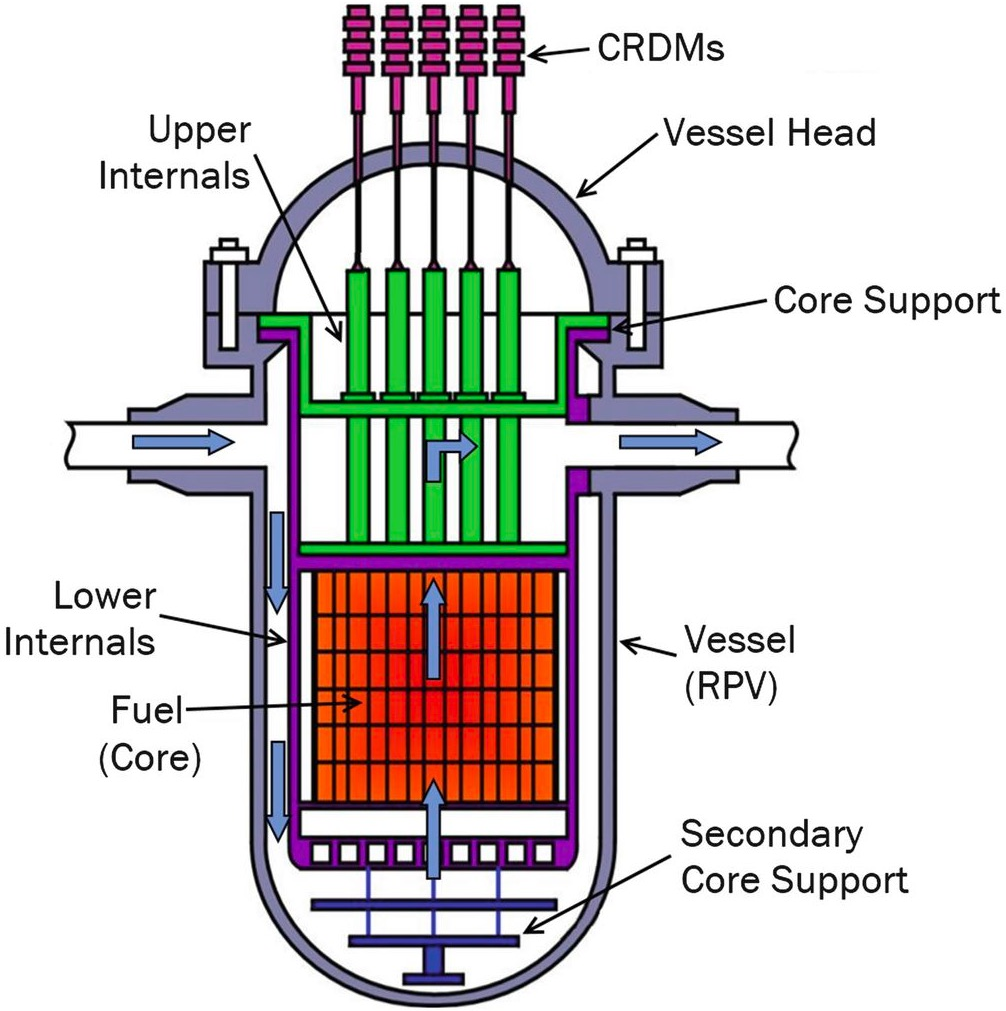
@sciremotesense

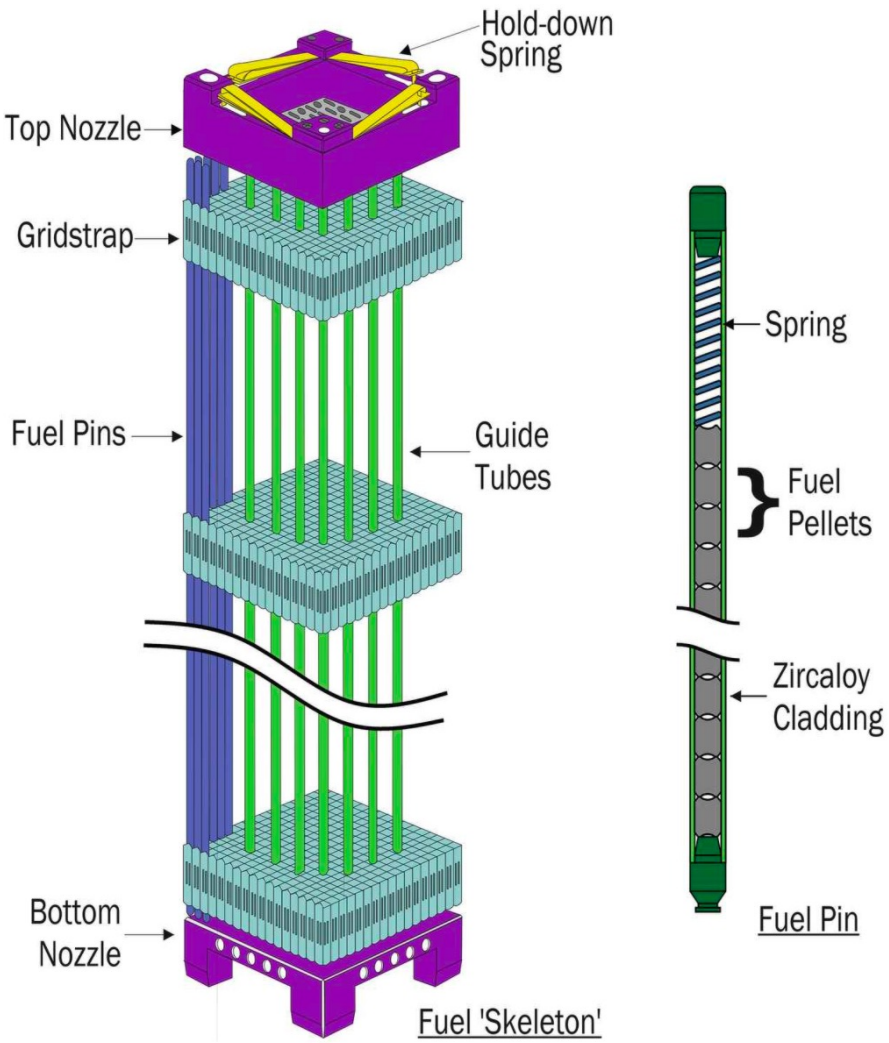
robin@rtwilson.com

(with pictures of the inside of a nuclear reactor!)

Started generating 1994


Containment Structure
Pressurizer
Steam Generator
Control Rods
Reactor Vessel
Turbine
Generator
Condenser


CRDMs
Upper
Internals
Vessel Head
Core Support
Lower
Internals
Vessel
(RPV)
Fuel
(Core)
Secondary
Core Support


Hold-down Spring
Top Nozzle
Gridstrap
Fuel Pins
Guide Tubes
Bottom Nozzle
Fuel 'Skeleton'
Spring
Fuel Pellets
Zircaloy Cladding
Fuel Pin

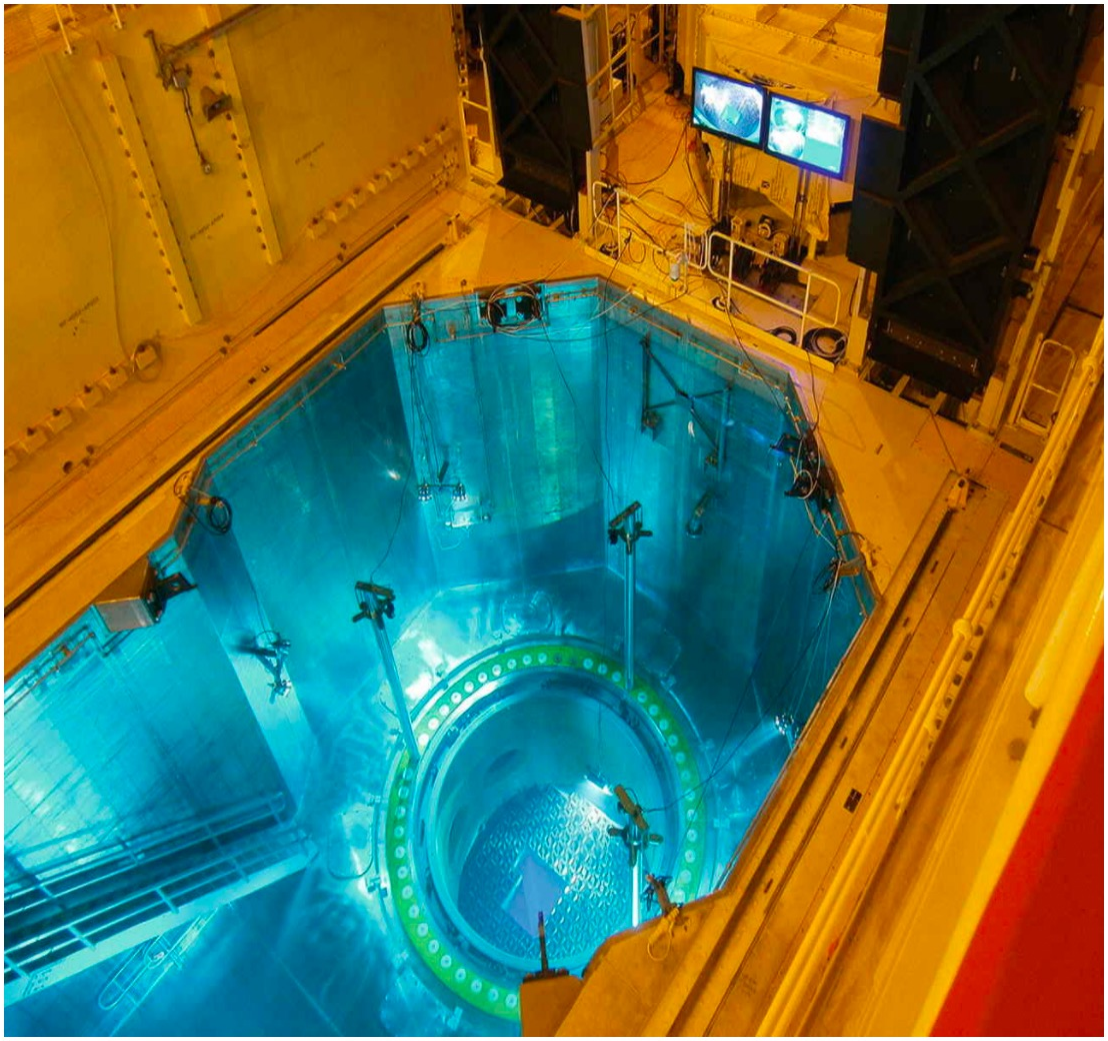


Photo: Colin Tucket

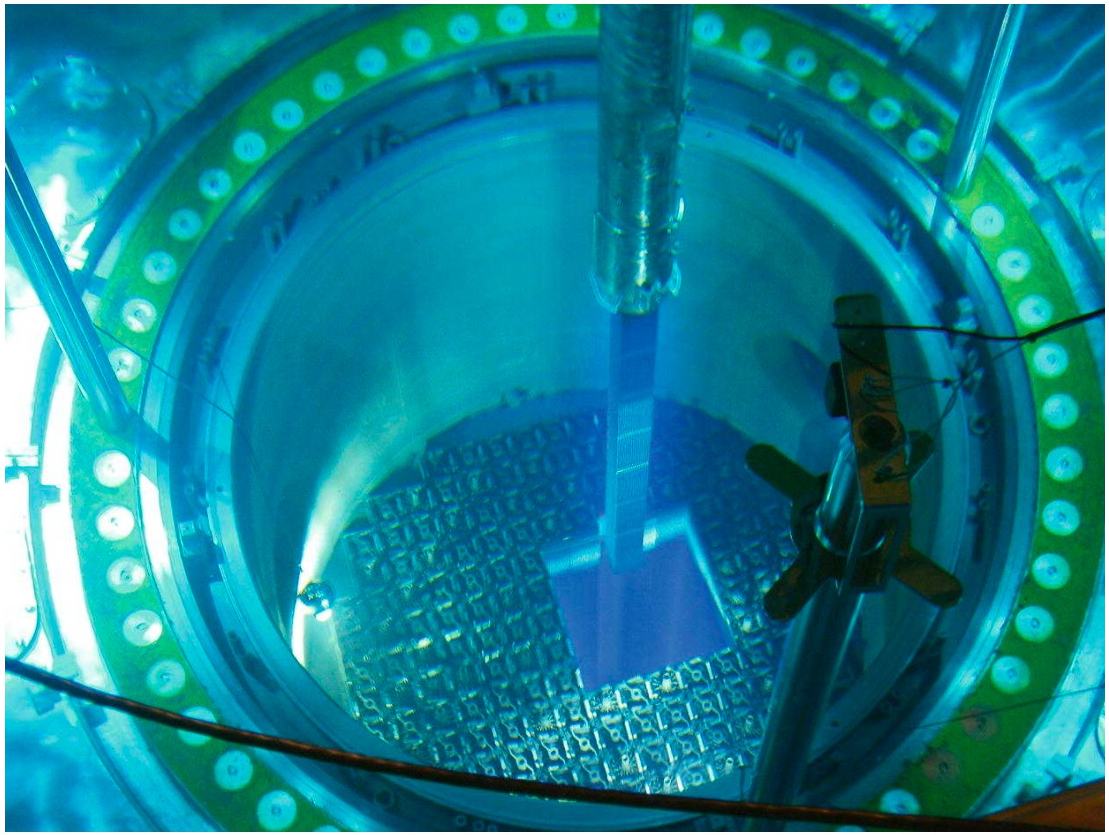
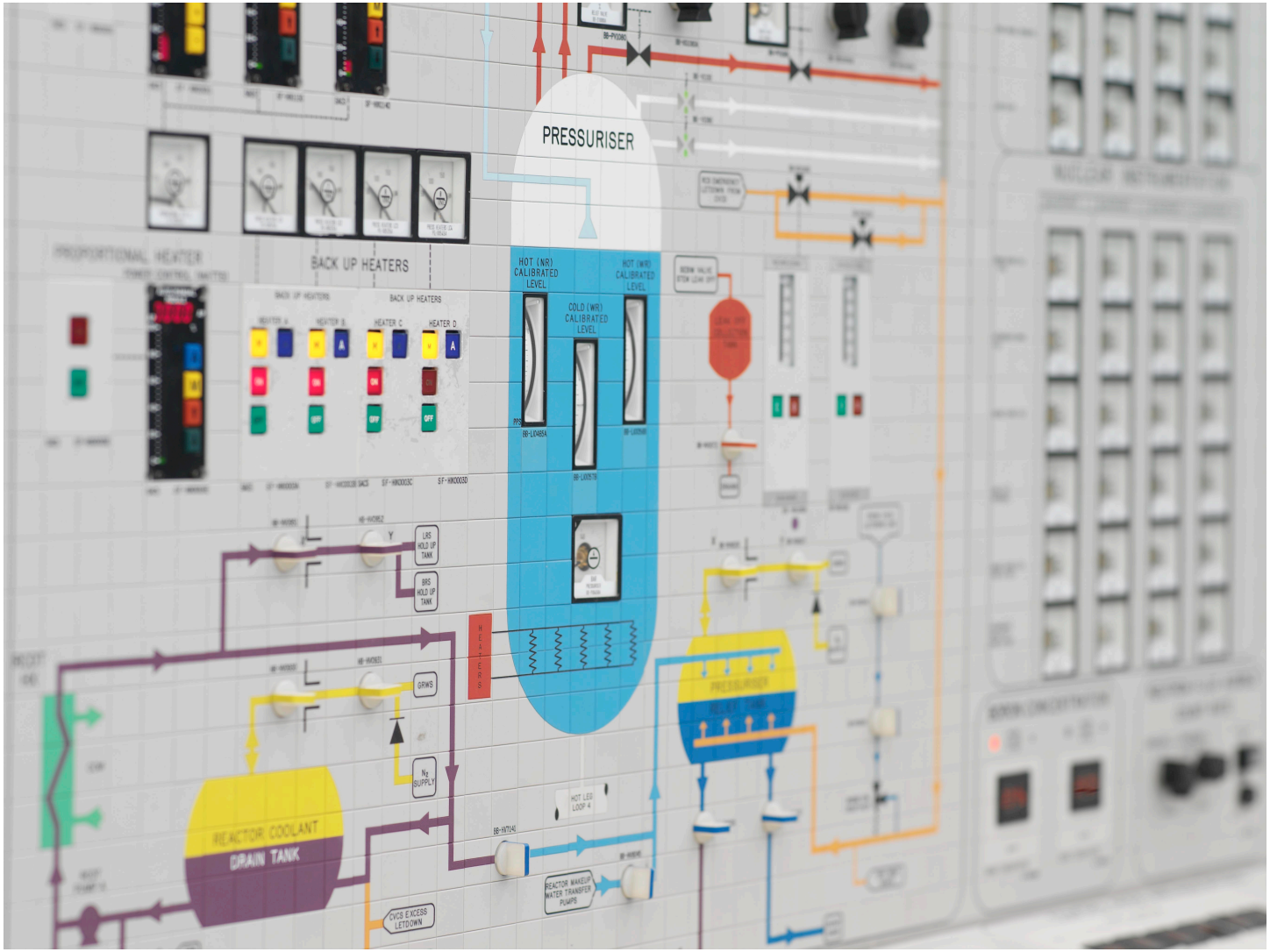
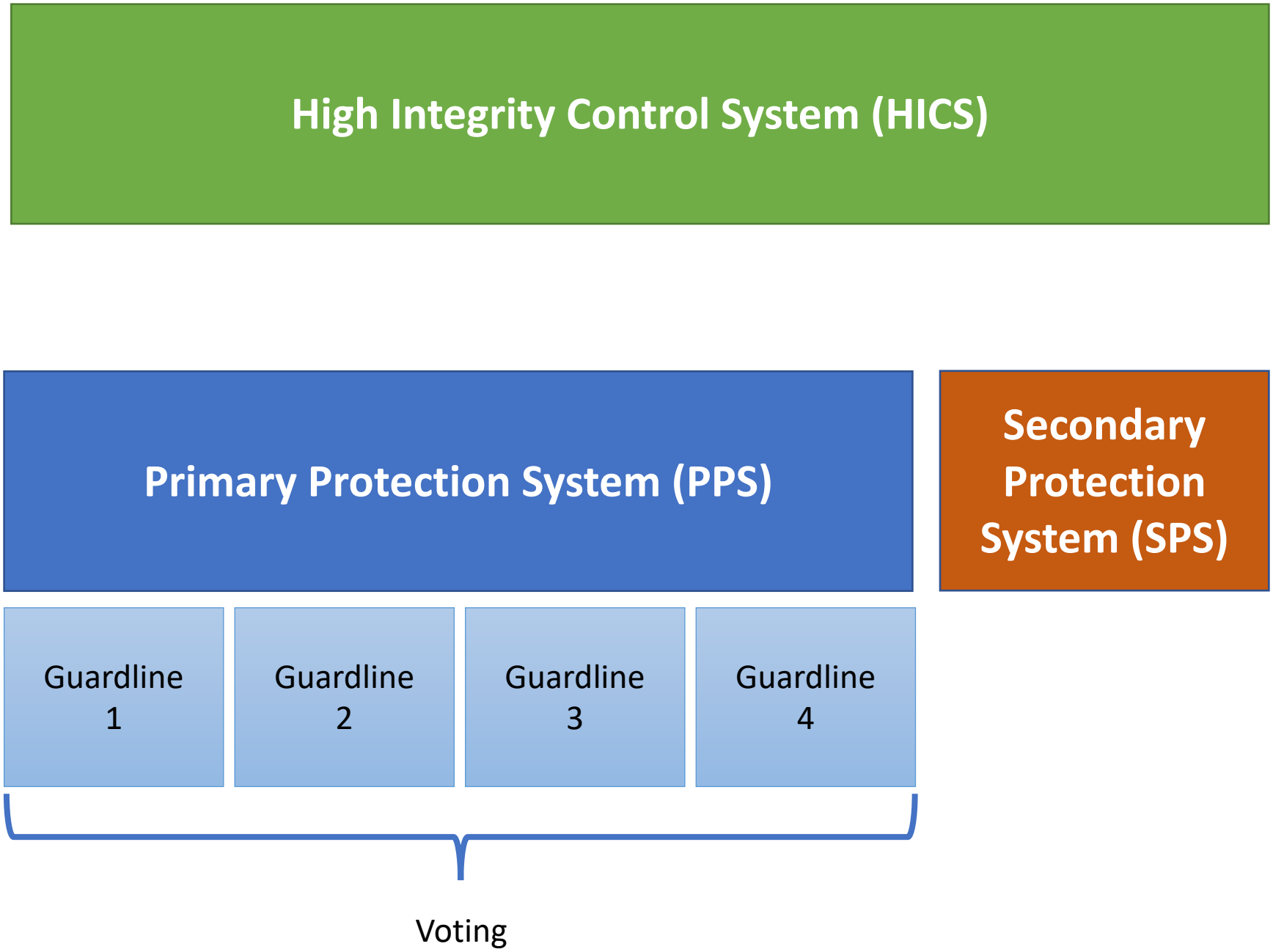


Photo: Colin Tucket


PRESSURISER
BACK UP HEATERS
HOT (NR) CALIBRATED LEVEL
COLD (WR) CALIBRATED LEVEL
HOT (WR) CALIBRATED LEVEL
HEATER A
HEATER B
HEATER C
HEATER D
ON
OFF
LRS HOLD UP TANK
BRS HOLD UP TANK
GRWS
N2 SUPPLY
REACTOR COOLANT DRAIN TANK
CVCS EXCESS LETDOWN
REACTOR MAKEUP WATER TRANSFER PUMPS
HOT LEG LOOP 4


High Integrity Control System (HICS)
Primary Protection System (PPS)
Secondary Protection System (SPS)
Guardline 1
Guardline 2
Guardline 3
Guardline 4
Voting

Trip parameters

source range neutron flux
intermediate range flux
power range flux
nitrogen-16 power measurement
core limit calculation for low DNBR (Departure from Nucleate Boiling Ratio)
linear power density (kW/m)
rod cluster control assembly misalignment calculations
rod cluster control assembly bank movement surveillance
rod cluster control assembly bank insertion calculations
pressuriser pressure
pressuriser level
reactor coolant system flow rate
reactor coolant cold leg narrow range temperature
steam generator narrow range water level
loss of 11 kV supply detected
both main turbines detected tripped

Trip actions

- Drop control rods
- Turn off stuff
- Trip turbines
- Alert staff

Post-trip actions

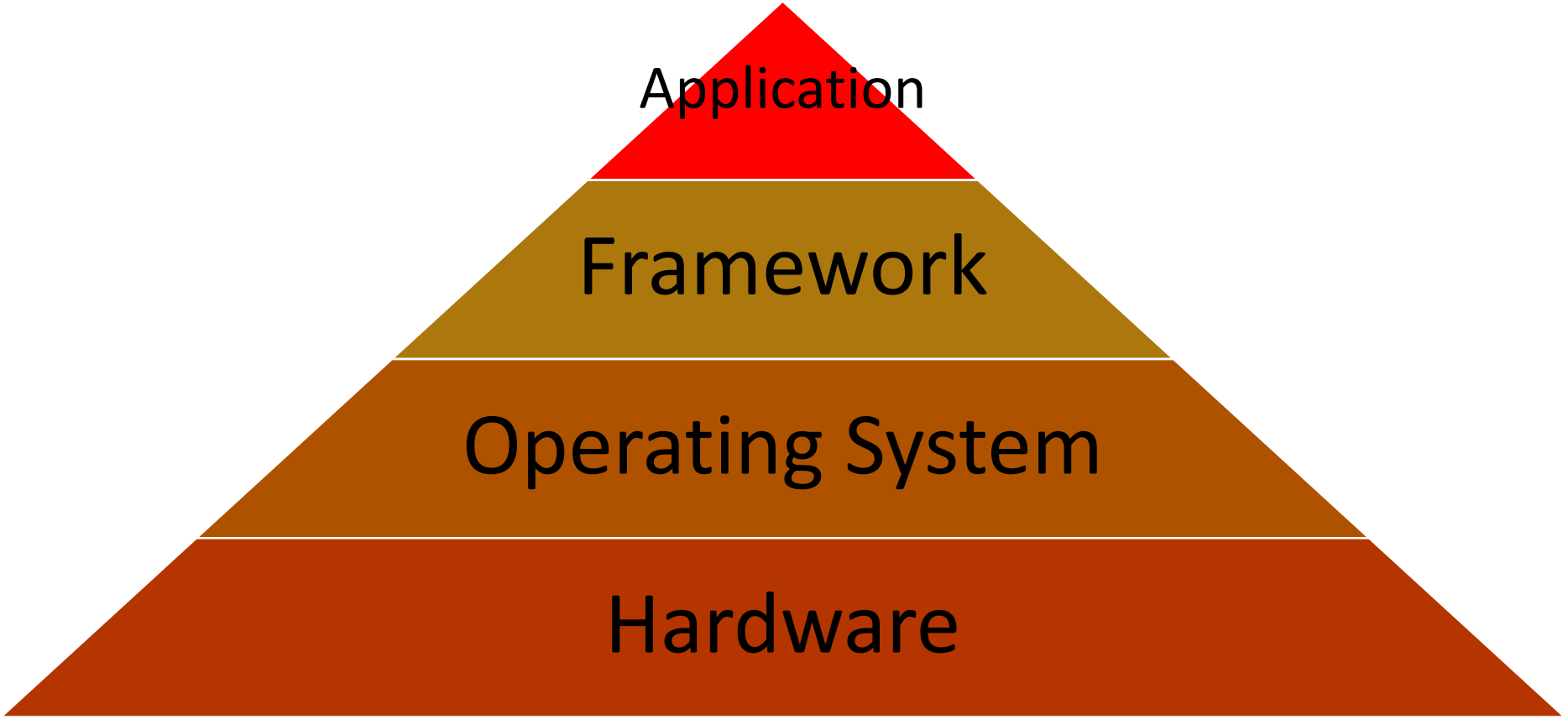
- Cooling – lots and lots
- Start loads of extra systems

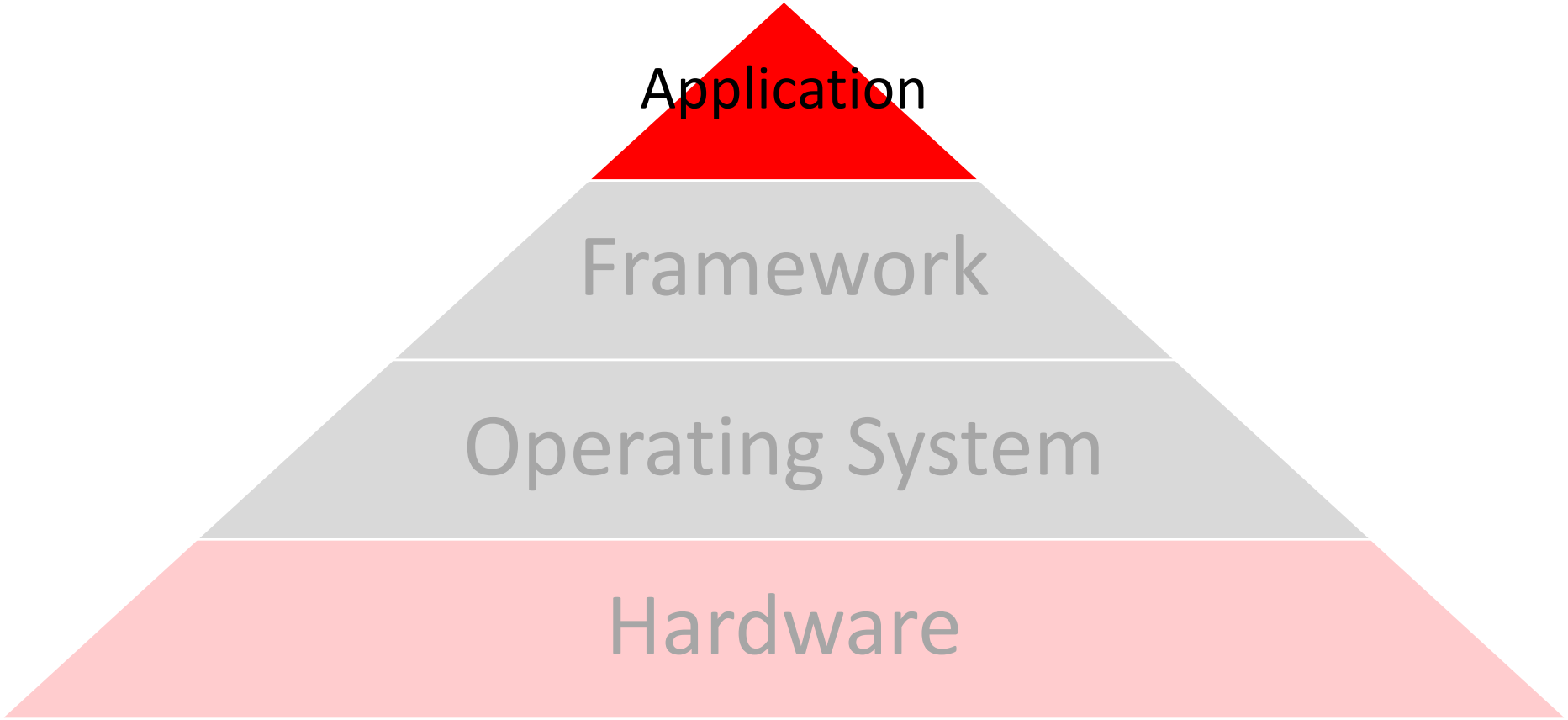
Safety critical software

First use of software PPS in UK

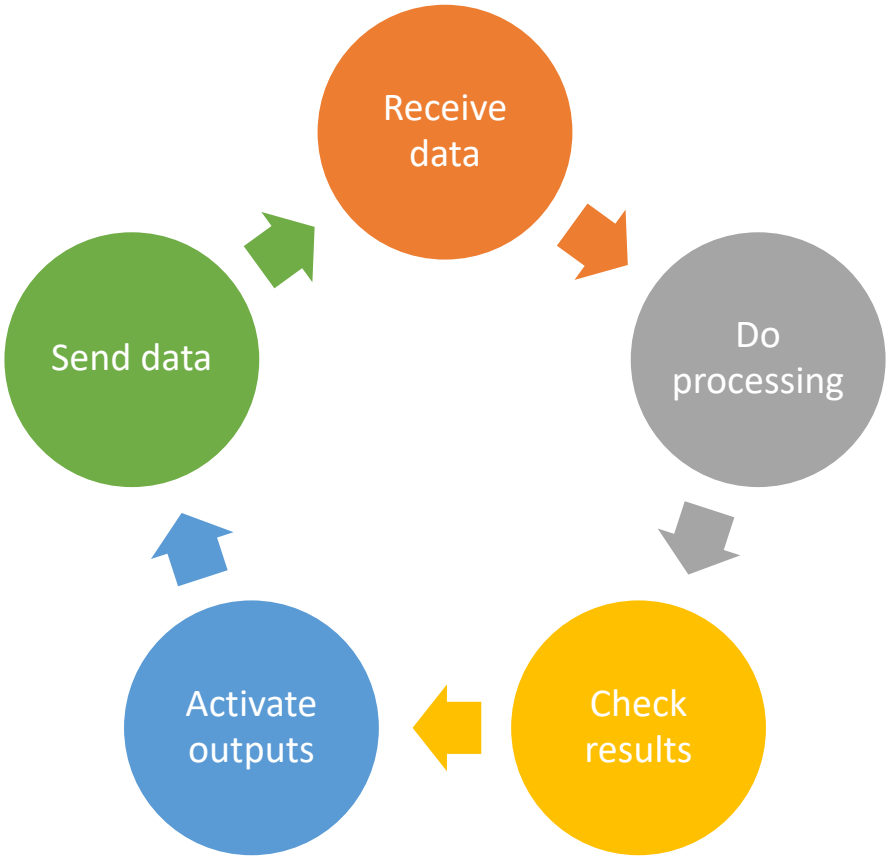
How can we make it with **no bugs?**
And tiny possibility of **crashing?**

High-integrity Software Engineering


Application
Framework
Operating System
Hardware


Application
Framework
Operating System
Hardware

Earthquakes!



x86 Assembly and C

Infinite loop with fixed loop timing

RS-422 communications

8086 processor + PROMs

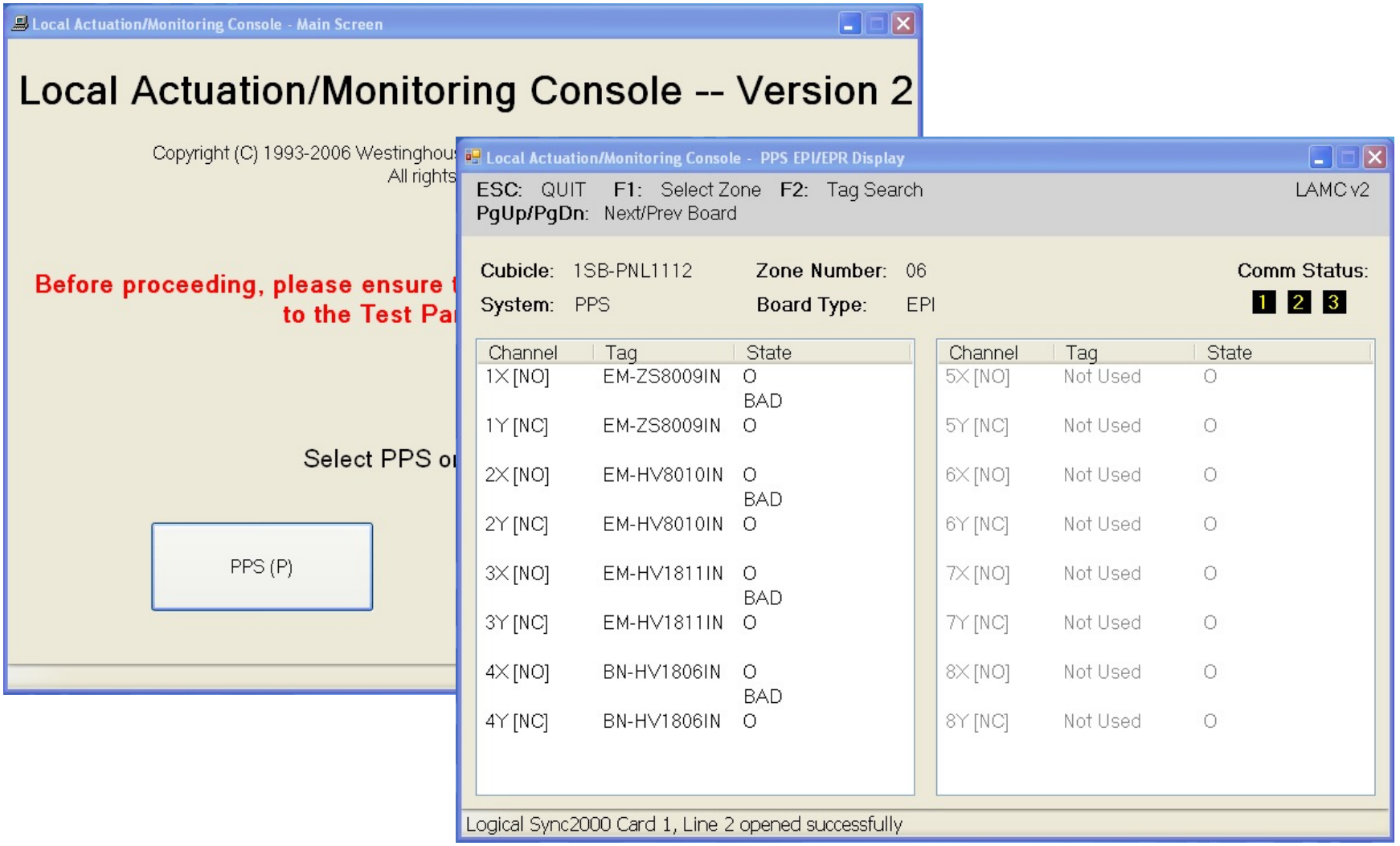

OFF
ON
1
2
3
4
5
6
7
ON
OFF
EPROM

MALPAS

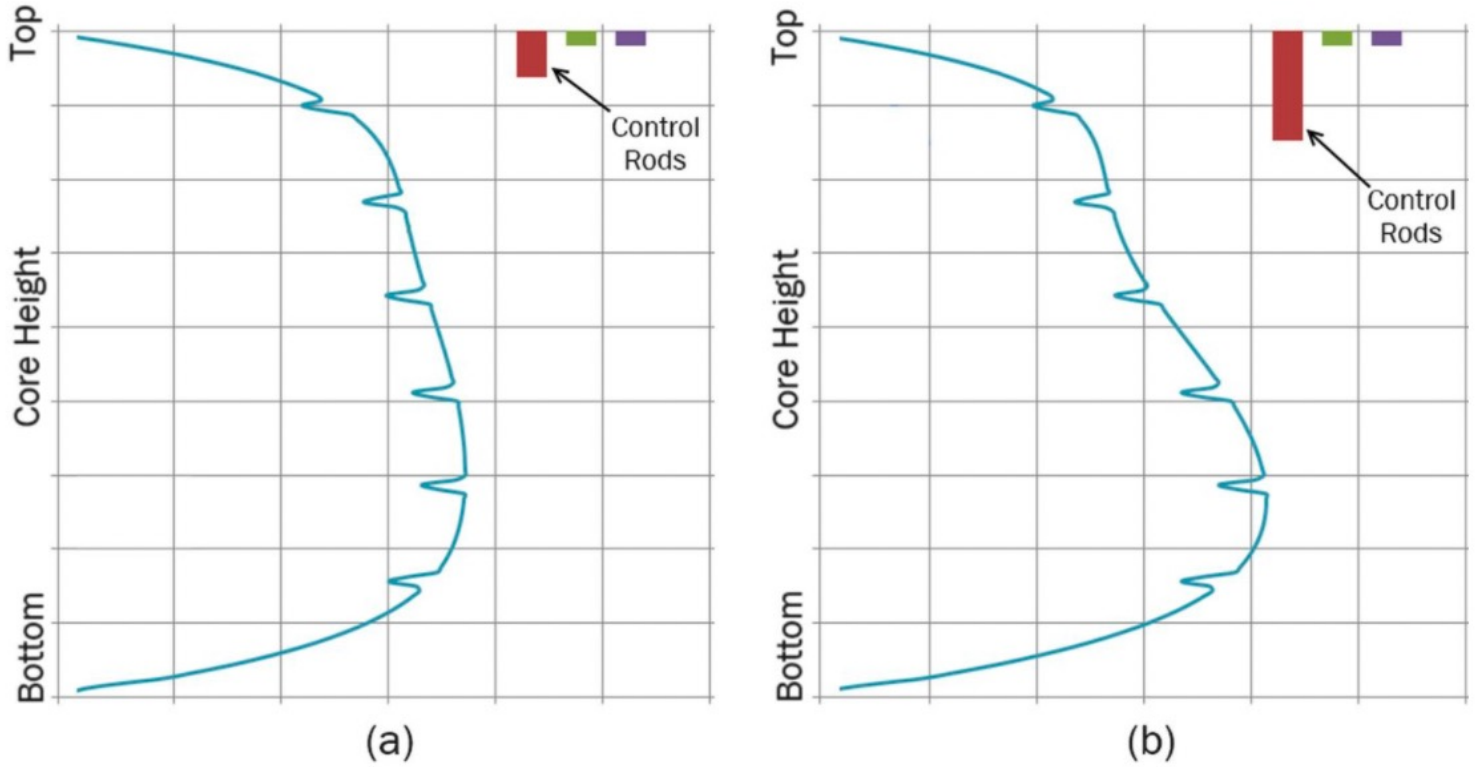
‘Prove’ software is correct

‘Safety Adjacent’ software


Local Actuation/Monitoring Console -- Version 2
Pro Visual C++/CLI

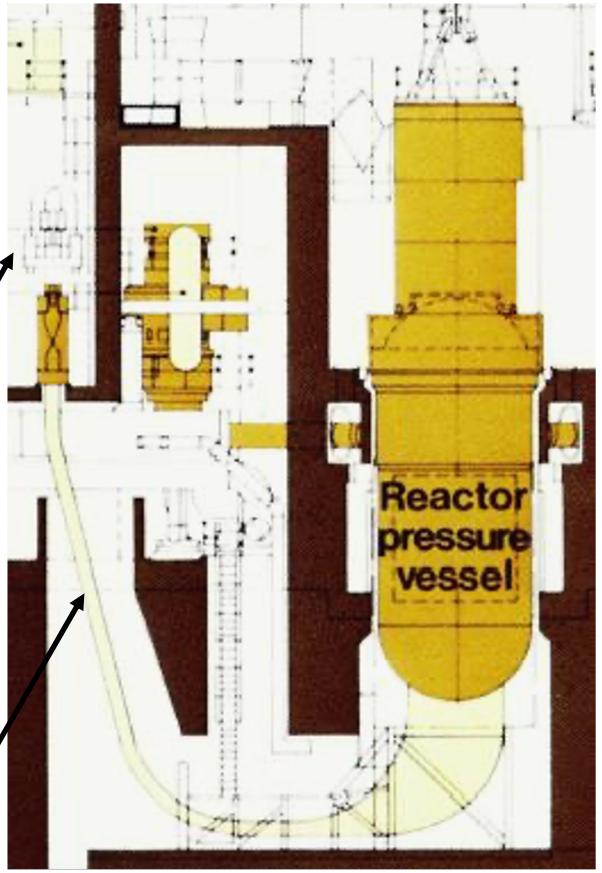

Local Actuation/Monitoring Console - Main Screen
Local Actuation/Monitoring Console -- Version 2
Copyright (C) 1993-2006 Westinghou
All rights
Before proceeding, please ensure t
to the Test Pa
Select PPS o
PPS (P)
Local Actuation/Monitoring Console - PPS EPI/EPR Display
ESC: QUIT F1: Select Zone F2: Tag Search
PgUp/PgDn: Next/Prev Board
LAMC v2
Cubicle: 1SB-PNL1112
Zone Number: 06
System: PPS
Board Type: EPI
Comm Status:
1 2 3
Channel Tag State
1X [NO] EM-ZS8009IN O
BAD
1Y [NC] EM-ZS8009IN O
2X [NO] EM-HV8010IN O
BAD
2Y [NC] EM-HV8010IN O
3X [NO] EM-HV1811IN O
BAD
3Y [NC] EM-HV1811IN O
4X [NO] BN-HV1806IN O
BAD
4Y [NC] BN-HV1806IN O
Channel Tag State
5X [NO] Not Used O
5Y [NC] Not Used O
6X [NO] Not Used O
6Y [NC] Not Used O
7X [NO] Not Used O
7Y [NC] Not Used O
8X [NO] Not Used O
8Y [NC] Not Used O
Logical Sync2000 Card 1, Line 2 opened successfully

Flux Mapping

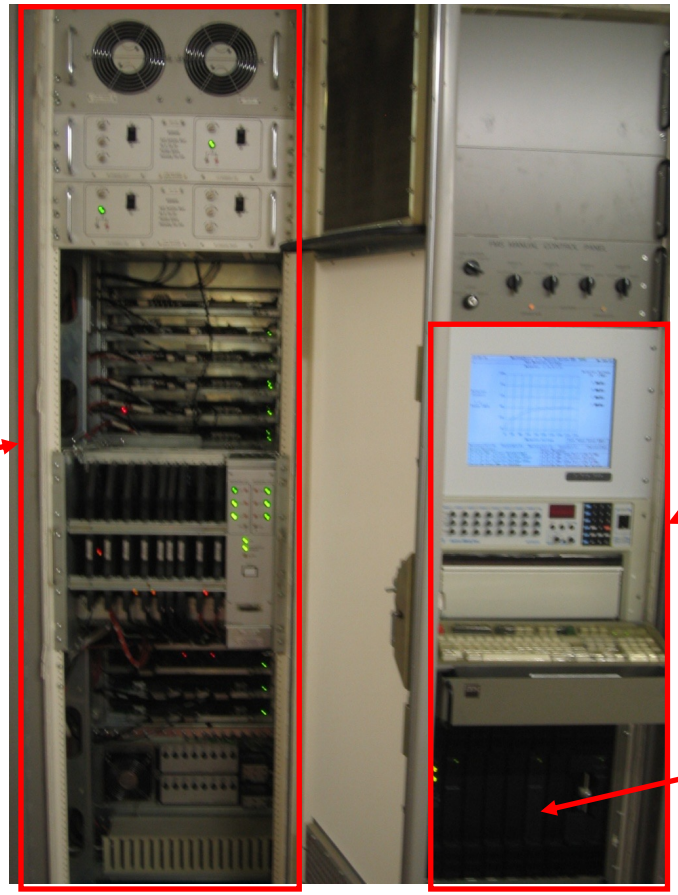


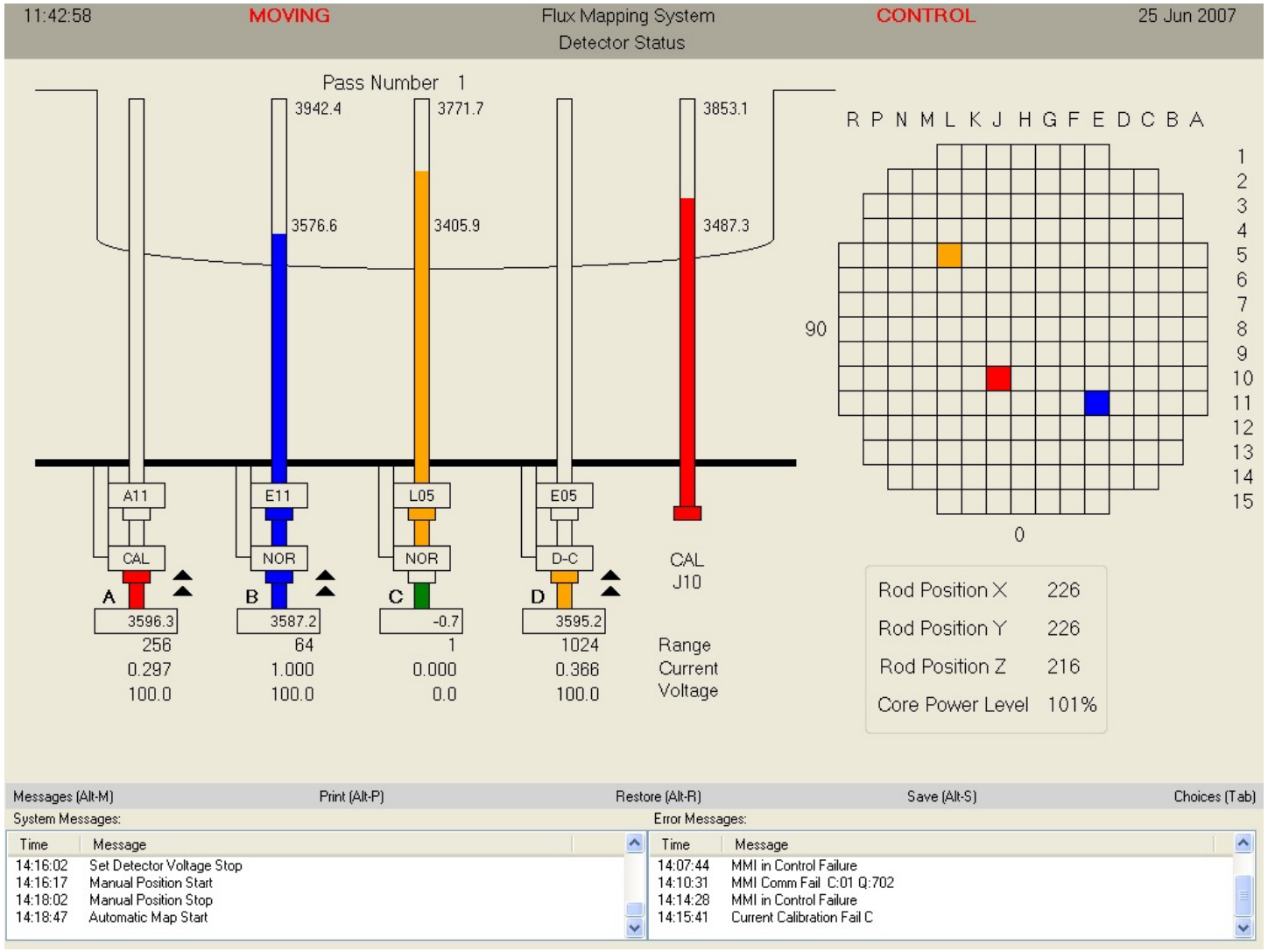
Detector Drive System

Thimble tubes



Flux Mapping System Man-Machine Interface (FMS MMI)

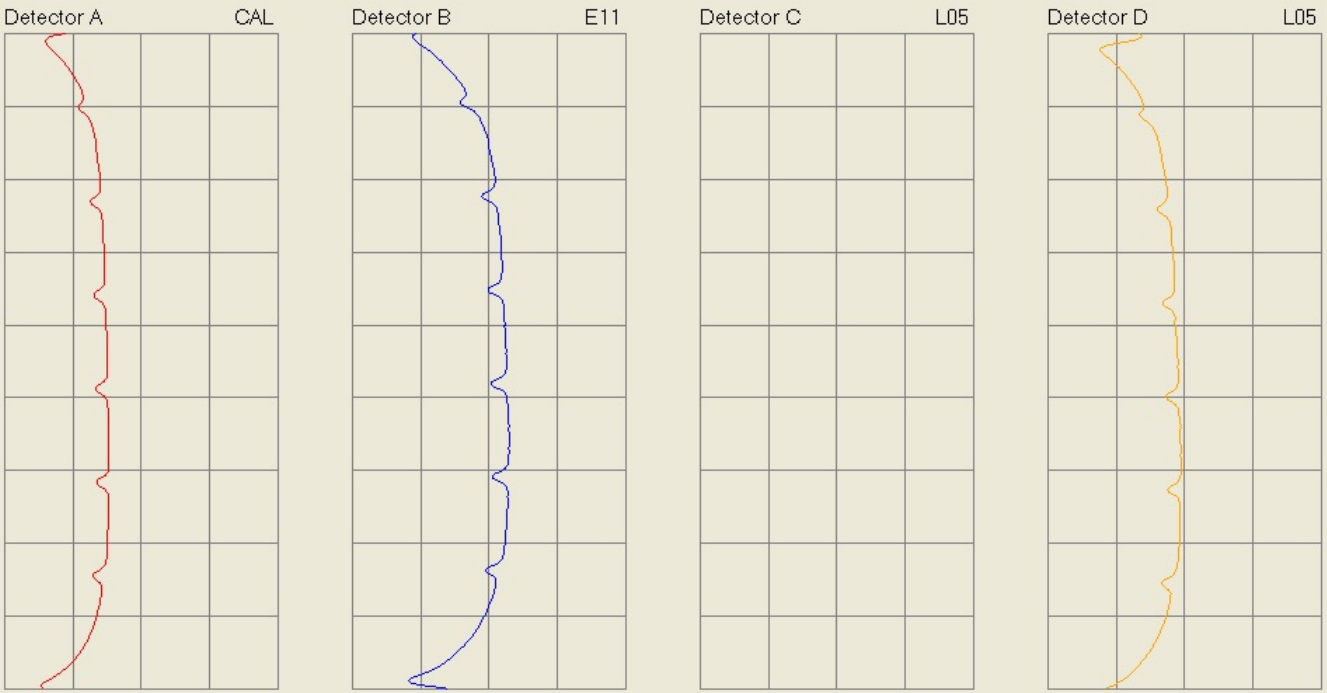



11:42:58
MOVING
Flux Mapping System
Detector Status
CONTROL
25 Jun 2007
Pass Number 1
3942.4
3771.7
3853.1
3576.6
3405.9
3487.3
A11
E11
L05
E05
CAL
NOR
NOR
D-C
A
B
C
D
3596.3
3587.2
-0.7
3595.2
256
64
1
1024
0.297
1.000
0.000
0.366
100.0
100.0
0.0
100.0
Range
Current
Voltage
CAL
J10
R P N M L K J H G F E D C B A
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
90
0
Rod Position X 226
Rod Position Y 226
Rod Position Z 216
Core Power Level 101%
Messages (Alt-M)
Print (Alt-P)
Restore (Alt-R)
Save (Alt-S)
Choices (Tab)
System Messages:
Time Message
14:16:02 Set Detector Voltage Stop
14:16:17 Manual Position Start
14:18:02 Manual Position Stop
14:18:47 Automatic Map Start
Error Messages:
Time Message
14:07:44 MMI in Control Failure
14:10:31 MMI Comm Fail C:01 Q:702
14:14:28 MMI in Control Failure
14:15:41 Current Calibration Fail C

11:44:45 MOVING Flux Mapping System CONTROL 25 Jun 2007

Live Graph Display

Map Filename: BWD11 Pass: 1



Range:	256	Range:	1024	Range:	1	Range:	1024
Current:	0.000	Current:	0.000	Current:	0.000	Current:	0.000
Voltage:	100.0	Voltage:	100.0	Voltage:	0.0	Voltage:	100.0

Messages (Alt-M) Print (Alt-P) Restore (Alt-R) Save (Alt-S) Choices (Tab)

System Messages:

Time	Message
14:16:02	Set Detector Voltage Stop
14:16:17	Manual Position Start
14:18:02	Manual Position Stop
14:18:47	Automatic Map Start

Error Messages:

Time	Message
14:07:44	MMI in Control Failure
14:10:31	MMI Comm Fail C:01 Q:702
14:14:28	MMI in Control Failure
14:15:41	Current Calibration Fail C

Other systems and anecdotes:

Loose Parts Monitoring System
Seismic Monitoring System
Interlocking of PPS cubicle keys
Potassium Smarties & calendars
Hot winding corridor
Security – including on journey
Outage
Low-level nuclear waste
Training control room – and carpet tiles
Positioning of turbine and reactor