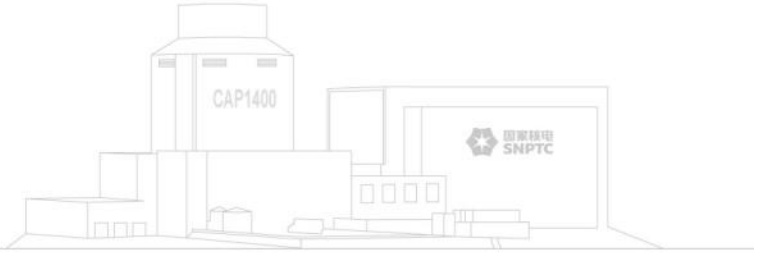
RAVONSICS-Challenging for Assuring Software Reliability of Nuclear I&C System

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

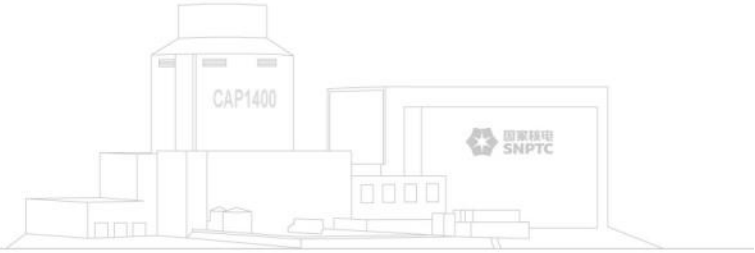
国家核电 SNPTC 国核自仪系统工程有限公司
STATE NUCLEAR POWER AUTOMATION SYSTEM ENGINEERING COMPANY

Content



RAVONSICS- Reliability And V&v Of Nuclear Safety I&C Software

Content



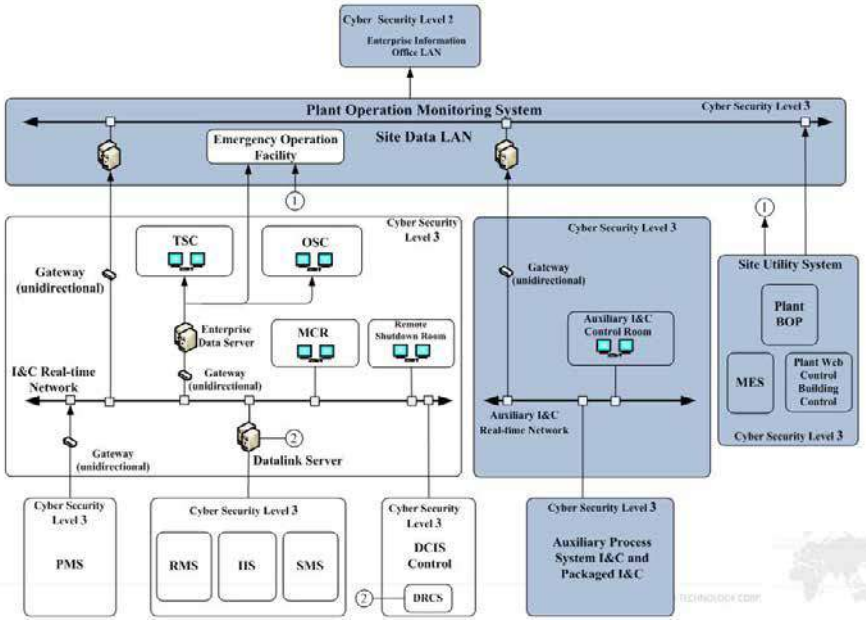
1. Background

China Nuclear Power Development Plan— 45 existing and under-construction Units, and 17 Units approved for preparatory work

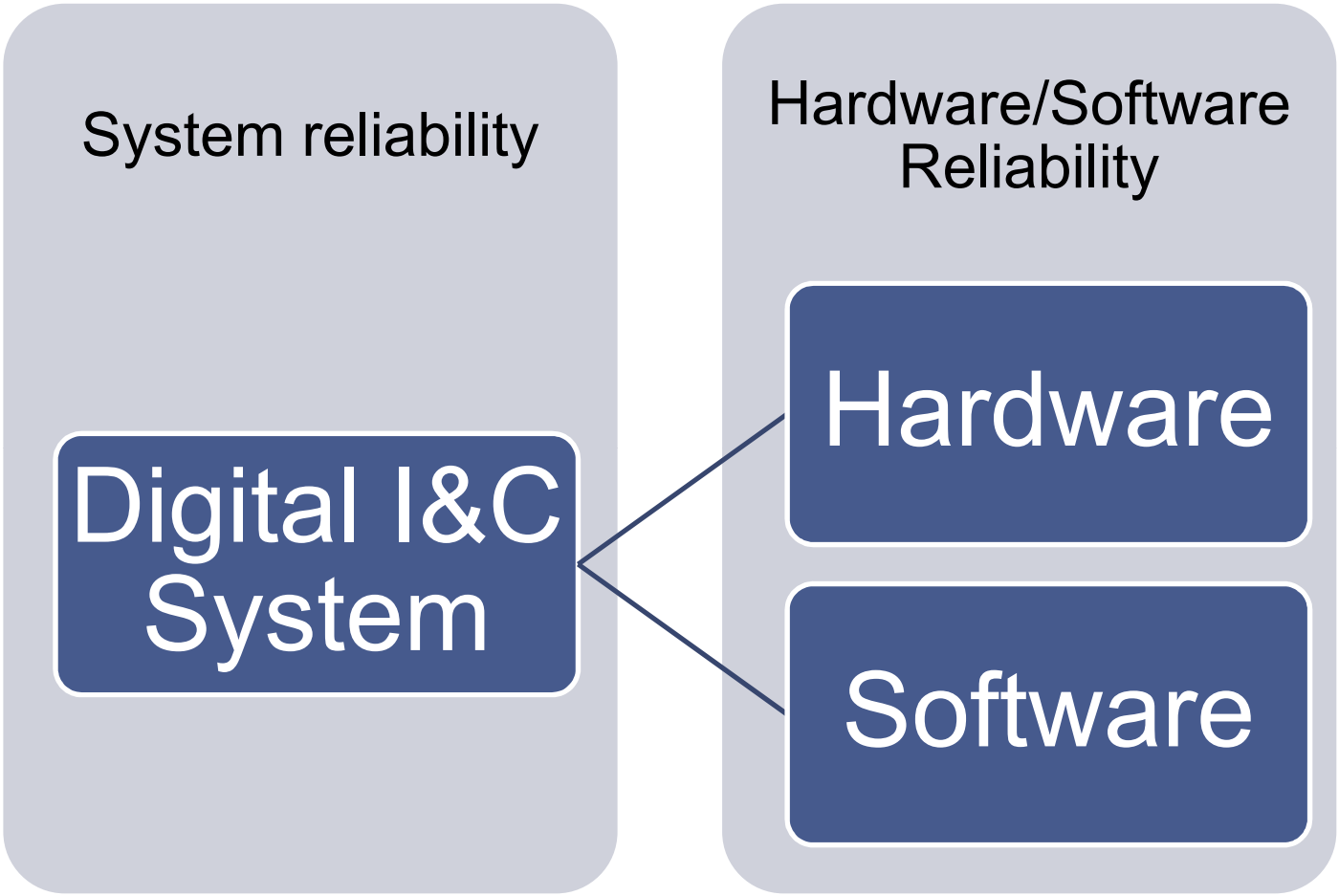
TABLE 8. APPROVED PREPARATORY WORK FOR NNP CONSTRUCTION

Project Name	Model	Installed Capacity (MW)	Expected Const. Year	Expected Operate Year
Approved NNP Const.				
YANGJIANG UNIT 5	ACPR1000	1086	2013	2018
YANGJIANG UNIT 6	ACPR1000	1086	2014	2019
TIANWAN UNIT 4	VVER1000	1060	2013	——
Approved Preparatory Work For NNP Const.				
HAIYANG UNIT 3				
HAIYANG UNIT 4				
TIANWAN UNIT 5				
TIANWAN UNIT 6				
XUDABAO UNIT 1				
XUDABAO UNIT 2				
LUFENG UNIT 1				
LUFENG UNIT 2				
HONGYANHE UNIT 5				
HONGYANHE UNIT 6				
FUQING UNIT 5				
FUQING UNIT 6				
SANMEN UNIT 3				
SANMEN UNIT 4				

-- Country Nuclear Power Profiles, 2014 Edition, IAEA



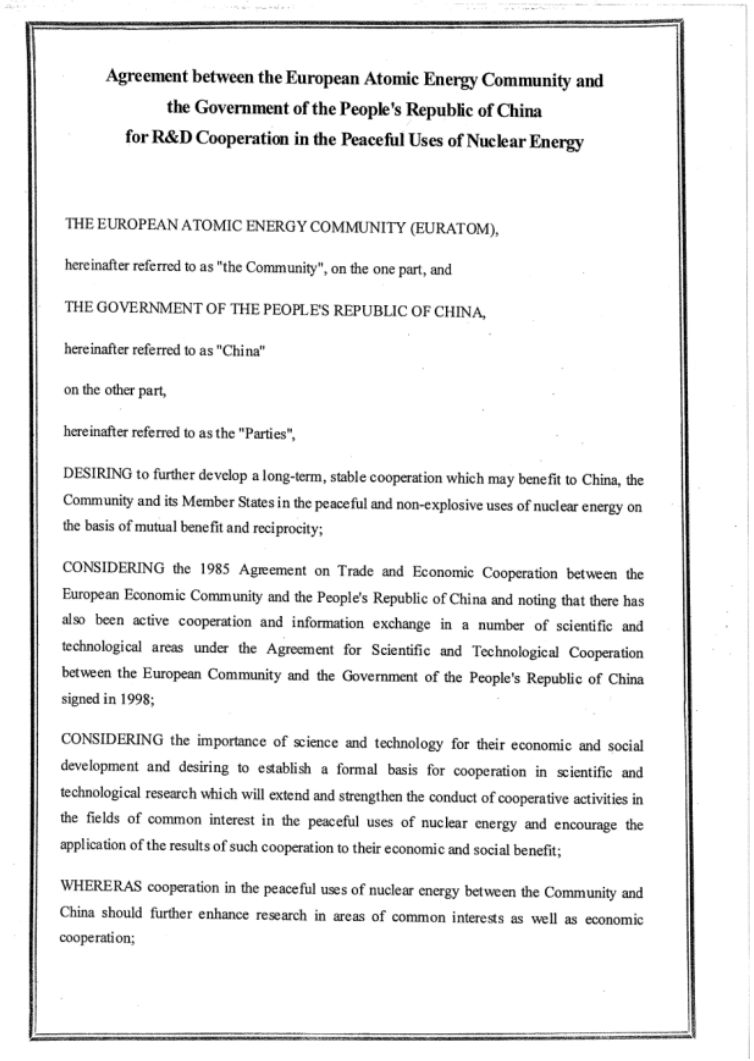
Digital I&C systems are widely applied in new and existing Units.



The characteristic of an item expressed by the probability that it will perform a required function under stated conditions for a stated time.—IEEE 577

The ability of a program to perform a required function under stated conditions for a stated period of time. –IEEE 1633

1. Background



Agreement between the European Atomic Energy Community and the Government of the People's Republic of China for R&D Cooperation in the Peaceful Uses of Nuclear Energy

THE EUROPEAN ATOMIC ENERGY COMMUNITY (EURATOM),

hereinafter referred to as "the Community", on the one part, and

THE GOVERNMENT OF THE PEOPLE'S REPUBLIC OF CHINA,

hereinafter referred to as "China"

on the other part,

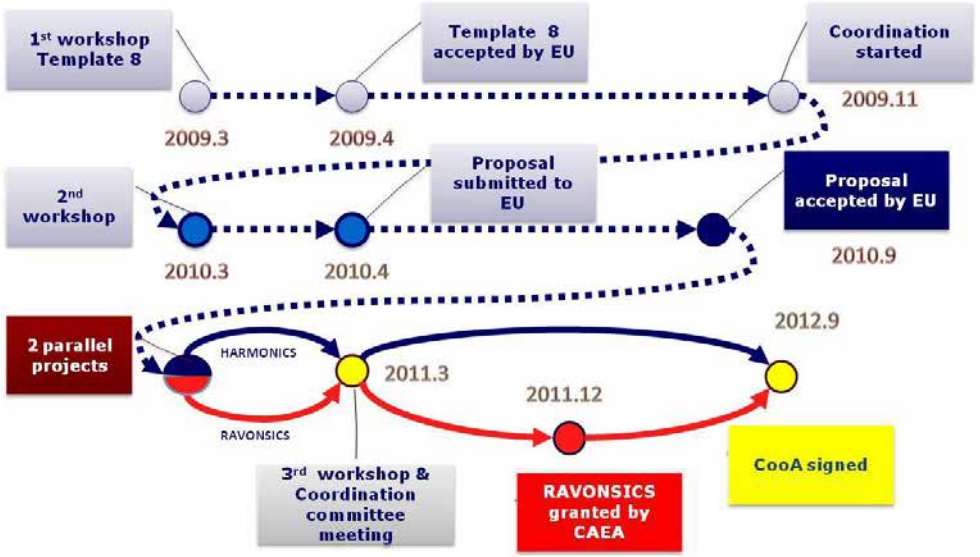
hereinafter referred to as the "Parties",

DESIRING to further develop a long-term, stable cooperation which may benefit to China, the Community and its Member States in the peaceful and non-explosive uses of nuclear energy on the basis of mutual benefit and reciprocity;

CONSIDERING the 1985 Agreement on Trade and Economic Cooperation between the European Economic Community and the People's Republic of China and noting that there has also been active cooperation and information exchange in a number of scientific and technological areas under the Agreement for Scientific and Technological Cooperation between the European Community and the Government of the People's Republic of China signed in 1998;

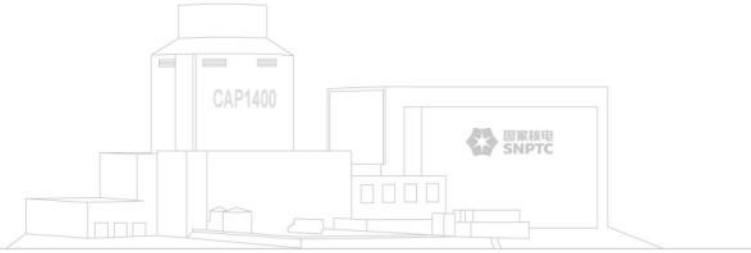
CONSIDERING the importance of science and technology for their economic and social development and desiring to establish a formal basis for cooperation in scientific and technological research which will extend and strengthen the conduct of cooperative activities in the fields of common interest in the peaceful uses of nuclear energy and encourage the application of the results of such cooperation to their economic and social benefit;

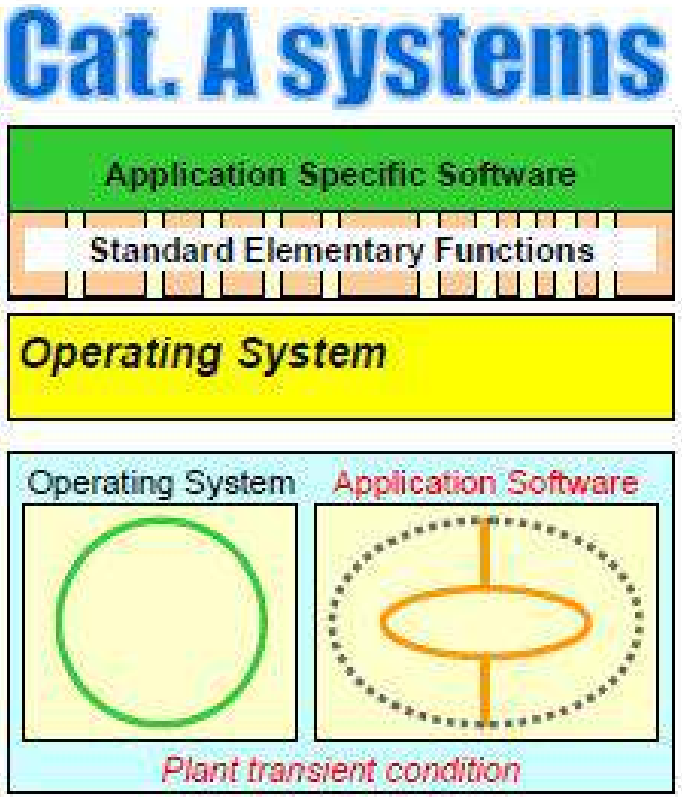
WHERERAS cooperation in the peaceful uses of nuclear energy between the Community and China should further enhance research in areas of common interests as well as economic cooperation;



RAVONSICS- Reliability and Verification and Validation of Nuclear Safety I&C software

Content





(-- Jan-Erik Holmberg, VTT)

Assessment of software reliability

Verification

Safety justification

Assessment of Software Reliability

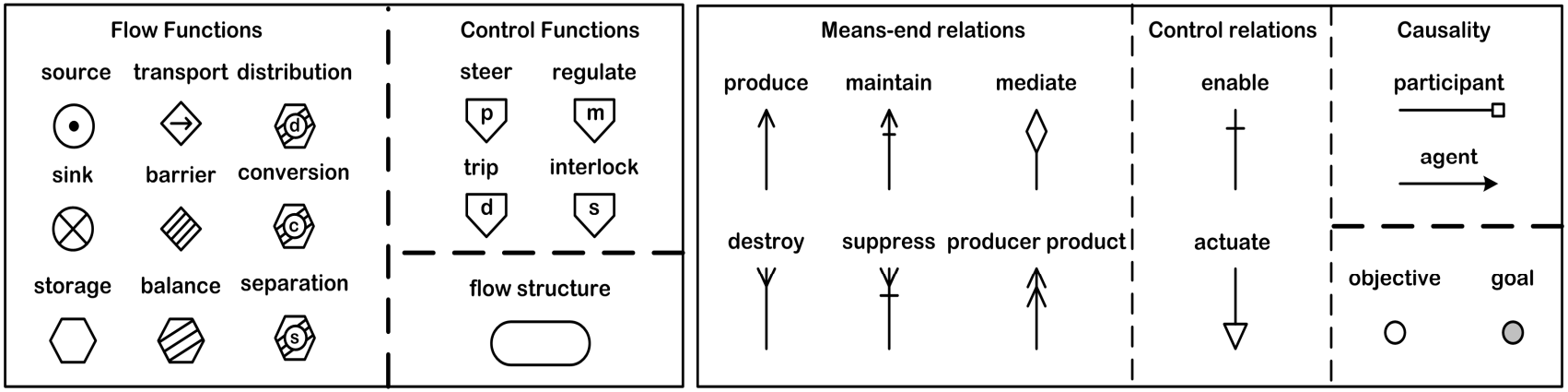
Multi-layer Flow Model(MFM)

Hierarchical Structure Model(HSM)

Bayesian Network

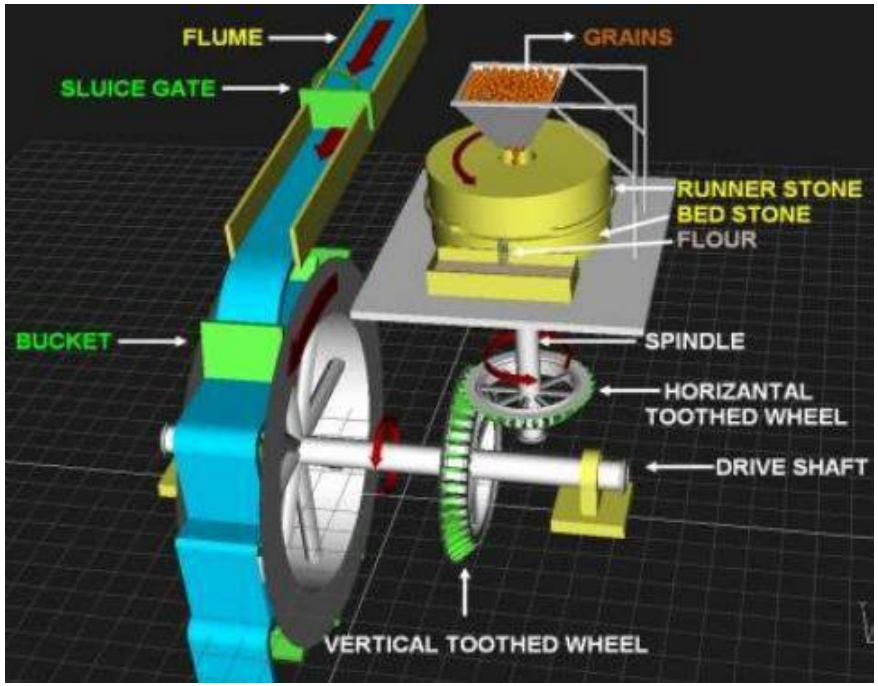
Assessment of Software Reliability
--MFM

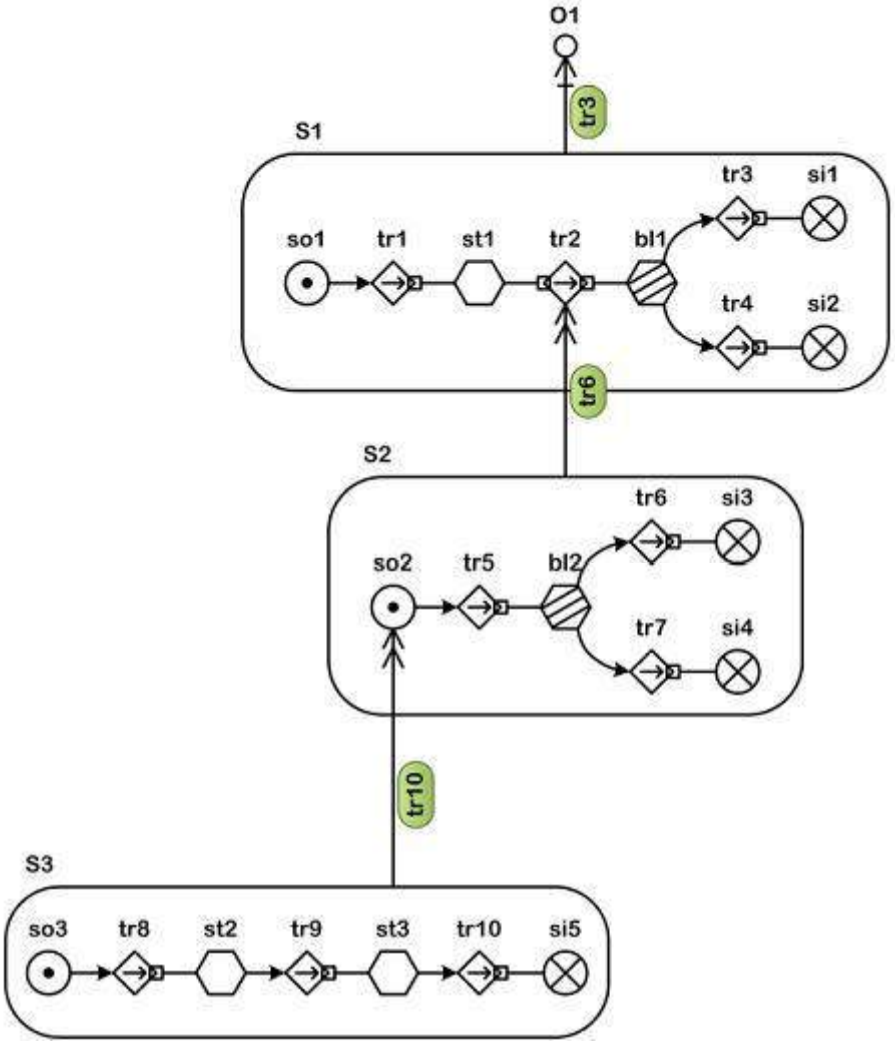
- MFM is a goal oriented functional modeling methodology invented by Professor Morten Lind in 1980s;
- Modeling the system by analyzing the actual mass flow, energy flow and information flow, that is easy to understand.



Graphical symbols of MFM—Lind, Morten

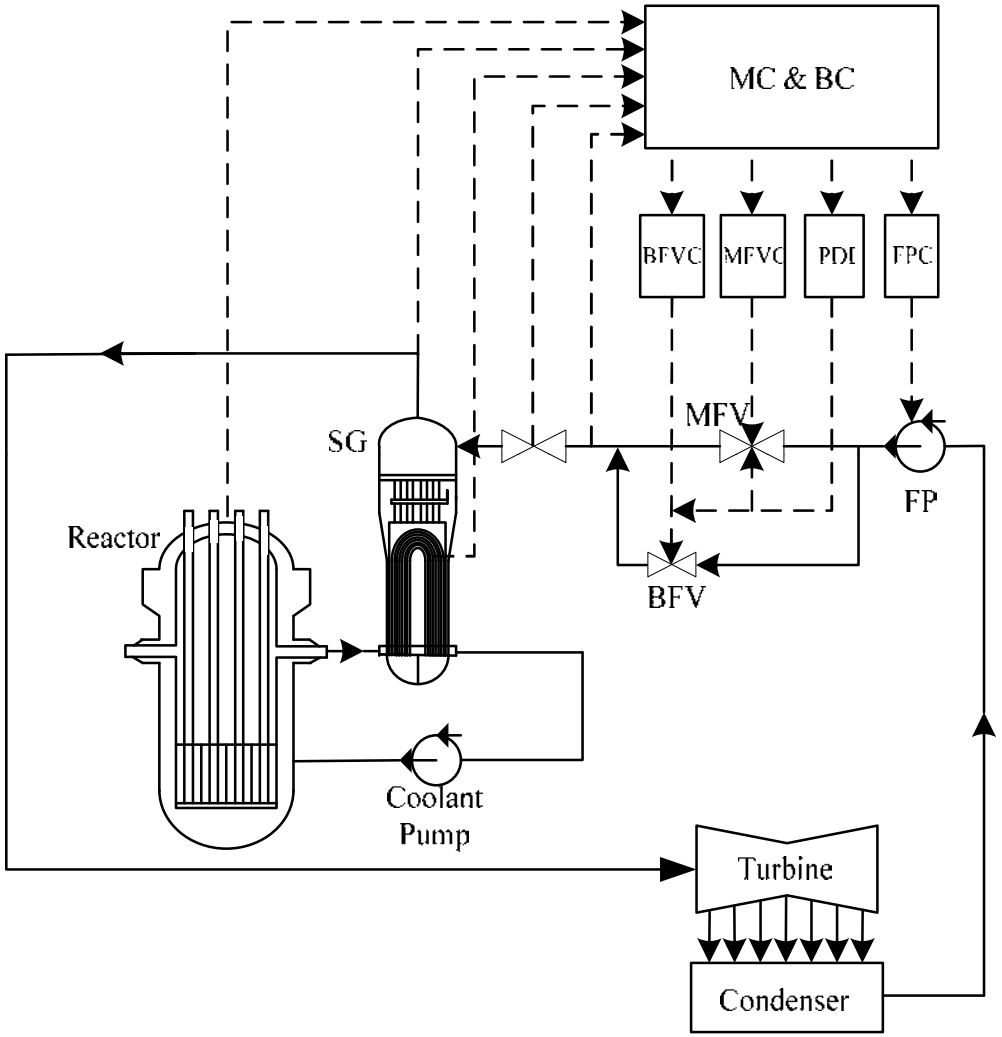
Assessment of Software Reliability
--MFM





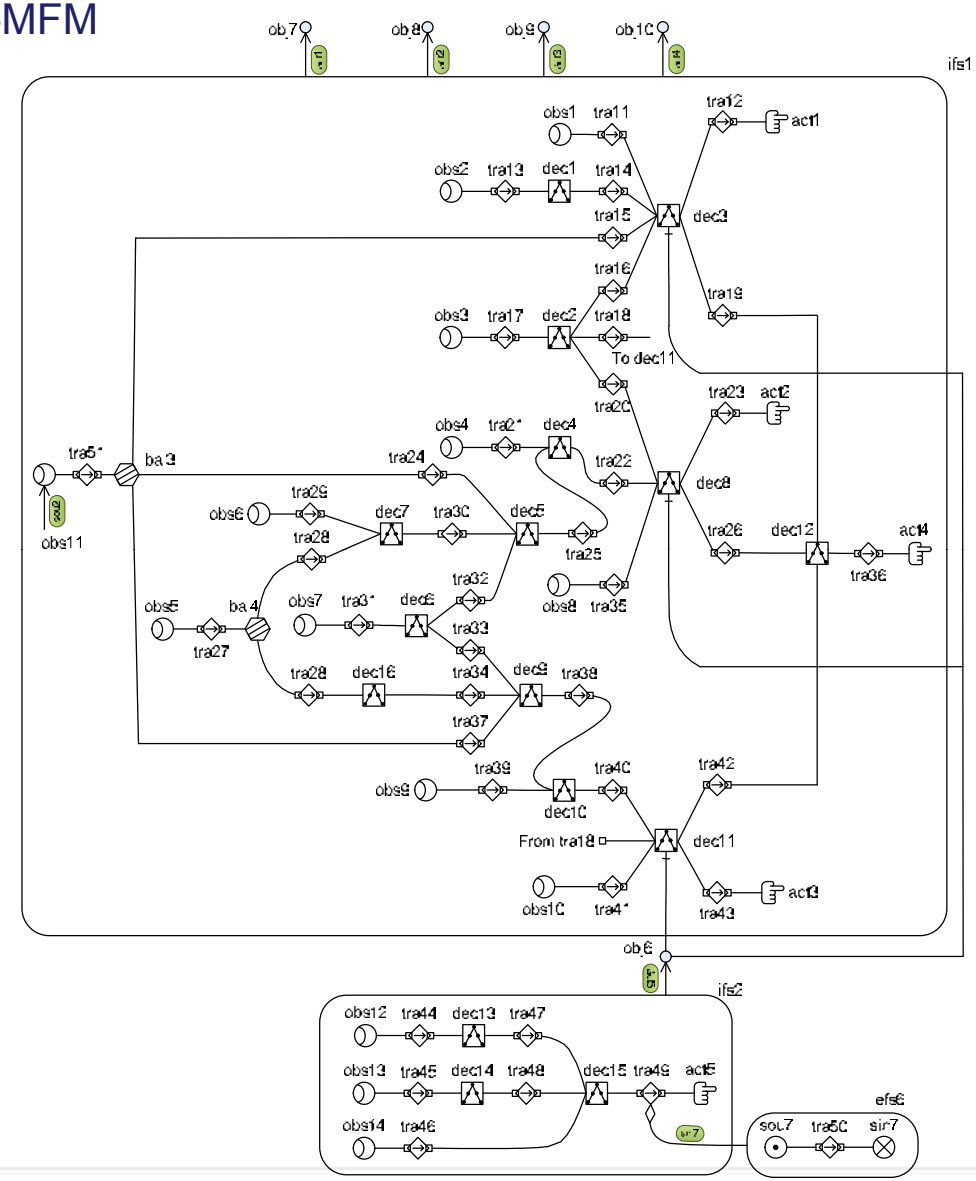
—Lind, Morten

Assessment of Software Reliability
--MFM



2. Research Topic

Assessment of Software Reliability --MFM



ifs1: information flow of controllers for describing the data collection and processing, and generating control signals

ifs2: information flow of computers for describing the information management of computers

efs6: energy flow of computers

Functions are grouped into flow structures at different levels to realize goals.
Flow structures are connected through relations.

By this way, the functions of a digital control system can be clearly understood.

MFM of Main Steam System with Process Control—Ming Yang, HEU

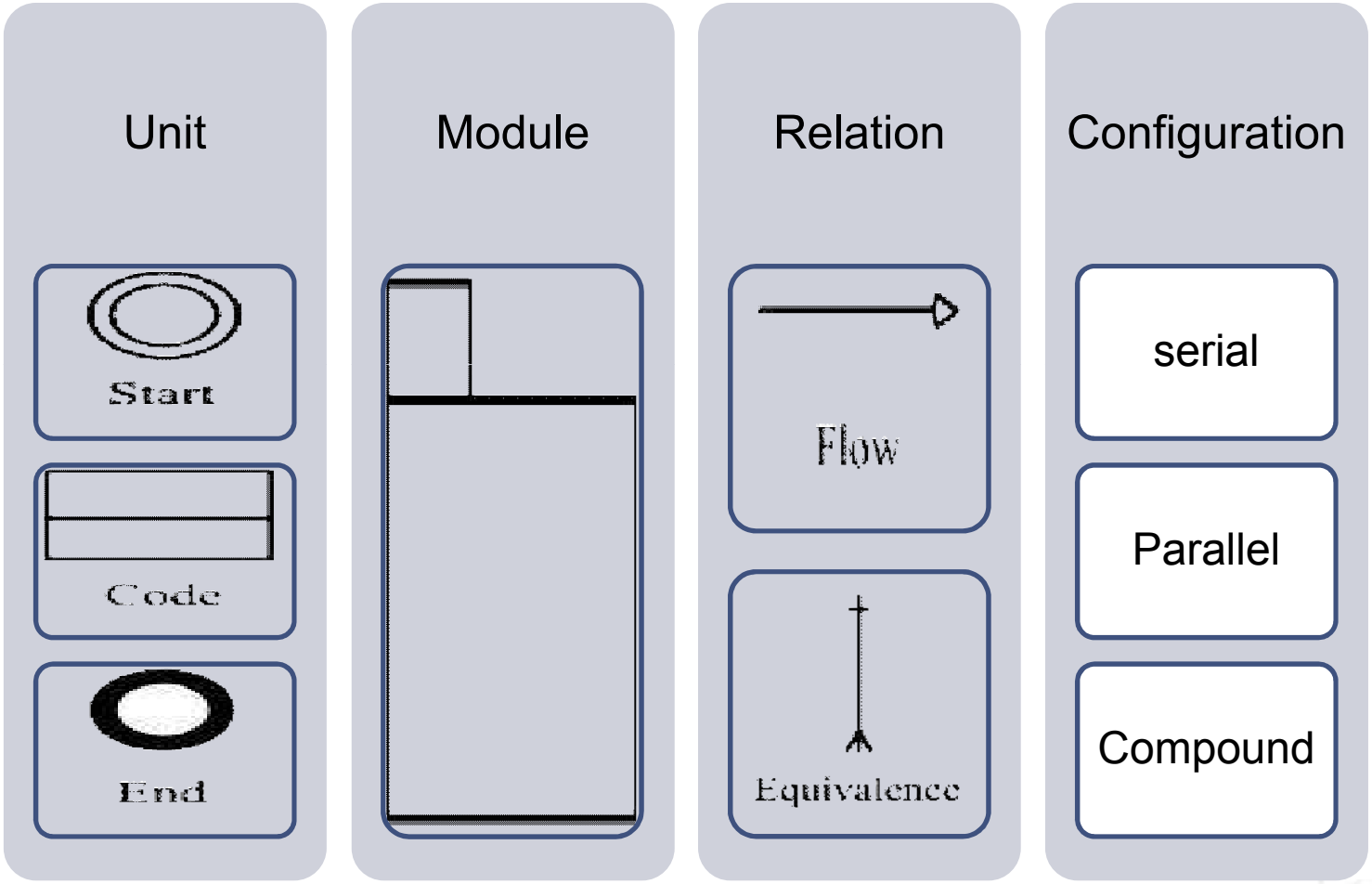
Assessment of Software Reliability
--HSM

■HSM is a model of the software structure. The basic idea of HSM is from MFM and Flow Network Model (FNM). Different with FNM, the software structure is organized at different layers of abstraction which enables an easy and step-by-step model extension.

■Modeling Elements of HSM

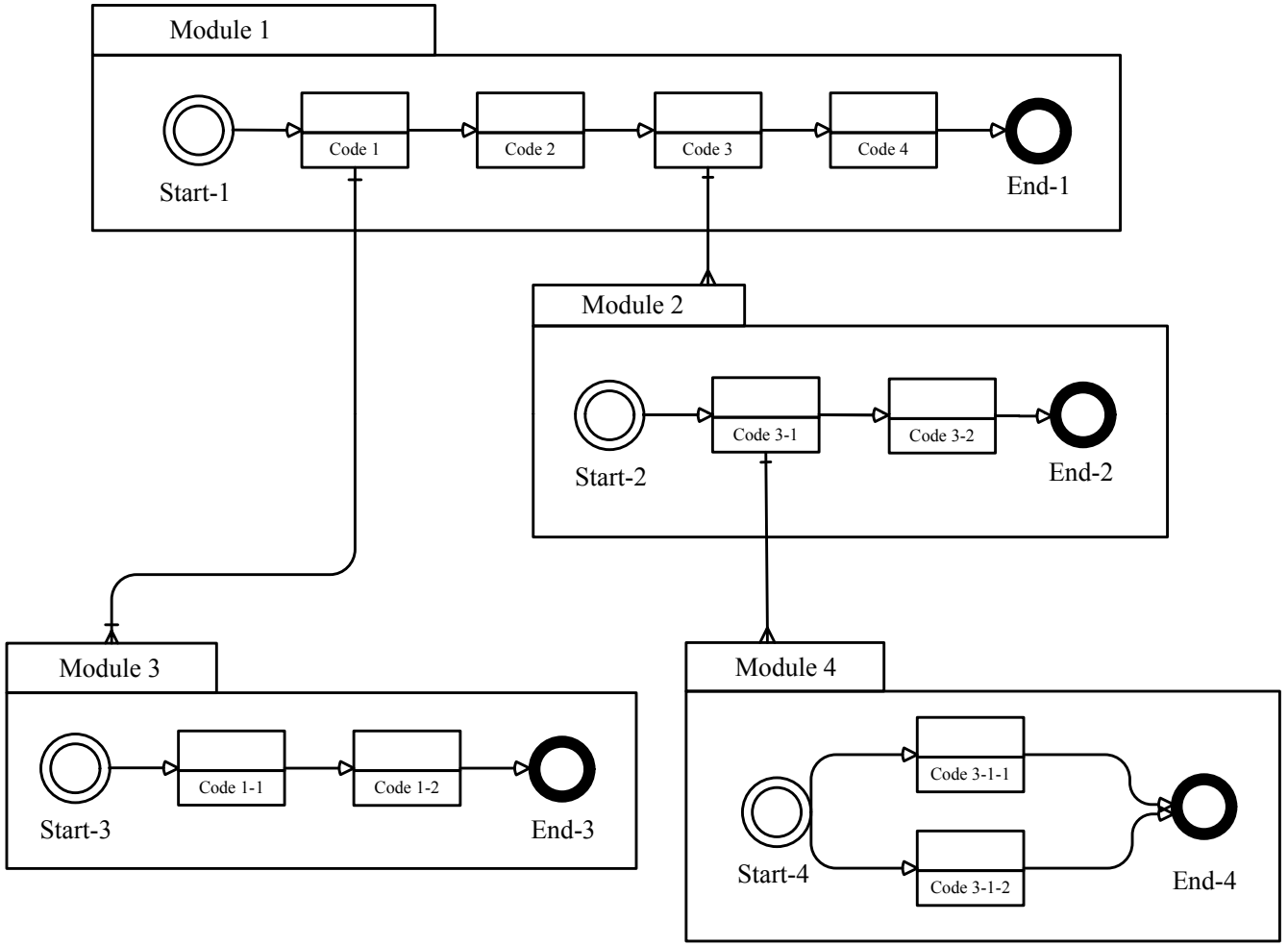
- **Unit**
- **Module**
- **Relation**
- **Configuration**

Assessment of Software Reliability
--HSM

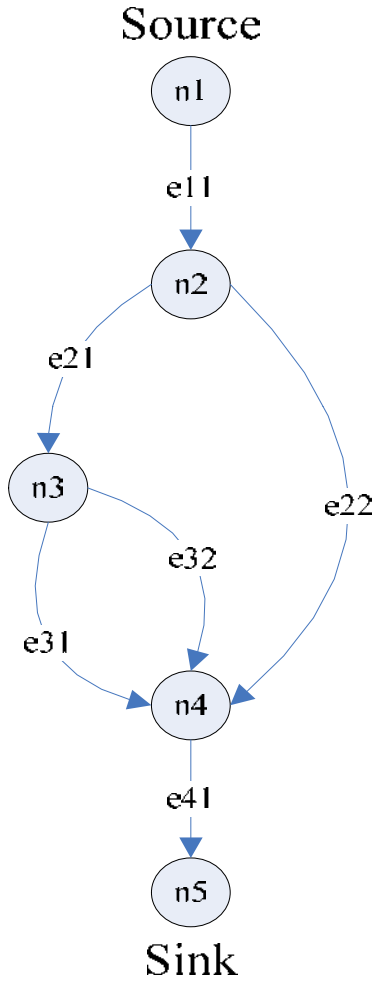


2. Research Topic

Assessment of Software Reliability
--HSM



Assessment of Software Reliability
--HSM



$$q_i = 10^{-m_i}$$

$$q_i = 10^{-h_i m_i}$$

$$r_i = 1 - q_i = 1 - 10^{-h_i m_i}$$

Serial Configuration

$$r_{S_C} = \prod_{i=1}^{n} r_i$$

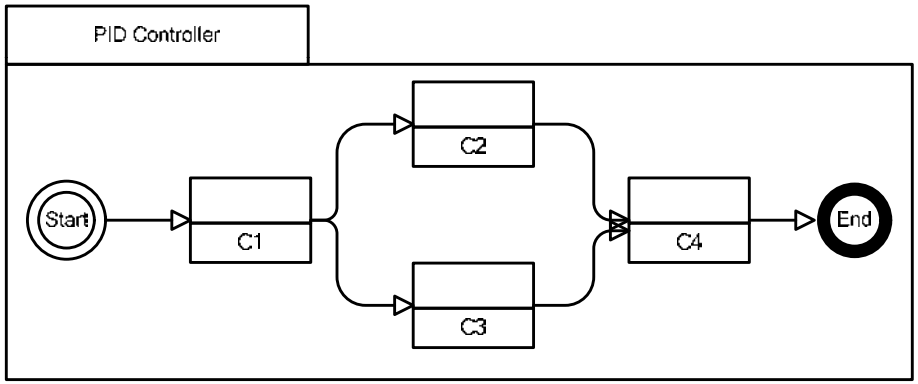
Parallel Configuration

$$r'_{p_C} = \sum_{i=1}^{n} \frac{T_{C_i} h_i}{T'_{P_C}} r_i$$

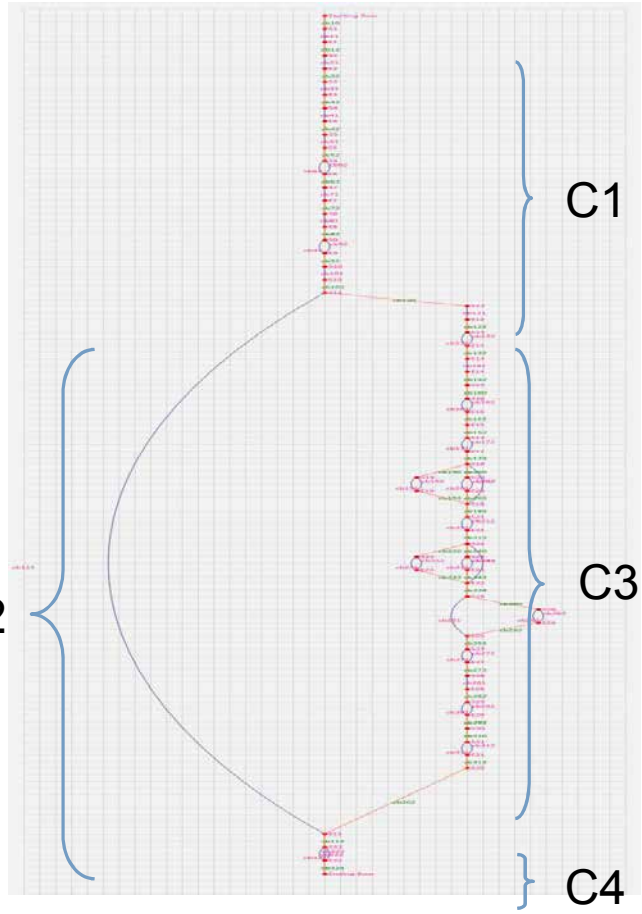
Assessment of Software Reliability
--HSM

PID Controller

- 186 lines
- FORTRAN code
- m_i =1.q_i=0.9
- 115,212 routes

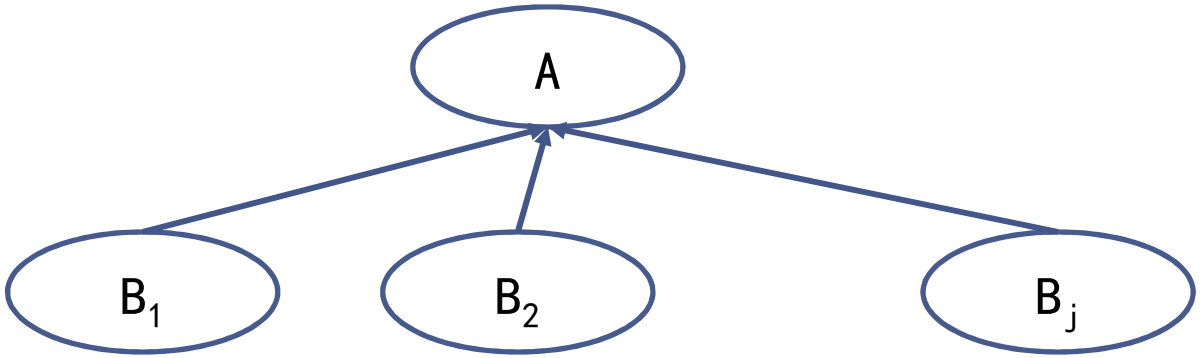


HSM Model



q_i= 0.9989976 after 5 tests
Failure probability will be 1E-6 after 30 tests.

Assessment of Software Reliability
--Bayesian Network



$$P(A) = \sum_{j=1}^{n} P(B_j)P(A|B_j)$$

Prior Probability $P(B_j)$ is gained by expert judgment.

Conditional Probability $P(A|B_j)$ is gained by Analytic Hierarchy Process.

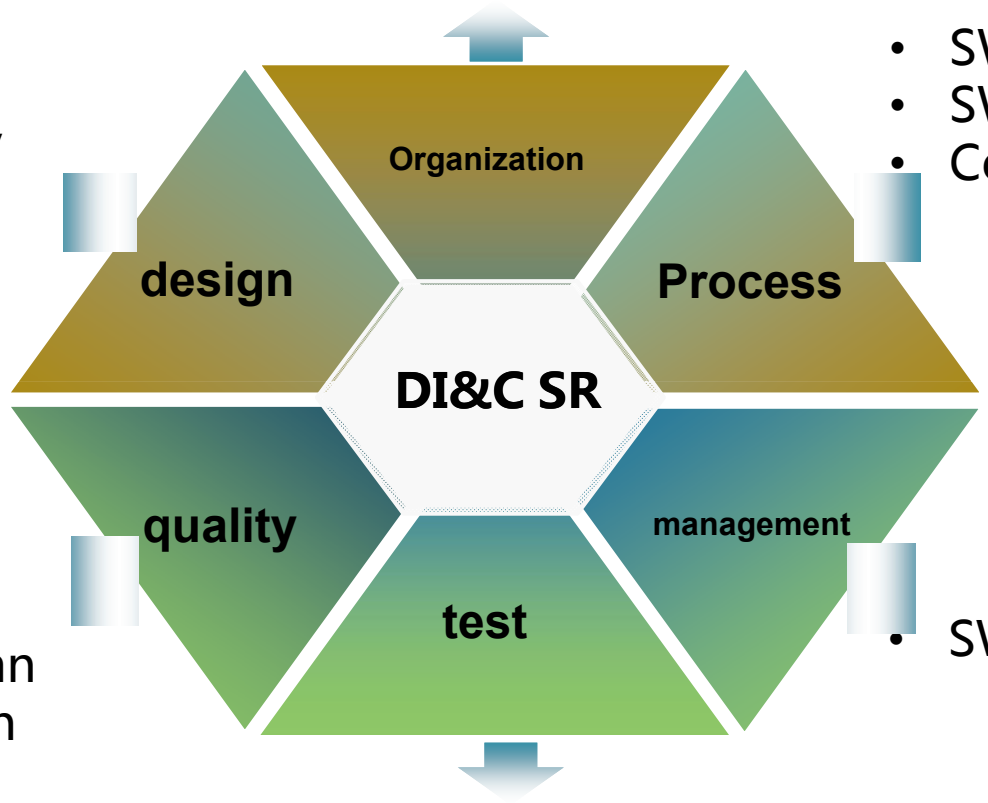
2. Research Topic

Assessment of Software Reliability
--Bayesian Network

- SW PM evaluation

- SW DRS
- SW DRS safety

- SW DDS
- SW PDP
- Code analysis

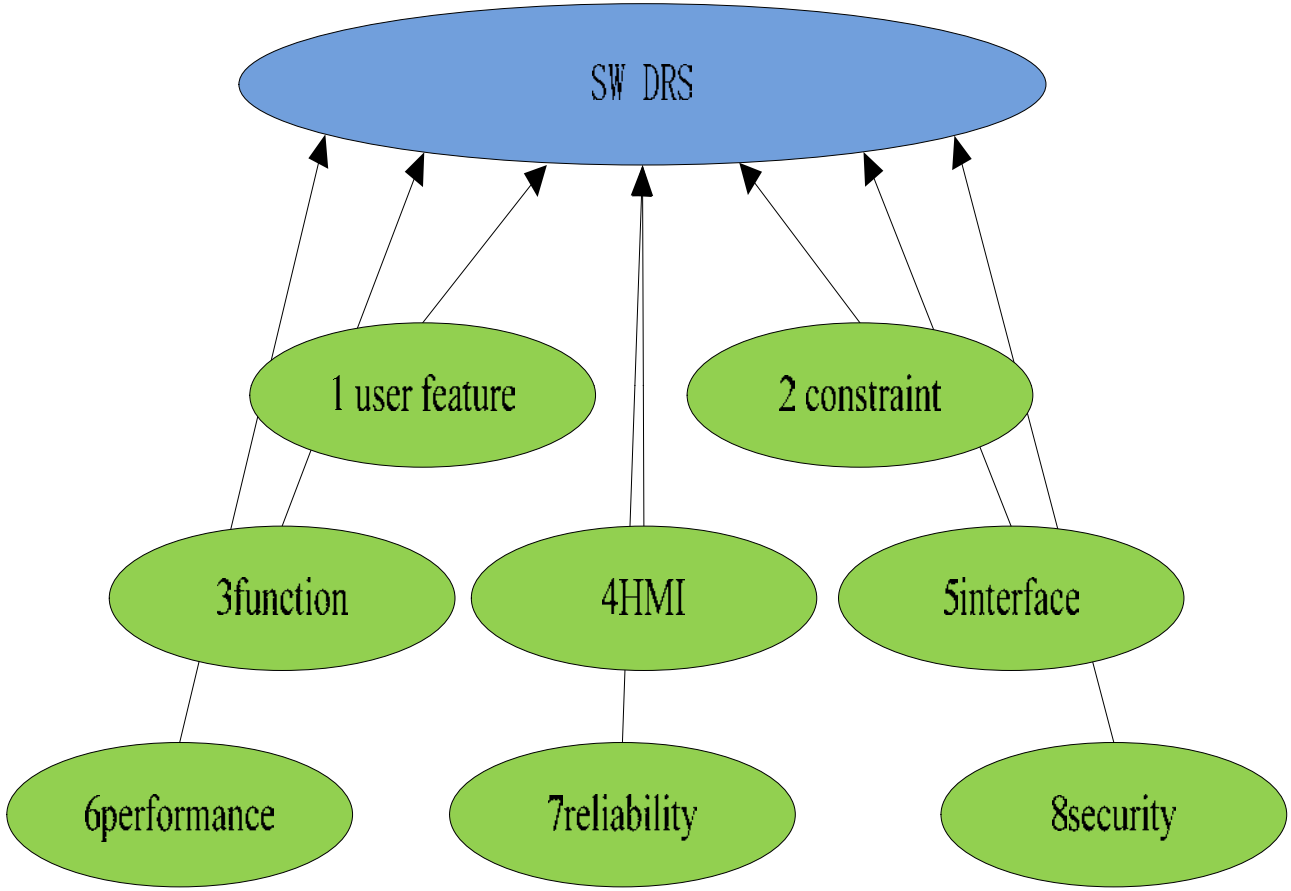


- SW quality plan
- SW safety plan

- SW CM

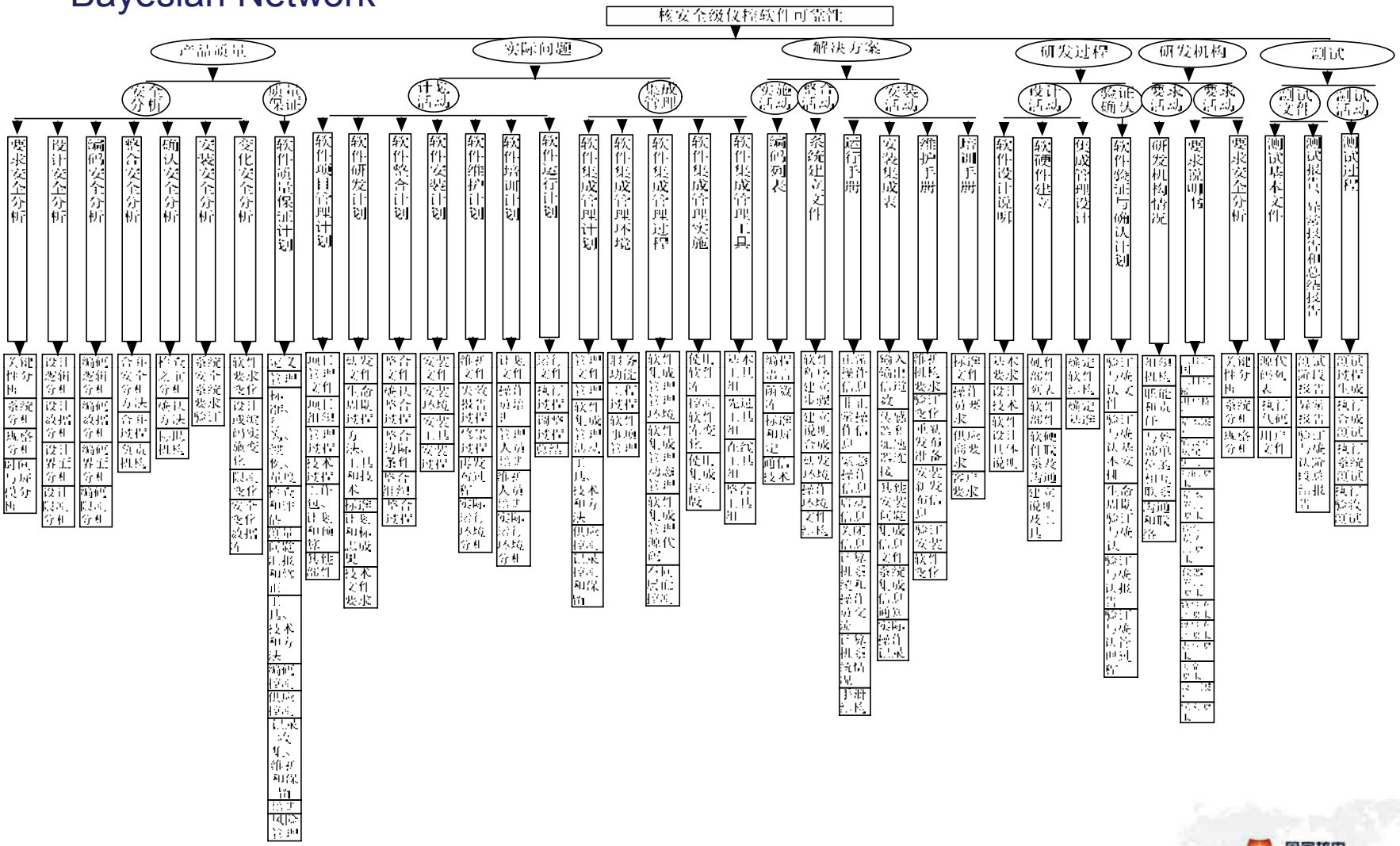
- SW integration
- SW installation
- SW maintenance
- SW V&V

Assessment of Software Reliability
--Bayesian Network



2. Research Topic

Assessment of Software Reliability
--Bayesian Network



Assessment of Software Reliability
--Bayesian Network

核安全级数字化仪控系统软件可靠性调查问卷

软件验证与确认过程评估

总体问题 * (必填, 单选)

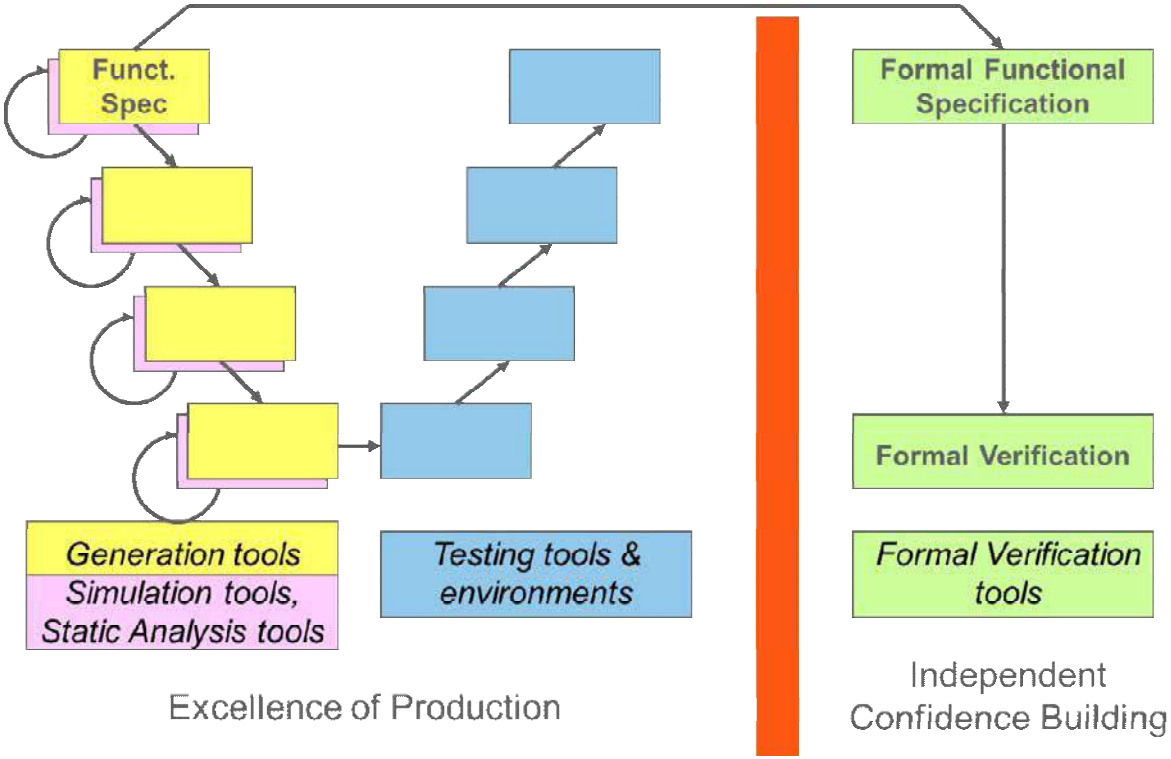
	80%符合	85%符合	90%符合	95%符合	100%符合
V&V是否引用了管理计划和质量保证计划	○	○	○	○	○
V&V的作用范围是否被定义	○	○	○	○	○
是否有一组有明确定义和有意义的目标来支持验证与确认的安全水平	○	○	○	○	○

软件生命周期管理的验证与确认问题 * (必填, 单选)

	80%符合	85%符合	90%符合	95%符合	100%符合
是否有足够的任务组合，以便完全支持V&V项目的目标	○	○	○	○	○
每个任务是否对被使用的方法和应用于这些方法的标准进行识别	○	○	○	○	○
每个任务需求的输入和输出是否确定	○	○	○	○	○
在每个活动期间是否定义了处理所遇到的异常情况的方法	○	○	○	○	○
是否详细叙述V&V安排和资源需求	○	○	○	○	○

Verification
--Formal Verification

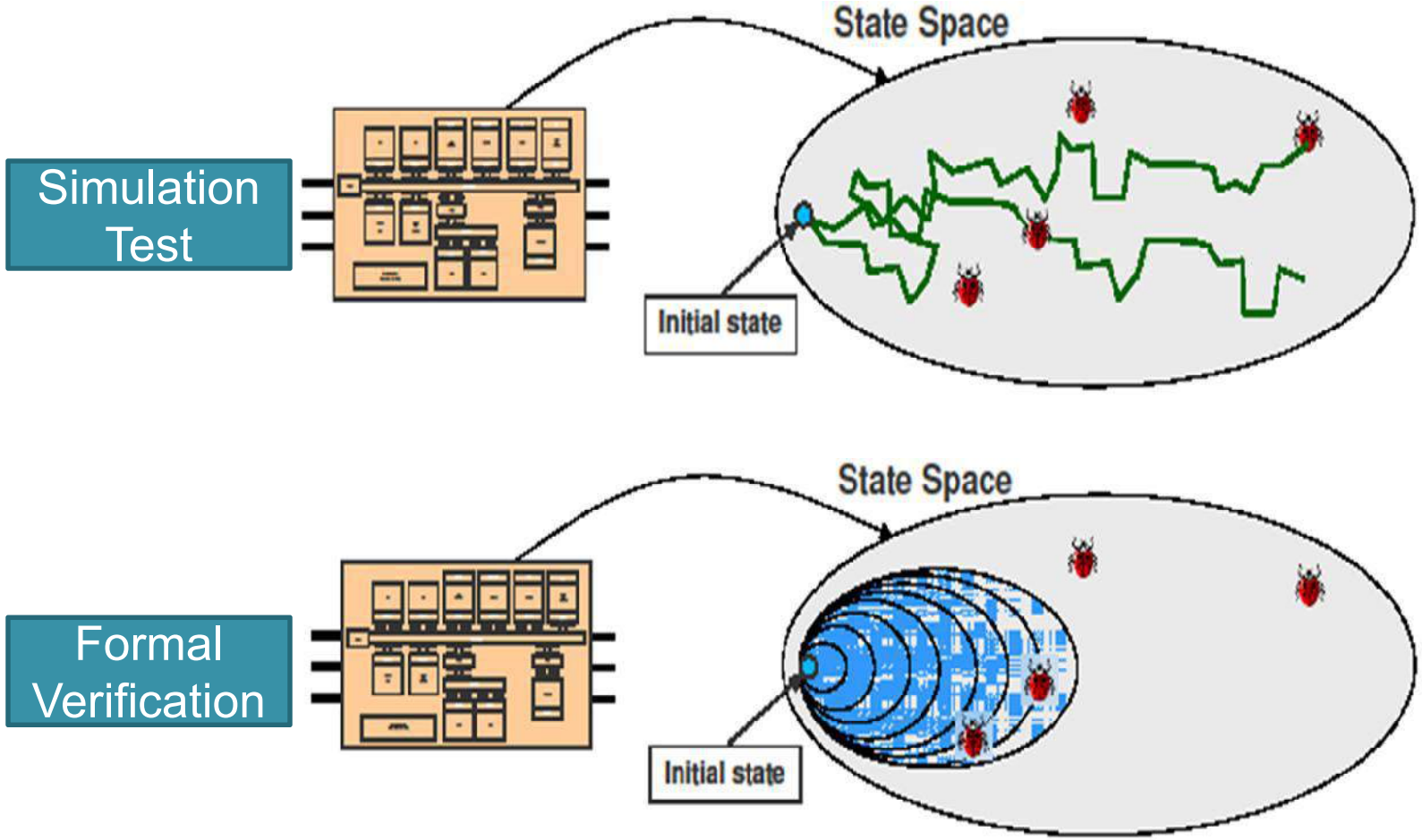
In the context of hardware and software systems, **formal verification** is the act of proving or disproving the correctness of intended algorithms underlying a system with respect to a certain formal specification or property, using formal methods of mathematics



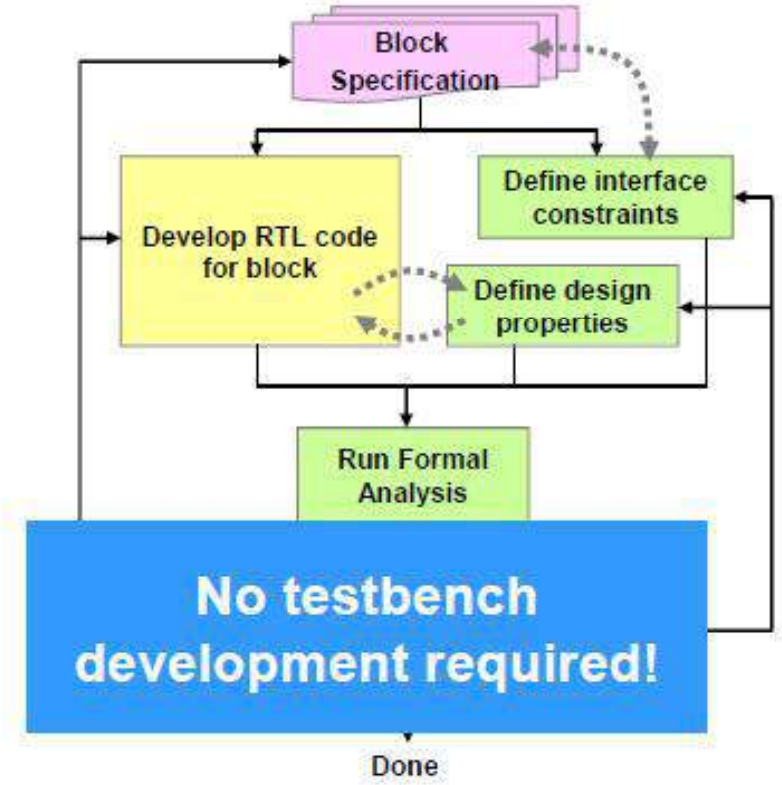
EPRI 1022983 Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays in Nuclear Power Plant I&C Systems

2. Research Topic

Verification
--Formal Verification



Verification
--Formal Verification

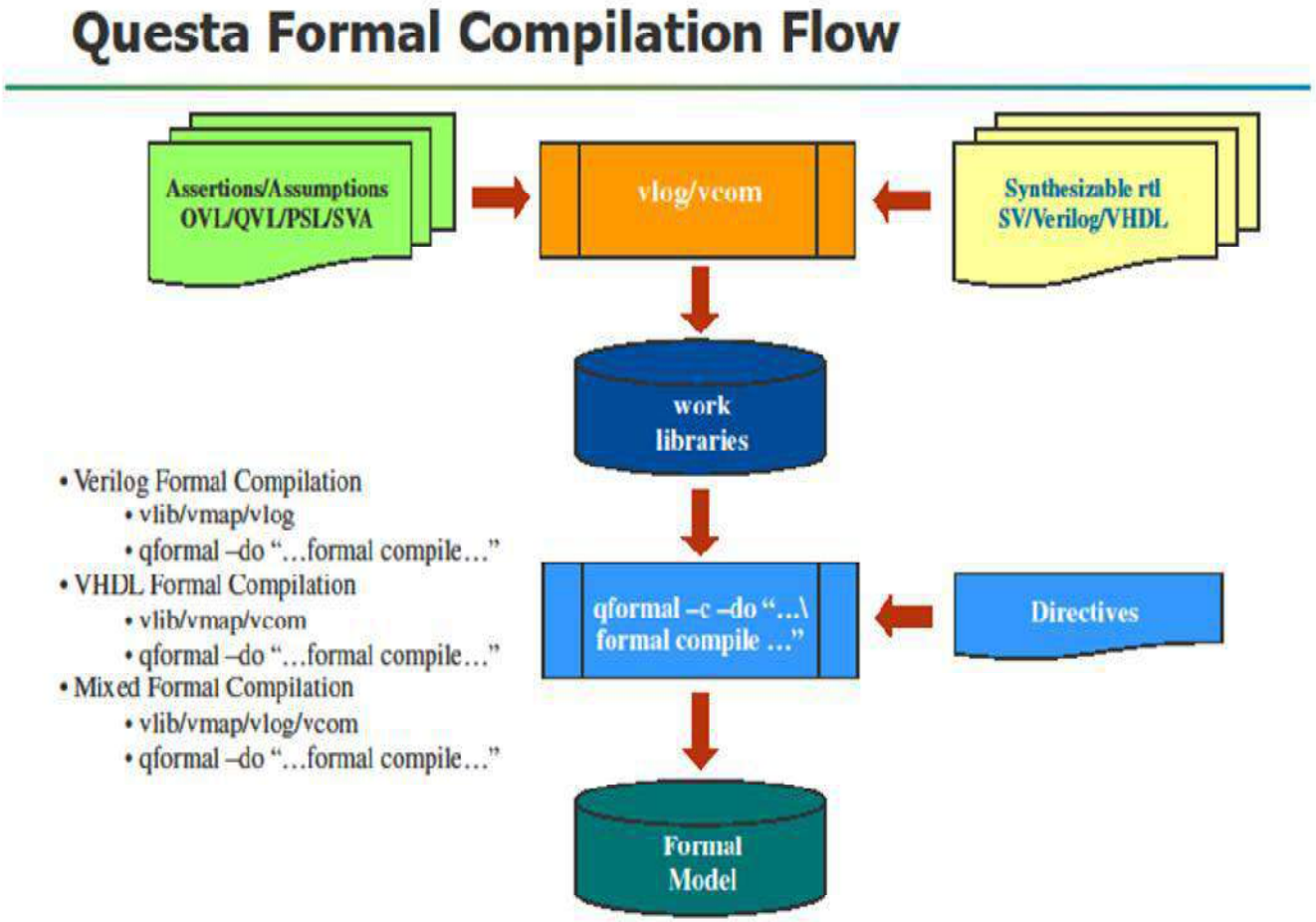


- Develop the formal specification based on Property Specification Language;
- Define the property of the VHDL or Verilog code by property assertion;
- Run the formal verification by tool.

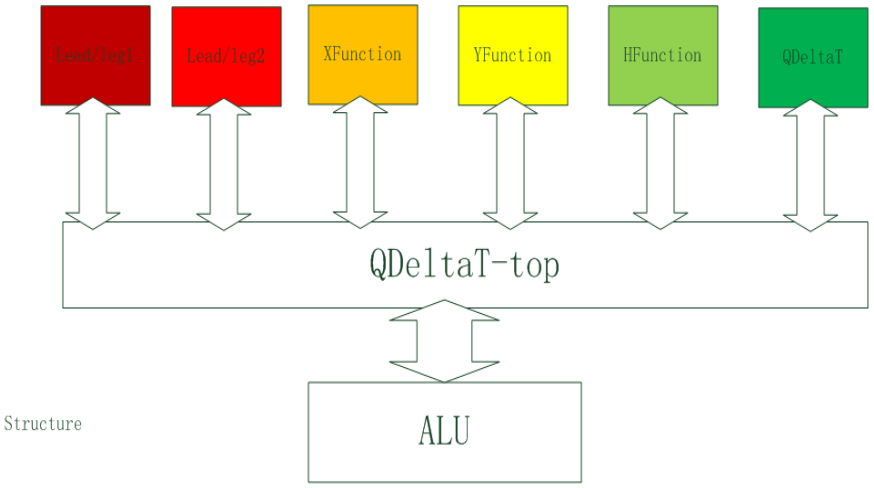
2. Research Topic

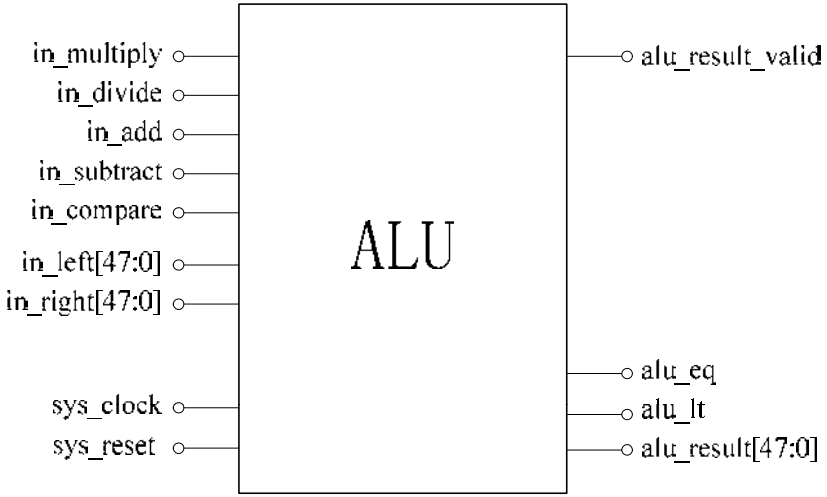
Verification

--Formal Verification



Verification
--Formal Verification





Properties

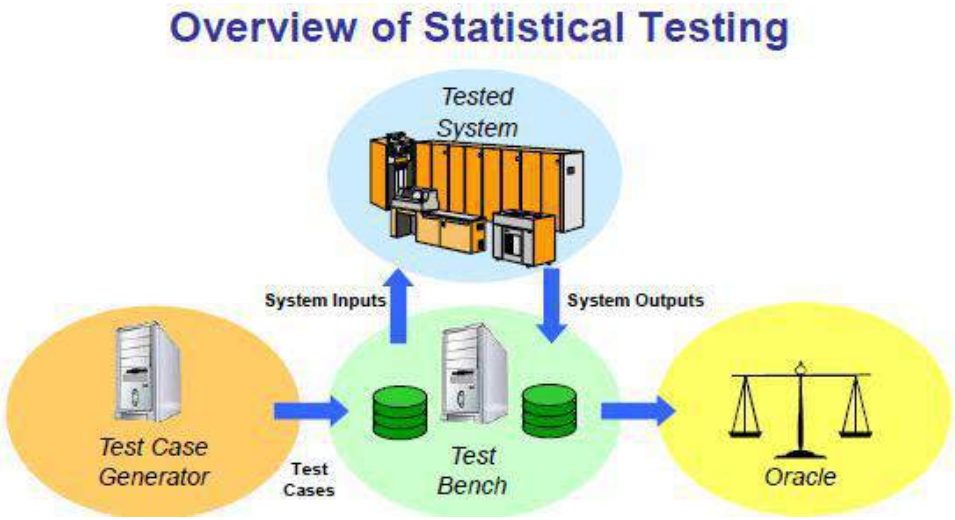
	Name	Type	Check	Radius	Clocks
F	check0.a_Multiply_result_chk	sva	sva	28	sys_clock
P	check0.a_Multiply_in_chk	sva	sva		sys_clock
P	check0.a_Multiply_over_chk	sva	sva		sys_clock
C	check0.cov_Multiply_in_chk	sva	sva	2	sys_clock
C	check0.cov_Multiply_over_chk	sva	sva	27	sys_clock
C	check0.cov_Multiply_result_chk	sva	sva	27	sys_clock

2. Research Topic

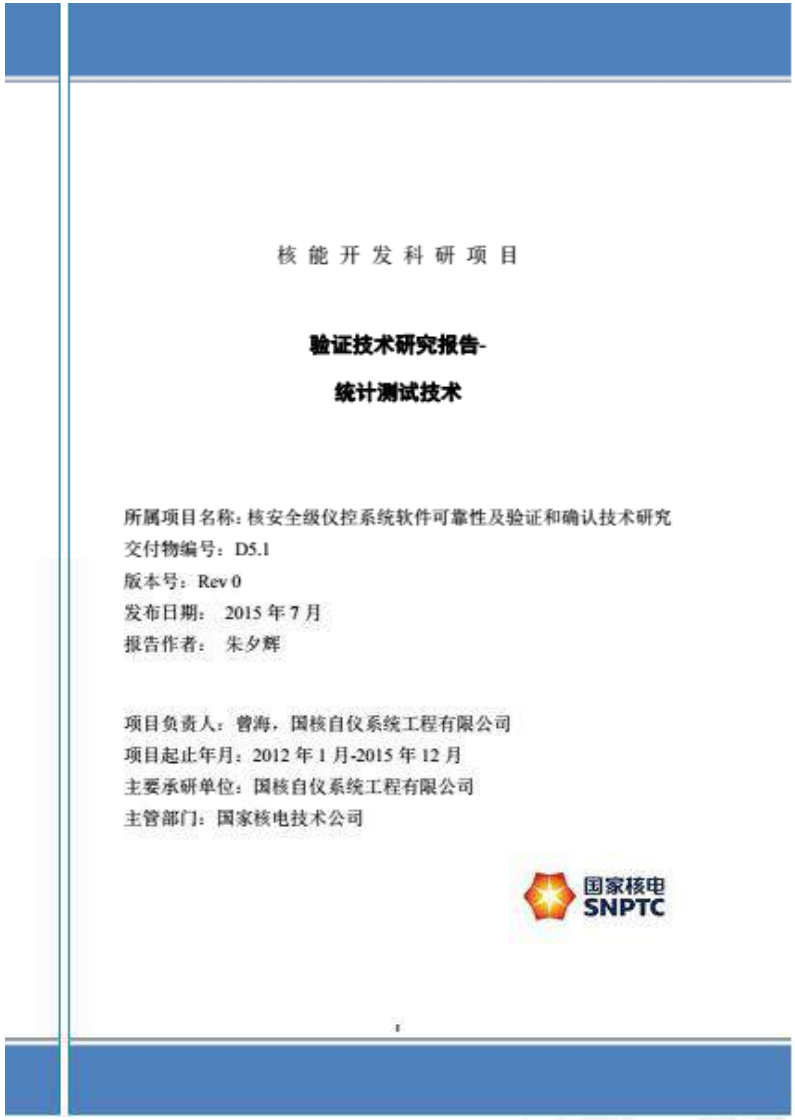
Verification
--Statistical Testing

"Software usually is tested to detect bugs, such that those identified be removed, and also to demonstrate that the software can perform its intended functions, possibly for licensing purposes. Different test strategies have been developed, for example, black-box and white-box testing. However, they are not designed for quantifying software reliability, that is, the failure probability on demand, and thus, cannot be used for that purpose [May 1995, Hamlet 1994,Kuball 2004]. The main reason is that the inputs to the software in these tests are not ***random samples from the operational profile***. Therefore, separate operationally representative tests must be undertaken. Such testing performed to support quantifying software reliability, i.e., the probability of failure on demand, is called statistical testing [IEC 1986]."
(NUREG/CR 7044- DEVELOPMENT OF QUANTITATIVE SOFTWARE RELIABILITY MODELS FOR DIGITAL PROTECTION SYSTEMS OF NUCLEAR POWER PLANTS)

Verification
--Statistical Testing



-- Nguyen Thuy, EDF R&D



核 能 开 发 科 研 项 目

验证技术研究报告-

统计测试技术

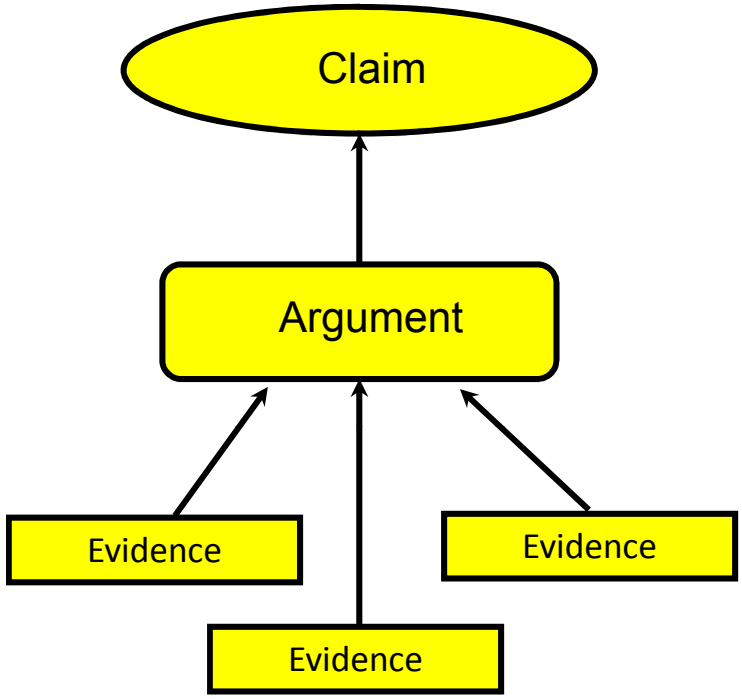
所属项目名称：核安全级仪控系统软件可靠性及验证和确认技术研究
交付物编号：D5.1
版本号：Rev 0
发布日期： 2015 年 7 月
报告作者： 朱夕辉

项目负责人：曾海，国核自仪系统工程有限公司
项目起止年月：2012 年 1 月-2015 年 12 月
主要承研单位：国核自仪系统工程有限公司
主管部门：国家核电技术公司

国家核电 SNPTC

Verification
--Safety justification

Safety case: “a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment”



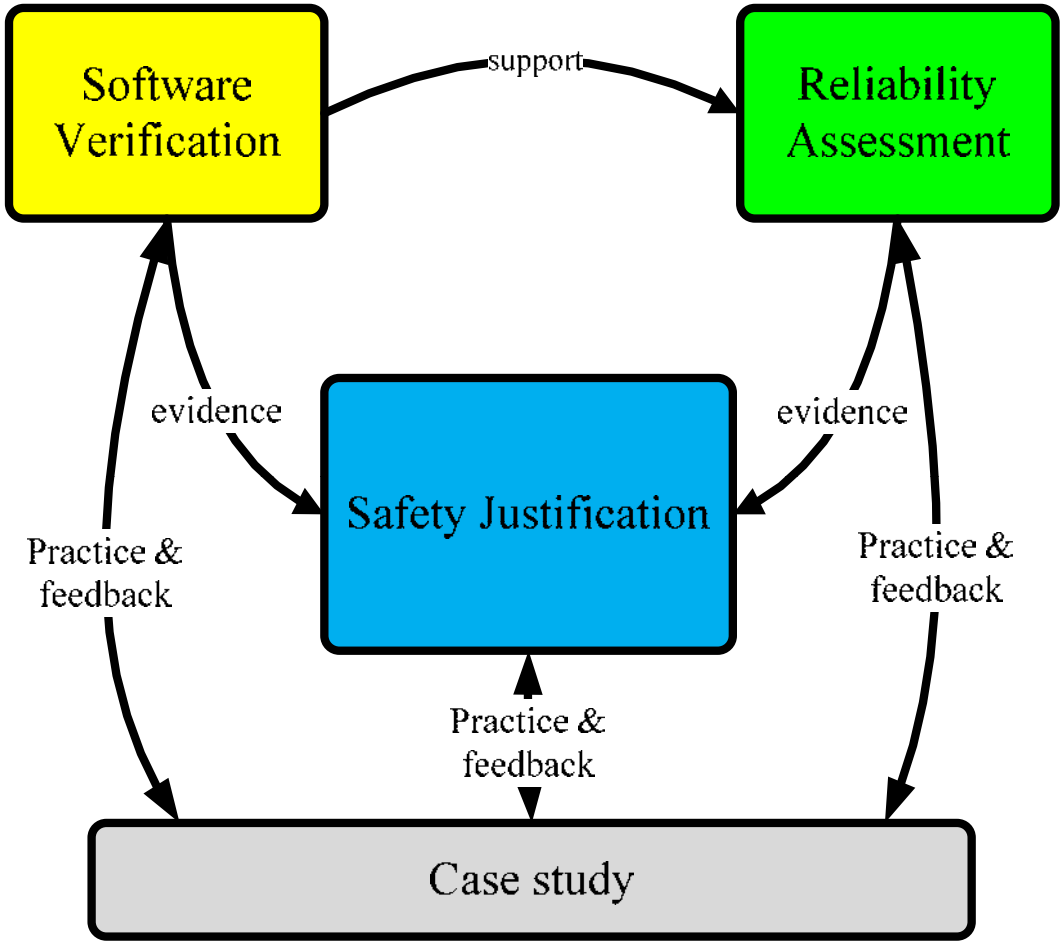
(-- Sofia Guerra, Adelard)

Verification
--Safety justification

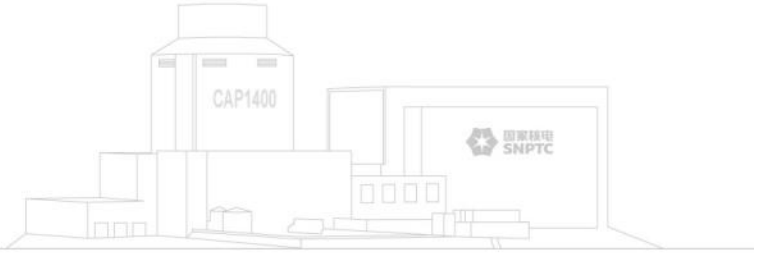
Safety case: “a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment”

(-- Sofia Guerra, Adelard)

2. Research Topic



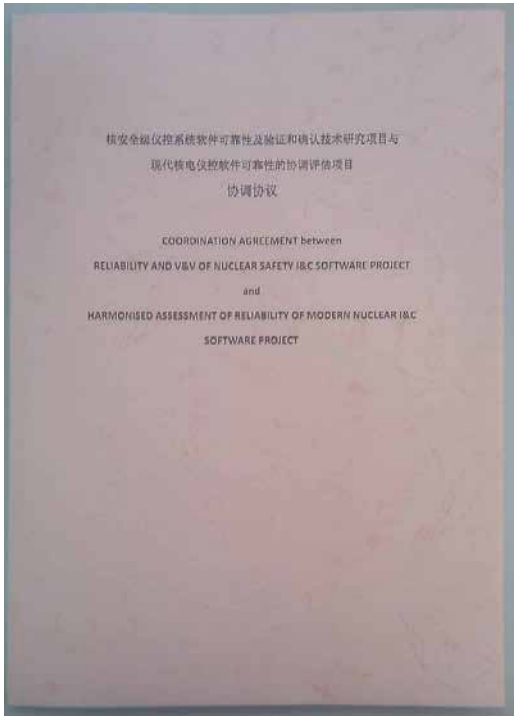
Content



3. International Cooperation

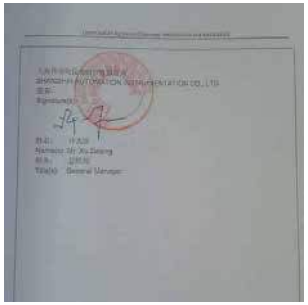
	No.	Participant organisation name	Country
HARMONICS	1	VTT	Finland
	2	Électricité de France (EDF)	France
	3	Institute for Safety Technology (ISTEC)	Germany
	4	Adelard LLP/CSR (ADEL)	UK
	5	Swedish Radiation Safety Authority (SSM)	Sweden
RAVONSICS	1	State Nuclear Power Automation System Engineering Corp. (SNPTC/SNPAS)	China
	2	Nuclear and Radiation Safety Center (NRSC)	China
	3	Institute for Standardization of Nuclear Industry	China
	4	Harbin University of Technology	China
	5	China Techenergy Co., Ltd. (CTEC)	China
	6	Shanghai Automation Instrumentation Co., Ltd (SAIC)	China

COORDINATION AGREEMENT (with 8 attachments)

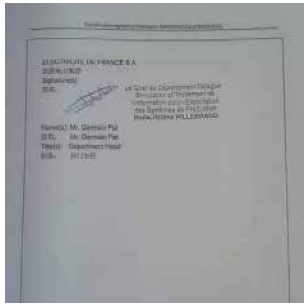

核安全仪控系统软件可靠性及验证和确认技术研究项目与
现代核电仪控软件可靠性的协调评估项目
协调协议

COORDINATION AGREEMENT between
RELIABILITY AND V&V OF NUCLEAR SAFETY I&C SOFTWARE PROJECT
and
HARMONISED ASSESSMENT OF RELIABILITY OF MODERN NUCLEAR I&C
SOFTWARE PROJECT








3. International Cooperation

- March, 2011, Kick-off meeting in Shanghai;
- April, 2011, HARMONICS meeting in Sweden;
- January, 2012, 1st RAVONSICS meeting in shanghai;
- April, 2012, HARMONICS workshop in Finland;

3. International Cooperation

- July, 2012, meeting in Sandiego；
- October, 2012, 2nd RAVONSICS meeting in Herbing and Coordination meeting;

3. International Cooperation

- December, 2013, 3rd RAVONSICS meeting in Shanghai;
- December, 2013, audit meeting from CAEA;

3. International Cooperation

- April, 2014, HARMONICS workshop；
- July, 2014, EU-China workshop；
- December, 2014, RAVONSICS workshop

3. International Cooperation

- September, 2015, peer review meeting

核安全级仪控系统软件可靠性及验证和确认技术研究项目

技术评审意见

2015 年 9 月 10 日至 11 日，国核自仪系统工程有限公司（以下简称国核自仪）在上海组织召开了国核自仪承研、哈尔滨工程大学参研的核能开发项目“核安全级仪控系统软件可靠性及验证和确认技术研究项目”（以下简称项目）技术评审会议（专家组名单见附件 1）。与会专家听取了项目组技术报告，审查了相关研究报告，经质疑和讨论，形成如下评审意见：

1. 该项目针对核安全级仪控系统软件，对软件可靠性评价、验证技术，以及软件安全评价方法等开展了广泛深入的研究，形成了相关研究报告（研究报告清单见附件 2）；
2. 项目采用软件可靠性层次化模型方法和贝叶斯信度网方法，对核安全级仪控系统软件可靠性建模和评估进行了深入研究。研究结果表明，采用软件可靠性层次化模型方法可对软件结构进行建模、关键路径分析、可靠性估计以及单元敏感性分析；采用贝叶斯信度网建立的软件可靠性评估模型，可以定量预计软件可靠性并识别影响软件可靠性的关键因素；
3. 项目针对安全案例 CAE 方法、形式验证技术、统计测试技术等国际前沿验证技术开展研究。研究结果表明，上述方法和技术适用于核安全级仪控系统软件安全评价和验证；
4. 项目开展了广泛的国内外合作和交流，促进了相关领域的技术融合。

专家组认为，项目对核安全级仪控系统软件可靠性评价及验证技术进行了全面深入的研究，研究工作满足核能开发项目任务书中研究目标、研究内容和预期成果的要求，达到国内领先水平，其中软件可靠性层次化模型方法为首次提出，为我国核安全级仪控系统软件安全评价奠定了良好的基础。

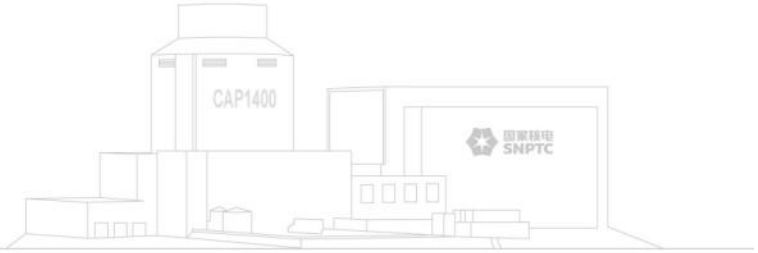
专家组建议，在已开展的调研工作基础上，对核安全级数字化仪控系统软件可靠性分析技术的国内外研究及应用现状进行进一步的分析总结。

专家组组长：

日期：2015年9月11日

1/3

Content



4. Conclusion

RAVONSICS is a good start of the software reliability assessment in China

RAVONSICS is also a good start of deep and broad international and national cooperation in China

More effort is required for every topics of RAVONSICS

更安全的核电
更美好的生活