

# Supplementary Document to “Detection of Actuator Enablement Attacks by Time Petri Nets in Supervisory Control”

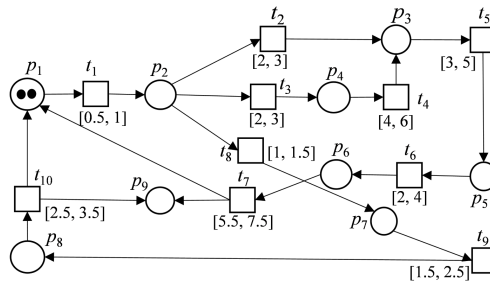
Journal Title  
XX(X):1–4  
©The Author(s) 2025  
Reprints and permission:  
sagepub.co.uk/journalsPermissions.nav  
DOI: 10.1177/ToBeAssigned  
www.sagepub.com/

SAGE

Zhenhua Yu<sup>1</sup>, Yifei Jia<sup>1</sup> and Xuya Cong<sup>1</sup>

## Example of Warehouse Order Processing System

The overall architecture of the warehouse order processing system is shown in Figure 1. This architecture enables a closed-loop management process from order inflow to completion. In the specific process design, the standard order processing flow includes two branches: sufficient stock and insufficient stock. Expedited orders utilize priority scheduling to optimize resource allocation and shorten the processing cycle. It should be noted that there are two tokens in  $p_1$ , representing two pending order tasks in the current system. To further clarify the practical implications of each core element in the system modeling process, Table 1 and Table 2 provide detailed definitions of the physical scenarios and functions corresponding to the places and transitions in the model, respectively.



**Figure 1.** The TPN model of the warehouse order processing system

<sup>1</sup>College of Artificial Intelligence and Computer Science, Xi'an University of Science and Technology, Xi'an 710054, China

### Corresponding author:

Xuya Cong, College of Artificial Intelligence and Computer Science, Xi'an University of Science and Technology, Xi'an 710054, China.

Email: congxuya@xust.edu.cn

**Table 1.** Physical meaning of places.

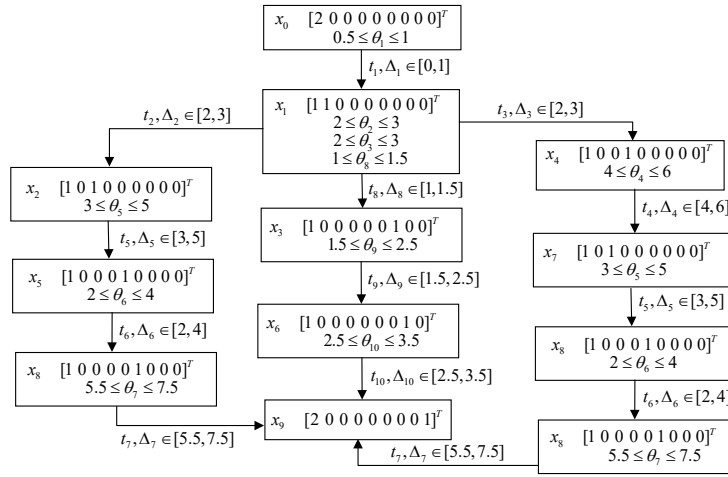
Places	Meaning
$p_1$	All pending orders
$p_2$	Waiting for the system to identify the order priority
$p_3$	Regular orders with sufficient inventory are pending sorting
$p_4$	Regular orders are pending stock replenishment
$p_5$	Regular orders are pending quality inspection
$p_6$	Regular orders are pending packaging
$p_7$	Rush orders with sufficient inventory are pending sorting
$p_8$	Rush orders are pending packaging
$p_9$	Order completed

**Table 2.** Physical meaning of transitions.

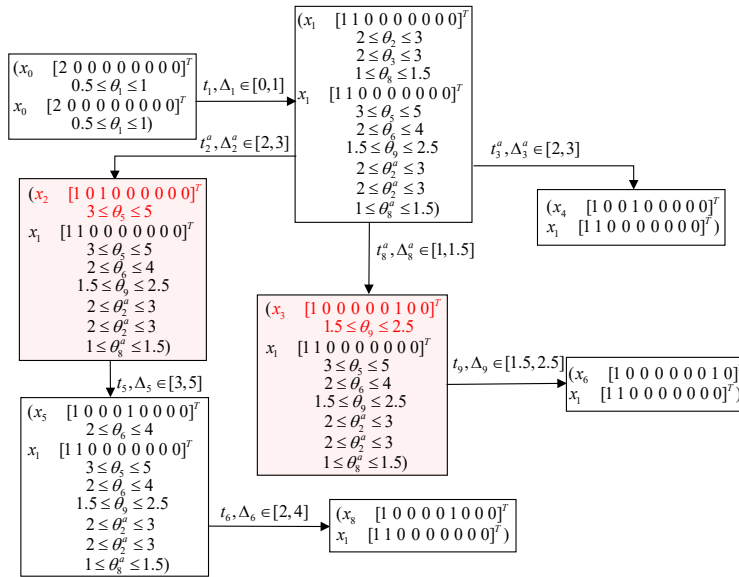
Option	Columns
$t_1$	Classification of pending orders
$t_2$	Check on sufficient inventory for regular orders
$t_3$	Check on insufficient inventory for regular orders
$t_4$	Regular order replenishment
$t_5$	Regular order sorting process
$t_6$	Regular order quality inspection process
$t_7$	Package regular orders and process new orders
$t_8$	Rush order inventory check
$t_9$	Rush order sorting
$t_{10}$	Package rush orders and process new orders

The MSCG corresponding to this system, which represents the plant  $G$  under investigation, is illustrated in Figure 2. Based on the physical properties of the transitions in Table 2, the system's uncontrollable event set is  $\Sigma_{uc} = \{\alpha_5, \alpha_6, \alpha_9\}$ . These events are typically automated and dominated by equipment, making external interference extremely difficult. Conversely, the controllable event set is  $\Sigma_c = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_7, \alpha_8, \alpha_{10}\}$ . The vulnerable event set is  $\Sigma_{c,v}^a = \{\alpha_2, \alpha_3, \alpha_8\}$ . They are the core targets for attack intervention because they correspond to events that affect critical decision-making, such as order flow direction and prioritization. The two types of states, "Regular Order with Sufficient Inventory Pending Sorting" and "Rush Order with Sufficient Inventory Pending Sorting," serve as the core nodes connecting order decision-making and physical execution. Anomalies in these states directly lead to the stagnation of the warehouse sorting function and the interruption of the supply chain flow, thereby disrupting the normal operational logic of the warehouse. Therefore, the unsafe state set for this system is defined as  $X_f = \{x_2, x_3, x_7\}$ . These states are critical for accurately describing the threats to system stability.

To prevent an increase in analysis complexity due to an excessively large attack time span, the time interval for the occurrence of attack events in this example is set to be the same as the firing time interval of the transitions. According to Algorithm 1, the attacked model  $G_a$  and the attacked supervisor  $H_a$  are constructed, respectively. By calculating  $G_a \otimes H_a$ , the attacked closed-loop controlled system  $G_M$  of this case is obtained, as shown in Figure 3.



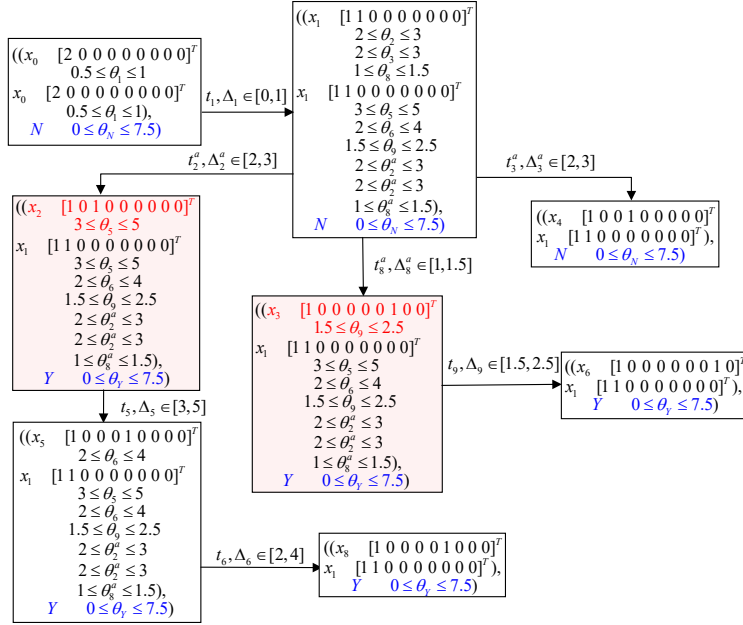
**Figure 2.** The MSCG of the TPN system in Figure 1



**Figure 3.** Attacked closed-loop system model  $G_M$

Since this system is a small-scale system, a diagnoser is used to determine the AE-safe controllability of the system. The diagnoser  $G_d$  is shown in Figure 4. According to Step 7 of Algorithm 2, we can obtain

$\{((x_2, x_1), Y), ((x_3, x_1), Y)\} \in FC$ . Since this set contains the unsafe states  $x_2$  and  $x_3$ , the system does not satisfy the AE-safe controllability condition.



**Figure 4.** The diagnoser  $G_d$