

## Formal methods in support of SMC design

**Citation for published version (APA):**

Bortnik, E. (2008). *Formal methods in support of SMC design*. [Phd Thesis 1 (Research TU/e / Graduation TU/e), Mechanical Engineering]. Technische Universiteit Eindhoven. <https://doi.org/10.6100/IR635700>

**DOI:**

[10.6100/IR635700](https://doi.org/10.6100/IR635700)

**Document status and date:**

Published: 01/01/2008

**Document Version:**

Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

**Please check the document version of this publication:**

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

**General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

[www.tue.nl/taverne](http://www.tue.nl/taverne)

**Take down policy**

If you believe that this document breaches copyright please contact us at:

[openaccess@tue.nl](mailto:openaccess@tue.nl)

providing details and we will investigate your claim.

# 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  
$$\parallel *(lift\_move ? b_1; (b_1 = 0 \rightarrow \Delta 5; lift\_done ! \parallel b_1 = 1 \rightarrow \Delta 5; lift\_done !))$$
- 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, ...the edge labeled with false **leads to the node of the statement that**  
line 3 **should be executed after the while construct.**
- Page 90, ...there is a transition  $\langle\langle l, \sigma \rangle, \langle l', \sigma' \rangle\rangle \in Tr$ , such that  $\sigma'(x) = \sigma(e)$ , and the  
line -6 values of...
- Page 90, ... $\langle\langle l, \sigma \rangle, \langle l', \sigma' \rangle\rangle \in Tr$ , such that  $\sigma'(x) = \sigma(e_i)$ , and the values of all other  
line -2 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, To the phrase  $I \subseteq N$  is a set of initial nodes<sup>3</sup>. the following footnote is added  
line 6 <sup>3</sup>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  $\text{skip} \parallel x := 1$  as an example. Then, the auxiliary initial node would have an empty label and two outgoing transitions: to the node labeled with  $\text{skip}$  and to the node labeled with  $x := 1$ .
- Page The header **5.2.4 Relation between original Chi models and their control flow graphs** is removed.  
104.

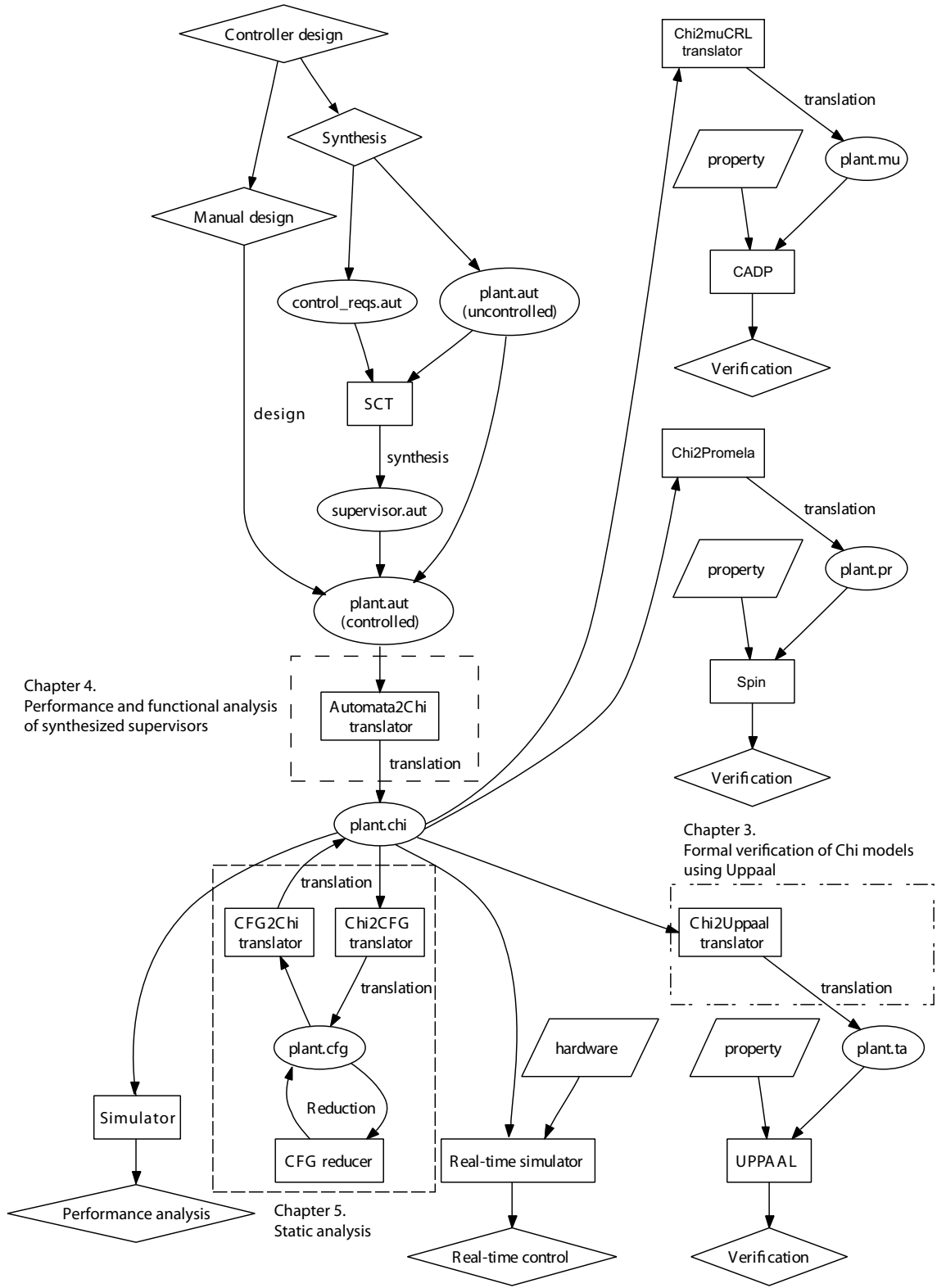


Figure 1.1: Functional and performance analysis using the  $\chi$  environment.

