# Formal methods in support of SMC design

# Errata

Page 6 — Fig. 1.1 *Functional and performance analysis using the $\chi$ environment* and its copy Figure 6.1 are replaced by the Fig. 1.1.

Page 12, line 11 — Signal emission operator $u \curvearrowright p$ behaves as $p$ for valuations where **a predicate** $u$ **over the variables (including the variable** time**)** holds; it is inconsistent for valuations where $u$ does not hold. It also emits a signal that can be inspected by processes in parallel.

Page 15, line -4 — The supervisor sends commands to the lift **to go up** *lift_move*!1 **or down** *lift_move*!0**. Similarly, it commands the pusher to retract** *pusher_move*!1 **or extract** *pusher_move*!0**. The supervisor is notified when the corresponding action has been performed via channels** *lift_done*, *pusher_done***.** We assume that extracting or retracting the pusher takes 2 time units, and lift movements take 5 time units. **The $\chi$ model of the pusher-lift system is depicted in Fig. 2.2.**

Page 16, line 5 — In Fig. 2.2 a parenthesis is removed
$\| *(\mathit{lift\_move}\,?\,b_1;\ (b_1 = 0 \rightarrow \Delta 5;\ \mathit{lift\_done}\,!\,[\!]\ b_1 = 1 \rightarrow \Delta 5;\ \mathit{lift\_done}\,!))$

Page 66, line 15 — Finally, two minor errors have been discovered by verification of property 4 and 5, one modeling mistake and one mistake in the manual transformation from the original $\chi$ model to the translatable $\chi$ model. **This kind of mistakes can be avoided by using only the translatable subset of $\chi$ to create models intended for further verification, and by implementing the transformations as a part of the translator in cases when it is possible.**

Page 88, line 4 — The reduced transition system is equivalent to the original one with respect to **a** CTL$^*$-X property $\phi$...

Page 89, line 3 — Furthermore, each sequential process has a set of local variables and cannot observe local variables of other processes. **It is assumed that there is no shared (global) variables.**

Page 90, line 3 ...the edge labeled with false **leads to the node of the statement that should be executed after the** while **construct.**

Page 90, line -6 ...there is a transition $\langle\langle l, \sigma\rangle, \langle l', \sigma'\rangle\rangle \in Tr$, such that $\sigma'(x) = \sigma(e)$, and the values of...

Page 90, line -2 ...$\langle\langle l, \sigma\rangle, \langle l', \sigma'\rangle\rangle \in Tr$, such that $\sigma'(x) = \sigma(e_i)$, and the values of all other program...

Page 91 In the Section 5.1.2, the following item should be added.

- $n$ is associated with the program location of a send or receive action, or a statement immediately following a communication action (send or receive).

Page 94, line 6 To the phrase $I \subseteq N$ *is a set of initial nodes*[3]. the following footnote is added

[3] We use a set of initial nodes to avoid auxiliary nodes and transitions. For instance, to create a control flow graph of an alternative composition with a single initial node we would need to add an auxiliary node and its outgoing transitions that would lead to the nodes labeled with the first statement of the corresponding process terms. Let us take a process term skip $[\!]$ $x := 1$ as an example. Then, the auxiliary initial node would have an empty label and two outgoing transitions: to the node labeled with skip and to the node labeled with $x := 1$.

Page 104. The header **5.2.4 Relation between original Chi models and their control flow graphs** is removed.

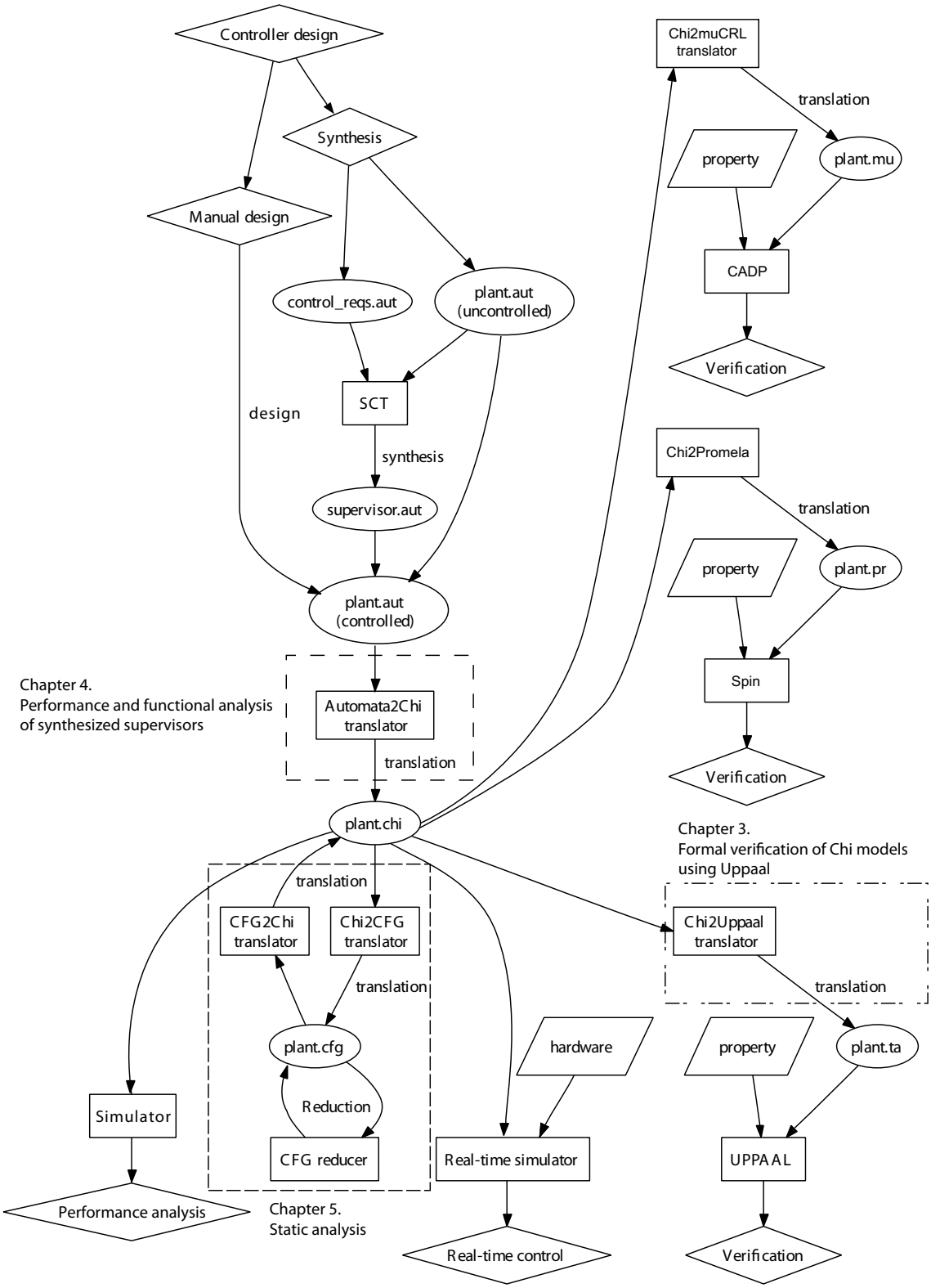


Figure 1.1: Functional and performance analysis using the $\chi$ environment.