Model: ResIsolation
Type: P/T Net
Origin: Academic

since
MCC 2024

Wendelin Serwe and Hubert Garavel
wendelin.serwe@inria.fr

This form is a summary description of the model entitled "ResIsolation" proposed for the Model Checking Contest @ Petri Nets. Models can be given in several instances parameterized by scaling parameters. Colored nets can be accompanied by one or many equivalent, unfolded P/T nets. Models are given together with property files (possibly, one per model instance) giving a set of properties to be checked on the model.

Description

This model contains the description of a System-on-Chip for analyzing the security property of resource isolation. The model is composed of a number of sources (from 8 to 13) and targets (from 1 to 5) connected via a bus. Resource isolation ensures that the information stored in targets is accessed only by authorized sources. Authorization is based on the two notions of security and privilege: access to a target is granted only if the security and privilege of the source are both greater or equal to those of the target.

In this model, any source can request to read and write information from/to any target, which then accepts or rejects the request. Sources with the highest security and privilege may also modify the security and/or privilege of the information stored in the target.

The various instances of this model have been derived from the LNT model presented in [1] by varying the number of sources and targets. Each LNT model was then translated to LOTOS, and then to an interpreted Petri net using the CADP toolbox. Finally, a P/T net was obtained by stripping out all data-related information (variables, types, assignments, guards, etc.) from the interpreted Petri net, leading to a NUPN (Nested-Unit Petri Net) model translated to PNML using the CÆSAR.BDD tool.

References

[1] Philippe Ledent, Radu Mateescu, and Wendelin Serwe. *Testing Resource Isolation for System-on-Chip Architectures*. In F. Lang and M. Volk (editors), proceedings of the 6th International Workshop on Models for Formal Analysis of Real Systems (MARS 2024), EPTCS 399, 2024, pp. 129–168, doi:10.4204/EPTCS.399.7.

Scaling parameter

Parameter name	**Parameter description**	**Chosen parameter values**
(N, P)	N is the number of sources and P the number of targets	(8,1), (8,2), (8,3), (8,4), (8,5), (9,1), (9,2), (9,3), (9,4), (9,5), (10,1), (10,2), (10,3), (10,4), (11,1), (11,2), (11,3), (12,1), (12,2), (13,1)

Size of the model

Parameter	Number of places	Number of transitions	Number of arcs	Number of units	HWB code
$(N = 8, P = 1)$	270	4850	83436	17	9–9–54
$(N = 8, P = 2)$	309	9493	184883	19	10–10–61
$(N = 8, P = 3)$	348	18744	406138	21	11–11–68
$(N = 8, P = 4)$	387	37211	885441	23	12–12–75
$(N = 8, P = 5)$	426	74110	1917704	25	13–13–82
$(N = 9, P = 1)$	299	9484	184865	19	10–10–60
$(N = 9, P = 2)$	338	18735	406120	21	11–11–67
$(N = 9, P = 3)$	377	37202	885423	23	12–12–74
$(N = 9, P = 4)$	416	74101	1917686	25	13–13–81
$(N = 9, P = 5)$	455	147864	4129597	27	14–14–88
$(N = 10, P = 1)$	328	18726	406102	21	11–11–66
$(N = 10, P = 2)$	367	37193	885405	23	12–12–73
$(N = 10, P = 3)$	406	74092	1917668	25	13–13–80
$(N = 10, P = 4)$	445	147855	4129579	27	14–14–87
$(N = 11, P = 1)$	357	37184	885387	23	12–12–72
$(N = 11, P = 2)$	396	74083	1917650	25	13–13–79
$(N = 11, P = 3)$	435	147846	4129561	27	14–14–86
$(N = 12, P = 1)$	386	74074	1917632	25	13–13–78
$(N = 12, P = 2)$	425	147837	4129543	27	14–14–85
$(N = 13, P = 1)$	415	147828	4129525	27	14–14–84

Structural properties

ordinary — *all arcs have multiplicity one* .... yes

simple free choice — *all transitions sharing a common input place have no other input place* .... no [a]

extended free choice — *all transitions sharing a common input place have the same input places* .... no [b]

state machine — *every transition has exactly one input place and exactly one output place* .... no [c]

marked graph — *every place has exactly one input transition and exactly one output transition* .... no [d]

connected — *there is an undirected path between every two nodes (places or transitions)* .... yes [e]

strongly connected — *there is a directed path between every two nodes (places or transitions)* .... no [f]

source place(s) — *one or more places have no input transitions* .... yes [g]

sink place(s) — *one or more places have no output transitions* .... yes [h]

source transition(s) — *one or more transitions have no input places* .... no [i]

sink transitions(s) — *one or more transitions have no output places* .... no [j]

loop-free — *no transition has an input place that is also an output place* .... yes [k]

conservative — *for each transition, the number of input arcs equals the number of output arcs* .... no [l]

subconservative — *for each transition, the number of input arcs equals or exceeds the number of output arcs* .... no [m]

nested units — *places are structured into hierarchically nested sequential units* [n] .... yes

[a] stated by CÆSAR.BDD version 3.7 on all 20 instances (see the aforementioned pairs (N, P)).

[b] stated by CÆSAR.BDD version 3.7 on all 20 instances (see the aforementioned pairs (N, P)).

[c] stated by CÆSAR.BDD version 3.7 on all 20 instances (see the aforementioned pairs (N, P)).

[d] stated by CÆSAR.BDD version 3.7 on all 20 instances (see the aforementioned pairs (N, P)).

[e] stated by CÆSAR.BDD version 3.7 on all 20 instances (see the aforementioned pairs (N, P)).

[f] from place 1 one cannot reach place 0.

[g] place 0 is a source place.

[h] stated by CÆSAR.BDD version 3.7 on all 20 instances (see the aforementioned pairs (N, P)).

[i] stated by CÆSAR.BDD version 3.7 on all 20 instances (see the aforementioned pairs (N, P)).

[j] stated by CÆSAR.BDD version 3.7 on all 20 instances (see the aforementioned pairs (N, P)).

[k] stated by CÆSAR.BDD version 3.7 on all 20 instances (see the aforementioned pairs (N, P)).

[l] stated by CÆSAR.BDD version 3.7 on all 20 instances (see the aforementioned pairs (N, P)).

[m] stated by CÆSAR.BDD version 3.7 on all 20 instances (see the aforementioned pairs (N, P)).

[n] the definition of Nested-Unit Petri Nets (NUPN) is available from `http://mcc.lip6.fr/nupn.php`

Behavioural properties

safe — *in every reachable marking, there is no more than one token on a place* . . . . yes [o]
dead place(s) — *one or more places have no token in any reachable marking* . . . . no [p]
dead transition(s) — *one or more transitions cannot fire from any reachable marking* . . . . no [q]
deadlock — *there exists a reachable marking from which no transition can be fired* . . . . yes [r]
reversible — *from every reachable marking, there is a transition path going back to the initial marking* . . . . no [s]
live — *for every transition t, from every reachable marking, one can reach a marking in which t can fire* . . . . no [t]

Size of the marking graphs

Parameter	Number of reachable markings	Number of transition firings	Max. number of tokens per place	Max. number of tokens per marking
$(N = 8, P = 1)$	1.12511e+09 [u]	?	1	9
$(N = 8, P = 2)$	1.22751e+10 [v]	?	1	10
$(N = 8, P = 3)$	1.34642e+11 [w]	?	1	11
$(N = 8, P = 4)$	1.47929e+12 [x]	?	1	12
$(N = 8, P = 5)$	1.62629e+13 [y]	?	1	13
$(N = 9, P = 1)$	1.11812e+10 [z]	?	1	10
$(N = 9, P = 2)$	1.22431e+11 [aa]	?	1	11
$(N = 9, P = 3)$	1.34476e+12 [ab]	?	1	12
$(N = 9, P = 4)$	1.47835e+13 [ac]	?	1	13
$(N = 9, P = 5)$	1.62572e+14 [ad]	?	1	14
$(N = 10, P = 1)$	1.11462e+11 [ae]	?	1	11
$(N = 10, P = 2)$	1.22271e+12 [af]	?	1	12
$(N = 10, P = 3)$	1.34394e+13 [ag]	?	1	13
$(N = 10, P = 4)$	1.47788e+14 [ah]	?	1	14
$(N = 11, P = 1)$	1.11287e+12 [ai]	?	1	12
$(N = 11, P = 2)$	1.22191e+13 [aj]	?	1	13
$(N = 11, P = 3)$	1.34352e+14 [ak]	?	1	14
$(N = 12, P = 1)$	1.11199e+13 [al]	?	1	13
$(N = 12, P = 2)$	1.22151e+14 [am]	?	1	14
$(N = 13, P = 1)$	1.11155e+14 [an]	?	1	14

[o] safe by construction – stated by the CÆSAR compiler.
[p] stated by CÆSAR.BDD version 3.7 on all 20 instances (see the aforementioned pairs (N, P)).
[q] stated by CÆSAR.BDD version 3.7 on all 20 instances (see the aforementioned pairs (N, P)).
[r] stated by CÆSAR.BDD version 3.7 on all 20 instances (see the aforementioned pairs (N, P)).
[s] the marking graph has deadlocks and contains more than one reachable marking.
[t] the net has at least one transition and its marking graph has deadlocks.
[u] stated by CÆSAR.BDD version 3.7.
[v] stated by CÆSAR.BDD version 3.7.
[w] stated by CÆSAR.BDD version 3.7.
[x] stated by CÆSAR.BDD version 3.7.
[y] stated by CÆSAR.BDD version 3.7.
[z] stated by CÆSAR.BDD version 3.7.
[aa] stated by CÆSAR.BDD version 3.7.
[ab] stated by CÆSAR.BDD version 3.7.
[ac] stated by CÆSAR.BDD version 3.7.
[ad] stated by CÆSAR.BDD version 3.7.
[ae] stated by CÆSAR.BDD version 3.7.
[af] stated by CÆSAR.BDD version 3.7.
[ag] stated by CÆSAR.BDD version 3.7.
[ah] stated by CÆSAR.BDD version 3.7.
[ai] stated by CÆSAR.BDD version 3.7.
[aj] stated by CÆSAR.BDD version 3.7.
[ak] stated by CÆSAR.BDD version 3.7.
[al] stated by CÆSAR.BDD version 3.7.
[am] stated by CÆSAR.BDD version 3.7.

[an] stated by CÆSAR.BDD version 3.7.