Verification of a primary-to-secondary leaking safety procedure in a nuclear power plant using coloured Petri nets

E. Németh [a] T. Bartha [a,*] Cs. Fazekas [b,a] K. M. Hangos [a]

[a] *Systems and Control Laboratory, Computer and Automation Research Institute, Budapest, Hungary*

[b] *Dept. of Information Systems, University of Pannonia, Veszprém, Hungary*

Abstract

This paper deals with formal and simulation based verification methods of a primary-to-secondary leaking (abbreviated as PRISE) safety procedure. The PRISE safety procedure controls the draining of the contaminated water in a faulty steam generator when a non-compensable leaking from the primary to the secondary circuit occurs. Because of the discrete nature of the verification, a Coloured Petri Net (CPN) representation is proposed for both the procedure and the plant model. We have proved by using a non-model-based strategy that the PRISE safety procedure is safe, there are no dead markings in the state-space, and all transitions are live; being either impartial or fair.

Further analysis results have been obtained using a model-based verification approach. We created a simple, low dimensional, nonlinear dynamic model of the primary circuit in a VVER-type pressurized water nuclear power plant for the purpose of the model-based verification. This is in contrast to the widely used safety analysis that requires an accurate detailed model. Our model also describes the relevant safety procedures, as well as all of the major leaking type faults. We propose a novel method to transform this model to a CPN form by discretization. The composed plant and PRISE safety procedure system has also been analysed by simulation using CPN analysis tools. We found by the model-based analysis —using both single and multiple faults— that the PRISE safety procedure initiates the draining when the PRISE event occurs, and no false alarm will be initiated.

Key words: Coloured Petri nets, nuclear power plants, verification of safety procedures
PACS: 28.41.Te, 28.41.Ak, 89.30.Gg

1 Introduction

Nuclear power plants (NPPs) are tightly regulated complex systems, where the issues related to their safety are of primary importance. Therefore, the verification and validation of the applied safety procedures are also essential.

A possible and widely used way of analysing the performance of safety procedures or systems is to perform *safety analysis* to investigate the effects of certain major hazardous faults, such as ruptures, by using detailed simulation. Most often, versions of the RELAP5 code [1] are applied. See e.g. [2] for a Large-Break Loss-Of-Coolant Accident (LBLOCA) fault, or [3] and [4] for a small break LOCA test in a pressurized water reactor (PWR). With the improvement of the codes (see e.g. [5], [6]), more and more complex scenarios could be analysed even for pressurized water vessel-type (VVER) reactors (present in countries of Central and Eastern Europe) [7]. Advanced accident analysis has also been incorporated into safety analysis reports [8]; not only for nuclear power plants [9], but also for nuclear research reactors [10].

The need to apply formal or at least computer-aided verification methods for safety systems has long been recognized, see e.g. [11]. This is especially important for nuclear power plants due to the large number of variables and the complexity of the plant and its dynamic behaviour. A recent paper [12] describes a methodology to use models based on thermal-hydraulic principles to evaluate reliability. The paper integrates the reliability evaluation results into Probabilistic Safety Assessment (PSA). This can be regarded as a continuation of earlier papers, e.g. [13] or [14]. A detailed simulation-based assessment of the emergency operating procedure (EOP) to mitigate the steam generator tube rupture (SGTR) initiating event in a PWR has been reported in [15].

It is well known, that NPPs possess complex nonlinear dynamics during abnormal events. In such circumstances the continuous dynamics is coupled by discrete events generated by the safety and operating procedures, together with operator actions (as demonstrated by the above mentioned safety analyses). This calls for applying the methodology of discrete-continuous hybrid systems [16]. An example, a hybrid stochastic approach for the modelling and analysis of fire safety systems has been presented in [17], where the discrete dynamics is described by Petri nets, and the continuous one is by a differential

* Corresponding author.
Email addresses: nemethe@sztaki.hu (E. Németh), bartha@sztaki.hu (T. Bartha), fazekas@scl.sztaki.hu (Cs. Fazekas), hangos@scl.sztaki.hu (K. M. Hangos).
[1] This work has been supported in part by the Control Engineering Research Group of the HAS at the Budapest University of Technology and Economics, and by the Hungarian Research Fund (OTKA) through grant K67625.

algebraic equation (DAE) model.

The difficulty in combining the traditional safety analysis methods with the verification lies in the problems of incorporating uncertainties related to the malfunctions into the RELAP5 based analysis. There are attempts to solve these problems in certain specific cases, see [18].

The aim of this paper is to propose a unifying approach for the verification of safety procedures in NPPs that strongly utilizes the structure and specialities of the problem domain, and supports both the modelling of the underlying plant dynamics and the verification of the procedures. For this reason, we selected coloured Petri nets (CPNs) [19], [20] as the formalism that allows modelling, formal analysis and simulation-based verification of safety procedures in NPPs.

- CPNs and Markov-graphs have been successfully used for reliability analysis of hybrid systems [21]. Moreover, it was shown in [22] that a process model described in a qualitative DAE form can also be represented as a CPN. Thus, we could use a powerful tool, the Design/CPN [23] to support the modelling of our plant and its safety procedure in the form of a joint CPN and perform the verification by using CPN analysis procedures.
- CPNs have also been successfully applied for modelling and verification of safety-critical software and control components in NPPs. A CPN-based integrated knowledge base development tool for the verification of the dynamic alarm system is introduced in [24]. A software requirements verification methodology based on combined CPN and Prototype Verification System (PVS) methods is described in [25]. Fuzzy CPNs have been used in an automated operating procedure system [26]. Even the human factor, i.e. the properties and dynamics of operator perception and actions could be described using CPNs [27].

The paper is organized as follows. First, we describe the problem statement including a short introduction to the plant and its dynamics, as well as to the investigated PRImary-to-SEcondary leaking (PRISE) safety procedure. Thereafter, our methods and results of the non model-based verification are presented. This is followed by the description of the simple hybrid continuous time state-space model and its CPN form. We developed these models to describe the dynamics of the plant and its relevant controllers, safety procedures and fault events. Our procedures and results of the model-based verification are presented afterwards. Finally, some conclusions are drawn.

2 The PRISE safety procedure and the aim of its verification

The safety procedure analysed in this paper was designed for the Paks Nuclear Power Plant (Paks NPP), located in Hungary. The plant operates four VVER-440/213 type pressurized water reactor (PWR) units with a total nominal (electrical) power of 1860 MW. About 40 percent of the electrical energy generated in Hungary is produced here. Considering the load factors, the Paks units belong to the leading ones in the world and have been among the top twenty-five units for years.

Fig. 1 shows the flowsheet of the primary circuit in Paks NPP (with certain units from the secondary circuit). The main equipment: the reactor, the steam generator(s), the reactor coolant (or primary) pump(s), the pressurizer and their connections are depicted in the figure. The sensors providing on-line measurements are indicated by small black rectangles. The controllers are denoted by double rectangles, their input and output signals are shown by dashed lines.

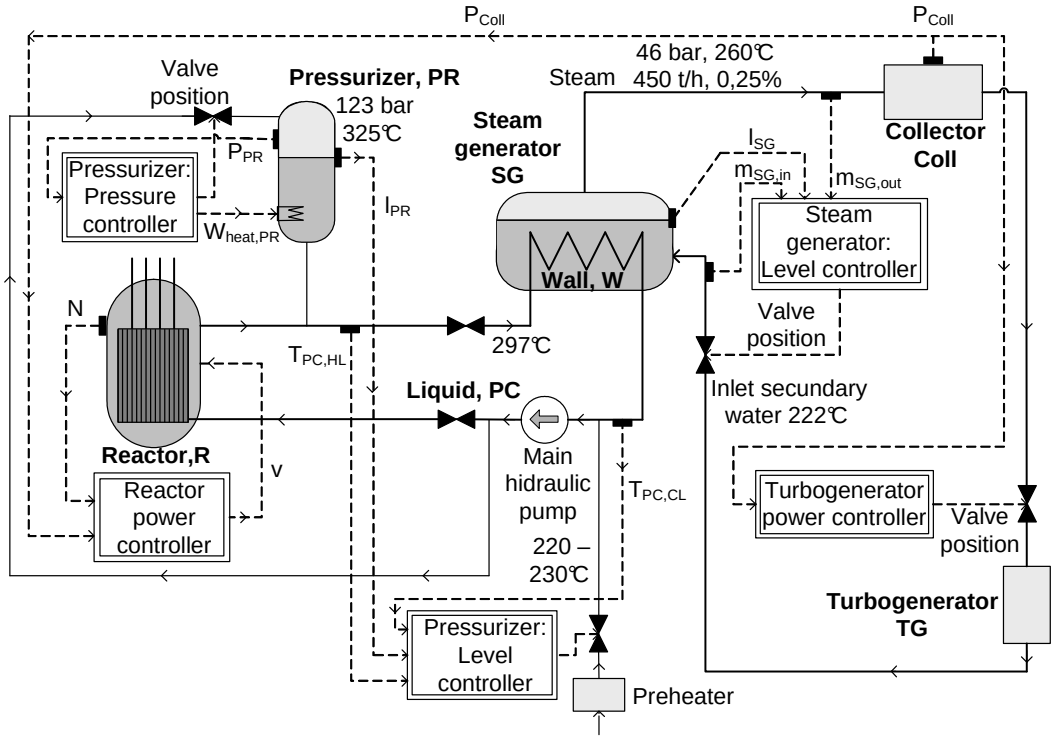

Fig. 1. The primary circuit and its operating units

2.1 The PRISE fault event and its process consequences

The *PRImary-to-SEcondary leaking* (abbreviated as PRISE) is one of the major failures of the NPP. A PRISE event occurs when there is a rupture or other leakage within the steam generator affecting either a few (3-10) tubes or their collector that contain the high-pressure activated liquid of the primary circuit. The PRISE event is the VVER-440/213 analogue of the well investigated Steam Generator Tube Rupture (SGTR) event (see e.g. [15], [28]) in the other pressurized water reactors.

In the unlikely case of a PRISE event, the corresponding safety procedures take care of the reactor trip (i.e. the emergency shutdown of the reactor) and then of the isolation of the faulty steam generator. However, there is a possibility to release some of the contaminated water to the environment, if the event is not handled properly. In order to prevent this possibility, the experts at the plant devised the following solution:

- they added a safety valve to each steam generator that drains the contaminated water into the containment, and
- they developed a new safety procedure, called the *PRISE safety procedure*, to control the operation of these safety valves.

As a preliminary safety analysis step, simulation investigations have been carried out by using a RELAP5 [1] based code fitted to the Paks NPP conditions [29]. These simulations included the PRISE initiating event, and also other major related rupture or leakage type events, such as LOss-Of-Coolant-Accident (LOCA) and leakage in the pressurizer. As a result, the event sequence generated by a PRISE event —when the initial plant state is in its *normal operating mode* and *no other fault occurs*— has been determined as follows (the description uses the notation list in the Appendix in Table 4):

(1) First the decrease of primary circuit pressure p_{PR} is observed that implies the safety event $p_{PR} < 11.2\ MPa$. This causes an automatic reactor trip when the control rods reach their bottom position ($\chi_{RSHUT} = 1$).
(2) When the secondary water and steam mass flowrates fall into a nominal low level, the reactor trip initiates the turbine shutdown. This causes the faulty steam generator water level ℓ_{SG} to increase.
(3) The water level increase will eventually initiate a level alarm in the faulty steam generator ($\Delta\ell_{SG} > +600\ mm$) that automatically initiates the isolation of the faulty steam generator resulting in an even more increase in ℓ_{SG}.

The purpose of the PRISE safety procedure is to initiate the draining *if and only if a PRISE event occurs*. This includes preventing the steam generators from being drained when a fault event (causing similar symptoms but not classified as a PRISE event) occurs, i.e. the PRISE safety procedure should be selective. In order to achieve this behaviour, the fault events causing similar symptoms have been examined by a thorough safety analysis using RELAP5 code [1], and the distinctive event sequence for the detection of the PRISE event has been selected.

When the system is not in a normal operating regime, but is either being started or shut down, the PRISE safety procedure is designed not to be active. The reactor operators manually initiate draining should the need arise.

Faults and operating regimes make the selective detection of a PRISE fault event complicated. Furthermore, one of the key sensors, the water level (ℓ_{SG}) sensor of the steam generators is highly unreliable. It tends to show randomly spuriously high level due to the solid scale content of the secondary water. This measurement error is even more frequent in the transient operation regime. The steam generator water level sensor is not part of the reactor safety system, therefore it is not duplicated.

With the above considerations, the technological and system experts at Paks Nuclear Power plant have designed a timed logical scheme, the *PRISE safety procedure*, in a heuristic way. The description of the inputs and outputs of the PRISE safety procedure is included in Table 1.

The designed safety procedure initiates the draining (OUTPUT-1) when a critical decrease in the primary pressure (INPUT-2 signal) is followed (after a specified time delay) by the increase of the steam generator water level (INPUT-1 signal). However, the draining is initiated only if the containment pressure signal (INPUT-3) keeps its nominal value (i.e. it is not increasing due to another, non-PRISE fault causing an inflow of the primary water into the containment). Also, the INPUT-1 signal must hold its active value for more than a certain time interval, otherwise it is regarded as inactive. This filtering function is used is to prevent the incorrect initiation of draining by the unreliable water level sensor measurement showing temporarily a spuriously high value.

The INPUT-4 and INPUT-9 input conditions inhibit the operation in a startup or shutdown situation. INPUT-5 resets the operation of the PRISE safety procedure after a reactor trip. INPUT-6 and INPUT-7 prevent the erroneous draining of the containment after the isolation of a steam generator caused by a non-PRISE fault.

Table 1
PRISE safety procedure I/O description

Notation	**Short name**	**Description**
INPUT-1	SG level high	Steam generator water level is increasing
	($\Delta\ell_{SG} > +600\ mm$)	(due to closure of the turbine)
INPUT-2	Primary pressure decreasing	The pressure of the primary water is decreasing
	($p_{PR} < 11.2\ MPa$)	(due to the PRISE or other leakage)
INPUT-3	Containment pressure is normal	The pressure of the containment is *not* increasing
	($p_{CN} < 0.1\ MPa$)	(no primary water inflow due to a non-PRISE fault)
INPUT-4	Primary temp. below nominal	Technical condition signifying that the reactor
	($T_{CL} < 245^{o}C$)	is in startup/shutdown operation
INPUT-5	Control rods fully down	Technical condition used to reset the operation
	($\chi_{RSHUT} = 1$)	of the PRISE safety procedure
INPUT-6	SG deltaP	Technical conditions to avoid erroneous draining of
INPUT-7	SG RAP 1/2	secondary water after isolation of steam generator
INPUT-8	SG inhibition	Technical condition used to take
		the SG inhibited state into consideration
INPUT-9	Primary pressure low	Technical condition signifying that the reactor
	($p_{PR} < 5\ MPa$)	is in startup/shutdown operation
OUTPUT-1	GFINH1 (SG is inhermetical)	Primary output of the PRISE safety procedure
		activating the secondary water drain
OUTPUT-2	ACTIVE	Auxiliary output used in control operations

The primary OUTPUT-1 of the procedure shows the presence of a PRISE event. Note that the auxiliary OUTPUT-2 signal indicates the presence of all but one of the symptoms of the PRISE situation.

3 Formal verification using coloured Petri nets

There are several approaches presented in the literature to the problem of formal verification and validation of programmable logic controller (PLC) based industrial control and monitoring systems. The interested reader can find many examples and case studies in the references [11], [30], and [31]. We refer to the classification presented in [32], which groups the existing methodologies according to three main aspects: *approach*, *description formalism*, and *analysis method*. Two important types of approaches can be distinguished:

- **Model based:** in these solutions a model of the process under control is included in the analysis. The properties checked by verification are statements on the controlled system.
- **Non model based:** these approaches analyse the formal description of the control system/algorithm without taking into account the process and its characteristics.

3.1 Coloured Petri net model of the PRISE safety procedure

Our choice for the description formalism of the PRISE safety procedure is the Coloured Petri net (CPN) [33]. CPN is an extension of Petri nets: most important differences are that places can contain coloured tokens (i.e. multi-sets) that can symbolize the data content in data flow models, and that CP nets are hierarchically structured using substitution transitions and subnets.

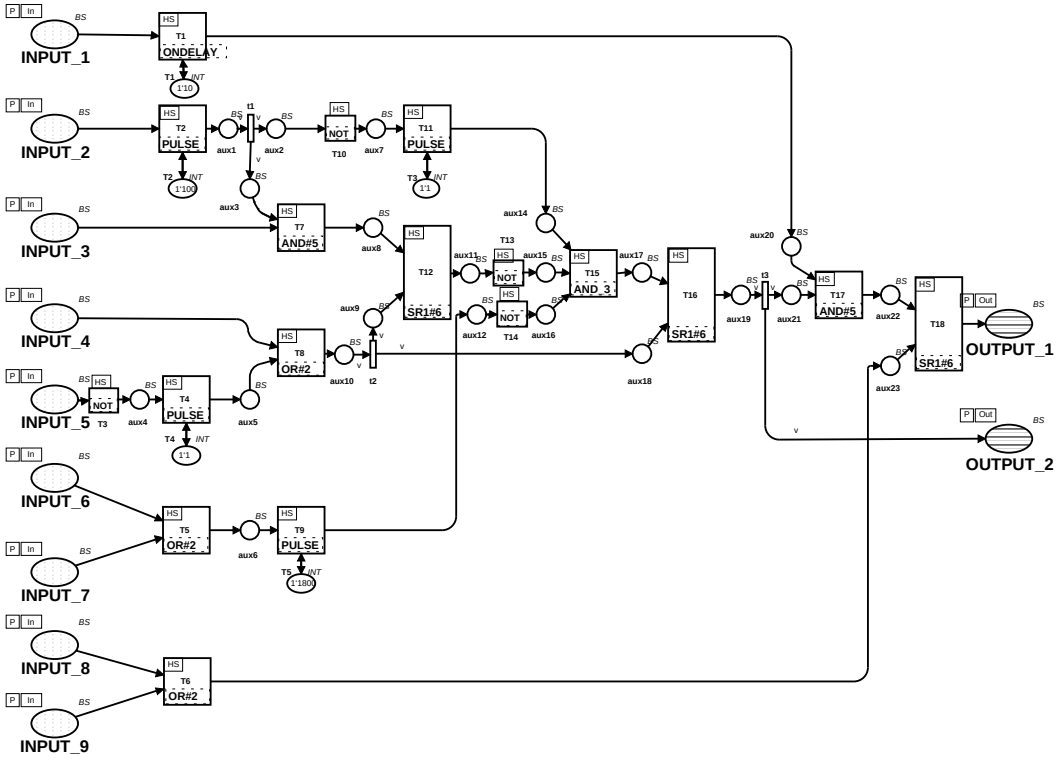

Fig. 2. The Coloured Petri net model of the PRISE safety procedure

Fig. 2 shows the high-level prime page of our CPN model. The larger rectangles are substitution transitions that denote subnets of the corresponding function blocks. The smaller net elements are simple places and transitions that are only needed for connecting the subnets.

The verification of the CPN model includes two major classes of checked properties: common attributes corresponding to the run-time environment in the digital control system (DCS), and problem-specific requirements concerning the PRISE safety procedure.

The run-time environment is a highly dependable digital process control computer. This uses a 50 millisecond long scan cycle. During each scan cycle the controller first samples its inputs, then evaluates all of its functional diagram pages, computes its new internal state, and sets the outputs. In the remaining time it performs self-tests.

In the CPN model the propagation of the tokens represents the flow of data through the functional diagram. In each scan cycle of the model a single coloured token is put into each input place. The colour of the input tokens carries the input data value. These tokens initiate the evaluation of the subnets modelling the function blocks. When every subnet has been evaluated, a single coloured token is generated into each output place, and the scan cycle ends. The CPN model has a feedback loop (not included in Fig. 2) that takes away every generated token from the outputs and simultaneously puts a new token into every input place, so that a new scan cycle can begin.

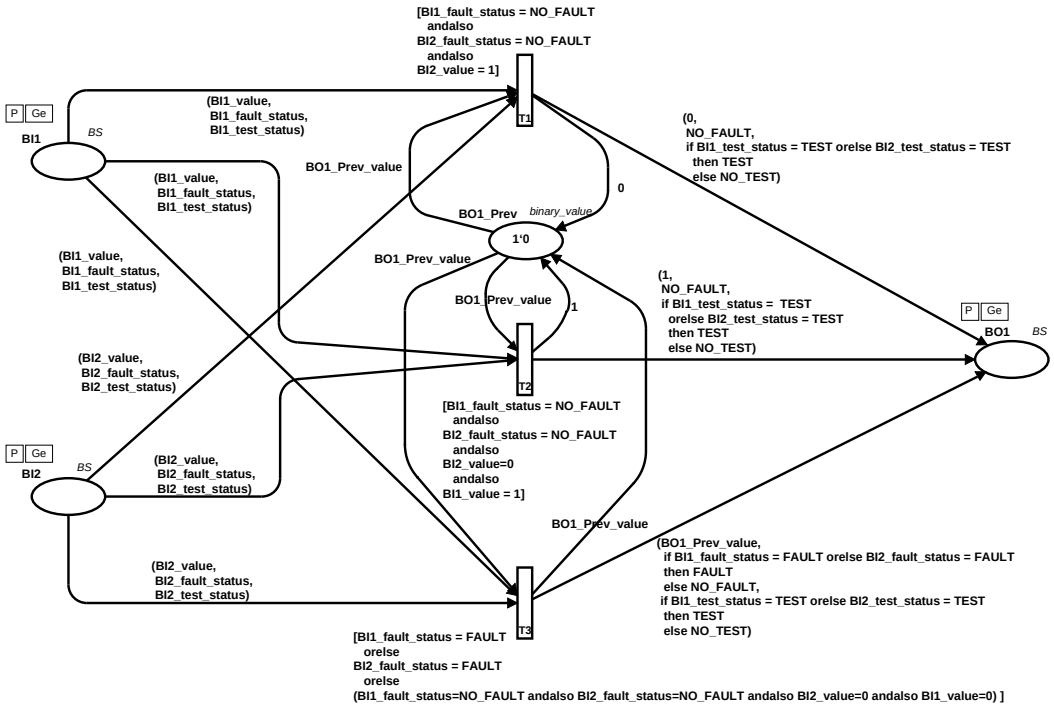

Fig. 3. The CPN subnet model of the SR1 function block

Fig. 3 presents the CPN model of the SR1 function block (Static RS flip-flop, preferred state on reset, priority on reset) mentioned in the timed logical description of the PRISE safety procedure. This subnet is substituted for each instance of the SR1 transition in the high-level model in Fig. 2. If the Set input is activated (BI1 input place is marked with a token coloured with value 1), the output is set to active (BO1 output place receives a token coloured with value 1). Similarly, the activation of the Reset input (BI2 input place) makes the output inactive (a coloured with value 0 is put into the BO1 output place). When both inputs are active, the Reset function dominates. With both inputs inactive, or when any of the input signals is invalid, then the SR1 function block maintains the actual state of the output signal. Initially the output is inactive.

3.2 Analysis of the coloured Petri net model

The advantage of Petri net and CPN models is that they have a broad selection of analysis techniques; some of which even avoid the state explosion problem [34]:

- **Structural analysis techniques** construct no state space at all, because they work directly on the structure of the Petri net. Results are *structural properties* and *invariants* (place or transition invariants).
- **Dynamic (reachability) analysis techniques** are based on the exhaustive construction and exploration of the state space (reachability graph). Dynamic analysis can be used even if a desired system property cannot be determined by structural analysis.
- **The lazy state space construction** method is also available to build reduced (interleaving) state spaces. The reduction is based on an appropriate equivalence function, which maps several equivalent states into one.

In addition to these techniques, many analysis tools based on Petri nets (e.g. PEP, PROD, Design/CPN) allow the verification of the model by checking *temporal expressions* using an integrated *model checker*.

3.2.1 Non-model-based results: dynamic properties of the PRISE CPN

The results of the dynamic analysis of the PRISE CPN provide a lot of important information for verification. The *dynamic properties* of the coloured Petri net model of the PRISE safety procedure are summarized in Table 2.

Table 2
Dynamic properties of the PRISE CPN model

Property	**Result**
Boundedness	The PRISE CPN is *multi-set bounded*.
	The PRISE CPN is *safe in the integer sense*.
Liveness	The PRISE CPN with feedback is *deadlock-free*.
	All transitions related to the primary output signal are *live*.
Fairness	Each live transition is at least *impartial* or *fair*.

Since all places in the net are *multi-set bounded*, the model has a finite (albeit large) state space. The *upper multi-set bounds* of places describe the operational range of the corresponding signals. The *lower multi-set bounds* of places prove that the resources (such as the inner state of the time dependent blocks) are preserved. The corresponding places contain a token in all states of the operation.

The net is *safe in the integer sense*, meaning that each place contains at most one coloured token in any state. This partially confirms that the both the intended data-flow behaviour and the functional structure is correctly expressed in the CPN model.

The PRISE CPN with the feedback loop is *deadlock-free*, therefore there are no dead markings. The safety logic will not "freeze" in any state of operation. All transitions involved in the activation of the primary output signal (OUTPUT-1) are *live*. Thus, the PRISE safety procedure is able to activate the emergency activity, and retains this capability during the whole operation.

The fairness property of each live transition is at least impartial or fair. This implies both of these two important attributes:

(1) they can fire infinite times, that is the functionality is repeatable, and
(2) neither "domination", nor "starvation" of the activities can occur.

3.2.2 Non model based results: CPN model checking

After the dynamic analysis of the CP net model we can see the basic characteristics of the PRISE safety logic, and have partially verified our model. However, there are also selectivity requirements concerning the PRISE, divided into two main types:

- *always if PRISE occurs* in every normal operation regime coupled with *sensor fault in* ℓ_{SG} that is highly unreliable,
- *never if PRISE does not occur* even if severe faults causing similar symptoms occur.

We can translate these requirements into verification goals the following way:

- **Operational requirement** ("it is always true that something good will eventually happen"): the PRISE safety procedure is always activated when a real PRISE accident has occurred (no actuation masking).
- **Safety requirement** ("something bad never happens" [34]): the draining of the secondary water is not activated if not a real PRISE accident has occurred (no erroneous actuation).

Although the PRISE safety procedure is relatively simple, its complete state-space is immense (it has approx. 10^{14} states) due to its cyclic operation (modelled by the feedback loop), and the internal sequential function blocks (the flip-flop, pulse and delay blocks). Thus, an exhaustive analysis of the state-space cannot be performed with most of the analysis tools (including our chosen tool, the Design/CPN).

Therefore we need to partition the state space in the non model based to be able to perform our analysis. We can analyse parts of the state space by defining constrained input scenarios. In our case study, we examined the initiation of the OUTPUT-1 (secondary water draining activation) signal under nominal conditions. Thus, all the input signals had either constant values or step-function values, except the "SG level high" (INPUT-1) signal. These inputs were set to match the activation conditions of the OUTPUT-1 signal. The level measurement is unreliable, therefore the INPUT-1 received a random, non-deterministically chosen binary value.

In order to prove the safety and operational requirements, we have proved several subconditions using both state space search methods and model checking:

(1) The OUTPUT-2 and OUTPUT-1 signals are activated in *all trajectories of the state space* (this is an operational condition, since the initial activation conditions are always present in the scenario under analysis).
(2) In all trajectories of the state space the OUTPUT-1 signal *can only be activated after the OUTPUT-2 signal*, and not in the reverse order.
(3) *Neither* the OUTPUT-2 nor the OUTPUT-1 signal *can be activated incorrectly* by the 'SG level high' signal when the enabling conditions are not present (that is while the INPUT-2 signal is still delayed).
(4) The "ONDELAY" functional block connected to INPUT-1 *correctly filters the transient behaviour* of the 'SG level high' signal: the filtered signal will only be activated if the 'SG level high' signal remains continuously active during the filtering interval. Shorter "spikes" of this signal cannot make the filtered signal to become active.
(5) The activation of the filtered 'SG level high' signal *will always activate* the OUTPUT-2 and subsequently the OUTPUT-1 signals when the other enabling conditions are present.

The main advantage of the non model based analysis is that the requirements for the safety procedure can be formulated and checked with respect to the functional specification. Consequently, this type of verification does not require a process engineering background. However, these advantages are counterbalanced by the complexity of the analysis and the immense state space, which make this analysis type impractical. A large portion of this huge state-space is generated by input sequences that are completely unrealistic due to physical and technological constraints. The answer is a model based approach by supplementing the model of the control logic with a model of the controlled process. Including the model of the reactor in the verification removes the "impractical" segment of the state-space from the analysis.

4 Modelling for safety procedure verification: a CPN model of the plant

A simple concentrated parameter continuous time model is developed in this section for fault diagnostic purposes. The developed model will then be transformed to a CPN. This CPN model will be used for the formal verification in the next section.

4.1 Simple dynamic continuous time model

There are a few papers in the literature that report on developing simple dynamic models for boiling water or pressurized water reactors (mainly for training and control purposes). Unfortunately, these models do not contain the description of the major leaking type faults that are vital for the PRISE safety procedure verification. Therefore, a systematic modelling procedure suggested for constructing process models [35] has been followed to construct a simple dynamic model of the primary circuit that is able to describe the above faults. A similar model developed for controller design purposes is reported in [36], where the nuclear reaction specific model elements have also be taken into account in their simplest form [37].

4.1.1 Simplifying assumptions

One does not need a full distributed parameter dynamic model commonly used for safety calculations [1] for the formal verification. Only the sequence of events and the timing between them is of importance. Therefore, simplifying modelling assumptions are used to develop a simple dynamic model. These simplifying assumptions specify the considered operating units, their general properties and the properties of the considered fault events.

$\mathcal{A}1$ *Perfectly stirred (concentrated parameter) operating units* are assumed that consist of the liquid in the primary circuit (PC), the 6 steam generators (SG), the pressurizer (PR), and the containment (CN). A joint balance volume is assumed for the liquid in the primary circuit and for the pressurizer.

$\mathcal{A}2$ *Only simplified mass and energy balances* are assumed for every balance volume, but only a mass balance is constructed for the containment. Moreover, *constant physico-chemical properties* are used for every balance volume.

$\mathcal{A}3$ *Controllers* are assumed to be "ideal" under normal operating conditions, i.e. they keep the reference value of their controlled variable without any error. In case of faults an input-constrained operation model is considered, when they produce a given upper or lower bound value of their controlled

variable. The following controllers are taken into account: PR-pressure, PC-mass through PR-level, SG-mass through steam outflow mass from SG.

$\mathcal{A}4$ *Safety procedures* are discrete controllers acting on the system when a safety condition is fulfilled. The simplest binary "on-off" operation of the reactor trip (emergency shutdown) and the steam generator isolation safety procedures is taken into account with the indicator variables χ_{RSHUT}, and χ_{SGLOC}, respectively.

$\mathcal{A}5$ The *PRISE* fault event is modelled as an instantaneous permanent fault indicated by the $(\chi_{PRISE} = 1)$ condition (while the indicator variable χ_{PRISE} is zero otherwise). The leaking has a constant known mass flow rate m_{PRISE} from the primary to the secondary circuit.

$\mathcal{A}6$ The *other faults* considered are: (i) leakage in the primary circuit indicated by χ_{LOCA} with a constant known mass flow rate, such that $m_{LOCA} >> m_{PRISE}$, (ii) leakage in the pressurizer indicated by χ_{PRLO} with a constant known mass flow rate $m_{PRLO} < m_{PRISE}$ (iii) sensor fault in SG level $\chi_{SGLFAIL}$. The first two are considered to be instantaneous and permanent, while the latter has a temporal, stochastic character.

$\mathcal{A}7$ The *reactor power control* is also assumed to be "ideal", i.e. the reactor power is either its nominal value W_R or only the remaining power W_{MINR} is emitted when it is shut down.

$\mathcal{A}8$ The *purge and normal supply* of the liquid in the primary circuit is neglected.

$\mathcal{A}9$ The *initial state* of any investigated scenario is the *normal operating state* of the system.

$\mathcal{A}10$ The *model output variables* should be the ones that are the inputs to the PRISE safety procedure

- pressure in the primary circuit p_{PR},
- secondary steam pressure p_{SG},
- level in the steam generator ℓ_{SG},
- pressure in the containment p_{CN},
- cold leg temperature in the primary circuit T_{CL}.

4.1.2 Continuous time model equations

Dynamic conservation balances form the basis of our dynamic engineering model. They are constructed for conserved extensive quantities over balance volumes (operating units). Such balances have been constructed for the overall mass and internal energy of the liquid in the primary circuit and in the steam generators, as well as for the overall mass in the containment. Thereafter, the intensive form of the energy balance equations has been computed to obtain differential equations for the measurable temperature $T_{\cdot}$ instead of its related internal energy $U_{\cdot}$, where $\cdot = PC, SG$. There are additional *algebraic equations* that complement the differential conservation balance equations.

Together with the continuous or state-switched continuous dynamics of the

Liquid in the primary circuit and pressurizer
Balance (state) equations

$$\frac{dM_{PC}}{dt} = -\chi_{PRISE} m_{PRISE} - \chi_{LOCA} m_{LOCA} - \chi_{M_{PR}\geq 0} \chi_{PRLO} m_{PRLO}$$

$$c_{P,PC} M_{PC} \frac{dT_{PC}}{dt} = (1 - \chi_{RSHUT}) W_R + \chi_{RSHUT} W_{MINR} - K_{loss,PC} \cdot (T_{PC} - T_0) - (1 - \chi_{SGLOC}) \cdot 6 \cdot K_{T,SG} (T_{PC} - T_{SG})$$

Output equations

$$M_{PR} = M_{PC} - M_{PC}^0$$
$$p_{PR} = \chi_{M_{PR}\geq 0} \cdot \pi(M_{PR}) \quad (\pi \ linear)$$
$$T_{CL} = T_{PC} - 15$$

The steam generator
Balance (state) equations

$$\frac{dM_{SG}}{dt} = (1 - \chi_{SGLOC})(m_{SGIN} - m_{SGOUT}) + \chi_{PRISE} m_{PRISE}$$

$$c_{P,SG} M_{SG} \frac{dT_{SG}}{dt} = (1 - \chi_{RSHUT}) \left((1 - \chi_{SGLOC}) c_{P,SG} m_{SGIN} (T_{SGIN} - T_{SG}) - m_{SGOUT} E_{evap} \right) + \chi_{RSHUT} \cdot m_r \cdot \left((1 - \chi_{SGLOC}) \left(c_{P,SG} m_{SGIN} (T_{SGIN} - T_{SG}) - m_{SGOUT} E_{evap} \right) \right) + (1 - \chi_{SGLOC}) K_{T,SG} (T_{PC} - T_{SG}) + \chi_{PRISE} m_{PRISE} (c_{P,PC} T_{PC} - c_{P,SG} T_{SG}) - K_{loss,SG} (T_{SG} - T_0)$$

Output equations

$$\ell_{SG} = L(M_{SG}) + \chi_{SGLFAIL} \ell^* \quad (L \ linear)$$
$$p_{SG} = \varphi(T_{SG}) \quad (\varphi \ linear)$$

Containment
Balance (state) equations

$$\frac{dM_{CN}}{dt} = \chi_{LOCA} m_{LOCA} + \chi_{M_{PR}\geq 0} \chi_{PRLO} m_{PRLO}$$

Output equations

$$p_{CN} = K_{CN} M_{CN} + p_0$$

Safety procedure conditions
Reactor emergency shutdown

$$\chi_{RSHUT} = (p_{PR} < p_{PR}^*)$$

Steam generator isolation

$$\chi_{SGLOC} = (\ell_{SG} > \ell_{SG}^*) \wedge (t_{ellap} > t_{ellap}^*)$$

Fig. 4. The model equations of the continuous model

plant, we consider the operation of the safety procedures as part of our plant model. The *reactor trip* (emergency shutdown) procedure shuts down the reactor when the pressure of the primary circuit p_{PR} is below a given level. Similarly, a steam generator is isolated by a *SG isolation* safety procedure if its water level ℓ_{SG} is too high, but here a timing condition is also applied to avoid the effect of the non-reliable level sensor.

The model equations are shown in Fig. 4. They will be used for the model-based verification of the PRISE safety procedure.

From the system theoretical viewpoint, this model describes a (partially) controlled system, that belongs to a concentrated parameter nonlinear hybrid model class. The state equations are the differential equations that originate from conservation balances. The output equations are algebraic equations that are all linear. Thus the continuous *state* and related *output* variables are

$$\begin{aligned} M_{PC}, T_{PC} \text{ and } p_{PR}, T_{CL} \\ M_{SG}, T_{SG} \text{ and } \ell_{SG}, p_{SG} \\ M_{CN} \text{ and } p_{CN} \end{aligned}$$

The state-dependent indicator or switching variables $\chi_{M_{PR}\geq 0}$, χ_{RSHUT} and χ_{SGLOC} make the dynamics to be hybrid even if no fault occurs. The faults are modelled as time-dependent discrete disturbances through their indicator variables χ_{PRISE}, χ_{LOCA}, χ_{PRLO} and $\chi_{SGLFAIL}$. These are considered as *discrete fault inputs* when the model-based verification is performed.

The *discrete outputs* from the hybrid engineering model is computed by a set of simple logical expressions

$$\begin{aligned} \text{INPUT} - 1 &= \ell_{SG} > \ell^*_{SG} \\ \text{INPUT} - 2 &= p_{PR} < p^*_{PR} \\ \text{INPUT} - 3 &= p_{CN} > p^*_{CN} \\ \text{INPUT} - 4 &= T_{CL} < T^*_{CL} \\ \text{INPUT} - 5 &= \chi_{RSHUT} \\ \text{INPUT} - 6 &= p_{SG} < p^*_{SG} \\ \text{INPUT} - 7 &= p_{SG} < p^*_{SG} \\ \text{INPUT} - 9 &= p_{PR} < p^{**}_{PR} \end{aligned} \tag{1}$$

with $p^{**}_{PR} << p^*_{PR}$, and with all the limit variables denoted by an upper index * are known constants.

4.2 The CPN form of the dynamic engineering model

From the methodological point of view, there are two entirely different approaches to describe and analyse hybrid dynamic systems. One way is to embed the discrete valued time-dependent variables into an existing dynamical model [16], for example into a state-space model. The other way, that is followed in this paper, is to extend the discrete event system techniques [38] with the continuous dynamical information in the form of waiting or execution

times to get a timed automaton or Petri net in the simplest case, or to define some more or less simple dynamics associated to each state and/or state transition.

Driven by the actual aim of modelling, analysis and/or control, further approximations can be or should be made to transform the description to a homogeneous discrete event system model form [39]. This allows to use, for example, the well-established methods for model analysis developed for discrete event systems. Thus the model developed in sub-section 4.1 is transformed here to a CPN form by discretization in both time and in the range of the variables similarly to [22].

The discretization procedure is illustrated with the part of the continuous time model that corresponds to the containment:

$$\frac{dM_{CN}}{dt} = \chi_{LOCA} m_{LOCA} + \chi_{M_{PR}\geq 0} \chi_{PRLO} m_{PRLO} \tag{2}$$

$$p_{CN} = K_{CN} M_{CN} + p_0 \tag{3}$$

The steps in obtaining a CPN version of a hybrid differential-algebraic equation model are as follows.

(1) Define a sampling time interval for the discretization.
(2) Divide the range space of the continuous state, input and output variables to intervals by an ordered set of landmark points. The landmark points can be conveniently chosen by the given limit values dictated by the safety application, such as p^*_{PR}, p^{**}_{PR}, in our case. The values of a variable within one of its intervals are regarded to be indistinguishable, they will be represented by a coloured token on a place of the CPN model that corresponds to the variable.
(3) The places of the CPN model correspond to the variables: a single place corresponds to each of the input, disturbance and output variables, while two places are associated with a state variable.
(4) Transitions correspond to the equations in the model: the output arc function of the transitions in the CPN model describe the algebraic expressions present in the equations.
(5) The state (differential) equations have been integrated by using a simple Euler method that is implemented by an algebraic equation computing the current value of the differential variable from its value at the previous discrete time step.
For example, the discretized-in-time version of Eq. (2) is:

$$M_{CN} = h \cdot (M_{CN,prev} + \chi_{LOCA} m_{LOCA} + \chi_{M_{PR}\geq 0} \chi_{PRLO} m_{PRLO})$$

with the sampling interval h and with $M_{CN,prev}(k) = M_{CN}(k-1)$ at the

kth sampling interval.

Fig. 5 shows part of the transformed CPN model that corresponds to the containment equations.

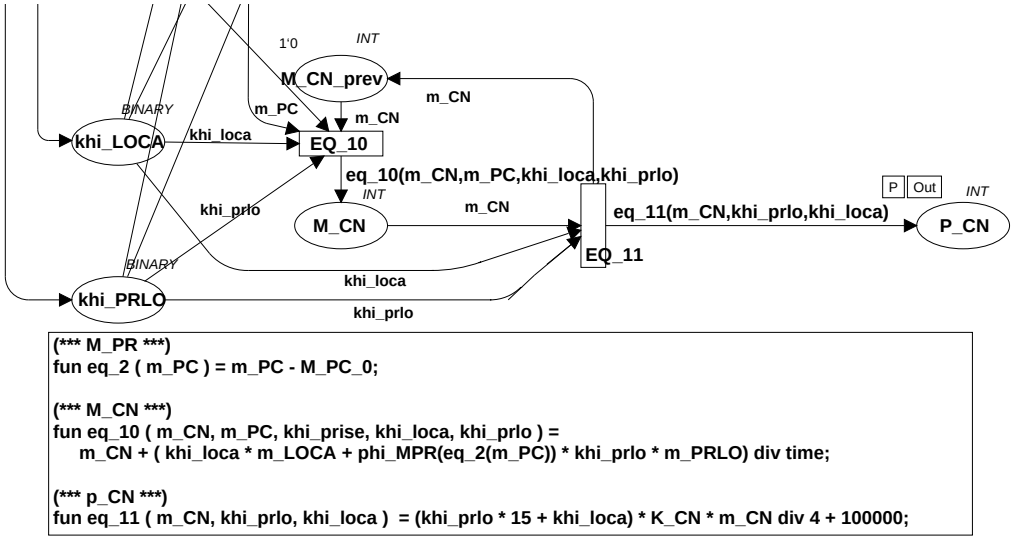

Fig. 5. The containment part in the CPN form of the engineering model

5 Model-based verification by simulation

The developed dynamic engineering model is used in this section for the model-based formal verification of the PRISE safety procedure. Because of the hybrid and nonlinear nature of the system dynamics in faulty conditions, the most commonly used verification method, the verification by using simulation is applied.

For NPPs a detailed dynamic simulator of the plant is usually applied as the model (see e.g. [40]), but then one needs to be able to modify the code and interface the safety procedure with the model. Instead, we shall use the CPN form of the engineering model developed above, and the CPN analysis tools [23] to perform the verification.

5.1 The composite system to be analysed

In order to focus the attention to the verification of the PRISE safety procedure, a composite CPN has been formed from the CPN model of the plant, and that of the PRISE safety procedure connected by a logical precalculation subnet realized also in CPN form as shown in Fig. 6. The precalculation block

implements the discretization of the range of the continuous variables to form digital inputs to the PRISE procedure block, similarly to an analog-digital converter using the equations (1).

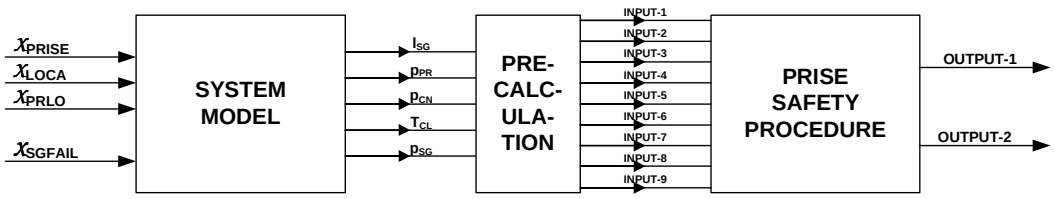

Fig. 6. The structure of the composite system

Thanks to the composition, the overall CPN model used for the formal verification has only four inputs, the fault indicator variables χ_{PRISE}, χ_{LOCA}, χ_{PRLO} and $\chi_{SGLFAIL}$ together with two logical outputs, where OUTPUT-1 corresponds to the initiation of the draining signal and OUTPUT-2 corresponds to the activation signal.

5.2 Time-dependent modelling of the water level sensor fault

As it has been mentioned before in sub-section 2.2 for the description of the PRISE safety procedure, the water level sensor of the steam generators causes most of the problems, because it can show spuriously high levels. The model equation (see in Fig. 4)

$$\ell_{SG} = L(M_{SG}) + \chi_{SGLFAIL}\ell^* \quad (L\ linear)$$

models this fault as an additive value to the real level driven by the fault indicator $\chi_{SGLFAIL}$, that is assumed to be time-dependent and stochastic.

5.3 Single leaking fault verification scenarios

In order to illustrate the method and results of the proposed model-based formal verification method, nine scenarios have been defined and analysed. These scenarios contain situations with at most two simultaneous faults with a single occurrence of a major leaking initiating event. The faults considered have been classified to be either major leaking faults (with indicator variables χ_{PRISE} for the PRISE event, χ_{LOCA} for the leakage in the primary circuit, and χ_{PRLO} for leakage in the pressurizer tank) with only one of them occurring simultaneously, or to be a sensor fault (with indicator variable $\chi_{SGLFAIL}$) that has been considered independently. The worst case scenarios have been considered where the major leaking fault occurs at the same time when the possible sensor fault starts.

- The "NO fault" situation corresponds to the nominal "easiest" case, when only a single leaking type fault (either PRISE or LOCA or PRLO) happens but the level sensor operates normally.
- The "SHORT fault" situation, when a 1 sec faulty behaviour is assumed for the water level sensor of the steam generator, can be compensated by the corresponding value checking element in the PRISE safety procedure.
- The "LONG fault" situation, when 15 sec faulty behaviour is assumed for the water level sensor, is a "worst case" scenario, because it cannot be compensated by the corresponding value checking element.

5.3.1 Verification results

The results of the verification test cases have been collected by using the utilities of the Design/CPN tool [23]. The initial state of the plant was a steady state that corresponds to the normal operating conditions. For each of the verification scenarios the time variation of the steam generator level sensor fault indicator variable $\chi_{SGLFAIL}$ of the water level signal (ℓ_{SG}), and the two output signals: the OUTPUT-2 (activation) and OUTPUT-1 (the draining initialization signal) of the system have been generated.

Fig. 7 shows an example of the time dependent results of the verification by simulation in the form of time plots generated by the Design/CPN tool in the case when the "LONG fault" situation is investigated. In the figure the draining initiation (OUTPUT-1) and the auxiliary activation (OUTPUT-2) signals are depicted by dashed and dotted lines, respectively. The steam generator level characterizing variables, the measured level (ℓ_{SG}, denoted by full line) and the sensor fault indicator variable ($\chi_{SGLFAIL}$, dashed-dotted line) are also shown.

The results show that only the PRISE fault event induces the OUTPUT-1 signal initiating the draining, even when a similar leaking fault (LOCA or PRLO) and a severe (LONG) level sensor signal fault occur. Although the auxiliary OUTPUT-2 signal becomes active for the PRLO situation — indicating that all but one symptom is present for initiating the draining— but the procedure still prevents the system to be drained, i.e. OUTPUT-1 does not become activated. This means that the PRISE safety procedure indeed safely initiates the draining, and it is selective with respect to the LOCA and PRLO events.

Because of the discrete nature of our dynamic model and the verification aim, only the occurrence times of the safety relevant events, the emergency reactor shutdown (χ_{RSHUT}), the draining initiation (OUTPUT-1) and the activation (OUTPUT-2) were recorded as simulation results (see Table 3). It is important to note that the occurrence times cannot be considered as accurate ones, but

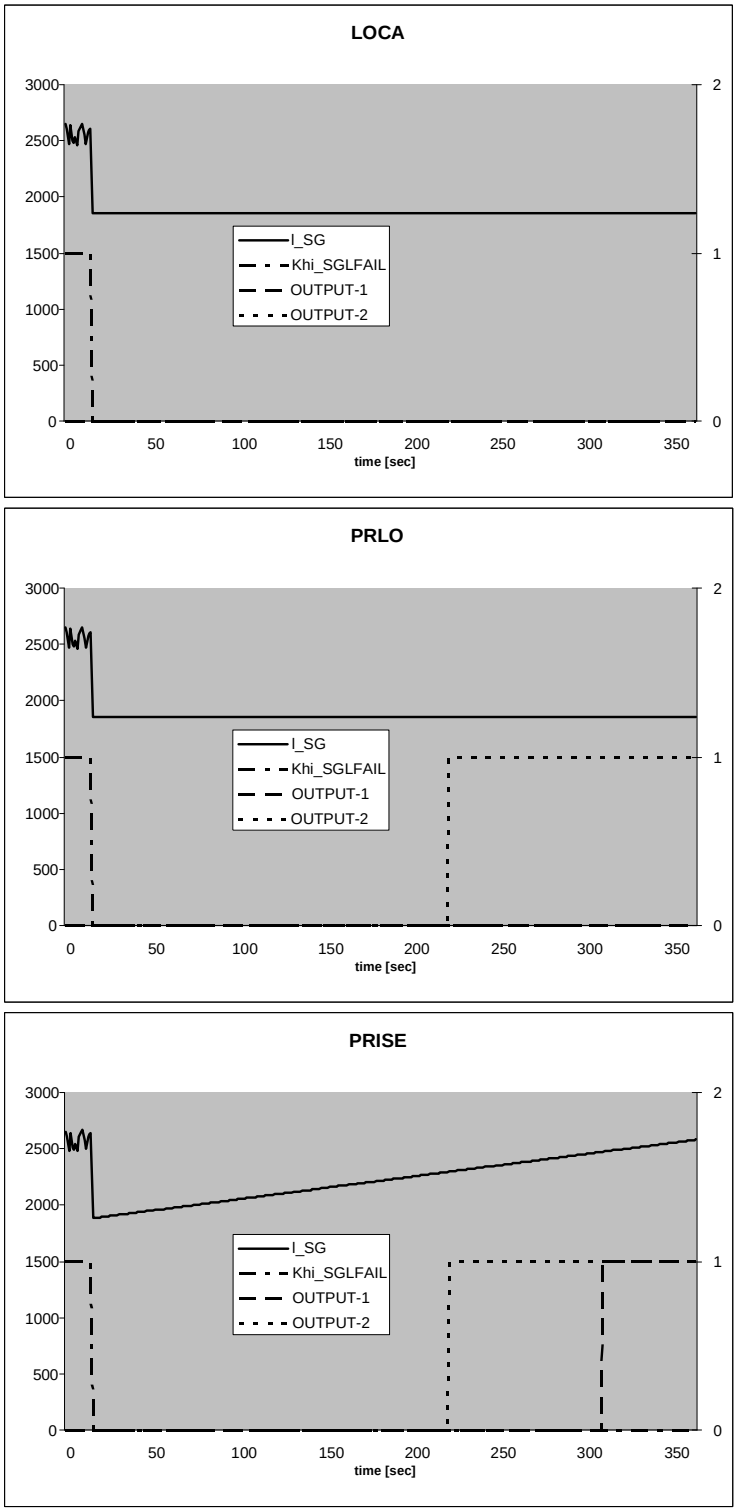

Fig. 7. Major leaking fault events combined with "Long" level sensor fault

the sequence of events is the one that matters for the verification.

The verification results are summarized in the top three rows of Table 3. In

each of the three multi-columns corresponding to NO, SHORT and LONG fault cases, the occurrence time of the signals OUTPUT-2, OUTPUT-1 (abbreviated as O2 and O1, respectively) and χ_{RSHUT} (the emergency shutdown of the reactor) are given.

Table 3
Simulation results: indicator variable occurrence times (sec)

	NO $\chi_{SGLFAIL}$			**SHORT** $\chi_{SGLFAIL}$			**LONG** $\chi_{SGLFAIL}$		
Scenario	O2	O1	χ_{RSHUT}	O2	O1	χ_{RSHUT}	O2	O1	χ_{RSHUT}
LOCA	–	–	124	–	–	125	–	–	134
PRLO	228	–	126	229	–	127	233	–	131
PRISE	233	311	131	233	311	131	233	311	121
LOCA & PRLO	–	–	1	–	–	1	–	–	1
LOCA & PRISE	–	–	1	–	–	1	–	–	1
PRLO & PRISE	137	–	35	130	–	28	134	–	33
LOCA & PRLO & PRISE	–	–	1	–	–	1	–	–	1

Abbreviations: O2 = OUTPUT-2, O1 = OUTPUT-1

5.4 Multiple leaking fault verification scenarios

Some multiple leaking fault verification scenarios have also been tested, combined again with the NO, SHORT and LONG level sensor fault situations. Observe that these cases involve four independent faults in the worst case. Their leaking types are independent major faults with very low probability.

The verification results are included in the last four rows of Table 3. Although the PRISE event is not detected by the tested safety procedure in any of the investigated cases (no occurrence of the OUTPUT-1 signal), but a reactor trip occurs almost immediately by the emergency shutdown procedure that is indicated by the occurrence time of the χ_{RSHUT}. This is technically correct, because the reactor emergency shutdown prevents the further increase of the level in the faulty steam generator, therefore no emission into the environment is possible.

6 Conclusion and future work

This paper proposes methods of formal and simulation based verification of the PRISE safety procedure. The verification aim is discrete in nature, so we developed a discrete dynamic representation of the safety procedure in the form of coloured Petri nets (CPNs). This allowed the powerful formal analysis techniques included in Design/CPN tool to be used for the verification. By

using a non-model-based strategy we could prove that the PRISE safety procedure is safe, there are no dead markings in the state-space, and all transitions are live with being either impartial or fair.

In this case the rapid growth of the search space prevented us to carry out a thorough verification. We partitioned the state space and selected the most important segment —the effect of the unreliable level measurement signal on the initiation of the safety procedure— for analysis.

We also developed a model-based approach for the verification of the PRISE safety procedure. This approach requires that both the safety procedure and the dynamic model of the plant are transformed into CPN form. In contrast to the standard safety analysis methodology that requires an accurate detailed dynamic model of the plant, we could use a simple low dimensional nonlinear dynamic model of the primary circuit in a VVER-type nuclear power plant. The model describes all of the major leaking type faults combined with a level sensor fault, and also includes the relevant safety procedures. Our paper proposes a novel method to transform the developed concentrated parameter hybrid model to its CPN form by discretization.

The model based verification has been performed by discrete dynamic simulation using the Design/CPN tool. As a result, the occurrence sequence of the fault relevant events, the reactor shutdown, the activation and the draining initiation was investigated under different scenarios including multiple faults. We found by the model-based analysis that the PRISE safety procedure initiates the draining when the PRISE event occurs, and no false alarm has been found.

Our further work is directed towards model-based formal verification using the composite CPN model of the plant and the safety procedure. Because of the size of the search space this will only be possible if the "lazy state space construction" approach based on equivalence classes (known in the CPN analysis methodology) will be applied.

References

[1] Information Systems Laboratories, Inc., Nuclear Safety Analysis Division, Rockville, Maryland, Idaho Falls, Idaho, USA. *RELAP5/MOD3.3 Code Manual, NUREG/CR-5535 Rev. P3*, March 2003.

[2] Y-S. Kim, B.-U. Bae, and G.-C. Park. Sweepout model implementation in RELAP5/MOD3.3 to improve RCS coolant inventory calculation during a LBLOCA. *Nuclear Engineering and Design*, 236:309–321, 2006.

[3] R.C. Borges, F. D'Auria, and A.C.M. Alvim. RELAP5/MOD3.2 post test simulation and accuracy quantification of LOBI test A1-93. In *2000 Relap5 International Users Seminar, Jackson Hole, Wyoming, USA*, 2000.

[4] Y. Kukita, K. Tasaka, H. Asaka, T. Yonomoto, and H. Kumamaru. The effects of break location on PWR small break LOCA: Experimental study at the ROSA-IV LSTF. *Nuclear Engineering and Design*, 122:255–262, 1990.

[5] Y. A. Hassan and S. Banerjee. Implementation of a non-condensable model in RELAP5/MOD3. *Nuclear Engineering and Design*, 162:281–300, 1996.

[6] H. S. Park, H. C. No, and Y. S. Bang. Analysis of experiments for in-tube steam condensation in the presence of noncondensable gases at a low pressure using the RELAP5/MOD3 code modified with a non-iterative condensation model. *Nuclear Engineering and Design*, 225:173–190, 2003.

[7] A. Prošek, B. Kvizda, B. Mavko, and T. Kliment. Quantitative assessment of MCP trip transient in a VVER. *Nuclear Engineering and Design*, 227:85–96, 2004.

[8] Incorporation of advanced accident analysis methodology into safety analysis reports. Technical report, International Atomic Energy Agency, IAEA-TECHDOC-1351, 2003.

[9] A. Bousbia-Salah and F. D'Auria. Use of coupled code technique for Best Estimate safety analysis of nuclear power plants. *Progress in Nuclear Energy*, 49:1–13, 2007.

[10] T. Hamidouche, A. Bousbia-Salah, E.K. Si-Ahmed, and F. D'Auria. Overview of accident analysis in nuclear research reactors. *Progress in Nuclear Energy*, 50:7–14, 2008.

[11] T. Mertke and T. Menzel. Methods and tools to the verification of safety-related control software. In *Proc. of the IEEE Int. Conf. on Sys., Man and Cybernetics, (SMC'2000), Nashville, USA*, pages 2455–2457, 2000.

[12] M. Marques, J.F. Pignatel, P. Saignes, F. D'Auria, L. Burgazzi, C. Müller, R. Bolado-Lavin, C. Kirchsteiger, V. La Lumia, and I. Ivanov. Methodology for the reliability evaluation of a passive system and its integration into a Probabilistic Safety Assesment. *Nuclear Engineering and Design*, 235:2612–2631, 2005.

[13] A.C.F. Guimarães and C.M.F. Lapa. Hazard and operability study using approximate reasoning in light-water reactors passive systems. *Nuclear Engineering and Design*, 236:1256–1263, 2006.

[14] J. Kim, W. Jung, and J.S. Son. The MDTA-based method for assessing diagnosis failures and their risk impacts in nuclear power plants. *Reliability Engineering and System Safety*, 93:337–349, 2008.

[15] J.M. Izquierdo-Rocha and M. Sánchez-Perea. Application of the Integrated Safety Assessment methodology to the emergency procedures of a SGTR of a PWR. *Reliability Engineering and System Safety*, 45:159–173, 1994.

[16] A. van der Schaft and H. Schumacher. *An Introduction to Hybrid Dynamical Systems, LNCIS 251.* Springer, London, 2000.

[17] E. Villani, P.I. Kaneshiro, and P.E. Miyagi. Hybrid stochastic approach for the modelling and analysis of fire safety systems. *Nonlinear Analysis*, 65:1123–1149, 2006.

[18] J.H. Choi, T.M. Kim, B.J. Moon, J.T. Seo, and Y.H. Kim. Containment pressure and temperature envelopes for a CANDU reactor equipment environmental qualification. *Nuclear Engineering and Design*, 236:2444–2451, 2006.

[19] K. Jensen. *Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use*, volume 1. Springer-Verlag, 1992.

[20] K. Jensen and G. Rosenberg. *High-level Petri nets: Theory and Application.* Springer-Verlag, 1991.

[21] R. Schoenig, J.-F. Aubry, T. Cambois, and T. Hutinet. An aggregation method of Markov graphs for the reliability analysis of hybrid systems. *Reliability Engineering and System Safety*, 91:137–148, 2006.

[22] M. Gerzson and K.M. Hangos. Analysis of controlled technological systems using high level Petri nets. *Computers and Chemical Engineering*, 19:S531–S536, 1995.

[23] Design/CPN – Computer Tool for Coloured Petri Nets. Technical report, http://www.daimi.au.dk/designCPN/, 2002.

[24] J.H. Park and P.H. Seong. An integrated knowledge base development tool for knowledge acquisition and verification for NPP dynamic alarm processing systems. *Annals of Nuclear Energy*, 29:447–463, 2002.

[25] H.S. Son and P.H. Seong. Development of a safety critical software requirements verification method with combined CPN and PVS: a nuclear power plant protection system application. *Reliability Engineering and System Safety*, 80:19–32, 2003.

[26] S.J. Lee and P.H. Seong. Development of automated operating procedure system using fuzzy colored Petri nets for nuclear power plants. *Annals of Nuclear Energy*, 31:849–869, 2004.

[27] M.C. Kim and P.H. Seong. A method for identifying instrument faults in nuclear power plants possibly leading to wrong situation assessment. *Reliability Engineering and System Safety*, 93:316–324, 2008.

[28] I. Parzer and S. Petelin. Minimum success criteria at SGTR combined with loss of secondary heat sink. In *2nd ASME-JSME Nuclear Engineering Joint Conference. Part 1 (of 2), San Francisco, USA*, pages 261–268, 1993.

[29] A. Hämäläinen, R. Kyrki-Rajamäki, S. Mittag, S. Kliem, F. P. Weiss, S. Langenbuch, S. Danilin, J. Hadek, and G. Hegyi. Validation of coupled neutron kinetic/thermal-hydraulic codes. Part 2: Analysis of a VVER-440 transient (Loviisa-1). *Annals of Nuclear Energy*, 29:255–269, 2002.

[30] A. Mader and H. Wupper. What is the method in applying formal methods to PLC applications? In *Proc. of the 4th Int. Conf. Automation of Mixed Processes: Hybrid Dynamic Systems (ADPM), Shaker Verlag*, pages 165–171, 2000.

[31] M.B. Younis and G. Frey. Formalization of existing PLC programs: A survey. In *Proc. of the IEEE/IMACS Multiconf. on Comp. Eng. in Sys. App. (CESA 2003), Lille, France*, pages Paper No. S2–R–00–0239, 2003.

[32] G. Frey and L. Litz. Formal methods in PLC programming. In *Proc. of the IEEE Int. Conf. on Sys., Man and Cybernetics (SMC'2000), Nashville, USA*, pages 2431–2436, 2000.

[33] K. Jensen. *Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use. Volume 2, Analysis Methods. Monographs in Theoretical Computer Science*. Springer-Verlag, 1997.

[34] M. Heiner. Verification and optimization of control programs by Petri nets without state explosion. In *Proc. 2nd Int. Workshop on Manufacturing and Petri Nets held at Int. Conf. on Application and Theory of Petri Nets (ICATPN '97)*, pages 69–84, 1997.

[35] K.M. Hangos and I.T. Cameron. *Process Modelling and Model Analysis*. Academic Press, London, 2001.

[36] Cs. Fazekas, G. Szederkényi, and K.M. Hangos. A simple dynamic model of the primary circuit in VVER plants for controller design purposes. *Nuclear Engineering and Design*, 237:1071–1087, 2007.

[37] G. Kessler. *Nuclear Fission Reactors*. Springer-Verlag, Wien, New-York, 1983.

[38] C.G. Cassandras and S. Lafortune. *Introduction to Discrete Event Systems*. Kluwer Academic Publishers, London, 1999.

[39] G. Lichtenberg and J. Luetzenberg. Using discrete invariants for fault detection of hybrid systems. In *Proceedings of the 15th International Workshop on Principles of Diagnosis, Carcassone, France*, 2004.

[40] H.-W. Huang, C. Shih, S. Yih, M.H. Chen, and J.M. Lin. Model extension and improvement for simulator-based software safety analysis. *Nuclear Engineering and Design*, 237:955–971, 2007.

Nomenclature

Table 4 contains the variables of the dynamic model and the PRISE safety procedure. The operating unit the variable belongs to is also indicated, that can be

- "R" for the reactor,
- "PC" for the liquid in the primary circuit,

- "PR" pressurizer,
- "SG" steam generator,
- "CN" containment.

Thereafter the identifiers of the physical parameters and their explanation are collected in Table 5.

The nominal value of the variables and the value of the parameters are the same as in [36].

Table 4
Variables

Identifier	**Unit: Variable**
M_{PC}	PC: water mass
T_{PC}	PC: water temperature
T_{CL}	PC: cold leg temperature
M_{PR}	PR: water mass
p_{PR}	PR: pressure
T_{SG}	SG: steam generator temperature
M_{SG}	SG: secondary water mass
p_{SG}	SG: steam pressure
ℓ_{SG}	SG: secondary water level
M_{CN}	CN: water mass
p_{CN}	CN: pressure
χ_{PRISE}	PC: PRISE indicator variable
χ_{LOCA}	PC: LOCA indicator variable
χ_{PRLO}	PR: leak indicator variable
χ_{RSHUT}	R: shutdown indicator variable
χ_{SGLOC}	SG: locked indicator variable
$\chi_{SGLFAIL}$	SG: level sensor failure ind. var.
$\chi_{M_{PR}\geq 0}$	PR: empty indicator variable

Table 5
Physical parameters

Unit	**Identifier**	**Parameter**
R	W_R	Reactor power
	W_{MINR}	Reactor remained power
PR	M^0_{PC}	Water mass in PC without PR
PC	$K_{T,SG}$	Heat transfer coefficient
	$K_{loss,PC}$	Heat loss transfer coefficient
	T_0	Reference temperature
	$c_{p,PC}$	Specific heat
SG	$c_{p,SG}$	Specific heat
	$K_{loss,SG}$	Heat loss transfer coefficient
	T_0	Reference temperature
	$E_{evap,SG}$	Evaporation coefficient
	m_{SGIN}	Inlet mass flow rate
	m_{SGOUT}	Purge mass flow rate
	T_{SGIN}	Inlet water temperature
	m_r	Reduced mass flow coefficient
CN	K_{CN}	Pressure coefficient
	p_0	Pressure offset
Errors	m_{PRISE}	PRISE mass flow rate
	m_{LOCA}	LOCA mass flow rate
	m_{PRLO}	Leaky PR mass flow rate
Outputs	ℓ^*_{SG}	Maximal water level in SG
	p^*_{PR}	Minimal pressure in PC
	p^{**}_{PR}	Safety pressure in PC
	p^*_{CN}	Maximal pressure in CN
	T^*_{CL}	Minimal water temperature in PC
	p^*_{SG}	Minimal pressure in SG
	t^*_{elap}	Minimal elapsed time