Hubert Garavel
hubert.garavel@inria.fr

This form is a summary description of the model entitled "FireWire" 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.

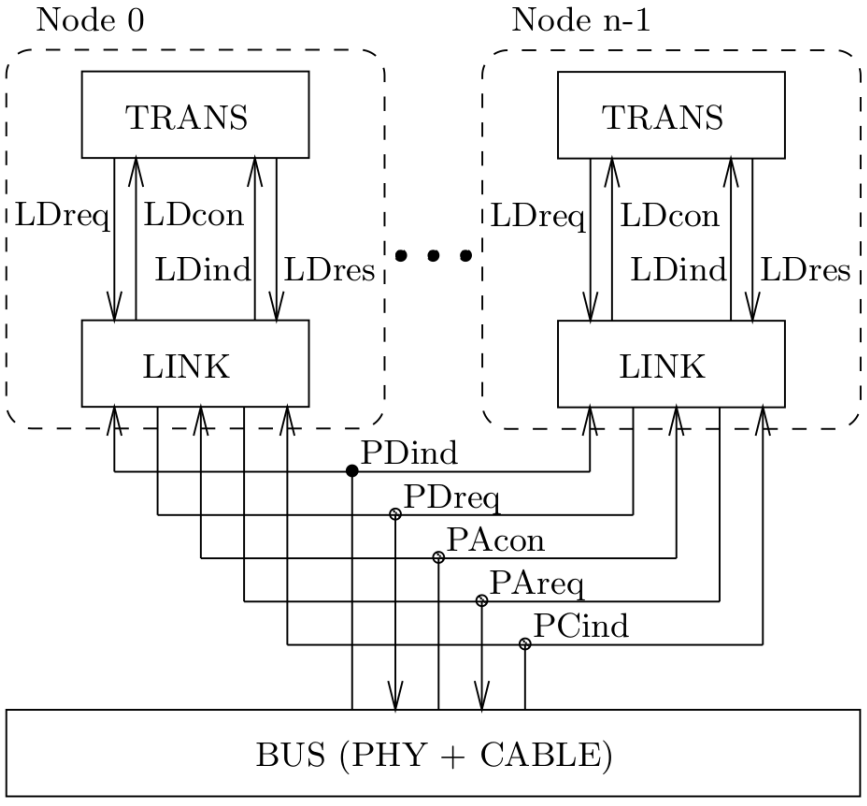
Description

IEEE 1394 (also called "FireWire") is an interface standard that specifies a serial bus architecture for high-speed communications. It can connect up to 63 peripherals in a tree or daisy-chain topology, and can perform both asynchronous and isochronous transfers simultaneously. It was developed between 1986 and 1995 by a large consortium gathering Apple, Panasonic, Philips, Sony, and many others contributors. This work resulted in an IEEE standard, followed by integration in many industrial products.

The asynchronous mode of the link layer protocol of IEEE 1394 was selected as an interesting case study for formal methods. Various formal specifications have been developed for it. Some of these specifications have been expressed in LOTOS or in LNT, a modern language that can be translated to LOTOS automatically [1] [2].

Each LOTOS specification (either written by hand or generated automatically) was then translated an interpreted Petri net using the CADP toolbox. A P/T net was than 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.

We kept only the NUPNs whose marking graphs had more than one million states, discarding other NUPNs that were considered too simple for the Model Checking Contest. This led to a collection of 20 NUPNs, which we ordered by increasing number of places.



The IEEE 1394 ("FireWire") serial bus protool

Hubert Garavel
hubert.garavel@inria.fr

References

[1] Mihaela Sighireanu and Radu Mateescu. *Validation of the Link Layer Protocol of the IEEE-1394 Serial Bus ("FireWire"): an Experiment with E-LOTOS.* In Proceedings of the 2nd COST 247 International Workshop on Applied Formal Methods in System Design (Zagreb, Croatia), June 1997. Full version of this paper is available as INRIA Research Report RR-3172.

[2] Hubert Garavel and Bas Luttik. *Four Formal Models of IEEE 1394 Link Layer.* 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. 21–100, doi:10.4204/EPTCS.399.5.

The source LNT and LOTOS files modelling the FireWire link layer are available from http://cadp.inria.fr/ftp/demos/demo_23.

Scaling parameter

Parameter name	Parameter description	Chosen parameter values
N	N is the instance number	from 1 to 20

Size of the model

Parameter	Number of places	Number of transitions	Number of arcs	Number of units	HWB code
$N = 1$	107	346	1271	10	2–9–31
$N = 2$	108	355	1311	10	2–9–31
$N = 3$	112	356	1308	10	2–9–32
$N = 4$	113	364	1349	10	2–9–31
$N = 5$	114	373	1389	10	2–9–31
$N = 6$	116	368	1362	10	2–9–32
$N = 7$	126	396	1471	10	2–9–32
$N = 8$	127	397	1475	10	2–9–32
$N = 9$	130	408	1525	10	2–9–32
$N = 10$	131	409	1529	10	2–9–32
$N = 11$	169	508	1883	14	2–13–41
$N = 12$	169	508	1889	14	2–13–41
$N = 13$	205	610	2309	14	2–13–41
$N = 14$	205	610	2315	14	2–13–41
$N = 15$	248	383	1144	9	5–5–31
$N = 16$	254	368	1032	9	5–5–32
$N = 17$	428	656	1904	17	6–9–57
$N = 18$	437	707	2170	17	6–9–56
$N = 19$	602	944	2776	25	7–13–82
$N = 20$	626	1031	3196	25	7–13–81

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]

[a] stated by CÆSAR.BDD version 3.7 on all 20 instances (20 values of N).
[b] stated by CÆSAR.BDD version 3.7 on all 20 instances (20 values of N).
[c] stated by CÆSAR.BDD version 3.7 on all 20 instances (20 values of N).
[d] stated by CÆSAR.BDD version 3.7 on all 20 instances (20 values of N).
[e] stated by CÆSAR.BDD version 3.7 on all 20 instances (20 values of N).

Hubert Garavel
hubert.garavel@inria.fr

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) ..... ✔

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)

(f) from place 1 one cannot reach place 0.
(g) place 0 is a source place.
(h) stated by CÆSAR.BDD version 3.7 to be true on 6 instance(s) out of 20, and false on the remaining 14 instance(s).
(i) stated by CÆSAR.BDD version 3.7 on all 20 instances (20 values of N).
(j) stated by CÆSAR.BDD version 3.7 on all 20 instances (20 values of N).
(k) stated by CÆSAR.BDD version 3.7 to be true on 6 instance(s) out of 20, and false on the remaining 14 instance(s).
(l) stated by CÆSAR.BDD version 3.7 on all 20 instances (20 values of N).
(m) stated by CÆSAR.BDD version 3.7 on all 20 instances (20 values of N).
(n) the definition of Nested-Unit Petri Nets (NUPN) is available from http://mcc.lip6.fr/nupn.php
(o) safe by construction – stated by the CÆSAR compiler.
(p) stated by CÆSAR.BDD version 3.7 to be false on 12 instance(s) out of 20, and unknown on the remaining 8 instance(s).
(q) stated by CÆSAR.BDD version 3.7 to be true on 2 instance(s) out of 20, false on the remaining 10 instance(s), and unknown on the remaining 8 instance(s).
(r) stated by CÆSAR.BDD version 3.7 to be true on 12 instance(s) out of 20, and unknown on the remaining 8 instance(s).
(s) stated by CÆSAR.BDD version 3.7 to be false on 12 instance(s) out of 20, and unknown on the remaining 8 instance(s).
(t) stated by CÆSAR.BDD version 3.7 to be false on 12 instance(s) out of 20, and unknown on the remaining 8 instance(s).

Hubert Garavel
hubert.garavel@inria.fr

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
$N = 1$	1.59266e+06 [u]	?	1	9
$N = 2$	1.71221e+06 [v]	?	1	9
$N = 3$	6.20421e+06 [w]	?	1	9
$N = 4$	1.48693e+06 [x]	?	1	9
$N = 5$	1.509e+06 [y]	?	1	9
$N = 6$	5.68136e+06 [z]	?	1	9
$N = 7$	8.03512e+06 [aa]	?	1	9
$N = 8$	1.46954e+07 [ab]	?	1	9
$N = 9$	6.92725e+06 [ac]	?	1	9
$N = 10$	1.26692e+07 [ad]	?	1	9
$N = 11$	$\geq$ 1.31457e+08 [ae]	?	1 [af]	13
$N = 12$	$\geq$ 1.16068e+08 [ag]	?	1 [ah]	13
$N = 13$	$\geq$ 1.03956e+08 [ai]	?	1 [aj]	13
$N = 14$	$\geq$ 9.05769e+07 [ak]	?	1 [al]	13
$N = 15$	3.51283e+06 [am]	?	1	5
$N = 16$	5.13512e+06 [an]	?	1	5
$N = 17$	$\geq$ 1.05167e+11 [ao]	?	1 [ap]	9
$N = 18$	$\geq$ 8.66329e+09 [aq]	?	1 [ar]	9
$N = 19$	$\geq$ 1.08113e+14 [as]	?	1 [at]	13
$N = 20$	$\geq$ 2.70436e+12 [au]	?	1 [av]	13

[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 the CÆSAR compiler.
[ag] stated by CÆSAR.BDD version 3.7.
[ah] stated by the CÆSAR compiler.
[ai] stated by CÆSAR.BDD version 3.7.
[aj] stated by the CÆSAR compiler.
[ak] stated by CÆSAR.BDD version 3.7.
[al] stated by the CÆSAR compiler.
[am] stated by CÆSAR.BDD version 3.7.
[an] stated by CÆSAR.BDD version 3.7.
[ao] stated by CÆSAR.BDD version 3.7.
[ap] stated by the CÆSAR compiler.
[aq] stated by CÆSAR.BDD version 3.7.
[ar] stated by the CÆSAR compiler.
[as] stated by CÆSAR.BDD version 3.7.
[at] stated by the CÆSAR compiler.
[au] stated by CÆSAR.BDD version 3.7.
[av] stated by the CÆSAR compiler.