中核控制系统工程有限公司
CHINA NUCLEAR CONTROL SYSTEM ENGINEERING CO., LTD.

CNCS

The Application of FPGA in Safety I&C System of Nuclear Power Plants

--- NicSys®8000N

Qi Kelin

Chief Engineer

Oct 13th 2015

www.cncs.bj.cn

CONTENTS

1 About CNCS

2 CNCS Products

3 NicSys®8000N

About Us

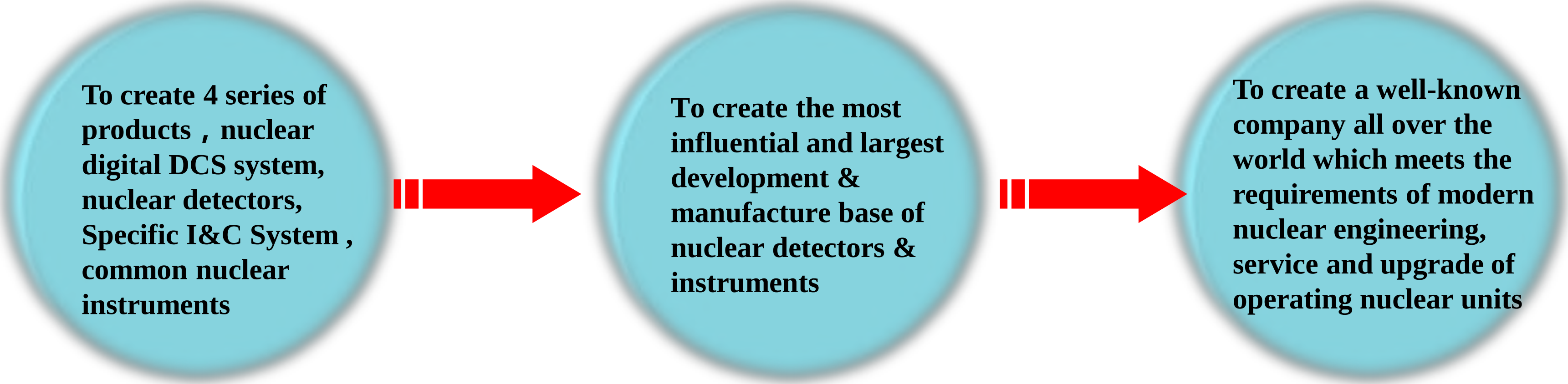
- CNNC holding subsidiary, a high technology company specified in developing digital I&C system for nuclear power plant and providing integration solution of I&C system.
- Possesses lots of I&C products for nuclear industry, including DCS platform, almost 100 kinds of nuclear instrument. CNCS is a professional supplier in nuclear I&C market that takes the longest product chain and most integrated category of products.
- Certificated with Germany TUV qualification of ISO9001：2008, manufacture & design license of nuclear safety equipment for civil use, 700 achievements of innovation of science, 25 software copyrights and 16 patents.

Company Strategy and Goals

为全球核能全产业链用户提供优质数字化仪控解决方案

Providing The High Quality Digital I&C Solution To Global Customer Of Nuclear Industry

Business philosophy	High Starting Point, High Standard, High Level
Core competence	Development, manufacture and implementation capabilities of nuclear DCS system, nuclear specified I&C instruments, nuclear detectors and in common use I&C equipment for nuclear.

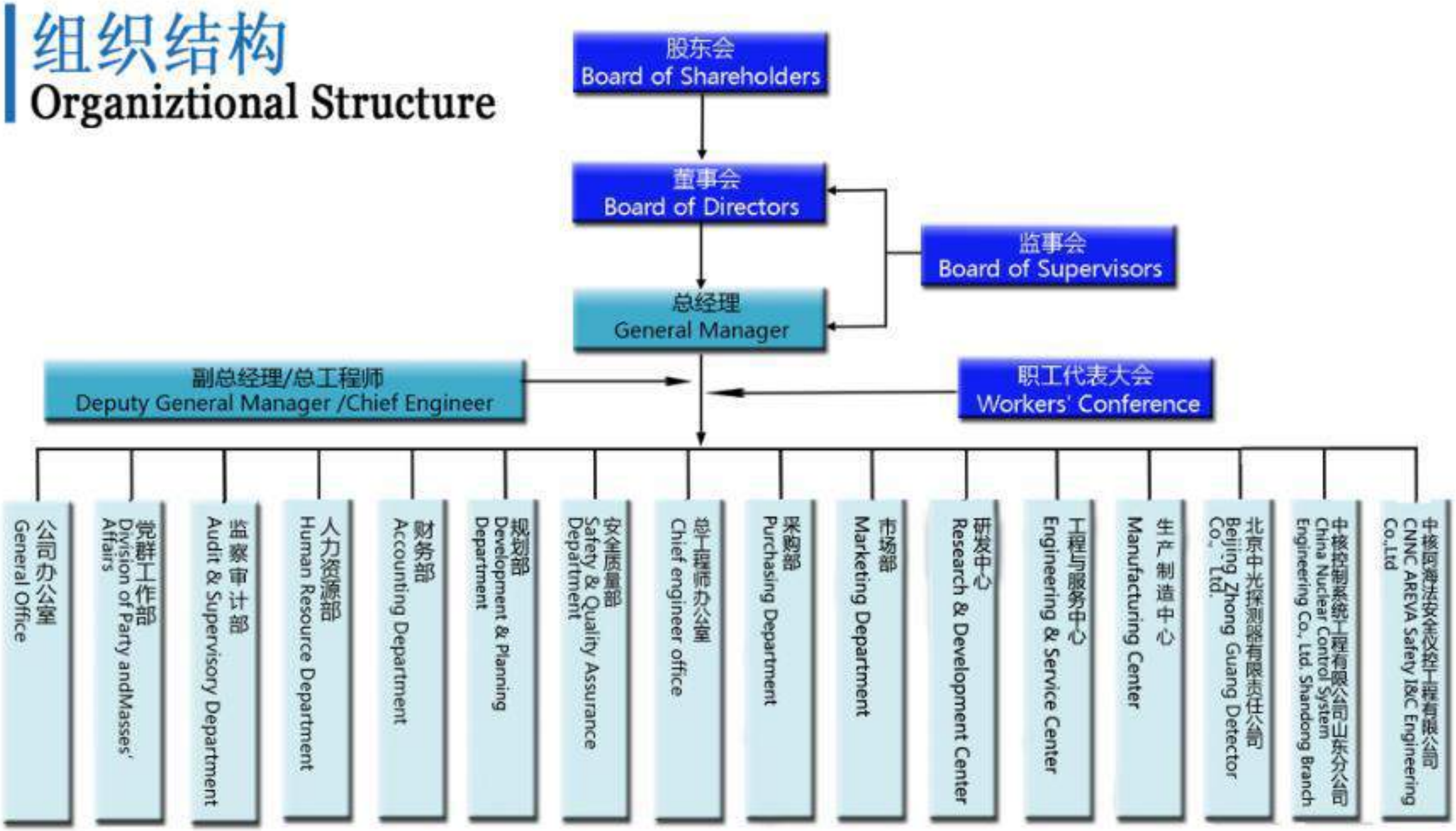


To create 4 series of products，nuclear digital DCS system, nuclear detectors, Specific I&C System , common nuclear instruments

To create the most influential and largest development & manufacture base of nuclear detectors & instruments

To create a well-known company all over the world which meets the requirements of modern nuclear engineering, service and upgrade of operating nuclear units

Organization structure



组织结构
Organiztional Structure

股东会
Board of Shareholders

董事会
Board of Directors

监事会
Board of Supervisors

总经理
General Manager

副总经理/总工程师
Deputy General Manager /Chief Engineer

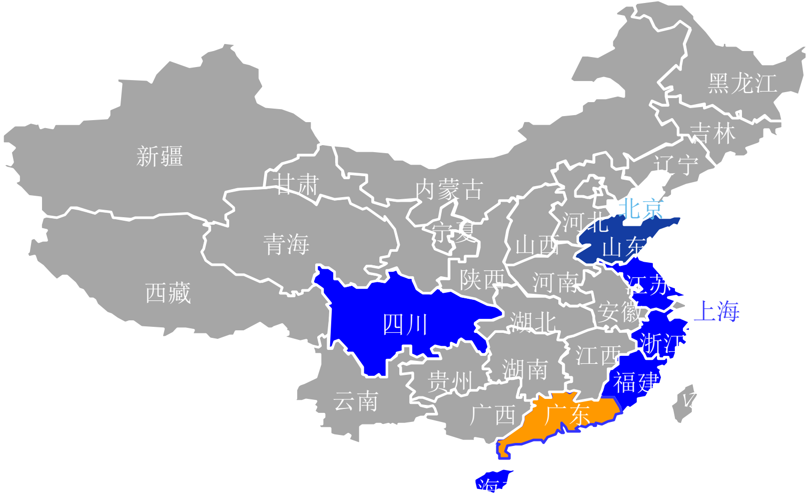
职工代表大会
Workers' Conference

- 公司办公室 General Office
- 党群工作部 Division of Party andMasses' Affairs
- 监察审计部 Audit & Supervisory Department
- 人力资源部 Human Resource Department
- 财务部 Accounting Department
- 规划部 Development & Planning Department
- 安全质量部 Safety & Quality Assurance Department
- 总工程师办公室 Chief engineer office
- 采购部 Purchasing Department
- 市场部 Marketing Department
- 研发中心 Research & Development Center
- 工程与服务中心 Engineering & Service Center
- 生产制造中心 Manufacturing Center
- 北京中光探测器有限责任公司 Beijing Zhong Guang Detector Co., Ltd.
- 中核控制系统工程有限公司山东分公司 China Nuclear Control System Engineering Co., Ltd. Shandong Branch
- 中核阿海法安全仪控工程有限公司 CNNC AREVA Safety I&C Engineering Co.,Ltd

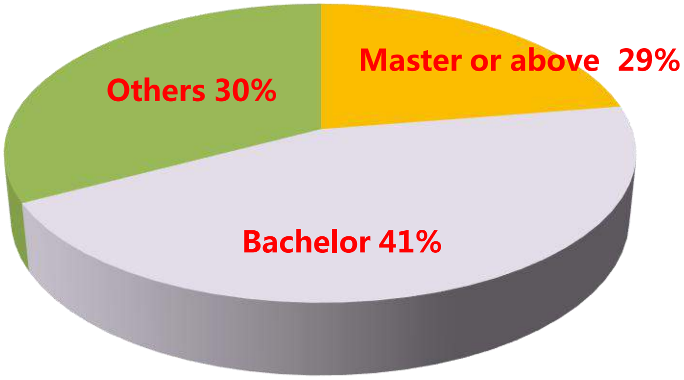
Human Resource and Achievements

CNCS has nearer 650 employees, including:

- 1 expert for special government allowances
- 15 professor of engineering
- 44 senior engineer
- 172 engineer
- 144 assistant engineer



Education Degree Proportion



- Achieve more than 100 electric and I&C projects
- 14 Units DCS for global NPP
- Provided instruments for Shenzhou spacecraft.
- Provided internal & external nuclear detectors, control instruments, protection instruments, measuring instruments, radiation measurement instruments for over 30 reactors
- Provided specific equipment for nuclear industry, such as nuclear fuel factory and post treatment factory
- Provided common nuclear equipment for health & epidemic prevention dept., environment monitoring dept., university, college and institutes

Main Products

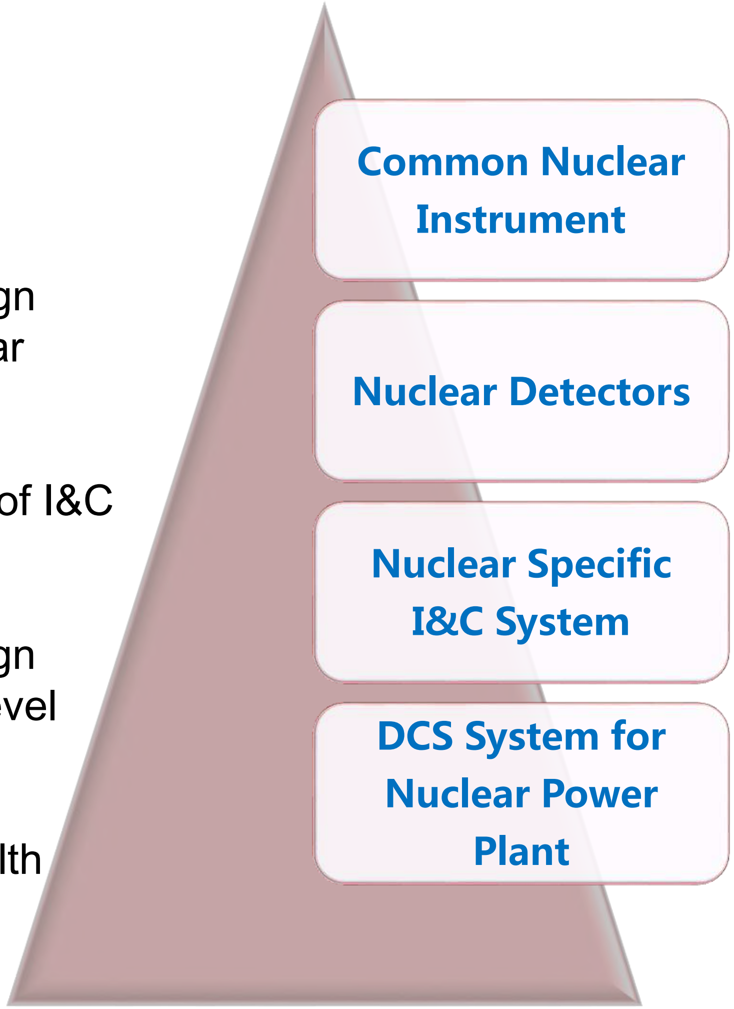
4 Series of Products

- Nuclear Digital Control System (DCS)
- Specific I&C System for Nuclear Power Plant
- Nuclear Detectors
- Common Nuclear I&C Instruments

4 Types of Business

- Provide service of development, manufacture, design and implementation on I&C products for new nuclear power plant and nuclear chemical industry
- Provide maintenance support and upgrade service of I&C system for operating nuclear units
- Provide service of development, manufacture, design and implementation on I&C products for civil high level business
- Provide nuclear instruments and equipment for health and epidemic prevention dept., environment monitoring dept., universities and colleges

I&C High Level Professional Market



Common Nuclear Instrument

Nuclear Detectors

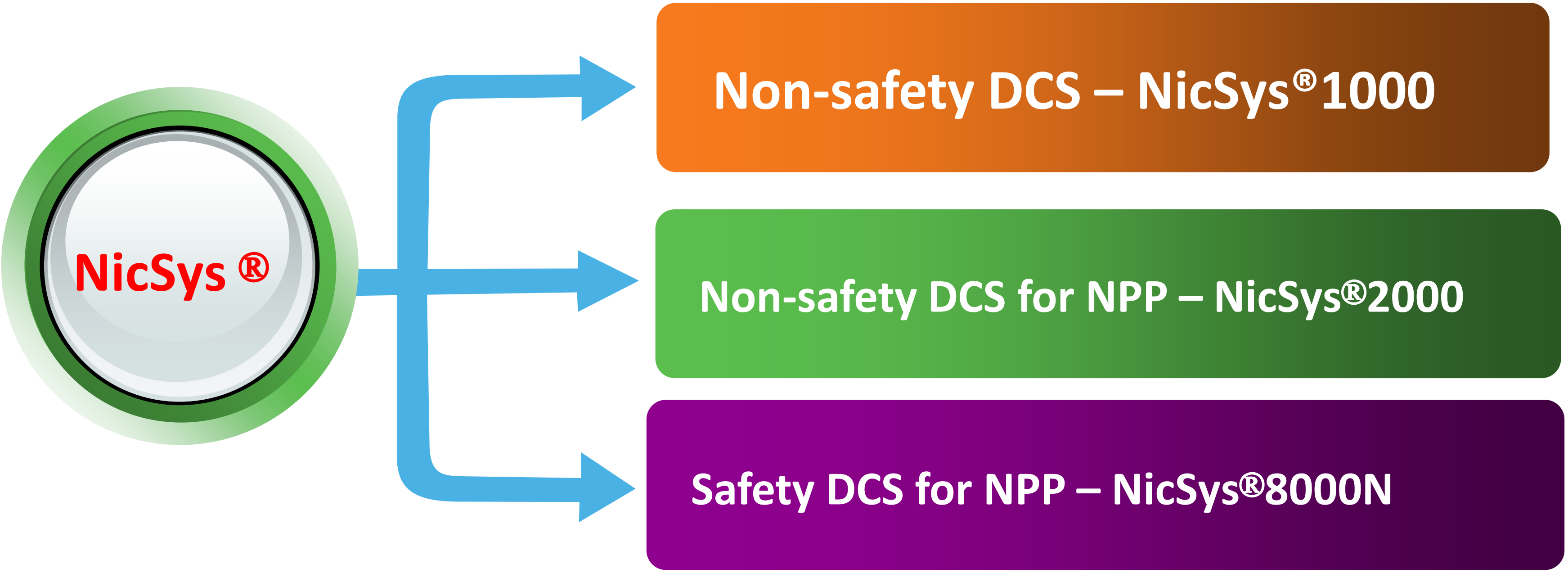
Nuclear Specific I&C System

DCS System for Nuclear Power Plant

Distributed Control System

NicSys® series

CNCS aims to localization of the nuclear power digital control system, independently R&D DCS platform of NicSys® series complying with quality requirements of nuclear standards.



NicSys ®

Non-safety DCS – NicSys®1000

Non-safety DCS for NPP – NicSys®2000

Safety DCS for NPP – NicSys®8000N

NicSys®8000N Platform

NicSys® 8000N

安全级DCS 平台

Safety I&C Platform

Why using FPGA for our safety DCS system

FPGA Technology Advantages

- Higher Safety
- Faster response time
- Simpler structure
- High security
- Equipment diversity
- Cost advantage

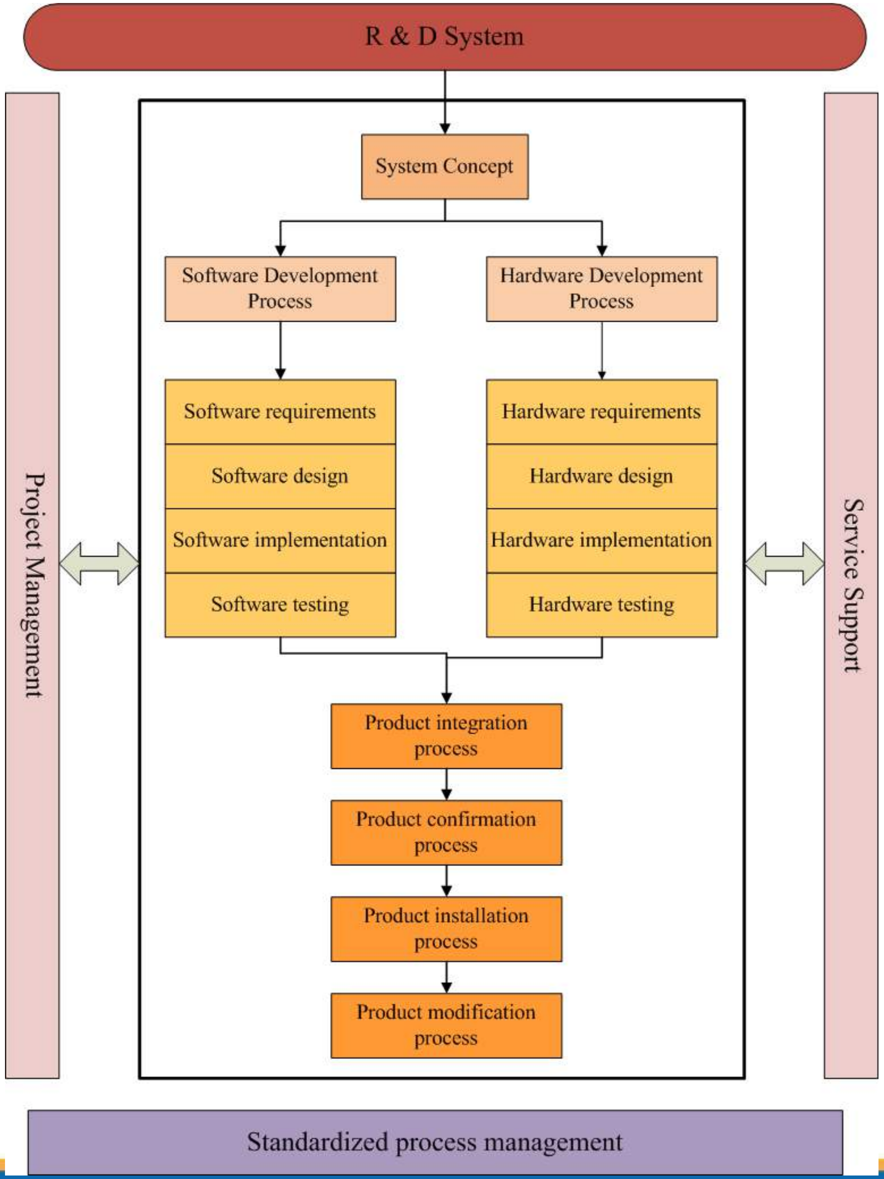
CNCS FPGA Application Route

1. Establish the infrastructure suitable for the development of FPGA
2. Research on the development standard for NicSys ® 8000N
3. Establish the development procedure for NicSys ® 8000N
4. Develop NicSys ® 8000N products
5. NicSys ® 8000N application

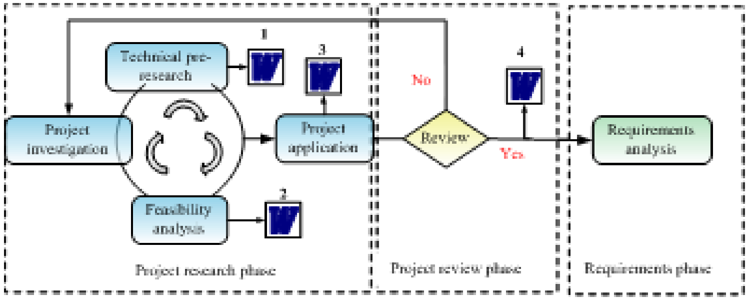
NicSys® 8000N Standards

IEC	IEEE	DO	GB/NB	Work Field
IEC61513	IEEE603	ARP4754	NB20026 GB13824	System design
IEC60880	IEEE7-4.3.2	DO178B/C	NB20054 GB13629	IE software design
IEC62566		DO254	NB20300	1E programmable hardware design
IEC60780	IEEE323		GB12727	Equipment certification
IEC61000			GB17626	EMC
	IEEE1012		Being developed	V&V
	IEEE730		EJ890	QA
	IEEE1228			Safety plan
	IEEE828		Being developed	CM

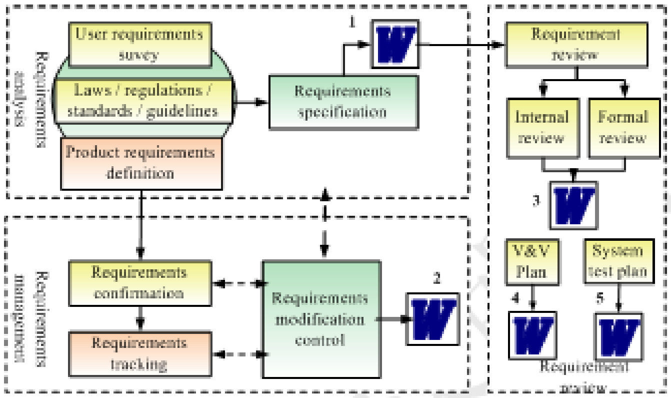
NicSys®8000N R&D system schematic diagram



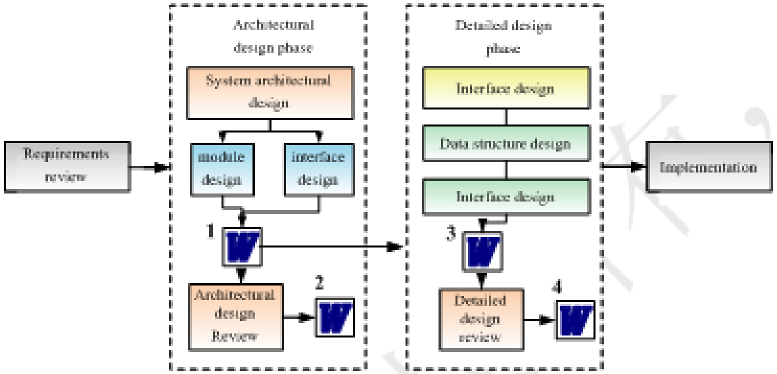
NicSys®8000N development process

Stage/ Management	Brief Process	Output Files	Work Instruction
Plan	 Technical pre-research 1 3 Project investigation Project application No 4 Review Yes Requirements analysis Feasibility analysis 2 Project research phase Project review phase Requirements phase	1. NicSys8000 pre-research record	NicSys8000 pre-research work instruction
		2. Feasibility analysis report NicSys8000 development feasibility assessment form	R & D project work instruction
		3. Project report	
		4. Project approval form	

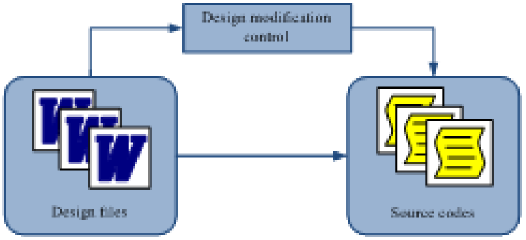
NicSys®8000N development process

Stage/ Management	Brief Process	Output Files	Work Instruction
Requirements	 Requirements analysis User requirements survey Laws / regulations / standards / guidelines Product requirements definition Requirements specification 1 Requirements management Requirements confirmation Requirements tracking Requirements modification control 2 Requirement review Internal review Formal review 3 V&V Plan System test plan 4 5 Requirement review	1. NicSys8000 requirements specification	IEEE std 830-1998 Product requirements analysis work instruction
		2. NicSys8000 requirements tracking report NicSys8000 requirements tracking matrix NicSys8000 requirement modification application form	Product requirements modification control procedures; Product requirements management work instruction Matrix tracking control procedures
		3. NicSys8000 requirements analysis phase VV summary report NicSys8000 requirements specification review comments form; NicSys8000 hazard/safety/criticality analysis	IEEE std 1012-2004 Requirements review work instruction
		4. NicSys8000 verification and validation plan	IEEE std 1012-2004 Verification and validation preparation instruction
		5. NicSys8000 system test plan NicSys8000 system test specification	System test work instruction
		6. NicSys8000 Hazard Analysis Report	IEEE std 1012-2004 Hazard Analysis work instruction
		7. NicSys8000 safety Analysis Report	IEEE std 1012-2004 Safety Analysis work instruction
		8. NicSys8000 criticality Analysis Report	IEEE std 1012-2004 Criticality Analysis work instruction

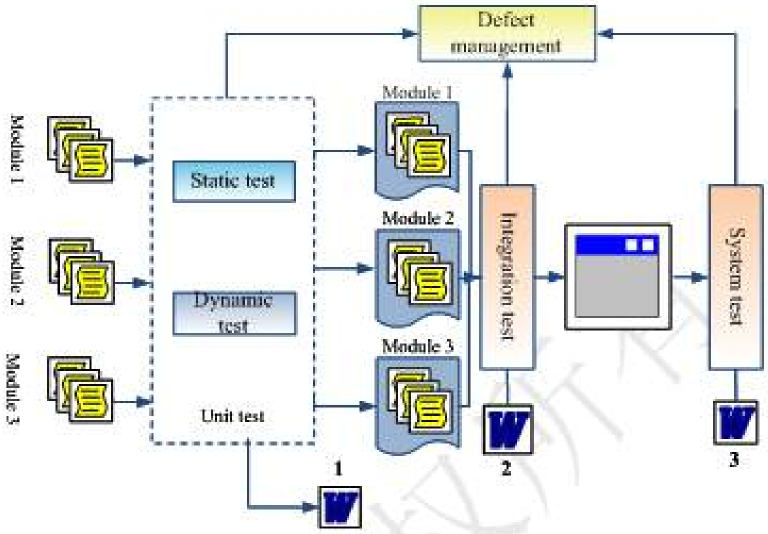
NicSys®8000N development process

Stage/ Management	Brief Process	Output Files	Work Instruction
Design	 Requirements review Architectural design phase System architectural design module design interface design 1 Architectural design Review 2 Detailed design phase Interface design Data structure design Interface design 3 Detailed design review 4 Implementation	1. NicSys8000 architectural design specification	Architectural design work instruction
		2. NicSys8000 architectural design review report NicSys8000 architectural design review comments form NicSys8000 architectural design phase V&V report	Architectural design review work instruction
		3. NicSys8000 detailed design specification	Detailed design work instruction
		4. NicSys8000 detailed design review report NicSys8000 detailed design review comments report NicSys8000 detailed design phase V&V report	Detailed design review work instruction
		5. NicSys8000 integration / unit test plan	Integration test work instruction Unit test work instruction
		6. NicSys8000 requirements tracking report	Requirements links work instruction
		7. NicSys8000 requirements tracking matrix	Requirements management work instruction Matrix tracking control procedures
		8. NicSys8000 design phase V&V summary report	
		9. NicSys8000 design specification review comments form	Anomaly management work instruction

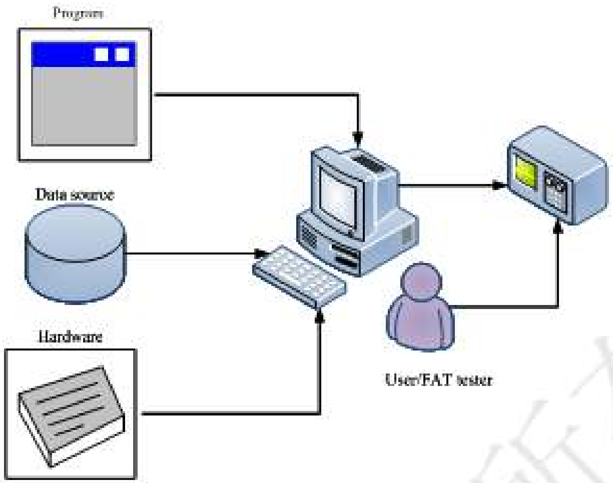
NicSys®8000N development process

Stage/ Management	Brief Process	Output Files	Work Instruction
Implementation		1. Source codes files	Encoding specification
		2. NicSys8000 development environment instruction manual	Development environment configuration instruction

NicSys®8000N development process

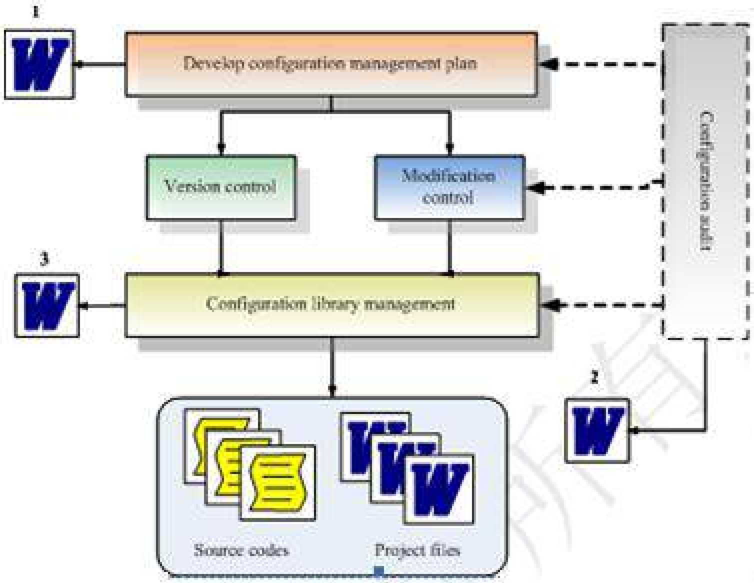
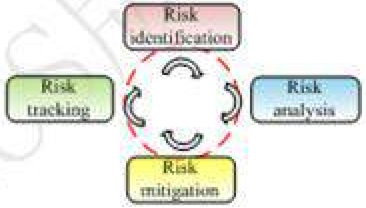
Stage/ Management	Brief Process	Output Files	Work Instruction
Testing	 Defect management Module 1 Module 2 Module 3 Static test Dynamic test Unit test Integration test System test 1 2 3	1. NicSys8000 unit test plan NicSys8000 unit test specification NicSys8000 unit test report	Test work instruction Anomaly management work instruction
		2. NicSys8000 integration test plan NicSys8000 integration test specification NicSys8000 integration test report	Anomaly management work instruction
		3. NicSys8000 system test plan NicSys8000 system test specification NicSys8000 system test report	Anomaly reporting control procedures
		4. NicSys8000 requirements tracking report	Requirements management work instruction
		5. NicSys8000 requirements tracking matrix	Matrix tracking control procedures
		6. NicSys8000 testing phase V&V summary report	

NicSys®8000N development process

Stage/ Management	Brief Process	Output Files	Work Instruction
Factory Acceptance		1. NicSys8000 version release plan NicSys8000 version release specification	Version release work instruction
		2. NicSys8000 factory acceptance test plan NicSys8000 factory acceptance test specification NicSys8000 factory acceptance test report	Factory acceptance test work instruction
		3. NicSys8000 instruction manual NicSys8000 user manual	User documentation Guidance
		4. NicSys8000 development summary report	
		5. NicSys8000 V&V summary report	

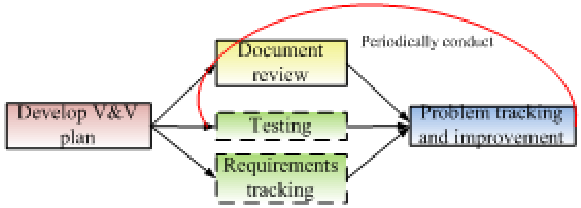
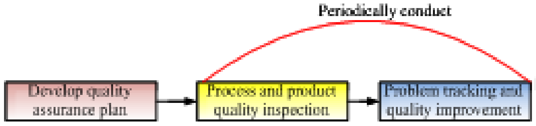
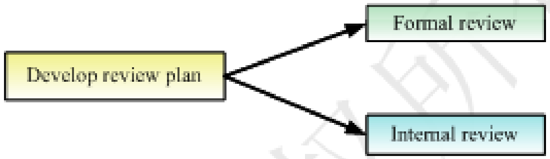
权所有，

NicSys®8000N development process

Stage/ Management	Brief Process	Output Files	Work Instruction
Configuration management	 1 Develop configuration management plan Version control Modification control 3 Configuration library management Configuration audit 2 Source codes Project files	1. NicSys8000 configuration management plan	IEEE std 828-1998 Version control work instruction
		2. NicSys8000 configuration audit report	Configuration management review work instruction
		3. NicSys8000 configuration status report	
Risk management	 Risk identification Risk tracking Risk analysis Risk mitigation	1. Project risk management report	Project risk management work instruction IEEE std 1540-2001
		2. Project risk check list	

CNCS版权所有 严禁复制

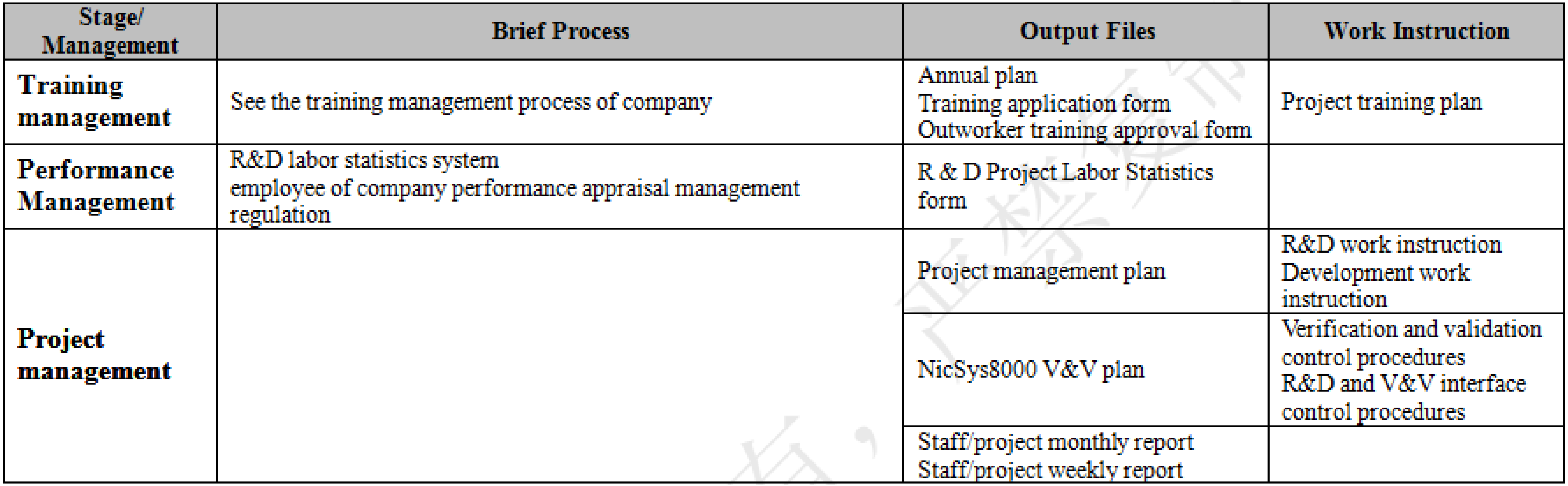
NicSys®8000N development process

Stage/ Management	Brief Process	Output Files	Work Instruction
V&V management	 Develop V&V plan Document review Testing Requirements tracking Problem tracking and improvement Periodically conduct	See the output files completed during the various stages of V&V process	IEEE 1012 V&V Std 2004 Verification and validation control procedures
Quality assurance	 Develop quality assurance plan Process and product quality inspection Problem tracking and quality improvement Periodically conduct	1. NicSys8000 quality assurance plan 2. NicSys8000 quality assurance report	IEEE Std 730-1998 Quality assurance work instruction
Review management	 Develop review plan Formal review Internal review	1. NicSys8000 design review application form 2. NicSys8000 design review report	IEEE Std 1028-1997 Design review and verification control procedures
File management	See the file management process of company	1. File approval form 2. Valid file inventory 3. File review comments form 4. File modification record	File control procedures
Procurement management	See the procurement management process of company	Procurement application form	Procurement control procedures

CNCS版权所有，严禁复制

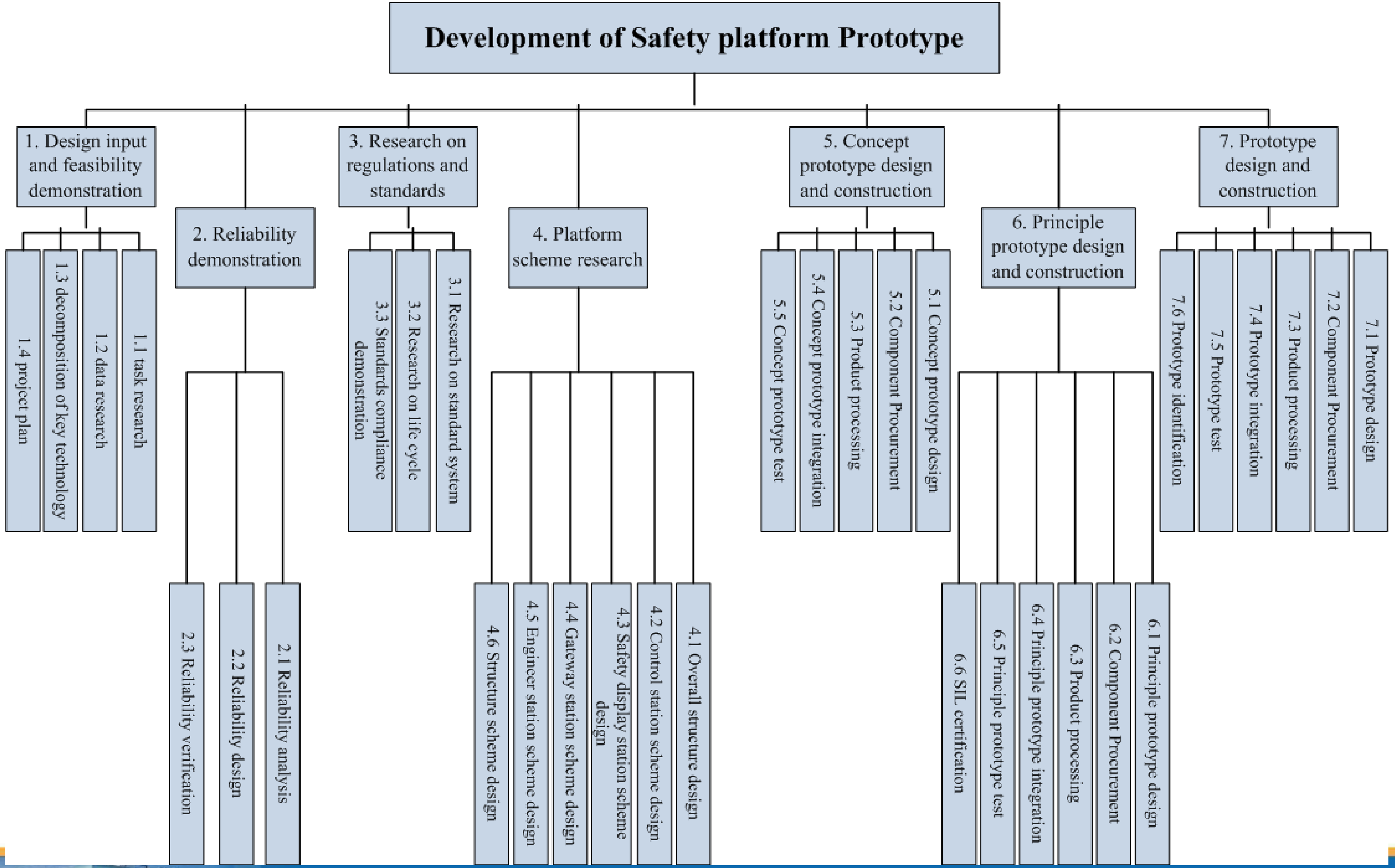
CNCS

NicSys®8000N development process



Stage/ Management	Brief Process	Output Files	Work Instruction
Training management	See the training management process of company	Annual plan Training application form Outworker training approval form	Project training plan
Performance Management	R&D labor statistics system employee of company performance appraisal management regulation	R & D Project Labor Statistics form	
Project management		Project management plan	R&D work instruction Development work instruction
		NicSys8000 V&V plan	Verification and validation control procedures R&D and V&V interface control procedures
		Staff/project monthly report Staff/project weekly report	

NicSys®8000N WBS



Development of Safety platform Prototype

- 1. Design input and feasibility demonstration
  - 1.1 task research
  - 1.2 data research
  - 1.3 decomposition of key technology
  - 1.4 project plan
- 2. Reliability demonstration
  - 2.1 Reliability analysis
  - 2.2 Reliability design
  - 2.3 Reliability verification
- 3. Research on regulations and standards
  - 3.1 Research on standard system
  - 3.2 Research on life cycle
  - 3.3 Standards compliance demonstration
- 4. Platform scheme research
  - 4.1 Overall structure design
  - 4.2 Control station scheme design
  - 4.3 Safety display station scheme design
  - 4.4 Gateway station scheme design
  - 4.5 Engineer station scheme design
  - 4.6 Structure scheme design
- 5. Concept prototype design and construction
  - 5.1 Concept prototype design
  - 5.2 Component Procurement
  - 5.3 Product processing
  - 5.4 Concept prototype integration
  - 5.5 Concept prototype test
- 6. Principle prototype design and construction
  - 6.1 Principle prototype design
  - 6.2 Component Procurement
  - 6.3 Product processing
  - 6.4 Principle prototype integration
  - 6.5 Principle prototype test
  - 6.6 SIL certification
- 7. Prototype design and construction
  - 7.1 Prototype design
  - 7.2 Component Procurement
  - 7.3 Product processing
  - 7.4 Prototype integration
  - 7.5 Prototype test
  - 7.6 Prototype identification

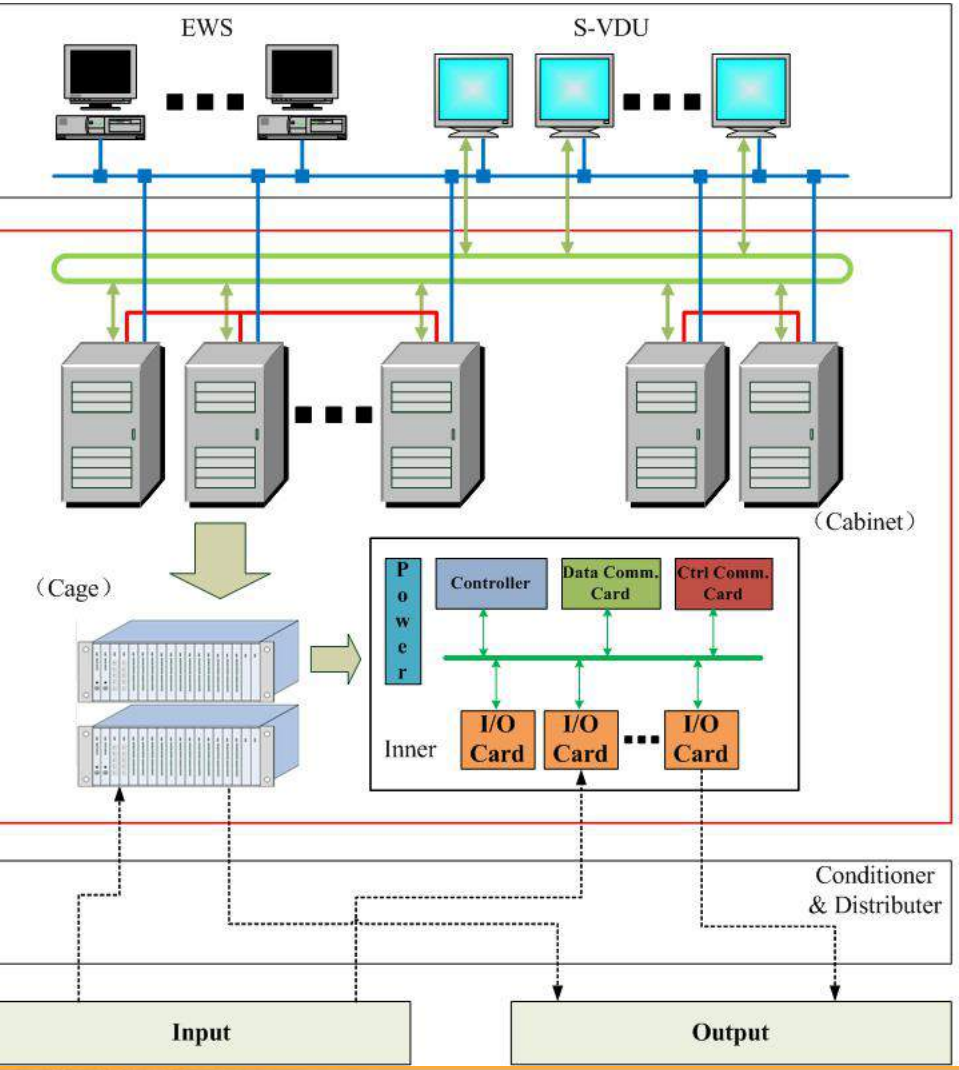
NicSys®8000N CTEs

NO.	Critical Technology Elements
1	Reliability design technology of safety product life cycle
2	The design and verification technology of the safety control station based on FPGA Technology
3	Safety field bus, point-to-point communication and multi-point communication, meet the requirements of safety level communication
4	Configuration software and verification technology based on graphical safety algorithm
5	Safety construction seismic analysis and design technology
6	Safety display unit (safety information display and device control technology)

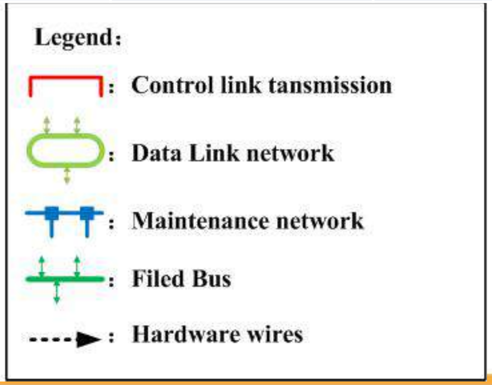
NicSys®8000N System overview

- The NicSys®8000N platform is a hardware-based architecture that uses a minimal set of hardware to implement a system with high reliability and integrity. The system incorporates self-test capability for detection and mitigation of the effects of failures within or external to the system.
- The key component in the NicSys®8000N platform design is a field-programmable gate array (FPGA). The PFGA programmable logic components can be programmed to duplicate the functionality of basic logic gates (such as AND, OR, XOR and NOT). These logic components can be combined into more complex combinational functions such as decoders or math functions.
- The development of the NicSys®8000N platform complies with the national nuclear safety regulations and industry standards. The system have most excellent RAMS features.
- The platform can be applied to many types of nuclear I&C system in NPPs, such as RPS, ESFAS and PAMS.

Platform Structure



Unit	Item	Description
Control unit	Cabinet	For carrying cage and other accessories
	Cage	For carrying all sorts of function modules
	Controller	Execution of the protection logic
	I/O Cards	Input and output function
	Communication Cards	Transmission of exchanged information
	Power Cards	Power supply for all function modules
S-VDU	S-VDU Device	HMI interface for platform display and operation
EWS software tools	Project management	For all project application management
	Configuration tool	Equipment, variable, algorithm, graphics configuration and check
	Debugging and simulation tools	The debugging and simulation of application logic and algorithm
	Compile tools	Translation application logic into the FPGA bin file
	Download tools	For download FPGA bin file into Controllers
	Maintenance tools	Variables monitoring and mandatory, parameter setting



Performance parameters

System capacity	
IO capacity	≥ 1200 digital input/output per channel ≥ 480 analog input/output per channel
Net capacity	≥ 10 control link nodes per chassis ≥ 2 data link nodes per chassis

System accuracy	
Analog input	≤ 0.1%(full scale)
Analog output	≤ 0.1%(full scale)

Processing cycle	
FPGA cycle	≤20ms
Communication cycle	≤20ms

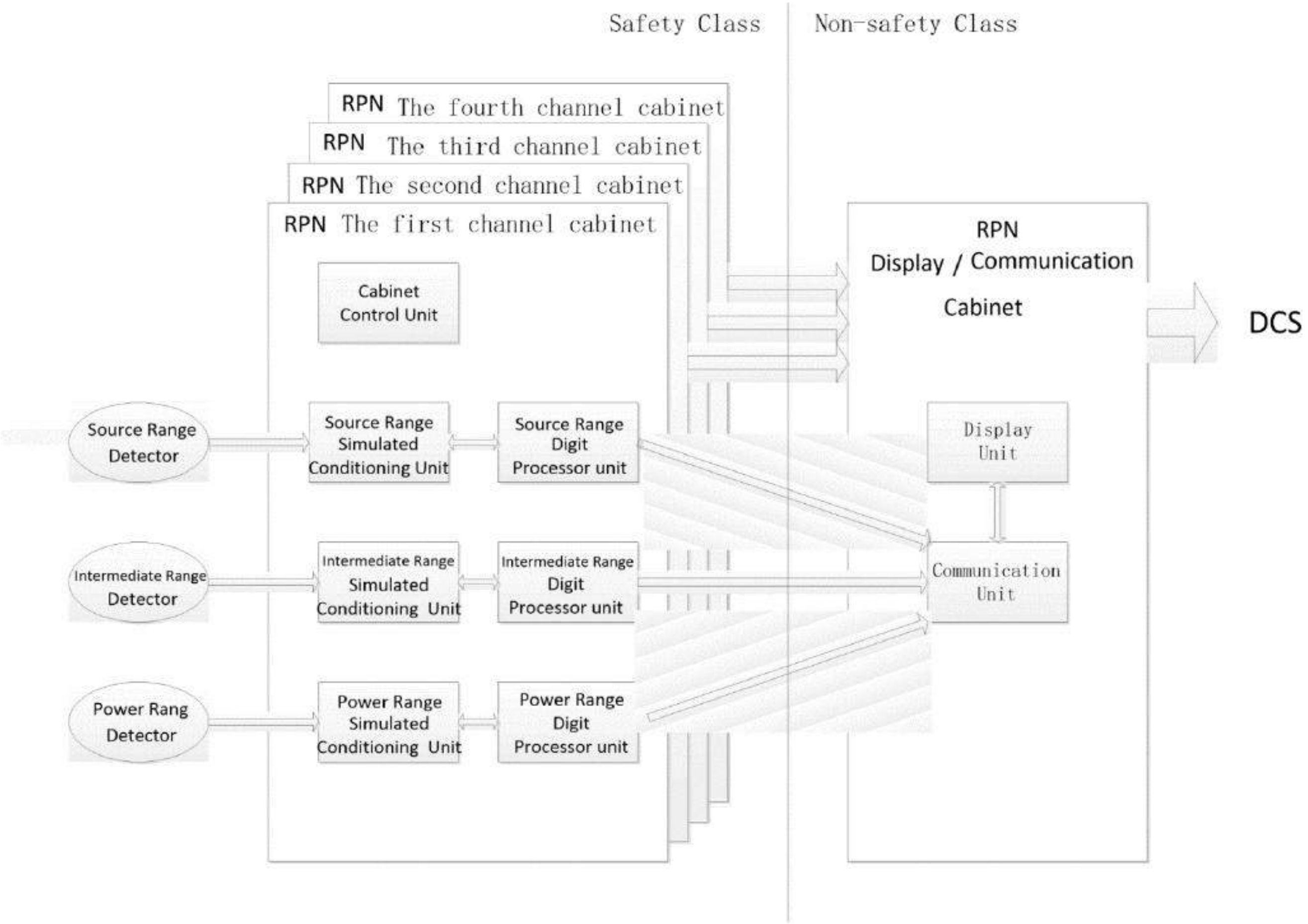
RAMS	
Reliability	anti-operation probability ≤ 10^{-7}； spurious initiating of reactor trip ≤ 0.1 time/year
Availability	≥ 99.99%
Maintainability	MTBF ≥ 10 years； MTTR ≤ 4hours
Safety	diagnostic coverage rate ≥ 99%

NicSys®8000N Prototype for Typical Safety Application

- RTS
- ESFAS
- PAMS
- RPN
- DGLS
- DPS

RPN system features based on NicSys ® 8000N

- ➢Three types, a total of 12 kinds of nuclear detector signal collecting, computing and processing
- ➢Quick response (< 100 ms)
- ➢Quad redundant channels design
- ➢Communicate with NC - DCS, display shutdown alarm signal
- ➢Support periodic test


Safety Class
Non-safety Class
RPN The fourth channel cabinet
RPN The third channel cabinet
RPN The second channel cabinet
RPN The first channel cabinet
Cabinet Control Unit
Source Range Detector
Source Range Simulated Conditioning Unit
Source Range Digit Processor unit
Intermediate Range Detector
Intermediate Range Simulated Conditioning Unit
Intermediate Range Digit Processor unit
Power Rang Detector
Power Range Simulated Conditioning Unit
Power Range Digit Processor unit
RPN Display / Communication Cabinet
Display Unit
Communication Unit
DCS

RPN System

Security functions performed by NicSys ® 8000N platform:

●Signal collection

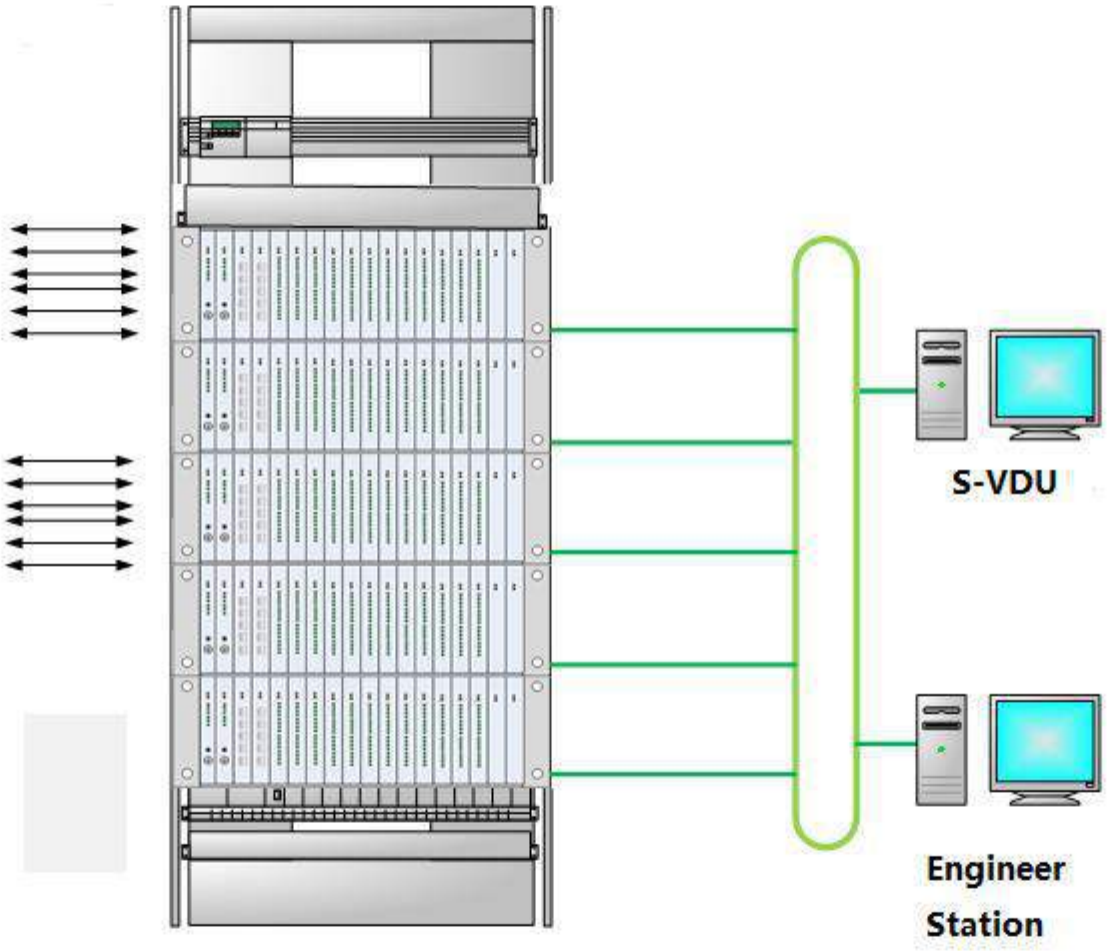
●Field signal rapid processing

●Safety shutdown logic computing

●Safety display

●Communicate with NC

●Periodic test



NicSys®8000N milestone

Year	Plan
2014	Complete Concept prototype
2015	Complete RPN verification prototype
2017	Complete safety control system verification prototype, including reactor protection system and engineering safety features actuation system
2019	NicSys®8000N release
2020	Implementation in the C5 project

THANKS!