A Preliminary Study on How to Design Digital Safety I&C System for AP1000

- Hidekazu Yoshikawa
- Amjad Nawaz
- Zhanguo Ma
- Ming Yang

College of Nuclear Science and Technology
Harbin Engineering University, Harbin, China

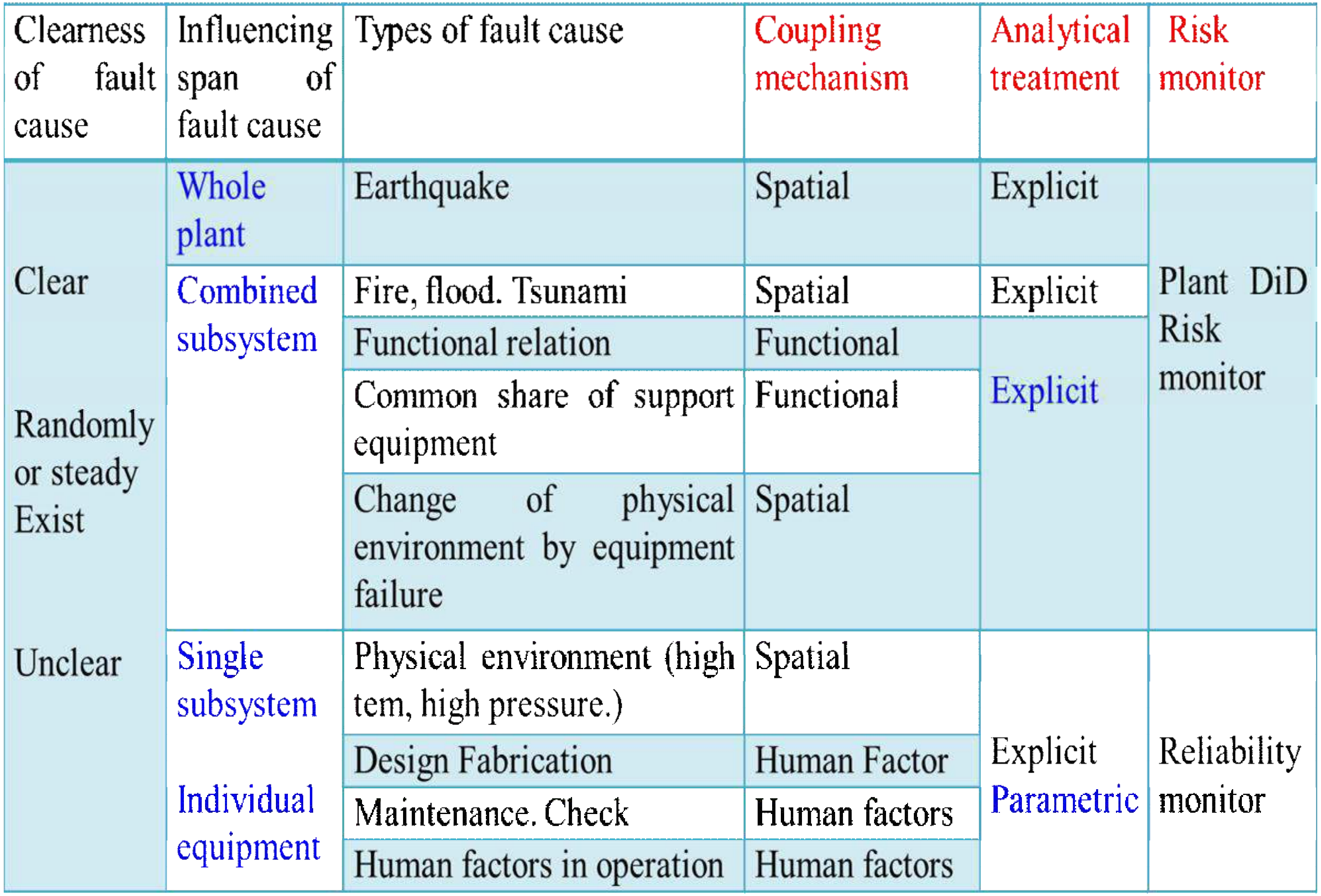
List of contents

- Introduction
- Authors' risk monitor system
- Reliability comparison by GO FLOW :Two types of safety systems of PWRs
- Configuration of I&C system of AP1000
- Authors' preliminary idea for designing digital I&C +HMIT for AP1000
- Conclusion

Defense in depth concept by IAEA

Level	Remarks
Layer1	Initial base for protection against not only internal but also external hazards such as earthquakes, aircraft crashes, blast waves, fire, flooding.
Layer 2	Incorporation of inherent plant features and systems for safety (ex. passive mechanism, automatic control)
Layer 3	Employ design principles to ensure high reliability such as redundancy, avoidance of common mode failure by separation, diversity, Employ automation to reduce human error.

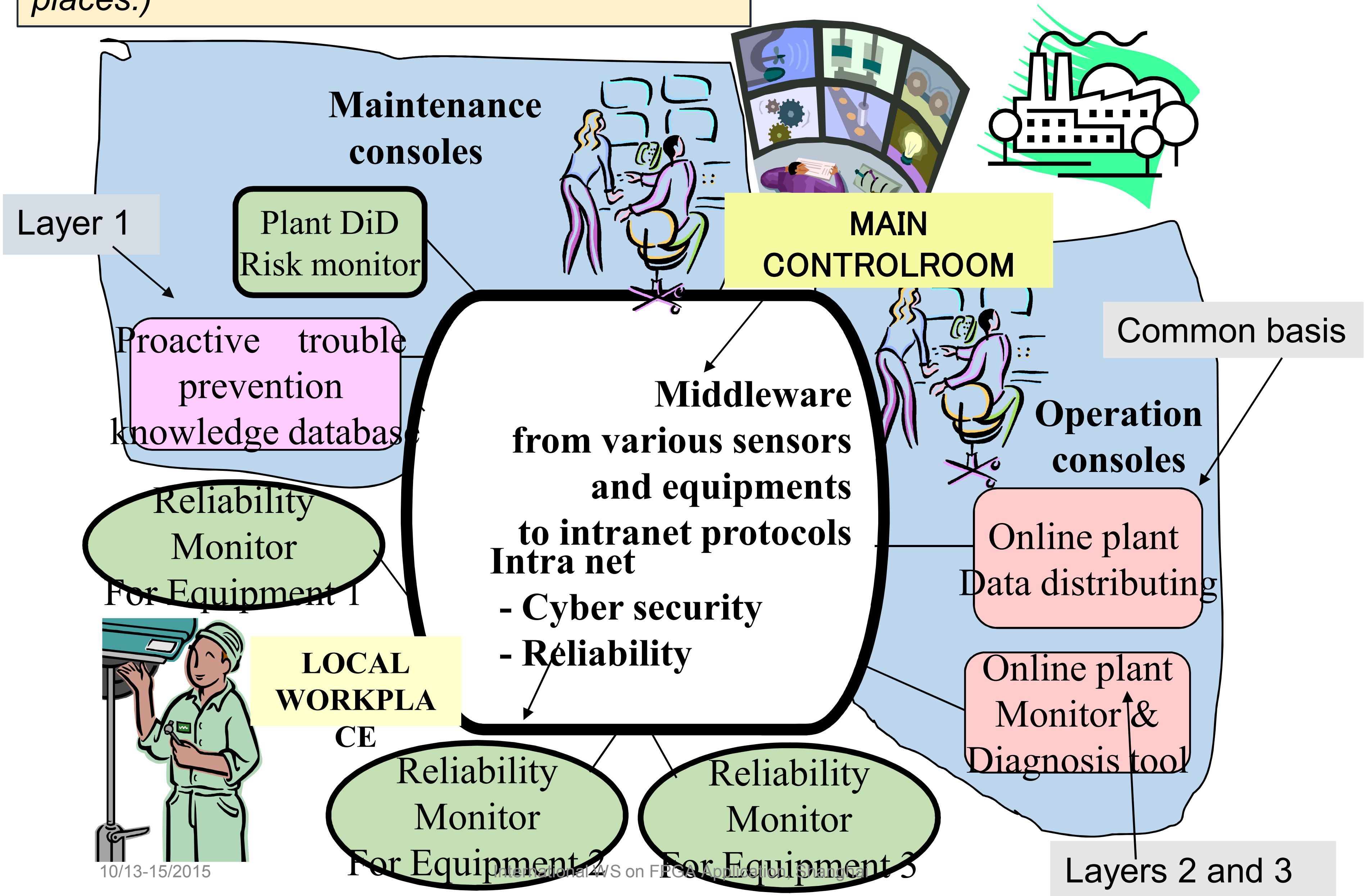
Classification of common cause failure



Clearness of fault cause	Influencing span of fault cause	Types of fault cause	Coupling mechanism	Analytical treatment	Risk monitor
Clear	Whole plant	Earthquake	Spatial	Explicit	Plant DiD Risk monitor
	Combined subsystem	Fire, flood. Tsunami	Spatial	Explicit	
		Functional relation	Functional	Explicit	
Randomly or steady Exist		Common share of support equipment	Functional		
		Change of physical environment by equipment failure	Spatial		
Unclear	Single subsystem	Physical environment (high tem, high pressure.)	Spatial	Explicit Parametric	Reliability monitor
	Individual equipment	Design Fabrication	Human Factor		
		Maintenance. Check	Human factors		
		Human factors in operation	Human factors		

Risk monitor system for layers 1 to 3（Users are plant operators in MCR and local work places.)

Large screen display



Maintenance consoles

Layer 1

Plant DiD Risk monitor

Proactive trouble prevention knowledge database

MAIN CONTROLROOM

Middleware from various sensors and equipments to intranet protocols

Intra net

- Cyber security
- Reliability

Common basis

Operation consoles

Online plant Data distributing

Online plant Monitor & Diagnosis tool

Reliability Monitor For Equipment 1

LOCAL WORKPLACE

Reliability Monitor For Equipment 2

Reliability Monitor For Equipment 3

Layers 2 and 3

Plant DiD risk monitor and reliability monitor

- Reliability is successful rate of a system’s performance that will fulfill its expected function when it is requested.
- Reliability evaluation for a sub-system is made by Reliability monitor using a combination of FMEA and GO FLOW model.
- Application studies have been conducted for safety systems of conventional PWR and AP1000

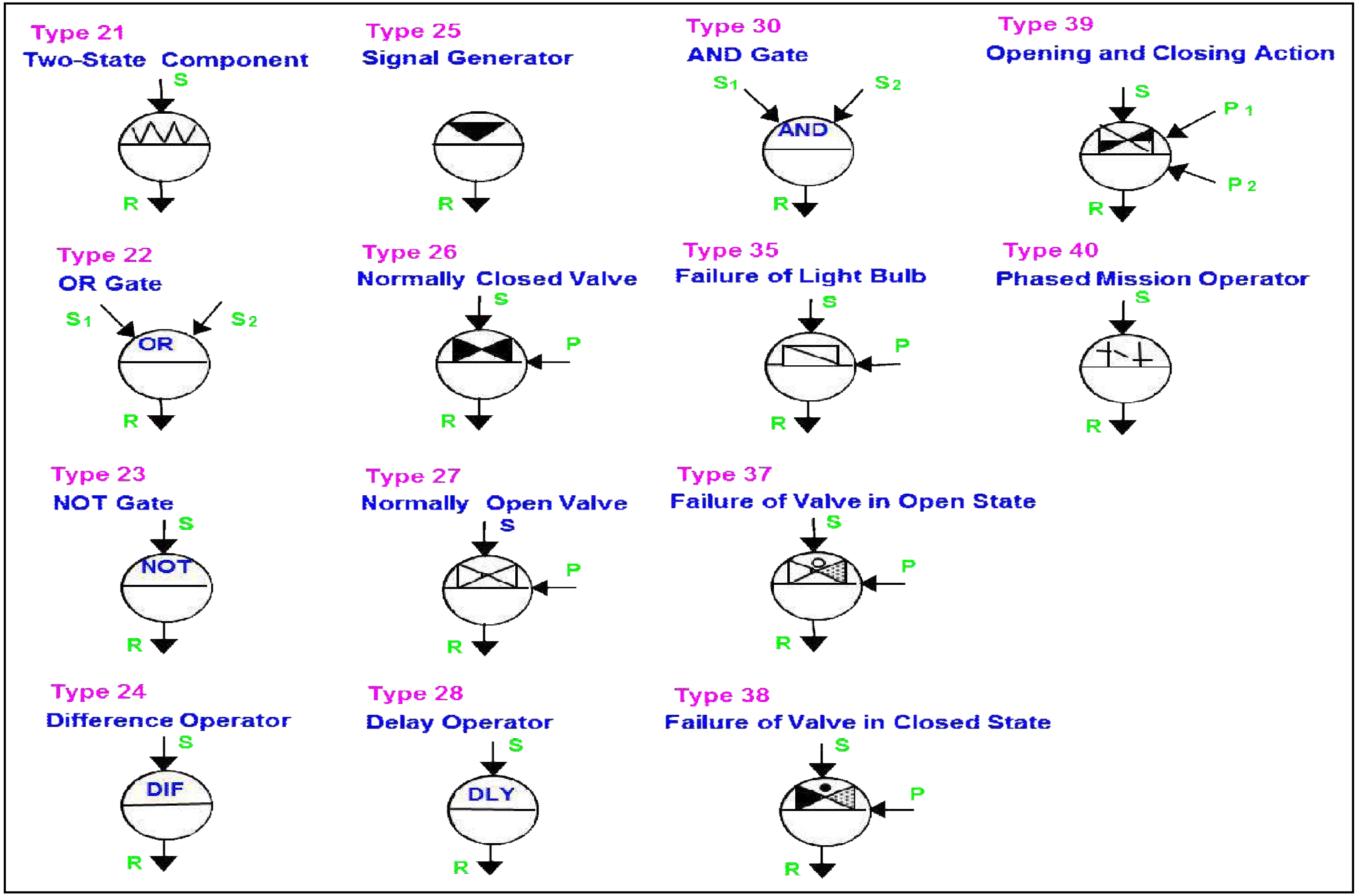
- The plant DiD risk monitor will identify every potential risk state caused by any conceivable event in the plant system as a whole where not only internal events but also external events arising from common cause factors and human factors should be taken into account.
- Software system has been under development to analyze complex human-machine interaction

Methods of Reliability Monitor: GO-FLOW

- GO-FLOW is success–oriented system analysis technique to evaluate system reliability/availability
- GO-FLOW method describes the dynamic behavior of target system by using 14 standardized operators to represent various logics used in control system.
- The graphic representation by those operators is called GO-FLOW chart
- GO FLOW program by T. Matsuoka can deal with systems analysis by easier way than by FT/ET used in conventional PSA

  - Can treat Phased mission （Operation mode of the plant will change with time)
  - Uncertainty analysis
  - Common cause failure (by parametric model)

14 operators used in GO-FLOW



Type 21
Two-State Component

Type 22
OR Gate

Type 23
NOT Gate

Type 24
Difference Operator

Type 25
Signal Generator

Type 26
Normally Closed Valve

Type 27
Normally Open Valve

Type 28
Delay Operator

Type 30
AND Gate

Type 35
Failure of Light Bulb

Type 37
Failure of Valve in Open State

Type 38
Failure of Valve in Closed State

Type 39
Opening and Closing Action

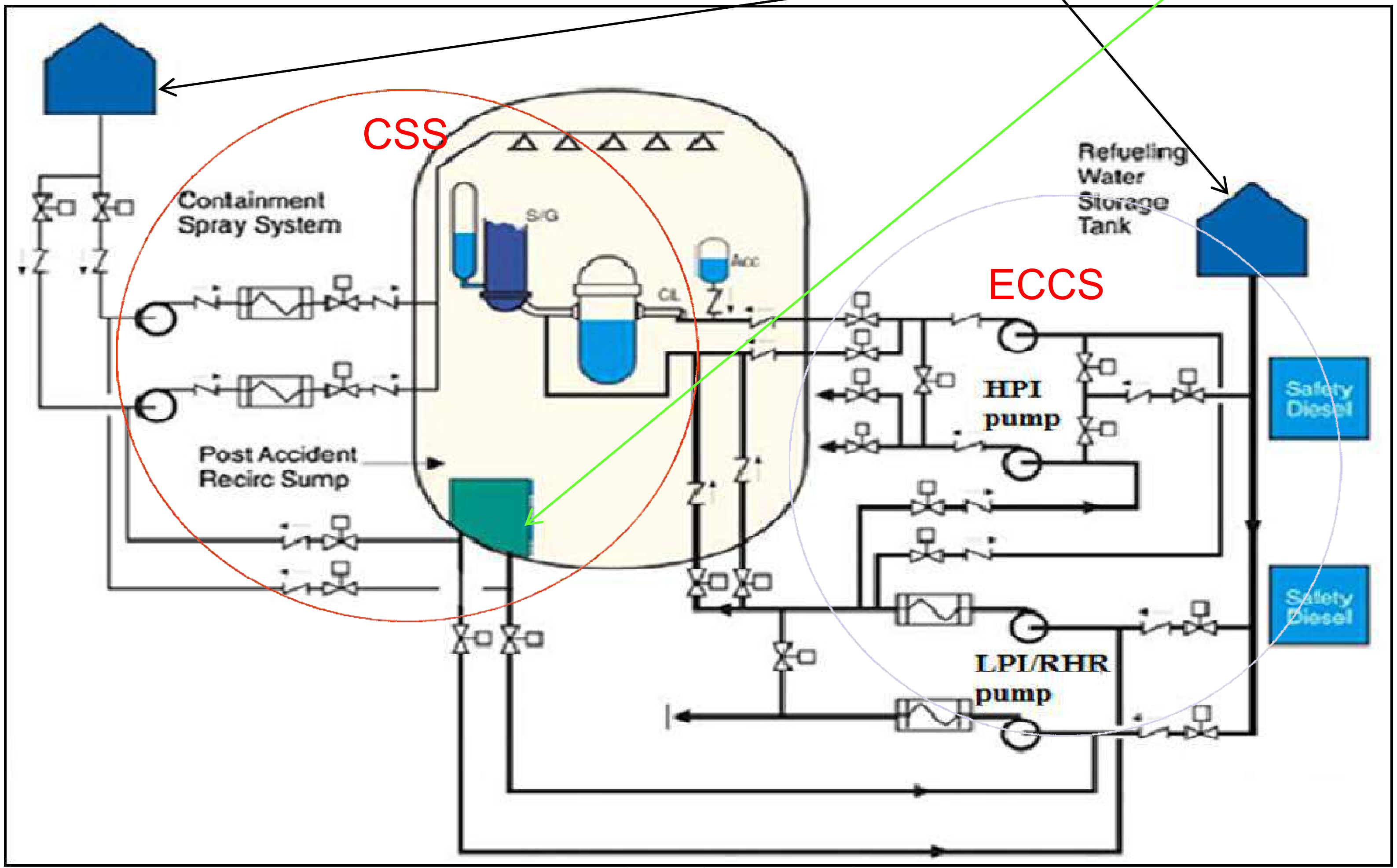
Type 40
Phased Mission Operator

Reliability comparison by GO FLOW
-Two types of safety systems of PWRs-

Active safety (Conventional PWR)	Passive safety (AP1000)
Active safety system actuated by external power source such as: Electric power, Human operator or even mechanically.	Passive safety system does not need electric power source to actuate by natural physical laws such as: Gravity, natural circulation, etc..
i. Containment spray system (CSS)	iii. Passive containment cooling system (PCCS)
ii. Emergency core cooling system (ECCS)	iv. Passive core cooling system (PXS)
	Automatic depressurization system (ADS)

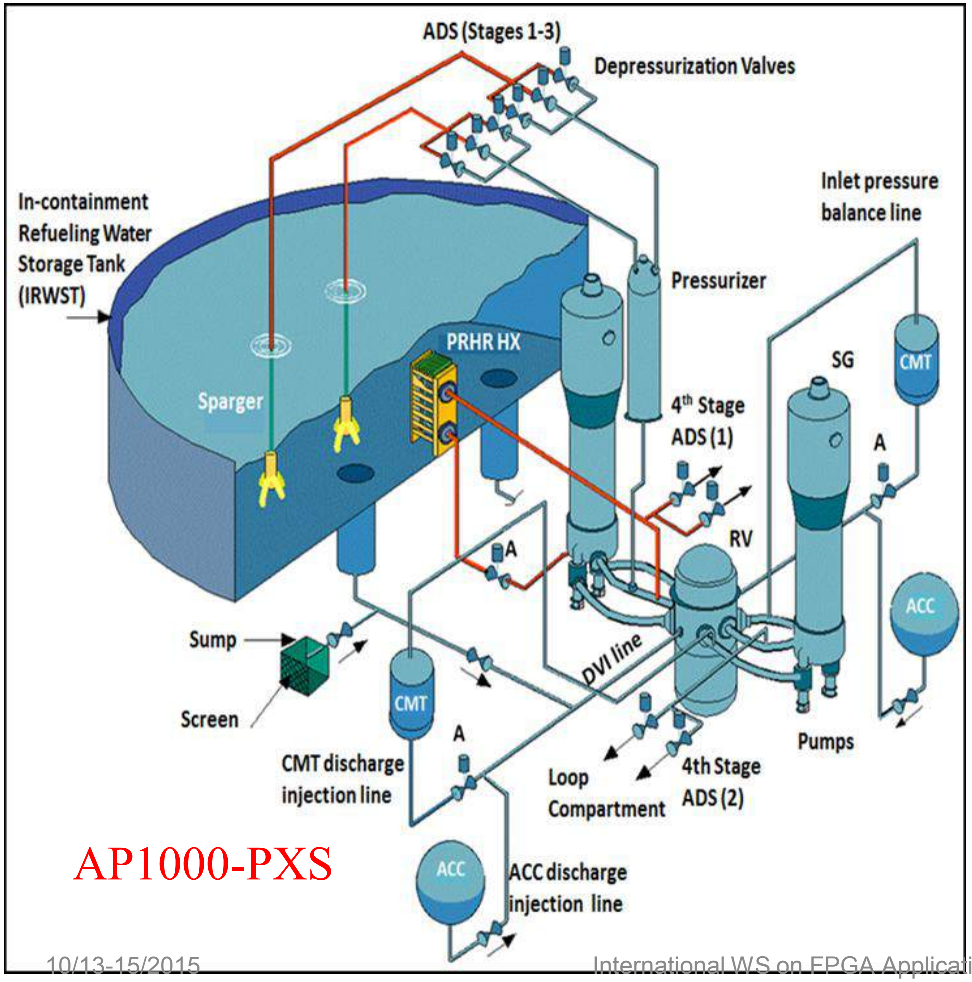
ECCS and CSS safety systems of conventional PWR

Common water sources for ECCS & CSS [RWST &SUMP]

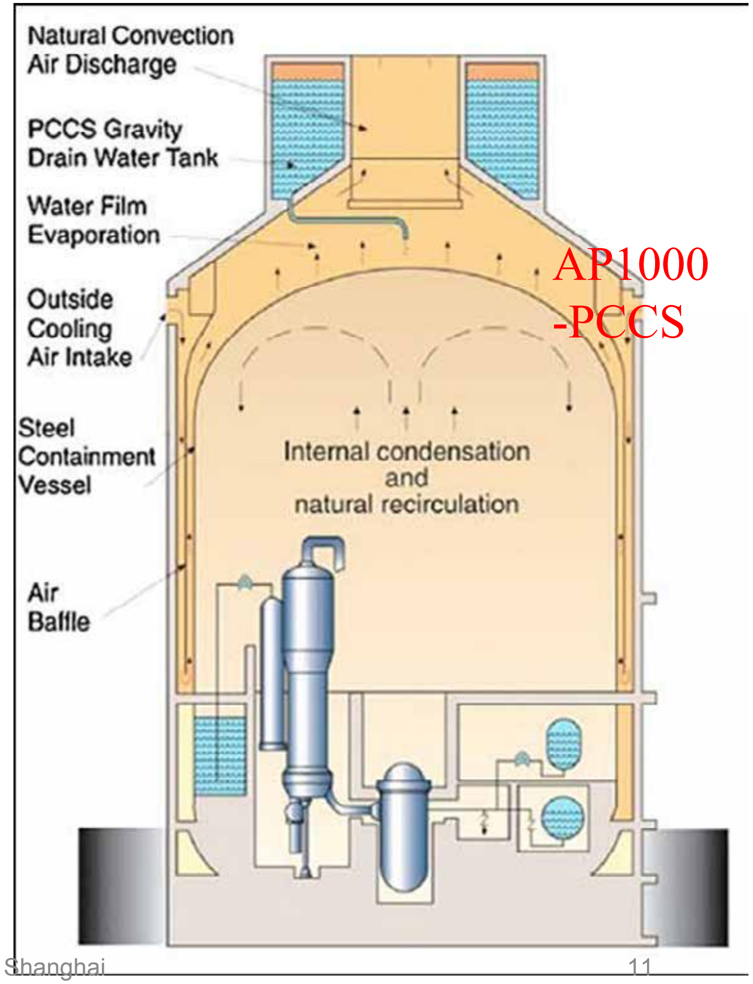


AP1000 Passive safety systems

- Passive core cooling system (PXS),
- Passive containment cooling system (PCCS),



AP1000-PXS


Natural Convection Air Discharge
PCCS Gravity Drain Water Tank
Water Film Evaporation
Outside Cooling Air Intake
Steel Containment Vessel
Internal condensation and natural recirculation
Air Baffle

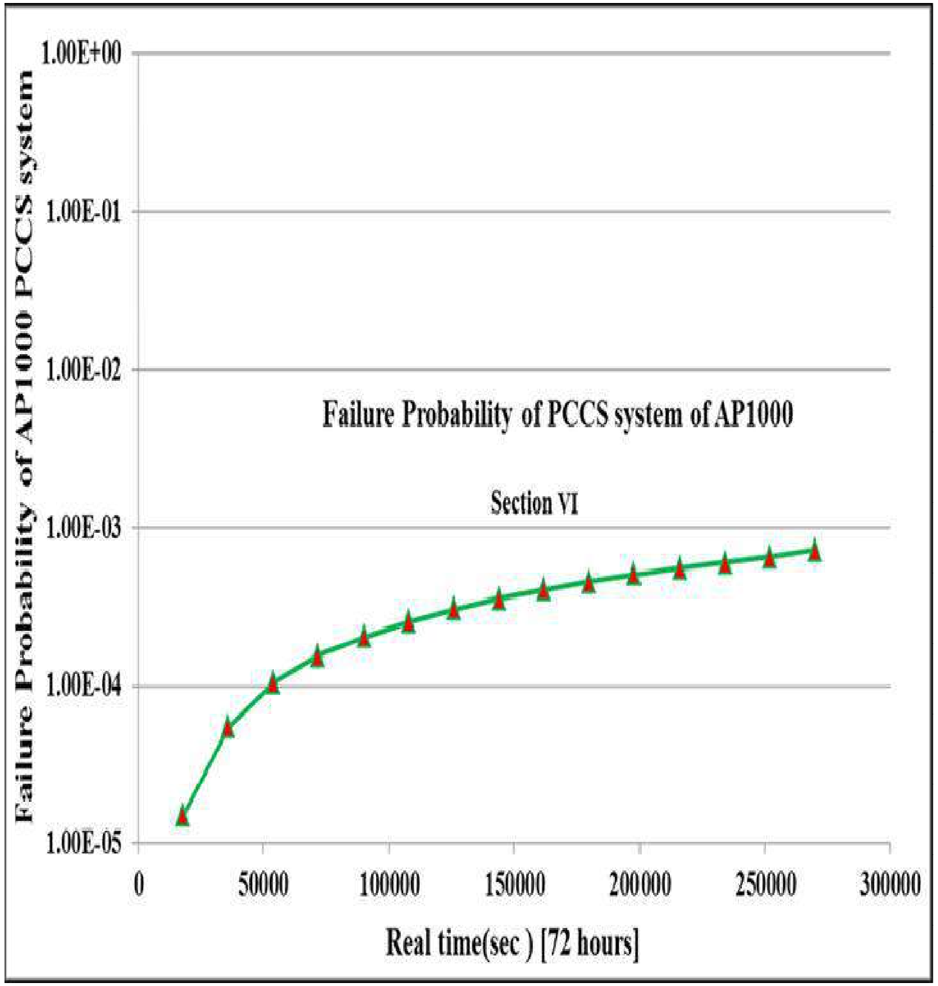
AP1000 -PCCS

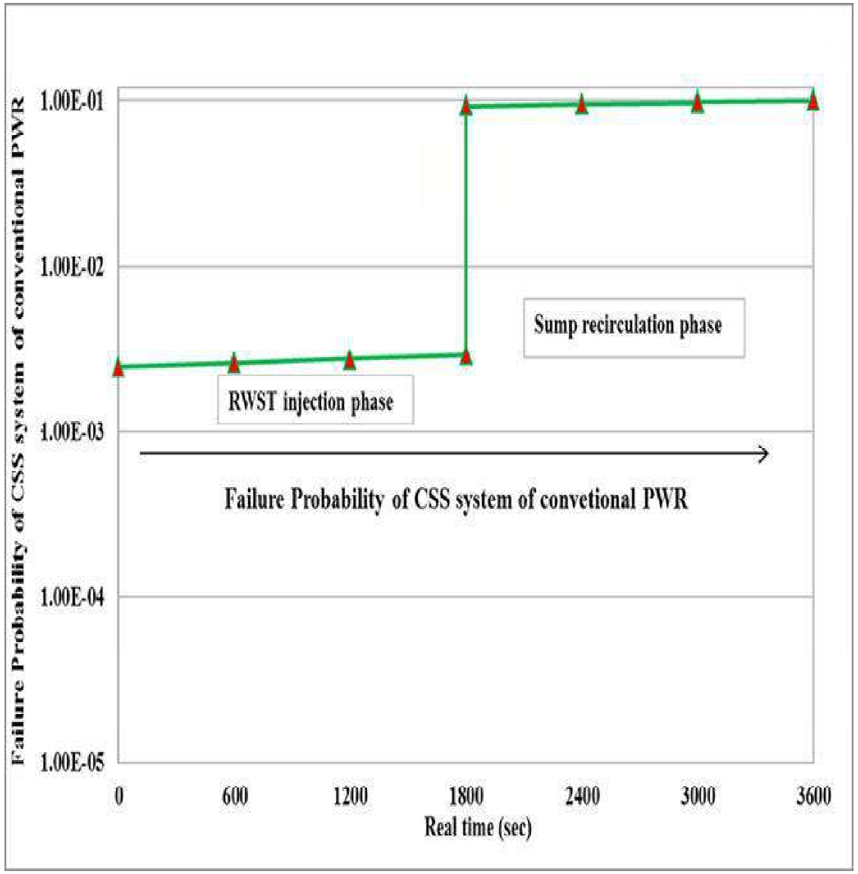
Difference between AP1000 passive and PWR active system

Conventional PWR		AP1000	
Safety systems	Subsystems and components	Safety systems	Subsystems
Emergency core cooling system (ECCS)	(i) Accumulator injection system (AIS) (ii) High Pressure Injection System (HPIS) (iii) Low pressure injection system (LPIS) ECCS composed of uses (i) Check valves, (ii) MOVs, (iii) HPIP (iv) RHRPs, (v) RHR-HX (vi) Need power source	Passive core cooling system (PXS)	a) Passive safety injection system (PSIS) (i) Accumulators injection (ii) Core Makeup Tanks (iii) In-containment refueling water storage tank (IRWST) (iv) Recirculation sump injection system (v) No power source (vi) PXS composed of all passive components, AOVs ,Squib valves, check valves b) Four stages automatic depressurization system (ADS) c) Passive residual heat removal system (PRHRS) d) All passive components
Containment spray System (CSS)	(i)Two parallel lines redundancy (i)CSP, (ii)CSHEX) and (iii)MOVs (iv)Need power source	Passive containment cooling system (PCCS)	PCCS composed of (i)Three parallel lines redundancy (i)PCCWS (ii)AOVs (iii)Normally open MOVs (iv)Function due to natural circulation of air and internal condensation (v) No power source
Water sources for ECCS and CSS are shared in common Accumulator Tanks, RWST, and Containment recirculation sump (CRS)		Water sources for PXS and PCCS are independent: Accumulator Tanks, Core Makeup Tanks, IRWST, Recirculation sump and PCCWST	

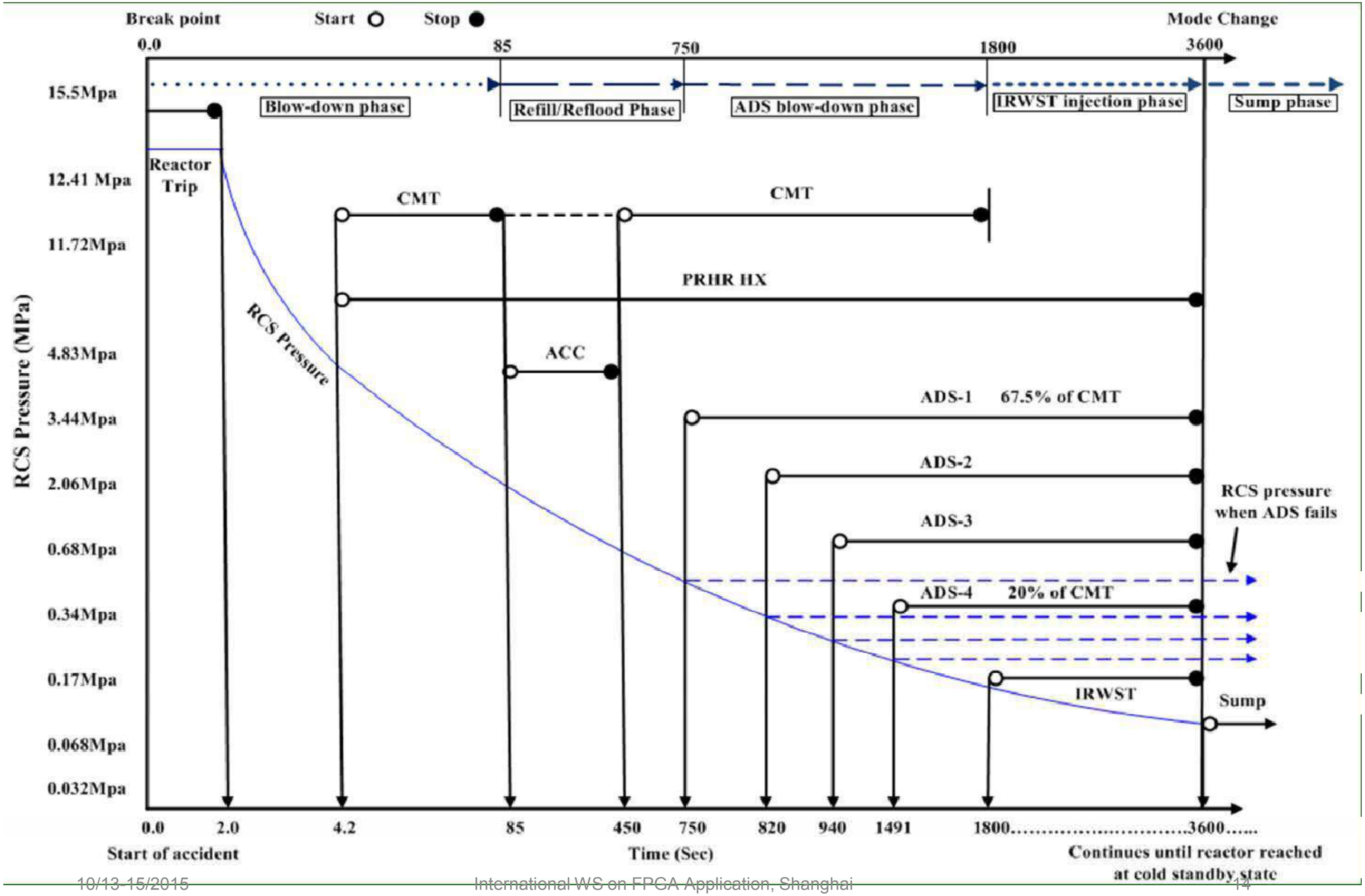
Inter-comparison of reliability between AP1000 and conventional PWR

(1) AP1000 passive containment cooling system vs. PWR containment spray system

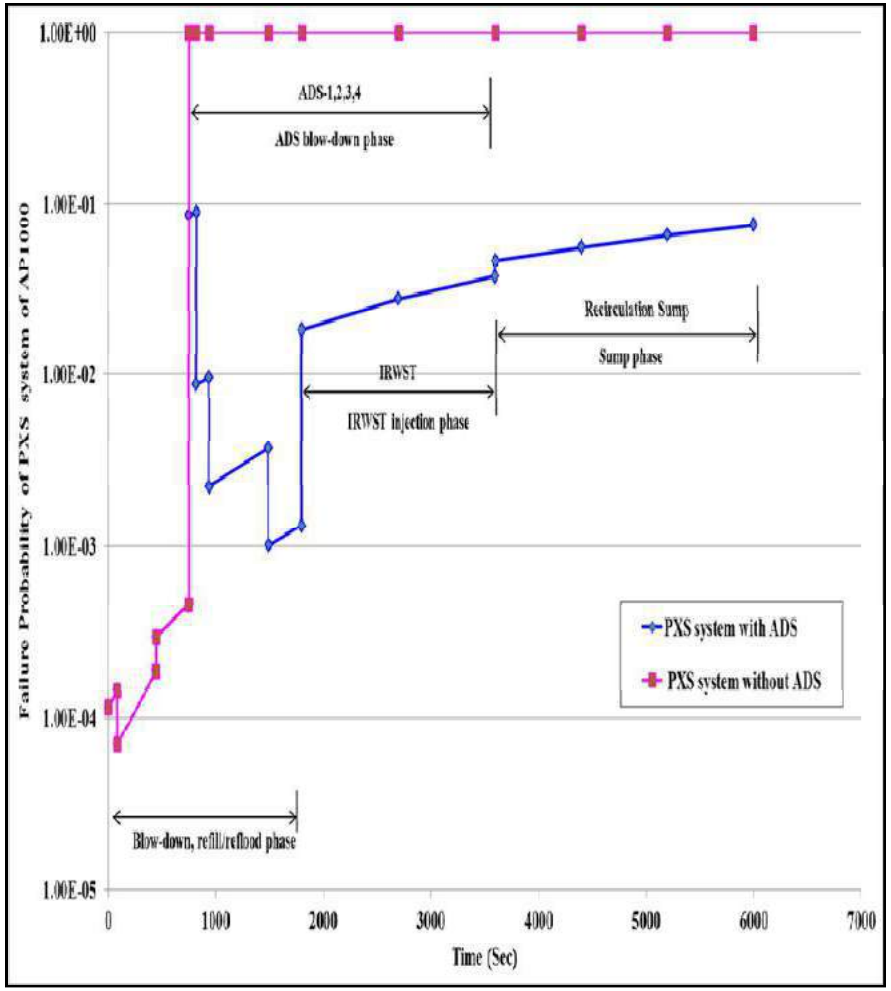


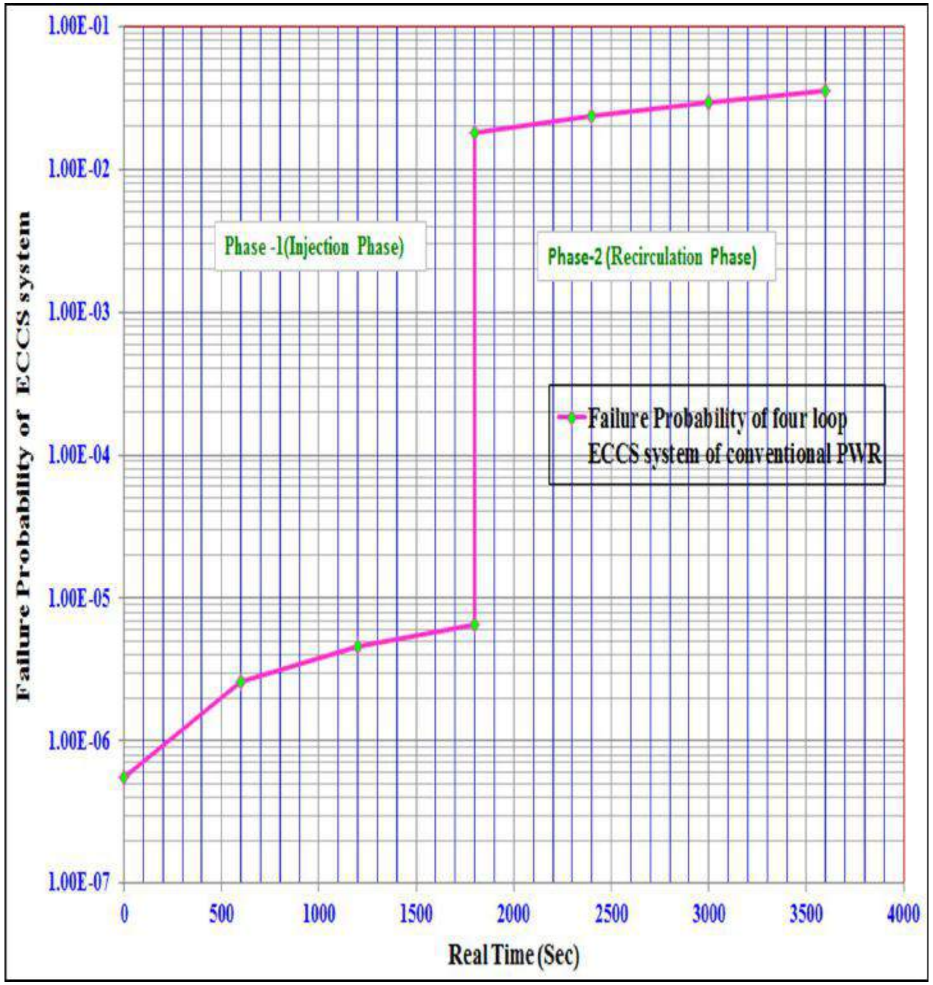


Timeline of AP1000-PXS with pressure drop curve



(2) Comparison between AP1000-PXS and PWR- ECCS





ADS system is a key system of AP1000 for the successful actuation of PXS and PCCS

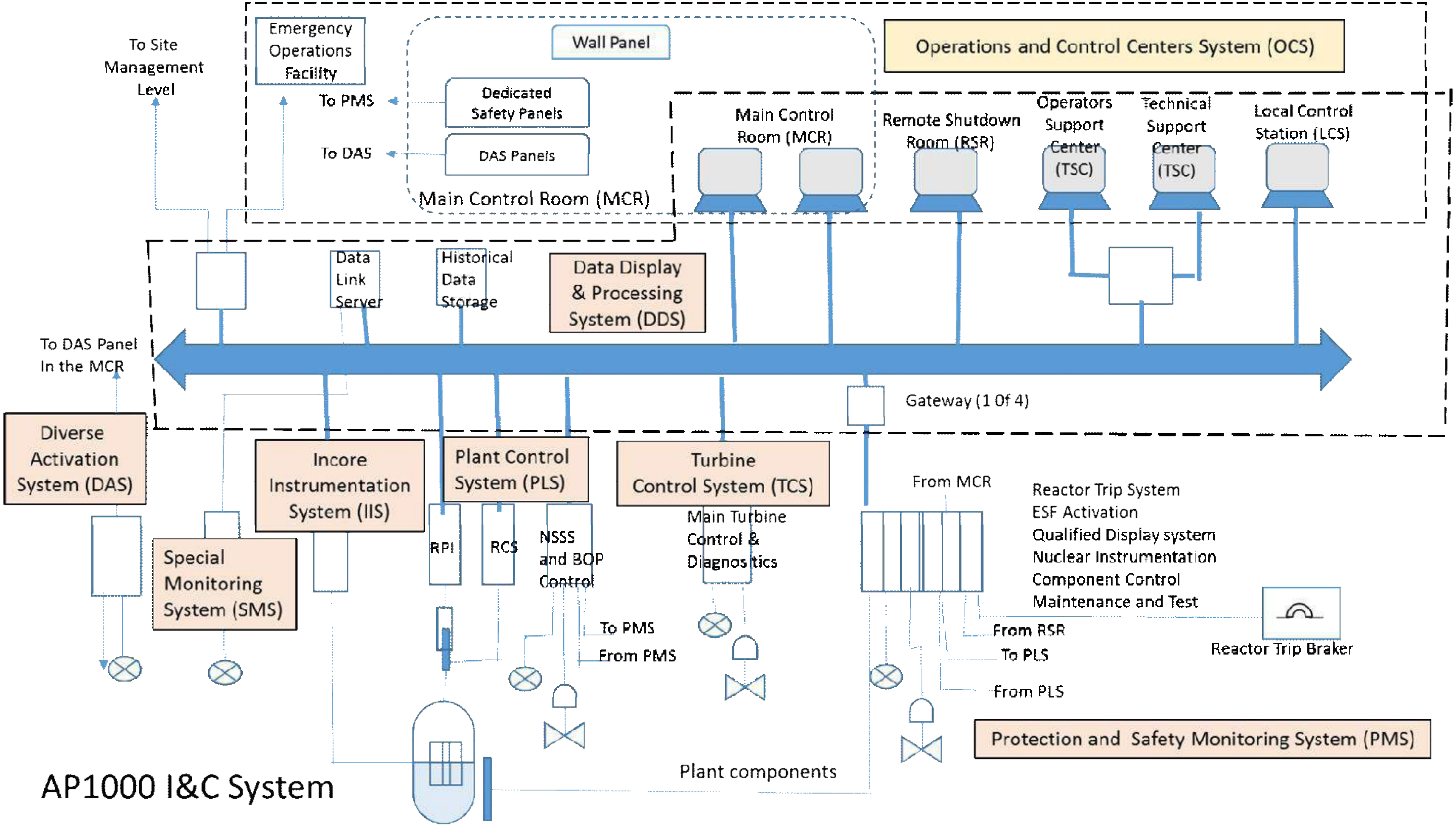
Two types of failure modes were basically considered for passive safety systems

a. Type A failure caused by structural failure (hardware failure, physical degradation), and
b. Type B failure caused by functional failure due to blocking of intended natural phenomena that can challenge and impair the passive safety by either natural laws or inherent characteristics.

Here no consideration was made on the reliability of I&C + HMIT system.

So the authors made a literature survey about I&C system design for AP1000.

A digital I&C system design for European AP1000


To Site Management Level
Emergency Operations Facility
To PMS
To DAS
Wall Panel
Dedicated Safety Panels
DAS Panels
Main Control Room (MCR)
Operations and Control Centers System (OCS)
Main Control Room (MCR)
Remote Shutdown Room (RSR)
Operators Support Center (TSC)
Technical Support Center (TSC)
Local Control Station (LCS)
Data Link Server
Historical Data Storage
Data Display & Processing System (DDS)
To DAS Panel In the MCR
Gateway (1 0f 4)
Diverse Activation System (DAS)
Special Monitoring System (SMS)
Incore Instrumentation System (IIS)
Plant Control System (PLS)
Turbine Control System (TCS)
RPI
RCS
NSSS and BOP Control
Main Turbine Control & Diagnostics
To PMS
From PMS
From MCR
Reactor Trip System
ESF Activation
Qualified Display system
Nuclear Instrumentation
Component Control
Maintenance and Test
From RSR
To PLS
From PLS
Reactor Trip Braker
Protection and Safety Monitoring System (PMS)
Plant components

AP1000 I&C System

AP1000 C & I System Design

**Two system classification (safety-related, non-safety related)*

**Based on US C&I standards, i.e., IEEE standards + USNRAC requirements*

Abb.	Full name	Notes
PMS	Protection and Monitor System	Digital platform (ABB-AC160) Common Interface Module (CIM) :Use FPGA
DAS	Diverse Actuation System	Originally designed by FPGA But by British Regulatory Review recommended WEC analogue 7340 series equipment
PLS	PLant control System	Digital platform (Ovation platform)
DDS	Data Display and Processing System	Digital platform (Ovation platform)
OCS	Operation and Control center System	
RMS	Radiation Monitoring System	
IIS	In-core Instrumentation System	
SMS	Special Monitoring System	
TOS	Turbine Operation System	

ONR-GDA-AR-11-006 Rev.8, 11 November 2011

Generic Design Assessment- New Civil Reactor Build Step 4 Control and Instrumentation Assessment of the Westinghouse AP1000 Reactor

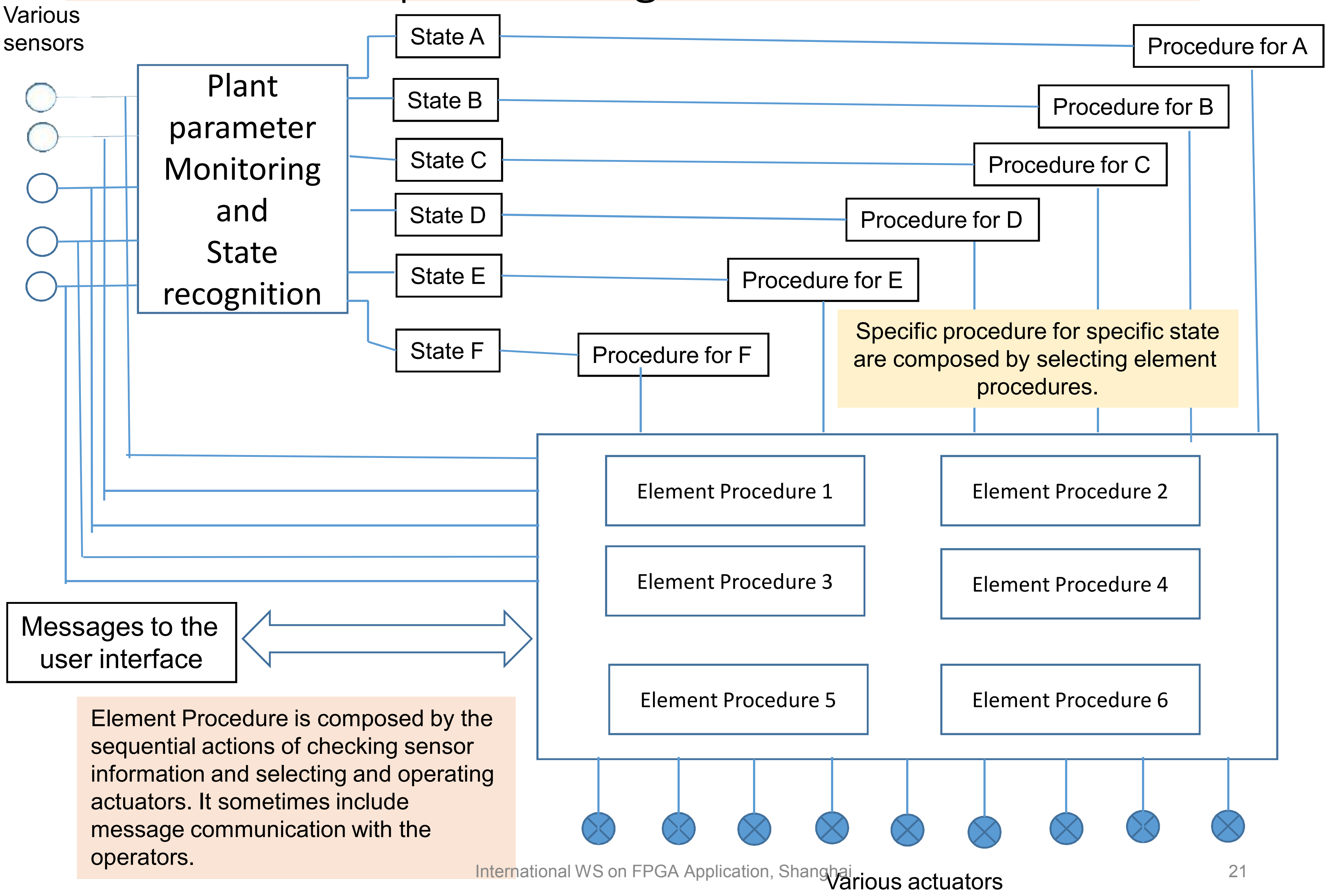
Trend of digital I&C in AP1000

- Basically similar configuration of digital I&C+HMIT employed in the current full digital Gen.III LWR.
- FPGA is going to be partly used in the whole digital I&C system, probably as the countermeasures to common cause failure or software reliability (because of easiness of regulatory approval?).
- One question is what should be HMIT system design for AP1000 of which conspicuous character is the adoption of passive safety & less human intervention by introduction of more automation?

Authors' preliminary works on digital I&C in AP1000

- At this point, by considering the advanced capabilities and functions of FPGA, more positive application of FPGA are expected for AP1000, to realize automatic human interface functions for plant management :
- (a) to monitor plant parameters to tell the plant situation by automatic diagnosis, and then automatic execution of procedures, or
- (b) to present diagnostic result and/or procedures to help operators to do by themselves.

General framework of automatic monitoring and procedure generation



Specific procedure for specific state are composed by selecting element procedures.

Element Procedure is composed by the sequential actions of checking sensor information and selecting and operating actuators. It sometimes include message communication with the operators.

Research subjects to realize automatic monitoring and procedure by FPGA

A. Preparation of simulation method of any plant operation mode for whole plant life

B. Create effective method of plant anomaly detection

C. Description of operation procedure to cope with operational transient and accident

D. V&V of the above methods by coupling with plant simulation practice

E. How to implement it as digital I&C and how FPGA will be utilized

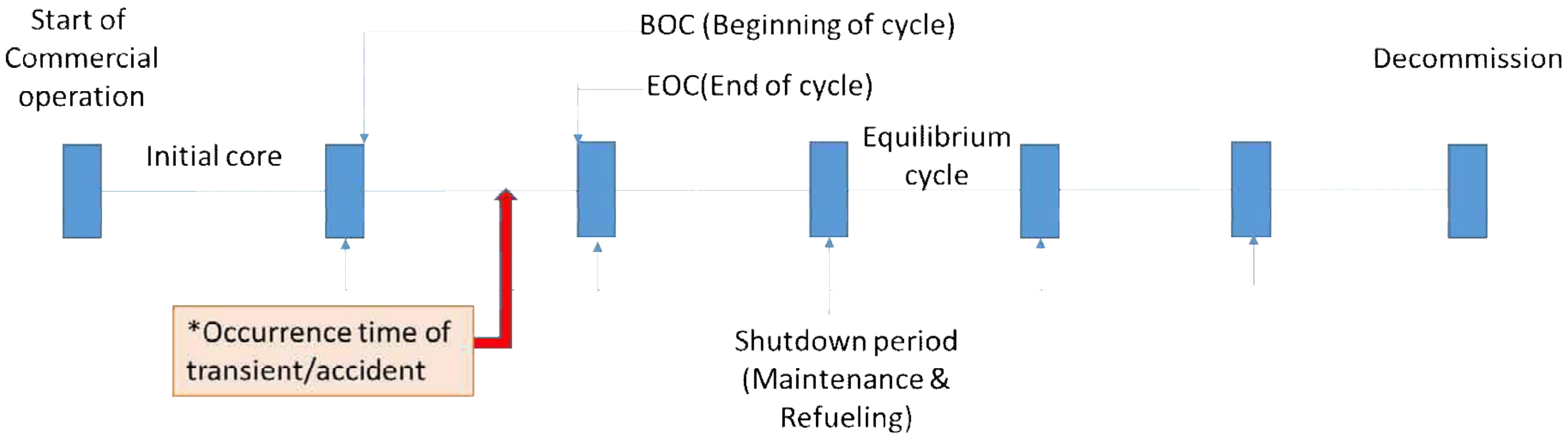
F. How to evaluate the proposed system (reliability, safety, etc.)

For the moment, just step A has been in progress for our AP1000 simulation.

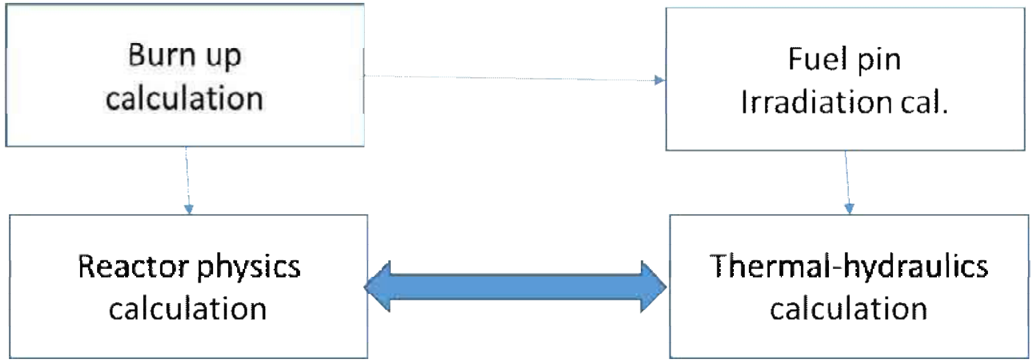
Simulation method for studying appropriate automatic algorithms for various stage of plant operation

- General method of steady state and transient/accident calculation in any operation mode
- Steady state reactor physics analysis for whole life of the plant with fuel irradiation effects
- Transient/accident analysis by considering specific character of AP1000 reactor design to be compared with conventional PWR (other than passive safety)

General method of steady state and transient/accident calculation in any operation mode


Start of Commercial operation
BOC (Beginning of cycle)
Decommission
EOC(End of cycle)
Initial core
Equilibrium cycle
*Occurrence time of transient/accident
Shutdown period (Maintenance & Refueling)

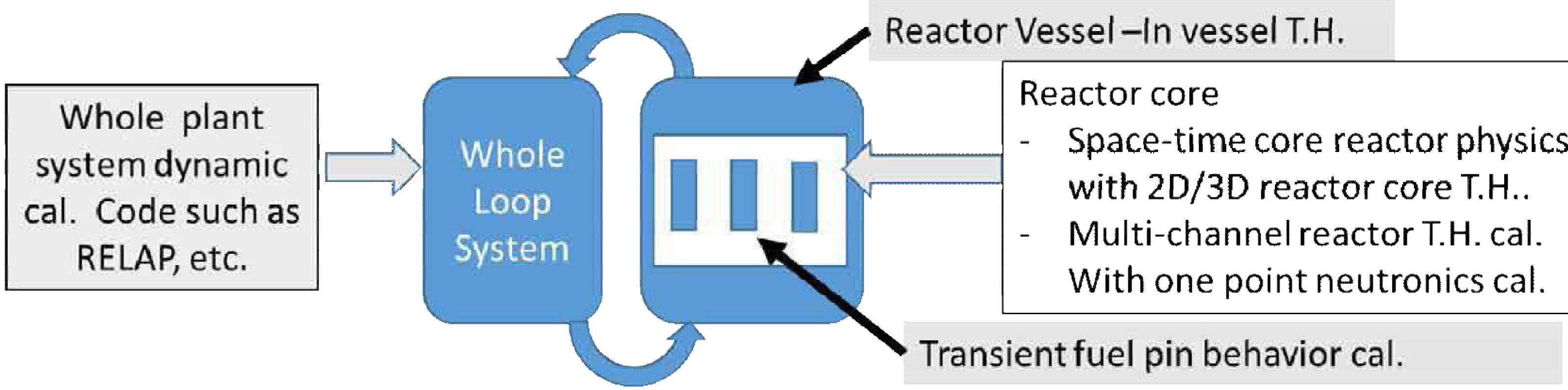
Steady state calculation of reactor core until occurrence time of transient/accident


Burn up calculation
Fuel pin Irradiation cal.
Reactor physics calculation
Thermal-hydraulics calculation

Assumed Conditions of Transient/Accident Calculation

Assumed conditions	Selection of occurrence time for transient/accident	Remark
Initial condition	Initial plant condition	Plant configuration based on state of plant configuration
	Initial core condition such as fuel rod, reactor power shape, coolant condition, reactivity feedback condition, etc.	Result of SS irradiation calculation
Disturbance condition	Types of transient/ accident scenario	LOF, TOP, LOCA, ATWS, etc.
	Influential factors to be assumed	External factors, human factors, common cause factors, etc.

Framework of Transient/Accident Calculation



Whole plant system dynamic cal. Code such as RELAP, etc.

Reactor Vessel –In vessel T.H.

Reactor core
- Space-time core reactor physics cal with 2D/3D reactor core T.H..
- Multi-channel reactor T.H. cal. With one point neutronics cal.

Transient fuel pin behavior cal.

Conclusion

- In this presentation, the authors’ study towards developing a new digital I&C+HMIT design method for AP1000 were presented.
- As far as the application of FPGA is concerned, the authors are expecting its positive use for “automatic human support” by noticing its advancing functions such as SoC FPGA.

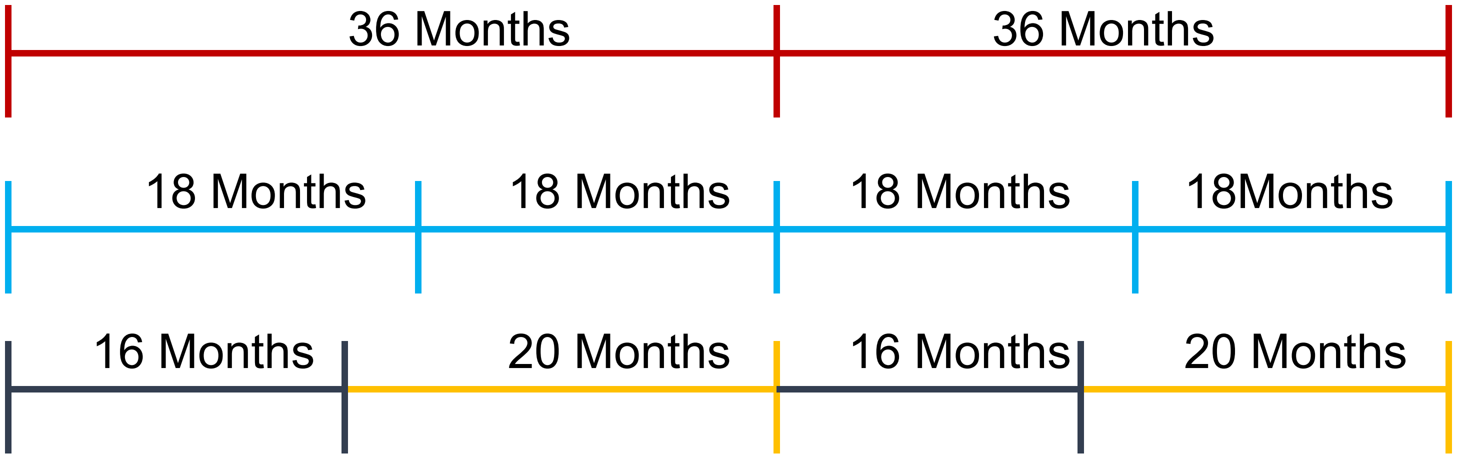
Thank you very much for your kind attention.

Any question and Comments?

Additional materials

Specific character of AP1000 reactor design

- AP1000 is designed for 18 month cycle but can also be used for 16/20 month cycle to meet high demand periods
- After every 36 month 129 fuel assemblies are required for 16/20 month cycle scheme as compare to 128 in case of 18 month cycle scheme

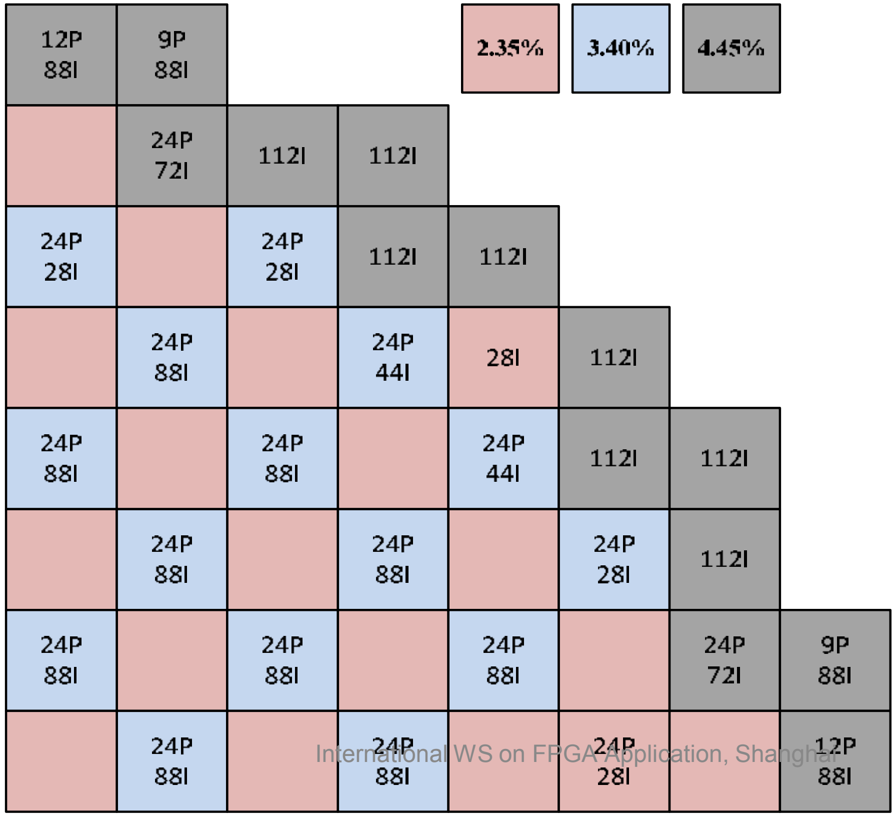


18 Month vs 16/20 Month Cycle

Fuel Loading Scheme

- The initial core has different loading pattern than the reload and equilibrium cores. Three batch loading scheme is used in AP1000 core.
- 64 fresh fuel assemblies are required to be loaded for 18 month cycle refueling. The core employs low leakage model to reduces radial core leakage and improves fuel utilization at central part of the core

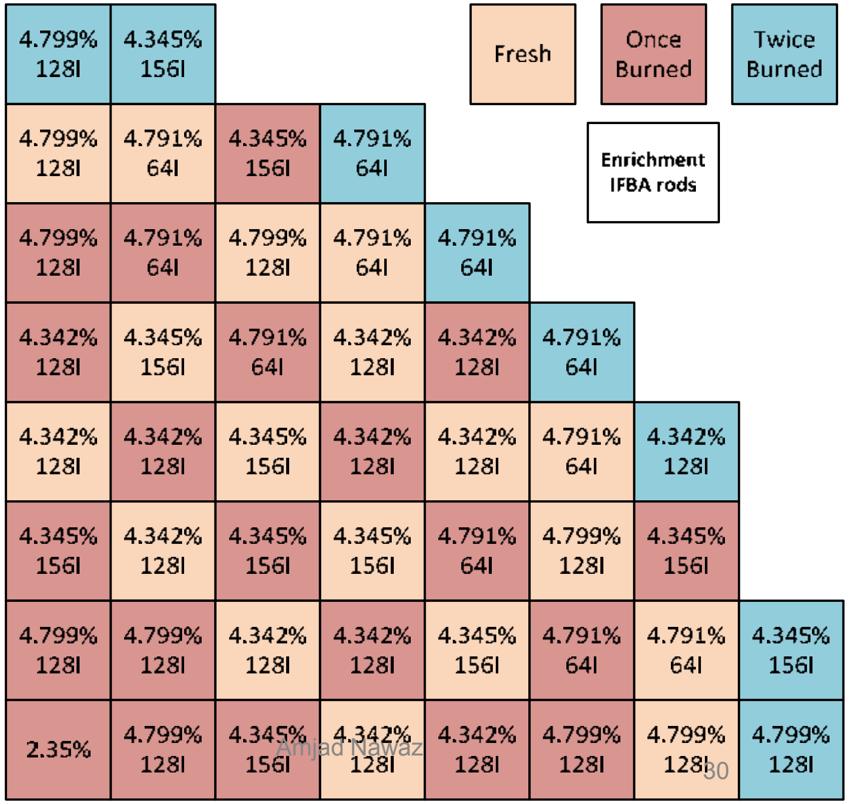
Initial Core



2.35% | 3.40% | 4.45%

12P 88I	9P 88I						
	24P 72I	112I	112I				
24P 28I		24P 28I	112I	112I			
	24P 88I		24P 44I	28I	112I		
24P 88I		24P 88I		24P 44I	112I	112I	
	24P 88I		24P 88I		24P 28I	112I	
24P 88I		24P 88I		24P 88I		24P 72I	9P 88I
	24P 88I		24P 88I		24P 28I		12P 88I

18 month Equilibrium core



Fresh | Once Burned | Twice Burned

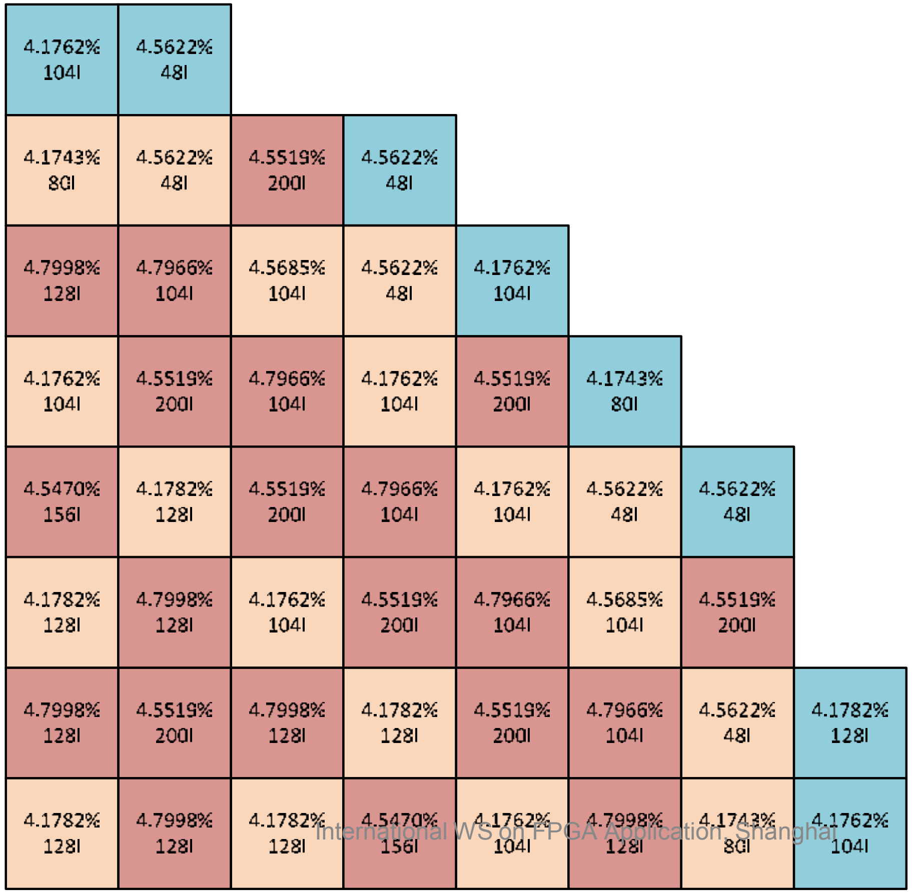
Enrichment
IFBA rods

4.799% 128I	4.345% 156I						
4.799% 128I	4.791% 64I	4.345% 156I	4.791% 64I				
4.799% 128I	4.791% 64I	4.799% 128I	4.791% 64I	4.791% 64I			
4.342% 128I	4.345% 156I	4.791% 64I	4.342% 128I	4.342% 128I	4.791% 64I		
4.342% 128I	4.342% 128I	4.345% 156I	4.342% 128I	4.342% 128I	4.791% 64I	4.342% 128I	
4.345% 156I	4.342% 128I	4.345% 156I	4.345% 156I	4.791% 64I	4.799% 128I	4.345% 156I	
4.799% 128I	4.799% 128I	4.342% 128I	4.342% 128I	4.345% 156I	4.791% 64I	4.791% 64I	4.345% 156I
2.35%	4.799% 128I	4.345% 156I	4.342% 128I	4.342% 128I	4.799% 128I	4.799% 128I	4.799% 128I

Fuel Loading Scheme

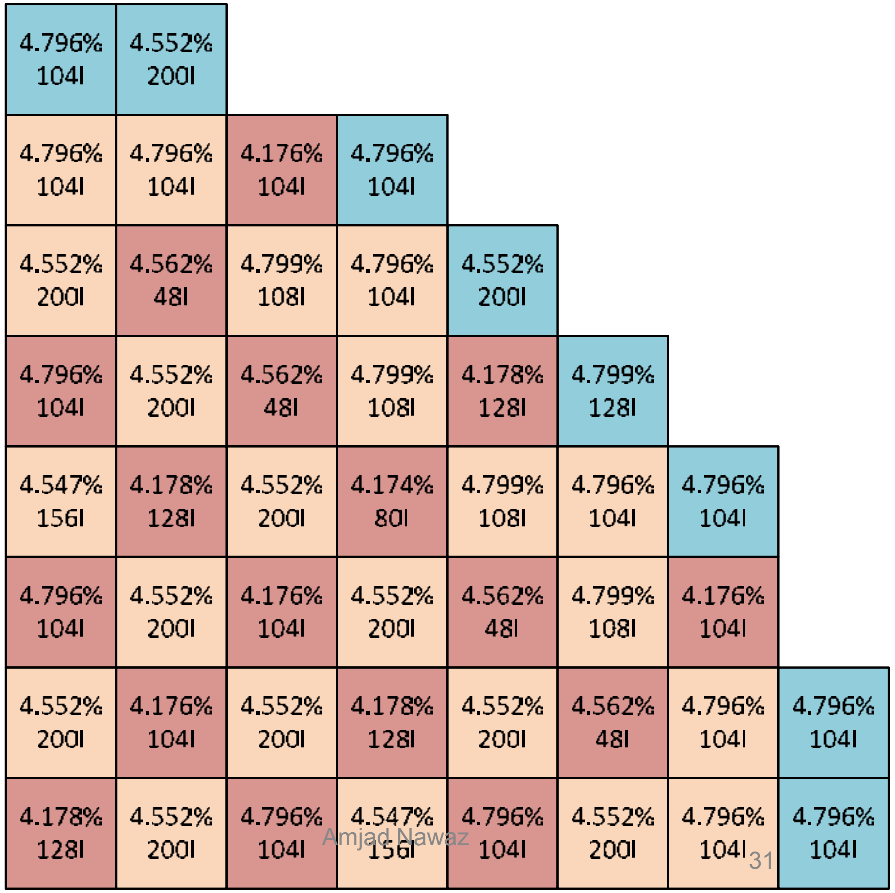
- At each refueling, 57 fresh fuel assemblies are loaded in the 16 month cycle equilibrium core, and 72 fresh fuel assemblies are required for 20 month cycle equilibrium core

16 month Equilibrium core



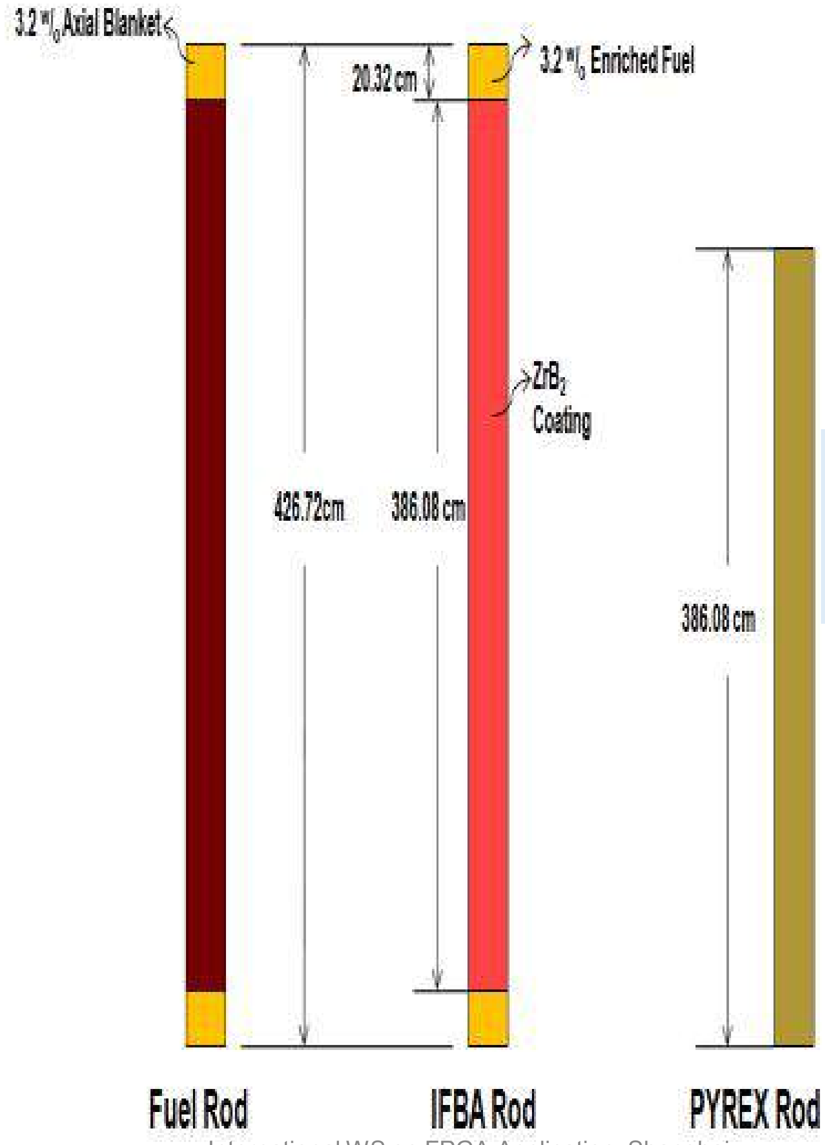
4.1762% 104I	4.5622% 48I						
4.1743% 80I	4.5622% 48I	4.5519% 200I	4.5622% 48I				
4.7998% 128I	4.7966% 104I	4.5685% 104I	4.5622% 48I	4.1762% 104I			
4.1762% 104I	4.5519% 200I	4.7966% 104I	4.1762% 104I	4.5519% 200I	4.1743% 80I		
4.5470% 156I	4.1782% 128I	4.5519% 200I	4.7966% 104I	4.1762% 104I	4.5622% 48I	4.5622% 48I	
4.1782% 128I	4.7998% 128I	4.1762% 104I	4.5519% 200I	4.7966% 104I	4.5685% 104I	4.5519% 200I	
4.7998% 128I	4.5519% 200I	4.7998% 128I	4.1782% 128I	4.5519% 200I	4.7966% 104I	4.5622% 48I	4.1782% 128I
4.1782% 128I	4.7998% 128I	4.1782% 128I	4.5470% 156I	4.1762% 104I	4.7998% 128I	4.1743% 80I	4.1762% 104I

20 month Equilibrium core



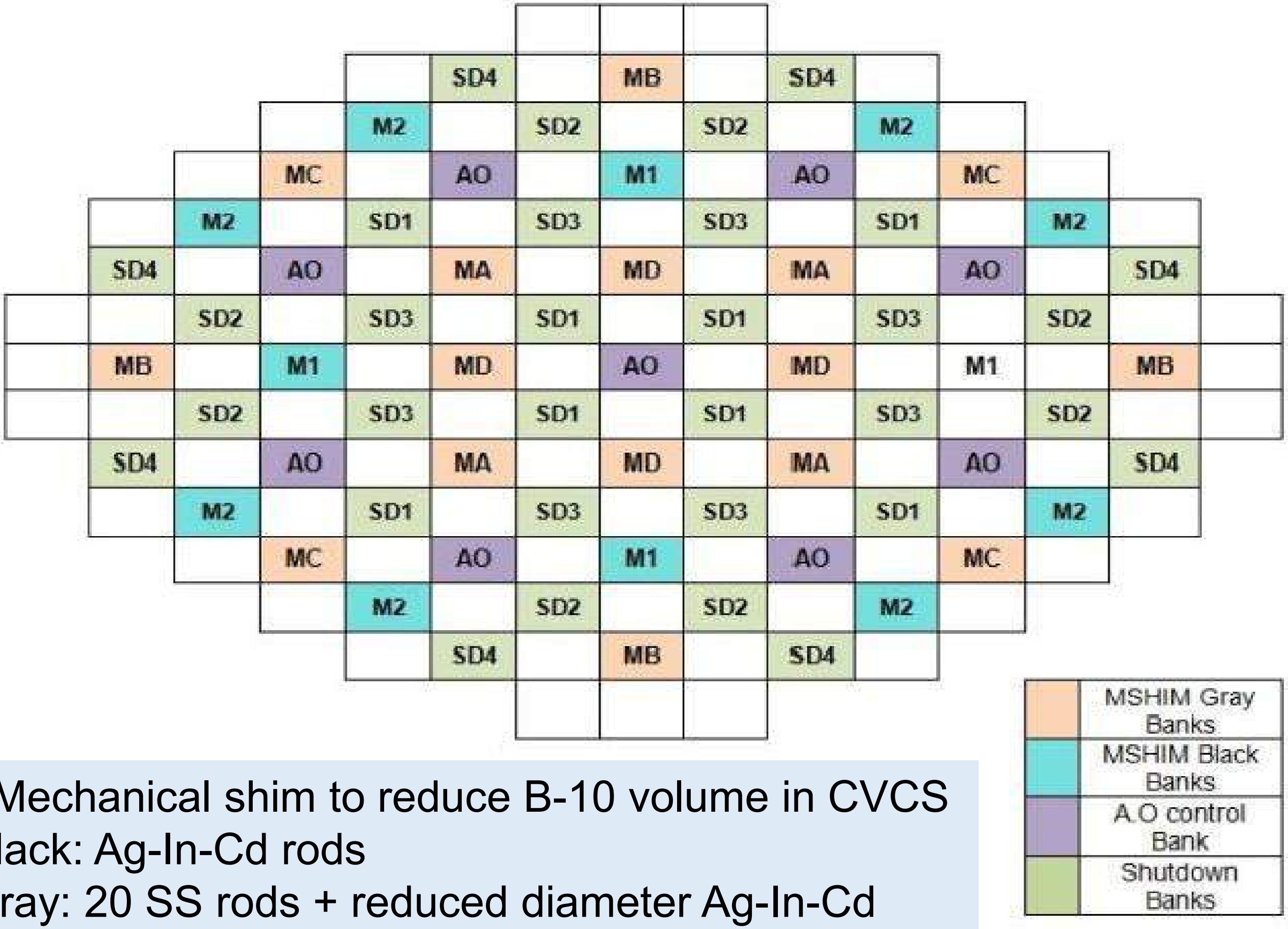
4.796% 104I	4.552% 200I						
4.796% 104I	4.796% 104I	4.176% 104I	4.796% 104I				
4.552% 200I	4.562% 48I	4.799% 108I	4.796% 104I	4.552% 200I			
4.796% 104I	4.552% 200I	4.562% 48I	4.799% 108I	4.178% 128I	4.799% 128I		
4.547% 156I	4.178% 128I	4.552% 200I	4.174% 80I	4.799% 108I	4.796% 104I	4.796% 104I	
4.796% 104I	4.552% 200I	4.176% 104I	4.552% 200I	4.562% 48I	4.799% 108I	4.176% 104I	
4.552% 200I	4.176% 104I	4.552% 200I	4.178% 128I	4.552% 200I	4.562% 48I	4.796% 104I	4.796% 104I
4.178% 128I	4.552% 200I	4.796% 104I	4.547% 156I	4.796% 104I	4.552% 200I	4.796% 104I	4.796% 104I

Axial Configuration of Fuel Rod, IFBA and PYREX



PYREX rod is only used in initial core to control excess reactivity

Control Rod Arrangement



					SD4		MB		SD4					
				M2		SD2		SD2		M2				
			MC		AO		M1		AO		MC			
		M2		SD1		SD3		SD3		SD1		M2		
	SD4		AO		MA		MD		MA		AO		SD4	
		SD2		SD3		SD1		SD1		SD3		SD2		
	MB		M1		MD		AO		MD		M1		MB	
		SD2		SD3		SD1		SD1		SD3		SD2		
	SD4		AO		MA		MD		MA		AO		SD4	
		M2		SD1		SD3		SD3		SD1		M2		
			MC		AO		M1		AO		MC			
				M2		SD2		SD2		M2				
					SD4		MB		SD4					

🟧	MSHIM Gray Banks
🟦	MSHIM Black Banks
🟪	A.O control Bank
🟩	Shutdown Banks

MSHIM= Mechanical shim to reduce B-10 volume in CVCS
MSHIM Black: Ag-In-Cd rods
MSHIM Gray: 20 SS rods + reduced diameter Ag-In-Cd
in SS cladding

Employed reactor physics analysis codes

- CASMO4E is a 2D multigroup neutron transport code used for burnup calculations of both PWRs and BWRs. CASMO4E uses ENDF/B-VI nuclear data library containing microscopic cross sections in 70 energy groups covering neutron energy range from 0 to 10 MeV.

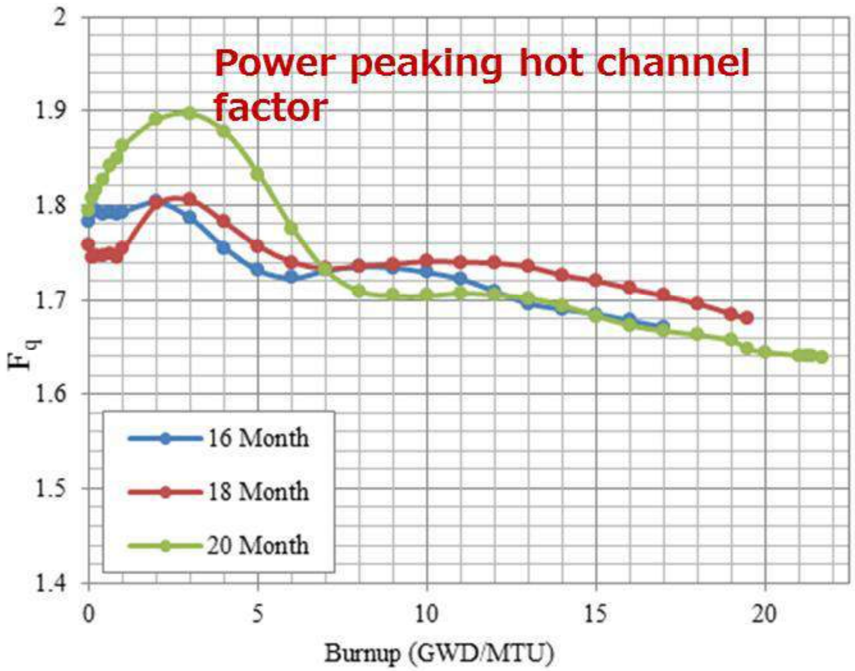
- CMSLINK processes CASMO4E card image files into a binary formatted nuclear data library used in SIMULATE-3.

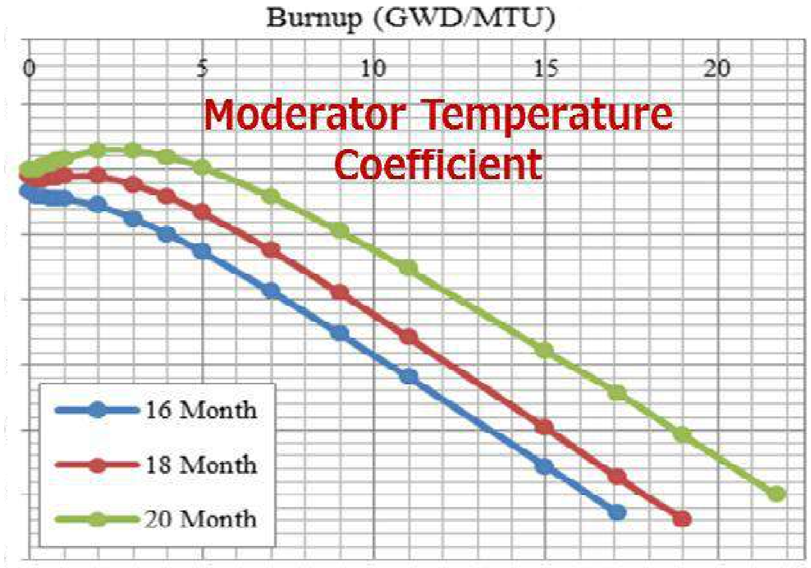
- SIMULATE-3 is 3D, two group diffusion code. It is designed for in-core fuel management and core design calculations. The code has provision of modeling 1/8, 1/4, 1/2 symmetry or full core models to perform the reactor core analysis.

CASMO4E and SIMULATE-3

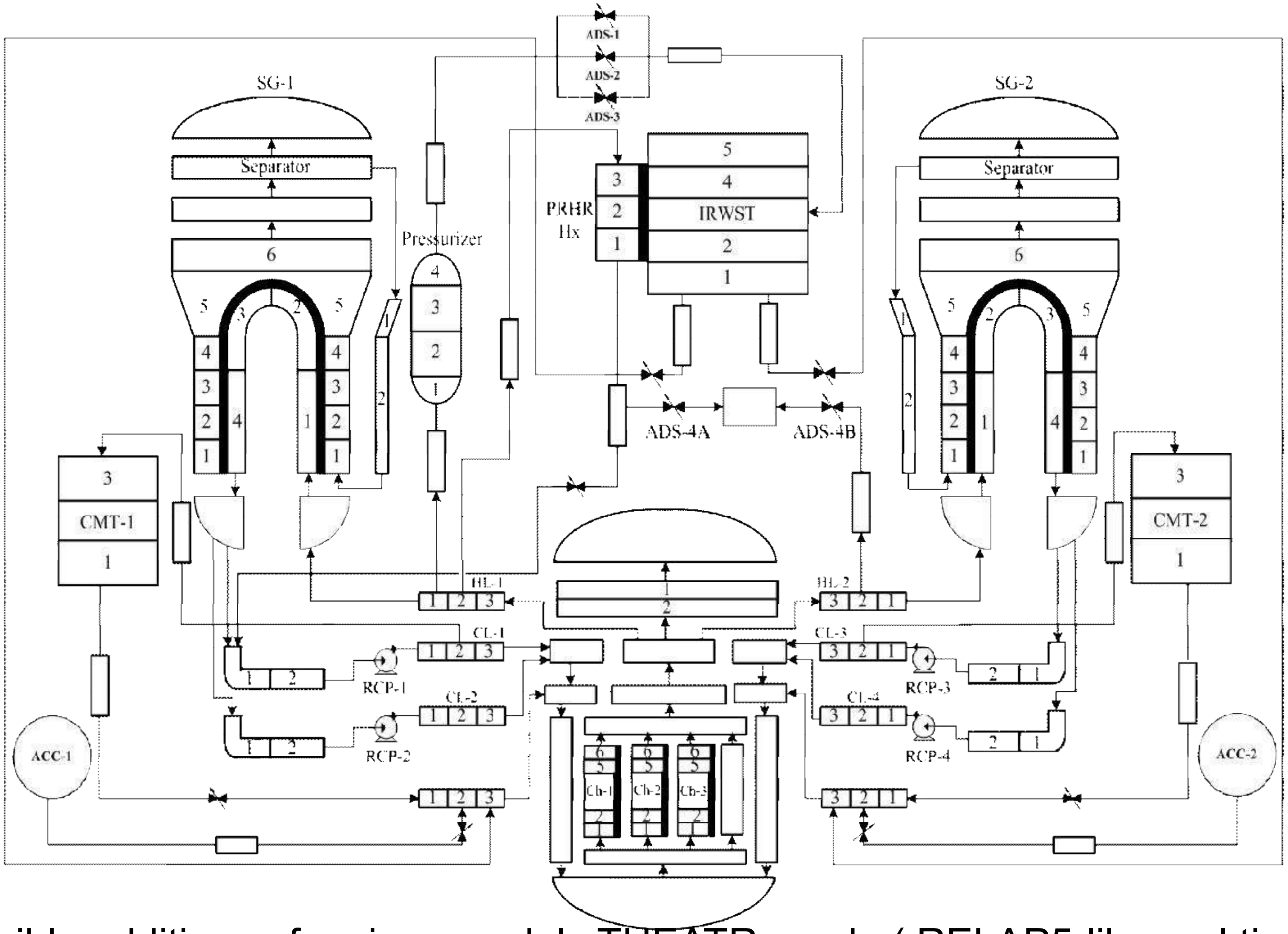
Results of Reactor Core Analysis

- Equilibrium Cores Analysis
- Fuel Depletion and FP Buildup
- Hot Channel Factors
- Burnup effect on reactivity coefficients
- Core Axial Power Shape
- Assembly average Relative Power Fraction (RPF)



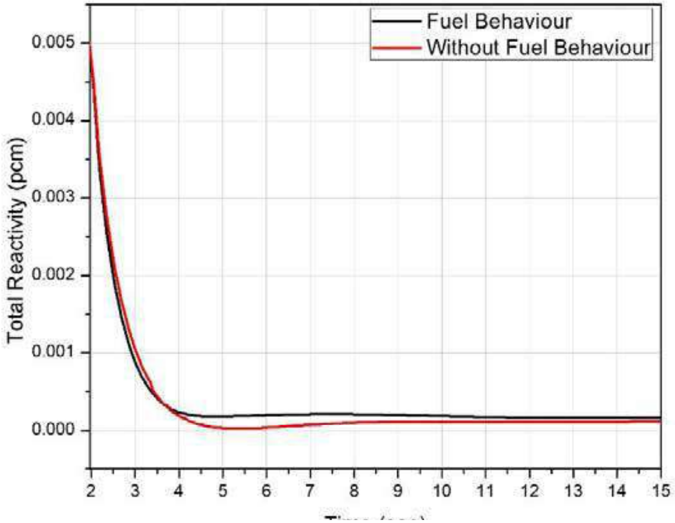


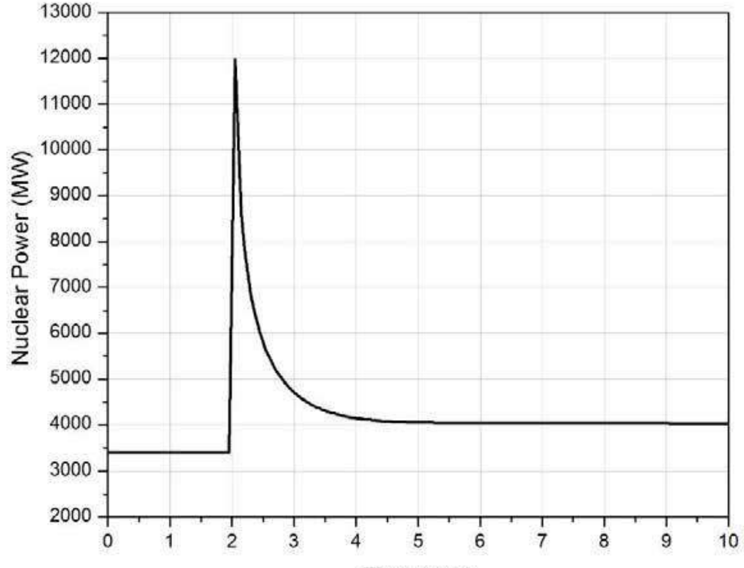
AP1000 nodalization scheme in THEATRe code

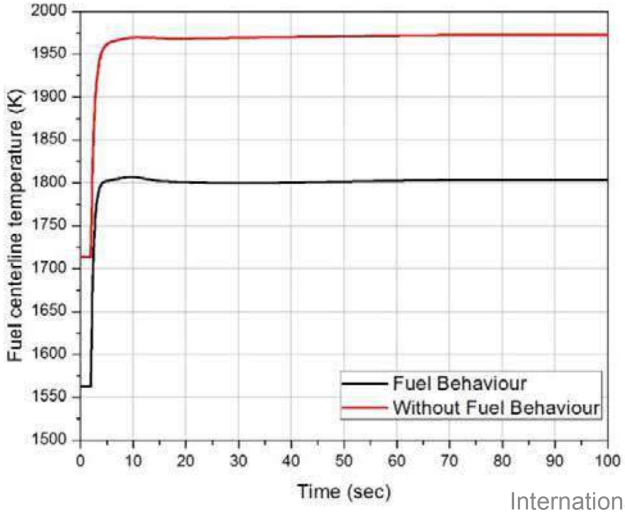


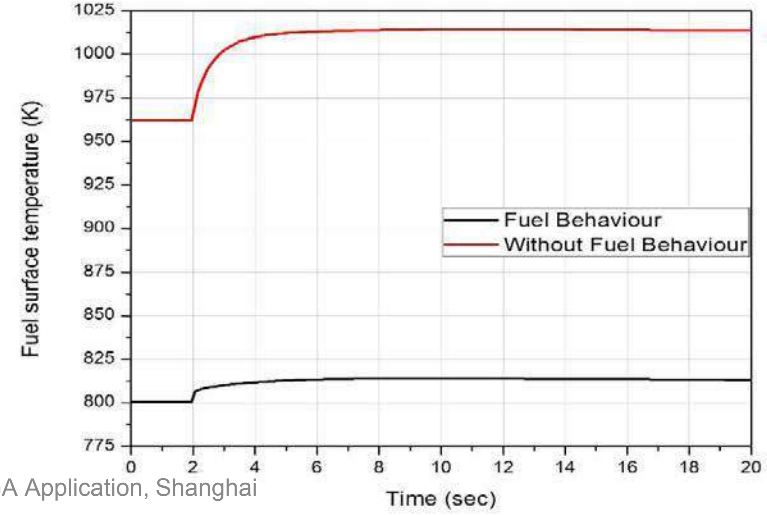
Flexible additions of various models THEATRe code (RELAP5-like real time plant simulation code) . For this study , transient fuel rod behavior model with steady-state irradiation effect was developed and coupled with it.

Comparison between with and without transient fuel pin model (Reactivity jump without scram, fresh fuel)

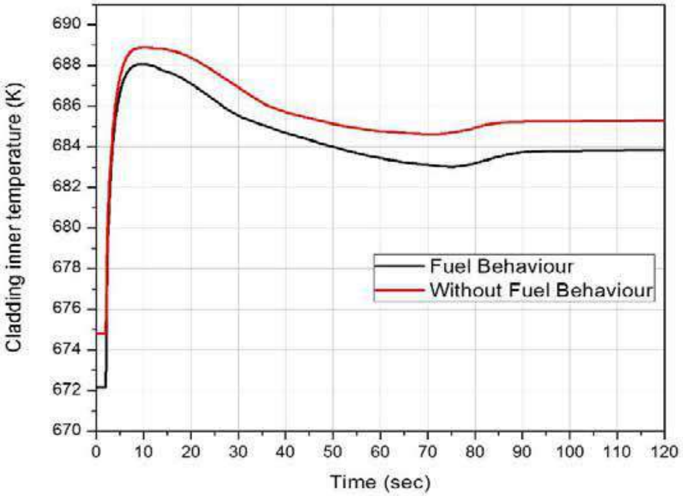


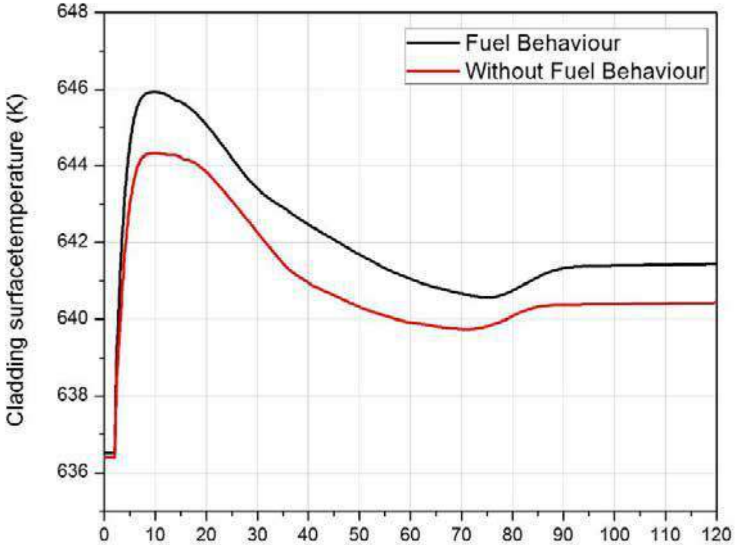


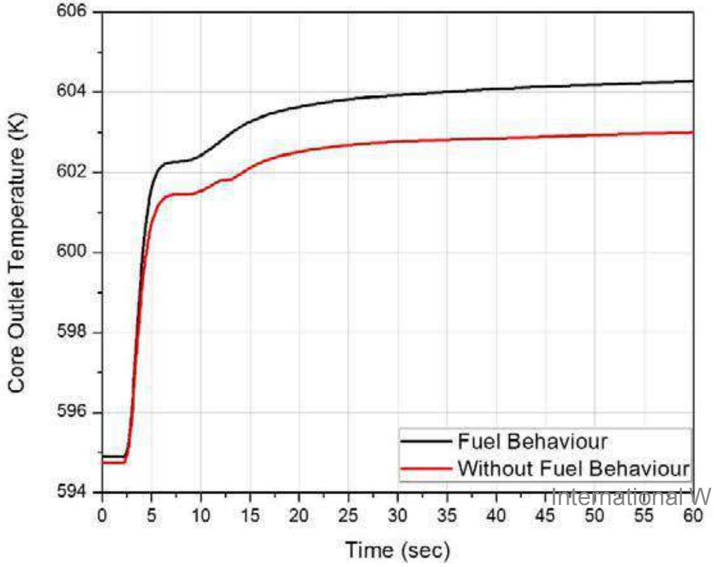


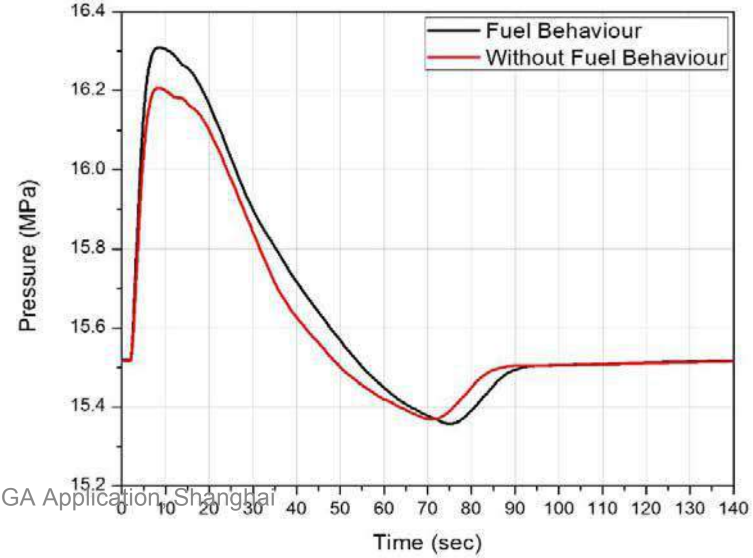


Comparison between with and without transient fuel pin model (Reactivity jump without scram, fresh fuel)


Cladding inner temperature (K)
Time (sec)
Fuel Behaviour
Without Fuel Behaviour


Cladding surfacetemperature (K)
Fuel Behaviour
Without Fuel Behaviour


Core Outlet Temperature (K)
Time (sec)
Fuel Behaviour
Without Fuel Behaviour


Pressure (MPa)
Time (sec)
Fuel Behaviour
Without Fuel Behaviour