Alexander Graf-Brill
agrafbrill@depend.cs.uni-saarland.de

*This form is a summary description of the model entitled "EnergyBus" 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

The EnergyBus (http://www.energybus.org) is an upcoming industrial standard for electric power transmission and management, based on the CANopen field bus. It is developed by a consortium assembling all major industrial players (such as Bosch, Panasonic, and emtas) in the area of light electric vehicles (LEV); their intention is to ensure interoperability between all electric LEV components. At the core of this initiative is a universal plug integrating a CAN-Bus (http://www.can-cia.org) with switchable power lines. The central and innovative role of the EnergyBus is to manage the safe electricity access and distribution inside a EnergyBus network.

The present P/T net was derived from a formal specification of the CANopen and EnergyBus features. This specification is written in LNT (*LOTOS New Technology*), which combines functional languages (to describe data types and user-defined functions operating on typed values) and process calculi (to describe concurrent components that synchronize using rendezvous and communicate via message passing). The LNT specification used was the version dated December 16, 2013, which is 1670-line long. This specification was translated to LOTOS, and then to an interpreted Petri net using the CADP toolbox. Finally, the present P/T net was obtained by stripping out all dataflow-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.

This work was done at Saarland University in the framework of the European FP7 project SENSATION.

## References

Alexander Graf-Brill. *Model-based Testing Approaches for the EnergyBus.* Master Thesis, Saarland University Faculty of Natural Sciences and Technology I, Department of Computer Science, Oct. 2013.

Alexander Graf-Brill, Holger Hermanns, and Hubert Garavel. *A Model-based Certification Framework for the EnergyBus Standard.* Proceedings of the 34th IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components, and Systems (FORTE'14), Berlin, Germany. Springer LNCS 8461, pages 84–99.

## Scaling parameter

This model is not parameterized.

## Size of the model

| | |
|---|---|
| number of places: | 157 |
| number of transitions: | 4430 |
| number of arcs: | 63389 |
| number of units: | 29 |
| HWB code (*height-width-bits*): | 4–25–73 |

## 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]

[a] 33585 arcs are not simple free choice, e.g., the arc from place 5 (which has 5 outgoing transitions) to transition 165 (which has 2 input places).
[b] transitions 165 and 166 share a common input place 5, but only the former transition has input place 103.

Alexander Graf-Brill
agrafbrill@depend.cs.uni-saarland.de

**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] ✓

## Behavioural properties

**safe** — *in every reachable marking, there is no more than one token on a place* ✓ [o]
**deadlock** — *there exists a reachable marking from which no transition can be fired* ? [p]
**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* ✗ [q]
**live** — *for every transition t, from every reachable marking, one can reach a marking in which t can fire* ✗ [r]

## Size of the marking graph

| | |
|---|---|
| number of reachable markings: | 2.132E+12 [s] |
| number of transition firings: | 4.086E+13 [t] |
| max. number of tokens per place: | 1 [u] |
| max. number of tokens per marking: | ∈ [21, 25] [v] |

[c] 4281 transitions are not of a state machine, e.g., transition 0.
[d] 142 places are not of a marked graph, e.g., place 0.
[e] stated by CÆSAR.BDD version 1.5.
[f] from place 1 one cannot reach place 0.
[g] place 0 is a source place.
[h] stated by CÆSAR.BDD version 1.5.
[i] stated by CÆSAR.BDD version 1.5.
[j] stated by CÆSAR.BDD version 1.5.
[k] 4221 transitions are not loop free, e.g., transition 74.
[l] 4192 transitions are not conservative, e.g., transition 0.
[m] 12 transitions are not subconservative, e.g., transition 0.
[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] found to be false by GreatSPN at MCC'2014.
[q] 825 transitions can never fire, e.g., transition 20.
[r] the net is not quasi-live and, thus, not live.
[s] computed at MCC'2014 by Marcie and PNMC.
[t] computed at MCC'2014 by Marcie.
[u] stated by the CÆSAR compiler; confirmed at MCC'2014 by GreatSPN and Marcie.
[v] lower and upper bounds given by the number of initial tokens and the number of leaf units.