Fabrice Kordon
Fabrice.Kordon@lip6.fr

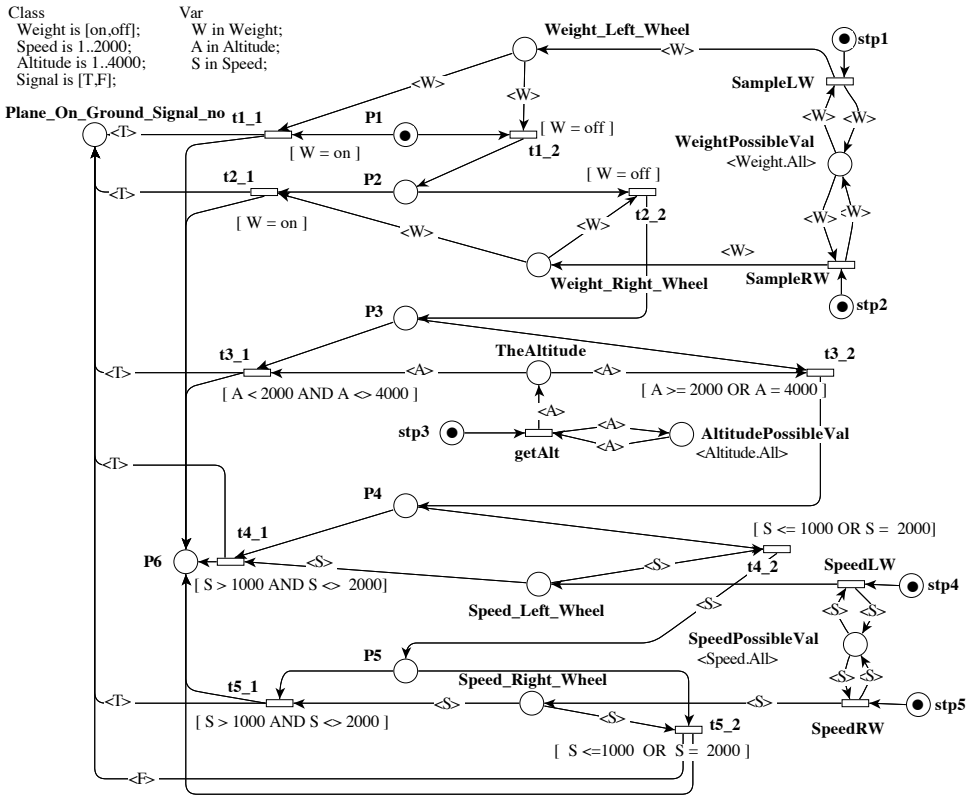
This form is a summary description of the model entitled "AirplaneLD" proposed for the Model Checking Contest @ Petri Nets. Models can be given in several instances parameterized by scaling parameters. Colored nets can be accompanied by one or many equivalent, unfolded P/T nets. Models are given together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

Description

This model was elaborated during a joint project with ONERA and Sextant Avionique dealing with the modeling and verification of critical components in airplane systems. This is a simplified version of a landing detector used to activate the flaps in the system.

The parameter of his model is used to deduce the maximum speed, the maximum altitude and two threshold values for the system (these threshold values are different from the original model, this does not change the complexity of the model).

In March 2020, Pierre Bouvier and Hubert Garavel provided a decomposition of all instances of this model into networks of communicating automata. Each network is expressed as a Nested-Unit Petri Net (NUPN) that can be found, for each instance, in the "toolspecific" section of the corresponding PNML file.



Graphical representation for $N = 1000$

References

[1] A. Diagne, P. Estraillier, F. Kordon, I. Vernier, J. Cazin, M. Doche, C. Seguin, and V. Wiels. Spécification et validation modulaires de systèmes avioniques : Projet FORMA – opération Vamos. Technical Report 4/3599.00/DERI, ONERA – CERT, December 1997.

Fabrice Kordon
Fabrice.Kordon@lip6.fr

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
N	A value from wich the maximum speed, the maximum altitude, and the associated thresholds are computed	10, 20, 50, 100, 200, 500, 1000, 2000, 4000

Size of the colored net model

number of places: 20
number of transitions: 15
number of arcs: 56

Size of the derived P/T model instances

Parameter	Number of places	Number of transitions	Number of arcs	Number of units	HWB code
$N = 10$	89	88	333	39	1–38–20
$N = 20$	159	168	638	69	1–68–23
$N = 50$	369	408	1553	159	1–158–26
$N = 100$	719	808	3078	309	1–308–29
$N = 200$	1419	1608	6128	609	1–608–32
$N = 500$	3519	4008	15278	1509	1–1508–35
$N = 1000$	7019	8008	30528	3009	1–3008–38
$N = 2000$	14019	16008	61028	6009	1–6008–41
$N = 4000$	28019	32008	122028	12009	1–12008–44

Structural properties

ordinary — *all arcs have multiplicity one* ..... ✔
simple free choice — *all transitions sharing a common input place have no other input place* ..... ✘ [a]
extended free choice — *all transitions sharing a common input place have the same input places* ..... ✘ [b]
state machine — *every transition has exactly one input place and exactly one output place* ..... ✘ [c]
marked graph — *every place has exactly one input transition and exactly one output transition* ..... ✘ [d]
connected — *there is an undirected path between every two nodes (places or transitions)* ..... ✔ [e]
strongly connected — *there is a directed path between every two nodes (places or transitions)* ..... ✘ [f]
source place(s) — *one or more places have no input transitions* ..... ✔ [g]
sink place(s) — *one or more places have no output transitions* ..... ✔ [h]
source transition(s) — *one or more transitions have no input places* ..... ✘ [i]
sink transitions(s) — *one or more transitions have no output places* ..... ✘ [j]
loop-free — *no transition has an input place that is also an output place* ..... ✘ [k]
conservative — *for each transition, the number of input arcs equals the number of output arcs* ..... ✘ [l]
subconservative — *for each transition, the number of input arcs equals or exceeds the number of output arcs* ..... ✔ [m]

[a] stated by CÆSAR.BDD version 2.6 on all 9 instances (10, 20, 50, 100, 200, 500, 1000, 2000, and 4000).
[b] stated by CÆSAR.BDD version 2.6 on all 9 instances (10, 20, 50, 100, 200, 500, 1000, 2000, and 4000).
[c] stated by CÆSAR.BDD version 2.6 on all 9 instances (10, 20, 50, 100, 200, 500, 1000, 2000, and 4000).
[d] stated by CÆSAR.BDD version 2.6 on all 9 instances (10, 20, 50, 100, 200, 500, 1000, 2000, and 4000).
[e] stated by CÆSAR.BDD version 2.6 on all 9 instances (10, 20, 50, 100, 200, 500, 1000, 2000, and 4000).
[f] stated by CÆSAR.BDD version 2.6 on all 9 instances (10, 20, 50, 100, 200, 500, 1000, 2000, and 4000).
[g] there exist 6 source places, e.g., place “stp3”.
[h] there exist 3 sink places, e.g., place “Plane_On_Ground_Signal_no_F”.
[i] stated by CÆSAR.BDD version 2.6 on all 9 instances (10, 20, 50, 100, 200, 500, 1000, 2000, and 4000).
[j] stated by CÆSAR.BDD version 2.6 on all 9 instances (10, 20, 50, 100, 200, 500, 1000, 2000, and 4000).
[k] stated by CÆSAR.BDD version 2.6 on all 9 instances (10, 20, 50, 100, 200, 500, 1000, 2000, and 4000).
[l] stated by CÆSAR.BDD version 2.6 on all 9 instances (10, 20, 50, 100, 200, 500, 1000, 2000, and 4000).
[m] stated by CÆSAR.BDD version 2.6 on all 9 instances (10, 20, 50, 100, 200, 500, 1000, 2000, and 4000).

Fabrice Kordon
Fabrice.Kordon@lip6.fr

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

Behavioural properties

safe — *in every reachable marking, there is no more than one token on a place* ..... ✔ [o]
dead place(s) — *one or more places have no token in any reachable marking* ..... ? [p]
dead transition(s) — *one or more transitions cannot fire from any reachable marking* ..... ? [q]
deadlock — *there exists a reachable marking from which no transition can be fired* ..... ? [r]
reversible — *from every reachable marking, there is a transition path going back to the initial marking* ..... ? [s]
live — *for every transition t, from every reachable marking, one can reach a marking in which t can fire* ..... ? [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
$N = 10$	43 463 [u]	183 664 [v]	1	38 [w]
$N = 20$	30 8303 [x]	1.3391×10^6 [y]	1	68 [z]
$N = 50$	4.47122×10^6 [aa]	?	1	158 [ab]
$N = 100$	3.48774×10^7 [ac]	?	1	308 [ad]
$N = 200$	2.75495e+08 [ae]	?	1	608 [af]
$N = 500$	4.27179e+09 [ag]	?	1	1508 [ah]
$N = 1000$	?	?	1	3008 [ai]
$N = 2000$	?	?	1	6008 [aj]
$N = 4000$	?	?	1	12008 [ak]

[n] the definition of Nested-Unit Petri Nets (NUPN) is available from http://mcc.lip6.fr/nupn.php
[o] stated by the BOUNDS tool of CosyVerif version 1.0 on all 9 instances (10, 20, 50, 100, 200, 500, 1000, 2000, and 4000).
[p] stated by CÆSAR.BDD version 3.5 to be false on 8 instance(s) out of 9, and unknown on the remaining instance.
[q] stated by CÆSAR.BDD version 3.5 to be false on 8 instance(s) out of 9, and unknown on the remaining instance.
[r] stated by CÆSAR.BDD version 3.5 to be true on 8 instance(s) out of 9, and unknown on the remaining instance.
[s] stated by CÆSAR.BDD version 3.5 to be false on 8 instance(s) out of 9, and unknown on the remaining instance.
[t] stated by CÆSAR.BDD version 3.5 to be false on 8 instance(s) out of 9, and unknown on the remaining instance.
[u] stated by Prod and CÆSAR.BDD version 2.6.
[v] stated by Prod in January 2016.
[w] number of initial tokens, because the net is sub-conservative.
[x] stated by Prod and CÆSAR.BDD version 2.6.
[y] stated by Prod in January 2016.
[z] number of initial tokens, because the net is sub-conservative.
[aa] stated by CÆSAR.BDD version 2.6.
[ab] number of initial tokens, because the net is sub-conservative.
[ac] stated by CÆSAR.BDD version 2.6.
[ad] number of initial tokens, because the net is sub-conservative.
[ae] stated by CÆSAR.BDD version 3.3.
[af] number of initial tokens, because the net is sub-conservative.
[ag] stated by CÆSAR.BDD version 3.3.
[ah] number of initial tokens, because the net is sub-conservative.
[ai] number of initial tokens, because the net is sub-conservative.
[aj] number of initial tokens, because the net is sub-conservative.
[ak] number of initial tokens, because the net is sub-conservative.