Cybernétix Case Study – Second Year Report

LIF

May 19, 2004

AMETIST DELIVERABLE 3.1.3

Project acronym: AMETIST
Project full title: Advanced Methods for Timed Systems
Project no.: IST-2001-35304

1 Introduction

The first case study was proposed by Cybernétix and concerns a smart card *personalization* machine HPX 4000 and machines of a related architecture. This machine realizes some of the later steps in the production of smart cards. It takes cards with an already integrated chip, programs them with personalized data and does some tests, and prints on them. The machine is designed to work on batches, i.e. it takes piles of "raw" cards and produces piles of programmed and printed cards. However, production need not be stopped at borders of batches.

The principle design goal for this machine in a very competitive market was to build relatively small machines (fitting into normal rooms) with a high throughput. For personalization, one of the determining factors is the programming or personalization time.

For an increased throughput, a parallel architecture with several programming stations is an obvious solution. Getting the cards from the input stations to the programming stations, from there to the printing stations and from there to the output, while removing cards failing the tests requires an efficient transport system.

For this transport system, Cybernétix invented and patented a dedicated conveyor belt for moving a sequence of cards and a mechanism for lifting cards from this conveyor to a programming station above. In particular, the mechanism allows to move the conveyor while a card is lifted and other cards may pass on the conveyor below.

The second challenge of the design is the development of a scheduling algorithm that routes the cards through the system on this given architecture in an efficient manner. Cybernétix found a particular algorithm for this baptized "SuperSingle Mode", which is equally part of the patent for the conveyor system.

A second concern for the scheduling focuses on *faulty cards*. A certain fraction of the cards contains electronic defects not detected before actually programming the cards. A defective card must be replaced by a new card without modifying the order of output and at the lowest possible cost.

For the SuperSingle Mode, Cybernétix invented a recovery method that actually required to modify the machine design (the length of the conveyor), which has been thoroughly tested in various failure scenarios and never failed. But the method is not strictly understood to be correct under any circumstances nor known to be optimal.

2 Brief summary of the first year contribution

During the first year the project focuses mostly on the modelling and analysis of the personalization machine *without* faulty cards. This permitted the automatic derivation of the scheduler (that turned to be the same SuperSingle mode). It was automatically analyzed using SMV, Spin, Petri nets, and Uppaal, though only the first two cases automatically synthesize the scheduler in a small-sized model (with only 4 personalization stations instead of the 16 or 32 stations used in the real machine). Besides, the performance of the SuperSingle mode was analyzed on ad-hoc mathematical models.

In addition, a modelling approach using scenarios was pursued in LSCs though this approach was still under development last year.

The faulty card scenario was also studied in one case using self stabilization techniques. However, a maximum of only one faulty card was allowed. An alternative architecture was also considered.

Meeting with Cybernétix Engineers

During the first year of AMETIST, Cybernétix was restructured and the Micro-informatics division, which also builds the HPX machines, became an independent unit and was moved to a different site (Rousset) from the contractor CYR "Cybernétix Recherche", who maintains the programming responsibility of the HPX machines and the direct research cooperation concerning the case study. While this makes communication with the engineers working directly on the HPX machines more difficult, the new unit not contractually involved in AMETIST has been cooperative and interested in the results.

A half day-meeting was held on october 10 to present the achievements up to that date and to discuss new challenges. The chief engineers, some of whom have a solid background in constraint solving, showed to have a good and realistic understanding of the results obtained. The overall conclusion was that the results found with AMETIST methodoly confirmed the engineers intuition and experience with the machine without proposing as yet a revolution.

However, the ideas of Angelika Mader about an alternative machine architecture found the engineers interest and the new challenges were in part based on this discussion. These challenges found their precision during october/november 2003 (including the implementation of a simulator, see below) and were presented to the consortium at December 1 in Munich, a bit late to hope for results already before the end of the second year. Should good results be obtained for these new challenges – which pose particularly difficult and highly cost relevant problems to the engineers – then it was estimated that this could indeed lead to reduced costs and better competitivity of the machines in the near future.

3 Contribution during the second year

[2] reports the SMV approach, including the faulty card scenario briefly described above. This work has been done during the first year of the project but only publish last year. (See also Deliverable 3.1.2).

Simulation environment for the smart card personalization process

Mathieu Agopian (CYR/LIF) developed an interactive simulation environment of the HPX personalization machine [1]. The basic structure of the simulated machine responds to the model study along the first year, but the simulation tool allows small changes in the architecture (e.g. number of personalization stations, gaps before the reject station). It implements the exact SuperSingle mode running on the HPX machines including the treatment of faulty cards but it also allows modifications of this algorithm. The simulator is amenable for automatic simulation, manual simulation, manual intervention (altering the normal behaviour of the algorithm), among other features. Simulated executions can be saved and loaded in order to reproduce previous results or even to visualize the execution of schedulers obtained by another method (e.g. using SMV, Uppaal, or Spin). Figure 3 shows a screenshot of the simulation tool running a model with 8 personalisation stations.

This tool is specially handy to obtain insights of the faulty card treatment (see Section 4.)

Scenario based modelling

Live Sequence Charts (LSCs) is a formal graphical inter-object scenario-based language. LSCs is taken as an example of a scenario based specification language which enables better modelling procedure using the Play-In/Play-Out approach. In comparison to other models, LSCs models are easier to read and maintain due to its scenario based nature. Maintaining a model usually involves adding new scenarios and removing old ones. In state based models, this means that the scenario has to be traced over all participating objects. With LSCs this procedure is straight forward.

[3] revisits previous work of last year and employs LSCs to systematically analyze the Cybernétix case study. Using scenarios, the specification can be refined little by little to synthesize a scheduler. The analysis is performed with the help of the Play-Engine modelling tool. This tool allows the user to construct a graphical user interface (GUI) with the features of the HPX machines (similar to the simulator explained above). This GUI provides a set of buttons and displays that allow to construct valid or invalid scenarios.

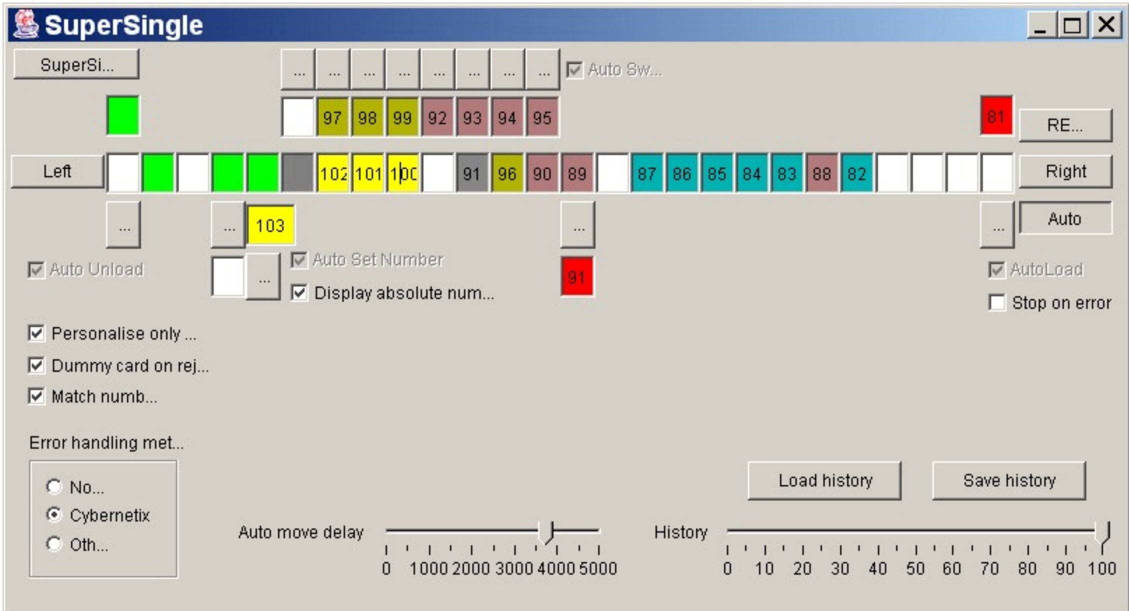

Figure 1: A screenshot of the simulation tool

Besides, the tool has been enhanced in order to translate the model of the personalization machine into an SMV model. This model is then used to extract schedulers and perform verifications.

Checking tight bound on cyclic schedulers

[4] analyzes a family of schedulers for the smart card personalization machine and focus on the optimality of the throughput. Schedulers are characterized by the number of cards and free slots on the conveyor belt per cycle using ad-hoc mathematical models. If k is the number of contiguous cards, and n is the number of contiguous slots, the family of (k, n)-cyclic schedulers is studied. Next, non-trivial bounds on the cycle time, and hence on the throughput, are provided. This is done by looking at certain special scheduling policies and using techniques known as destructive bounding. Finally, schedulers are checked for optimally on those bounds.

In particular, the $(k, 0)$-cyclic scheduler corresponds to the batch mode and is shown to be the only one *not* meeting its lower bound, while the $(k, 1)$-cyclic scheduler —corresponding to the SuperSingle mode— is optimal (meets the lowest bound) and it has the best throughput possible among the (k, n)-cyclic scheduler class.

4 New challenges

During the first year the smart card personalization machine has been study in great detail with respect to a particular kind of architecture and without faulty cards.

The faulty cards case has been proved to be difficult to analyze. The unpredictability of a faulty card does not permit a systematic optimal solution. In particular, [2] obtained different solutions that depend on the position of the faulty card on the machine. Hence, the aim behind the faulty card treatment needed to be revised. After a meeting with Cybernétix personnel, the following two points where settled:

1. The faulty card treatment already provided by Cybernétix machines needs to be proved to be correct in the sense that (a) personalized cards should be consecutive numbered at the output (in order to agree with the printed number), and (b) no faulty card is produced at

the output. Although this requirement has already been stated in the previous year, only now the Cybernétix treatment of faulty card was well understood (currently implemented in the simulator [1]).

2. As mentioned, the principle design goal for the personalization machine is to build relatively small machines with a high throughput. Cybernétix faulty card treatment requires that the length of the conveyor belt contains one extra slot for each personalization station, which almost duplicates the size of the machine *only* to treat faulty cards. (Notice in Figure 3 the extra slots on the right hand side of the simulator, after the last rejecting station. A similar situation can be observed on the real machine.) A challenge posed by Cybernétix is to find an alternative method to treat faulty cards that reduces the number of extra slots. The solution is not obvious as a major constraints is that cards should not be moved out from the belt to a buffer (which would sensibly increase the likelihood of malfunctioning).

Further challenges posed by Cybernétix involves modularity on the architecture of the machine. So far, the study focus on a single production block formed by the personalization stations and single processing machines (such as printers). In such architecture, the SuperSingle mode was proved to be optimal. However, HPX machines have been design to be modular and it would be normal to arrange several production blocks of different lengths. For instance, a card may contain both a contact processing cheap and a wireless connection. A personalization machine may thus include an array of 6 contact personalization stations for the electric connection, and another array of 2 contactless personalization stations for the wireless connection. In this kind of machines, the SuperSingle mode underperforms the batch mode. A challenge in this direction is to find new scheduling algorithms that have good performance and behave well under modular schemes.

5 Conclusion and outlook for the third year

In the first year, the Cybernétix case study drew more attention of the consortium than anticipated. Several relevant challenges – as far as current technology permits – were solved before schedule. The remaining problems are more difficult and partly communicated to the consortium only in December 2003.

It is therefore not surprising that the second year shows less activities on this case studies than the first very fruitful year. Activities in the new challenges are ongoing and not yet finished.

From the point of view of communication beyond the consortium, the Cybernétix case study has started to have visible impact in the second year. The work addressed by Tim Nieberg [4] is an example. Noticeably, the scheduling problem of the smart card personalization machine matches the challenge of state of the art techniques and is hence likely to become a benchmark case study.

Summarizing, the contributions for the second year within the WP3-CS1 include:

- [3] concludes research initiated during the first year.
- The interactive simulation environment [1].
- The statement of new challenges (see Section 4).
- Insertion of the case study in the scientific community beyond the AMETIST project.

For the third year we expect to achieve the following:

- Verification of the Cybernetix solution to the faulty card problem, including the determination of shortest machine size.
- Synthesis of faulty card handling (for rather small instances).
- Synthesis of cyclic schedules.

- Performance analysis of the two-process problem using different architectures and simulation with timed automata

References

[1] M. Agopian. A simulation tool for the SuperSingle mode, 2003. Available from World Wide Web: `http://www.cmi.univ-mrs.fr/~niebert/docs/SuperSingleSimulator.zip`. Not a paper, a tool.

[2] B. Gebremichael and F.W. Vaandrager. Control synthesis for a smart card personalization system using symbolic model checking. In *Proceedings First International Workshop on Formal Modeling and Analysis of Timed Systems (FORMATS 2003),* September 6-7 2003, Marseille, France, volume 2791 of *LNCS*. Springer Verlag, 2003. Available from World Wide Web: `http://www.cs.kun.nl/ita/publications/papers/fvaan/smart.html`.

[3] Hillel Kugler and Gera Weiss. Planning a production line with LSCs. Research report, Weizmann, 2004. Available from World Wide Web: `http://ametist.cs.utwente.nl/INTERNAL/PUBLICATIONS/WISPublications/cybernetix.zip`.

[4] Tim Nieberg. On cyclic plans for scheduling a smart card personalisation system. Technical Report TR-CTIT-04-01, CTIT, University of Twente, January 2004. Invited presentation at the 6th AMETIST Meeting, December 1-2, 2003, Muenchen.