Global generic model for reliability analysis of the digital instrumentation and control systems

MA Zhanguo[1], YOSHIKAWA Hidekazu[2], and YANG Ming[3]

1. College of Nuclear Science and Technology, Harbin Engineering University, 150001, Harbin, Heilongjiang, China (mazhanguo2013@163.com)
2. College of Nuclear Science and Technology, Harbin Engineering University, 150001, Harbin, Heilongjiang, China (yosikawa@kib.biglobe.ne.jp)
3. College of Nuclear Science and Technology, Harbin Engineering University, 150001, Harbin, Heilongjiang, China (myang.heu@gmail.com)

Abstract: Formal modeling techniques for the analysis of the Digital Instrument and Control system (DI&C) by High level Petri net (HLP-net) is proposed in this paper. HLP-net is an extension of Petri net is a powerful modeling technique to model the discrete event system. The proposed model uses the hierarchical modeling capability of HLP-net, which includes different levels of abstraction, in order to offer quite general and generic method for a large scale DI&C system behavior. This paper uses the digital reactor protection system as the example system that is adopted as the generic model for the safety I&C system. The designer can choose the specific level of abstraction and use the model to simulate and verify the DI&C system design. And both the hardware and software reliability are integrated in the proposed model. By using this proposed model not only the simulation of dynamic behavior is possible, but also the formal verification of the DI&C system properties becomes enabled based on the proposed HLP-net model.

Keyword: dynamic modeling, petri net, formal verification, hierarchical systems, DI&C

1 Introduction

The instrument and control (I&C) systems that protect, control, supervise and monitor the plant process serve as the nervous system of a nuclear power plant. As the historical transition, there are three types of I&C systems that are the traditional analog based system, the analog with digital hybrid system and the fully digital system. The tendency of the I&C system with the IT innovation is that the analog system is replacing by the digital system and the newly constructed NPPs are all adopting the fully DI&C system. In China, the DI&C system application was start from the Qinshan Phase III, with two 700 MW(e) CANDU reactors, and Tianwan-1 and -2, with two 1000 MW(e) VVERs. And the old Nuclear Power Plants (NPPs) are modifying and upgrading the previous designed I&C system such as the KIT/KPS system. The newly constructed NPPs such as CPR1000, AP1000 and the EPR nuclear reactor are all fully DI&C systems.

The main contributions from the I&C system are safety and economics for the NPP. Also new challenges are introduced by the DI&C systems such as the safety, security and licensing-driven issues, the management of the knowledge, the software logic, and so on[1]. And the reliability of the DI&C system becomes the most concerned issues and several groups are working on them. The OECD/NEA Working Group Risk Task Group[2] is working on the digital system reliability field. And a China-EU nuclear cooperation project called HARMONICS - RAVONSICS is working on the reliability evaluation and V&V of software for nuclear safety critical I&C system. Nowadays the DI&C systems are simply and conventionally analyzed using the failure mode and effects analysis (FMEA) and fault tree (FT) modeling in probabilistic risk analyses (PRA) or probabilistic safety assessments (PSA). The goal is to model the DI&C system reliability. However, it is not clear enough which failure modes or at which detailed level the systems are modeled. So the dynamic approaches are still in the trial stage and are difficult to apply in the full NPP PRA models. There is a general consensus that the protection systems should be modeled in PRA, while the control systems can be treated limitedly[2].

High Level Petri nets[3] (HLP-nets) are based on extensions to normal Petri nets. HLP-nets extend the

Received date: April 8, 2015
(Revised date: May 5, 2015)

modeling capabilities of the traditional place transition (P/T) net. HLP-nets tokens can be defined from different data types ranging from simple to complex. The token can encode a vast amount of information that determines transition firing. Places are associated with the pre-defined data type. A transition can be programmed using special constructs and functions. Additional constructs can be used to enable or disable transition firing. Input and output arcs can have expressions and functions related to them. The HLP-net has strong capability to model the discrete event system. The DI&C is a typical timed, concurrent and distributed system. The HLP-net can easily model the DI&C system using the hierarchy capability, the complex data definition capability and the discrete event processing capability.

In this paper, the safety I&C system is focused on and the Reactor Protection System (RPS) is selected as the example system. Using the HLP-net, a dynamic reliability model is proposed. In the model, both the hardware and software reliability are integrated and the verification of the system can be done. In the report, it is said that the Petri Net can be used for the reliability analysis of DI&C system[4].

This paper concerns on the formal reliability modeling of the DI&C based on the HLP-net. The proposed example model which is the generic model can be applied to the whole DI&C system. Also the global behavior of the DI&C hardware and software can be verified using the colored Petri Net (CPN) Tools[6].

The remaining of this paper is organized as following: Section 2 present challenges of modeling the safety I&C system and the informal description of the HLP-net. Section 3 presents the safety I&C system for the reactor protection system (RPS) and analysis of the system failure mode. Section 4 presents the proposed HLP-net model representing the reliability and behavior of a safety I&C system and the simulation result. Section 5 lists the possible uses of the HLP-net model. Section 6 concludes the paper.

2 The high level Petri Net description and advantages for the DI&C

2.1 Challenges of modeling the DI&C system

When modeling the reliability of the DI&C system, the following challenges need to be considered[5].

- At which level of detail of the DI&C hardware system should be modeled, such as the unit level, the component level.
- For the DI&C system, at which level to model the software.
- Not all the failure modes of the DI&C system including the hardware and software are clear enough.
- How to consider software failures.
- The selection of plausible failure data, including failure data for hardware and software is a pending issue.
- How to consider CCF (Common Cause Failure).
- How to account for human errors.

Currently, in the proposed high level model, the CCF and human errors are not modeled.

2.2 Traditional Petri Net

A Petri Net is a directed bipartite graph with vertex subnets places (denoted as circles) and transitions (denoted as rectangles). A directed arc connects a place and a transition. The arc can be either from the place to the transition that is an input arc or from the transition to the place that is an output arc. The places are called the input or output places respectively when connecting with a transition by input or output arc. The place can be assigned a nonnegative number of tokens that are denoted as small filled circles. It is called that the place are marked with the token. The state of a Petri net is characterized by the distribution of the tokens at the places. A Petri Net is defined by its structure which is the static model of the system and its initial state which is the start point of the dynamic model. The arc is labeled with the nonnegative integers which defines the input or output weights. A transition is enabled, if each of its input places contains at least the input weight labeled tokens. And enabled transition can fire, but which enabled transition fires is random. If the transition fires, then the firing remove the input weight labeled tokens from all of its input places and adds the output weight labeled tokens to all of its output places. Thus the token distribution of the places in the Petri Net is changing with the firing of the transition. This is known as the traditional Petri Net.

2.3 High level Petri Net – the extension of the Petri Net

The classic Petri Net that is the P/T net has very limited capability to deal with the different type of information such as the time information, the control algorithm, and so on. And node is explosive with the increase of the system state[3]. The High Level Petri Net (HLP-net) is the extension of the classic Petri Net in the following.

- A signature (Signature is a mathematical structure comprising a set of sorts and a set of operators) defines the domains (Domain is the input set) and the functions that are used in the Petri net. It only names the sorts (Sort is a symbol representing the name of a set) and the operations along with their parameter. For each sort, the signature implicitly defines a multi-set sort which denotes the multi-set over the domain of the original sort. The operations may have the multi-set sorts as parameter sorts as well as result sorts.
- A set of variables along with their type. From the variables and the operations of the signature, terms of the corresponding sorts can be built.
- Each place is equipped with a sort, which defines the domain of the legal tokens on this place. The marking of a place is a multi-set over the corresponding domain. The initial marking of the place is represented by such a term.
- Each arc is annotated with a multi-set term over the sort of the involved place. This term is often called the arc-inscription. The arc-inscription defines which tokens are removed from or added to the corresponding place when the transition fires.
- Each transition is equipped with a term of sort BOOL. This transition guard imposes additional restrictions on the firing of a transition.

Such Petri Net extension composes the HLP-net and including:

- Colored Petri Net (CPN) associate the color to the token which is different from one type of token to the other. Any arbitrary type of data can be defined as the color set. Different type of data used in the DI&C system can be modeled based on its properties. For example, we can define the real color set for the process variables. And the product can define any complicated data type. Also data with the time stamp can be defined and calculated in the CPN.

For example, consider the color set COTROLLER×BOOL timed and associated token (TrainA, true) @0. In this case, it is said that Train A controller is working at the time of 0.

- Timed Petri nets allow modeling the time information related to the hardware status of the DI&C system. Delay of the firing of the transition can be specified based on the definition. The delay can be deterministic or probabilistic.
- Pre and post conditions at the transition enforce the judgment of the event. For example, checking each controller status for the hardware system working status to determine the system is working on 2-out-of-4, 2-out-of-3, 2-out-of-2 or down status.
- Hierarchical HLP-nets allow to break the model into different level of modules that are detailed enough to analyze for different purpose. Each module is called as a sub-model. This function allows the construction of a larger model as a set of smaller models connected to each other using the pre-defined interfaces that are substitution transitions and fusion places. The top model will be much easier to understand while the sub models can be modified and changed independently of the upper module. The upper level model can be made by a set of a substitution transitions. A downer model can be associated with each substitution transitions to model its achievement.

The Petri Net, HLP-net and CPN relationship is summarized in the below Fig. 1. In a word, HLP-net is the extension of the traditional Petri Net and CPN is one kind of the High Level Petri Net.

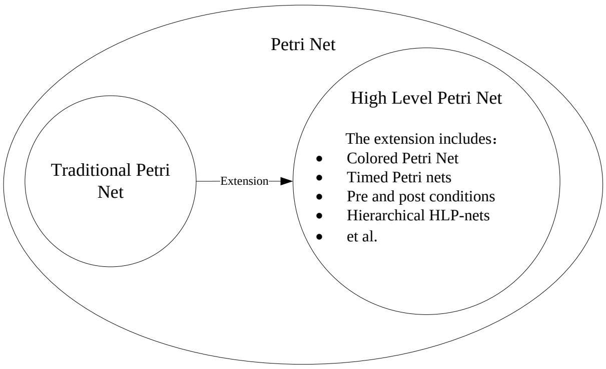


Fig.1 The relationship between Petri Net, HLP-net and Colored Petri Net.

2.4 Colored Petri Net – one example of the HLP-net

In the CPN concept, there is the color set. The color set in the CPN is the definition of the data type that can be used by the model. The color set can be defined from different data types ranging from simple to complex *i.e.* arbitrary type comparing the traditional Petri Net that have only one type that can be assigned to the token. The predefined color set is associated with the Places. Each place is assigned one data type in the color set and this specifies the tokens that the place can have. A colored token is also associated data value that can be of simple or complex type. So the token in the CPN is encoded a vast amount of information that determines the transition firing. The transition can be programmed as the guard and the action. The guard is programmed as the Boolean expression that evaluates to be true or false. The guard determines whether the transition can be fired when the transition is enabled. The action can be programmed as any user defined function which processing the values in the token and calculating the output for the output arcs. For a transition to be enabled the input arcs expression need to bind successfully with the token present in the input places and the transition guard. For the arc in the CPN, there is an arc function comparing the token weight. The arc function can reprocess the output value.

In the CPN Tools, the parameters, complex data types, arc inscriptions, complex firing rules etc. and programmable in functional languages offer a substantial degree of control of the Petri Net in the hierarchical manner.

3 The safety I&C system-reactor protection system in the nuclear power plant

3.1 System architecture and the working flow

The Reactor Protection System (RPS) automatically trips the reactor to maintain the reactor core integrity and the reactor coolant system pressure boundary when the plant process variables approach the specified safety limited conditions. As the RPS is the most important system in the NPP, there are some basic requirements for the safety I&C system design such as single failure criterion, redundancy, defense-in-depth and diversity, independence that prevents propagation of failures, and so on. The architecture, the hardware and software of the digital safety I&C systems are designed to following all the safety-related I&C requirements in NPPs. However, the dissimilarities between different I&C platforms may be significant. It is not only the physical design e.g. some I&C platform is designed based on the PLC (Programmable Logic Controller), some is designed based on the FPGA (Field-Programmable Gate Array) but also the functional design, *e.g.* the failure diagnosis and the logic may differ.

In this paper, a microprocessor based digital safety I&C system is focused on. This safety I&C system achieves high reliability through segmentation of primary and backup trip functions, use of four redundant trains, failed equipment bypass functions, and microprocessor self-diagnostics including data communications. 0 shows the architecture of the system. The RPS is designed and composed of four redundant and independent trains. Four redundant measurements use the separated sensors from the four separated trains which are designed for each variable used for the reactor trip expect the source range and intermediate range nuclear instrument sensors and main turbine stop valve position instrument sensors which only have two trains sensors. The selected analog measured variables are converted to digital by the analog-to-digital converters. After the necessary calculations and processing, the variables are compared against the applied set-point for each one. A partial trip signal for a given variable is generated when one train’s measurement exceeds its limit. Each train sends its own partial trip signal to each of the other three trains over isolated data links. The RPS will generate a reactor trip signal if two or more trains of the same variable are in the partial trip state. Each train of the RPS consists of two separate digital controllers to achieve defense-in-depth through functional diversity. Two different parameters are monitored by the separate sensors that interface to two separate digital controllers within the RPS. Each of controllers process these inputs to generate reactor trip a signals. This two-fold diversity is duplicated in each redundant RPS train. The processing of diverse parameters results in functional redundancy within each RPS train. The reactor trip signal from each of the four RPS trains is sent to a corresponding reactor trip actuation train. Each of the four RT actuation trains consists of two reactor trip breakers. The reactor is tripped when two or more reactor trip actuation trains receive a reactor trip signal.

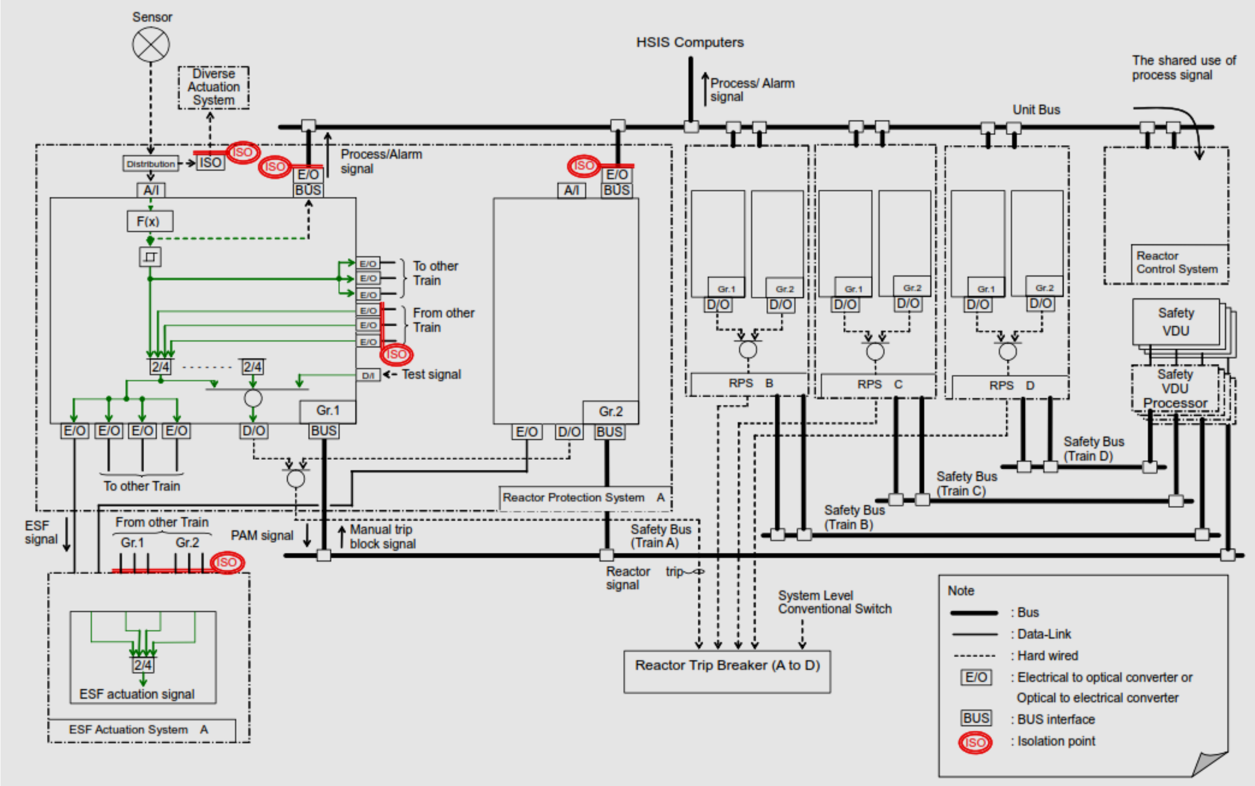


Fig.2 The architecture of the safety DI&C system.

3.2 System failure mode

When modeling the DI&C including the hardware and the software, the first issue that should be determined is that the detailed level for the reliability model. Considering the data that can be used for the reliability analysis, the hardware is modeled in the module level. The hardware is divided into four parts that are input part, processing part, communication part and output part. The FMEA of each part are listed in Table 1.

The FMEA of the hardware are based on the hardware and firmware design.

- For the input part, there are self-diagnosis and cross channel comparison to diagnose the status of the input as the fail high, fail low or as is.
- For the processing part, the self-diagnosis and the alarm are used to diagnose if there is data output.
- For the communication part, only the alarm are used to warn that there is no data output.
- For the output part the alarm and the manual periodic test are used to diagnose the hardware working status.

When each part is failed, there is effect on the logic that is used to cause the reactor trip. And the working mechanism should be modeled in the hardware working logic part. Different part failures have different influences in the DI&C system hardware working logic. And for each failure, it should be modeled. For example, when the RPS input part is fail high the reactor trip logic becomes the 1-out-of-3 from 2-out-of-4. When the RPS input part is fail as, the logic is still 2-out-of-3 of the remaining three trains. All the hardware working mechanism is included in the model as shown in the in the 0.

And the software is divided in two separated parts[5]:

- Platform software (providing the platform for the hardware and software components and tools for the application software design). The platform software performs the basic function and support for the DI&C system such as communication between units, basic system interface and so on.
- Application software (providing the application that is the processing of the process variables). The application software performs the logic in the controller such as the variable limit judgment.

In the current proposed model, the application software part is modeled as the variables processing. The reactor trip and alarm function are treated as the states.

Table 1 Failure mode and effect analysis table

Failure Mode	**Method of Failure Detection**	**Local Failure Effect**	**Effect on Protective Function**
RPS input part - fail high	Self-diagnostic alarm from the affected RPS train. Cross channel comparison.	Bi-stable changes to trip state and partial trip signal is generated in the affected RPS train.	RT logic becomes 1-out-of-3 due to the input failure. Remaining three trains provide reactor trip.
RPS input part - fail low	Self-diagnostic alarm from the affected RPS train. Cross channel comparison.	Bi-stable changes to trip state and partial trip signal is generated in the affected RPS train.	RT logic becomes 1-out-of-3 due to the input failure. Remaining three trains provide reactor trip.
RPS input part - fail as is	Cross channel comparison.	Bi-stable does not change to trip state in the affected RPS train when process reaches to trip level.	RT logic becomes 2-out-of-3 due to the input failure. Remaining three trains provide reactor trip.
RPS Processing part - No data output	Self-diagnostic alarm from the affected RPS train. Annunciation of breaker opened in the affected RTB trains.	Partial trip signal does not reach to other RPS trains when process reaches to trip level. If the processing part is failed, the trip signal from the failed RPS train is provided to the RTB, the breaker is opened in the affected RTB train.	RTB circuit becomes 1-out-of-3 due to the processing failure. Remaining three trains provide reactor trip.
RPS Communication part - No data output	Annunciation of communication error from the affected other RPS trains.	Partial trip signal does not reach to other RPS trains when process reaches to trip level. Trip signals from other RPS trains dose not reach to the affected train when process reaches to trip level.	RT logic becomes 2-out-of-3 due to the communication failure. Remaining three trains provide reactor trip.
RPS Output part - spurious trip	Annunciation of breaker opened in the affected RTB train	Breaker is opened in the affected RTB train.	RTB circuit becomes 1-out-of-3 due to the output failure.
RPS Output part - fail as is	Manual periodic test.	Breaker does not open in the affected RTB train when process reaches to trip level.	RTB circuit becomes 2-out-of-3 due to the output failure.

4 High level Petri Net model for the safety I&C system

The main objective of this work was to develop the global formal models which can represent the reliability of the safety I&C system. Also the obtained models allow the formal validation of the hardware working logic and software control logic for the validation of the design.

When researching the digital safety I&C system, it is treated as to part: hardware and software. Either part has the uncertainty and the logic that can be modeled using the hierarchical HLP-net.

The HLP-net model is made using the software environment of the CPN Tools. The general behaviors of the DI&C systems are:

i. The self diagnosis of the hardware;
ii. The self diagnosis and the cross channel comparison for each variable;
iii. The alarm display and the working logic treatment;
iv. Data processing for each variable.

The model in obtained in three levels hierarchy that are Top Level models, Middle Level models and Low Level models. 0 gives the Top Level model which represents both the hardware and software as the global generic reliability model for the DI&C. The hardware status is calculated and transformed to the software because the software is working based on the hardware status. Each substitution transition models a specific function of the DI&C system.

- The substitution transition “SafetyControlSystem” models hardware reliability of the system.
- The hardware working logic of the system is represented by the substitution transition “HardwareWorkingLogic”.
- The software control logic is modeled by the substitution transition “SoftwareControlLogic”. And there is substitution in this model to model the controller processing.

0 gives the model of the safety I&C system hardware. In the CPN model, the hardware failure phenomena and the reparation are considered. The failure phenomena are considered to follow the exponential law, with the following cumulative distribution function:

$$F(\mathrm{t}) = 1 - e^{-\lambda_c t} \quad (1)$$

where the $\lambda_c = \dfrac{1}{MTTF_c}$ is the rate parameter.

An Erlang law is applied for the repair time. The cumulative distribution function is as the following:

$$F(\mathrm{t}) = 1 - \sum_{k=0}^{n-1} \frac{1}{k!} e^{-\mu_c t} (\mu_c t)^k \quad (2)$$

where $\mu_c = \dfrac{1}{MTTR_c}$ is the rate parameter and $n = 4$ is the order parameter.

0 gives the model of the safety I&C system hardware working logic. If all the four hardware controllers are working, the voter is working on the 2-out-of-four logic. If any one of the four controllers is failed, the voter is working on the 2-out-of-3 logic. If two of the four controllers are failed, the voter is working on the 2-out-of-2 logic. If more than two controllers are failed, the system is down.

0 gives the model of the safety I&C system software data flow. The plant process data is supposed that it can be input from the simulator of the NNP. The plant data is got and parsed in the controller and then the software logic such as the alarm and limit judgment is calculated.

The safety DI&C systems are in most cases implemented on a pre-qualified, or certified, automation system platform.

In the current proposed model, only the application software is modeled and only simulated the variables processing in the controller. The uncertainty model of the software is not considered as there is no software data support the simulation. In the future more detailed software uncertainty model will be developed.

0 gives the logic model used by the application software. It can also model the signal processing flow in the controllers. The data is parsed as the process variables and then judge the logic to generate the reactor trip signal and alarms.

0 gives the definitions of the color set, variables, and functions.

5 The use of the HLP-net model

The obtained HLP-net model allows the simulation and the formal analyses of the DI&C system reliability and the formal verification of the hardware and software logic.

5.1 Reliability assessment using the simulation

The reliability assessment is carried out by means of Monte Carlo simulation that is the only way for the performance evaluation when Markovian hypothesis is not verified due to the Erlang laws that modeling the repair process. The following indicators can be assessed: the availability, MTTFF, MTBF and MTTR for the entire system and for each controller. The probability is assessed by the ratio between the average marking of the places that describe the states characterizing the searched indicator and the sum of the average marking of all places belonging to the invariants.

These indicators are measured by the indicator defined as:

$$P\left(state_I\right)=\frac{M^*\left(state_I\right)}{\sum\limits_{P_i\in P_{subset_I}} M^*\left(P_i\right)} \qquad (3)$$

where $state_I$ is the state that characterizes the probabilistic indicator I, $M^*\left(state_I\right)$ is the average marking and P_{subset_I} is the places subset of invariant.

The reliability data of the non-safety I&C system that is used for the simulation is listed in the table 2.

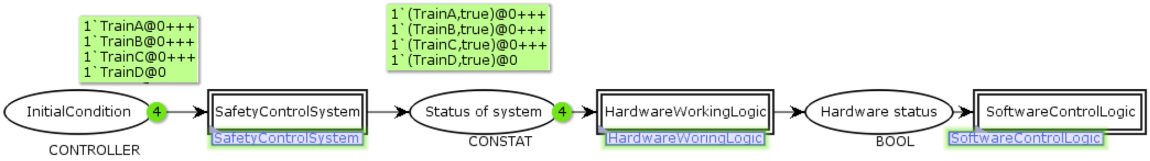


Fig.3 Top Level: The DI&C global generic reliability model integrate the hardware and software.

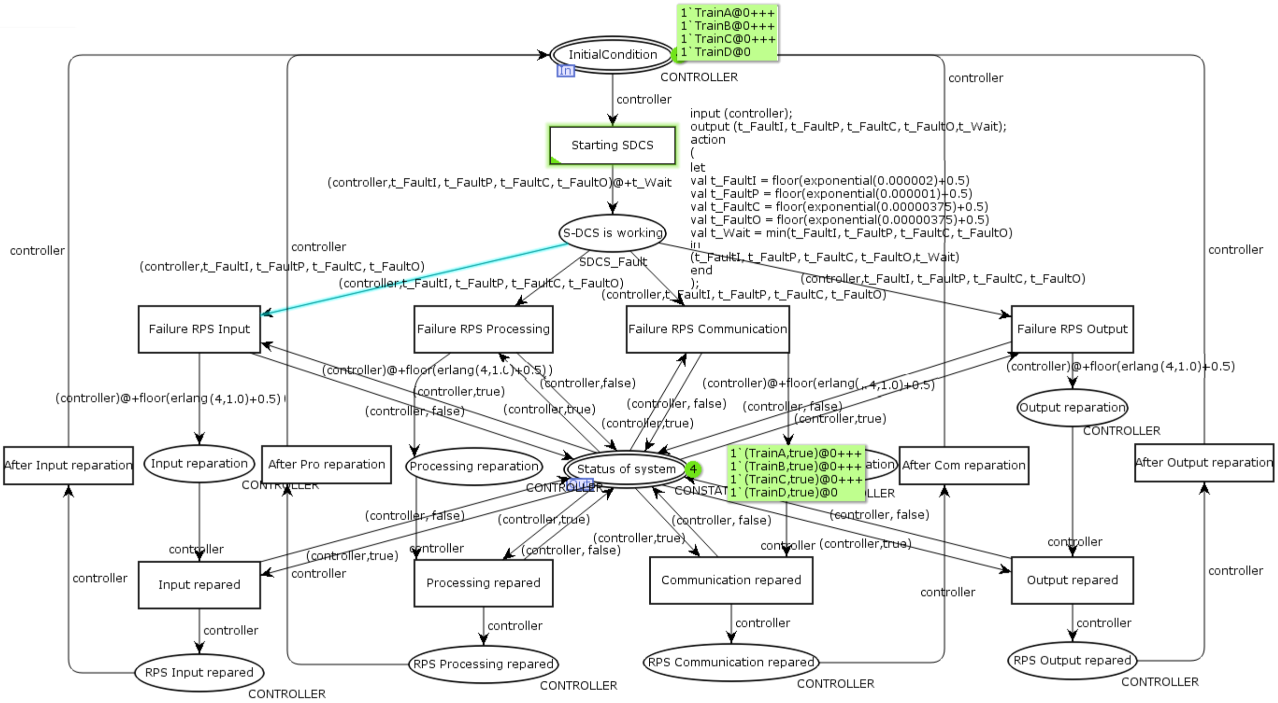

```
input (controller);
output (t_FaultI, t_FaultP, t_FaultC, t_FaultO,t_Wait);
action
(
let
val t_FaultI = floor(exponential(0.000002)+0.5)
val t_FaultP = floor(exponential(0.000001)+0.5)
val t_FaultC = floor(exponential(0.00000375)+0.5)
val t_FaultO = floor(exponential(0.00000375)+0.5)
val t_Wait = min(t_FaultI, t_FaultP, t_FaultC, t_FaultO)
in
(t_FaultI, t_FaultP, t_FaultC, t_FaultO,t_Wait)
end
);
```

Fig.4 Middle Level: Hardware logic.

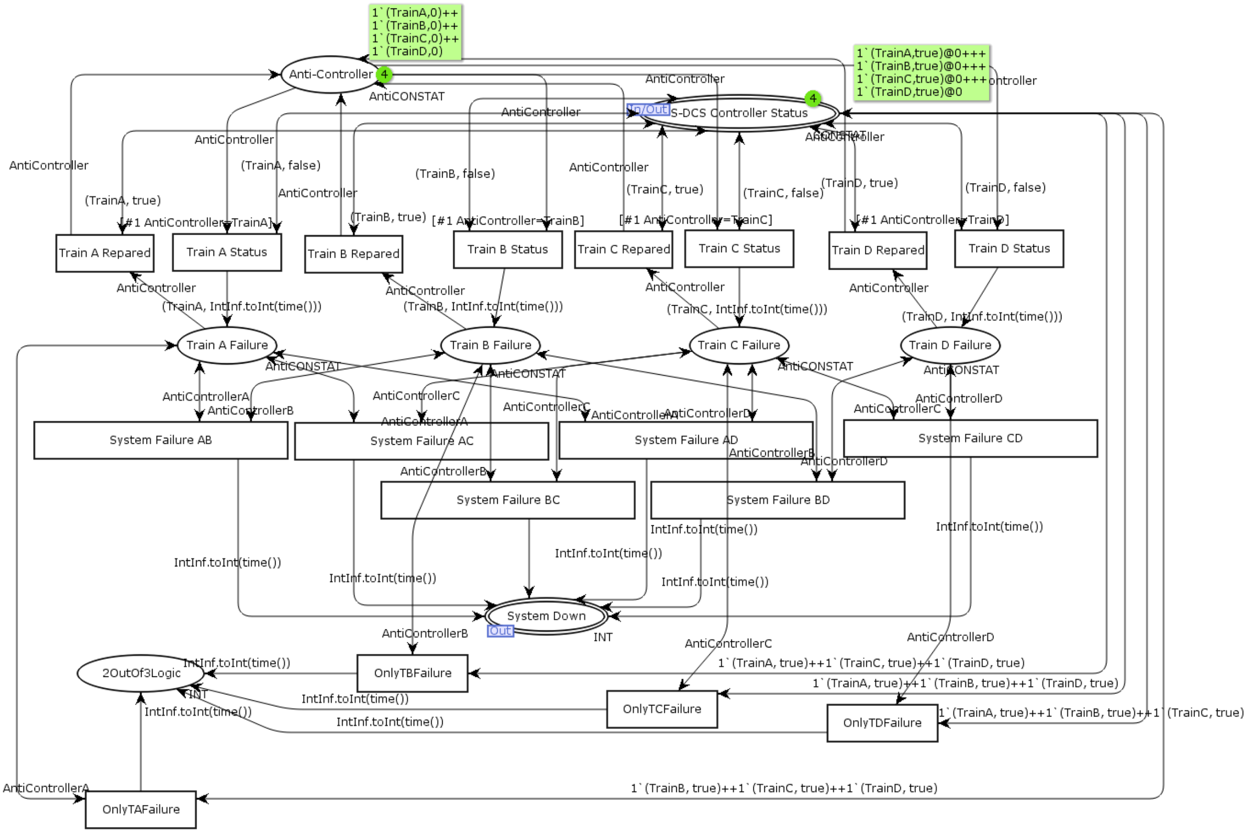
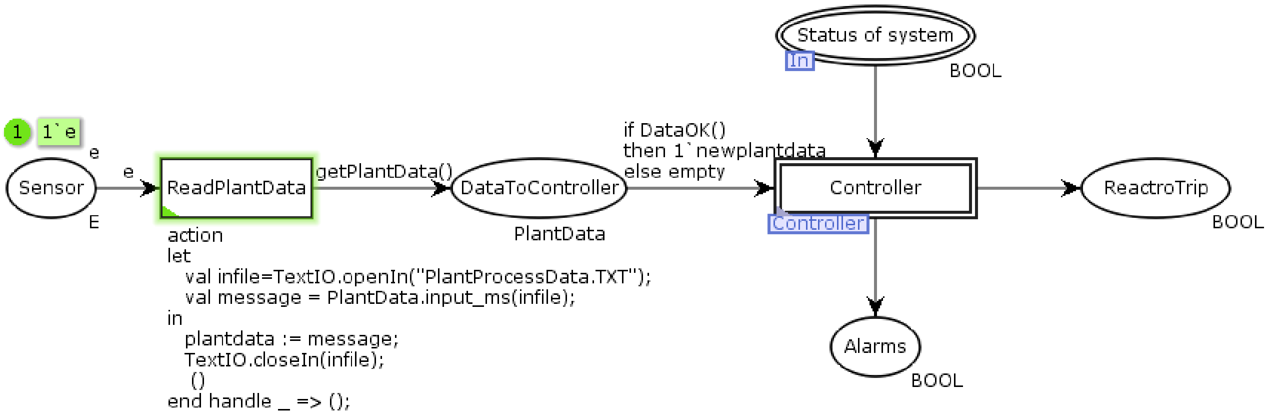


Fig.5 Middle Level: Hardware working status.



```
action
let
   val infile=TextIO.openIn("PlantProcessData.TXT");
   val message = PlantData.input_ms(infile);
in
   plantdata := message;
   TextIO.closeIn(infile);
    ()
end handle _ => ();
```

Fig.6 Middle Level: Software control model.

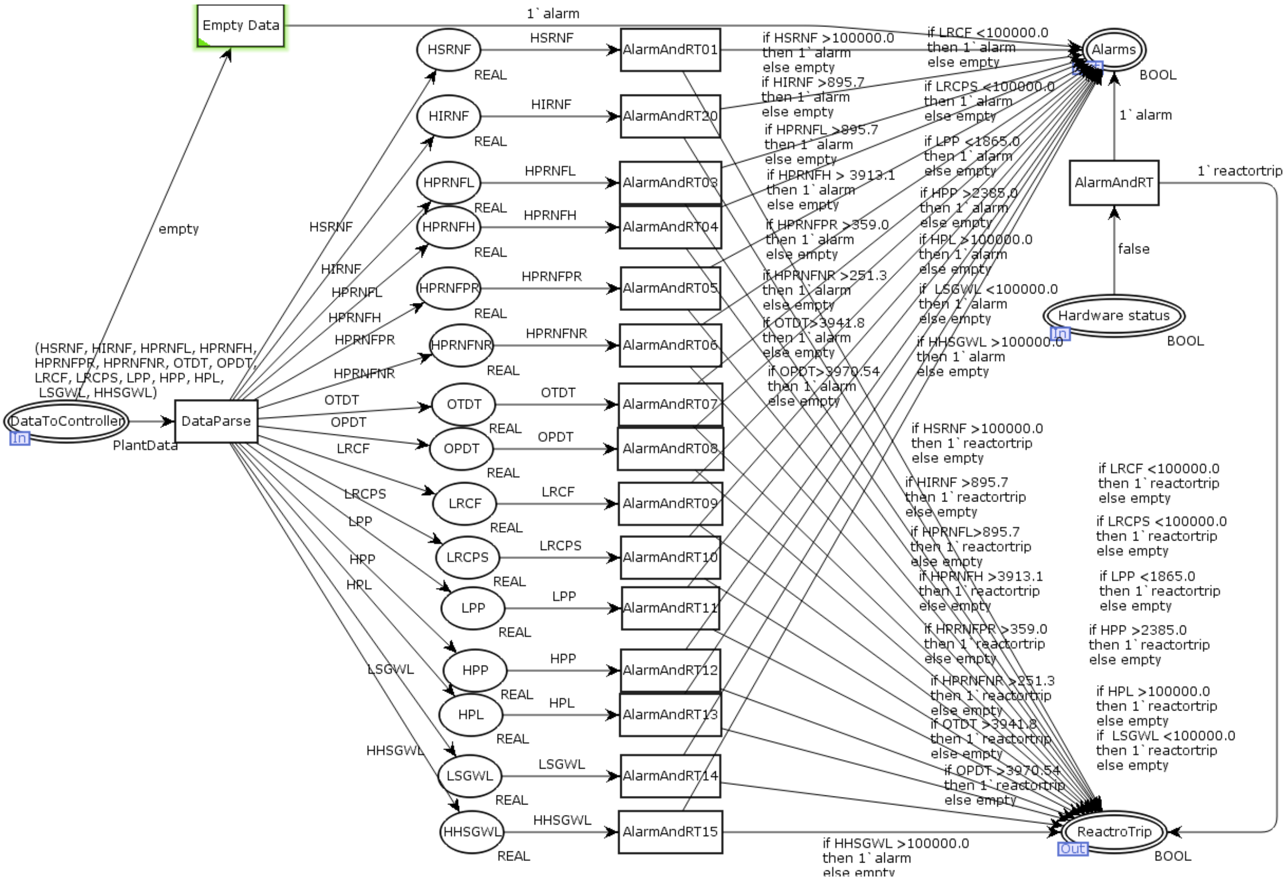

Empty Data
1`alarm
empty
DataToController
In
PlantData
DataParse
(HSRNF, HIRNF, HPRNFL, HPRNFH, HPRNFPR, HPRNFNR, OTDT, OPDT, LRCF, LRCPS, LPP, HPP, HPL, LSGWL, HHSGWL)
HSRNF
HIRNF
HPRNFL
HPRNFH
HPRNFPR
HPRNFNR
OTDT
OPDT
LRCF
LRCPS
LPP
HPP
HPL
LSGWL
HHSGWL
REAL
AlarmAndRT01
AlarmAndRT20
AlarmAndRT03
AlarmAndRT04
AlarmAndRT05
AlarmAndRT06
AlarmAndRT07
AlarmAndRT08
AlarmAndRT09
AlarmAndRT10
AlarmAndRT11
AlarmAndRT12
AlarmAndRT13
AlarmAndRT14
AlarmAndRT15
if HSRNF >100000.0 then 1`alarm else empty
if HIRNF >895.7 then 1`alarm else empty
if HPRNFL >895.7 then 1`alarm else empty
if HPRNFH > 3913.1 then 1`alarm else empty
if HPRNFPR >359.0 then 1`alarm else empty
if HPRNFNR >251.3 then 1`alarm else empty
if OTDT>3941.8 then 1`alarm else empty
if OPDT>3970.54 then 1`alarm else empty
if LRCF <100000.0 then 1`alarm else empty
if LRCPS <100000.0 then 1`alarm else empty
if LPP <1865.0 then 1`alarm else empty
if HPP >2385.0 then 1`alarm else empty
if HPL >100000.0 then 1`alarm else empty
if LSGWL <100000.0 then 1`alarm else empty
if HHSGWL >100000.0 then 1`alarm else empty
Alarms
BOOL
1`alarm
AlarmAndRT
1`reactortrip
false
Hardware status
In
BOOL
if HSRNF >100000.0 then 1`reactortrip else empty
if HIRNF >895.7 then 1`reactortrip else empty
if HPRNFL>895.7 then 1`reactortrip else empty
if HPRNFH >3913.1 then 1`reactortrip else empty
if HPRNFPR >359.0 then 1`reactortrip else empty
if HPRNFNR >251.3 then 1`reactortrip else empty
if OTDT >3941.8 then 1`reactortrip else empty
if OPDT >3970.54 then 1`reactortrip else empty
if LRCF <100000.0 then 1`reactortrip else empty
if LRCPS <100000.0 then 1`reactortrip else empty
if LPP <1865.0 then 1`reactortrip else empty
if HPP >2385.0 then 1`reactortrip else empty
if HPL >100000.0 then 1`reactortrip else empty
if LSGWL <100000.0 then 1`reactortrip else empty
if HHSGWL >100000.0 then 1`alarm else empty
ReactroTrip
Out
BOOL

Fig.7 Low Level: Controller logic model.

Table 2 The reliability data for the I&C components

Component	Description	Failure rate [/h]	Repair time
CPU	Processor Module	2.00E-06	4 hours
DIM	Digital Input Module	4.00E-06	
DOM	Digital Output Module	7.50E-06	
AIM	Analog Input Module	7.50E-06	
AOM	Analog Output Module	7.50E-06	
COM	Communication Module	7.50E-06	

Table 3 System performance simulation results

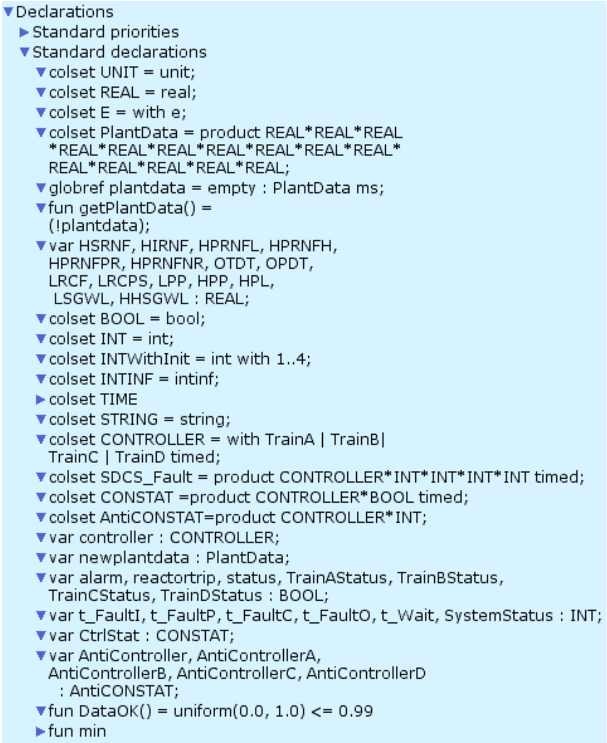
Indicator	Train A	Train B	Train C	Train D	Whole system
MTTFF (in hour)	94266.267	94393.8	102632.367	96953.2	/
MTBF (in hour)	96643.8765	94596.19438	93460.87407	98895.99853	/
MTTR (in hour)	4	3.996254682	3.924109209	3.986764706	/
Unavailability (%)	0.0000414	0.0000422	0.0000420	0.0000403	0

In the CPN Tools this indicators are indicated by monitor functions that are the functions developed in Standard ML language used to inspect the CPN during its simulation. In this paper, four types of indicators are monitored and calculated. They are MTTFF (Mean Time To First Failure), MTBF (Mean Time Between Failures), MTTR (Mean Time To Repair) and Unavailability. For MTTFF the monitor should record the time of the first entity failure. For the MTBF, the monitor should record every failure time. For the MTTR, the monitor should record the every reparation time. The unavailability should record the duration of the state while the system is not working. The calculation result for the indicators is listed in the table 3.

Based on the simulation and calculation results, the following conclusions for the non-safety I&C system can be got:

1. The indicators for the each train system are nearly the same as the components for each system are identically same.
2. As the reparation time for each component is really short comparing with the MTBF. So the availability of each system is very high.
3. As the component is successfully repaired after every component failure, there is no failure occurrence for the whole I&C system during

the simulation. The availability for the whole system is 100%.



```
▼Declarations
  ▶Standard priorities
  ▼Standard declarations
    ▼colset UNIT = unit;
    ▼colset REAL = real;
    ▼colset E = with e;
    ▼colset PlantData = product REAL*REAL*REAL
     *REAL*REAL*REAL*REAL*REAL*REAL*REAL*
     REAL*REAL*REAL*REAL*REAL;
    ▼globref plantdata = empty : PlantData ms;
    ▼fun getPlantData() =
     (!plantdata);
    ▼var HSRNF, HIRNF, HPRNFL, HPRNFH,
     HPRNFPR, HPRNFNR, OTDT, OPDT,
     LRCF, LRCPS, LPP, HPP, HPL,
      LSGWL, HHSGWL : REAL;
    ▼colset BOOL = bool;
    ▼colset INT = int;
    ▼colset INTWithInit = int with 1..4;
    ▼colset INTINF = intinf;
    ▶colset TIME
    ▼colset STRING = string;
    ▼colset CONTROLLER = with TrainA | TrainB|
     TrainC | TrainD timed;
    ▼colset SDCS_Fault = product CONTROLLER*INT*INT*INT*INT timed;
    ▼colset CONSTAT =product CONTROLLER*BOOL timed;
    ▼colset AntiCONSTAT=product CONTROLLER*INT;
    ▼var controller : CONTROLLER;
    ▼var newplantdata : PlantData;
    ▼var alarm, reactortrip, status, TrainAStatus, TrainBStatus,
     TrainCStatus, TrainDStatus : BOOL;
    ▼var t_FaultI, t_FaultP, t_FaultC, t_FaultO, t_Wait, SystemStatus : INT;
    ▼var CtrlStat : CONSTAT;
    ▼var AntiController, AntiControllerA,
     AntiControllerB, AntiControllerC, AntiControllerD
       : AntiCONSTAT;
    ▼fun DataOK() = uniform(0.0, 1.0) <= 0.99
    ▶fun min
```

Fig.8 The definitions in the HLP-net models.

5.2 Formal Performance verification

The Petri Net is the formal method that is widely used to model the concurrent and distributed system. Comparing with other formal methods such as the FSM (Finite State Machine) and the Markov Chain and so on, the Petri Net methodology can not only simulate using the Monte Carlo simulation but also do the formal validation and verification based on the state space of the Petri Net models.

The proposed HLP-net models allow formal validation of some properties of the system. This validation may be performed based on the state space of the HLP-NET which is directly generated by the CPN tools. The properties that could be verified are:
The deadlock free states: A deadlock is a situation where in two or more components are waiting for the other to finish, and thus neither ever does.

The controller safety property: the controller must immediately restart after it has been repaired.
The controller liveness property which means every state is reachable: from any state, the controller is always possible to restart.

The use of hierarchical model has major advantages. Indeed, add to the ability to make easier the modeling of the complex system, such alternative allows to independently verify each sub-net properties. Hierarchical modeling allows having more compact and understanding models. Using each sub-net makes easier the validation of individual component or task.

6 Conclusions

This paper presents the HLP-net reliability model of DI&C system. The proposed model integrates the hardware and software. The models include not only the hardware and software uncertainty, but also the hardware logic and the controller software control logic.

The proposed model is one of integrated PSA (performance simulation) and deterministic (formal verification) method. This model is the attempt for the model of the nuclear plant DI&C system as there is no common and effective methodology to model it. Hopefully, the model will be integrated with the nuclear plant PSA model.

The models can be simulated to validate the hardware working logic and software control logic in the controller and to analyze the performance of the system. As the HLP-net models, they have several major advantages.

i. They allow the formal validation of the DI&C system properties for the design.
ii. The models are the generic one for the safety DI&C system.
iii. They include different level of abstraction. In the HLP-net, each operation is represented by a transition. When more detail information about the system for a specific model must be included, the corresponding transition will be defined as the substitution transition and added in the model.
iv. In the model, the subnets are substitutable. In one substitution transition, there can be different subnets. Based on the abstraction level, the designer can choose the suitable subnets.

For the proposed model, they also have some disadvantages that need to be considered or improved when modeling the system:

i. The hardware is modeled as input, processing, communication and output parts. If the hardware is considered in more detailed level, the model will be very large and complex.

ii. The model is supposed that the hardware is based on the microprocessor. If the system is designed based on other type such as FPGA, the model need to change.

iii. The uncertainty of the software need to be modeled in more detail.

Acknowledgement

This paper is funded by the International Exchange Program of Harbin Engineering University for Innovation-oriented Talents Cultivation.

References

[1] IAEA: Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series NP-T-3.12 2011.

[2] AUTHÉN STEFAN and HOLMBERG JAN-ERIK, "Reliability Analysis of Digital Systems In A Probabilistic Risk Analysis For Nuclear Power Plants". Nuclear Engineering and Technology, Vol.44 No.5, pp 471-482 2012.

[3] Final Draft International Standard ISO/IEC 15909 "High-level Petri Nets - Concepts, Definitions and Graphical Notation", 2000.

[4] CHU T.-L., YUE M., MARTINEZ-GURIDI G. and LEHNER J., "Review of Quantitative Software Reliability Methods", BNL-94047-2010, Brookhaven National Laboratory 2010.

[5] HAAPANEN P., HELMINEN A., PULKKINEN U.: "Quantitative reliability assessment in the safety case of computer-based automation systems", STUK-YTO-TR 202, STUK, Helsinki 2004.

[6] JENSEN Kurt, KRISTENSEN Lars Michael, WELLS Lisa: "Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems", Int J Softw Tools Technol Transfer (2007) 9: pp 213-254.