01 Jul 2008

Security Property Violation in CPS Through Timing

Han Tang

Bruce M. McMillin
Missouri University of Science and Technology, ff@mst.edu

Recommended Citation

H. Tang and B. M. McMillin, "Security Property Violation in CPS Through Timing," *Proceedings of the 28th International Conference on Distributed Computing Systems Workshops, 2008*, Institute of Electrical and Electronics Engineers (IEEE), Jul 2008.
The definitive version is available at https://doi.org/10.1109/ICDCS.Workshops.2008.79

The 28th International Conference on Distributed Computing Systems Workshops

Security Property Violation in CPS through Timing

Han Tang * Bruce M. McMillin *
{ff@mst.edu}
Department of Computer Science
Intelligent Systems Center
Missouri University of Science and Technology, Rolla, MO 65409-0350

Abstract

Security in a Cyber-Physical System (CPS) is not well-understood. Interactions between components in the Cyber and Physical domains lead to unintended information flow. This paper makes use of formal information flow models to describe leakage in a model CPS, the Cooperating FACTS Power System. Results show that while a casual observer cannot ascertain confidential internal information, when application semantics, including timing, are considered, this confidentiality is lost. Model checking is used to verify the result. The significance of the paper is in showing an example of the complex interactions that occur between the Cyber and Physical domains and their impact on security.

1 INTRODUCTION

Cyber-Physical Systems (CPSs) are integrations of computation with physical processes. Embedded computers and networks monitor and control physical processes, usually with feedback loops, and physical processes affect computations and vice versa [12]. CPS applications include high confidence medical devices and systems, traffic control and safety, advanced automotive systems, process control, energy conservation, environmental control, avionics, instrumentation and critical infrastructure control systems (such as electric power, water resources, and communications systems).

Various issues in the study of CPSs need to be addressed including complex interactions of timing, frequency [19], security [21], and fault tolerance. This paper focuses on the security aspects of CPSs. Among the various security aspects of confidentiality, integrity and availability, this paper focuses on the confidentiality of CPSs, especially on information flow security. The physical nature of a CPS tends to expose information flow through actions at the *cyber-physical boundary*.

Many CPSs consist of similar elements. In the Cooperating FACTS Power System (CFPS), an intelligent controller communicates with other intelligent controllers and makes decisions via distributed decision making. In the CFPS, an intelligent controller sits on lines of an electric power system to balance the power flow of the entire power system. Throughout this paper the CFPS is used as the example to identify and model the information flow in a CPS. The CFPS serves as a real world example to show the applicability of the proposed process.

The family of Flexible AC Transmission System (FACTS) devices are power electronic-based controllers that can rapidly inject or absorb active and reactive power, thereby affecting power flow across transmission lines; a FACTS device changes the amount of power flowing on a particular power line. The use of FACTS devices in a power system can potentially overcome limitations of the present manually/mechanically controlled transmission system [3][6]. A FACTS Device consists of an embedded computer that depends on a low voltage control system for signal processing, which, in turn, depends on a low and a high voltage power conversion system for rapidly switching power into the power line. Each FACTS device controls the power flow on one power line (ControlledLine) and multiple FACTS devices interact with each other via exchanging messages over a network (Communication). The net effect of the FACTS devices and the power grid is that each power line and FACTS device is affected by other power lines and FACTS devices.

The Unified Power Flow Controller (UPFC) device is a type of FACTS device [6][18] that can modify active power flow on a power line. In this paper, the FACTS devices specifically refer to UPFC devices.

FACTS devices are primarily used to prevent cascading

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

1545-0678/08 $25.00 © 2008 IEEE
DOI 10.1109/ICDCS.Workshops.2008.79

failures in a power system; one or more lines are lost due to a downed line or overloaded line and the resulting redirected power flow stresses the network. Too much power may flow over lines of inadequate capacity and one-by-one the lines overload and trip out until a large portion of the power system has failed [6]. FACTS device coordination is required to prevent cascading failures [5][6]. The FACTS devices themselves communicate over an interconnected computing network to reach agreement on how power should be routed or re-routed in the presence of a failure (or contingency in the world of power systems). After reaching a decision, each FACTS device acts locally.

Distributed computing management of a power system is different from a traditional centralized power network management system; the FACTS devices, collectively, manipulate entire CFPS in a decentralized way, making distributed decisions to control the power system. New security issues emerge in this management scheme. In [18], a broad investigation into the operational and security challenges that the FACTS devices face has been discussed. The North American Electric Regulatory Corporation (NERC) provides a basis to define permanent cyber security standards [2]. These provide a cyber security framework (Standard CIP-002-1 to CIP-009-1) to identify and assist with the protection of critical cyber Assets to ensure reliable operation of the electric power system. Distributed management of the CFPS must protect the confidentiality of internal distributed decisions to that vulnerabilities to attack are reduced.

This paper identifies the vulnerability of information flow in a CPS from analyzing the example system's execution sequences. Several formal information flow properties are proven. The introduction of timing into the system divulges confidential decision making among the FACTS devices at the cyber/physical boundary.

2 BACKGROUND

2.1 INFORMATION FLOW SECURITY

A security model is used to describe any formal statement of a system's confidentiality, integrity and availability requirements [15]. Using information flow, principals can infer properties of objects from observing system behavior. This is a potential hazard in the Cyber-Physical world. To be more specific, inferring confidential information from the observable information flow is a potential source of critical information leakage; the information flow of CFPS needs to be carefully analyzed. Various security models that analyze multi-level security system behavior from the access control or execution sequence perspective have been discussed for decades to address the information flow problems of a system in the defense community. However, most of the related publications [14][16] have not been directly applied to CPSs. One of the reasons formal security models are less popular outside the defense area is due to the complexity. Two important models for this work are Nondeducibility and Bisimulation-Based NonDeducibility. Following typical notation, $\tau \in Tr$ are system traces,$\tau\backslash_x$ is a trace purged of all events in the domain of x, $\tau\,|_x$ is a trace restricted to all events in the domain of x, $E_1|E_2$ is the parallel composition of event E_1 and E_2, H, L are High-Level and Low-Level security domains with high-level and low-level user in each domain, and I, O are Inputs and Outputs.

2.1.1 Noninterference Model

A system is considered Noninterference secure if a low-level user's output does not depend on whether a high-level user is in the system [10]. $NI(ES) \equiv \forall \tau_L \in Tr : \tau\,|_L = \tau\backslash_H\,|_L$

2.1.2 Nondeducible Model

A system is considered Nondeducible secure if it is impossible for a low-level user, through observing visible events, to deduce anything about the sequence of inputs made by a high-level user. In other words, a system is Nondeducible secure if the low-level observation is compatible with any of the high-level inputs [14] [15] [16]. $ND(ES) \equiv \forall \tau_L, \tau_H \in Tr : \exists \tau \in Tr : \tau\,|_L = \tau_L \wedge \tau\,|_{H\cap I} = \tau_H$

2.1.3 Bisimulation-based Non-Deducibility on Composition Model

A system is considered to have the Bisimulation-based Non-Deducibility on Composition (BNDC) property, if it can preserve its security after composition [7]. A system ES is BNDC if for every high-level process P, a low-level user cannot distinguish ES from $(ES|P)\backslash H$ (ES composed with any other process P and purged high-level events). In other words, a system ES is BNDC if what a low-level user sees if the system is not modified by composing any high-level process P with ES. $BNDC(ES) \equiv \forall \pi \in E_H, ES/H \approx_B (ES|\pi)\backslash H$ where ES/H changes all the H events in ES into internal events.

3 INFORMATION FLOW IN A CYBER-PHYSICAL SYSTEM

Lack of confidentiality of information flow in a CPS can have catastrophic effects. As an example, consider an instance of the IEEE 118 bus electric power system [13][1]. This is a highly stressed system with many lines near overload. There are critical lines that, if removed, will cause cascading failures throughout the system. From the analysis in [13][1], if a critical line is removed, several succeeding lines trip one-by-one due to overload, leading eventually to

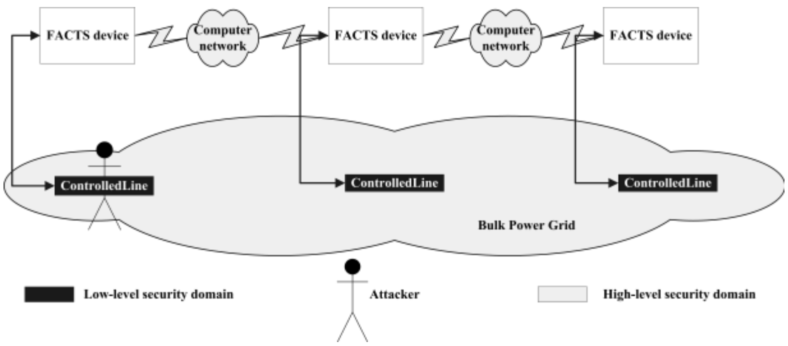

Figure 1. Architecture of CFPS

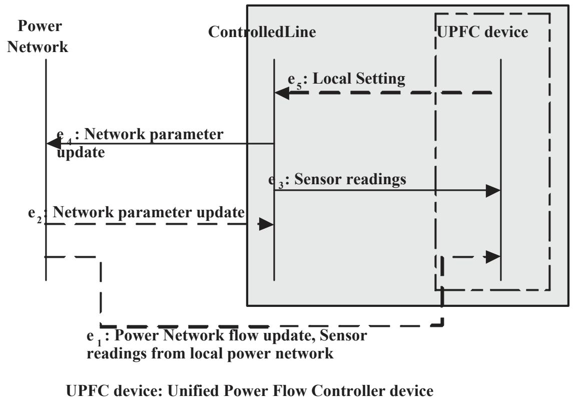
Power Network
ControlledLine
UPFC device
e5: Local Setting
e4: Network parameter update
e3: Sensor readings
e2: Network parameter update
e1: Power Network flow update, Sensor readings from local power network
UPFC device: Unified Power Flow Controller device

Figure 2. Information flow analysis at the UPFC device level

a cascading failure. If attackers know these critical lines together with a good guess of line capacity, they can carry out an effective attack causes a cascading failure of the system simply by physically removing a critical line. The confidential information leaked by information flow will assist or accelerate the attackers.

3.1 DEFINING INFORMATION FLOW IN CFPS

In a CFPS, decisions are made cooperatively and distributively. The decision making information is what needs to be kept confidential. The internal settings and control operations of a single UPFC or the interaction between multiple UPFCs are defined as confidential (in the High-Level domain) in [18].

Figure 1 shows the interaction between the UPFC and the power system. An attacker is shown in Figure 1 and can only read the power flow over the low-level object, ControlledLine, which is in the Low-Level domain. ControlledLine is inherently exposed due to the physical nature of its open access. The UPFC is a high-level object in the High-Level domain. Since the attacker usually will not be able to attack the UPFC itself due to physical protection such as those required by CIP-006-1, we force the system boundary to stop at ControlledLine.

Theorem 1, the system constructed of the UPFC device connected with ControlledLine is Nondeducible secure [21].

As shown in Figure 2, changes in power flow over ControlledLine can be affected by the local settings or by Network Parameter Updates that propagate. Even more, it could be affected by the topology change of power lines (such as a line trip), which triggers the redistribution of the power flow for the system. That is to say, by only observing the events interfering with the ControlledLine, no clue of where the information is from can be formed. From the interface model point of view, the system is secure such that no confidential information is exposed through information flow[1]

The remainder of this paper casts this model of the CFPS using the formal process algebra SPA.

3.1.1 SPA

Security Process Algebra (SPA, for short) [7] [9][11] is an extension of the Calculus of Communicating Systems (CCS) [17] - a language proposed to specify concurrent systems, that defines an algebra consisting of operators for building systems using a bottom-up approach from smaller subsystems. The basic building blocks are atomic activities, called actions; unlike CCS, in SPA, actions belong to two different levels of confidentiality, thus allowing the specification of multilevel (actually, two-level) systems. The BNF Syntax of SPA to describe the system is [9]:

$E ::= 0|\mu.E|E_1+E_2|E_1|E_2|E\backslash L|E\backslash_I L|E/L|E[f]|Z$

where 0 is the empty process, which does no action; $\mu.E$ does action μ and then behaves like E; E_1+E_2 can alternatively choose to behave like E_1 or E_2; $E_1|E_2$ is the parallel

[1] However, in Theorem 3 of [21] we show that an attacker, with semantic knowledge of power electronics, can deduce control settings by monitoring ControlledLine

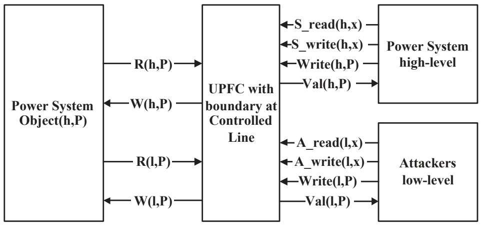

Figure 3. UPFC device security boundary at ControlledLine

composition of E_1 and E_2, where the executions of the two systems are interleaved, $E\backslash L$ can execute all the actions E is able to do, provided that they do not belong to $L\cup\bar{L}$ ($\bar{L}$ refer to the output); $E\backslash_I L$ requires that the actions of E do not belong to $L\cap I$; E/L turns all the actions in L into internal τ's; if E can execute action μ, then $E[f]$ performs $f(\mu)$; finally, Z does what E does, if $Z\equiv_{def} E$.

3.1.2 SPA Model for the UPFC at the ControlledLine boundary

The following model encodes the system of Theorem 1 in SPA.

```
$UPFC\_ControlledLine\_no\_time =$
    $(Behavior2|Object(0,P_{CL})|Object(1,Pinit))\backslash L$
$Behavior2 = M\_read(l,x)$
    $.if(l == x).then.$
        $r(x,y).val(l,y).Behavior2)$
    $else.Behavior2$
    $+M\_write(l,x)$
    $.if(l >= x).then.$
        $write(l,z).\bar{W}(x,z).Behavior2$
    $else.if(x == l).then.$
        $write(l,z).\bar{W}(1,z).Behavior2$
    $else.Behavior2$
$Object(x,y) = \bar{R}.Object(0,P) + W(x,y).Object(x,y)$
```

Here $M\_read(l,x)/M\_write(l,x)$ stand for events where the subject of security level l reads/writes to an object of security level x. y and z are the values (or states) of the object. The above SPA describes the system behavior and possible executions. The system behavior is shown in Figure 3.

3.1.3 SPA Model of the UPFC with timing constraints

In a Cyber-Physical system, security requirements are coupled with other kinds of requirements such as nonfunctional requirements, e.g. performance requirements. In the CFPS, the security requirement of information security has the potential of coupling with the real-time requirement of the system. However, the security models that are widely used do not always consider real-time or temporal behavior of the system. The analysis in the previous section, which uses the current available security models, cannot illustrate the possible security issues involving these temporal aspects.

Observe Figure 1; if the attacker passively attaches power flow meters to the low-level object ControlledLine and logs power flow data, the attacker could observe some significant changes of the power flow at certain time intervals and infer the system update rate. For example, the data given in Table 3.1.3 gives a glimpse of a line flow log. Here, the data are based on lab data which is aiming at testing the load change and the UPFC's response.

Table 1. Timestamped observation of ControlledLine

Time(ms)	Line flow (pu)
150000	-0.34248
150005	-0.3425
150010	-0.34254
...	-0.34252
...	-0.34252
...	...
190505	-0.42768
190510	-0.42064
190515	-0.41765
190520	-0.41056
...	
190610	-0.42059
190625	-0.41751
190630	-0.41038
190635	-0.40723
...	
190800	-0.42031
...	

From this trace, it can be seen that the attacker gathers the line flow information every 5ms. In other words, it has a sampling rate of 200Hz. Observing the change rate of the line flow, the attacker can infer that after a significant line flow change (at 190505ms), at least every 5ms, there is a change that causes the line flow to drop. However, around every 100ms, the line flow will be balanced back to a higher setting. Knowledgeable attackers could start a brief analysis of the CFPS based on acquired information:

- 190505 ms, some contingency happens (location not yet known) that causes the ControlledLine to have a flow change of around 20%
- At least every 5ms, the line flow drops by 2%, which means there is something withdrawing power flow from the ControlledLine at least every 5ms
- At least every 100ms, the line flow is changed by 6%,

which means there is some other mechanism injecting power flow to the ControlledLine at least every 100ms

With the above observation, the attacker obtains knowledge about the system response time of the UPFC, which is around 5-100ms.

The above analysis regarding the system's behavior, with temporal constraints taken into consideration, is based on our lab experience. A formal description needs to be given in order to use a model checking tool to prove the correctness of the security of information flow with timing considerations. Previous literature [8][11] has introduced ways of adapting time in the security model. Time is represented by a tick to describe the system's time in a discrete manner according to the global clock. (e.g. system = write. . .system), where internal events will always follow write events and take a unit of time. In the current approach, to include the temporal constraints in the SPA, the CFPS's behavior is chosen by extending the value passing SPA by one more value, the time interval. The line flow change observation is based on the information of ControlledLine, so we set the security boundary of the FACTS device to the ControlledLine.

$$UPFC\_ControlledLine_{time} =$$
$$\quad (Behavior2_t | Object(0, P_{int}, t) | Object(1, P_{int}, t)) \backslash L$$
$$Behavior2_{time} = M\_read(l, x, t)$$
$$\quad .(if(l == x).then.$$
$$\qquad R(x, y, t).val(l, y, t).Behavior2_{time})$$
$$\quad else.Behavior2_{time}$$
$$\quad + M\_write(l, x, t)$$
$$\quad .(if(l >= x)then$$
$$\qquad write(l, z, t).\bar{W}(x, z, t).Behavior2_{time}$$
$$\quad else.if(x == l)then$$
$$\qquad write(l, z, t).\bar{W}(1, z, t).Behavior2_{time}$$
$$\quad else.Behavior2_{time}$$
$$Object(x, P, t) = \bar{R}(x, P, t).Object(x, P, t)$$
$$+ W(x, P', t).Object(x, P', t)$$

Figure 4 shows the CFPS behavior with timing constraints. This formal expression of the system's execution sequence and the temporal constraints form the input to model checking. As seen from the informal analysis, the conclusion has been drawn that the real-time constraints do affect the security properties. In this case, the security requirement on information flow needs to be updated with the real-time constraints to reflect the situation.

4 RESULTS

The SPA models (without and with timing) were encoded into CoPS to check for BNDC. CoPS is an automatic checker of a multilevel system's security properties [4]. In order to include timing in the CoPS model, a special operation called "tick" is used. "Tick" does nothing but act as an atomic operation and represents the clock of the entire system moving by one unit of time. Figure 5 lists the timing constraints of the CFPS system. These can be translated into a corresponding number of tick operations in the CoPS model. The actual frequency ratio between the objects is 1000:330:1, however, in the CoPS model used a reduced number of ticks is used to reduce the complexity of model checking. The pattern of the frequencies is kept close to this ratio, but is not exact. Details of the CoPS model input are found in [20].

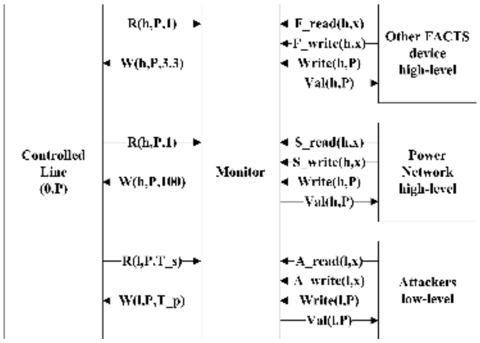

Figure 4. Behavior of FACTS considering timing constraints

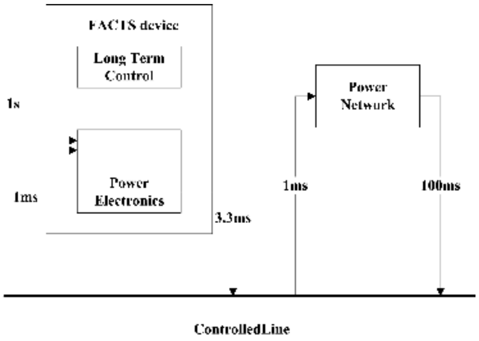

Figure 5. CFPS timing constraints and corresponding model to interpret the elapse of time

Table 2. Results of applying CoPS against UPFC models described by SPA

System	Satisfy BNDC	Number of States	Compo -sable
ControlledLine (Without Time)	Yes	36	Yes
ControlledLine (With time)	No	49	No

From the results listed in Table 2, conclusions can be drawn that for the security properties of UPFC system, without considering the timing constraints, the UPFC system satisfies BNDC. This is a stricter result than those stated in Theorem 1, since Section Theorem 1 only claims the UPFC system with the security boundary at ControlledLine, satisfies Nondeducibility. However, as stated in [14], some systems that satisfy the Nondeducible security property are not composable. This affects further consideration of the composed UPFC system with other systems to preserve security.

Conceptually, the system satisfies the BNDC because the internal events brought by LTC have been taken into consideration. These internal events lead to e_4. Being more specific, the event system shown in Figure 2, has been modified to allow e_4 to be a legal trace in the system by introducing the internal event τ. The system traces became $\{\{\}, \tau.e_4, e_1e_4, e_2e_4, e_1e_2e_4, \ldots\}$. This system satisfies BNDC since from the observation point of view, the observed result is compatible with any high-level input even when composed with other systems [9].

By contrast, the CFPS with timing constraints does not satisfy BNDC and is not composable. Intuitively, the failure to satisfy BNDC by adding timing information to the CFPS shows it is highly possible that timing constraints can be deduced or inferred by the observer. Timing is a common property in a CPS. It is something both trusted security domains and others can observe and forms an inherent vulnerability to confidentiality.

5 CONCLUSION

This paper illustrates the importance of information flow security in a CPS, provides a model of the information flow in a CPS, and formalizes the system and using automatic checking tools to prove security properties. BNDC is important as CPSs are usually more or less composed of various physical and cyber systems. However, the failure to satisfy BNDC under timing indicates that CPSs have inherent composability limitations. This paper's contribution is to bring information flow analysis to bear on understanding the security limitations of Cyber-Physical systems.

References

[1] *Missouri S&T FACTS Interaction Laboratory: http://filpower.umr.edu/.*

[2] *Standard CIP-002-1 through Standard CIP-009-1, ftp://www.nerc.com/pub/sys/all_updl/standards/sar/ Cyber_Security_Standards_Board_Approval_02May06.pdf.*

[3] IEEE Power Engineering Society FACTS Application Task Force, FACTS Applications. 1996.

[4] Cops. *http://www.dsi.unive.it/ mefisto/CoPS/index.php*, accessed October 30, 2007.

[5] A. Armbruster, M. Gosnell, B. McMillin, and M. Crow. Power Transmission Control Using Distributed Max-Flow. In *Procs of the 29th Annual IEEE International Computer Software and Applications Conference (COMPSAC)*, 2005.

[6] M. Crow, B. McMillin, and S. Atcitty. An Approach to Improving the Physical and Cyber Security of a Bulk Power System with FACTS. In *Electrical Energy Storage Applications and Technologies Conferences (EESAT)*, 2005.

[7] R. Focardi and et al. The compositional security checker: A tool for the verification of information flow security properties. *IEEE Transaction on Software Engineering*, 23(9), Sept. 1997.

[8] R. Focardi, R. Gorrieri, , and F. Martinelli. Real-time information flow analysis. *IEEE Journal on Selected Areas in Communications*, 21(1), Jan. 2003.

[9] R. Focardi and R. Gorrieri. A classification of security properties for process algebras. *Computer Security*, 3(1):5–33, 1994/1995.

[10] J. A. Goguen and J. Meseguer. Security Policies and Security Models. In *Proc. of the IEEE Symposium on Security and Privacy (SSP'82)*, pages 195–204. IEEE Computer Society Press, 2002.

[11] J. Huang and A. W. Roscoe. Extending noninterference properties to the timed world. In *Proceedings of the 2006 ACM Symposium on Applied Computing*. ACM Press,, April 23 - 27, 2006.

[12] E. A. Lee. Cyber-Physical Systems - Are Computing Foundations Adequate? In *Position Paper for NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*, October 16 - 17, 2006.

[13] A. Lininger, B. McMillin, M. Crow, and B. Chowdhury. Use of Max-Flow on FACTS devices. In *39th North American Power Symposium (NAPS 2007)*, pages 288–294, September 30 - October 2, 2007.

[14] D. McCullough. A hookup theorem for multilevel security. *IEEE Trans. on Software Engineering*, 1996.

[15] J. McLean. *Encyclopedia of Software Engineering - Security Models*. 1994.

[16] J. McLean. A general theory of composition for a class of 'possibilistic' security properties. *IEEE Transactions on Software Engineering*, 22(1):53–67, Jan. 1996.

[17] R. Milner. *Communication and Concurrency*. Prentice Hall, 1989.

[18] L. R. Phillips, M. Baca, J. Hills, J. Margulies, B. Tejani, B. Richardson, , and L. Weiland. *Analysis of Operations and Cyber Security Policies for a System of Cooperating Flexible Alternating Current Transmission System (FACTS) Devices*. Sandia National Laboratory, SAND-2005-7301, 2005.

[19] Y. Sun, B. McMillin, X. F. Liu, and D. Cape. Verifying Noninterference in a Cyber-Physical System: The Advanced Electric Power Grid. In *Proceedings of the Seventh International Conference on Quality Software (QSIC)*, pages 363–369, Portland, OR, October 2007.

[20] H. Tang. Security Analysis of a Cyber-Physical System. Master's thesis, University of Missouri-Rolla, August 2007.

[21] 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*, pages 43–56. Springer, 2008.