Fatma Jebali and Eric Jenn
fatma.jebali@inria.fr

This form is a summary description of the model entitled "AutoFlight Control System" 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 is derived from a subsystem of an AutoFlight Control System (AFCS) provided by Thales Avionics. The AFCS improves the quality of flight and enhances the operational capability of an aircraft. The architecture of the model comprises two parts: the FCP (*Flight Control Panel*), which enables the pilot to interact with the system, and the AFS (*Automatic Flight System*), which acquires the altitude target. Each part is divided into a command channel, which implements the expected functionality, and a monitoring channel, which checks whether the command channel operates correctly. Communications are performed using various protocols (AFDX, A429, etc.). To ensure availability, a high level of redundancy is built inside the system.

This collection of P/T nets was derived from a GRL model of the AFCS, seen as a GALS (*Globally Asynchronous, Locally Synchronous*) system. Each instance was first translated to LNT, then to LOTOS, and then to an interpreted Petri net using the GRL2LNT compiler and 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.

Each instance of the model is parameterized by the number N of times a given component is replicated to ensure redundancy. For the purpose of the Model Checking Contest, N has been given some large values that may not be found in real aircrafts.

Each instance is also parameterized by its version V, which specifies how the NUPN has been produced from the LOTOS specification. V is either equal to "a" if the NUPN has been generated *after* applying all the structural and data-flow optimizations of the CÆSAR compiler for LOTOS, or to "b" if the NUPN has been generated *before* these optimizations.

References

[1] Pierre-Alain Bourdil, Bernard Berthomieu, and Eric Jenn. *Model-Checking Real-Time Properties of an AutoFlight Control System Function.* Proceedings of the 2014 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW'14), pages 120–123, IEEE Computer Society, 2014. Available from http://dx.doi.org/10.1109/ISSREW.2014.40.

[2] Fatma Jebali, Frédéric Lang, and Radu Mateescu. *GRL: A Specification Language for Globally Asynchronous Locally Synchronous Systems.* Proceedings of the 16th International Conference on Formal Engineering Methods (ICFEM'14), Luxembourg. LNCS 8829, pages 219–234, Springer, 2014. Available from https://hal.inria.fr/hal-01082348.

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
(N, V)	N is the number of times each component is replicated and V is the version defined above	$\{1, 2, 3, 4, 5, 6, 12, 24, 48, 96\} \times \{a, b\}$

Fatma Jebali and Eric Jenn
fatma.jebali@inria.fr

Size of the model

Parameter	Number of places	Number of transitions	Number of arcs	Number of units	HWB code
$N = 1, V = a$	32	30	100	10	2–9–20
$N = 1, V = b$	114	112	264	17	6–9–45
$N = 2, V = a$	57	55	180	16	2–15–33
$N = 2, V = b$	206	204	478	29	11–15–77
$N = 3, V = a$	82	80	260	22	2–21–45
$N = 3, V = b$	298	296	692	41	16–21–109
$N = 4, V = a$	107	105	340	28	2–27–57
$N = 4, V = b$	390	388	906	53	21–27–140
$N = 5, V = a$	132	130	420	34	2–33–68
$N = 5, V = b$	482	480	1120	65	26–33–171
$N = 6, V = a$	157	155	500	40	2–39–80
$N = 6, V = b$	574	572	1334	77	31–39–203
$N = 12, V = a$	307	305	980	76	2–75–147
$N = 12, V = b$	1126	1124	2618	149	61–75–391
$N = 24, V = a$	607	605	1940	148	2–147–281
$N = 24, V = b$	2230	2228	5186	293	121–147–764
$N = 48, V = a$	1127	1113	3458	258	2–257–499
$N = 48, V = b$	3950	3936	9104	513	205–257–1333
$N = 96, V = a$	2251	2225	6914	514	2–513–995
$N = 96, V = b$	7894	7868	18200	1025	409–513–2663

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

[a] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).
[b] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).
[c] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).
[d] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).
[e] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).
[f] from place 1 one cannot reach place 0.
[g] place 0 is a source place.
[h] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).
[i] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).
[j] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).
[k] stated by CÆSAR.BDD version 2.6 to be true on 10 instance(s) out of 20, and false on the remaining 10 instance(s).
[l] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).
[m] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).
[n] the definition of Nested-Unit Petri Nets (NUPN) is available from http://mcc.lip6.fr/nupn.php

Fatma Jebali and Eric Jenn
fatma.jebali@inria.fr

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
$N = 1, V = a$	253 [u]	?	1	9
$N = 1, V = b$	4.8882e+07 [v]	?	1	9
$N = 2, V = a$	6949 [w]	?	1	15
$N = 2, V = b$	1.61545e+13 [x]	?	1 [y]	15
$N = 3, V = a$	157681 [z]	?	1	21
$N = 3, V = b$	$\geq$ 1.93957e+18 [aa]	?	1	21
$N = 4, V = a$	3.33202e+06 [ab]	?	1	27
$N = 4, V = b$	$\geq$ 1.8815e+23 [ac]	?	1	27
$N = 5, V = a$	6.818e+07 [ad]	?	1	33
$N = 5, V = b$	$\geq$ 8.49661e+27 [ae]	?	1 [af]	33
$N = 6, V = a$	1.37192e+09 [ag]	?	1	39
$N = 6, V = b$	$\geq$ 8.93441e+32 [ah]	?	1 [ai]	39
$N = 12, V = a$	$\geq$ 6.59488e+16 [aj]	?	1 [ak]	75
$N = 12, V = b$	$\geq$ 5.95493e+62 [al]	?	1 [am]	75
$N = 24, V = a$	$\geq$ 2.04086e+27 [an]	?	1 [ao]	147
$N = 24, V = b$	$\geq$ 7.21195e+122 [ap]	?	1 [aq]	147
$N = 48, V = a$	$\geq$ 5.43952e+41 [ar]	?	1 [as]	257
$N = 48, V = b$	$\geq$ 1.92227e+213 [at]	?	1 [au]	257
$N = 96, V = a$	$\geq$ 1.85519e+74 [av]	?	1 [aw]	513
$N = 96, V = b$	?	?	1 [ax]	513

[o] safe by construction – stated by the CÆSAR compiler.
[p] stated by CÆSAR.BDD version 3.3 to be true on 1 instance(s) out of 7, and unknown on the remaining 6 instance(s).
[q] stated by CÆSAR.BDD version 2.6 to be false on 9 instance(s) out of 20, and unknown on the remaining 11 instance(s).
[r] stated by CÆSAR.BDD version 2.6 to be true on 8 instance(s) out of 20, and unknown on the remaining 12 instance(s).
[s] stated by CÆSAR.BDD version 2.6 to be false on 8 instance(s) out of 20, and unknown on the remaining 12 instance(s).
[t] stated by CÆSAR.BDD version 2.6 to be false on 8 instance(s) out of 20, and unknown on the remaining 12 instance(s).
[u] stated by CÆSAR.BDD version 2.6.
[v] stated by CÆSAR.BDD version 2.6.
[w] stated by CÆSAR.BDD version 2.6.
[x] stated by CÆSAR.BDD version 2.6.
[y] stated by the CÆSAR compiler.
[z] stated by CÆSAR.BDD version 2.6.
[aa] stated by CÆSAR.BDD version 2.6.
[ab] stated by CÆSAR.BDD version 2.6.
[ac] stated by CÆSAR.BDD version 2.6.
[ad] stated by CÆSAR.BDD version 2.6.
[ae] stated by CÆSAR.BDD version 2.6.
[af] stated by the CÆSAR compiler.
[ag] stated by CÆSAR.BDD version 2.6.
[ah] stated by CÆSAR.BDD version 2.6.
[ai] stated by the CÆSAR compiler.
[aj] stated by CÆSAR.BDD version 2.6.
[ak] stated by the CÆSAR compiler.
[al] stated by CÆSAR.BDD version 2.6.
[am] stated by the CÆSAR compiler.

Fatma Jebali and Eric Jenn
fatma.jebali@inria.fr

(an) stated by CÆSAR.BDD version 2.6.
(ao) stated by the CÆSAR compiler.
(ap) stated by CÆSAR.BDD version 2.6.
(aq) stated by the CÆSAR compiler.
(ar) stated by CÆSAR.BDD version 2.6.
(as) stated by the CÆSAR compiler.
(at) stated by CÆSAR.BDD version 3.3.
(au) stated by the CÆSAR compiler.
(av) stated by CÆSAR.BDD version 2.6.
(aw) stated by the CÆSAR compiler.
(ax) stated by the CÆSAR compiler.