ROMANIAN JOURNAL OF MATHEMATICS AND COMPUTER SCIENCE, 2012, VOLUME 2, ISSUE 2, p.36-43

# VERIFICATION OF N-M SWITCHING CONTROL SYSTEM: A CASE STUDY IN TEMPORAL LOGIC MODEL CHECKING

**Changil Choe[*], Hyejong Hong[**] and Kukhwan Kim[***]**

**Abstract**

Production factories in which stable voltage is critical, e.g., electro-plating factory, require constantly stable voltage to minimize loss by adjusting incoming voltage in real time even if low-quality electricity is supplied from outside. To solve such problem often being raised from the factories located in the area with unstable electricity supply, we designed N-M switching control system and verified its correctness using LTL model checking.

**Mathematics Subject Classification 2010 :** 03B44, 68Q60
**Keywords:** Switching control system, Verification, LTL model checking

## 1. Introduction

Production under unstable electricity condition may cause serious loss of expense such as large amount of rejects, in factories that include processes requiring highly stable electricity. For example, professional precious metal plating companies require to keep stable voltage at all times they work. In case such factories or companies are situated in the unstable power supply area, voltage stabilization is raised more importantly. Numerous works were devoted to design and implement stable voltage supplier, which was presented and summarized in many papers and monographs, e.g., [1].

N-M switching control system was motivated to meet the requirement raised from a plating factory for eating utensil set [2]. The quality of electricity being supplied to the factory was not good, that is., some days low or high voltage electricity were supplied. From the standpoint of profits of the factory, it was better to produce only in workplaces for which can supply normal voltage by adjusting and distributing

*, *** *Faculty of Mathematics, Kim Il Sung University, D.P.R.K*
*mathcci@yahoo.com*
** *Central Information Agency of Science and Technology, D.P.R.K*

incoming voltage in real time, rather than all workplaces were exposed to the production failure of acceptable goods. .

In this paper, we describe working mechanism of N-M switching control system, briefly called N-M system in this paper, and present a method to verify correctness of its design using LTL model checking. N-M system is a real-time voltage normalization and distribution system that divides whole workplaces of factory into N sections, adjusts voltage height by switching between N levels and supply normalized voltage to sections according to the given priority. N-M system may suspend electricity supply to all sections temporarily in worst cases, i.e., incoming voltage to itself from outside is too low or high.

N-M system must satisfy many real-time requirements for the stable voltage supply to each work section. We don't concentrate on describing the details of N-M system and the whole specifications of its requirements, rather focus on showing our method to verify N-M system for its time-dependant requirements using LTL model checking technique. LTL is a kind of temporal logic having strong expressive power to specify time-dependant properties of real-time systems and LTL-based model checking technique is now widely used in verification of real-time systems, e.g. [3-9].

Section 2 describes N-M system and its design requirements. Section 3 shows our method verifying N-M system against design requirements using LTL model checking. Section 4 is the conclusion.

## 2. N-M Switching Control System and its Requirement

In this section, we describe working mechanism, implementation method and time-dependant requirements of N-M system.

**Working mechanism.**

Whole workplaces of factory are divided into N sections $W_1, W_2, \cdots, W_N$ by considering relative independence of work. Power supply priority is assigned to each section according to the importance or processing order of products. For example, we may give highest priority to silver-plating workplace. For the convenience of

description, we assume that $W_i$ has higher priority than $W_j$ if $i < j$. Voltage is adjusted at M levels $L_1, L_2, \cdots, L_M$. There are three states for each level, that is, low voltage state $\ell$, normal voltage state $n$ and high voltage state $h$. This standard is set considering technical requirements of production. We briefly describe working mechanism of N-M system below.

System starts control in level $L_{m_0}$ where $m_0 = \lceil M/2 \rceil$ and does one of the following three behaviors.

- Increase voltage by switching level into $L_{m_0+1}$, if the incoming voltage is low.
- Supply electricity to section $W_1$, if the incoming voltage is normal.
- Decrease voltage by switching level into $L_{m_0-1}$, if the incoming voltage is high.

Let us assume that system is in level $L_m$ and current electricity supplying sections are $W_1, W_2, \cdots, W_n$.

- System suspends electricity supply to $W_n$, if the incoming voltage is low.
- System supplies electricity to section $W_{n+1}$, if the incoming voltage is normal.
- System decreases voltage by switching level into $L_{m-1}$, if the incoming voltage is high.

For the practical design and implementation, it must be considered more items than described above. The purpose of the paper is to show verification method of N-M system, and thus we don't consider some details of the system.

**Implementation**

Control of N-M system is realized using the values of N+M+3 bit string $w_1, \cdots, w_N$, $\ell_1, \cdots, \ell_M$, $d_1, d_2, d_3$, each corresponding to the sections $W_1, W_2, \cdots, W_N$, voltage adjustment level $L_1, L_2, \cdots, L_M$ and voltage states $\ell$, $n$, $h$ in each level. $w_i = 0$ means that electricity is not supplied to section $W_i$ and $\ell_j = 1$ means that voltage adjustment level is $L_j$. $d_2 = 1$ means that voltage state is normal in current level and $d_2 = 0$ means that voltage state is not normal. For example, in case N=3 and M=2, bit value string 111 10 010 denotes that normal voltage is supplied to all sections by increasing voltage adjustment level to the maximum.

The number of possible bit value string is $2^{N+M+3}$ for N+M+3 bit, but some bit value string does not occur in control. For example, in the above case, following string

does not occur.

010 01 010, 010 11 001

This is because system does not supply electricity to $W_{i+1}$ unless $W_i$ is supplied with electricity and voltage adjustment can not be in different level at the same time. Exact number of bit value strings occurring in control is (N+1)*(4*M). This is not small number and it may fail to implement correct control system if the design is not verified.

**Requirements**

We only consider 8 requirements of N-M system for the purpose of the paper, though there are many other requirements to be verified.

$D_1$: System decreases work section by one, if the voltage state is low in maximum level.

$D_2$: System suspends electricity supply to all sections, if the voltage state is high in minimum level.

$D_3$: System keeps current supplying sections and levels up by one, if voltage state is low and leveling up is possible.

$D_4$: System keeps current supplying sections and levels down by one, if voltage state is high and leveling down is possible.

$D_5$: System increases work section by one, if voltage state is normal in current level.

$D_6$: System keeps current supply, if all sections are supplied with electricity and voltage state is normal in current level.

$D_7$: System does not supply electricity to $W_{i+1}$ unless $W_i$ is supplied with electricity.

$D_8$: It is possible to supply electricity to all sections.

## 3. Verification of N-M Switching Control System

In this section, we present our method to verify N-M switching control system for its requirements using LTL model checking technique. For this, we construct formal model of N-M system and write formal specification of its requirements, according to

the syntax and semantics of LTL. Then we check satisfaction relation between model and specifications using LTL model checking tool NuSMV.

**LTL model of N-M switching control system**

Semantics of LTL is defined using transition system. A transition system is a triple $M = (S, \to, L)$ consisting of

- a set $S$ of states,
- a transit ion relation $\to \subseteq S \times S$, where every state has at least one successor,
- a labeling function $L : S \to 2^{AP}$ assigning a set of atomic propositions to each state $s \in S$.

An example of transition system is given in Fig 1. Here, $AP = \{p, q, r\}$ and

- $S = \{s_0, s_1, s_2\}$,
- $\to = \{(s_0, s_1), (s_0, s_2), (s_1, s_0), (s_1, s_2), (s_2, s_2)\}$,
- $L = \{s_0 \mapsto \{p, q\}, s_1 \mapsto \{q, r\}, s_2 \mapsto \{r\}\}$.

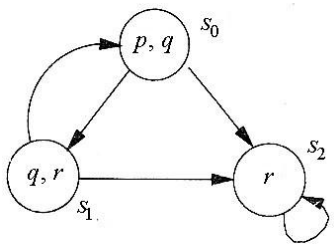


Fig 1. A transition system.

N-M system is well modeled as a transition system. For modeling of N-M system, we use the following N+M+3 atomic propositions.

$W_i$ $(i = 1, \cdots, N)$ : Section $W_i$ is supplied with electricity.

$L_j$ $(j = 1, \cdots, M)$ : Voltage adjustment level is $L_j$.

$\ell$ : Voltage is low in current level.

$n$ : Voltage is normal in current level.

$h$ : Voltage is high in current level.

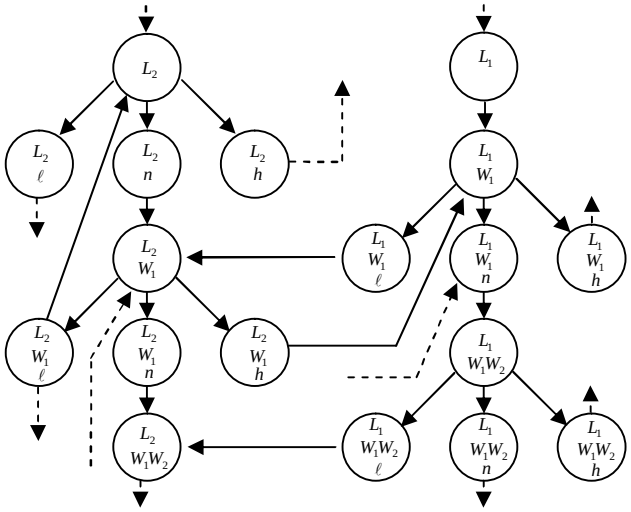


Fig 2. A part of transition system model of N-M switching control system.

As we mentioned above, the number of states of N-M system is (N+1)*(4*M). It is difficult to draw complete transition system model of N-M switching system in a page. We only show a part of model in Fig 2. From the figure, Readers can know how the transition system model of N-M system is constructed in general.

**LTL Specification of requirements**

A LTL formula $\phi$ is built up from a finite set of atomic propositions, the propositional operators $\neg, \wedge, \vee, \rightarrow$ , and the temporal modal operators $X, F, G, U, W, R$. Among the temporal operators, $X, F$ and $G$ are used in this paper. LTL formulas are estimated on the path of transition system. Let $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \cdots$ be a path of a transition system $M$ .

• $X\phi$ means that $\phi$ has to hold at the next state $s_1$ of the first state $s_0$ of the path.

• $F\phi$ means that $\phi$ eventually has to hold at a state $s_i (i \geq 1)$ somewhere on the path.

• $G\phi$ means that $\phi$ has to hold at all states $s_i (i \geq 0)$ on the path.

Let $s_0$ be the initial state of a transition system $M$ and $\phi$ be a LTL formula. It is called that $\phi$ is satisfied by $M$, denoted by $M, s_0 \models \phi$, if $\phi$ holds on every path of $M$, starting from $s_0$.

Requirements of N-M system, described in section 2, can be specified with LTL operators as follows.

$D_1$: $G(L_1 \wedge \ell \wedge W_1 \wedge \cdots \wedge W_i \rightarrow X(W_1 \wedge \cdots \wedge W_{i-1}))$ $\quad i = 1, \cdots, N$

$D_2$: $G(L_M \wedge h \rightarrow X(\neg W_1 \wedge \cdots \wedge \neg W_N))$

$D_3$: $G(L_j \wedge \ell \wedge W_1 \wedge \cdots \wedge W_i \rightarrow X(L_{j+1} \wedge W_1 \wedge \cdots \wedge W_i))$ $\quad i = 1, \cdots, N$

$j = 1, \cdots, M-1$

$D_4$: $G(L_j \wedge h \wedge W_1 \wedge \cdots \wedge W_i \rightarrow X(L_{j-1} \wedge W_1 \wedge \cdots \wedge W_i))$ $\quad i = 1, \cdots, N$

$j = 2, \cdots, N$

$D_5$: $G(n \wedge W_1 \wedge \cdots \wedge W_i \rightarrow X(W_1 \wedge \cdots \wedge W_{i+1}))$ $\quad i = 1, \cdots, N-1$

$D_6$: $G(n \wedge W_1 \wedge \cdots \wedge W_N \rightarrow X(W_1 \wedge \cdots \wedge W_N))$

$D_7$: $G\neg(\neg W_i \wedge W_j)$ $\quad 1 \le i < j \le N$

$D_8$: This requirement cannot be specified as a LTL formula directly. The negation of $D_8$, i.e., there is no case when all sections are supplied with electricity, is specified as the LTL formula as follows.

$D_8^{'}$: $\neg F(W_1 \wedge \cdots \wedge W_N)$

Therefore, if $D_8^{'}$ is not satisfied by a transition system, then $D_8$ is satisfied by it and vice versa.

**Model checking**

Using temporal logic model checker NuSMV, we checked the satisfaction relation between transition system model and LTL specifications of N-M switching control system. Through several executions of NuSMV and debugging, we could construct the transition system model $M$ of N-M switching system, satisfying

$$M, s_0 \models D_1, \cdots, D_7, D_8^{'}.$$

Based on this result, we revised design and implemented correct N-M switching control system matching factory's requirement.

## 4. Conclusion

Temporal logic model checking is very useful technique to design and implement real-time systems like N-M switching control system. We believe that verification method presented in the paper can be used in other cases when design and verify control systems.

## References

[1] A. Pressman, K. Billings, and T. Morey. Switching Power Supply Design, 3rd Ed, McGraw-Hill Professional, 2009.

[2] C. Changil and K. Kukhwan. Design and implementation of N-M switching control system, Journal of Kim Il Sung University, 2011. Vol 64, No2, 23-35.

[3] E. M. Clarke, O. Grumberg, and D. A. Peled. Model Checking. MIT Press, 1999.

[4] A. Pnueli, The temporal logic of programs. *Proceedings of the 18th Annual Symposium on Foundations of Computer Science (FOCS)*, 1977, 46–57.

[5] M. Huth and M. Ryan. Logic in Computer Science: Modelling and Reasoning about Systems, Cambridge University Press, 1999, ISBN 978-0521656023, 175-221.

[6] A. Pnueli. The temporal semantics of concurrent programs. Theoretical Computer Science, 13(1):45–60, 1981.

[7] B. Berard, M. Bidoit, A. Finkel, F. Laroussinie, A. Petit, L. Petrucci, and Ph. Schnoebelen. Systems and Software Verification. Model-Checking Techniques and Tools. Springer, 2001.

[8] E. M. Clarke and J. M. Wing. Formal methods: state of the art and future directions. ACM Computing Surveys, 28(4):626–643, 1996.

[9] A. Cimatti, E.M. Clarke, E. Giunchiglia, F.Giunchiglia, M. Pistore, M. Roveri, R. Sebastiani, A. Tacchella. “NuSMV 2: An opensource tool for symbolic model checking,” International Conference on Computer-Aided Verification, 2002.