Chapter 12

NONDEDUCIBILITY-BASED ANALYSIS OF CYBER-PHYSICAL SYSTEMS

Thoshitha Gamage and Bruce McMillin

Abstract Controlling information flow in a cyber-physical system (CPS) is challenging because cyber domain decisions and actions manifest themselves as visible changes in the physical domain. This paper presents a nondeducibility-based observability analysis for CPSs. In many CPSs, the capacity of a low-level (LL) observer to deduce high-level (HL) actions ranges from limited to none. However, a collaborative set of observers strategically located in a network may be able to deduce all the HL actions. This paper models a distributed power electronics control device network using a simple DC circuit in order to understand the effect of multiple observers in a CPS. The analysis reveals that the number of observers required to deduce all the HL actions in a system increases linearly with the number of configurable units. A simple definition of nondeducibility based on the uniqueness of low-level projections is also presented. This definition is used to show that a system with two security domain levels could be considered "nondeducibility secure" if no unique LL projections exist.

Keywords: Cyber-physical systems, information flow security, nondeducibility

1. Introduction

Cyber-physical systems (CPSs) are systems with pure cyber components that are highly integrated with pure physical components. However, in certain cases, the high integration causes information leakage to unauthorized parties mainly due to physical manifestations. This is especially true when it comes to preserving the confidentiality of high-level (HL) user interactions.

Gas distribution and electrical power distribution networks are examples of CPSs. Much of the work related to CPSs has focused on maintaining integrity in SCADA systems [3, 10]. However, in the case of a distributed system, confidentiality is also important because information about the system state can be used by an adversary to determine where to attack the system. Preventing

C. Palmer and S. Shenoi (Eds.): Critical Infrastructure Protection III, IFIP AICT 311, pp. 169–183, 2009.

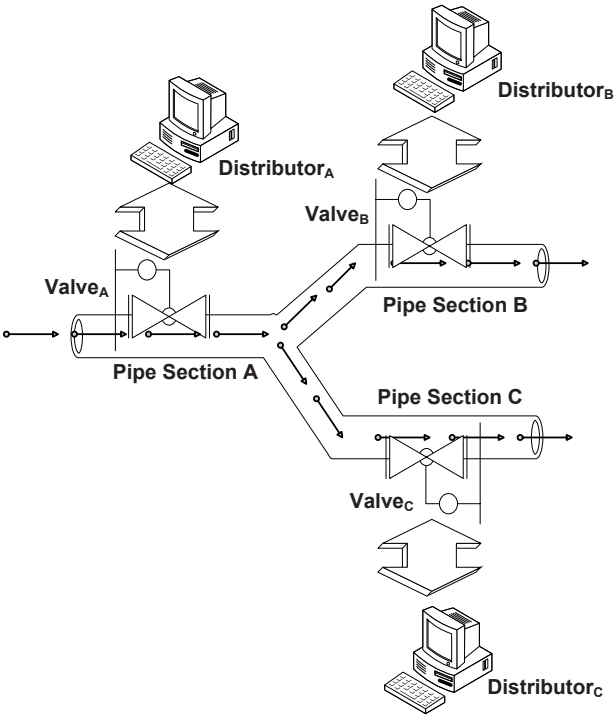


Figure 1. Gas pipeline with three distributors.

the unauthorized disclosure of sensitive information via physical interactions has opened up a new dimension of security – How much can an observer learn about a system by examining its physical operation?

To clarify the issue, consider the gas distribution pipeline system in Figure 1. When Distributor$_C$ applies a change at Valve$_C$, flow changes occur throughout the network. Knowing the topology of the system and how it operates, a rival distributor (Distributor$_B$), who is also fed by the same main distributor (Distributor$_A$), may be able to derive gas flow values in Distributor$_C$'s network. Thus, the confidentiality of Distributor$_C$'s actions is compromised and unintended information leakage occurs between the two competing distributors.

CPSs have inherent obfuscation features that can leave a low-level (LL) observer in doubt about the actions that could have contributed to a physical change. These features can be used to prevent information leakage. This paper focuses on measuring the confidentiality of CPSs using information flow coupled with physical commodity flow analysis.

2. Information Flow Properties

Confidentiality, integrity and availability are three major security goals. Several formal security models (e.g., Bell-LaPadula, Biba and HRU models) have

been proposed. However, most of these models focus on access control, which on its own, is insufficient to preserve information flow security.

The Bell-LaPadula model, for example, does not restrict HL actions from being observed by LL users; this indirectly violates the "no write down" (*–security) property [4]. Covert channels exist even in the best-designed systems [5]. Furthermore, interactions between the cyber and physical aspects of a CPS can lead to information flow security violations [13].

Information flow properties, also termed "possibilistic security properties" [7], are useful for describing the confidentiality of systems. These properties define ways for restricting unintended information disclosure between different user groups, primarily an HL user group with a secret to preserve, and an LL user group that should not acquire the secret.

Noninterference [6], noninference [9] and nondeducibility [11] are the three principal information flow properties.

Noninterference is the most restrictive of the three properties. It requires HL inputs not to interfere with LL outputs.

Noninference is a less restrictive property. It states that, for every legal "execution" of a system, the execution produced by purging all HL actions should also be a legal trace. Note that an execution is an interleaved sequence of system inputs and outputs of the system.

Nondeducibility, the least restrictive of the three properties, describes the ability to deduce HL inputs based on LL outputs.

The amount of information deducible about HL actions depends on several factors. This paper examines the effect of the number of LL observers on the level of deducibility. A simple DC circuit model is used to conduct a comprehensive analysis on the deducibility property for systems that permit physical observations.

3. Nondeducibility

Sutherland's definition of nondeducibility [11] states that, given two information functions $f_1()$ and $f_2()$, a set of state transition sequences Σ, a particular state sequence and the existence of a certain state sequence with a known output on $f_2()$, then information flows from $f_1()$ to $f_2()$ if and only if:

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

A state sequence is also called an "execution" [1].

To better understand Equation (1), consider two functions, *projection* and *trace*, which are defined as follows. Given a certain user group G, an execution of the system σ and an initial state q_0, the *projection* function $proj(G, \sigma, q_0)$ provides a sequence of outputs of σ that G is permitted to see. The *trace* function $trace(\sigma, q_0)$ takes σ and q_0 as inputs and yields all the input commands (or events) in σ. These functions are borrowed from the state machine (or event machine) abstraction of systems, which is frequently used by the information flow security research community [1, 7, 8, 14]. The implicit notion of "permit" allows the subcategorization of user groups based on security clearances. In

classical theory, these are a set of HL subjects/users G_{HL}/U_{HL} and a set of LL subjects/users G_{LL}/U_{LL}.

With reference to Equation (1), consider $f_1() \equiv proj()$ and $f_2() \equiv trace()$. Further, assume that an LL user $u_i \in G_{LL}$ sees the same projection output $\mathcal{X}$ for two different executions σ_i and σ_j ($proj(u_i, \sigma_i, q_0) = proj(u_i, \sigma_j, q_0)$) but sees different trace results. Knowing how the system behaves, u_i can rule out certain HL input commands because they are incapable of producing $\mathcal{X}$. However, u_i is unable to deduce the specific HL input action that caused $\mathcal{X}$. Thus, the "uniqueness of output events" impacts the deducibility, which, in turn, leads to the following lemma.

LEMMA 1 *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 and only if function $f_1()$ does not produce any unique outputs.*

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

$$\begin{aligned}
&\neg\{(\exists\sigma \in \Sigma)(\exists \mathfrak{z} : f_2^{-1}(\mathfrak{z}) \neq \lambda), \forall\bar{\sigma} \in \Sigma : f_1(\sigma) = f_1(\bar{\sigma}),\ (f_2(\bar{\sigma}) \neq \mathfrak{z})\} \\
&= (\exists\sigma \in \Sigma)(\exists \mathfrak{z} : f_2^{-1}(\mathfrak{z}) \neq \lambda), \forall\bar{\sigma} \in \Sigma : f_1(\sigma) = f_1(\bar{\sigma}) \Rightarrow (f_2(\bar{\sigma}) \neq \mathfrak{z}) \\
&= (\forall\sigma \in \Sigma)(\forall \mathfrak{z} : f_2^{-1}(\mathfrak{z}) \neq \lambda), \neg\{\forall\bar{\sigma} \in \Sigma : f_1(\sigma) = f_1(\bar{\sigma}) \Rightarrow (f_2(\bar{\sigma}) \neq \mathfrak{z})\} \\
&= (\forall\sigma \in \Sigma)(\forall \mathfrak{z} : f_2^{-1}(\mathfrak{z}) \neq \lambda), \exists\bar{\sigma} \in \Sigma : \neg\{f_1(\sigma) = f_1(\bar{\sigma}) \Rightarrow (f_2(\bar{\sigma}) \neq \mathfrak{z})\} \\
&= (\forall\sigma \in \Sigma)(\forall \mathfrak{z} : f_2^{-1}(\mathfrak{z}) \neq \lambda), \exists\bar{\sigma} \in \Sigma : f_1(\sigma) = f_1(\bar{\sigma}) \wedge (f_2(\bar{\sigma}) = \mathfrak{z}).
\end{aligned}$$

Lemma 1 describes the requirement for information flow not to occur between two information functions of a system. In other words, for every HL action $\mathfrak{z}$ of a system that produces a certain LL observation $\mathcal{X}$, if it is possible to find another execution with the same $\mathcal{X}$ but that was caused by a different HL action, the system preserves the nondeducibility of input actions. This result is used in the discussion of observability and the number of observers requirement later in this paper.

4. Motivation

Given a CPS, suppose that it is possible to identify and distinguish between different user groups based on their security clearances and to determine the information or actions that need to be kept secret. Using Lemma 1, what is the minimum number of LL observers required to fully deduce all the HL actions of the CPS?

This paper answers the question using a distributed power electronics control device (FACTS) network as an example CPS. FACTS stands for flexible AC transmission systems. FACTS devices are installed at strategic locations along

power distribution networks, primarily to increase fault tolerance and avoid cascading failures [2]. The devices are configurable and programmable, and are capable of injecting or absorbing active and reactive power from a set of transmission lines under their control.

When a faulty line is detected, FACTS devices cooperate with other devices on the network to derive distributed power flow redistribution decisions. Once the decisions are made, changes are applied to the corresponding physical transmission lines to re-stabilize the overall network. Thus, some aspects of the cyber domain decisions eventually manifest themselves in the physical domain as flow changes in power lines. Prior work [12] has shown that, in terms of information flow security, an external observer could deduce the local action on a particular power line or lines, and infer the overall state of the system based on external flow change measurements. However, this paper does not address the question of how many cooperating observers are required to fully discover changes in the system state.

5. Deducible Observations

Modeling an actual AC power distribution network for the purpose of analysis is a difficult task. To simplify the analysis, we model the power distribution network as a simple DC circuit. In this model, the variable resistors R_i denote configurable/programmable devices and the edges between resistors denote transmission lines. External observers position themselves at connection points and other strategic locations to observe flow changes along the edges. Each R_i is considered to be an HL user ($\forall i : R_i \in U_{HL}$) while each observer is considered to be an LL user ($\forall j : \text{Observer}_j \in U_{LL}$). The HL input commands $\acute{I}$ for the system are the changes to resistance $\forall i : R_i \uparrow$, $R_i \downarrow \in \acute{I}$, while the LL observable outputs $\acute{O}$ are the voltage and current readings $V \uparrow$, $V \downarrow$, $I \uparrow$, $I \downarrow$ $\in \acute{O}$.

The system dynamics of the DC circuit model adequately reflect the actual system and, in terms of real power, can be extended to the power grid [2]. Due to their high cost, FACTS devices are deployed sparsely in a real network. Thus, the minimum number of observers required to fully deduce the system state can characterize the information security of the system. The analysis considers two topologies, series-connected and parallel-connected networks. Each topology has basic and extended network configurations.

This model considers the steady-state behavior of the system and assumes that only one $\acute{i}_i \in \acute{I}$ occurs at a given time. This input command can lead to several LL observable changes at different observation points. Thus, an execution σ in this case, consists of a single HL input action followed by the resulting LL observable events. Furthermore, it is also assumed that the LL observers have sufficient knowledge of the system and topology to derive the expected outcome for each HL input. The voltage source is assumed to be maintained constant throughout the analysis.

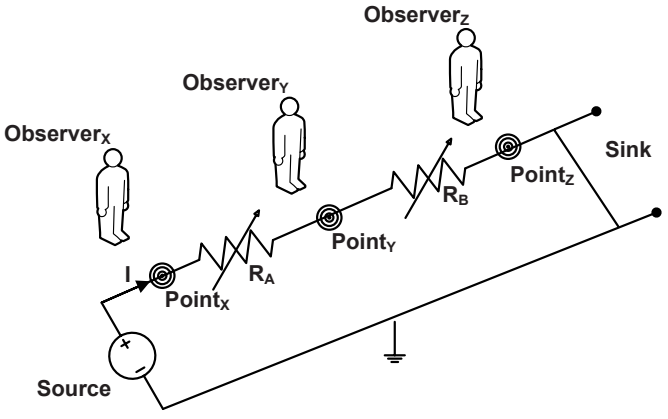


Figure 2. Two-resistor series-connected circuit.

5.1 Series-Connected Circuits

Figure 2 shows a two-resistor series-connected DC circuit with three observation points. Note that the resistors correspond to variable power electronic devices.

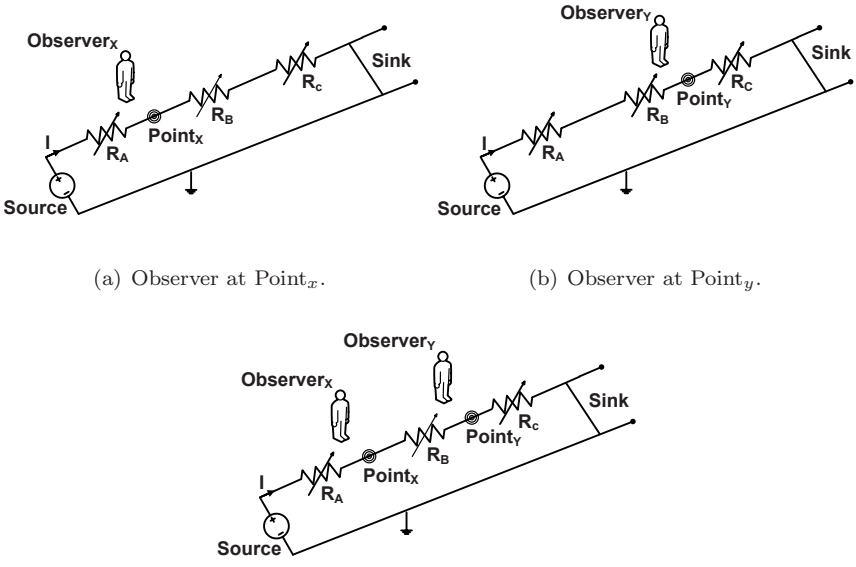
Table 1. Low-level observation matrix for a series-connected circuit.

	LL Observations			
HL	$\mathbf{V_y} \uparrow$	$\mathbf{V_y} \downarrow$	$\mathbf{I_y} \uparrow$	$\mathbf{I_y} \downarrow$
$R_A \uparrow$		$\surd$		$\surd$
$R_B \uparrow$		$\surd$		$\surd$
$R_A \downarrow$	$\surd$		$\surd$	
$R_B \downarrow$	$\surd$		$\surd$	

Table 1 presents the LL observation matrix for a two-resistor series circuit with one deducible observer. Note that $\acute{I} = \{R_A \uparrow, R_A \downarrow, R_B \uparrow, R_B \downarrow\}$ while $\acute{O} = \{I \uparrow, I \downarrow, V_y \uparrow, V_y \downarrow\}$. As a result, there are four legal executions $\sigma_k : 1 \leq k \leq 4$ corresponding to each HL input command. These are denoted as rows in Table 1. The first entry of each row denotes the corresponding trace, $trace(\sigma_k, q_0)$, for each execution σ_k. The remaining row entries correspond to projections.

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

Proof: Consider two executions $\sigma_1 = \{R_A \uparrow, V_y \downarrow, I_y \downarrow\}$ and $\sigma_2 = \{R_B \uparrow, V_y \downarrow, I_y \downarrow\}$. Without loss of generality, assume that Observer$_y$ in Figure 2 sees the projection $\{V_y \downarrow, I_y \downarrow\}$, which, according to Lemma 1, corresponds to



(a) Observer at Point$_x$.

(b) Observer at Point$_y$.

(c) Two observers.

Figure 3. Three-resistor series circuit with two deducible observers.

$f_1(\sigma) \equiv proj(U_{LL}, \sigma_1, q_0)$. The corresponding trace for σ_1 yields $R_A \uparrow$ where $f_2(\sigma) \equiv trace(\sigma_1, q_0)$. However, there exists another execution σ_2 with the same projection, $f_1(\bar{\sigma}) = \{V_y \downarrow, I_y \downarrow\}$, but with a different trace $f_2(\bar{\sigma}) = R_B \uparrow$.

For Observer$_y$ in Figure 2, the only distinct projections are $\{V_y \downarrow, I_y \downarrow\}$ and $\{V_y \uparrow, I_y \uparrow\}$. However, neither of them are unique projections because there is another execution for each case with the same projection but caused by a different trace (see Table 1). Thus, in Observer$_y$'s view, there are no unique LL projections, which preserves nondeducibility.

A "deducible observer" is an observer who can take multiple readings (e.g., voltage and current) that can be used to deduce HL information. Note that Observer$_x \in U_{LL}$ at the source and Observer$_z \in U_{LL}$ at the sink do not observe any voltage changes due to the nature of the layout. In contrast, Observer$_y \in U_{LL}$ can see voltage changes, albeit with multiple possibilities. Thus, Observer$_y$ is the only "deducible observer" in this network.

Figure 3 shows an extended series circuit, which is derived from Figure 2 by incorporating an additional resistor $R_C \in U_{HL}$. In the analysis that follows, only deducible observers are considered (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 the same circuit with a single deducible observer at Point$_y$. Table 2 summarizes the LL observations for the extended circuit.

Table 2. Observation matrix for an extended series circuit.

	LL Observations					
HL	$\mathbf{V_x}\uparrow$	$\mathbf{V_x}\downarrow$	$\mathbf{V_y}\uparrow$	$\mathbf{V_y}\downarrow$	$\mathbf{I}\uparrow$	$\mathbf{I}\downarrow$
$R_A\uparrow$		√		√		√
$R_B\uparrow$	√			√		√
$R_C\uparrow$	√		√			√
$R_A\downarrow$	√		√		√	
$R_B\downarrow$		√	√		√	
$R_C\downarrow$		√		√	√	

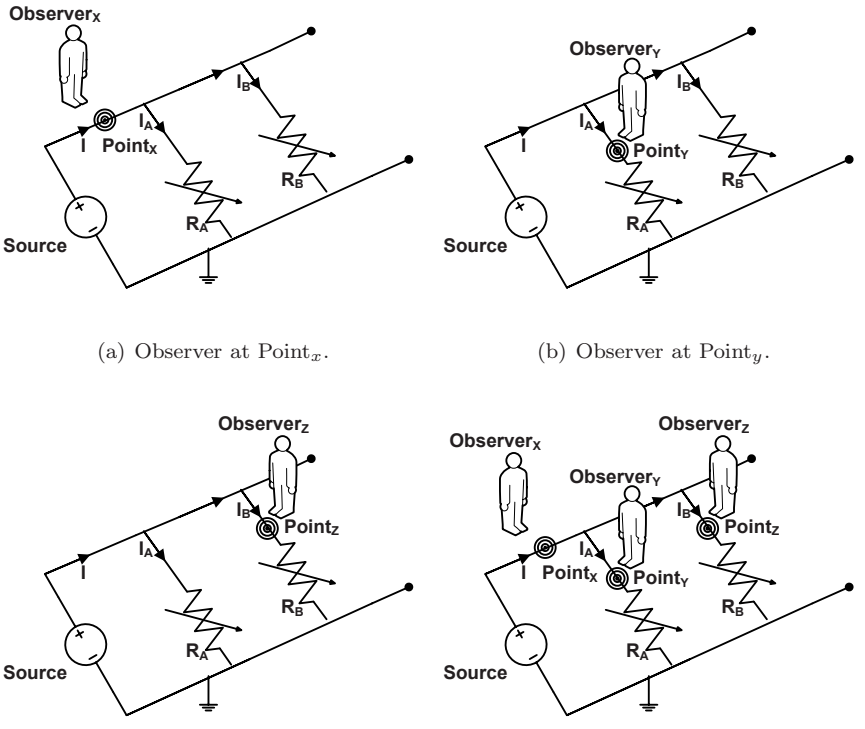
LEMMA 3 *A series circuit with $n \geq 3$ configurable units is fully deducible with a minimum of n distinct readings and n – 1 observers.*

Proof: To prove Lemma 3, it is sufficient to show that there is a violation of Lemma 1. From Table 2, consider the execution $\sigma = \{R_A\uparrow, V_x\downarrow, V_y\downarrow, I\downarrow\}$. By Lemma 1, for the Observer$_x$ and Observer$_y$ combination, the collective projection of σ is $f_1(\sigma) = \{V_x\downarrow, V_y\downarrow, I\downarrow\}$. According to Table 2, this is a unique projection that allows the observers to deduce $f_2(\sigma) = R_A\uparrow$. In fact, all the collective projections for this observer combination are unique. This, in turn, leads to full deducibility of all HL actions with two observers and three distinct readings.

For Observer$_x$ at Point$_x$, the projection $\{V_x\uparrow, I\downarrow\}$ is compatible with the traces $R_B\uparrow$ and $R_C\uparrow$. Similarly, the projection $\{V_x\downarrow, I\uparrow\}$ is compatible with the traces $R_B\downarrow$ and $R_C\downarrow$. By Lemma 1, the actions of R_B and R_C are nondeducible from Observer$_x$'s point of view. However, for the same observer, the projections $\{V_x\downarrow, I\downarrow\}$ and $\{V_x\uparrow, I\uparrow\}$ are unique corresponding to traces $R_A\uparrow$ and $R_A\downarrow$. Thus, whenever R_A makes an HL change, Observer$_x$ can deduce it exactly. In summary, Observer$_x$ is able to deduce R_A but not R_B or R_C. Similarly, it is not hard to see that Observer$_y$ at Point$_y$ in isolation (Figure 3(b)) can deduce the actions of R_C but not those of R_A or R_B (see Table 2). For this reason, the network is "partially deducible."

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

Note that multiple configurable units are located after Point$_x$ and only one configurable unit before Point$_x$. Given an observation point, configurable unit locations before and after the observation point are called "pre-locations" and "post-locations," respectively. Similarly, for Point$_y$, there are multiple pre-locations but only one post-location.



(a) Observer at Point$_x$.

(b) Observer at Point$_y$.

(c) Observer at Point$_z$.

(d) Three observers.

Figure 4. Parallel circuit with three observers.

5.2 Parallel-Connected Circuits

Figure 4 shows all the possible single observer scenarios for a two-resistor parallel-connected DC circuit with three deducible observers. It is not possible to observe any V changes at any of the "deducible points." However, Observer$_x$ at the source can be considered to be a deducible observer because the total current I branches into two currents I_A and I_B along the parallel links of the circuit. The corresponding LL observation matrix is presented in Table 3.

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

Proof: This network also violates the condition of Lemma 1. Consider the scenario of multiple cooperating observers shown in Figure 4(d). Without loss of generality, consider the execution $\sigma = \{R_A \uparrow, I_A \downarrow, I \downarrow\}$. By Lemma 1, $f_1(\sigma) = \{I_A \downarrow, I \downarrow\}$ and $f_2() = R_A \uparrow$ for the observer combination Observer$_x$ and Observer$_y$. From Table 3, it is clear that this projection is unique. This

Table 3. Observation matrix for a parallel circuit with three observers.

	LL Observations					
HL	$\mathbf{I_A} \uparrow$	$\mathbf{I_A} \downarrow$	$\mathbf{I_B} \uparrow$	$\mathbf{I_B} \downarrow$	$\mathbf{I} \uparrow$	$\mathbf{I} \downarrow$
$R_A \uparrow$		$\surd$				$\surd$
$R_B \uparrow$				$\surd$		$\surd$
$R_A \downarrow$	$\surd$				$\surd$	
$R_B \downarrow$			$\surd$		$\surd$	

allows the two collaborative observers to deduce the exact HL action ($R_A \uparrow$). Further examination of Table 3 reveals that this is true for all other executions of the network. In fact, any combination of two observers can deduce all the HL actions; thus, with just two observers, the entire network is deducible.

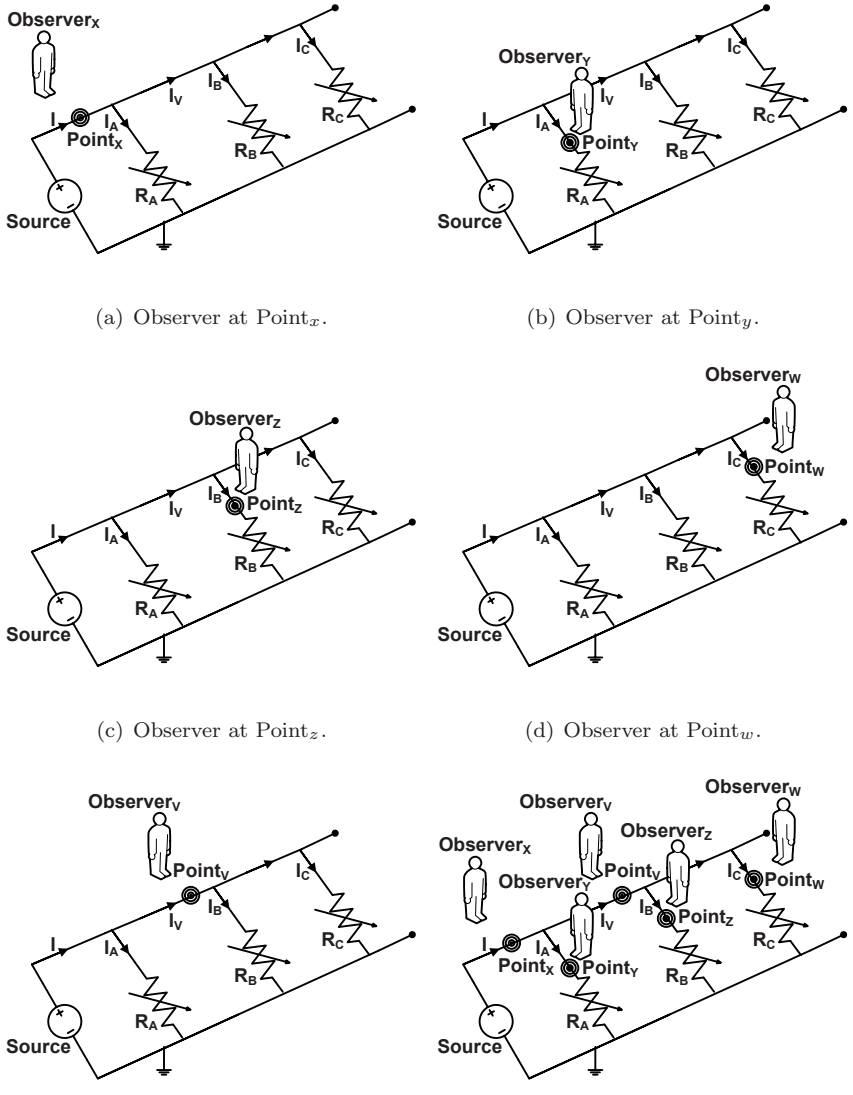
Note that a single deducible observer at Point_z (Figure 4(c)) cannot derive any information about R_A's actions. This is because there are no corresponding observations for traces $R_A \uparrow$ and $R_A \downarrow$ in the $I_B \uparrow$ and $I_B \downarrow$ columns in Table 3. However, for Observer_z, R_B's actions are deducible. Similarly, a single observer at Point_y cannot deduce anything about R_B's actions (see Figure 4(b)) but can deduce R_A's actions. As for Observer_x in Figure 4(a), $I \downarrow$ is consistent with either $R_A \uparrow$ or $R_B \uparrow$ whereas $I \uparrow$ is consistent with $R_A \downarrow$ and $R_B \downarrow$. Thus, a single observer is able to "partially deduce" the network.

Figure 5 shows a three-resistor parallel-connected DC circuit with five deducible observers. Table 4 shows the corresponding LL observation matrix.

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: To prove that only three observers are sufficient to fully deduce the network in Figure 5(f), we use Lemma 4 and consider one additional parallel path compared with Figure 4(d). However, not all combinations of three observers provide full deducibility. For example, an observer combination such as Observer_x, Observer_y and Observer_v cannot even notice the actions of R_B or R_C. For this observer combination, $\{I_V \downarrow, I \downarrow\}$ is a legal projection that is compatible with two traces $R_B \uparrow$ and $R_C \uparrow$. Thus, the placement of observers is also important.

There are two post-locations and one pre-location for Observer_v's view of the system. Interestingly, Observer_v cannot observe pre-location changes and any post-location change preserves nondeducibility. Similarly, Observer_x has three post-locations and, as the last two columns of Table 4 show, a single observable change is compatible with any of these post-locations. Furthermore, an observer along a parallel path can only observe changes in that particular path.



(a) Observer at Point$_x$.

(b) Observer at Point$_y$.

(c) Observer at Point$_z$.

(d) Observer at Point$_w$.

(e) Observer at Point$_v$.

(f) Five observers.

Figure 5. Parallel circuit with five observers.

6. Summary of Results

This section summarizes the results for DC circuits with series-connected and parallel-connected units.

Table 4. Observation matrix for a parallel circuit with five observers.

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

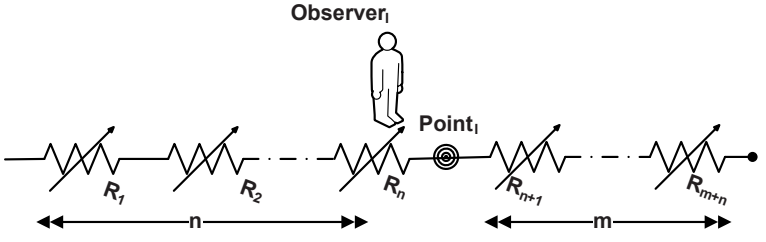


Figure 6. Series system with $n+m$ configurable units and one observer.

6.1 Circuits with Series-Connected Units

Figure 6 shows a pure series-connected system with Observer$_i$ at Point$_i$ with n pre-location paths and m post-location paths. Lemmas 2 and 3 can be used to prove the following theorem related to observability for 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 seen by an Observer$_i$ is consistent with a change α in one of the n pre-locations or a change β in one of the m post-locations with $\alpha = \bar{\beta}$.*

Proof: This theorem is proved using mathematical induction.
Base Case 1: 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 $V\uparrow$. Thus, the claim is true for the base case.
Base Case 2: 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, the claim is true for the base case.
Inductive Hypothesis: Assume that the claim holds for a system with $n+m$ resistors.
Inductive Step: If the observation point is moved by one location to the right, the system consists of $n+1$ pre-locations and $m-1$ post-locations. Since no

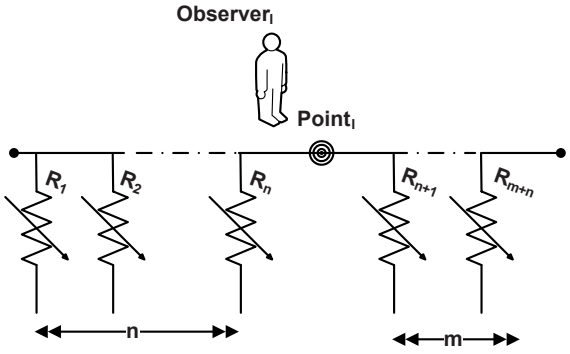


Figure 7. Parallel system with $n + m$ configurable units and one observer.

other parameter of the system is changed and the claim holds for the $n+m$ configuration, the claim holds for a system with $(n+1)+(m-1)$ configurable units.

6.2 Circuits with Parallel-Connected Units

Parallel-connected topologies are highly relevant to AC power distribution networks. These topologies can be modeled using pure parallel-connected configurable units in our DC model. Figure 7 shows a pure parallel-connected system with Observer$_i$ at Point$_i$ with n pre-location paths and m post-location paths.

- For a parallel-connected system with a single change at a time, an observation made by Observer$_i$ is consistent with m post-location path unit changes.
- For the same system, changes in any of the n pre-location 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$_i$.

Lemmas 4 and 5 can be used to prove the following theorem for parallel-connected networks. The proof, which is not presented here, employs mathematical induction.

THEOREM 2 *(Observability of Parallel Connected Configurable Units): For a pure parallel-connected system consisting of n pre-location paths and m post-location paths with respect to an Observer$_i$, a minimum of $m + n$ observers are required to fully deduce all HL actions. A combination of n pre-location deducible observers and $m-1$ post-location deducible observers must be selected in addition to Observer$_i$.*

7. Conclusions

This paper has attempted to provide a new perspective on information flow properties in systems with cyber-physical interactions. In particular, it has presented a detailed analysis of the minimum number of observers required to fully deduce HL actions in a CPS. Furthermore, a simplified definition of nondeducibility based on the uniqueness of LL projections has been presented. The results of the analysis lead to two corollaries related to the minimum number of "deducible observers" required to fully deduce a system.

COROLLARY 1 *To fully deduce all HL actions, a series-connected system with k configurable units requires a minimum of k distinct readings and k–1 deducible observers.*

COROLLARY 2 *To fully deduce a parallel system with k = n+m configurable units, an Observer$_i$ requires a minimum of n pre-location observers and m–1 post-location observers. Thus, including Observer$_i$, a minimum of k = n+(m–1)+1 observers are required.*

The observer-based view of the system can be considered as an LL domain view of the HL actions in a CPS. The focus of this paper has been on full deducibility of a CPS. However, certain HL actions are accurately deducible with fewer observers than identified above. For example, whenever Observer$_x$ in Table 2 sees $\{V_x \downarrow, I \downarrow\}$, he can deduce that $R_A \uparrow$ was the cause. This is termed as "partial deducibility."

Our future work will analyze the effect of multiple, simultaneous HL changes on nondeducibility. Also, it will investigate hybrid series/parallel networks with a variety of configurations.

Acknowledgments

This work was partially supported by NSF MRI Award CNS 0420869, CSR Award CCF-0614633 and the Missouri S&T Intelligent Systems Center.

References

[1] B. Alpern and F. Schneider, Defining liveness, *Information Processing Letters*, vol. 21(4), pp. 181–185, 1985.

[2] A. Armbruster, M. Gosnell, B. McMillin and M. Crow, Power transmission control using distributed max-flow, *Proceedings of the Twenty-Ninth International Conference on Computer Software and Applications*, vol. 1, pp. 256–263, 2005.

[3] K. Barnes and B. Johnson, Introduction to SCADA Protection and Vulnerabilities, Technical Report INEEL/EXT-04-01710, Idaho National Engineering and Environmental Laboratory, Idaho Falls, Idaho, 2004.

[4] D. Bell and L. LaPadula, Secure Computer Systems: Mathematical Foundations, MITRE Technical Report 2547, Volume I, The MITRE Corporation, Bedford, Massachusetts, 1973.

[5] R. Focardi and R. Gorrieri, Classification of security properties (Part I: Information flow), in *Foundations of Security Analysis and Design, Tutorial Lectures*, R. Focardi and R. Gorrieri (Eds.), Springer, Berlin-Heidelberg, Germany, pp. 331–396, 2001.

[6] J. Goguen and J. Meseguer, Security policies and security models, *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 11–22, 1982.

[7] J. McLean, A general theory of composition for a class of "possibilistic" properties, *IEEE Transactions on Software Engineering*, vol. 22(1), pp. 53–67, 1996.

[8] N. Nagatou and T. Watanabe, Run-time detection of covert channels, *Proceedings of the First International Conference on Availability, Reliability and Security*, pp. 577–584, 2006.

[9] C. O'Halloran, A calculus of information flow, *Proceedings of the First European Symposium on Research in Computer Security*, pp. 147–159, 1990.

[10] P. Pires and L. Oliveira, Security aspects of SCADA and corporate network interconnections: An overview, *Proceedings of the International Conference on the Dependability of Computer Systems*, pp. 127–134, 2006.

[11] D. Sutherland, A model of information, *Proceedings of the Ninth National Computer Security Conference*, pp. 175–183, 1986.

[12] H. Tang and B. McMillin, Security of information flow in the electric power grid, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 43–56, 2007.

[13] H. Tang and B. McMillin, Security property violation in CPS through timing, *Proceedings of the Twenty-Eighth International Conference on Distributed Computing Systems*, pp. 519–524, 2008.

[14] A. Zakinthinos and E. Lee, A general theory of security properties, *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 94–102, 1997.