哈爾濱工程大學

The reliability model for the FPGA-based instrument and control system using Colored Petri Net

Zhanguo Ma, Hidekazu Yoshikawa, Ming Yang

Harbin Engineering University

College of Nuclear Science and Technology

Outline

1. **FPGA applications in NPP**
2. **Fault tolerance techniques of I&C system**
3. **Reliability model for FPGA based Module**
4. **Petri Net methodology and CPN models**
5. **Future work**

Part 1

FPGA applications in NPP

FPGA based I&C platforms and applications in NPP

FPGA based Platform	RadICS	Advanced Logic System (ALS)	Nuclear Protection and Control (NuPAC)	Toshiba FPGA based I&C system
Company	Radiy, Ukraine	Westinghouse , USA	Lockheed Martin (USA) &SNPAS (China)	Toshiba, Japan
FPGA Technology	Flash	Flash	Flash	Antifuse
Application	•Reactor Trip System, •Engineered Safety Features Actuation System, •Rods Control System, •Reactor Power Control & Limitation System •Other systems: Fire Alarm System, Seismic Sensor.	•Main steam and feedwater isolation system •AP1000 DAS	•Reactor Trip System •Engineered Safety Features Actuation System	•Power Range Neutron Monitor system, •Reactor Trip and Isolation system for the boiling water reactor. •Primary safety I&C system for ABWR in South Texas

Other applications in NPP

- In Canada, FPGA was first designed as the emulator, then it was designed for the safety related system in the CANDU plant
- In France, EDF started to replace the rod control system and is supporting the research for the FPGA applications in the safety related systems
- Priority logic MALTAC platform and AP1000 NPP
- The FPGA is more and more extensive applied both for the new NPP I&C system design and the operating plants update
- The reliability evaluation of the FPGA based system is drawn the more and more concerns

Comparison Microprocessor and FPGA

The microprocessor and the FPGA based are the two dominated technical solution for the NPP I&C design.

Micropro cessor	FPGA
Based on operation system, peripheral hardware and software associated drivers	Flat hardware logic
Instruction are executed sequential	Process separate functions independently and in parallel
Difficult to separate as they based on the same operation system and other software service	Ancillary functions can be separated from the main I&C function
Upgrade including the operation system and supporting software drives, take more time	Directly upgraded the I&C logic functions
Software process, software and hardware product	Software process, hardware product
More experience and easy for the complicated HMI	Difficult for the complicated HMI

Part 2

Fault tolerance techniques of I&C system

Fault tolerance & fault coverage

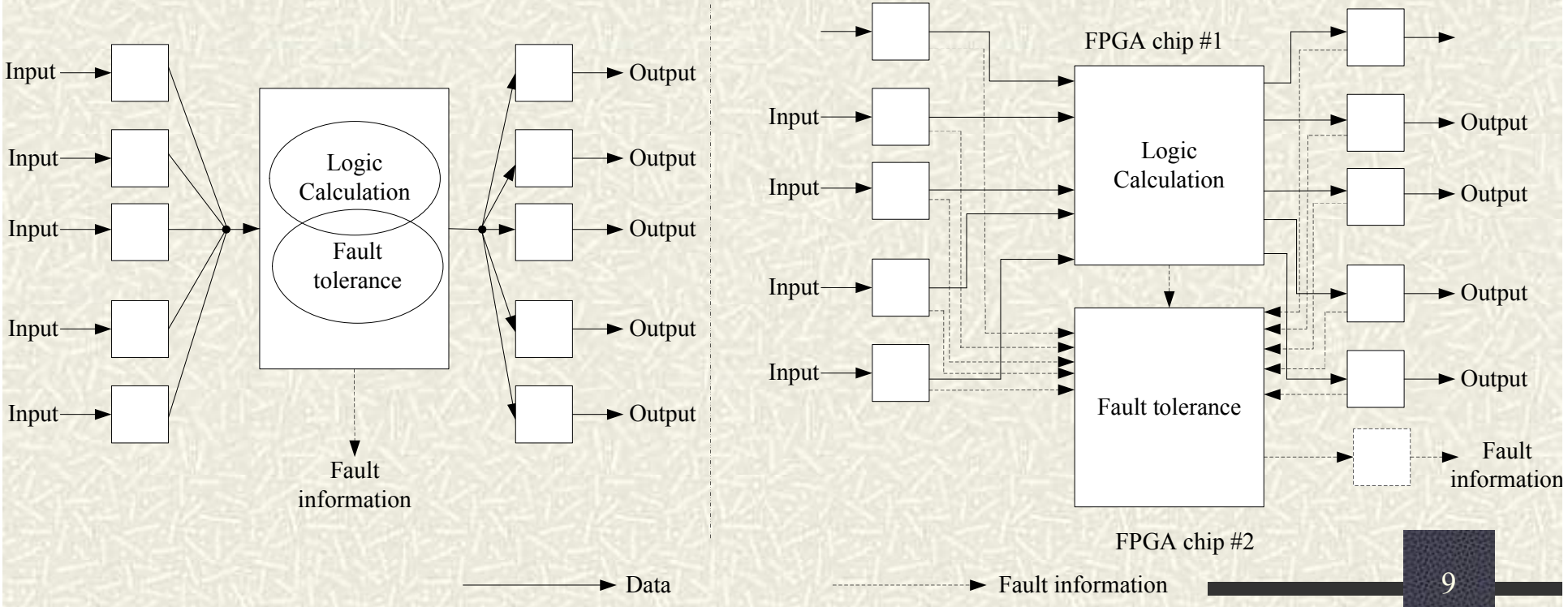
- The fault tolerance is the system's property that enables a system to correctly perform the specific required function in the event of failure of the components or sub-system.

- The fault coverage is the evaluation of the fault tolerance design and it is the ability to perform fault detection, fault isolation or fault recovery.

$$C = \Pr(fault \quad detected \,\&\, recovery \mid fault \quad existence)$$

Fault tolerance design for FPGA based system

- Fault tolerance design is equally applied both for the microprocessor and FPGA based I&C system.
- The main difference is the fault techniques can be designed in a separated FPGA chip.

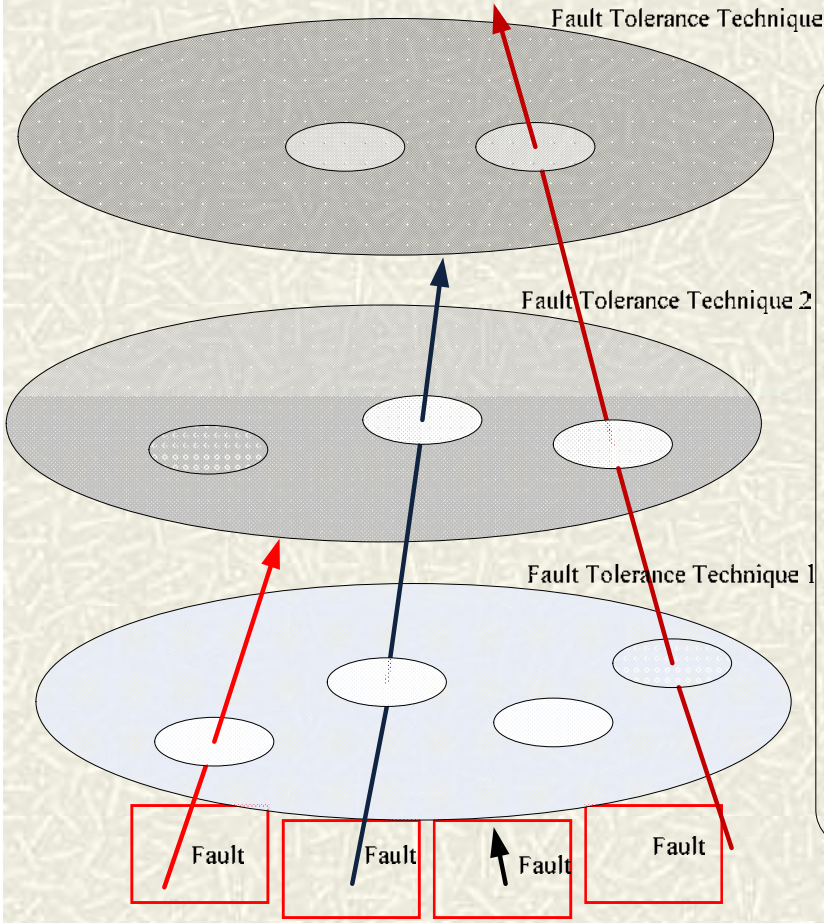


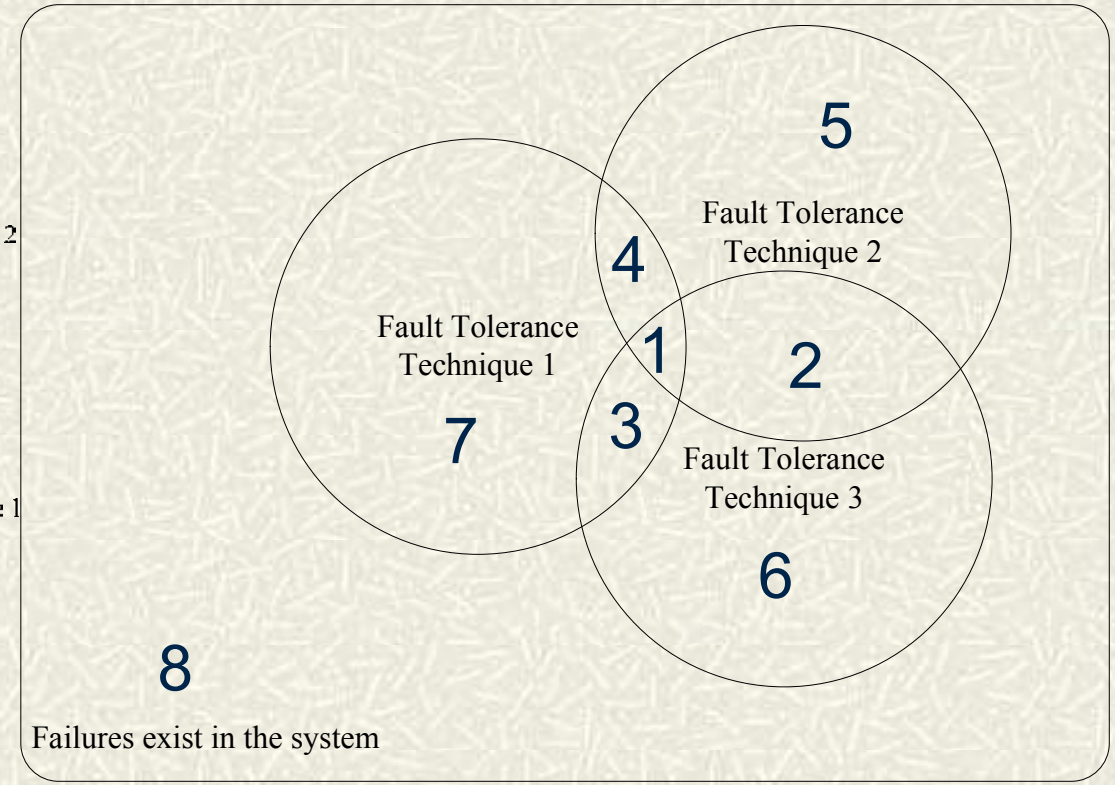
Fault tolerance techniques

- Fault tolerance design:
  - enhance the safety and reliability
  - alleviate the maintenance for the digital I&C system

- Characters:
  - There is may impact on the main control function when it failed. But there is less or no impact for the FPGA solution as they are designed in separated chip.
  - The specific fault tolerance technique can detect and recover certain faults.
  - Certain faults may be detected by several fault tolerance techniques, than some certain fault may not be detected by any fault tolerance techniques.
  - For different fault tolerance technique, it takes different time to detect and recover the fault.

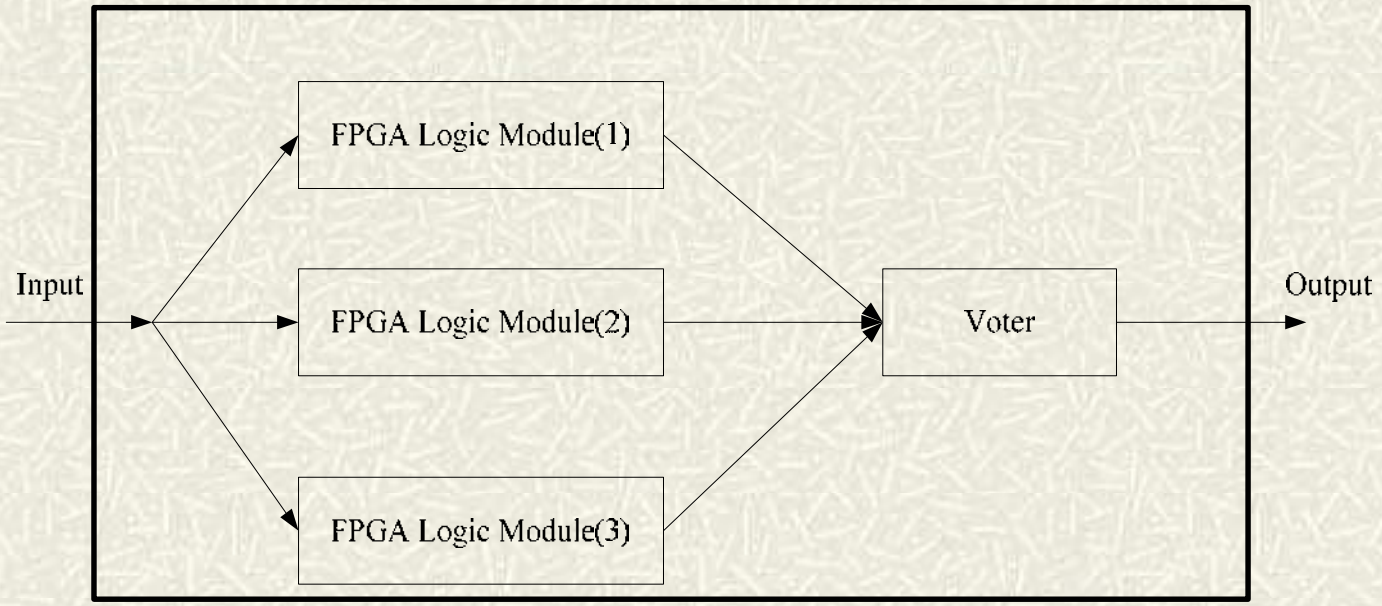
Fault and fault tolerance design





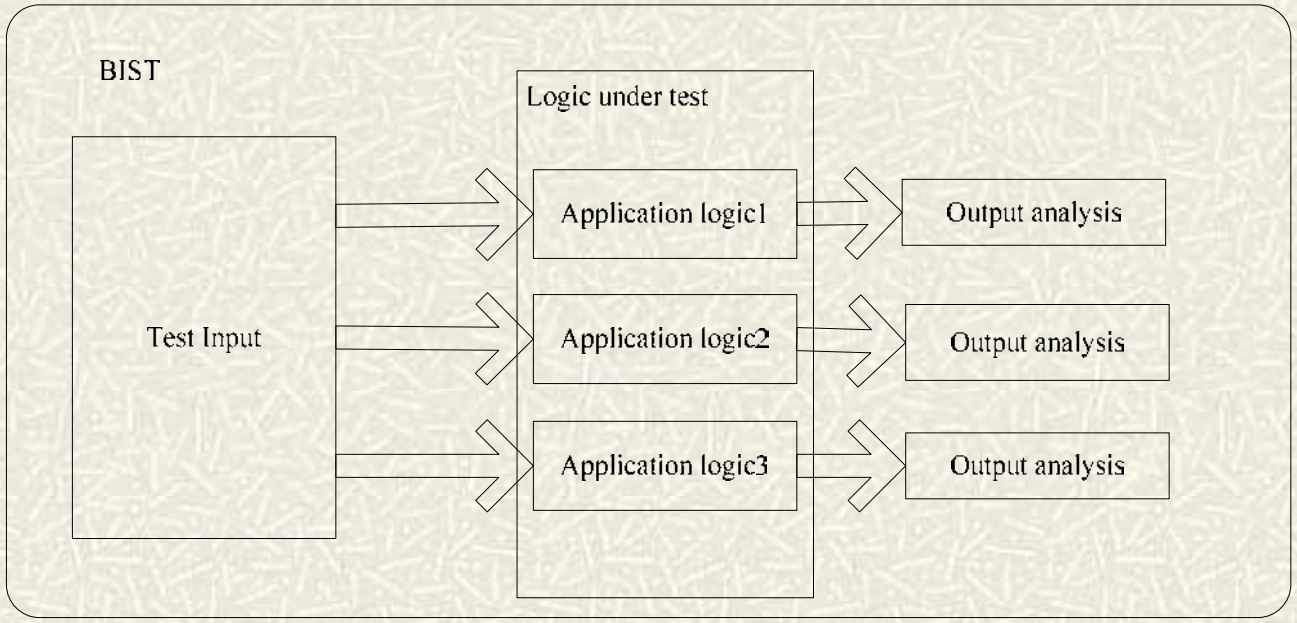
Fault tolerance design of the FPGA based I&C system

I. Module Redundancy uses additional hardware to compare the logic result to determine the logic function is correctly calculated or not such Triple Modular Redundancy (TMR).



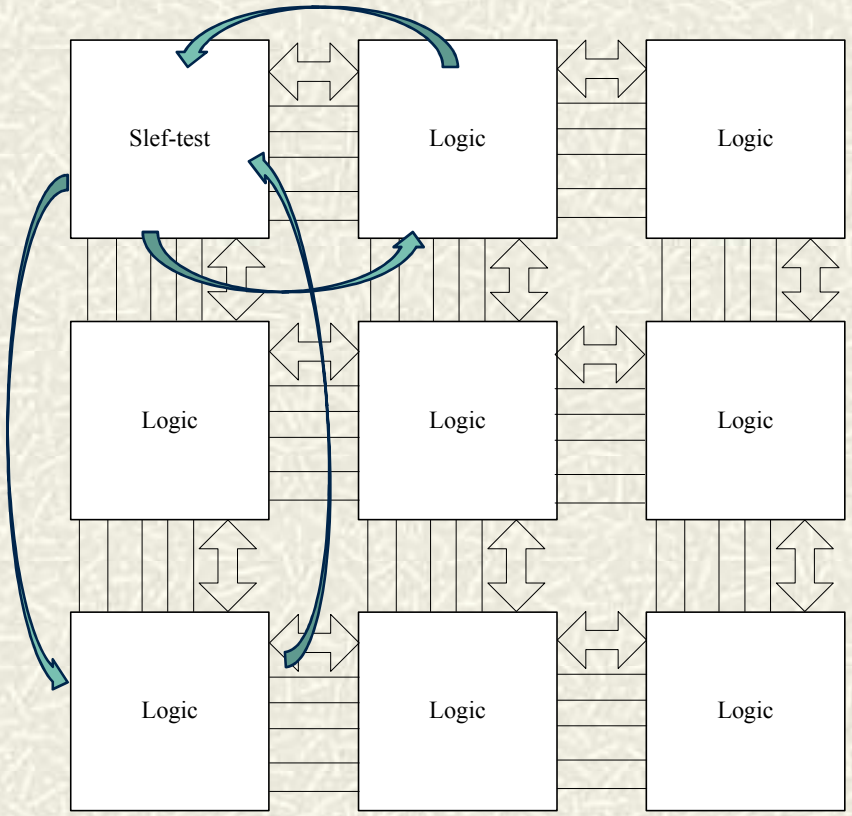
Fault tolerance design of the FPGA based I&C system

II. Offline test methods perform any test when FPGA is not running operationally. When the test requires no further external test equipment, it is known as the Built-In-Self-Test (BIST).



Fault tolerance design of the FPGA based I&C system

II. Roving test methods perform a progressive scan of the FPGA structure by swapping blocks of functionality with a block carrying out a test function.

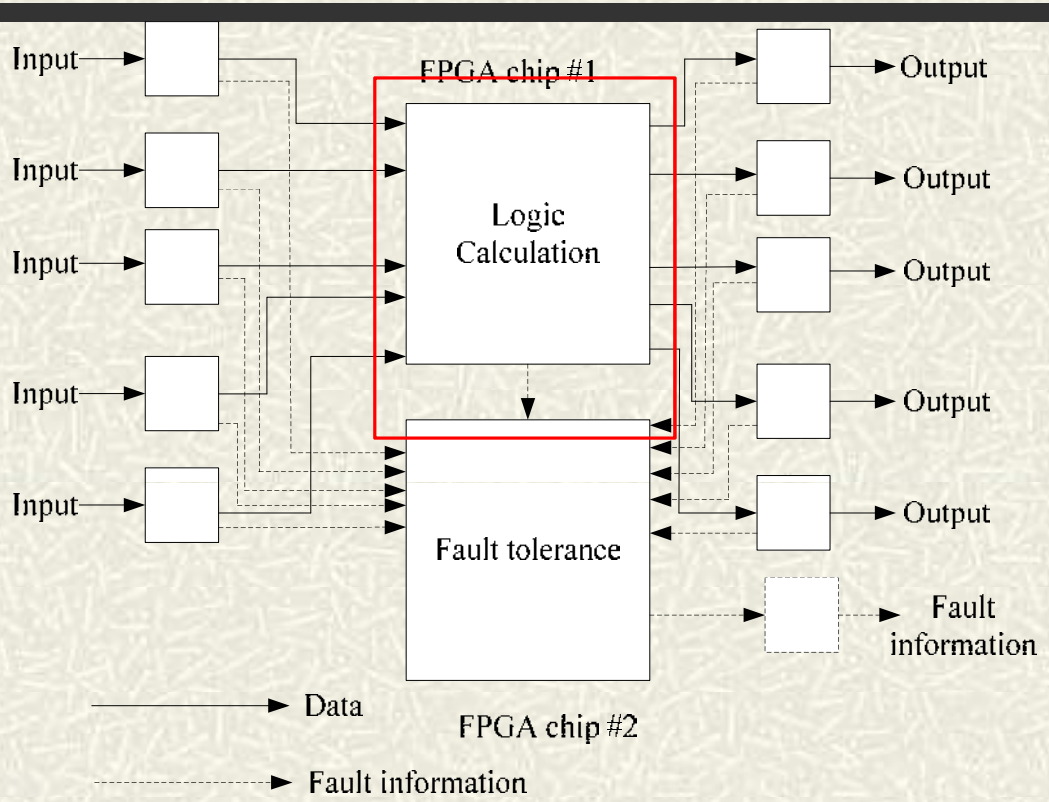


- The coverage for one of the technique i is C_i

Part 3

Reliability model for FPGA based Module

Module Reliability



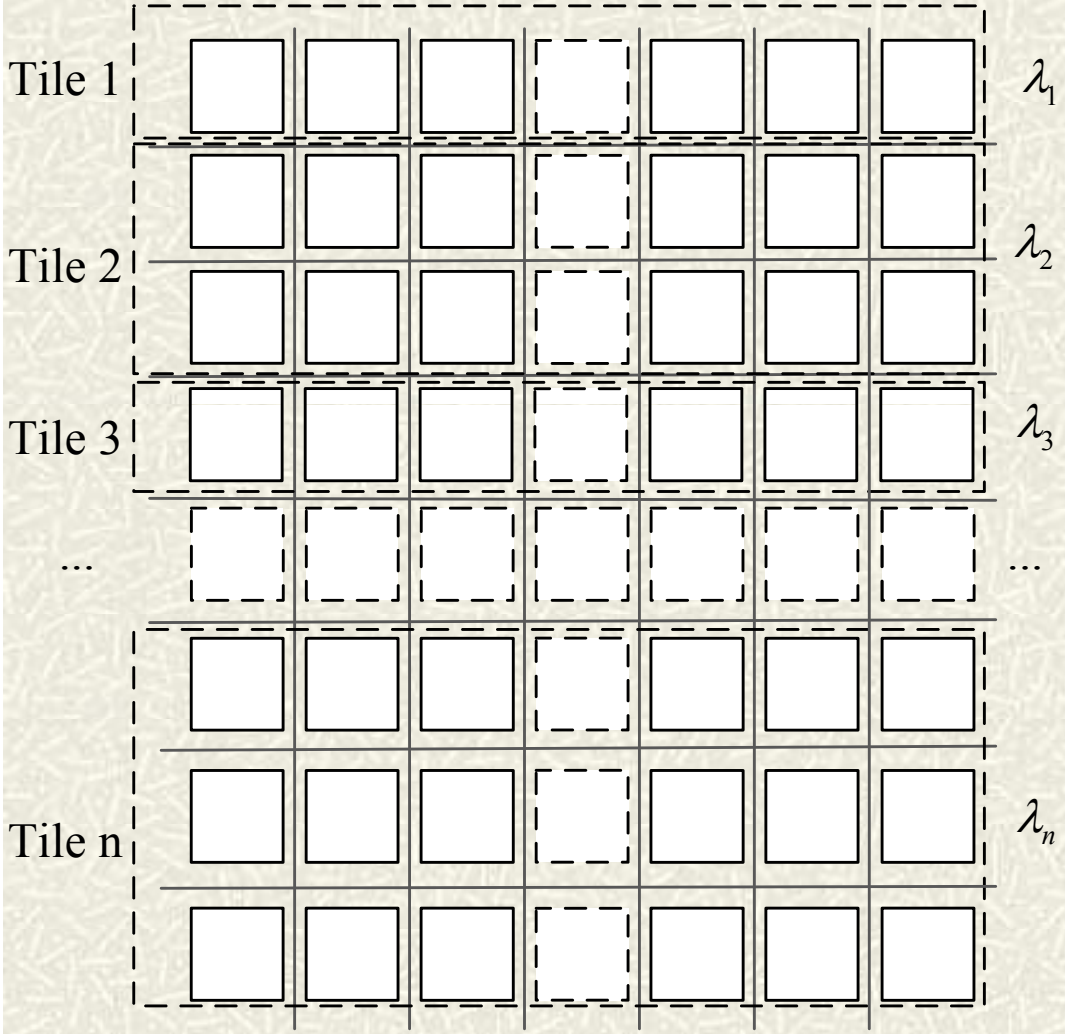
For the module, the reliability can be calculated by:

$$R(t) = e^{(-\lambda t)} \qquad 3.1$$

λ is the failure probability at $t + \Delta t$

t is the hardware running time

FPGA reliability



$$R(t) = 1 - \prod_{i=1}^{n} (1 - R_i(t)) \qquad 3.2$$

$$= 1 - \prod_{i=1}^{n} (1 - e^{(-\lambda_i t)})$$

λ_n is the failure probability for one tile and it is less than λ

In the calculation model, $\lambda_n = \lambda$

$$R(t) = 1 - (1 - e^{(-\lambda t)})^n \qquad 3.3$$

The reliability calculation

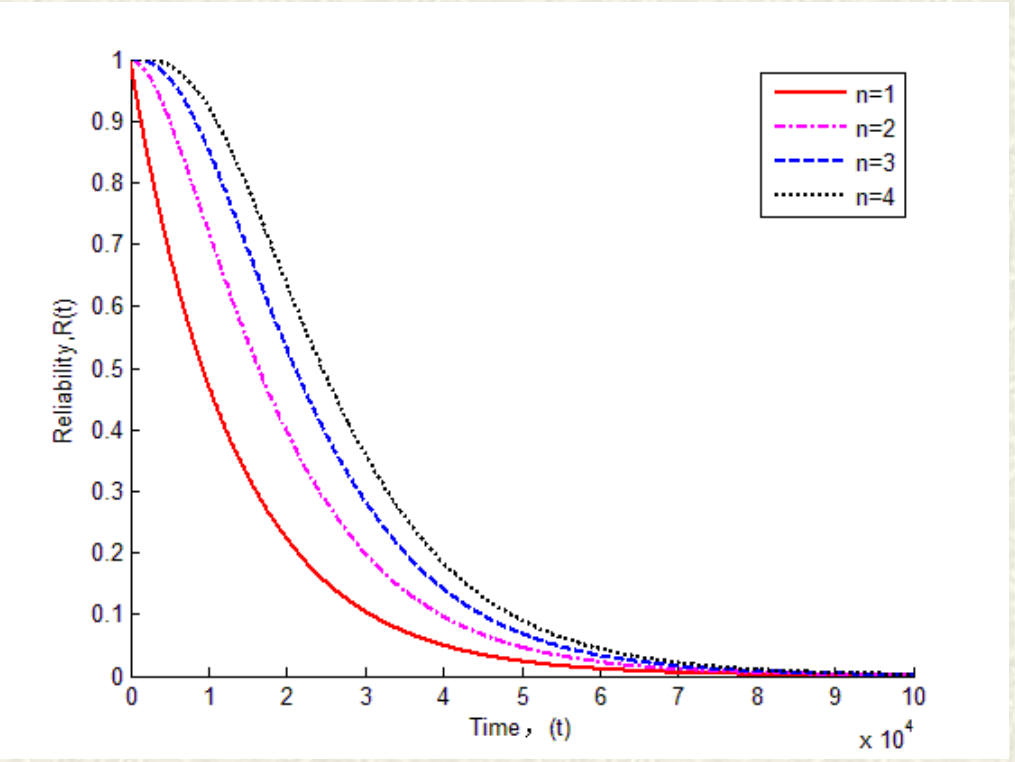
$$MTTF = \int_0^\infty R(t)dt = \int_0^\infty \left[1-(1-e^{(-\lambda t)})^n\right]dt = \frac{1}{\lambda}+\frac{1}{2\lambda}+\cdots+\frac{1}{n\lambda} \qquad 3.4$$

- The tile optimal number n=4

$$MTTF = \frac{1}{\lambda}+\frac{1}{2\lambda}+\frac{1}{3\lambda}+\frac{1}{4\lambda} \qquad 3.5$$

$$MTTF = \frac{1}{\lambda} \qquad 3.6$$

$$\lambda_M = \frac{1}{MTTF} = \frac{12}{25}\lambda \qquad 3.7$$



Parameter for each fault technique

λ_i is the failure probability for the fault tolerance technique *i*

$$\lambda_i = C_i \cdot \lambda_M \qquad 3.8$$

After the fault is detected, the fault should be repaired. The reparation time follows the Erlang law.

$$F(\mathrm{t}) = 1 - \sum_{k=0}^{n-1} \frac{1}{k!} e^{-\mu_c t} (\mu_c t)^k \qquad 3.9$$

k means the number of modules

$$\mu_c = \frac{1}{MTTR_c}$$

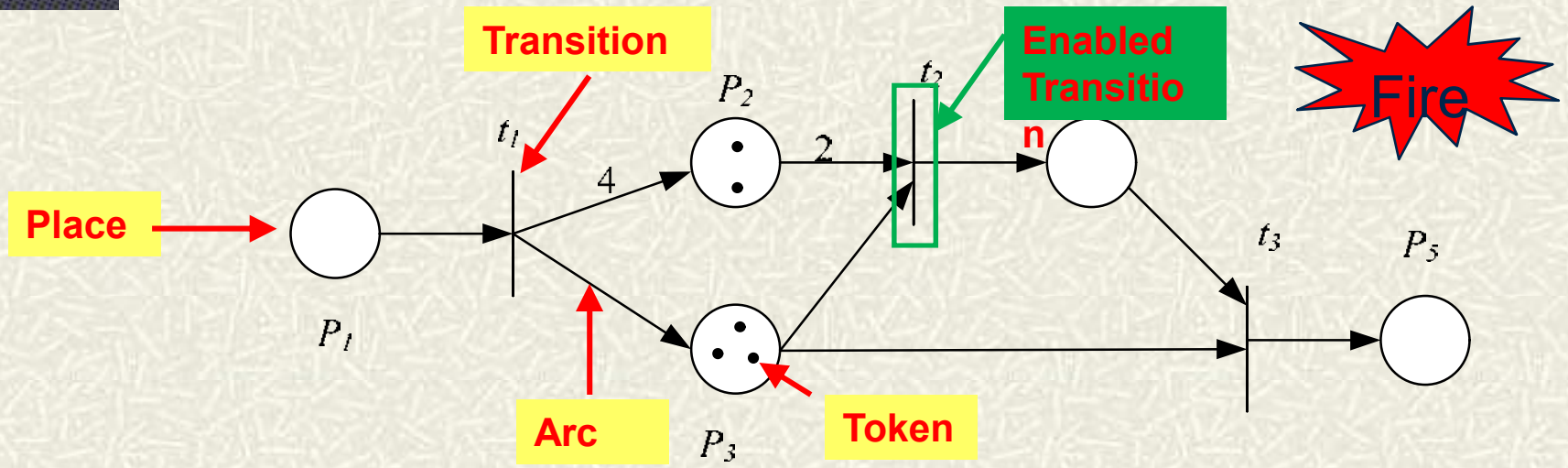
Part 4

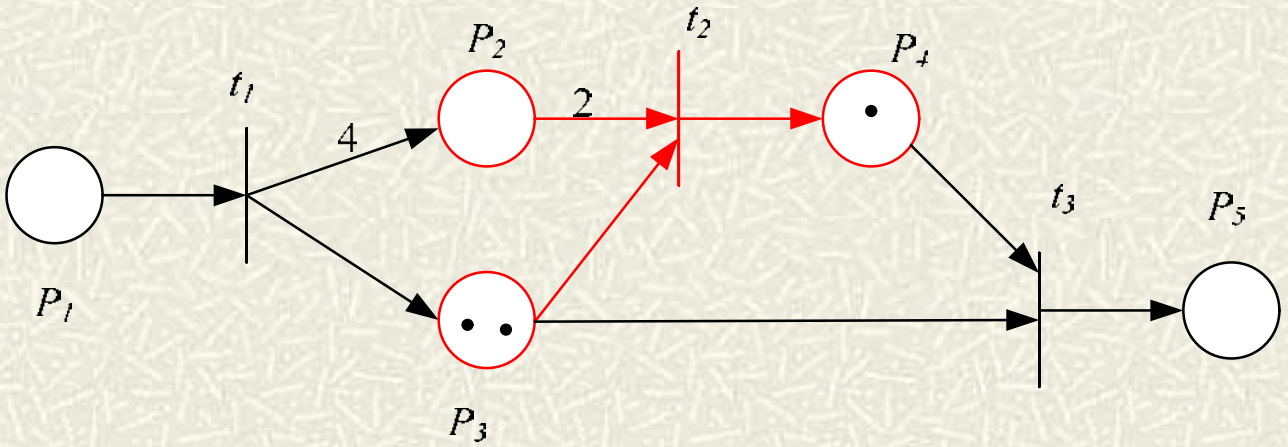
Petri Net methodology and CPN models

Methodology-WHY

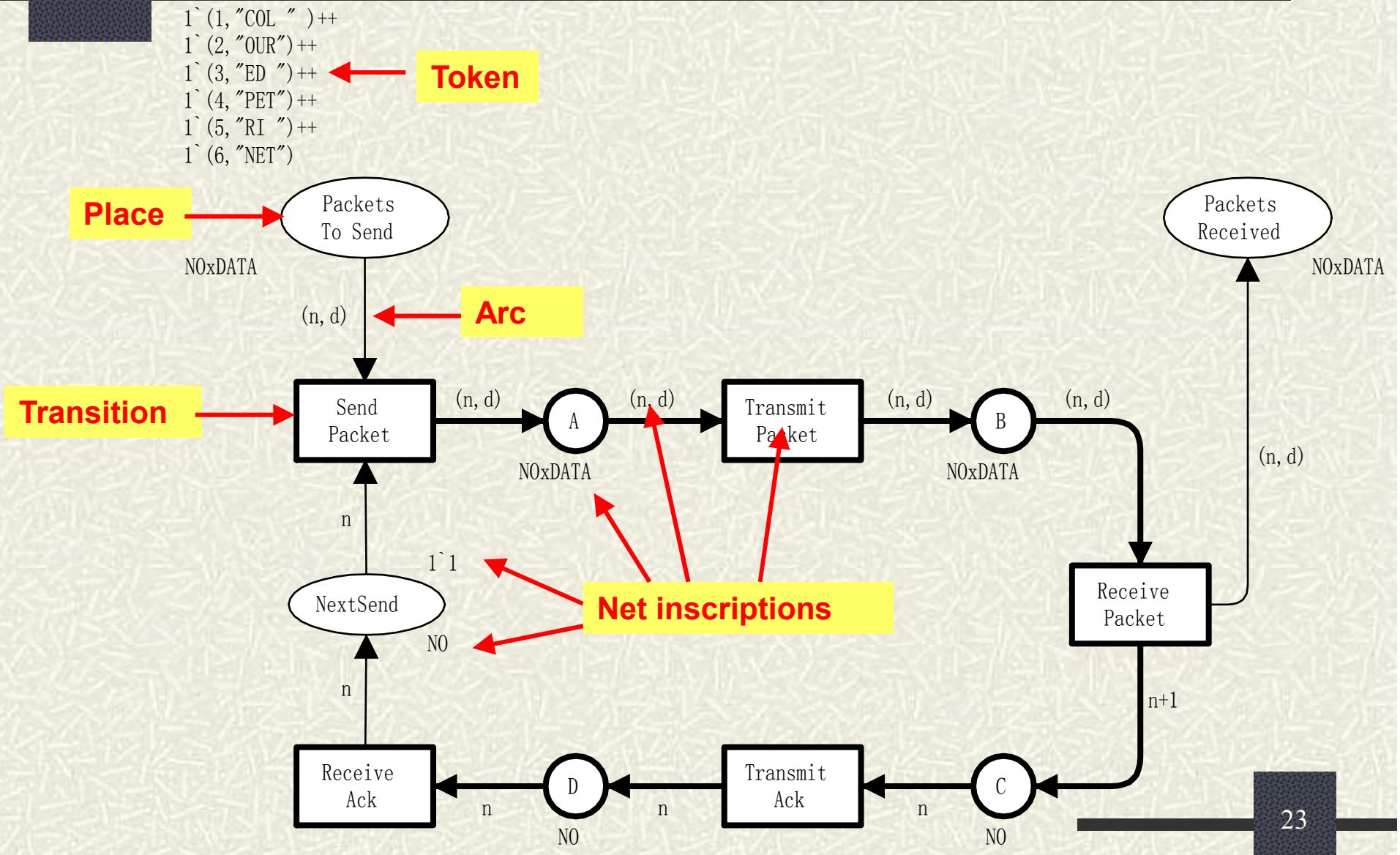
- The traditional models and methods have their limitation, especially for the dynamic character and for the software part of the I&C system.
- The NRC Technical reference NUREG/CR-6901 reports that the Petri Net is one of the possible methodologies to model the D-I&C

Methodology-Petri Net





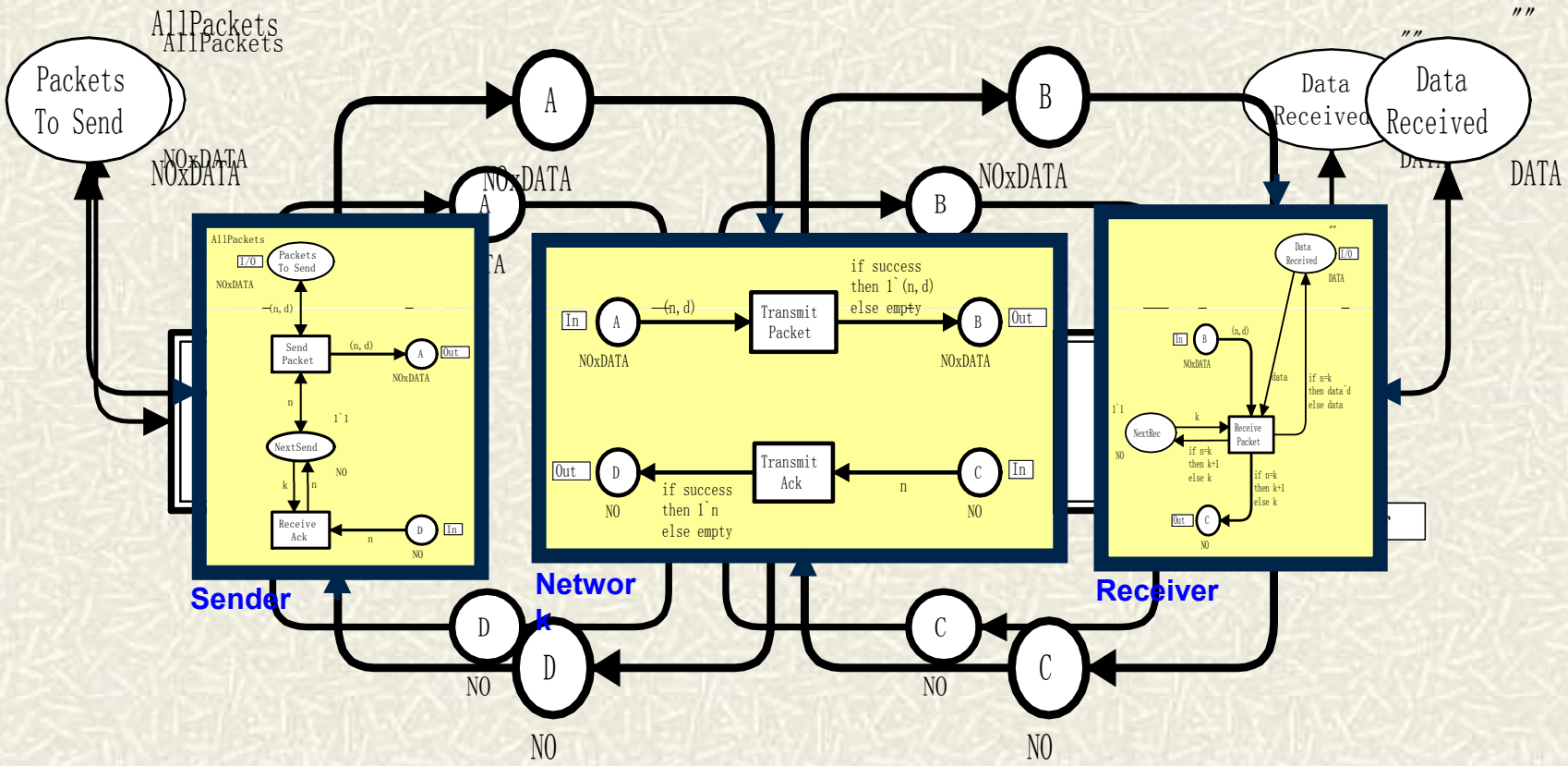
Methodology-Colored Petri Net



Methodology-Differences

Type Items	Petri Net	Colored Petri Net
Token	Token; Only the nonnegative integer.	Colored Token; Arbitrary data type from simple to complex data and supporting the user defined data type.
Transition	Transferring the tokens that is removing the tokens from the input and produce the tokens for the output.	Transferring the data. The transition can be programmed as the guard. The guard determines whether the transition can be fired. The transition can be programmed as the action. The action can be any user defined function that processes the data in the token.
Arc	Labeled by the nonnegative integer defining the input and output weight.	Arc function re-processes the output value from the transition action processing the data.
Marking	The amount of token in each place.	The data and information in each place defined as the color set.
Firing rule	Meet the input arc labeled weight.	Meet the input arc function. Meet the transition guard condition.

Methodology-Hierarchical CPN

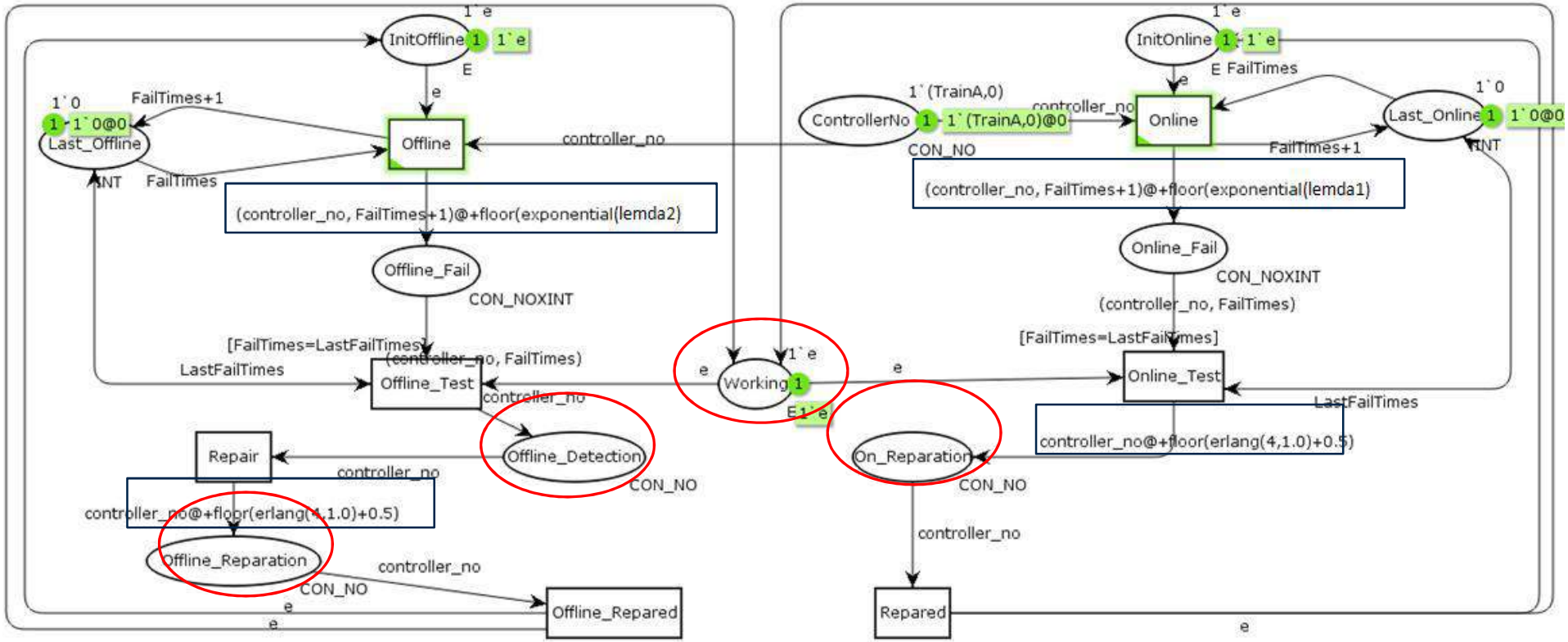


Methodology

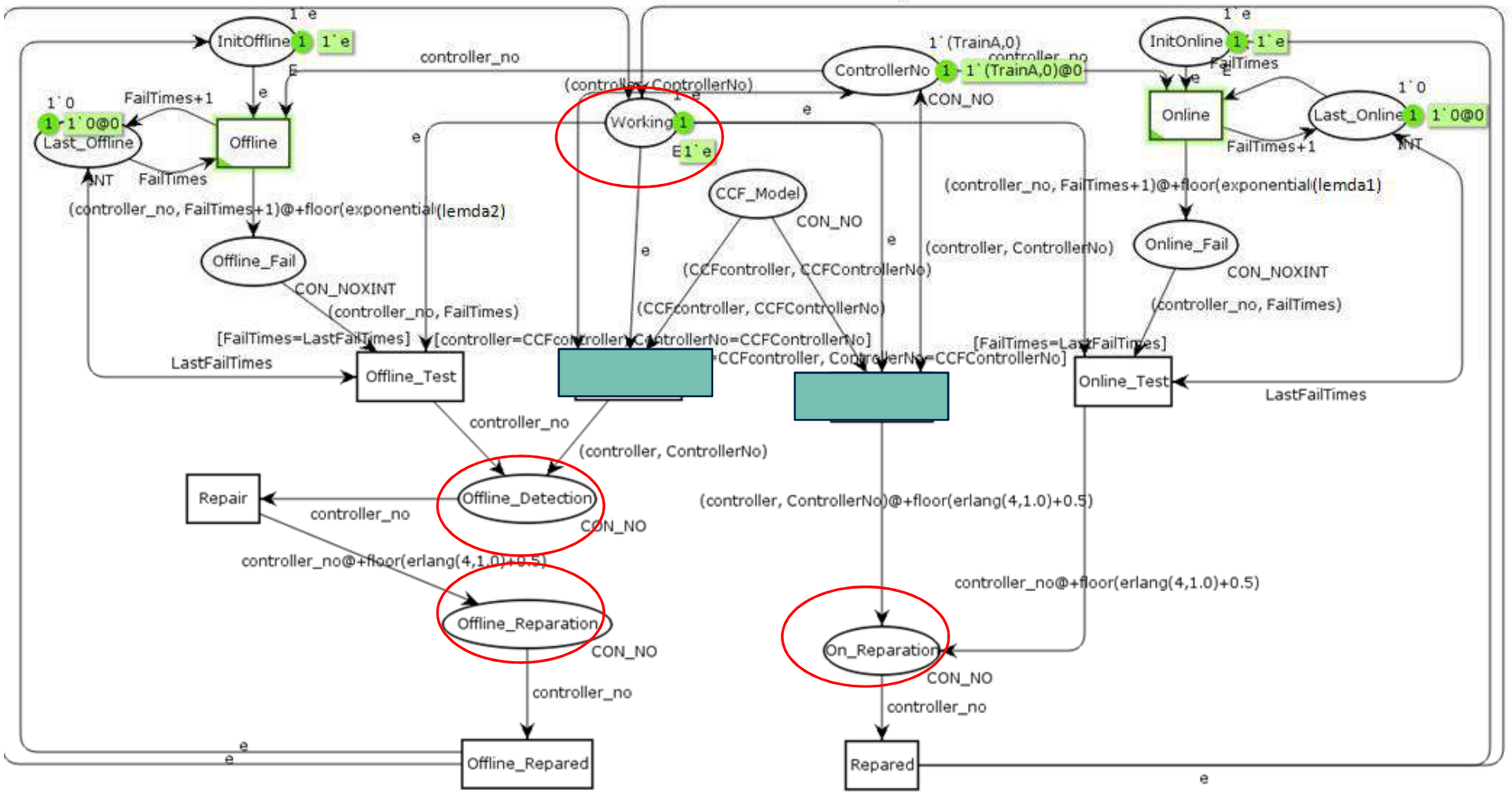
- There is port place and socket place used for the data exchanges of the different level of the model.

	Petri Net	Colored Petri Net	Hierarchical CPN
Application	Low Level Petri net Graphical notation and suited for the theoretical model ● concurrency system ● Hardware system Relatively simple and limited capability.	High Level Petri net Petri Net and Programmed language suited for the practise model as: ● compact modeling ● parameterisable models Industrial application such as: ▪ communication protocols, ▪ data networks, ▪ distributed algorithms, ▪ embedded systems, ▪ business processes and workflows, ▪ manufacturing systems, ▪ agent systems.	High Level Petri net Modeling the complex systems nearly the same with the CPN. Modeling in the hierarchical manner.

Module level CPN model



Module level CPN model



Part 5

Future work

Future work

Currently , the module level CPN model is finished. The following work is:

- The detailed CCF model will be integrated using CPN;
- The system level model for the RPS hardware configuration will be model using CPN;
- The simulation and some reliability indicators will be calculated such as the MTTF.

哈爾濱工程大學

Thanks for your attention

College of Nuclear Science and Technology

mazhanguo2013@163.com

Harbin Engineering University