Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080655

Analysis of the Composition of Non-Deducibility in Cyber-Physical Systems

Jingming Wang[1,2] *and Huiqun Yu*[1,*]

[1] Department of Computer Science and Engineering, East China University of Science and Technology, Shanghai 200237, China
[2] School of Computer and Information Engineering,Chuzhou University, Anhui 239012, China

Received: 25 Nov. 2013, Revised: 23 Feb. 2014, Accepted: 24 Feb. 2014
Published online: 1 Nov. 2014

Abstract: Cyber-Physical Systems (CPSs) are integrations of computation and physical processes. Now researchers are confronted with the difficulty in the analysis and verification of information confidentiality in complex CPSs owing to physically observable behavior and physical components appended to cyber systems. This problem can be solved effectively by using some simple or small systems to compose the complex CPSs while achieving the confidentiality of the composite system by preserving that of small systems. Firstly, the paper introduces the definition of non-deducibility and the definition and operation of Petri net and four compositions (sequence, iteration, parallel and alternative composition) for non-deducibility (ND). Secondly, this paper analyzes the ND security model, which is extremely attractive since the physical actions of CPSs are inherently observable, in the abstract cyber-physical natural gas pipeline system based on Petri net. Finally, this paper gives the conditions in which the ND security property will not be changed after the four representative compositions, the proofs of which are provided. The contribution of this study is providing a formal method and laying a foundation for exploring the confidentiality and information security in CPSs.

Keywords: Cyber-Physical Systems, Information Flow Security, Petri Net, Non-Deducibility.

1. Introduction

In recent years, systems design has increasingly developed in the direction of CPSs [1]. CPSs are integrations of computation and physical processes. Researchers are now confronted with the difficulty in the analysis and verification of information confidentiality of complex CPSs owing to physical observable behavior and physical components appended to cyber systems. A considerable challenge to analyze this property is the representation of physical systems interactions at the cyber-level. Fig. 1 demonstrates the interactions in CPSs.

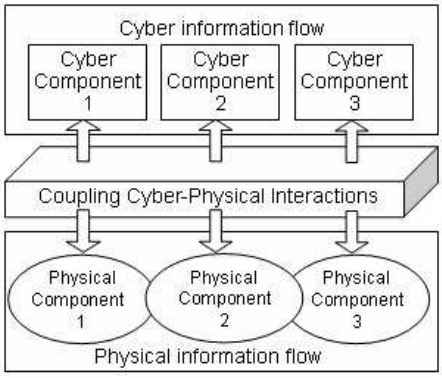

Figure 1: *Cyber – physical interactions*

Access control security policies could be used to protect the data confidentiality in the composition of CPSs. However, these methods are still unsatisfactory since they are only to solve direct flow of information and the indirect information flow still exists, such as through the covert channels [2,3]]. A better approach to computer security is to control both the direct and indirect transmissions by imposing some information flow rules [2,4], which are realized in information flow security models, such as non-deducibility model discussed in this paper.

* Corresponding author e-mail: yhq@ecust.edu.cn

In addition, researchers and engineers of CPSs have to conduct further studies on composable security models. The reasons are as follows.

(1) In general, CPSs are composite systems which do not stand alone. In order to share the resources of information, computation, software and hardware,there are always attempts to hook small systems together into a network system.

(2) The divide-and-conquer approach is effective in the design of large-scale CPSs. Therefore, it is really necessary to study the information security properties (e.g., ND information flow security property) of composition.

In 1986, non-deducibility [5] property, which is extremely attractive since the physical actions of CPSs are inherently observable, was first proposed by Sutherland. Other researchers also did a lot of work at this property in recent years, such as [6,7]. However, there is little Petri-net-based research on ND composition and its application in CPSs.

This paper analyzes the non-deducibility security property in the abstract natural gas pipeline system based on Petri net, which is a typical application of CPSs. Furthermore, this paper gives the conditions in which the property will be preserved after representative composition methods (sequence, iteration, parallel and alternative composition) based on Petri net, and provided the proofs of these results. The main contribution of this paper is to provide a formal method and lay a foundation for studying information confidentiality and security in CPSs.

The rest paper is organized as follows:

Section 2 introduces some basic definitions of non-deducibility and Petri net, the additional operation on Petri net and four representative compositions on Petri net. In Section 3, the ND property of the natural gas pipeline system is analyzed and proved based on Petri net. Section 4 elaborates on the application of the four compositions to ND security model in cyber-physical systems. Finally, some conclusions are drawn in Section 5.

2. Basic definitions

2.1. Non-deducibility

Non-inference information security model is too strong if a system cannot run without a high-level transition. Non-deducible model is more appropriate than non-inference in such cases. A system is non-deducible secure if nothing can be inferred about the transition sequence of high-level input transitions based only on observation of low-level transitions. That is to say that a system is non-deducible secure if there is always more than one execution transition sequences resulting in the same low-level view trace.

Definition 1 Formally, a net system is non-deducibility secure if and only if

$\forall \sigma \in TS(N), \exists \sigma' \in TS(N) \wedge next(m_0,\sigma) \overset{L}{\simeq} next(m_0,\sigma')$

Where,$next(m_0,\sigma)$ denotes the result statement set for a non-determined system. $\sigma \in TS(N)$ denotes any trace of the system N.

2.2. Petri net

Carl Adam Petri first used network structure to simulate the communication systems in his doctoral dissertation in 1962. The network structure model is the prototype of Petri net. As a formal tool with well-defined rigorous semantics, Petri net can be efficiently used to model and verify the security properties of a system model [8,9]. In order to define security properties more conveniently and efficiently, the definitions and operations of the elementary Petri net are adapted. The definition of flow relations between places is changed to describe the undermined result statement after the firing of one transition in order to model and analyze the undermined system.

Definition 2 A tuple $N=(S,T,F)$ is a net, where

(1)S and T are the sets of places and transitions, and $S \cap T = \emptyset$.

(2)$F \subseteq (2^S \times T \times 2^S)$ is the set of flow relation.

Definition 3 Let $N=(S,T,F)$ be a net. A multiset over the set s is called marking. Given a marking m and a place s, m(s) denotes the tokens number of place s.

A pair (N,m_0) is a net system, where N is a net and m_0 is a marking of N, which is called initial marking in general. With abuse of notation, (S,T,F,m_0) is used to denote the Petri net system. The operator $\oplus$ denotes union operation: $(m \oplus m')(s) = m(s) + m'(s)$ for all $s \in S$ and denotes difference operation: $(m \backslash m')(s) = m(s) - m'(s)$.

Let $t \in T$, ${}^{\cdot}t = \{Q \in 2^S | \exists Q' \in 2^S, (Q,t,Q') \in F\}$ denotes the set of preset of t and $t^{\cdot} = \{Q' \in 2^S | \exists Q \in 2^S, (Q,t,Q') \in F\}$ denotes the set of postset. Accordingly, the preset of s is described as ${}^{\cdot}s = \{(s',t) | \exists Q, Q' \in 2^S, ((Q,$ $t,Q') \in F \wedge s' \in Q \wedge s \in Q')\}$ and the postset is $s^{\cdot} = \{(t,s') | \exists Q,$ $Q' \in 2^S, ((Q,t,Q') \in F \wedge s \in Q \wedge s' \in Q')\}$. $\exists Q, Q' \in 2^S$, s.t. $S_1 \in Q, S_2 \in Q', (Q,t,Q') \in F, \forall s \in Q, m(s) \geq 1$ is the sufficient and necessary condition that a transition t is enabled at marking m. If a transition t is fired at marking m, then the marking m' is $m' = (m \backslash Q) \oplus Q'$. This also is written as $m[t\rangle m'$.

The set of marking reachable from m is defined as the least set of markings, denoted by $[m\rangle$, such that

(1)$m \in [m\rangle$.

(2)if $m' \in [m\rangle$ and there exists a transition t such that $m'[t\rangle m''$ then $m'' \in [m\rangle$.

The set of firing sequences is defined as follow inductively:

(1)m_0 is a firing sequence.

(2)if $m_0[t_1\rangle m_1 \cdots [t_n\rangle m_n$ and $m_n[t_{n+1}\rangle m_{n+1}$ are two firing sequences, then $m_0[t_1\rangle m_1 \cdots [t_n\rangle m_n[t_{n+1}\rangle m_{n+1}$ is also a firing sequence.

Let $m_0[t_1\rangle m_1 \cdots [t_n\rangle m_n$ is a firing sequence, we call $t_1 \cdots t_n$ is a transition sequence. We use σ to range over transition sequences. The set of transition sequence of a net N s denoted by $TS(N)$.

Definition 4 If $\forall m \in [m_0\rangle, \forall s \in S \Rightarrow m(s) \leq 1$, (S,T,F,m_0) is a safe net system.

Since any bounded net system could be converted to an equivalent safety net system, therefore, this paper discusses the safe net system for the sake of simplicity.

2.3. Operations on Petri net

This paper aims to analyze multilevel systems that can perform different levels of actions. For example, the interaction of the system with high-level actions represents the interaction with high level users and the interaction of the system with low-level actions represents the interaction with low level users. This paper is to verify if the interplay between the high-level user and the high part of the system can affect a low-level users view of the system.

Thereby, this section defines some operations on Petri net. The set of transitions of Petri net is partitioned into two disjointed subsets: the set of high level transitions denoted by H and the set of low level transitions denoted by L, we use (S,L,H,F,m_0) to denote the net system mentioned above.

Definition 5 Let $N=(S,H\cup L,F,m_0)$, the operation of a transition sequence of net system is defined as follows:

$$\begin{cases} \varepsilon/H=\varepsilon \\ \delta t/H=\begin{cases}(\delta/H)t & t\in L \\ \delta/H & t\in H\end{cases}\end{cases} \quad \begin{cases} \varepsilon/L=\varepsilon \\ \delta t/L=\begin{cases}(\delta/L)t & t\in H \\ \delta/L & t\in L\end{cases}\end{cases}$$

Where, ε is a null transition. For example, assume $\sigma = l_1l_2h_1l_1h_2$, then $\sigma/L = h_1h_2$.

For a non-determined system the result statement will not be unique after the firing of a transition of a net system $N=(S,H\cup L,F,m_0)$, We call it result statement set denoted by $next(m_0,\sigma)$, $\sigma \in TS(N)$. However, for determined systems the result statement is unique, denoted by $step(m_0,\sigma)$.

Definition 6 A net system $N=(S,H\cup L,F,m_0)$, $m\in[m_0\rangle$, $View_L(m)=\{(s,m(s))|\exists t\in L,\ Q,Q'\in 2^s,(Q,t,Q')\in F\wedge s\in Q\}$.

Two statements of Petri net are low-level equal if the tokens of all places are same from a low-level users view.

Definition 7 To a net system $N=(S,H\cup L,F,m_0)$, two statements are low-level equal, if and only if:

$\forall m_1,m_2\in[m_0\rangle, m_1 \overset{L}{\simeq} m_2 iff View_L(m_1)=View_L(m_2)$

Definition 8 To a net system $N=(S,H\cup L,F,m_0)$, two results statement sets are low-level equal, if and only if:

$\forall A,B\subseteq[m_0\rangle, A\overset{L}{\simeq}B, iff \exists m_1\in A,m_2\in B, s.t. View_L(m_1)=View_L(m_2)$

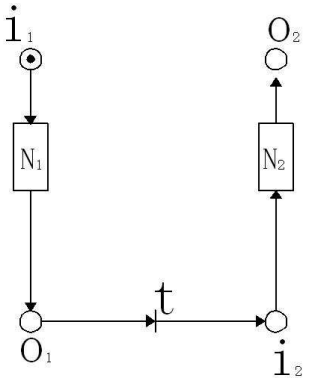

Figure 2: *Sequence composition*

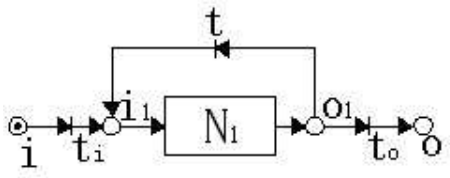

Figure 3: *Iteration composition*

2.4. The definitions of composition

Owing to its well-defined rigorous semantics, Petri net has been applied in many areas to model and verify the security properties of a system model, but it is very difficult to use it to model complex systems.

However, the analysis will be simplified if we can combine small nets into a complex net system without changing the security properties of these small nets. Thus, this section elaborates on sequence, iteration, parallel and alternative compositions.

Definition 9 Let $N_1=(S_1,H_1\cup L_1,F_1,m_{01})$, $N_2=(S_2,H_2\cup L_2,F_2,m_{02})$ be two Petri net systems, such that $S_1\cap S_2=\emptyset$ and $(H_1\cup L_1)\cap(H_2\cup L_2)=\emptyset$. For $N=(S,H\cup L,F,m_0)$, if

(1)$S=S_1\cup S_2$

(2)$H=H_1\cup H_2$, $L=L_1\cup L_2\cup\{t\}$

(3)$F=F_1\cup F_2\cup\{(o_1,t),(t,i_2)\}$

We say N is the sequence composition of N_1 and N_2, denoted by $N=N_1\cdot N_2$. Fig. 2 demonstrates the composition.

Definition 10 Let $N_1=(S_1,H_1\cup L_1,F_{11},m_{01})$ be a Petri net system. For $N=(S,H\cup L,F,m_0)$, if

(1)$S=S_1\cup\{\mathrm{i},\mathrm{o}\}$

(2)$T=T_1\cup\{t_i,t_o,t\}$, $\{t_i,t_o,t\}\subseteq L$

(3)$\{t_i,t_o,t\}\subseteq L$

We say N is the iteration composition of N_1, denoted by $N=N_1*$. Fig. 3 demonstrates the composition.

Definition 11 Let $N_1=(S_1,H_1\cup L_1,F_1,m_{01})$ and $N_2=(S_2,H_2\cup L_2,F_2,m_{02})$ be two Petri net systems, such that

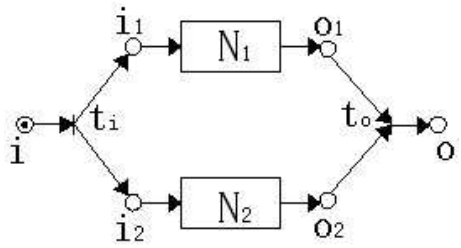

Figure 4: *Parallel composition*

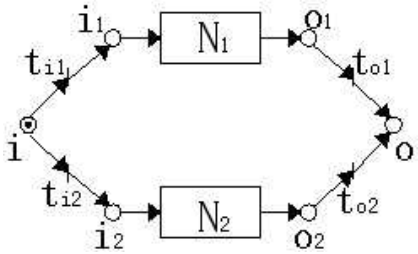

Figure 5: *Alternative composition*

$S_1 \cap S_2 = \emptyset$ and $(H_1 \cup L_1) \cap (H_2 \cup L_2) = \emptyset$. For $N = (S, H \cup L, F, m_0)$, if

(1)$S = S_1 \cup S_2 \cup \{i, o\}$

(2)$S = S_1 \cup S_2 \cup \{i, o\}$, $\{t_i, t_o\} \subseteq$ L

(3)$F = F1 \cup F2 \cup \{(i, t_i), (t_i, i_1), (o_1, t_o), (t_2, o), (t_i, i_2), (o_2, t_o)\}$

We say N is the parallel composition of N_1 and N_2, denoted by $N{=}N_1||N_2$.

Fig. 4 demonstrates the composition.

Definition 12 Let $N_1 = (S_1, H_1 \cup L_1, F_1, m_{01}), N_2 = (S_2, H_2 \cup L_2, F_2, m_{02})$ be two Petri net systems, such that $S_1 \cap S_2 = \emptyset$ and $(H_1 \cup L_1) \cap (H_2 \cup L_2) = \emptyset$. For $N = (S, H \cup L, F, m_0)$, if

(1)$S = S_1 \cup S_2 \cup \{i, o\}$

(2)$T = T_1 \cup T_2 \cup \{t_{i1}, t_{i2}, t_{o1}, t_{o2}\}$

(3)$F = F_1 \cup F_2 \cup \{(i, t_{i1}), (i, t_{i2}), (t_{i1}, i1), (t_{i2}, i2),$

We call N is alternative composition of N_1 and N_2, denoted by $N{=}N_1{+}N_2$. Fig.5 demonstrates the composition.

3. Modelling the ND property in cyber-physical system

3.1. The definition of ND security model

Security models depict the systems confidentiality, integrity and availability. If information flows from high level users to low level users, and at the same time the low level users observe something about high level user activity, then confidential information of system can be deduced by the low level users by information flow.

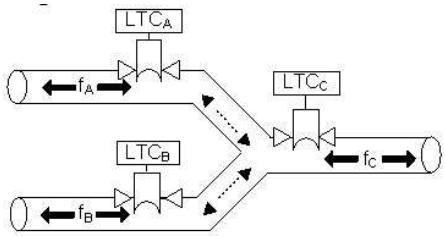

Figure 6: *Pipeline network*

In 1986, non-deducibility [5,10] property was first proposed by Sutherland. non-deducibility is originally defined as follows: given two functions f1 and f2, a state transition sequences set and a particular state sequence with a known output on f1(), then information will flow from f1() to f2() if and only if $(\exists\sigma \in \Sigma)(\exists z : f_2^{-1}(z) \neq \lambda), \forall\overline{\sigma} \in \Sigma : f_1(\sigma) = f_1(\overline{\sigma}), (f_2(\overline{\sigma}) \neq z)$.

Theorem 1 Information will not flow from f1 to f2 if there does not exist any unique output produced by function f1. Proof. The negation of the equation describes the requirement for information not to flow from f1 to f2.

$$\neg\{(\exists\sigma \in \Sigma)(\exists z: f_2^{-1}(z) \neq \lambda), \forall\overline{\sigma} \in \Sigma : f_1(\sigma) = f_1(\overline{\sigma}), (f_2(\overline{\sigma}) \neq z)\} = (\exists\sigma \in \Sigma)(\exists z: f_2^{-1}(z) \neq \lambda), \forall\overline{\sigma} \in \Sigma : f_1(\sigma) = f_1(\overline{\sigma})$$
$$\Rightarrow (f_2(\overline{\sigma}) \neq z) = (\forall\sigma \in \Sigma)(\forall z: f_2^{-1}(z) \neq \lambda), \neg\{\forall\overline{\sigma} \in \Sigma : f_1(\sigma) = f_1(\overline{\sigma})$$
$$\Rightarrow (f_2(\overline{\sigma}) \neq z)\} = (\forall\sigma \in \Sigma)(\forall z: f_2^{-1}(z) \neq \lambda), \exists\overline{\sigma} \in \Sigma : \neg\{f_1(\sigma) = f_1(\overline{\sigma})$$
$$\Rightarrow (f_2(\overline{\sigma}) \neq z)\} = (\forall\sigma \in \Sigma)(\forall z: f_2^{-1}(z) \neq \lambda), \exists\overline{\sigma} \in \Sigma : f_1(\sigma) = f_1(\overline{\sigma}) \wedge (f_2(\overline{\sigma}) = z)$$

Definition 13 Formally, a net system is ND secure if and only if

$$\forall\sigma \in TS(N), \exists\sigma' \in TS(N) \ \wedge next(m_0, \sigma) \overset{L}{\simeq} next(m_0, \sigma')$$

3.2. Abstract cyber-physical system

The natural gas pipeline system, as a typical application of cyber-physical systems, provides rich computational and physical processes and their interactivity [10]. Flow control systems (FCSs) in the system automate or control the state of gas or fluid in the pipeline. FCS devices directly coordinate with certain physical components to maintain control over the pipeline, such as coordinating with actuators by actuating signals. The embedded computer in FCS devices comprises long-term control (LTC) unit, which is responsible for communicating with other FCSs and coordinating the gas commodity distribution. LTCs execute two commands, i.e., raising and lowering the flow.

Fig.6 shows a gas pipeline network with three LTCs that control the sub-networks A, B, and C respectively,

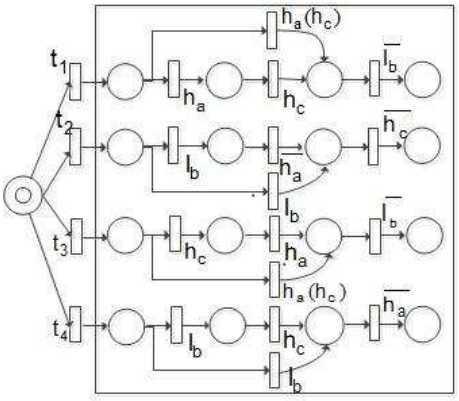

Figure 7: *Pipeline systemmodel*

which are geographically separated in large distances. Either of the two gas flow commands, i.e., the raising and lowering of the flow, that LTC C executes on its controlled pipe will affect neighbouring sub-networks necessarily, results in observable actions at location A and location B in the network of pipes, and the following invariant holds:

$$fc = fa + fb \tag{1}$$

Where fa, fb and fc represent the changes of gas flow of the pipes controlled at A, B, and C respectively.

As shown in Fig.7, the transitions in the system are represented by h_a, h_c and l_b, and $\bar{h}_a$, $\bar{h}_c$ and $\bar{l}_b$ are their corresponding output. Here, $h_a(h_c)$ represents a high level action that changes the flow at A(C), which results in a change at $h_c(h_c)$, due to the coordination between A and C. B possibly experiences a change in physical flow at A and C in the form of a low-level output, $\bar{l}_b$. The gas pipeline system is modelled in Fig. 7 using Petri net.

3.3. Analysis of ND property in natural gas pipeline system

Theorem 2 The gas flow in the pipeline system is ND secure.

Proof. Considering the set of executable transition sequences $TS(N) = \{h_a h_c \bar{h}_b, h_a \bar{h}_b, h_c \bar{h}_b, h_b \bar{h}_a \bar{h}_c, h_b \bar{h}_c, h_b \bar{h}_a, h_b \bar{h}_c \bar{h}_a, h_c h_a \bar{h}_b\}$, every high level transition is compatible with a low level transition. That is to say, changes experienced at a controlled line could be the result of any high level transition or their inter-cross. Thus, a low-level observer could not deduce which high level action performed what change. Hence, According to definition 3 the gas pipeline system flow is ND secure.

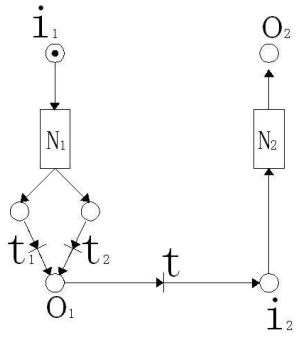

Figure 8: *The conditions for sequence composition*

4. Analysis of four compositions of non-deducibility model in cyber-physical system

This section gives and proves sufficient and necessary conditions for four representative compositions based on Petri net for ND security model in CPSs. These results allow the CPSs designers to connect small or individual systems, verified to be ND secure, to form a ND secure complex CPS.

4.1. Sequence composition

Theorem 3 Let $N_1 = (S_1, H_1 \cup L_1, F_1, m_{01})$ and $N_2 = (S_2, H_2 \cup L_2, F_2, m_{02})$ be two Petri net systems which are ND, then $N = N1 \cdot N2$ is ND iff:

$\forall(s', t') \in {}^{\cdot}o_1$, if $t' \in H_1$, then $\exists(s'', t'') \in {}^{\cdot}o_1$. Fig.8 demonstrates the sufficient and necessary conditions for sequence composition.

Proof. (1) Sufficiency: N is ND Let $(s_1{}', t_1{}') \in {}^{\cdot}o_1$, and do not exist $(s'', t'') \in {}^{\cdot}o_1$. Considering the transition sequence $\sigma = \sigma_1 t_1{}' t \in TS(N)$, such that $next(m_0, \sigma) \overset{L}{\simeq} next(m_0, \sigma')$, then N is not ND. So the assumption does not hold.

(2)Necessary:$\forall(s', t') \in {}^{\cdot}o_1$, if $t' \in H_1$, then $\exists(s'', t'') \in {}^{\cdot}o_1$

Let $\forall\sigma \in TS(N)$, if $\sigma \in TS(N_1)$, there will be a transition sequence *sigma'*, such that, because N_1 is ND. Therefore, N is ND. If $\sigma \notin TS(N_1)$, there will be a transition sequence $\sigma_1 t' t \sigma_2$, where $\sigma_1 \in TS(N_1)$, $\sigma_2 \in TS(N_2)$. If $t' \in L$, it is obvious that N is ND. If $t' \in H_1$, then $\exists(s'', t'') \in {}^{\cdot}o_1$, such that $next(m_0, \sigma) \overset{L}{\simeq} next(m_0, \sigma')$, where $\sigma = \sigma_1 t' t \sigma_2$ and $\sigma' = \sigma_1 t'' t \sigma_2$. Therefore, N is ND secure.

4.2. Iteration composition

Theorem 4 Let $N1 = (S_1, H_1 \cup L_1, F_1, m_{01})$ be a Petri net system which is ND, then $N = N_1*$ is ND if and only if

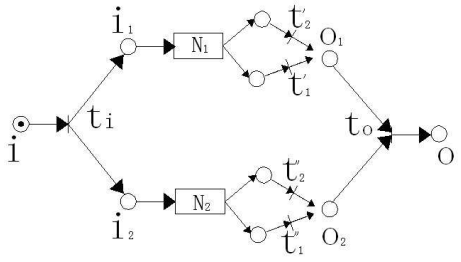

Figure 9: *The conditions for parallel composition*

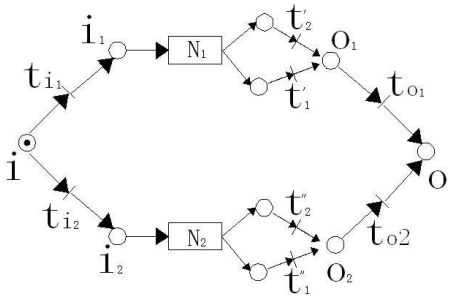

Figure 10: *The conditions for alternative composition*

$\forall(s',t') \in {}^{\cdot}o_1$, if $t' \in H$, then $\exists(s'',t'') \in {}^{\cdot}o_1$. Owing to the sufficient and necessary conditions for iteration composition are similar to sequence composition, so Fig.8 demonstrates the sufficient and necessary conditions for iteration composition.

Proof. (1) Sufficiency: N is ND secure
Assuming $(s_1{}',t_1{}') \in {}^{\cdot}o_1, t_1{}' \in H_1$ and not exist $(s'',t'') \in {}^{\cdot}o_1$. We consider the transition sequence $\sigma = t_i\sigma_1 t_1{}' t_o \in TS(N)$, where $\sigma_1 \in TS(N_1)$. N is not ND since there is not the corresponding σ'', such that $next(m_0,\sigma) \stackrel{L}{\simeq} next(m_0,\sigma')$, Similarly, we can give the proof for the $\sigma = t_i\sigma_2 t_2{}' t_o \in TS(N)$, if $\sigma_2 \in TS(N_2)$. N is not ND. So the assumption does not hold.

(2)Necessary: $\forall(s_1{}',t_1{}') \in {}^{\cdot}o_1, (s_2{}',t_2{}') \in {}^{\cdot}o_2$, $t_1{}' \in H$ then $\exists(s_1{}'',t_1{}'') \in {}^{\cdot}o_1$ and $t_2{}' \in H$ and $\exists(s_2{}'',t_2{}'') \in {}^{\cdot}o_1$.

Let $\forall\sigma \in TS(N)$, if $\sigma \in TS(N_1)$, there will be a transition sequence σ', such that $next(m_0,\sigma) \stackrel{L}{\simeq} next(m_0,\sigma')$, because N_1 is ND. Likewise, we can prove the conclusion if $\sigma \in TS(N_2)$. If $\sigma \notin TS(N_1)$ and $\sigma \notin TS(N_2)$, we suppose $\sigma = t_i\sigma_1 t' t_o$, where$\sigma_1 \in TS(N_1)$. If $t' \in L$, it is obvious that N is ND. If $t' \in H_1$, according to the assumption, $\exists(s'',t'') \in {}^{\cdot}o_1$, such that, where $\sigma = t_i\sigma_1 t' t_o$ and $\sigma = t_i\sigma_1 t'' t_o$. Since N is sequence composite by place i and o, it is ND from theorem 3. Therefore, N satisfies ND.

4.3. Parallel composition

Theorem 5 Let $N_1 = (S_1, H_1 \cup L_1, F_1, m_{01})$ and $N_1 = (S_1, H_1 \cup L_1, F_1, m_{01})$ be two Petri net systems which are ND. Then $N = N1||N2$ is ND if and only if $\forall(s_1{}',t_1{}') \in {}^{\cdot}o_1, (s_2{}',t_2{}') \in {}^{\cdot}o_2$, if $t_1{}' \in H$, then $\exists(s_1{}'',t_1{}'') \in {}^{\cdot}o_1$ and if $\exists(s_1{}'',t_1{}'') \in {}^{\cdot}o_1$ then $\exists(s_2{}'',t_2{}'') \in {}^{\cdot}o_1$. Fig.9 demonstrates the sufficient and necessary conditions for parallel composition.

Proof. (1) Sufficiency: N is ND secure

Assuming $(s_1{}',t_1{}') \in {}^{\cdot}o_1$, $(s_1{}',t_1{}') \in {}^{\cdot}o_1$ and do not exist $(s'',t'') \in {}^{\cdot}o_1$. We consider the transition sequence $\sigma = t_i\sigma_1 t_1{}' t_o \in TS(N)$, where $\sigma_1 \in TS(N_1)$. N is not ND since there is not the corresponding σ'', such that $next(m_0,\sigma) \stackrel{L}{\simeq}$
$next(m_0,\sigma')$, Similarly, we can give the proof for the $\sigma = t_i\sigma_2 t_2{}' t_o \in TS(N)$, if $\sigma_2 \in TS(N_2)$. N is not ND. So the assumption does not hold.

(2)Necessary:$\forall(s_1{}',t_1{}') \in {}^{\cdot}o_1, (s_2{}',t_2{}') \in {}^{\cdot}o_2$, if $t_1{}' \in H$, then $\exists(s_1{}'',t_1{}'') \in {}^{\cdot}o_1$, and if $t_2{}' \in H$ then $\exists(s_2{}'',t_2{}'')$
$\in {}^{\cdot}o_1$.

Let $\forall\sigma \in TS(N)$, if $\sigma \in TS(N_1)$, there will be a transition sequence σ', such that, because N_1 is ND. Likewise, we can prove the conclusion if $\sigma \in TS(N_2)$. If $\sigma \notin TS(N_1)$ and $\sigma \notin TS(N_2)$, we suppose $\sigma = t_i\sigma_1 t' t_o$, where $\sigma_1 \in TS(N_1)$. If $t' \in L$, it is obvious that N is ND. If $t' \in H_1$, according to the assumption, $\exists(s'',t'') \in {}^{\cdot}o_1$, such that $next(m_0,\sigma) \stackrel{L}{\simeq} next(m_0,\sigma')$, where $\sigma = t_i\sigma_1 t' t_o$ and $\sigma = t_i\sigma_1 t' t_o$. Since N is sequence composite by place i and o, it is ND from theorem 3. Therefore, satisfies ND.

4.4. Alternative composition

Theorem 6 Let $N_1 = (S_1, H_1 \cup L_1, F_1, m_{01})$ and $N_2 = (S_2, H_2 \cup L_2, F_2, m_{02})$ be two Petri net systems which are ND. If $\forall(s_1{}',t_1{}') \in {}^{\cdot}o_1, (s_2{}',t_2{}') \in {}^{\cdot}o_2$, if $t_1{}' \in H$ then $\exists(s_1{}'',t_1{}'') \in {}^{\cdot}o_1$ and if $t_2{}' \in H$ then $t_2{}' \in H$, then $N = N_1 + N_2$ is ND. Fig.10 demonstrates the sufficient and necessary conditions for alternative composition.

Proof. (1)Sufficiency: N is ND secure Similarly, assuming $(s_1{}',t_1{}') \in {}^{\cdot}o_1$, $t_1{}' \in H_1$ and do not exist $(s'',t'') \in {}^{\cdot}o_1$. We consider the transition sequence $\sigma = t_{i1}\sigma_1 t_1{}' t_{o1} \in TS(N)$, where $\sigma_1 \in TS(N_1)$. N is not ND since there is not the corresponding σ'', such that $next(m_0,\sigma) \stackrel{L}{\simeq} next(m_0,\sigma')$, Similarly, we can give the proof for the $\sigma = t_{i2}\sigma_2 t_2{}' t_{o2} \in TS(N)$, if $\sigma_2 \in TS(N_2)$. So the assumption does not hold.

(2)Necessary $\forall(s_1{}',t_1{}') \in {}^{\cdot}o_1, (s_2{}',t_2{}') \in {}^{\cdot}o_2$, *if* $t_1{}'$
$\in H$ *then* $\exists(s_1{}'',t_1{}'') \in {}^{\cdot}o_1$ and *if* $t_2{}' \in H$ *then*$\exists(s_2{}'',t_2{}'')$
$\in {}^{\cdot}o_1$

Similarly, let $\forall\sigma \in TS(N)$, if $\sigma \in TS(N_1)$, there will be a transition sequence σ', such that $next(m_0,\sigma) \stackrel{L}{\simeq} next($
$m_0,\sigma')$ because is ND. The proof is similar if $\sigma \in TS(N_2)$. If $\sigma \notin TS(N_1)$, we suppose the sequence $\sigma = t_{i1}\sigma_1 t' t_{o1}$, where $\sigma_1 \in TS(N_1)$. If $t' \in L$, it is obvious that N is ND. If $t' \in H_1$, according to the assumption, then $\exists(s'',t'') \in {}^{\cdot}o_1$, such that $next(m_0,\sigma) \stackrel{L}{\simeq} next(m_0,\sigma')$, where $\sigma = t_{i1}\sigma_1 t' t_{o1}$ and $\sigma = t_{i1}\sigma_1 t'' t_{o1}$.Since N is sequence composite by place i and o, it is ND secure from theorem 3. Therefore, N is ND.

5. Conclusions

CPSs are composite heterogeneous systems and embody complex interactions between cyber components and physical components. Securing the confidentiality of CPSs requires security models to represent the interactions. ND security model is extremely attractive since the physical actions of CPSs are inherently observable.

In this paper, we present a rigorous formal method for CPSs security specification and show its applicability to the abstract cyber-physical natural gas pipeline flow network system. Four compositions of ND of CPSs are elaborated on a unified framework of Petri net. This paper also gives and proves the sufficient and necessary conditions for the four compositions. The results allow a system designer to connect small components verified to be ND secure to form a heterogeneous ND secure cyber-physical system. We believe that the present study provides a formal method and the foundation for exploring confidentiality and information security in CPSs.

6. Acknowledgements

This work was partially supported by the NSF of China under grants No. 61173048 and No. 61300041, and Specialized Research Fund for the Doctoral Program of Higher Education of China under grant No. 20130074110015, and NSF of Anhui, China under Grant No. KJ2011ZD06, and NSF of Chuzhou University, Anhui, China under grant No. 2013RC004 and No. 2012qd08.

References

[1] T.Gamage and B.McMillin, Nondeducibility-Based Analysis of Cyber-Physical Systems,IFIP Advances in Information and Communication Technology, Editor, C. Palmer and S. Shenoi. Springer Boston, **311**, 169-183 (2009).

[2] R.Focardi and R.Gorrieri, The Compositional Security Checker: a tool for the verification of information flow security properties,IEEE Transactions on Software Engineering, **23**, 550-571 (1997).

[3] C.Li, J.Shiguang, Z.Conghua and Z.Yi, Covert Channel Capacity Analysis Based on Entropy,International Symposium on Information Science and Engineering, ISISE'08, 363-367 (2008).

[4] M. Hussain, A high bandwidth covert channel in network protocol, Proc. 2011 International Conference on Information and Communication Technologies (ICICT), **2011**, 1-6.

[5] D. Sutherland, A Model of Information, Proc. the 9th National Computer Security Conference, 175-183 (1986).

[6] A.Maamir, A.Fellah and L.A.Salem, Fine Granularity Access Rights for Information Flow Control in Object Oriented Systems, Proc. International Conference on Information Security and Assurance, ISA 2008., 122-128 (2008).

[7] Ren S, Zhang T, Mu DJ, Study of Reversible Information Hiding Scheme Based on GHM and ASA, Applied Mathematics & Information Sciences, **6**, 253-260 (2012).

[8] S. Frau, R. Gorrieri and C. Ferigato, Petri Net Security Checker: Structural Non-interference at Work, Formal Aspects in Security and Trust,Editor, D. Pierpaolo, G. Joshua and M. Fabio. Springer-Verlag, 210-225 (2009).

[9] S. C. Song, Z. Cong-hua, J. Shi-guang and L. Hai-yang, Analysis for the composition of information flow security properties on Petri net, Proc. 2010 2nd International Conference on Information Science and Engineering (ICISE), **2010**, 1859-1863.

[10] R. Akella, H. Tang and B.M. McMillin, Analysis of information flow security in cyberCphysical systems, International Journal of Critical Infrastructure Protection, **2010**, 157-173.

Jingming Wang received his B.S. degree from AnHui Normal University in 2002, M.S. degree from Peking University in 2005. He is currently a doctor candidate of East China University of Science and Technology. His research interests include software engineering, information flow security and formal methods. He is a student member of the China Computer Federation.

Huiqun Yu received his B.S. degree from Nanjing University in 1989, M.S. degree from East China University of Science and Technology (ECUST) in 1992, and Ph.D. degree from Shanghai Jiaotong University in 1995, all in computer science. He is currently a Professor of computer science with the Department of Computer Science and Engineering at ECUST. From 2001 to 2004, he was a Visiting Researcher in the School of Computer Science at Florida International University. His research interests include software engineering, high confidence computing systems, cloud computing and formal methods. He is a member of the ACM, a senior member of the IEEE, and a senior member of the China Computer Federation.