Aymane Bouzafour, Marc Renaudin, and Hubert Garavel
aymane.bouzafour@tiempo-secure.com

since
MCC 2018

This form is a summary description of the model entitled "ASLink" 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

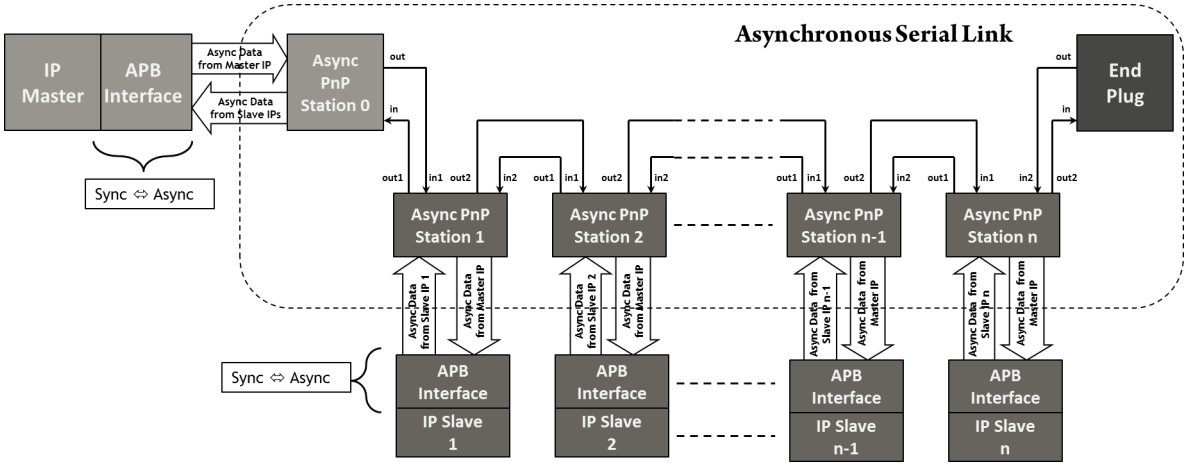
This model describes a hardware circuit component designed at Tiempo Secure [(a)], namely, an on-chip asynchronous serial link, the architecture of which is illustrated in the Figure below. This link enables the interconnection of a set of IP [(b)] slaves designed by other vendors. Each IP slave is synchronous, must be reused as such, and can be accessed through a standard interface such as ARM's AMBA-APB [(c)].

The asynchronous serial link establishes a bridge between, on the one hand, the set of IP slaves, which are daisy-chained, and, on the other hand, a synchronous master IP. It is easily configurable to fit any number of IP slaves and locations. A key feature of the link is its design based on asynchronous logics [1][2], which brings physical and logical reliability (due to the delay-insensitive implementation) and easy integration in SoCs [(d)] with multiple power and clock domains (because of the variability tolerance, the absence of clock, and the low wire count of the asynchronous implementation).

Following the modelling and verification methodology [3] adopted at Tiempo Secure, the asynchronous serial link was formally specified using the LNT language supported by the verification tools available in the CADP toolbox. The considered LNT specification covers the architectural part delimited by the dashed line in the Figure below. A scalable family of ten LNT specifications was made by increasing from one to ten the number of IP slaves connected to the asynchronous link.

Each LNT specification was translated automatically 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.

Each instance of the model is parameterized by the number N of IP slaves, and also 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.



Architecture of the Asynchronous Serial Link

[(a)] http://www.tiempo-secure.com
[(b)] see http://en.wikipedia.org/wiki/Semiconductor_intellectual_property_core
[(c)] see http://en.wikipedia.org/wiki/Advanced_Microcontroller_Bus_Architecture
[(d)] see http://en.wikipedia.org/wiki/System_on_a_chip

Aymane Bouzafour, Marc Renaudin, and Hubert Garavel
aymane.bouzafour@tiempo-secure.com

References

[1] Marc Renaudin. *Asynchronous Circuits and Systems: A Promising Design Alternative.* In *Microelectronics for Telecommunications: Managing High Complexity and Mobility* (MIGAS'2000), special issue of the Microelectronics Engineering Journal, vol. 54, num. 1–2, Elsevier, Dec. 2000.

[2] Jens Sparsø. *Asynchronous Circuit Design: A Tutorial.* Technical University of Denmark, March 2006. Available from http://www.imm.dtu.dk/~jsp.

[3] Aymane Bouzafour, Marc Renaudin, Hubert Garavel, Radu Mateescu, and Wendelin Serwe. *Model-checking Synthesizable SystemVerilog Descriptions of Asynchronous Circuits.* In Proceedings of the 24th IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC'18), Vienna, Austria, May 2018.

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
N	N is the number of IP slaves	from 1 to 10

Size of the model

Parameter	Number of places	Number of transitions	Number of arcs	Number of units	HWB code
$N = 01, V = a$	431	735	2801	83	4–75–196
$N = 01, V = b$	846	1148	3624	105	12–75–284
$N = 02, V = a$	626	1008	3820	118	4–104–281
$N = 02, V = b$	1242	1621	5041	153	13–104–409
$N = 03, V = a$	821	1281	4839	153	4–133–366
$N = 03, V = b$	1638	2094	6458	201	14–133–534
$N = 04, V = a$	1016	1554	5858	188	4–162–451
$N = 04, V = b$	2034	2567	7875	249	15–162–659
$N = 05, V = a$	1211	1827	6877	223	4–191–536
$N = 05, V = b$	2430	3040	9292	297	16–191–784
$N = 06, V = a$	1406	2100	7896	258	4–220–621
$N = 06, V = b$	2826	3513	10709	345	17–220–909
$N = 07, V = a$	1601	2373	8915	293	4–249–706
$N = 07, V = b$	3222	3986	12126	393	18–249–1034
$N = 08, V = a$	1796	2646	9934	328	4–278–791
$N = 08, V = b$	3618	4459	13543	441	19–278–1159
$N = 09, V = a$	1991	2919	10953	363	4–307–876
$N = 09, V = b$	4014	4932	14960	489	20–307–1284
$N = 10, V = a$	2186	3192	11972	398	4–336–961
$N = 10, V = b$	4410	5405	16377	537	21–336–1409

Structural properties

ordinary — *all arcs have multiplicity one* ..... ✔
simple free choice — *all transitions sharing a common input place have no other input place* ..... ✗ [e]
extended free choice — *all transitions sharing a common input place have the same input places* ..... ✗ [f]
state machine — *every transition has exactly one input place and exactly one output place* ..... ✗ [g]
marked graph — *every place has exactly one input transition and exactly one output transition* ..... ✗ [h]
connected — *there is an undirected path between every two nodes (places or transitions)* ..... ✔ [i]

[e] stated by CÆSAR.BDD version 2.7 on all 20 instances (10 values of N).
[f] stated by CÆSAR.BDD version 2.7 on all 20 instances (10 values of N).
[g] stated by CÆSAR.BDD version 2.7 on all 20 instances (10 values of N).
[h] stated by CÆSAR.BDD version 2.7 on all 20 instances (10 values of N).
[i] stated by CÆSAR.BDD version 2.7 on all 20 instances (10 values of N).

Aymane Bouzafour, Marc Renaudin, and Hubert Garavel
aymane.bouzafour@tiempo-secure.com

strongly connected — *there is a directed path between every two nodes (places or transitions)* ..... ✗ (j)
source place(s) — *one or more places have no input transitions* ..... ✓ (k)
sink place(s) — *one or more places have no output transitions* ..... ✗ (l)
source transition(s) — *one or more transitions have no input places* ..... ✗ (m)
sink transitions(s) — *one or more transitions have no output places* ..... ✗ (n)
loop-free — *no transition has an input place that is also an output place* ..... ✓ (o)
conservative — *for each transition, the number of input arcs equals the number of output arcs* ..... ✗ (p)
subconservative — *for each transition, the number of input arcs equals or exceeds the number of output arcs* ..... ✗ (q)
nested units — *places are structured into hierarchically nested sequential units* (r) ..... ✓

Behavioural properties

safe — *in every reachable marking, there is no more than one token on a place* ..... ✓ (s)
deadlock — *there exists a reachable marking from which no transition can be fired* ..... ?
reversible — *from every reachable marking, there is a transition path going back to the initial marking* ..... ?
quasi-live — *for every transition t, there exists a reachable marking in which t can fire* ..... ?
live — *for every transition t, from every reachable marking, one can reach a marking in which t can fire* ..... ?

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
$N = 01, V = a$	$\geq$ 5.73973e+07 (t)	?	1 (u)	$\in [17, 75]$ (v)
$N = 01, V = b$	$\geq$ 6.31258e+10 (w)	?	1 (x)	$\in [2, 75]$ (y)
$N = 02, V = a$	$\geq$ 4.57198e+08 (z)	?	1 (aa)	$\in [26, 104]$ (ab)
$N = 02, V = b$	$\geq$ 5.60932e+12 (ac)	?	1 (ad)	$\in [2, 104]$ (ae)
$N = 03, V = a$	$\geq$ 290305 (af)	?	1 (ag)	$\in [35, 133]$ (ah)
$N = 03, V = b$	$\geq$ 1.24479e+22 (ai)	?	1 (aj)	$\in [2, 133]$ (ak)
$N = 04, V = a$	$\geq$ 6.9673e+06 (al)	?	1 (am)	$\in [44, 162]$ (an)
$N = 04, V = b$	$\geq$ 4.86333e+27 (ao)	?	1 (ap)	$\in [2, 162]$ (aq)
$N = 05, V = a$	$\geq$ 1.67215e+08 (ar)	?	1 (as)	$\in [53, 191]$ (at)
$N = 05, V = b$	$\geq$ 1.27462e+33 (au)	?	1 (av)	$\in [2, 191]$ (aw)
$N = 06, V = a$	$\geq$ 2.08612e+20 (ax)	?	1 (ay)	$\in [62, 220]$ (az)
$N = 06, V = b$	$\geq$ 3.43882e+38 (ba)	?	1 (bb)	$\in [2, 220]$ (bc)
$N = 07, V = a$	$\geq$ 2.00858e+23 (bd)	?	1 (be)	$\in [71, 249]$ (bf)
$N = 07, V = b$	?	?	1 (bg)	$\in [2, 249]$ (bh)
$N = 08, V = a$	$\geq$ 1.25256e+26 (bi)	?	1 (bj)	$\in [80, 278]$ (bk)
$N = 08, V = b$	?	?	1 (bl)	$\in [2, 278]$ (bm)
$N = 09, V = a$	$\geq$ 1.18847e+29 (bn)	?	1 (bo)	$\in [89, 307]$ (bp)
$N = 09, V = b$	?	?	1 (bq)	$\in [2, 307]$ (br)
$N = 10, V = a$	?	?	1 (bs)	$\in [98, 336]$ (bt)
$N = 10, V = b$	?	?	1 (bu)	$\in [2, 336]$ (bv)

(j) from place 1 one cannot reach place 0.
(k) place 0 is a source place.
(l) stated by CÆSAR.BDD version 2.7 on all 20 instances (10 values of N).
(m) stated by CÆSAR.BDD version 2.7 on all 20 instances (10 values of N).
(n) stated by CÆSAR.BDD version 2.7 on all 20 instances (10 values of N).
(o) stated by CÆSAR.BDD version 2.7 on all 20 instances (10 values of N).
(p) stated by CÆSAR.BDD version 2.7 on all 20 instances (10 values of N).
(q) stated by CÆSAR.BDD version 2.7 on all 20 instances (10 values of N).
(r) the definition of Nested-Unit Petri Nets (NUPN) is available from http://mcc.lip6.fr/nupn.php
(s) safe by construction – stated by the CÆSAR compiler.
(t) stated by CÆSAR.BDD version 2.7.

Aymane Bouzafour, Marc Renaudin, and Hubert Garavel
aymane.bouzafour@tiempo-secure.com

(u) stated by the CÆSAR compiler.
(v) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(w) stated by CÆSAR.BDD version 2.7.
(x) stated by the CÆSAR compiler.
(y) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(z) stated by CÆSAR.BDD version 2.7.
(aa) stated by the CÆSAR compiler.
(ab) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(ac) stated by CÆSAR.BDD version 2.7.
(ad) stated by the CÆSAR compiler.
(ae) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(af) stated by CÆSAR.BDD version 2.7.
(ag) stated by the CÆSAR compiler.
(ah) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(ai) stated by CÆSAR.BDD version 2.7.
(aj) stated by the CÆSAR compiler.
(ak) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(al) stated by CÆSAR.BDD version 2.7.
(am) stated by the CÆSAR compiler.
(an) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(ao) stated by CÆSAR.BDD version 2.7.
(ap) stated by the CÆSAR compiler.
(aq) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(ar) stated by CÆSAR.BDD version 2.7.
(as) stated by the CÆSAR compiler.
(at) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(au) stated by CÆSAR.BDD version 2.7.
(av) stated by the CÆSAR compiler.
(aw) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(ax) stated by CÆSAR.BDD version 2.7.
(ay) stated by the CÆSAR compiler.
(az) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(ba) stated by CÆSAR.BDD version 2.7.
(bb) stated by the CÆSAR compiler.
(bc) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(bd) stated by CÆSAR.BDD version 2.7.
(be) stated by the CÆSAR compiler.
(bf) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(bg) stated by the CÆSAR compiler.
(bh) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(bi) stated by CÆSAR.BDD version 2.7.
(bj) stated by the CÆSAR compiler.
(bk) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(bl) stated by the CÆSAR compiler.
(bm) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(bn) stated by CÆSAR.BDD version 2.7.
(bo) stated by the CÆSAR compiler.
(bp) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(bq) stated by the CÆSAR compiler.
(br) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(bs) stated by the CÆSAR compiler.
(bt) lower and upper bounds given by the number of initial tokens and the number of leaf units.
(bu) stated by the CÆSAR compiler.
(bv) lower and upper bounds given by the number of initial tokens and the number of leaf units.