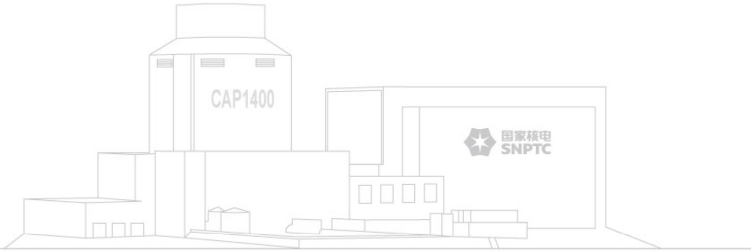
A Diverse Integrated I&C Solution for NPPs

The 8th International Workshop on Application of FPGA in NPPs
October 13-16, 2015, Shanghai, China

国家核电
SNPTC

目录



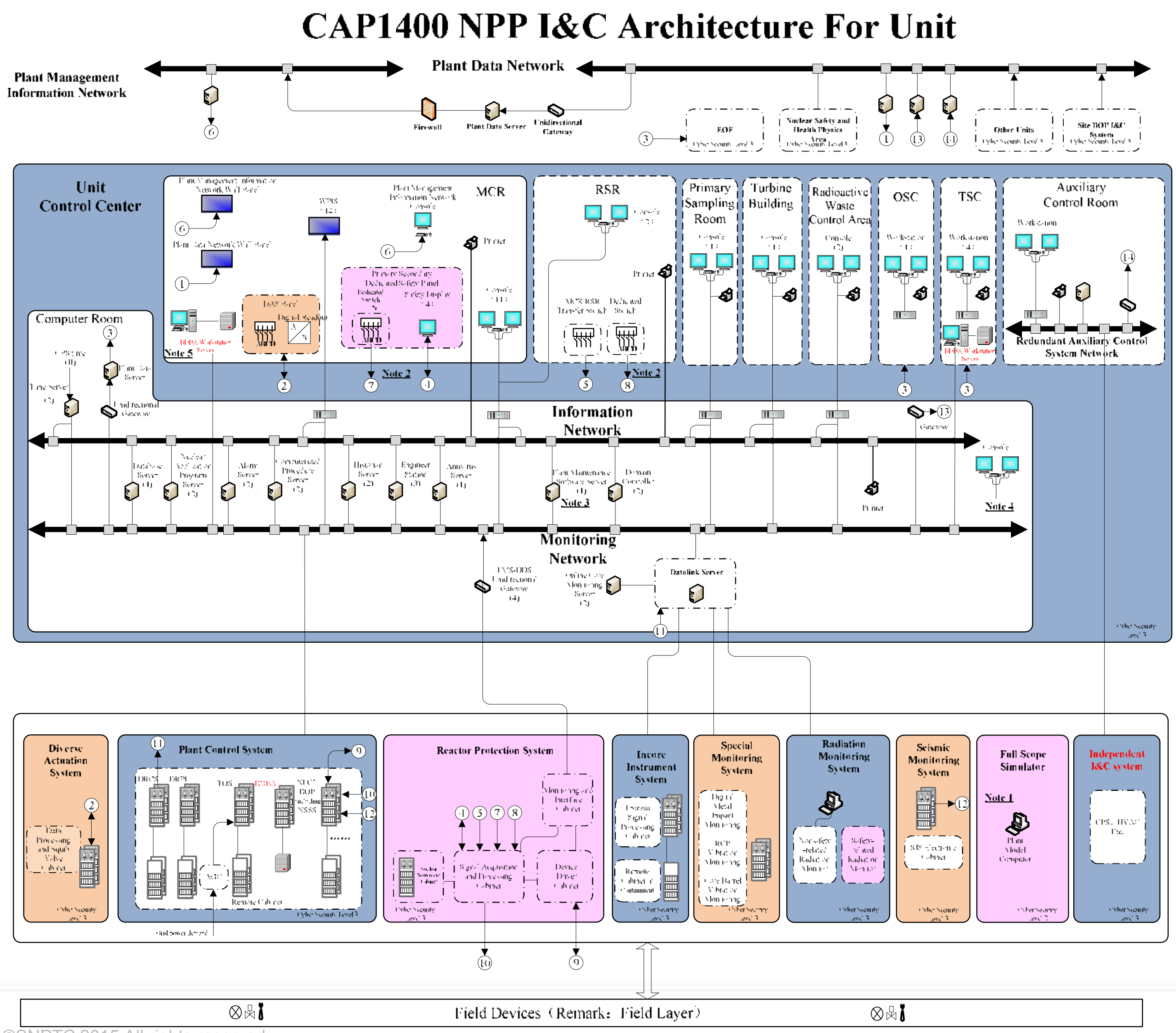
1. Integrated I&C Solution of CAP1400

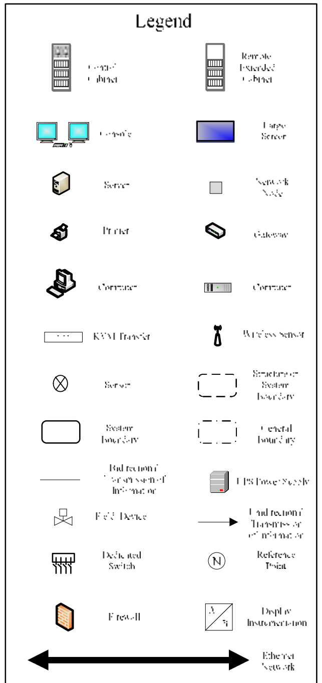
2. Diversity Requirements and Assessment

3. Diversity between different process chips

4. Conclusion

1.Integrated I&C Solution of CAP1400





Note：

1.There' s no interface between STS and I&C system；

2.Dedicated switch sends command signal to the four divisions of PMS(A、B、C、D)through hard wire；

3.Plant maintenance software server is utilized to on-line configure, test, check, diagnose smart instrumentation and actuators, and to record relevant events;

4.Consoles could be shared by servers and/or workstations via KVM router;

5.Dedicated UPS supports the workstation or server for BDBA.

Products

NuCON

Nuclear Plant Control System

NuSIM

Nuclear Full Scope Simulator

NuPAC

New Generation of RPS and Its Platform Based on FPGA Technology

NuBAC

Diverse Actuation System

NuTEC

Nuclear SMS and SJS

NuNIS

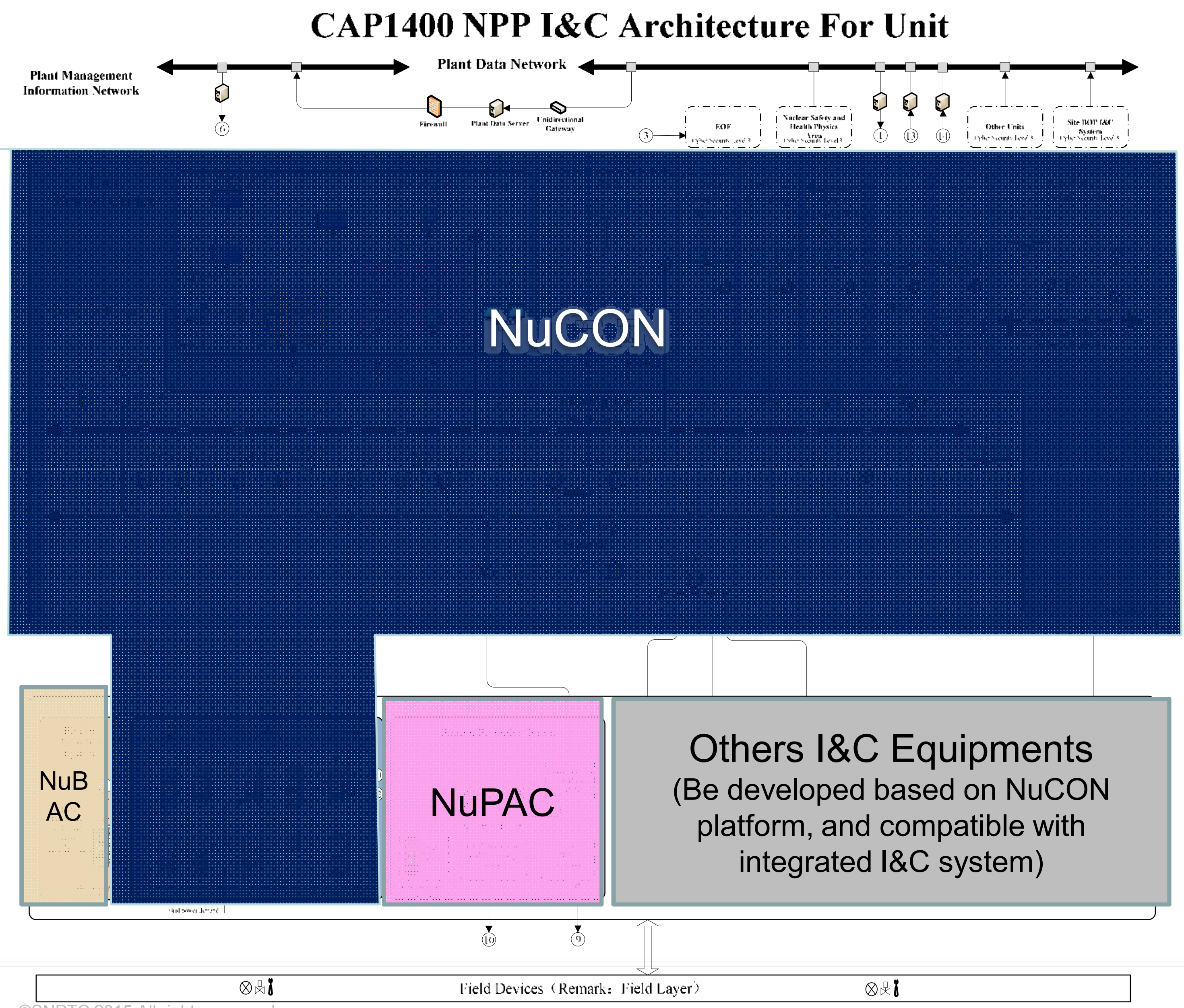
NuRAD

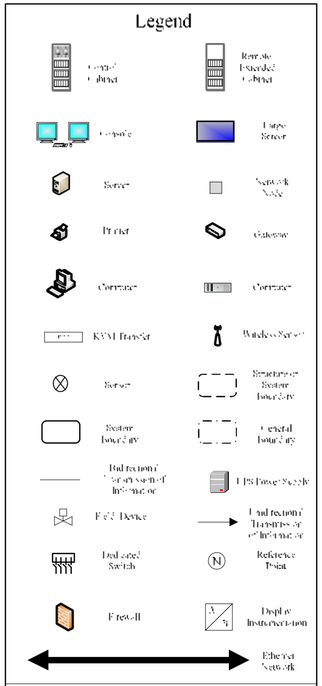
Radiation Monitoring System

NuRIC

DRCS and DRPI

1.Integrated I&C Solution of CAP1400





Note：

1.There’ s no interface between STS and I&C system；

2.Dedicated switch sends command signal to the four divisions of PMS(A、B、C、D)through hard wire；

3.Plant maintenance software server is utilized to on-line configure, test, check, diagnose smart instrumentation and actuators, and to record relevant events;

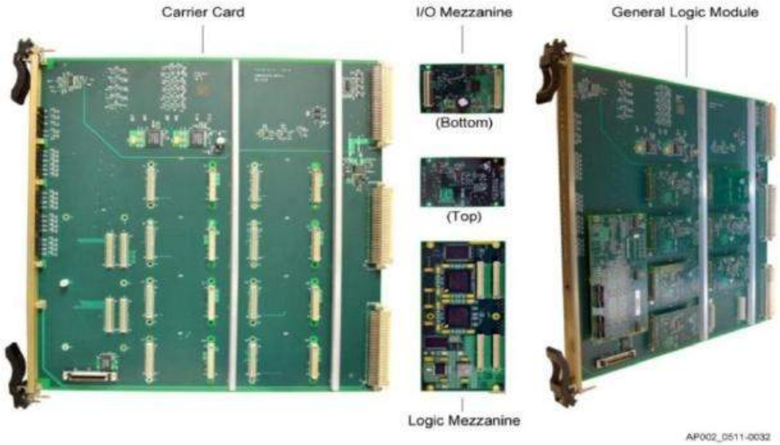
4.Consoles could be shared by servers and/or workstations via KVM router;

5.Dedicated UPS supports the workstation or server for BDBA.

NuCON

Main Features
□ All hardware including modules, chassis, and operator workstation are qualified as Seismic category I equipment;
□ Cyber Security level 3 compliance per GB/T 22239—2008 Information security technology— Baseline for classified protection of information system
□100M/1000M M-net, redundant 100M/1000M R-net, redundant 100M IO-net
□ All redundant controllers configuration with minimum processing cycle of 10ms, one type controller for all applications in NPP
□ Multi-function I/O components to minimize types, reduce the maintenance cost
□ Signal channel to channel isolation
□ Hot swap capability
□ SOE function integrated in DI module, Time Resolution less than 1ms
□ Operation conditions: operation temp -25～60℃, relative humidity 5%～95%
□ Standard IEC 61000 EMC and/or MIL EMC standard compliant
□ CE, FCC, CCC certified, IEC 61508 SIL-3 certification is in process
□ Stainless steel chassis/cabinets available for in-containment application

NuPAC



Reliable safety I&C platform with dedicated design, state of art technology and complete source code (VHDL) IV&V, being reviewed by NRC and NNSA

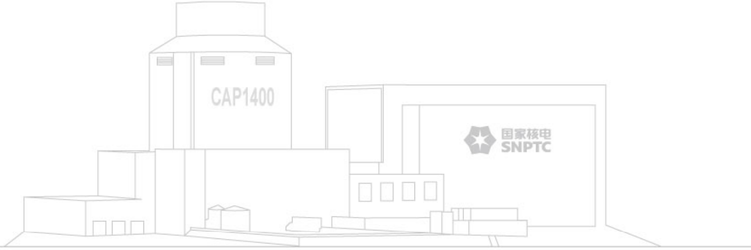
NuPAC

Main Features
□ Firmware technology (FPGA) Vs Software (CPU) technology, Diverse Safety and operational I&C
□ Meet both China NNSA and U.S NRC regulation requirements
□ No third party IP source code, increase verifiability and protection from cyber attack
□ Reduce risk caused by complex commercial software and operational environment
□ 5Mb/s Point- to-point RS422/485 to reduce the communication uncertainty
□ Redundant point-to-point backplane bus in chassis
□ FGPA chips provide Long-term lifetime support and portability when upgrading
□ Function distribution among GLMs in each safety division (no central controllers)
□ Flexible configuration for different RPS system-level architecture
□ Minimum standardization and modularization components, reduce the maintenance cost
□ Wide range operation conditions: operation temp 4～60℃, relative humidity 5%～95%
□ IEC 61000 and/or MIL EMC standard compliant, Category I Seismic qualification
□ Hot swap capability, and complete signal channel to channel isolation
□ MTBF of mezzanine card is greater than 170,000 hours

NuBAC- Diverse Actuation System

- Non-class 1E system, is the backup of RPS, SSE qualified.
- Provide defense-in-depth when common cause failure happen in RPS;
- The protect functions of DAS is diverse with RPS.

目录



1. Integrated I&C Solution of CAP1400

2. Diversity Requirements and Assessment

3. Diversity between different process chips

4. Conclusion

Requirement 24: Common cause failures

The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of ***diversity****, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.*

---- No. SSR-2/1 Safety of Nuclear Power Plants: Design

2.Diversity Requirements and Assessment

4.23. Diversity in I&C systems is the principle of monitoring different parameters, using different technologies, different logic or algorithms, or different means of actuation in order to provide several ways of detecting and responding to a significant event.

4.25. The adequacy of the diversity provided with respect to the above criteria should be justified.

4.28. Claims for diversity based only on a difference in manufacturers' names are insufficient without consideration of this possibility.

4.29. With regard to the diversity of software, experience indicates that independence of failure modes may not be achieved if multiple versions of software are developed to the same software requirements specification.

---- No. NS-G-1.3 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants

2.Diversity Requirements and Assessment

	NuPAC	NuCON	NuBAC
CM Tool	• Windchill • Rational ClearCase • Rational ClearQuest • Rational DOORS • Mentor Reqtracer(Mentor Graphic) • Mentor library manager(Mentor Graphic)	• Windchill • Rational ClearCase • Rational ClearQuest • Rational DOORS	Rational DOORS
Electronics Development Tool	• Mentor Design Capture • Mentor Expedition • PTC Creo • OrCAD Pspice	Cadence	Altium
PL/Software Development Tool	• Actel libero IDE • Windriver WorkBench • Mentor Modelsim • Aldec Riviera • VHDL	• Visual studio 2010、 • QNX Momentics • DD IDE • Verilog HDL	•Quartus •C Language
Operating System	• VxWorks (for safety parameter video display only)	• Windows 7（HMI） • QNX 6.5（controller）	/
Chip	Flash based FPGA （Microsemi Corporation）	CPU	SRAM based FPGA （Altera）
PCB Vendor	• P.C.B.A Electronics (Wuxi) Ltd. • Shanghai Dahua Instrument Factory	• Advantech Co. Ltd • Adlink Technology Inc.	Suyuan Electronics Ltd.
Program Team	• Development Team • Test Team • IV&V Team • Third party IV&V Team	• Development Team • Test Team	• Development Team (third party - SAIC) • Test Team

Defense in Depth and Diversity (D3) Compliance

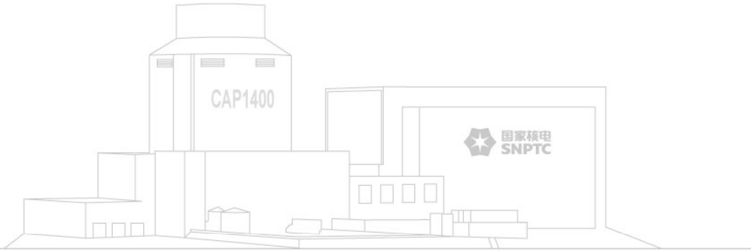
2.Diversity Requirements and Assessment

Diversity Attributety		Strategy									
		A1	A2	B1	B2	B3	C1	C2	C3	C4	C5
Design	Different technology	x	x	—	—	—	—	—	—	—	—
	Different approach-same technology	—	—	x	x	x	—	—	—	—	—
	Different architecture	i	i	i	i	i	x	x	x	x	x
Equipment manufacture	Different manufacturer-different design	x	—	x	—	x	—	—	—	—	—
	Same manufacture-different design	—	x	—	x	—	—	—	—	—	—
	Different manufacture-same design	—	—	—	—	—	x	—	x	x	x
	Same manufacture-different version	—	—	—	—	—	—	x	—	—	—
Logic processing equipment	Different logic processing architecture	i	i	i	i	i	x	x	—	x	x
	Different logic processing version in same architecture	—	—	—	—	—	—	—	x	—	—
	Different component integration architecture	i	i	i	i	i	—	—	x	—	—
	Different data-flow architecture	i	i	—	—	—	—	—	—	—	—
Functional	Different underlying mechnism	i	i	i	i	i	—	—	—	—	—
	Different purpose, function, control, logic, or actuation means	i	i	x	x	x	x	x	x	x	x
	Different response time scale	—	—	—	—	—	—	—	—	—	—
Life-cycle	Different design organizations/companies	x	—	x	—	x	x	—	x	x	x
	Different management teams within same company	—	x	—	x	—	—	x	—	—	—
	Different design/development teams (designers, engineers, programmers)	i	i	i	x	i	i	x	i	i	i
	Different implementation/validation teams (testers, installers, or certification personnel)	i	i	i	x	i	i	x	i	i	i
Signal	Different parameters sensed by different physical effects	x	x	x	x	x	x	x	x	x	x
	Different parameters sensed by same physical effects	x	x	x	x	x	x	x	x	x	x
	Same parameter sensed by a different redundant set of similar sensors	x	x	x	x	x	x	x	x	x	x
Logic	Different algorithms, logic, and program architecture	i	i	x	x	x	x	x	x	x	x
	Different timing or order of execution	i	i	i	i	i	—	—	—	—	—
	Different runtime environment	i	i	i	i	i	x	x	x	x	x
	Different functional representation	i	i	i	i	i	x	x	x	x	x

Note: x: intentional diversity, i: inherent diversity, -: not applicable or no information

--NUREG 7007

目录



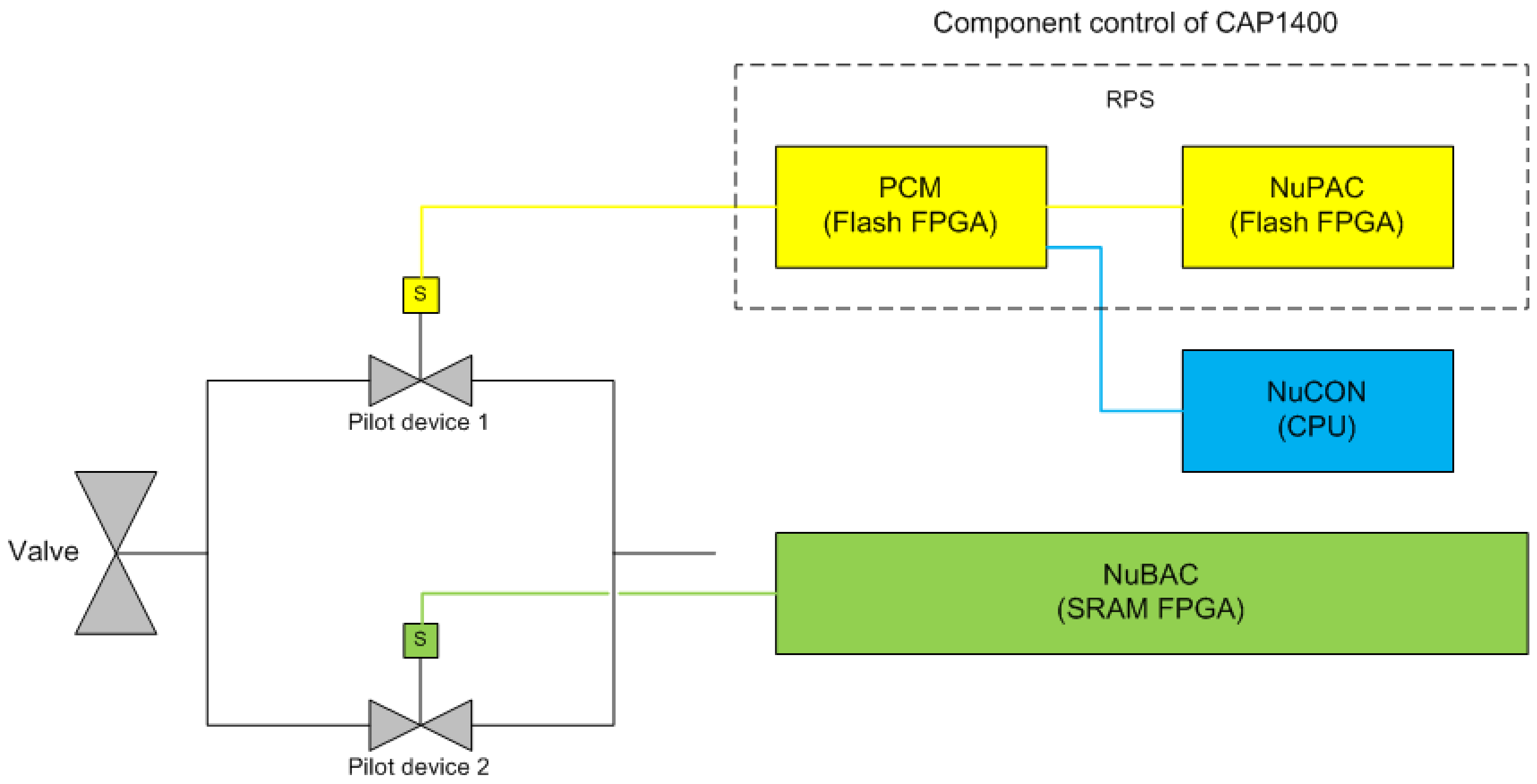
1. Integrated I&C Solution of CAP1400

2. Diversity Requirements and Assessment

3. Diversity between different process chips

4. Conclusion

How diverse it shall be if both systems use FPGA?



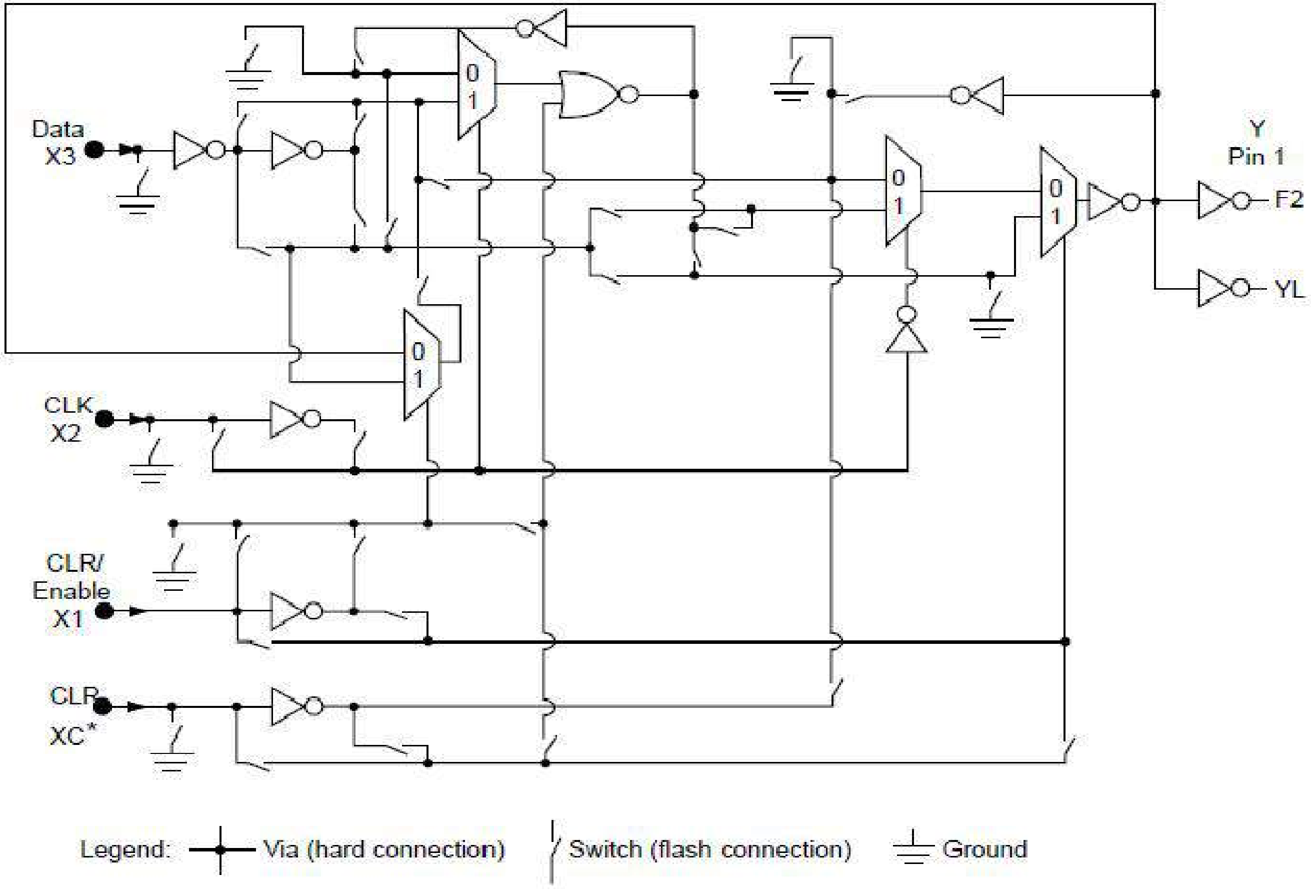
3. Difference between different FPGA chips

Diversity Attribute		Rank	DCE WT	Strategy name								
				A			B			C		
				INT	INH	Score	INT	INH	Score	INT	INH	Score
Design	Different technology	1	0.500	x		0.500						
	Different approach-same technology	2	0.333				x		0.333			
	Different architecture	3	0.167		i	0.167		i	0.167	x		**0.167**

Intentional diversity is provided through the selection of distinct technology approaches. The specific form of technology difference employed in this classification involves the use of different digital technologies ***(e.g., FPGA or CPLD vs general-purpose CPU)*** *as the basis for different systems, redundancies, or subsystems.*

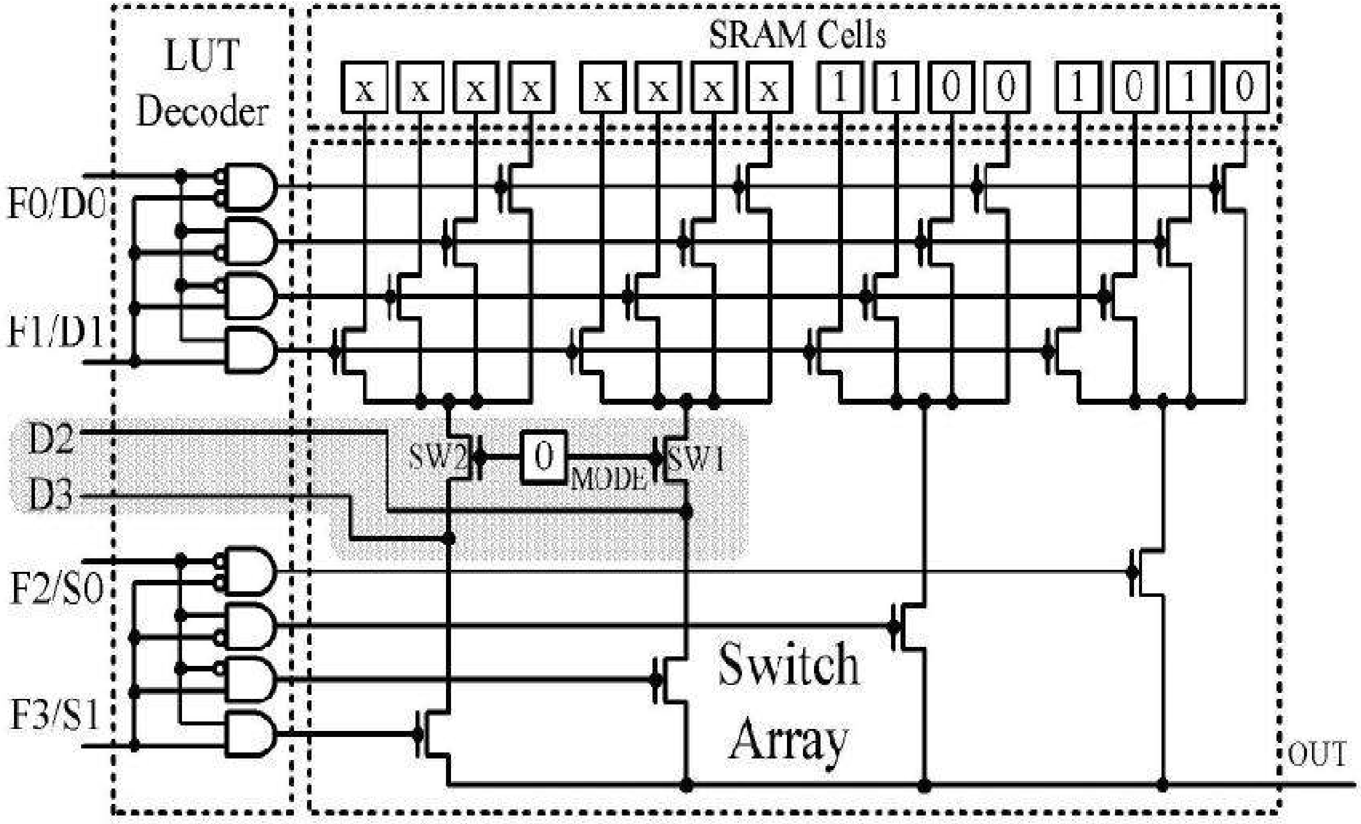
What about different FPGA technology?

Flash FPGA VS SRAM FPGA (ProASIC3E VS Cyclone IV)



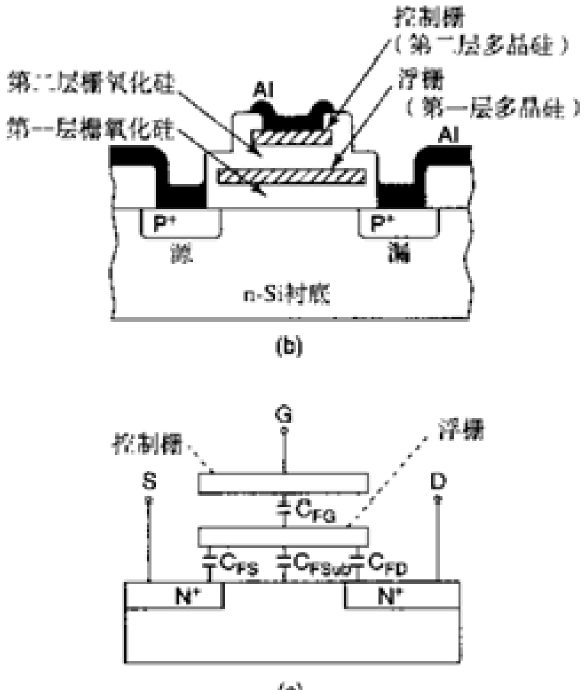
Versatile architecture of FLASH FPGA: switches stored in FLASH unit are configurable to realize different hardware logic

Flash FPGA VS SRAM FPGA (ProASIC3E VS Cyclone IV)



Lookup table architecture of SRAM FPGA: truth table stored in SRAM cells is used to realize different hardware logic

Flash FPGA VS SRAM FPGA (ProASIC3E VS Cyclone IV)



(b)

(c)

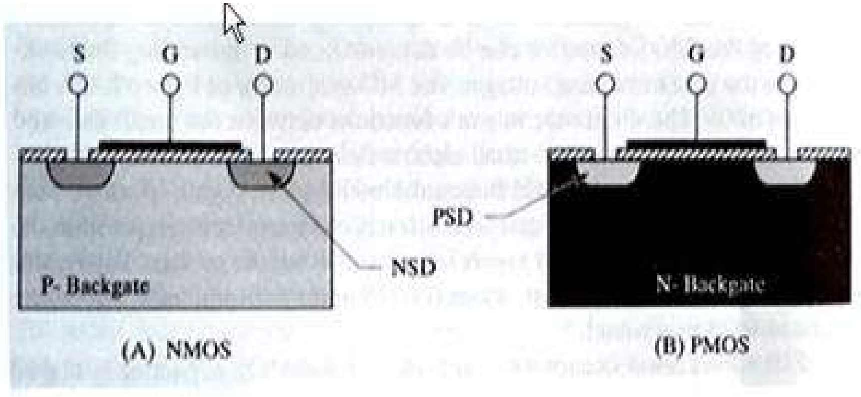


图 1 MOSFET 晶体管的截面图：NMOS（A）和 PMOS（B）

Flash transistor

SRAM transistor

Flash FPGA VS SRAM FPGA (ProASIC3E VS Cyclone IV)

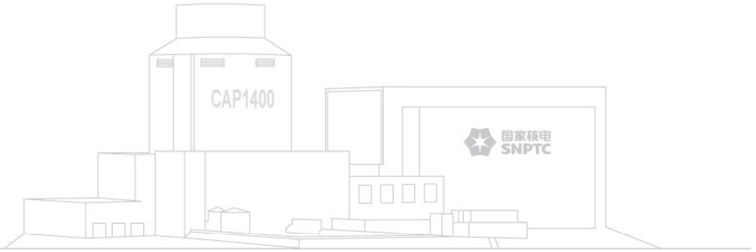
No.	difference	FLASH FPGA	SRAM FPGA
1	CLB architecture	Versatile	Look up table
2	Logic storage cell	Flash connection	SRAM cell
3	Transistor architecture	Transistor contains 2 layers of Polysilicon (to form floating gate as storage cell)	Transistor contains one layer of Polysilicon (to store data with one pair of coupled inverters)
4	size	130nm	60nm
5	Power off characteristic	Data is retained when power is off	Data is lost when power is off
6	Configuration chip	No need	Configuration chip is needed for start-up
7	manufacture	UMC	TSMC
8	Designer	Microsemi	Altera
9	Tool	Libero	Quartus
10	Language	VHDL	Verilog

Flash FPGA VS SRAM FPGA

- There is big difference between FLASH FPGA and SRAM FPGA, adequate mitigation of potential CCF vulnerabilities will be provided by these 2 distinctly different technology per NUREG 7007.
- It is justifiable to take FLASH FPGA and SRAM FPGA as distinctly different approach per NUREG 7007, and follow Strategy B ways to evaluate the Diversity of corresponding systems.

Diversity Attribute		**Rank**	**DCE WT**	Strategy name								
				A			**B**			**C**		
				INT	**INH**	**Score**	**INT**	**INH**	**Score**	**INT**	**INH**	**Score**
Design	Different technology	1	0.500	**x**		**0.500**						
	Different approach-same technology	2	0.333				**x**		**0.333**			
	Different architecture	3	0.167		i	0.167		i	0.167	**x**		**0.167**
Equipment manufacturer	Different manufacturer - different design	1	0.400	**x**		0.400	**x**		0.400			
	Same manufacturer-different design	2	0.300									
	Different manufacturer-same design	3	0.200							**x**		**0.200**
	Same manufacturer--different version	4	0.100									

目录



1. Integrated I&C Solution of CAP1400

2. Diversity Requirements and Assessment

3. Diversity between different process chips

4. Conclusion

4. Conclusion

There is big difference between FLASH FPGA and SRAM FPGA, adequate mitigation of potential CCF vulnerabilities will be provided by these 2 distinctly different technology , and It is justifiable to take FLASH FPGA and SRAM FPGA as distinctly different approach per NUREG 7007, and follow Strategy B ways to evaluate the Diversity of corresponding systems.

“Nu” serial of products provide diverse integrated solution for NPP I&C systems, with state of art technologies utilized in CAP1400 design.

国家核电
SNPTC

Safe Nuclear Energy
Better Natural Life