Observing for Changes: Nondeducibility Based Analysis of Cyber-Physical Systems

Thoshitha T. Gamage [*] Bruce M. McMillin[*]
{ttgdp5@mst.edu, ff@mst.edu}
Department of Computer Science
Missouri University of Science and Technology, Rolla, MO 65409-0350

Abstract

Preserving Information Flow properties in a Cyber-Physical System (CPS) is challenging because cyber domain decisions and changes manifest themselves as visible changes in the physical domain. In this paper, a nondeducibility based observability analysis for CPSs is presented. In many such systems a single low level observer's capacity to deduce high level actions range from limited to none. Yet, a collaborative set of observers strategically located throughout a network may be able to fully deduce all high level actions. In order to understand the effect of multiple observers in a CPS, this paper models a distributed power electronics control device network using a simple DC circuit. After analyzing this model, it was possible to show that the number of observers required, to fully deduce all high level actions of a system, linearly increase with the number of configurable units. Further, a simplified definition for nondeducibility based on "uniqueness of low level projections" is presented. This definition is used to show if a system with two levels of security domains needs to be nondeducibility secure, there should not exist any unique low level projections.

[*]This work was supported in part by NSF MRI award CNS-0420869 and CSR award CCF-0614633, and in part by the MST Intelligent Systems Center.

1 Introduction

Modern systems are vastly complex. Recent trends in system design has lead to the development of more and more *cyber-physical* and *pervasive* systems. Cyber-physical systems (CPSs) are systems with pure cyber components highly integrated with pure physical components. Some of the reasons behind such integration are to provide better resource utilization, control, fault tolerance and performance. However, it is also understood that physical manifestations of such systems could lead to information leakage to unintended and unwanted parties.

Most modern commodity transportation systems exhibit cyber-physical behavior. Two interesting and important CPSs of this kind are the national gas distribution network and national power distribution network. Systems which were considered "standalone" a decade back, have now evolved into becoming complex interconnected networks. For example, modern cars allow the driver the ability to talk to other cars, the manufacturer, security agents and emergency respondent crews while operating the vehicle, connecting a vivid and wide variety of systems together.

While most modern CPSs are able to provide extensive functional capabilities, the security aspect of these systems is under intense scrutiny of the research community. Much of the work done in this area is on integrity and SCADA protection[1, 2]. Yet, for distributed systems, confidentially becomes a much more important issue since by divulging the state of the system, an adversary is able to determine where to attack the system. Access control based security models have proven to be sufficient in preventing unauthorized access, modifications and altercations in cyber domain. Yet, preventing unauthorized disclosure of secret information due to physical interactions has opened up a completely new dimension to the conventional way of looking at system security; how much can an observer learn about a system's confidential operation by examining its physical operation?

In a CPS, decisions and interactions of the cyber domain are manifested on the physical domain as observable changes. Consider a section of a gas distribution pipeline shown in Figure 1. Notice that whenever one of the distributors makes a change to his section of the pipeline – by releasing or tightening the corresponding valve – there would be physically observable changes such as pressure or flow in other parts of the pipeline. As an example, after observing pressure and/or flow changes on the local section of the pipe, $distributor_b$ may be able to derive gas flow values of $distributor_c$ who is also known to be fed by the same main distributor $distributor_a$. In terms of security, here we see an unintended information leakage occurring between two competitive distributors.

However, the very nature of this system may provide enough obfuscation, leaving a low level (LL) observer in doubt as to what actions could have contributed to such a physical change. These obfuscating features of CPSs could be utilized to prevent information leakage, with the use of a special brand of security properties called *"Information Flow Properties"*.

This paper concentrates on measuring the confidentiality of CPSs using information flow coupled with physical commodity flow analysis. The rest of this paper is laid out as follows. Section 2 is a brief introduction to the concept of information flow security. Section 3 is an analysis on the formal definition of nondeducibility, including a reexamination of the nondeducibility and an alternative definition for it based on the definition found in [3]. This is followed up by Section 4, a discussion on the role of observers and the effect of multiple ob-

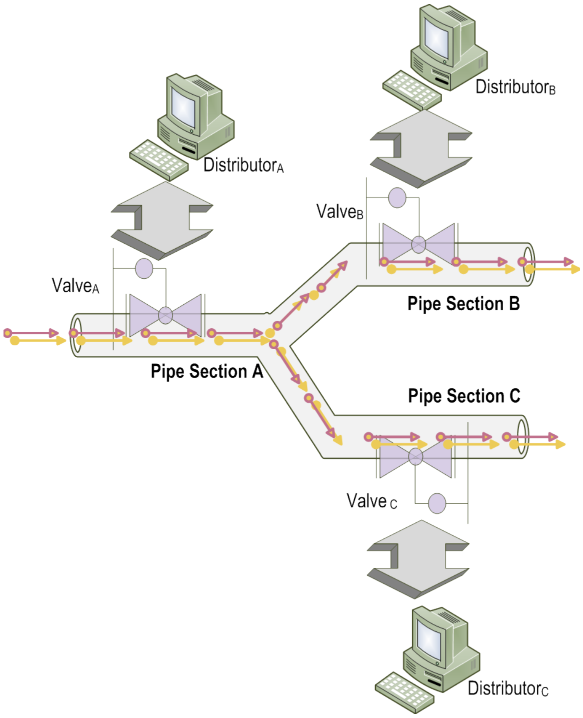


Figure 1. A Section of a Gas Distribution Pipeline with Three Distributors

servers in deducing high level (*HL*) information from a CPS. Section 5 presents the authors' findings on the number of observers requirement. Section 6 is an exclusive summary of the results including two theorems on observability of series and parallel-connected circuits. A conclusion is provided in Section 7.

2 Information Flow Properties and Security

The traditional notion of security has evolved around the means providing and preserving confidentiality, integrity and availability. These being the core concepts of computer security, have lead to many formal and reputed security models. Some examples for such formal security models are Bell-Lapadula(BLP) Model[4, 5], Biba Model[6] and HRU model[7]. Unfortunately, most of these formal security models concentrate on providing access control and, access control alone is not able to preserve information flow security of a system.

Information Flow (IF) properties are used to better describe confidentiality of systems. It has been shown that interactions between cyber aspects and physical aspects in CPSs lead to violations of information flow security of systems[8]. The BLP model for example is easy to understand and implement yet, does not model a CPS that well. BLP does not restrict *HL* actions from being observed from *LL* users, which indirectly violates the "no write down" notion of the *-*property*[4]. Further, covert channels may still exist even in best-designed systems[9].

IF properties define ways of restricting or preventing unintended and unwanted information disclosure between different user groups. These properties are also termed "possibilistic security properties"[10]. Recent research interest in this area has shown steady inclines, mainly attributed to the cyber-physical nature of modern systems. In the context of IF security, there is an implicit concept of two basic user groups: a *HL* user group with a secret to preserve, and a *LL* user group, which should be prevented from acquiring the secret.

There are many IF properties listed in literature. However, it is possible to identify three primary properties namely, noninterference[11], noninference[12] and nondeducibility[3]. Out of these three properties, ***noninterference*** could be considered as the most restrictive property. A system is said to be noninterference secure if *HL* inputs do not interfere with *LL* outputs. A comparatively less restrictive property is the ***noninference*** property which states that, for every legal execution of a system, the execution produced by purging all *HL* actions should also be a legal trace. The concept of "execution" is explained further in in Section 3.

Nondeducibility is yet another information flow property. This property describes the ability to deduce *HL* inputs based on *LL* outputs and could be considered as the most relaxed among the three primary IF properties listed above. The amount of *HL* action information deducible depends on several factors. This study examines the effect of the number of *LL* observers on the level of deducibility. Based on a simple DC circuit based model, a comprehensive analysis on deducibility security for systems with physical observations is provided.

3 Nondeducibility

Nondeducibility was first introduced by Sutherland in 1986. The original definition of nondeducibility[3] states that, given two information functions $f_1()$ and $f_2()$, a set of state transition sequences Σ and a particular state sequence[*] with a known output on $f_1()$, information flows from $f_1()$ to $f_2()$ if and only if,

$$(\exists \sigma \in \Sigma)(\exists z : f_2^{-1}(z) \neq \lambda), \forall \bar{\sigma} \in \Sigma : f_1(\sigma) = f_1(\bar{\sigma}), (f_2(\bar{\sigma}) \neq z) \quad (1)$$

What does the above definition imply? In order to understand the concept behind nondeducibility more clearly, let's consider the system in concern as a state machine[†]. A state machine M consists of $S = \{s_1, s_2, \ldots\}$ set of subjects, $Q = \{q_1, q_2, \ldots\}$ set of system states and a set of commands or events $C = \{c_1, c_2, \ldots\}$. Commands are further sub categorized as input commands $I \subset C$ denoted $\acute{I} = \{\acute{i}_1, \acute{i}_2, \ldots\}$ and output events $\acute{O} \subset C$ denoted $\acute{O} = \{\acute{o}_1, \acute{o}_2, \ldots\}$ respectively. Following an input command $\acute{i} \in \acute{I}$, the state machine makes a transition to a new state $T : C \times Q \rightarrow Q$ which results in changes to state variables of the machine. These changes are depicted as a particular output $\acute{o} \in \acute{O}$. A sequence of inputs $\acute{I}^*$ causes a sequence of state transitions T^* (an execution) resulting in a sequence of outputs $\acute{O}^*$.

Further, two functions – *projection function* $proj(G, \sigma, q_0)$ and *trace function* $trace(\sigma, q_0)$ – are defined as follows. Given a set of subjects[‡] $G \subset S$, an execution σ and an initial state q_0, the *projection function* results in a sequence of outputs $\acute{o}^* \in \acute{O}^*$ of σ which G is permitted to see. Formally, this is denoted as $proj(G, \sigma, q_0) = \acute{o}^*$. Similarly, $trace(\sigma, q_0) = \acute{i}^*$ is the set of input

[*] A state sequence is also defined as an ***execution*** in[13]

[†] The notion of modeling a system as a state machine is found throughout the literature[14, 15, 16, 13, 10] with in certain cases, also denoted as an event machine.

[‡] Subjects in a state machine depicts users in the corresponding system

commands which contributed to produce $\acute{o}^*$. The implicit notion of *"permit"* makes way to sub categorize subjects based on some security clearance. In classical theory, these would be a set of *HL* subjects/users[§] G_{hl}/U_{hl} and a set of *LL* subjects/users G_{ll}/U_{ll}.

The above formal definition of a system leads to the following reexamination of (1). Consider $f_1() \equiv proj()$ and $f_2() \equiv trace()$. Assume that a *LL* subject (or a user) $s_i \in G_{ll}$ sees the same projection output $\acute{o}_i^*$ for two different executions σ_i and σ_j but sees different trace results. Knowing how the system behaves, s_i is able to deduce that $\acute{o}_i^*$ was probably due to a particular set of inputs $\acute{i}_i^* \subset \acute{I}$. This is denoted as $trace(\sigma_i, q_0) = \acute{i}_i^*$. Yet, since $trace(\sigma_j, q_0) \neq \acute{i}_i^*$ and knowing some of the elements of $\acute{i}_i^*$ are *LL* inputs, s_i is able to deduce and/or narrow down which particular *HL* actions caused $\acute{o}_i^*$.

Nondeducibility can be also argued as a way of identifying *uniqueness* of events of a system. Thus, in the context of nondeducibility, information flow between two functions describes the amount of knowledge deducible by members of one user group about the actions of another user group by looking at the same data in different ways. Having analyzed the *"requirement for information flow to occur"*, the following lemma is presented as the *"requirement for information flow not to occur"* between two functions of a system.

Lemma 1 (**Nondeducibility**). *Given a set of executions Σ and two information functions $f_1()$ and $f_2()$, information does not flow from $f_1()$ to $f_2()$ if there does not exist any unique outputs produced by function $f_1()$.*

Proof. The negation of the equation (1) describes the requirement for information not to flow between functions. In doing so, the universal quantifiers in (1) become existential quantifiers.

$$\begin{aligned}
&\neg\{(\exists\sigma \in \Sigma)(\exists \text{ƶ} : f_2^{-1}(\text{ƶ}) \neq \lambda), \forall\bar{\sigma} \in \Sigma : f_1(\sigma) = f_1(\bar{\sigma}), (f_2(\bar{\sigma}) \neq \text{ƶ})\}\\
&\quad = (\exists\sigma \in \Sigma)(\exists \text{ƶ} : f_2^{-1}(\text{ƶ}) \neq \lambda), \forall\bar{\sigma} \in \Sigma : f_1(\sigma) = f_1(\bar{\sigma}) \implies (f_2(\bar{\sigma}) \neq \text{ƶ})\\
&\quad = (\forall\sigma \in \Sigma)(\forall \text{ƶ} : f_2^{-1}(\text{ƶ}) \neq \lambda), \neg\{\forall\bar{\sigma} \in \Sigma : f_1(\sigma) = f_1(\bar{\sigma}) \implies (f_2(\bar{\sigma}) \neq \text{ƶ})\}\\
&\quad = (\forall\sigma \in \Sigma)(\forall \text{ƶ} : f_2^{-1}(\text{ƶ}) \neq \lambda), \exists\bar{\sigma} \in \Sigma : \neg\{f_1(\sigma) = f_1(\bar{\sigma}) \implies (f_2(\bar{\sigma}) \neq \text{ƶ})\}\\
&\quad = (\forall\sigma \in \Sigma)(\forall \text{ƶ} : f_2^{-1}(\text{ƶ}) \neq \lambda), \exists\bar{\sigma} \in \Sigma : f_1(\sigma) = f_1(\bar{\sigma}) \wedge (f_2(\bar{\sigma}) = \text{ƶ})
\end{aligned}$$

□

In order to make this simplified definition more meaningful, it is related to the earlier discussion on projection and trace functions in the following manner. If there is always more than one execution resulting in the same *LL* projection, s_i is not able to deduce what *HL* actions caused *LL* observations. In other words, to preserve nondeducibility, there must exist more than one possible *HL* trace for an observed *LL* projection. This result is utilized in the discussion of observability and number of observers requirement in subsequent Sections.

4 Related Work and Motivation

The previous section presented a formal condition required to be held, in order to preserve nondeducibility of a system. As appealing as it may seem, there are several factors, which

[§] Conceptually, the terms user groups and subject groups infer the same idea here onwards affect the level of nondeducible security preservable in a system. Out of these, defining what information of the system needs to be kept secret and identifying user groups based on what they should and should not observe are two of the most important factors. Yet, the very nature of modern systems has proven its increasingly hard to identify and distinguish these factors. Provided that it was possible to distinguish different user groups[¶] and determine what needs to be kept secret, let's look at another interesting aspect of nondeducibility; the effect of number of observers needed to deduce *HL* information from a system.

4.1 The Role of Observers on Nondeducibility of a CPS

Distributed power electronics control devices are installed in strategic locations along the national power distribution network, primarily to increase the fault tolerance and to avoid cascading failures[17]. When a faulty line is detected, these devices cooperate with other similar devices on the network, to come up with new, distributed power flow redistribution decisions. These decisions are communicated between devices and changes are made to the physical transmission lines to re-stabilize the overall network.

FACTS[‖] devices are configurable and programmable devices. Since a particular device is capable of injecting or absorbing active and reactive power of a set of transmission lines under its control, some aspects of the distributed decision (made in cyber domain) will eventually reflect on the physical domain as flow changes in power lines. Prior work in [18] showed that, for a single FACTS device, in terms of information flow security, an external observer with the capability to measure flow changes might be able to deduce what was the local action on a particular power line(s) and infer what the overall state of the system is. However, this work does not address the question of how many cooperating observers would it require to fully discover changes in the system state?

In reality, due to the high individual cost of a FACTS device, they are deployed sparsely in the network. Thus, few observers will be required to fully determine the system state, and, determining this number will characterize the information security of the system. Modeling an actual AC power distribution network for the purpose of analysis has proven a difficult task thus, the power distribution network is modeled as a simple DC circuit. Although this is not a fully accurate or a realistic model of the actual power distribution network, it provides adequate information to understand the dynamics of an actual system.

5 Deducible Observations

In the following section, a DC circuit based model is built to analyze deducibility of a system. This section branches out into two subsections based on the two basic types of topology – series-connected and parallel-connected – employed in this study. Further, extended circuit models are introduced to better illustrate and analyze nondeducibility, ultimately resulting in theorems which describe general systems.

[¶] For the simplicity of this discussion, authors consider two user groups namely, *HL* users U_{hl} and *LL* users U_{ll}

[‖] FACTS stands for Flexible AC Transmission Systems. This is another name given to distributed control of power electronics devices mentioned earlier

In relation to the state machine model introduced in Section 3, the DC circuit model is formally defined as follows. The model consists of variable resistors R_i – denoting configurable/programmable devices of the network, external observers $observer_j$ and edges between resistors – denoting transmission lines. Each R_i is considered as a HL user $\forall i : R_i \in U_{hl}$ while observers are considered as LL users $\forall j : observer_j \in U_{ll}$. The command set C consists of increase or decrease in resistance $R_i\{\uparrow | \downarrow\} \in \acute{I}$, change in current readings $I\{\uparrow | \downarrow\} \in \acute{O}$ and voltage readings $V\{\uparrow | \downarrow\} \in \acute{O}$.

This model considers *steady state behavior of the system* thus, only one $\acute{i}_i \in \acute{I}$ occurs at a given time. However, this single input action may propogate as multiple and/or different output changes along the edges, which an $observer_j$ is capable of observing. As an example, in Figure 2, $R_A \uparrow$ results in $V_y \downarrow$ and $I_y \downarrow$. Here, the confidential information is the actual input action i.e. $R_A \uparrow$. $observer_j$'s objective is to deduce what HL action(s) "specifically" caused particular LL observations in this case, $V_y \downarrow$ and $I_y \downarrow$. The voltage source is considered to be kept constant throughout the analysis.

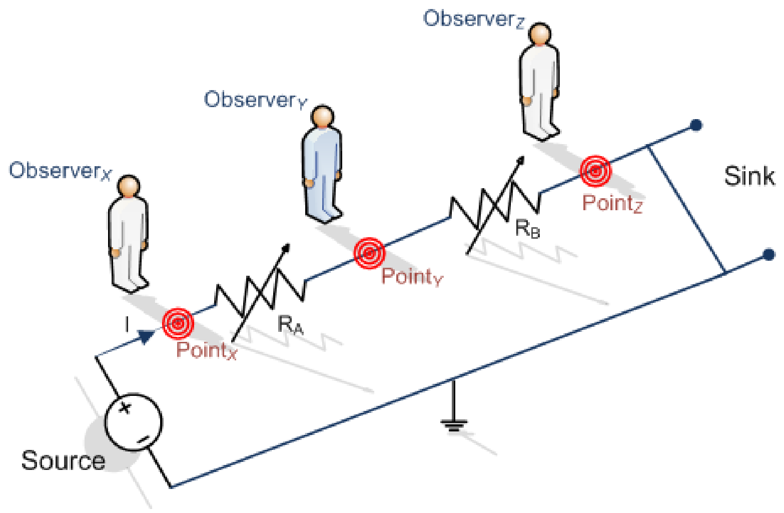


Figure 2. A two resistor series connected DC circuit. Resistors corresponds to variable power electronic devices

5.1 Series Connected Circuits

A simple form of all circuit models is the series-connected circuit. Figure 2 shows a two resistor series-connected DC circuit with three observation points. The corresponding low level observation matrix is given in Table 1. Here HL denotes High Level and LL denotes Low Level.

Note that here, $\acute{I} = \{R_A \uparrow, R_A \downarrow, R_B \uparrow, R_B \downarrow\}$ while $\acute{O} = \{I \uparrow, I \downarrow, V_y \uparrow, V_y \downarrow\}$. As a result, there are four(4) legal executions $\sigma_k : 1 \leq k \leq 4$, corresponding to each HL input command. These are denoted as rows in Table 1. Futher, the first entry of each row denotes the corrsponding *trace* denoted $trace(\sigma_k, q_0)$ for each execution σ_k. The rest of the entries correspond to *projections*.

	LL Observations			
HL Change	$V_y \uparrow$	$V_y \downarrow$	$I_y \uparrow$	$I_y \downarrow$
$R_A \uparrow$		√		√
$R_B \uparrow$		√		√
$R_A \downarrow$	√		√	
$R_B \downarrow$	√		√	

Table 1. Low level observation matrix for a two resistor series-connected DC circuit with one deducible observer

Lemma 2. *In a base series-connected circuit with two configurable units, the placement of any number of observers preserves nondeducibility.*

Proof. Consider two traces $\sigma_1 = \{R_A \uparrow, V_y \downarrow, I_y \downarrow\}$ and $\sigma_2 = \{R_B \uparrow, V_y \downarrow, I_y \downarrow\}$. For $observer_y$ in Figure 2, the corresponding *projections* would be $proj(U_{ll}, \sigma_1, q_0) = proj(U_{ll}, \sigma_2, q_0) = \{V_y \downarrow, I_y \downarrow\}$. Nevertheless, the corresponding *traces* are different as seen in $trace(\sigma_1, q_0) = R_A \uparrow$ and $trace(\sigma_2, q_0) = R_B \uparrow$. Same explaination applies for the other two executions as well. Thus there are no unique *LL* projections which according to 1, preserves Nondeducibility.

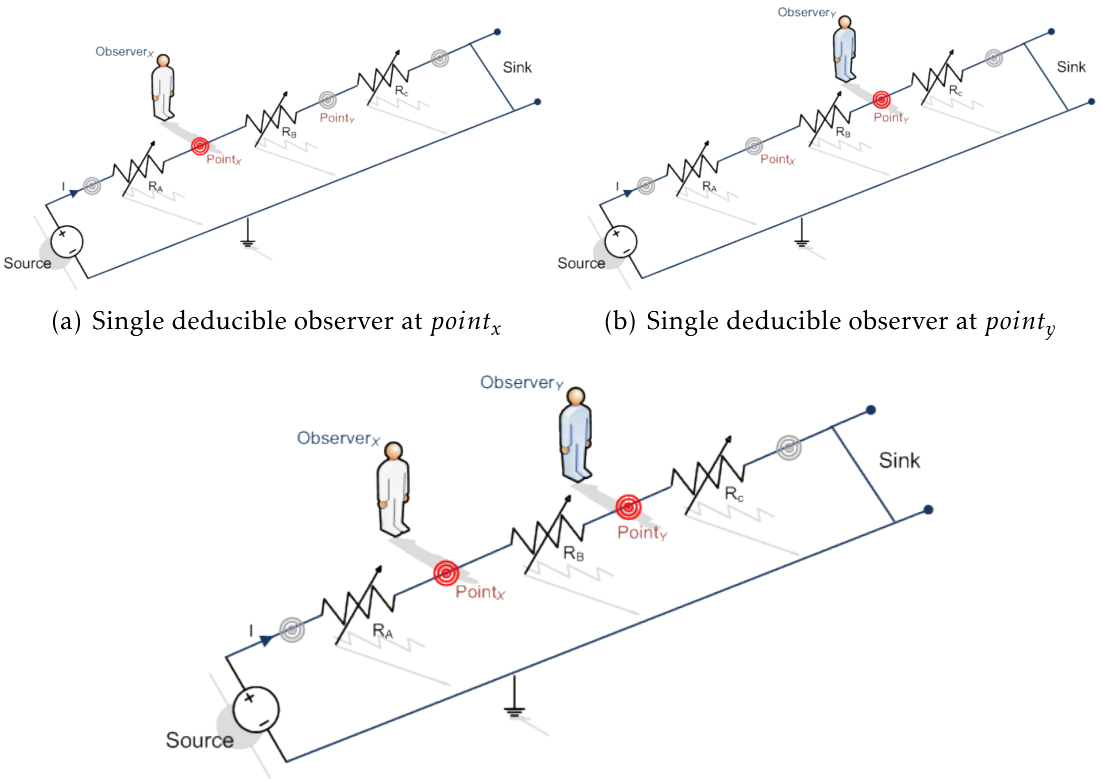
In relation to Lemma 1, assume that $observer_y$ sees $\{V_y \downarrow, I_y \downarrow\}$ which corresponds to $f_1(\sigma) \equiv proj(U_{ll}, \sigma_1, q_0)$. The corresponding *trace* for σ_1 yeilds $R_A \uparrow$. However, there exists another execution (σ_2) with the same projection – $f_1(\bar{\sigma}) \equiv proj(U_{ll}, \sigma_2, q_0) = \{V_y \downarrow, I_y \downarrow\}$ but with a different trace – $f_2(\bar{\sigma}) \equiv trace(\sigma_2, q_0) = R_B \uparrow$.

Notice that $observer_x \in U_{ll}$ at the source and $observer_z \in U_{ll}$ at the sink, will not observe any voltage changes due to the physical nature of this layout. In contrast, $observer_y \in U_{ll}$ is able to see voltage changes, although with multiple possibilities. For example, a decrease in voltage reading at $point_y$ $V_y \downarrow$ could be due to either $R_A \uparrow$ or $R_B \uparrow$ and an increase in voltage $V_y \uparrow$ could be due to either $R_A \downarrow$ or $R_B \downarrow$. further, $observer_y$ is considered as the only *"deducible observer"* for this network. **A deducible observer** is an observer who can take multiple readings, in most cases different in types (for example, voltage and current as in this case), which can be used to deduce *HL* information.

The interesting point about the above observation matrix is that, $observer_y$ does not see any unique *LL* output traces. Thus, he is not able to deduce what part of the overall system (whether it's R_A or R_B) made the *HL* change contributed to a *LL* observation. □

5.1.1 Extended Series Connected Circuit

Figure 3 shows an extended series circuit derived from Figure 2, by appending one additional resistor $R_C \in U_{hl}$. For the analysis which follows, only deducible observers are considered which in this case are $observer_x$ and $observer_y$. Figure 3(a) shows a three resistor series-connected DC circuit with a single deducible observer at $point_x$ and Figure 3(b) shows a similar circuit with a single deducible observer at $point_y$. Table 2 presents a summary of *LL* observations for the afore mentioned extended circuit.



(a) Single deducible observer at $point_x$

(b) Single deducible observer at $point_y$

(c) Two deducible observers at points x and y

Figure 3. A Three Resistor Series Connected DC Circuit with Two Deducible Observers

Lemma 3. *A series circuit with $n \geq 3$ configurable units is fully deducible, with a minimum of n distinct readings and $n-1$ observers.*

Proof. Consider $observer_x$ at $point_x$. According to Table 2, the projection $\{V_x \uparrow, I \downarrow\}$ is compatible with two traces – $R_B \uparrow$ and $R_C \uparrow$. In otherwords, for the execution $\sigma = \{R_B \uparrow, V_x \uparrow, I \downarrow\}$, there exists another execution $\bar{\sigma} = \{R_C \uparrow, V_x \uparrow, I \downarrow\}$ with $proj(U_{ll}, \sigma, q_0) = proj(U_{ll}, \bar{\sigma}, q_0)$ but $trace(U_{ll}, \sigma) \neq trace(U_{ll}, \bar{\sigma})$. Similarly, the projection $V_x \downarrow, I \uparrow$ is compatible with two traces – $R_B \downarrow$ and $R_C \downarrow$. What this means is, just by simply obsevering $V_x \uparrow, I \downarrow$ (or $V_x \downarrow, I \uparrow$), $observer_x$ can not deduce whether it was $R_B \uparrow$ or $R_C \uparrow$ (or $R_B \downarrow$ or $R_C \downarrow$) which caused the changes.

Having said that, there are two unique projections – $\{V_x \downarrow, I \downarrow\}$ and $\{V_x \uparrow, I \uparrow\}$ – corresponding to traces $R_A \uparrow$ and $R_A \downarrow$. thus, whenever R_A commits a HL change, $observer_x$ is able deduce it exactly. In summary, $observer_x$ is able to deduce R_A but not R_B or R_C.With similar reasoning, it is not hard to see that $observer_y$ at $point_y$ in isolation (as shown in Figure 3(b)) can only deduce actions of R_C but not that of either R_A or R_C (refer Table 2).

Notice there are multiple configurable units after $point_x$[**] and only one configurable unit before[††]. Similarly, w.r.t. $point_y$, there are multiple pre-locations but only one post-location. However, if $observer_x$ and $observer_y$ collaborate and share their local knowledge as in Figure 3(c), each and every HL action would result in a unique LL projection. For example, consider

[**] hereafter named as **post-location**s w.r.t. a certain observation point

[††] named **pre-location**

the collective projection $\{V_x \uparrow, V_y \uparrow, I \downarrow\}$ which corresponds to the HL trace $R_C \uparrow$. According to Table 2, there are no other legal executions with the same LL projection. Thus, the network shown in Figure 3 is fully deducible with two(2) observers and three(3) distinct readings.

	LL Observations					
HL Change	$V_x \uparrow$	$V_x \downarrow$	$V_y \uparrow$	$V_y \downarrow$	$I \uparrow$	$I \downarrow$
$R_A \uparrow$		√		√		√
$R_B \uparrow$	√			√		√
$R_C \uparrow$	√		√			√
$R_A \downarrow$	√		√		√	
$R_B \downarrow$		√	√		√	
$R_C \downarrow$		√		√	√	

Table 2. Low level observation matrix for a three resistor series-connected DC circuit with two deducible observers

It is not hard to see that, every additional resistor appended to the circuit in Figure 3(c) will produce at least one additional and distinct reading and would require one additional observer to observe it. Thus, the number of observers and distinct reading required to fully deduce the network increase linearly with the increase in configurable units. Since changes to I is equally visible to any observer, the number of observers required is always one less than that of the number of configurable units. □

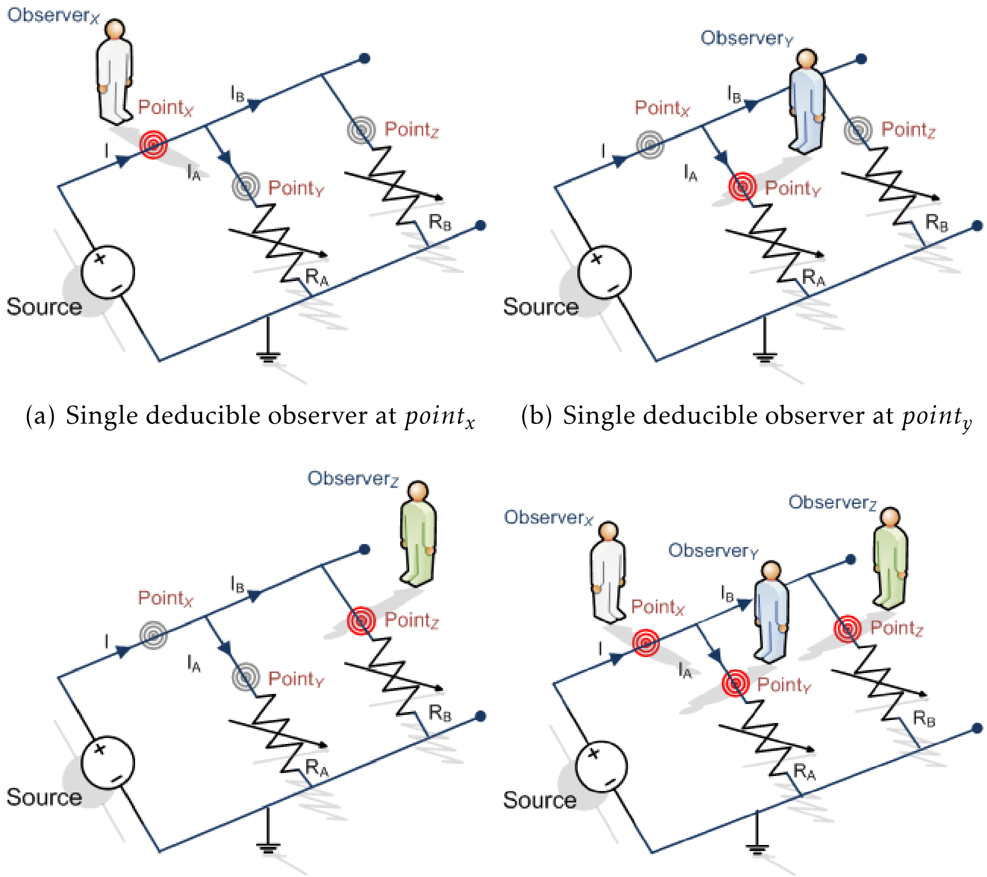
5.2 Parallel Connected Circuits

Figure 4 shows an illustration of a two resistor parallel-connected DC circuit, including all possible single observer scenarios. Here, it is not possible to observe any V changes at any of the "deducible points". Yet, $observer_x$ at the source can be considered as a deducible observer simply because, the total current I branches out into two currents I_A and I_B along the parallel links of the circuit. The LL observation matrix for this setup is presented in Table 3.

Lemma 4. *In a base parallel-connected circuit with two parallel resistors, any combination of two observers is sufficient to fully deduce the circuit.*

Proof. Consider a single deducible observer at $point_z$ shown in Figure 4(c). $observer_z$ is not able to derive any information about actions of R_A. This is because, $I_B \uparrow$ and $I_B \downarrow$ columns in Table 3 does not have any entries for traces $R_A \uparrow$ and $R_A \downarrow$. Similarly, a single observer at $point_y$ is not able to derive anything about actions of R_B (see Figure 4(b)). As for $observer_x$ in Figure 4(a), $I \downarrow$ is consistent with either $R_A \uparrow$ and $R_B \uparrow$ where as $I \uparrow$ is consistent with either $R_A \downarrow$ and $R_B \downarrow$. What this concludes is that, with a single observer, this setup is nondeducible secure.

A scenario of multiple cooperating observers is shown in Figure 4(d). By analyzing the corresponding LL observation matrix in Table 3, it is possible to see that any combination of two observers are able to formulate unique projections for all HL traces. More specifically,



(a) Single deducible observer at $point_x$ (b) Single deducible observer at $point_y$

(c) Single deducible observer at $point_z$ (d) Three deducible observers

Figure 4. A Two Resistor Parallel Connected DC Circuit with Three Deducible Observers

	LL Observations					
HL Change	$I_A \uparrow$	$I_A \downarrow$	$I_B \uparrow$	$I_B \downarrow$	$I \uparrow$	$I \downarrow$
$R_A \uparrow$		√				√
$R_B \uparrow$				√		√
$R_A \downarrow$	√				√	
$R_B \downarrow$			√		√	

Table 3. Low level observation matrix for a two resistor parallel-connected DC circuit with three deducible observers

either $observer_x \& observer_y$ or $observer_x \& observer_z$ or $observer_z \& observer_y$ can make the system nondeducibility insecure.

As an example, consider the observer combination $observer_x \& observer_y$. The corresponding set of collaborative projections are $\{I_A \downarrow I \downarrow\}$, $\{I_B \downarrow I \downarrow\}$, $\{I_A \uparrow I \uparrow\}$ and $\{I_B \uparrow I \uparrow\}$. Note that all these projections are unique projections corresponding to $\{R_A \uparrow\}$, $\{R_B \uparrow\}$, $\{R_A \downarrow\}$ and $\{R_B \downarrow\}$

traces respectively. A simple analysis of the entries in Table 3 would show that this argument is true for other observer combinations as well. □

5.2.1 Extended Parallel Connected Circuit

An illustration for a three resistor parallel-connected DC circuit, including all five individual observer scenarios is shown in Figure 5. Table 4 is the corresponding *LL* observation matrix for Figure 5.

Lemma 5. *For a pure parallel-connected circuit with n parallel resistors, a minimum of n "strategically placed" observers are required to fully deduce the circuit.*

Proof. Proving that only three(3) observers are sufficient to fully deduce the network (shown in Figure 5(f)) is not that hard, taking into account Lemma (4) and one additional parallel path compared to Figure 4(d). However, not all combinations of three observers are capable of full deducibility. For example, an observer combination such as $\{observer_x, \wedge observer_y, \wedge observer_v\}$ can not even notice actions of R_B or R_C. For this observer combination, $\{I_V \downarrow, I \downarrow\}$ is a legal projection which is compatible with two traces – $R_B \uparrow$ and $R_C \uparrow$. Thus, the placement of observers is also important to fully deduce the network.

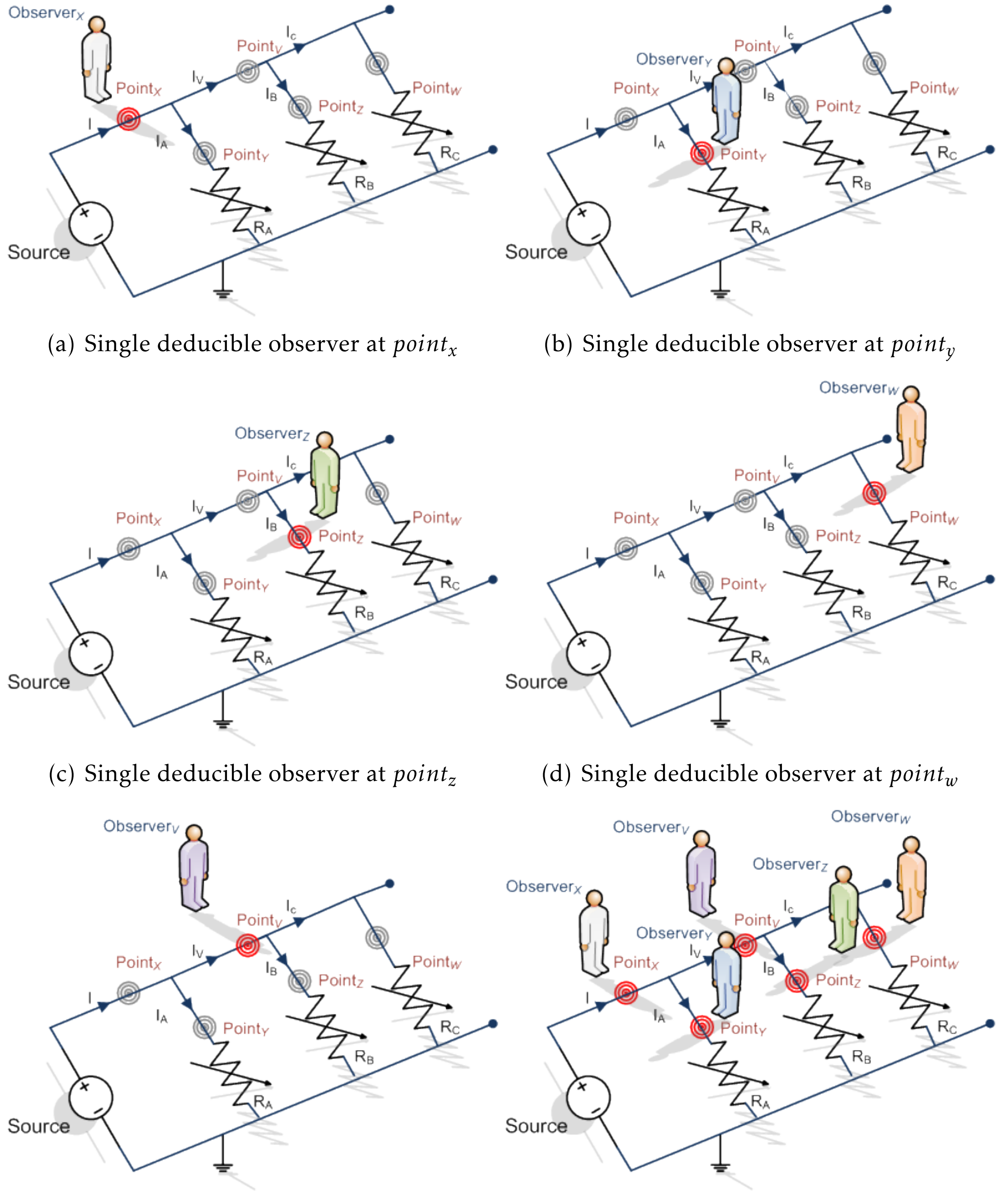
	LL Observations									
HL Change	$I_A \uparrow$	$I_A \downarrow$	$I_B \uparrow$	$I_B \downarrow$	$I_C \uparrow$	$I_C \downarrow$	$I_V \uparrow$	$I_V \downarrow$	$I \uparrow$	$I \downarrow$
$R_A \uparrow$		√								√
$R_B \uparrow$				√				√		√
$R_C \uparrow$						√		√		√
$R_A \downarrow$	√								√	
$R_B \downarrow$			√				√		√	
$R_C \downarrow$					√		√		√	

Table 4. Low level observation matrix for a three resistor parallel-connected DC circuit with five deducible observers

There are two post-locations(post parallel paths) and one pre-location(pre parallel path) w.r.t. *observer*$_v$'s view of the system. Interestingly, *observer*$_v$ can not observe pre-location changes and any post-location change observed at *point*$_V$ is compatible it either of the post-locations – preserves nondeducibility. Similarly, *observer*$_X$ has three(3) post-locations and as the last two columns of Table 4 shows, a single observable change is compatible with any of these post-locations. Further, an observer along any parallel path can only observe changes in that particular path. □

6 Summarized Results

In this section, an exclusive summary of the results observed for the two types of networks analyzed is presented including two derived theorems.



(a) Single deducible observer at $point_x$

(b) Single deducible observer at $point_y$

(c) Single deducible observer at $point_z$

(d) Single deducible observer at $point_w$

(e) Single deducible observer at $point_v$

(f) Five deducible observers

Figure 5. A Three Resistor Parallel Connected DC Circuit with Five Deducible Observers

6.1 Circuits With Only Series Connected Units

As a result of Lemma 2 and Lemma 3, it is possible to come up with the following Theorem on the observability of series-connected configurable units.

Theorem 1. *Observability of Series Connected Configurable Units: In a purely series-connected system with $n + m$ configurable units where n+$m \geq 3$, a single change observed by an observer$_i$ is*

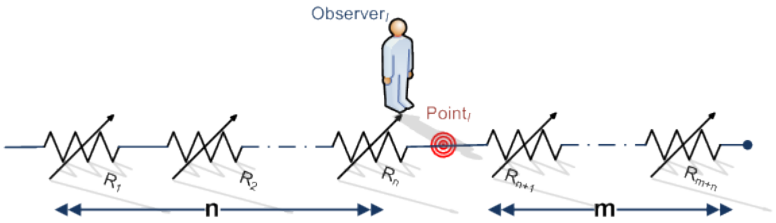


Figure 6. A Pure Series Connected System with $n+m$ configurable units and a Single Observer

consistent with either a change α in one of the n pre-locations or change β in one of the m post-locations with $\alpha = \bar{\beta}$.

Proof. This theorem can be proven using mathematical induction as follows.
Base case 01: From Lemma 2 (Figure 3(a)) with $n = 1, m = 2, \alpha =\uparrow$ and $\beta =\downarrow$. We see that $R_1 \uparrow, R_2 \downarrow, R_3 \downarrow$ is consistent with $V \downarrow$ and $R_1 \downarrow, R_2 \uparrow, R_3 \uparrow$ is consistent with $V \uparrow$.
Base case 02: From Lemma 2 (Figure 3(b)) with $n = 2, m = 1, \alpha =\uparrow$ and $\beta =\downarrow$. We see that $R_1 \uparrow, R_2 \uparrow, R_3 \downarrow$ is consistent with $V \downarrow$ and $R_1 \downarrow, R_2 \downarrow, R_3 \uparrow$ is consistent with $V \uparrow$. Thus, we see that the claim is true for the base cases.
Inductive Hypothesis: Assume the claim hold for a system with $n+m$ resistors.
Inductive Step: Let's move the observation point by one location to the left. Now, the system consists of $n+1$ pre-locations and $m-1$ post-locations. Since no other parameter of the system changed and the claim held for $n+m$ configuration, the claim holds for a system with $(n+1)+(m-1)$ configurable units.

□

6.2 Circuits With Only Parallel Connected Units

Most relevant to AC power distribution networks are the parallel connected topologies. In the realm of our corresponding DC model, these are the pure parallel-connected configurable units. Figure 7 shows a single observer *observer$_i$* at *point$_i$* with n pre-parallel paths and m post-parallel paths.

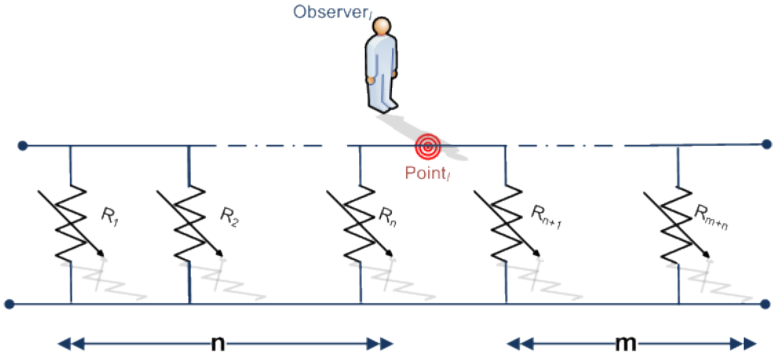


Figure 7. A Pure Parallel Connected System with $n+m$ configurable units and a Single Observer

- For a parallel-connected system with a single change at a time, an observation made by a single observer $observer_i$ is consistent with m post-parallel path unit changes.

- For the same system, changes in any of the n pre-parallel path units are not visible to $observer_i$.

- Two or more actions at any post-locations may compensate each other and cancel out the likelihood of an observation being made at $point_i$. Thus, a set of changes at post-locations can also be hidden from $observer_i$.

In addition, using the results of Lemma 4 and Lemma 5, the following theorem for parallel-connected networks is also presented.

Theorem 2. *Observability of Parallel Connected Configurable Units: For a pure parallel-connected system consisting of n pre-parallel paths and m post-parallel paths with respect to an $observer_i$, a total of $m+n$ minimum observers are required to fully deduce all HL actions. The combination of observers need to be selected as n pre-location deducible observers, and $m-1$ post-location deducible observers in conjunction with $observer_i$.*

Although not explicitly provided here, the above claim is also provable using mathematical induction.

7 Conclusion

This paper presented our results and findings on the number of minimum observers required to fully deduce systems with configurable units. Further, a simplified definition for *Nondeducibility* which is based on the "uniqueness" of *LL* projections was also presented. This study modeled a Cyber-Physical System using a simple DC circuit and analyzed the dynamics of the model for two types of connectivity: pure series-connected and pure parallel-connected. All observers were considered as *LL* users of the system with configurable units being *HL* users. The findings of this study lead to the following two corollaries on the minimum number of "deducible observers" required to fully deduce a system.

Corollary 1. *For series-connected systems with k number of configurable units, a minimum of k distinct readings and $k-1$ number of "deducible observers" are required to fully deduce all HL actions.*

Corollary 2. *To fully deduce a parallel system with $k = n+m$ number of configurable units, an $observer_i$ would require a minimum of n pre-location observers and $m-1$ post-location observers. Thus, including himself, the total minimum number of observers required would be $k = n+(m-1)+1$.*

The observer based view of the system can be considered as a *LL* domain view of *HL* action system such as a Cyber-Physical System (CPS). The findings in this paper show that the minimum number of observers requirement linearly increase with the number of configurable units. The focus of this paper was on full deducibility of a CPS however, with lesser number of observers than what's mentioned above, it would still be possible to *partially deduce* the system.

As an example, whenever $observer_y$ in Table 1 sees $\{V_y \downarrow, I_y \downarrow\}$, he is capable of deducing that either $R_A \uparrow$ or $R_B \uparrow$ has occurred.

Also noteworthy is the fact that the actual system behavior of a CPS such as the FACTS network considered in this study, is much more complex and different from a simple DC circuit. It is unrealistic to consider FACTS devices are directly connected to other FACTS devices. Nevertheless, interms of real power, the DC power model can be extended to the power grid [17]. Authors also consider the findings in this paper as a new starting point towards understanding how information flow properties behave in systems with cyber-physical interactions.

Future work in this area is aimed at analyzing the effect of multiple, simultaneous HL changes on the nondeducibility and to analyze hybrid connection networks(none pure series nor pure parallel networks as in this work) with different series and parallel connection configurations.

References

[1] P. S. M. Pires and L. A. H. Oliveira, "Security aspects of SCADA and corporate network interconnection: An overview," *Dependability of Computer Systems, International Conference on*, vol. 0, pp. 127–134, 2006.

[2] K. Barnes, B. Johnson, and R. Nickelson, "Introduction to SCADA protection and vulnerabilities," Idaho National Engineering and Environmental Laboratory, Idaho Falls, ID, USA, Tech. Rep. INEEL/EXT-04-01710, march 2004.

[3] D. Sutherland, "A model of information," in *In Proceeding of the 9th National Computer Security Conference*, Baltimore, MD, September 1986, pp. 175–183.

[4] D. E. Bell and L. J. LaPadula, "Secure computer systems: Mathematical foundations," MITRE Corporation, Tech. Rep. MTR-2547, March 1973.

[5] D. E. Bell and L. J. Lapadula, "Secure computer system: Unified exposition and multics interpretation," The MITRE Corporation, Tech. Rep. ESD-TR-75-306, 1976.

[6] K. J. Biba, "Integrity considerations for secure computer systems," MITRE Corporation, Bedford, MA, Tech. Rep. ESD-TR-76-372, April 1977.

[7] M. A. Harrison, W. L. Ruzzo, and J. D. Ullman, "Protection in operating systems," *Commun. ACM*, vol. 19, no. 8, pp. 461–471, 1976.

[8] H. Tang and B. M. McMillin, "Security property violation in CPS through timing," in *ICDCSW '08: Proceedings of the 28th International Conference on Distributed Computing Systems Workshops*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 519–524.

[9] R. Focardi and R. Gorrieri, "Classification of security properties (part i: Information flow)," in *FOSAD '00: Revised versions of lectures given during the IFIP WG 1.7 International School on Foundations of Security Analysis and Design on Foundations of Security Analysis and Design*. London, UK: Springer-Verlag, 2001, pp. 331–396.

[10] J. McLean, "A general theory of composition for a class of "possibilistic" properties," *IEEE Transactions on Software Engineering*, vol. 22, no. 1, pp. 53–67, 1996.

[11] J. Goguen and J.Meseguer, "Security policies and security models," in *Proceedings of the 1982 IEEE Symposium on Security and Privacy*, 1982.

[12] C. O'Halloran, "A calculus of information flow," in *ESORICS 90 – First European Symposium on Research in Computer Security*. AFCET, 1990, pp. 147–159.

[13] B. Alpern and F. B. Schneider, "Defining liveness," Cornell University, Ithaca, NY, USA, Tech. Rep., 1984.

[14] A. Zakinthinos and E. S. Lee, "A general theory of security properties," in *Proceedings of the 18th IEEE Computer Society Symposium on Research in Security and Privacy*, 1997.

[15] J. McLean, "A general theory of composition for trace sets closed under selective interleaving functions," *IEEE Symposium on Security and Privacy*, p. 79, 1994.

[16] N. Nagatou and T. Watanabe, "Run-time detection of covert channels," in *ARES '06: Proceedings of the First International Conference on Availability, Reliability and Security*, 2006, pp. 577–584.

[17] A. Armbruster, M. Gosnell, B. McMillin, and M. L. Crow, "Power transmission control using distributed max flow," in *COMPSAC '05: Proceedings of the 29th Annual International Computer Software and Applications Conference*, vol. 1. Washington, DC, USA: IEEE Computer Society, 2005, pp. 256–263.

[18] H. Tang and B. McMillin, "Analysis of the security of information flow in the advanced electric power grid using flexible alternating current transmission system (FACTS)," in *Critical Infrastructure Protection*. Springer Boston, 2008, pp. 43 – 56.