MODELING AND SIMULATION OF THE PRIMARY CIRCUIT OF THE PAKS NUCLEAR POWER PLANT FOR CONTROL AND DIAGNOSIS

Erzsébet Németh[1], **Csaba Fazekas**[1], **Gábor Szederkényi**[1], **Katalin M. Hangos**[1]

[1]Process Control Research Group, Systems and Control Laboratory
Computer and Automation Research Institute
H-1518 Budapest, P.O. Box 63, Hungary

szeder@sztaki.hu (Gábor Szederkényi)

Abstract

Two related but different dynamic simulators of the primary circuit of the Paks Nuclear Power Plant in Hungary are described in this paper that have been built from a simple dynamic model based on first engineering principles. For dynamic analysis and controller design purposes a simple continuous time discrete-continuous hybrid state-space model has been developed that is implemented in the MATLAB/SIMULINK environment. This model has been extended by the fault models of non-compensable major leaking faults, and has been discretized to obtain a discrete event system model in the form of a coloured Petri net (CPN). The CPN model has been used to verify a safety procedure that initiates the draining of the liquid in the primary circuit when a non-compensable primary-to-secondary leaking fault occurs.

Keywords: process modeling, dynamic simulation, energy systems, discrete event simulation, safety procedures

Presenting Author's Biography

Gábor Szederkényi is a senior researcher in the Process Control Research Group of the Computer and Automation Research Institue of the Hungarian Academy of Sciences. He received his M.Sc. (Eng) in Information Technology and his Ph.D. in Information Science from the University of Veszprém in 1998 and 2002, respectively. His research interests include the analysis and control of nonlinear dynamical systems and system identification.

1 Introduction and motivation

This paper presents two related but different simulators of the primary circuit of a VVER-440 type nuclear power plant located in Hungary that are based on the simplified dynamic model of the system constructed from first engineering principles. The main motivation of our work is the continuous effort for making the operation of the power plant more safe and more effective. This goal is supported by two important factors: firstly, the significant development of the last decades in process modeling and control theory (see e.g. [1] and [2]) and secondly, the improving quality of the hardware and software environment providing the necessary amount of measured data. However, the diagnostic and control solutions that were designed and implemented at the building time of the power plant usually did not take into consideration the detailed nonlinear dynamics of the operating units. This means that there is a lot of space for the improvement of control loops and safety procedures using our current knowledge.

The Paks Nuclear Power Plant was founded in 1976 and started its operation in 1981. The plant operates four VVER-440/213 type reactor units with a total nominal (electrical) power of 1860 MWs. 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.

2 Dynamic model of the primary circuit

A systematic modeling procedure suggested for constructing process models [1] has been followed to construct a simple dynamic model of the primary circuit. The modeling assumptions and the detailed derivation of the model equations can be found in [3].

The structure of the primary circuit can be seen in Fig. 1. Four operation units are identified in the primary circuit and an unique identifier is used for each of the operating units in the subscript of their related variables and parameters (R - reactor, PC - primary circuit, PR - pressurizer, SG - steam generator).

The *state-space model* of the primary circuit is the following.

$$\frac{dN}{dt} = \frac{\left(p_1 v^2 + p_2 v + p_3\right)\beta}{\Lambda} N + S \quad (1)$$

$$\frac{dM_{PC}}{dt} = m_{in} - m_{out} \quad (2)$$

$$\frac{dT_{PC}}{dt} = \frac{1}{c_{p,PC} M_{PC}} \big[c_{p,PC} m_{in} \left(T_{PC,I} - T_{PC}\right) + + c_{p,PC} m_{out} 15 + W_R - W_{loss,PC} - - 6 \cdot K_{T,SG} \left(T_{PC} - T_{SG}\right) \big] \quad (3)$$

$$\frac{dM_{SG}}{dt} = m_{SG,in} - m_{SG,out} \quad (4)$$

$$\frac{dT_{SG}}{dt} = \frac{1}{c^L_{p,SG} M_{SG}} \big[- m_{SG,out} E_{evap,SG} + + c^L_{p,SG} m_{SG,in} \left(T_{SGSW} - T_{SG}\right) - - \left(c^V_{p,SG} - c^L_{p,SG}\right) m_{SG,out} T_{SG} + + K_{T,SG} \left(T_{PC} - T_{SG}\right) - W_{loss,SG} \big] \quad (5)$$

$$\frac{dT_{PR}}{dt} = \frac{1}{c_{p,PR} M_{PR}} \big[\chi_{m_{PR}>0} c_{p,PC} m_{PR} T_{PC,HL} + + \chi_{m_{PR}<0} c_{p,PR} m_{PR} T_{PR} - W_{loss,PR} + + W_{heat,PR} - c_{p,PR} m_{PR} T_{PR} \big] \quad (6)$$

The output equations are as follows:

$$W_R = c_\Psi N \quad (7)$$

$$p_{SG} = p^T_*(T_{SG}) \quad (8)$$

$$\ell_{PR} = \frac{1}{A_{PR}} \left(\frac{M_{PC}}{\varphi(T_{PC})} - V^0_{PC} \right) \quad (9)$$

$$p_{PR} = p^T_*(T_{PR}) \quad (10)$$

where p^T_* and $\varphi(T_{PC})$ are quadratic functions while m_{PR} is the mass flow rate between the liquid in the primary circuit and the liquid in the pressurizer.

The definition of the variables and parameters can be found in Tables 1 and 2.

Tab. 1 Variables with type (**s**tate, **i**nput, **o**utput, **d**isturbance).

Identifier	Variable	Type
N	R neutron flux	s
v	R control rod position	i
W_R	R reactor power	o
m_{in}	PC inlet mass flow rate	i
m_{out}	PC purge mass flow rate	d
$T_{PC,I}$	PC inlet temperature	d
$T_{PC,CL}$	PC cold leg temperature	(s)
$T_{PC,HL}$	PC hot leg temperature	(s)
p_{PR}	PR pressure	o,(s)
T_{PR}	PR temperature	s
ℓ_{PR}	PR liquid level	o,(s)
$W_{heat,PR}$	PR heating power	i
T_{SG}	SG steam generator temperature	s
$m_{SG,in}$	SG inlet mass flow rate	i
$m_{SG,out}$	SG steam mass flow rate	d
$T_{SG,SW}$	SG inlet water temperature	d
p_{SG}	SG steam pressure	o

Tab. 2 Parameters of the primary circuit model with their reliability domain. "*NE.*" means that the parameter is not estimated and its value is a priori known.

Notation	Definition	Domain
β	Total fraction of delayed neutrons	*NE.* 0.0064
Λ	Generation time	*NE.* $10^{-5}\ s$
c_Ψ	Constant in the power equation	*NE.* $13.75 \cdot 10^6\ W/\%$
$E_{evap,SG}$	Evaporation energy (at 260 ^oC)	*NE.* $1.658 \cdot 10^6 J/kg$
(p_1, p_2, p_3)	Rod's parameters	-
S	Source	-
$c_{p,PC}$	Specific heat	$\approx 4900\ J/kg/K$
$K_{T,SG}$	Heat transfer coefficient	$\approx 10^7\ W/K$
$W_{loss,PC}$	Heat loss	$\approx 1 - 2\ MW$
$W_{loss,SG}$	Heat loss	$\approx 10^5\ W$
$c^L_{p,SG}$	Specific heat of water	$\approx 4700\ J/kg/K$
$c^V_{p,SG}$	Specific heat of vapour	$\approx 2800\ J/kg/K$
$c_{p,PR}$	Specific heat	$> 5080\ J/kg/K$
$W_{loss,PR}$	Heat loss	$\approx 10^5\ W$
V^0_{PC}	Volume of primary circuit	$230 - 250\ m^3$

The system variables can be classified as follows:

- *State variables*: differential variables in the differential equations, N, M_{PC}, T_{PC}, T_{PR}, M_{SG}, T_{SG}
- *Input variables*: manipulable variables affected by the considered controllers (PR-pressure, PC-mass

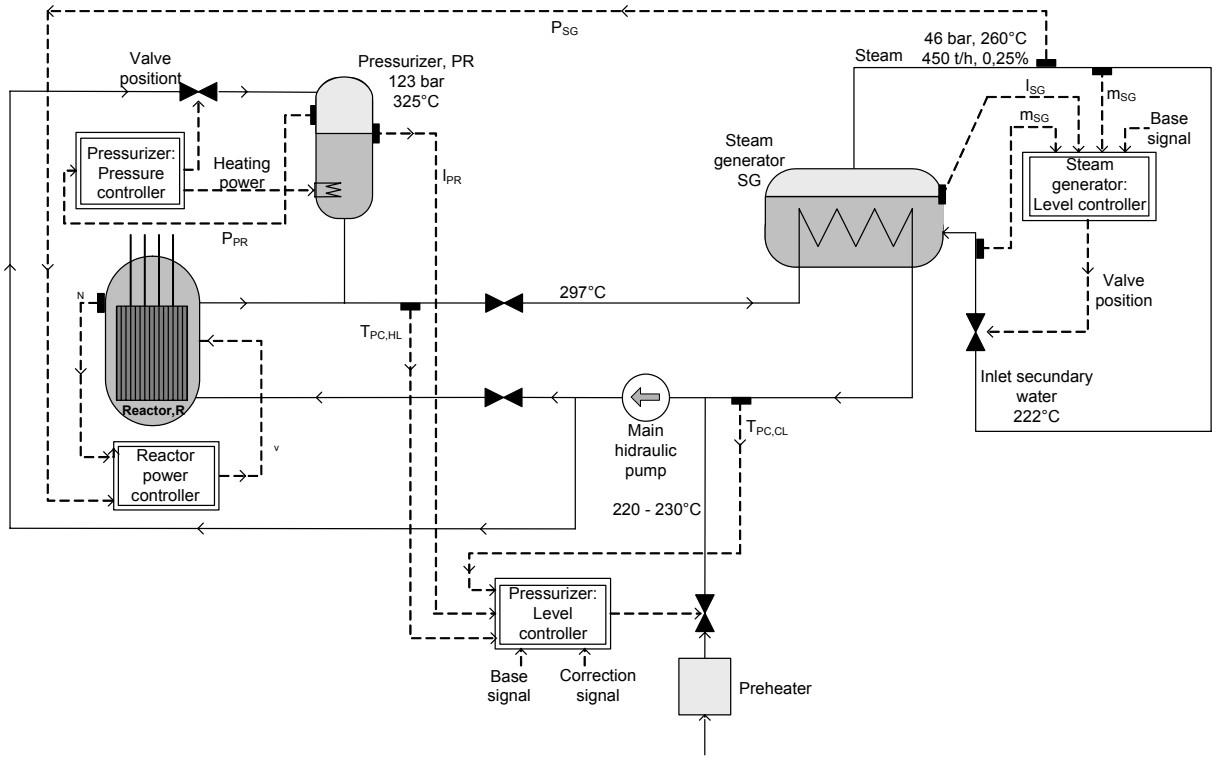

Fig. 1 Structure of the primary circuit

through PR-level, SG-level, R-power controllers), v, m_{in}, $m_{SG,in}$, $W_{heat,PR}$

- *Disturbances*: all other possibly time-dependent variables appearing on the right-hand side of the differential equations, m_{out}, $m_{SG,out}$, m_{PR}, $T_{SG,SW}$, $T_{PC,I}$
- *Output variables*: measurable variables that are regulated by the considered controllers, N (W_R), p_{SG}, ℓ_{PR} (M_{PC}), p_{PR}

We have to note, that in normal operational mode, the amount of liquid in the primary circuit is constant, i.e. $m_{in} = m_{out}$. However, our model contains both variables separately, because this constant mass is realized by level controller of pressurizer what we have to design.

From a mathematical viewpoint, the above state-space model is a discrete-continuous hybrid ordinary differential equation, where the discrete (switching) behaviour is generated by the indicator function $\chi_{m_{PR}>0}$.

3 The simulator of the primary circuit and its applications

3.1 Simulation environment

The model is implemented in MATLAB/SIMULINK [4] environment. Each operating unit corresponds to a block, see Fig. 2. The differential equations and different parts of an operating unit are also realized in a block separately as seen in Fig. 3 in the case of the liquid in the primary circuit. Differential equations are realized with a simple integrator element as seen in Fig. 4.

Different data sources (see later) are applied with different sampling time. To make the data uniform, the measured data are re-sampled with sampling time $10\ s$. The measurement data are stored in $.mat$ files in SI units.

3.2 Simulation method

From the mathematical point of view, the model is a set of differential and algebraic equations (a DAE model) where the algebraic equations can be substituted into the differential ones (an index 0 model). The *ode15s* solver in MATLAB is used for the numerical solution because some measured data are noisy and this numerical method gives much faster result with the same accuracy then the standard *ode45*. This solver is a multistep, variable-order solver based on the appropriate numerical differentiation formulas [4].

3.3 Application: identification of the primary circuit dynamics

The identification method is based on the model decomposition (see details [3, 5]). It is seen from the state equations (1)-(6) and the measured variables, that the parameters in the neutron flux balance equation (1) can be estimated independently of the others, thus the reactor forms an independent component of the model. Then the coupled equations (2)-(5) describing the dynamics of the liquid in the primary circuit and the steam

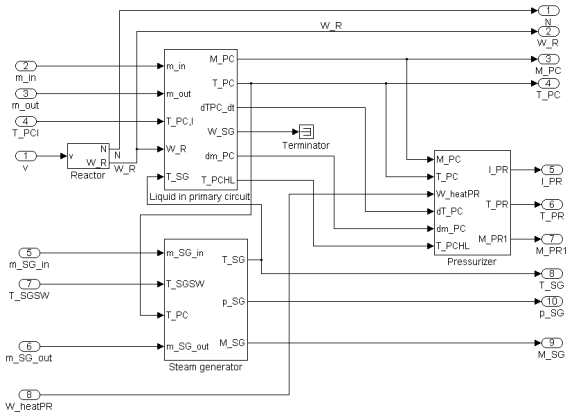

Fig. 2 Block structure of the simulator in MATLAB/SIMULINK

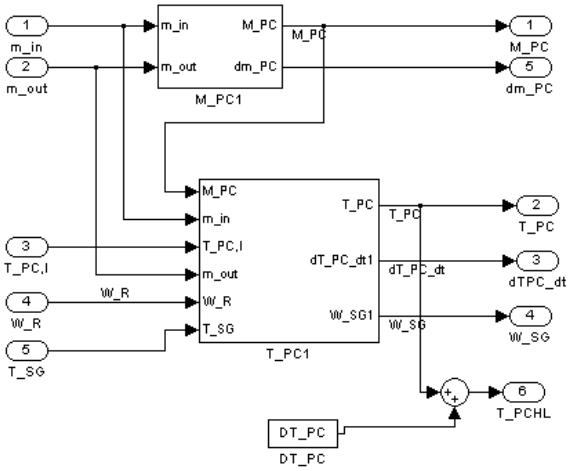

Fig. 3 Block structure of the primary circuit liquid model in MATLAB/SIMULINK

generator form another component that uses the reactor power as its 'virtual input'. Finally, the third component is the pressurizer that depends on the dynamics of the water in the primary circuit.

The parameter estimation has been carried out sequentially and component-wise following the dependencies outlined above. If the dynamic model equation(s) is/are nonlinear in its/their parameters, an optimization-based parameter estimation method, the Nelder-Mead simplex method [6, 7] available in MATLAB has been used. For error value we measure the fit in terms of the 2-norm between the measured and the model-predicted output signals.

Measured data from 1., 3. and 4. units of Paks Nuclear Power Plant were collected for parameter estimation purposes. In order to span a relatively wide operating domain, transient data of increasing and decreasing the power of the units when shifting from day to night load conditions and back have been used. The measured data are originated from two different systems: a so called Unit Computer and a reactor defense system.

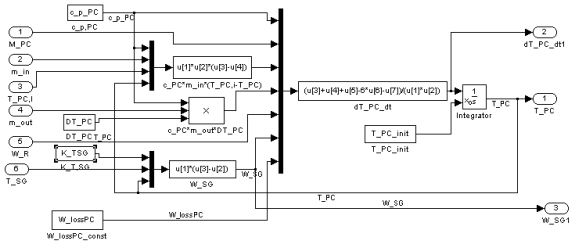

Fig. 4 Block structure of differential equation of the temperature of primary circuit liquid in MATLAB/SIMULINK

In Fig. 5 one can see an example curve fitting during the estimation of reactor's parameters for unit 3. In Table 3 one can found the values of the estimated parameters in case of unit 3.

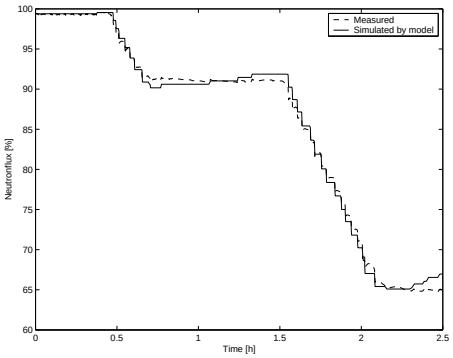

Fig. 5 The measured and estimated neutron flux in unit 3

Tab. 3 The estimated values of the physical parameters of unit 3.

	Parameter	Unit	Value
R	p_1	$1/m^2$	-0.0191
	p_2	$1/m$	-0.00860
	p_3	1	-0.0305
	S	$\%/s$	1939
PC	$K_{T,SG}$	W/K	$9.6926 \cdot 10^6$
	$K_{loss,PC}$	W/K	$9.9079 \cdot 10^6$
	$c_{p,PC}$	J/kgK	4909
SG	$M_{SG}(0)$	kg	32627
	$c^L_{p,SG}$	J/kgK	4356
	$c^V_{p,SG}$	J/kgK	3775
	$W_{loss,SG}$	W	$1.006 \cdot 10^5$
PR	$c_{p,PR}$	J/kgK	6873
	$W_{loss,PR}$	W	$1.68 \cdot 10^5$
	V^0_{PC}	m^3	239

4 A simulator based on a coloured Petri net model of the primary circuit

For safety-critical diagnostic purposes, coloured Petri nets (CPNs) [8, 9, 10] have been selected as a unifying modeling tool that allows modeling, and simulation-based verification of safety-critical procedures in NPPs. In addition, a process model in a qualitative differential

algebraic equation (DAE) form can also be represented as a CPN [11]. Thus we could use a powerful tool, the Design/CPN [12] to support the modeling of our plant and its safety procedure in the form of a joint CPN and perform the verification by using CPN analysis procedures.

4.1 The CPN model of the primary circuit

Unfortunately, the model described in section 2 for identification and controller design purposes does not contain the description of the major leaking type faults that are vital for the PRISE safety procedure verification. Therefore, we have extended the simple dynamic model of the primary circuit so that it is able to describe the above faults. The developed model will then be transformed to a CPN, and it will be used for the verification.

4.1.1 Simplifying assumptions

In addition to the simplifying modeling assumptions used for developing the model described in section 2, the following key assumptions have been applied to describe the considered fault events.

$\mathcal{A}1$ *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, steam outflow mass from SG.

$\mathcal{A}2$ *Safety procedures* are discrete controllers acting on the system when a safety condition is fulfilled. The operation of the reactor emergency shutdown and the steam generator isolation safety procedures are taken into account with the indicator variables χ_{RSHUT}, and χ_{SGLOC}, respectively.

$\mathcal{A}3$ The *PRISE* fault event is modeled 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 flowrate m_{PRISE} from the primary to the secondary circuit.

$\mathcal{A}4$ The *other faults* considered are: (i) leakage in the primary circuit indicated by χ_{LOCA} with a constant known mass flowrate, such that $m_{LOCA} >> m_{PRISE}$, (ii) leakage in the pressurizer indicated by χ_{PRLO} with a constant known mass flowrate $m_{PRLO} < m_{PRISE}$ (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.

4.1.2 Continuous time model equations

The model equations are shown in Fig. 6. 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: M_{PC}, T_{PC}, and p_{PR}, T_{CL}; M_{SG}, T_{SG} and ℓ_{SG}, p_{SG}; M_{CN} and p_{CN}.

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

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

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

Output equations

$$M_{PR} = M_{PC} - M0_{PC}$$
$$p_{PR} = \chi_{M_{PR}\geq 0} \cdot \pi(M_{PR}) \quad (\pi \ linear)$$
$$T_{CL} = T_{PC} - 15$$

The steam generator
Balance (state) equations

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

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

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. 6 The model equations of the continuous time model

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 modeled 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.

4.1.3 The CPN form of the dynamic engineering model

Driven by diagnostic aim of modeling, we transform the description to a homogenous discrete event system model form [13]. This allows to use, for example, the well-established methods for model analysis developed for discrete event systems [8, 9]. Thus the model developed in subsub-section 4.1.2 has been transformed to a CPN form by discretization in both time and in the range of the variables similarly to [11].

4.2 Application: simulation-based verification of a primary-to-secondary leaking (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.

4.2.1 The PRISE safety procedure and its CPN form

The *PRImary-to-SEcondary leaking – abbreviated as PRISE* – is one of the major non-compensable leaking of parts of the primary circuit, that occurs when there is a breakage or other leaking within the steam generator vessel affecting either a few (3-10) tubes or their collector that contain the high-pressure activated liquid of the primary circuit.

The purpose of the PRISE safety procedure is *initiating the draining if and only if a PRISE event occurs*. This includes to prevent the steam generators to be drained when a fault event causing similar symptoms but not being a PRISE event occurs, i.e. the PRISE safety procedure should be selective. In order to achieve this behavior, the fault events causing similar symptoms should also be thoroughly analyzed and the distinctive event sequence for PRISE is to be detected.

With the above considerations, the technological and system experts at Paks Nuclear Power plant have designed a timed logical scheme shown in Fig. 7 in a heuristic way that has been transformed to its CPN form [14].

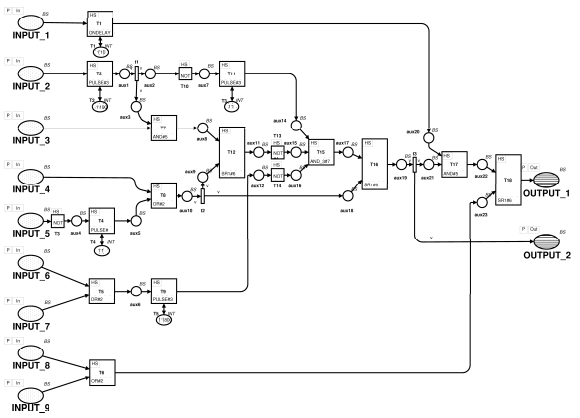

Fig. 7 The CPN description of the PRISE safety procedure

The description of the inputs and outputs of the PRISE safety procedure are included in Table 4.

The stand-alone dynamic properties of the CPN model of the PRISE safety procedure are also detailed in [14]. Some important results are: (i) the PRISE CPN is multiset bounded and safe in the integer sense; (ii) the PRISE CPN with feedback is deadlock free and all transitions related to the primary output are live; (iii) each live transition is at least impartial or fair.

Tab. 4 PRISE safety procedure I/O description

Notation	Short name	Description
INPUT-1	SG level high ($\ell_{SG} > +600\ mm$)	Steam generator water level is increasing (due to closure of the turbine)
INPUT-2	Primary pressure decreasing ($p_{PR} < 112\ bar$)	The pressure of the primary water is decreasing (due to the PRISE or other leakage)
INPUT-3	Containment pressure is normal ($p_{CN} < 1.01\ bar$)	The pressure of the containment is not increasing (due to primary water inflow)
INPUT-4	Primary temp. below nominal ($T_{CL} < 245^oC$)	Technical condition signifying that the reactor is in startup/shutdown operation
INPUT-5	Control rods fully down ($\chi_{RSHUT} = 1$)	Technical condition used to reset the operation of the PRISE safety procedure
INPUT-6	SG deltaP	Technical conditions used to avoid erroneous draining of secondary water after isolation of the steam generator
INPUT-7	SG RAP 1/2	
INPUT-8	SG inhibition	Technical condition used to take the SG inhibited state into consideration
INPUT-9	Primary pressure low ($p_{PR} < 50\ bar$)	Technical condition signifying that the reactor 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

4.2.2 The composite system to be analyzed

For NPPs the detailed dynamic simulator is usually applied as the model (see e.g. [15]), but it needs to be able to modify the code and interface the safety procedure with the model.

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 sub-net realized also in CPN form as shown in Fig. 8. The precalculation block implements the discretization of the range of the continuous variables to form digital inputs to the PRISE procedure block.

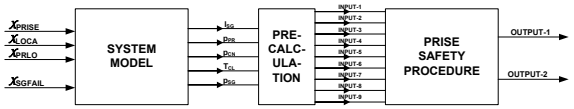

Fig. 8 The structure of the composite system

4.2.3 Verification scenarios

The water level sensor of the steam generators causes most of the problems, because it can show spuriously high level when it is faulty. The model equation (see in Fig. 6) $\ell_{SG} = L(M_{SG}) + \chi_{SGLFAIL}\ell^*$ (where L is 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. Three deterministic time-dependent fault scenarios have been defined for the fault indicator $\chi_{SGLFAIL}$: (a) No fault; (b) Short fault, when a 1 sec faulty behavior is assumed that can be compensated by the corresponding delay element in the PRISE safety procedure; (c) Long fault, with a 15 sec faulty behavior.

In order to illustrate the results of the model-based formal verification method by simulation, nine fault scenarios have been defined and analyzed that contain situations with at most two simultaneous faults. The faults considered have been classified to be either major leaking faults (with indicator variables χ_{PRISE}, 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 sensor fault ($\chi_{SGLFAIL}$) that has been considered independently.

Behaviour of the "Long fault" case

The "Long fault" situation, when 15 sec faulty behavior is assumed for the water level sensor, is a "worst case" scenario, because it can not be compensated by the corresponding value checking element. Therefore the time dependent behavior of the key input and output signals has been analyzed in details for all of the three considered leaking fault cases. Figure 9 depict the time dependent results of the verification in the form of time plots created by the Design/CPN tool.

It is seen 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 level sensor signal fault occur. It is important to note that 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 shows that the PRISE safety procedure initiates the draining if and only if the PRISE event occurs in the domain of the considered fault scenarios.

5 Conclusions

Two related but different dynamic simulators of the primary circuit of the Paks Nuclear Power Plant in Hungary are described in this paper that have been built from a simple dynamic model based on first engineering principles.

For dynamic analysis and controller design purposes a simple continuous time discrete-continuous hybrid state-space model has been developed that is implemented in the MATLAB/SIMULINK environment. The model has been used for a parameter identification study where the model parameters with physical meaning has been estimated. The calibrated model is used for controller design purposes in an ongoing study.

The control-oriented model has been extended by the fault models of non-compensable major leaking faults, and has been discretized to obtain a discrete event system model in the form of a coloured Petri net (CPN). The CPN model has been used to verify a safety procedure that initiates the draining of the liquid in the primary circuit when a non-compensable primary-to-secondary leaking fault occurs.

6 References

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

[2] Alberto Isidori. *Nonlinear Control Systems*. Springer, Berlin, 1995.

[3] 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, Accepted*, 2007.

[4] Mathworks. *Using Matlab version 6.5*. The Mathworks Inc., Natick, 2002.

[5] Cs. Fazekas, G. Szederkényi, and K. M. Hangos. Model identification of the primary circuit at the paks nuclear power plant. *Proceedings of The 26th IASTED International Conference on Modelling, Identification, and Control, MIC 2007, Innsbruck, Austria*, 2007.

[6] J.A. Nelder and R. Mead. A simplex method for function minimization. *Computer Journal*, 7:308–313, 1965.

[7] J.C. Lagarias, J.A. Reeds, M.H. Wright, and P.E. Wright. Convergence properties of the nelder-mead simplex method in low dimensions. *SIAM Journal of Optimization*, 9:112–147, 1998.

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

[9] K. Jensen. *Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use Volume 2*. Springer-Verlag, 1995.

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

[11] M. Gerzson and K.M. Hangos. Analysis of controlled technological systems using high level petri nets. *Comp. Chem. Engineering*, 19(Suppl):S531–S536, 1995.

[12] Meta Software Corporation. *Design/CPN – Computer Tool for Coloured Petri Nets*. Meta Software Corporation, http://www.daimi.au.dk/designCPN/, 2002.

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

[14] E. Németh and Bartha T. Formal verification of function block based specifications of safety-critical software. In *Proceedings of the 8th International Conference on MITIP*, pages 211–218, Budapest, Hungary, 2006.

[15] 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(9):955–971, 2007.

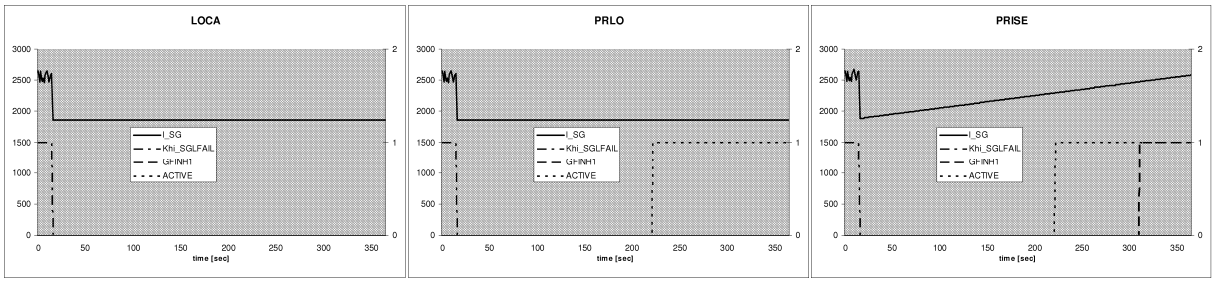

Fig. 9 Major leaking fault events combined with "Long" level sensor fault