Chapter 4

SECURITY OF INFORMATION FLOW IN THE ELECTRIC POWER GRID

Han Tang and Bruce McMillin

Abstract The confidentiality of information in a system can be breached through unrestricted information flow. The formal properties of non-deducibility and non-inference are often used to assess information flow in purely cyber environments. However, in a "cyber-physical system" (CPS), i.e., a system with significant cyber and physical components, physical actions may allow confidential information to be deduced or inferred. This paper conducts an information flow analysis of a CPS using formal models of confidentiality. The specific CPS under study is the advanced electric power grid using cooperating flexible alternating current transmission system (FACTS) devices. FACTS devices exchange confidential information and use the information to produce physical actions on the electric power grid. This paper shows that even if the information flow satisfies certain security models, confidential information may still be deduced by observation or inference of a CPS at its cyber-physical boundary. The result is important because it helps assess the confidentiality of CPSs.

Keywords: Cyber-physical systems, power grid, information flow, confidentiality

1. Introduction

Major critical infrastructures such as the electric power grid, oil and gas pipelines, and transportation systems are cyber-physical systems (systems with significant cyber and physical assets) [5]. These infrastructures incorporate large-scale distributed control systems and multiple security domains. This paper focuses on the security analysis of the cooperating FACTS power system (CFPS), which is a representative cyber-physical system (CPS).

The CFPS consists of the electric power grid (generators, loads and transmission lines) and several flexible alternating current transmission system (FACTS) devices. These FACTS devices are power electronic flow control devices that stabilize and regulate power flow. Coordinated under distributed control, they

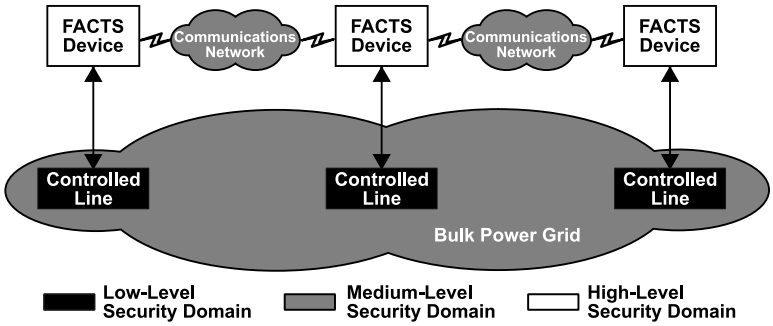

Figure 1. Cooperative FACTS power system (CFPS) network.

can be used to mitigate cascading failures such as those that occurred during the 2003 United States blackout (when a few critical lines downed due to natural causes resulted in cascading failures in the power grid).

Security is of paramount concern within a CFPS as malicious actions can cause improper operation leading to exactly the types of failures that the CFPS is designed to prevent. Confidentiality, integrity and availability are vital concerns in a CFPS. Much work has been done on ensuring integrity and availability, but relatively little on guaranteeing confidentiality. Information about the state of the power grid can divulge the locations of critical lines; a malicious action on one or more of these transmission lines can cause a cascading failure [3]. Thus, preventing the disclosure of information related to the state of the system is critical to reducing the vulnerability of the power grid.

This paper focuses on the confidentiality of CFPS information and its dependence on physical actions by FACTS devices. In particular, it analyzes the flow of information between CFPS components using several prominent security models [6–9, 14].

2. Background

Figure 1 presents a CFPS network with FACTS devices that cooperate by passing messages over a communications network. Each FACTS device controls the power flow on one line (controlled line) that is part of the bulk power grid. In this work we assume that the communications network is secure and that FACTS devices are secured using physical controls.

2.1 FACTS Devices and CFPS

FACTS devices are power-electronic-based controllers that can rapidly inject or absorb active and reactive power, thereby affecting power flow in transmission lines. A FACTS device (Figure 2) consists of an embedded computer that relies on a low voltage control system for signal processing. The embedded computer, which depends on low and high voltage power conversion systems for rapidly switching power into the power line, incorporates two software com-

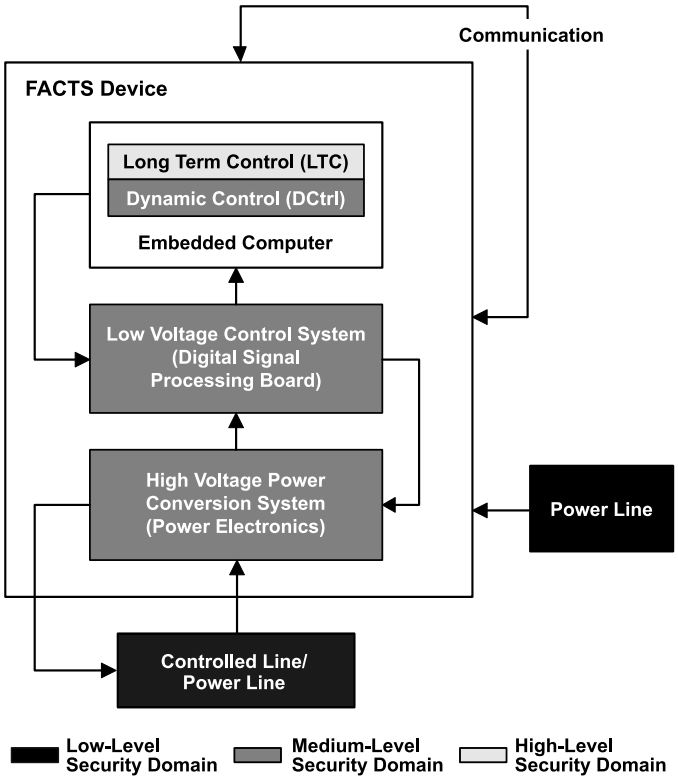

Figure 2. FACTS device.

ponents, the long term control (LTC) and the dynamic control (DCtrl) subsystems.

A FACTS device changes the amount of power flowing in a particular power line (controlled line). A unified power flow controller (UPFC) device [4, 11] is a FACTS device that can modify the active flow of power in a line. The FACTS devices considered in this paper are UPFC devices.

Coordination of multiple FACTS devices is crucial. When transmission lines are down (due to a naturally-occurring fault or a malicious attack), the remaining power flow overstresses the power grid. In such a situation, too much power may flow over lines of insufficient capacity. This causes the lines to overload and trip in a domino effect, resulting in a large-scale power outage [3]. The FACTS devices, in coordination, can stop this domino effect by rebalancing power flow in the grid by modifying the flow in a few key transmission lines [1].

FACTS devices operate autonomously, but they depend on information received from their participation in a CFPS to determine their response. The CFPS uses a distributed max-flow algorithm [1] for the LTC subsystem to rebalance power flow. The LTC runs on embedded computers located in different FACTS devices to compute a FACTS device setting that is communicated to

the dynamic control subsystem. The dynamic control subsystem sets the power electronics to enforce a particular power flow on the controlled line. Since power lines are interconnected, this has the effect of redistributing power flow over a regional or wider level within the power network. Each FACTS device continually monitors its own behavior in response to system changes and the responses of neighboring devices.

2.2 Related Work

The North American Electric Regulatory Commission (NERC) has spearheaded an effort to define cyber security standards [10]. The standards are intended to provide a framework for protecting critical cyber assets and ensuring that the electric power grid operates reliably. In particular, Standards CIP-002-1 through CIP-009-1 address security issues in the power grid.

Phillips and co-workers [11] have conducted a broad investigation of the operational and security challenges involving FACTS devices. Their analysis is based on best practices for supervisory control and data acquisition (SCADA) systems. Unlike SCADA systems, however, FACTS devices manipulate a CFPS in a decentralized manner so that new security issues emerge. While confidentiality, integrity and availability are discussed in the context of a CFPS, the problem of analyzing confidentiality in a CFPS is not considered. The research described in this paper builds on the work of Phillips and colleagues and engages various security models [6–9, 14] to provide a strong theoretical foundation for the analysis of confidentiality in a CFPS.

3. Problem Statement and Methodology

While the information flow between FACTS devices is secure, the confidentiality of information can still be compromised at the cyber-physical boundary by observing controlled lines in the bulk power grid. At some point, the settings of FACTS devices are exposed to the local power network via the actions of FACTS devices on physical power lines (controlled lines). This situation is not unique to a CFPS. Many critical infrastructure systems have similar elements: intelligent controllers that communicate with other controllers and make decisions using a distributed algorithm. The CFPS examined in this work is a model system, and the results developed here should be applicable to a wide range of cyber-physical systems.

3.1 Problem Statement

Decisions in a CFPS are made cooperatively. The analysis in [11] indicates that FACTS device settings and control operations are treated as confidential information. The results of the analysis are summarized in Table 1.

A CFPS has three security levels (Table 2). In the high-level security domain, a computer network is employed by the LTC for communications. In the medium-level security domain, the dynamic control and power electronics

Table 1. Confidential information in a CFPS (adapted from [11]).

Data	**Type**	**Source**	**Function**
Dynamic Control Feedback	Digital	Dynamic Control	Obtain and pass computed setpoint changes to prevent oscillations
Data Exchange with FACTS Neighbors	Analog and Digital (Ethernet)	Neighbor FACTS	Data needed to implement the distributed max-flow algorithm

Control	**Type**	**Source**	**Function**
Control Exchange with FACTS Neighbors	Digital (Ethernet)	Neighbor FACTS	Information needed for cooperative agreement on FACTS changes

Table 2. Security levels in a CFPS.

Security Level	**Security Entities**	**Reasons**
High-Level	Long Term Control, Parameters of the Entire CFPS	Contains critical information for the distributed control algorithm and computed settings with a global view of the power grid
Medium-Level	Dynamic Control, DSP Board, Power Electronics	Contains settings received from high-level entities and generates local settings according to local control algorithms
Low-Level	Controlled Line, Local Power Network	Open access to some power lines or information about a part of the power grid can be obtained

subsystems have implicit communications with other FACTS devices. In the low-level security domain, power line settings create implicit communications in the power network. Implicit communications occur when the power setting of a controlled line is changed and the power flow in the system is redistributed correspondingly. A confidentiality breach occurs when an observer in the low-level security domain can observe or deduce information in a higher-level security domain.

The following assumptions are adopted in our work:

- **Assumption 1:** Messages sent by the LTC subsystem are legitimate and correct. Note that LTC security is outside the scope of this paper.

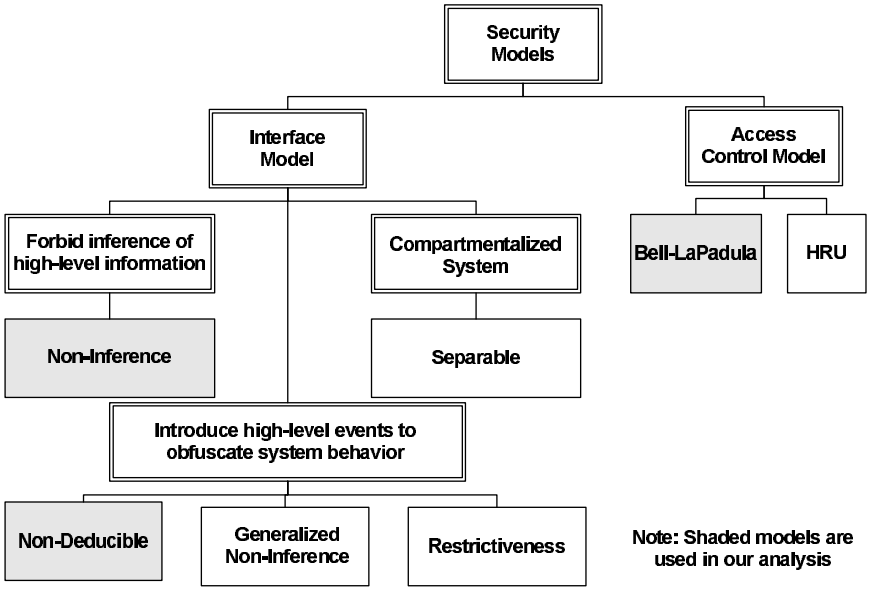

Figure 3. Partial taxonomy of the security models in [8].

- **Assumption 2:** The communications network used by the LTC subsystems to exchange max-flow algorithm messages is secure. In other words, communications between LTCs is secure.
- **Assumption 3:** The power flow information of the entire power network is secure, although some power lines can be measured and local topologies are observable.

Assumptions 1 and 2 define the scope of the problem addressed in this paper, which is to investigate the security of information flow in a CFPS. Assumption 3 provides the basis for our analysis, which is to determine the information that can be obtained through observation.

3.2 Methodology

The inference of confidential information from observable information flow raises serious security issues. Consequently, the information flow in a CFPS needs to be carefully analyzed.

Several security models have been proposed for analyzing the behavior of multi-level security systems from the access control or execution sequence perspectives [6–9, 14]. Figure 3 presents a taxonomy of security models. The models in the shaded boxes are considered in our work.

- **Non-Inference Model:** A system is considered secure if and only if for any legal trace of system events, the trace resulting from a legal trace that is purged of all high-level events is still a legal trace [8].

- **Non-Deducible Model:** A system is considered secure if it is impossible for a low-level user who observes visible events to deduce anything about the sequence of inputs made by a high-level user. In other words, a system is non-deducible if a low-level observation is not consistent with any of the high-level inputs [6, 8]. The term "consistent" means that low-level outputs could result from a high-level input.
- **Bell-LaPadula Model:** This access control model [2] specifies security rules that can be enforced during execution. All entities are either subjects or objects. Subjects are active entities and objects are passive containers of information. The model specifies the following rules for untrusted subjects:
  - Subjects may only read from objects with lower or equal security levels.
  - Subjects may only write to objects with greater or equal security levels.

A CFPS conforms with this multi-level security structure. The non-inference model applies to a CFPS because no low-level input results in high-level outputs. Similarly, the non-deducible model applies because high-level outputs are observable. If a system [6] is non-deducible, then a low-level user of the system will not learn any high-level information through the system. The Bell-LaPadula model is used to illustrate how breaches of confidentiality can occur using a perspective that is different from that employed by the two inference-based models.

4. CFPS Analysis

Security models can be used to identify where a CFPS may divulge information to a lower-level security domain. In our approach, information flow is first analyzed at the component level. Next, the components are combined to build a UPFC device, and information flow at the UPFC device level is analyzed to assess the security of the system.

4.1 Information Flow in UPFC Components

The principal components of a UPFC device include the LTC, dynamic control, digital signal processing (DSP) and power electronics subsystems (Figure 2). The information flow in a UPFC device is shown in Figure 4, where each component is considered to be a security entity. Figure 5 illustrates the information flow in the principal UPFC components using the pictorial notation for traces introduced in [6]. In the figure, the horizontal vectors represent system inputs and outputs. The broken lines and solid lines represent higher-level and lower-level events, respectively.

We now prove three lemmas regarding the components of a UPFC device. These lemmas are used to prove theorems about non-inference and other security properties of the composed system.

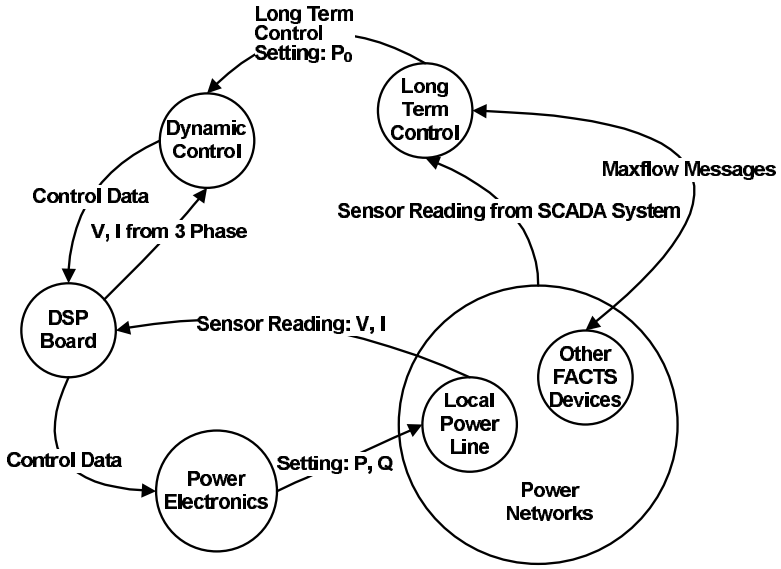

Figure 4. Information flow in a UPFC device.

Lemma 1: The DSP operation is non-inference secure.
Proof: As shown in Figure 5(a), the DSP board is a non-deterministic system, which is built up from traces of the form: $\{\{\}, e_1, e_3, e_4, e_1e_2, e_1e_3, e_1e_4, e_3e_4, e_1e_2e_3, e_1e_2e_4, e_1e_3e_4, e_1e_2e_3e_4, \ldots\}$, where e_1 is a low-level input (LI) event, e_2 is a high-level output (HO) event, e_3 is a high-level input (HI) event and e_4 is an HO event. Note that ... denotes interleavings of listed traces in the system. This system satisfies the definition of non-inference [8, 14] because by purging any legal trace of events not in the low-level security domain, the result is either e_1 or $\{\}$, which are both legal traces of the system. Thus, the DSP board itself is non-inference secure as information flow from the high-level security domain does not interfere with the low-level security domain.

Lemma 2: The dynamic control operation is non-inference secure.
Proof: The dynamic control subsystem is a non-deterministic system (see Figure 5(b)), which contains traces of the form: $\{\{\}, e_1, e_2, e_1e_3, e_1e_2, e_2e_3, e_1e_2e_3, \ldots\}$, where e_1 is an LI event, e_2 is an HI event and e_3 is an HO event. When a legal trace is projected to the low-level security domain or events that are not in the low-level security domain are purged, the result is either e_1 or $\{\}$, which are also legal traces. Therefore, the dynamic control subsystem satisfies the non-inference security model.

The LTC subsystem (see Figure 5(c)) is a non-deterministic system with only high-level events. It is obvious that there is no interference between the high-level security domain and the low-level security domain for the LTC. In other words, there is no information flow out of the high-level security domain.

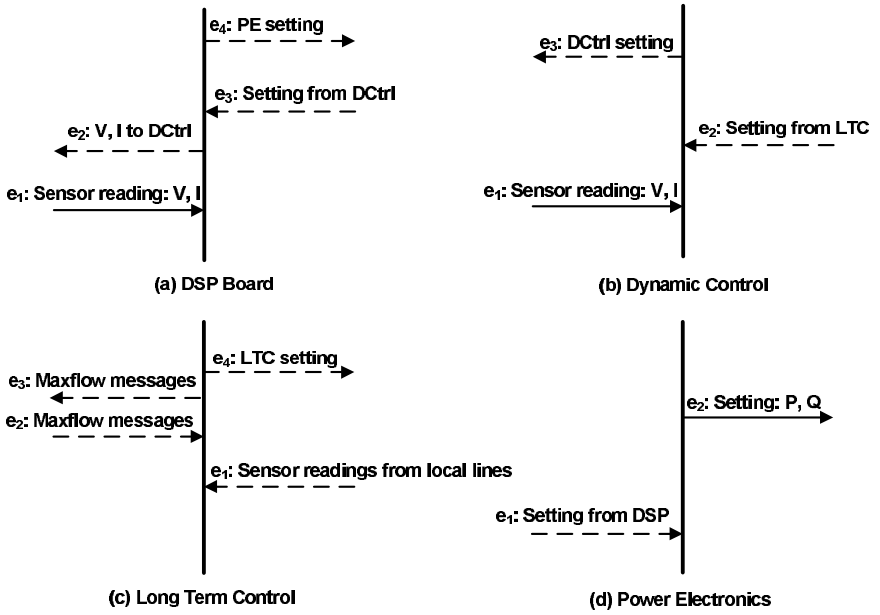

Figure 5. Information flow in UPFC components.

Lemma 3: The power electronics operation is not non-inference secure.
Proof: The power electronics system (see Figure 5(d)) contains the traces: $\{\{\}, e_1, e_1e_2, \ldots\}$. When any legal trace is projected to the low-level security domain, the result is either e_2 or $\{\}$, where e_2 is not a legal trace. Thus, the power electronics system is not non-inference secure. In this system, e_1 (HI) infers e_2 (LO), which means if e_2 occurs, e_1 must occur before e_2.

As a result of the causal relationship between e_1 and e_2, high-level information is downgraded and passed to the low-level security domain. The power electronics system is also not secure from the perspective of the Bell-LaPadula model [2] because high-level information is written to the low-level domain.

4.2 Information Flow in Composed Devices

This section analyzes information flow in a composed UPFC device. After the individual UPFC components are composed, information flows at the UPFC device level are either internal and external flows (Figure 6) or external flows only (Figure 7).

Theorem 1: The composition of the DSP, dynamic control, LTC and power electronics subsystems in a UPFC device is non-inference secure based on external events only.
Proof: From Lemmas 1 and 2, the DSP and dynamic control subsystems are non-inference secure. Connecting DSP and dynamic control subsystems to an

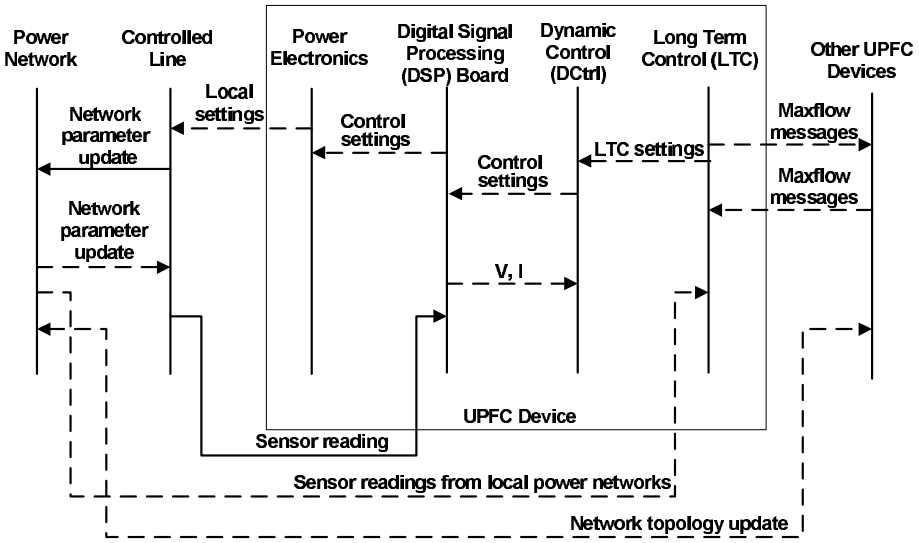

Figure 6. Information flow at the UPFC device level (internal and external flows).

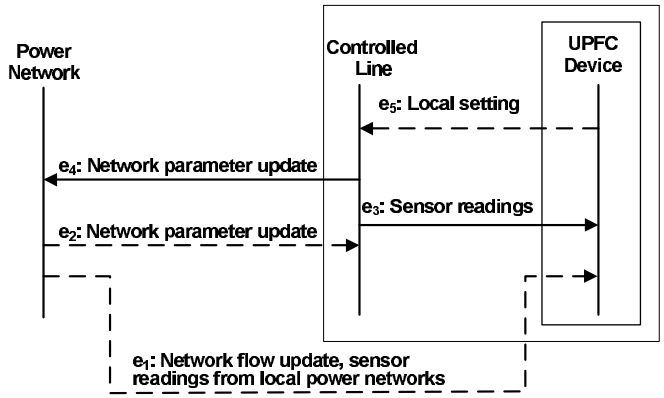

Figure 7. Information flow at the UPFC device level (external flow only).

LTC preserves the non-inference property. Upon examining Figure 7, we see that a UPFC device (considering only its external events) is a non-deterministic system containing the traces: $\{\{\}, e_1, e_3, e_5, e_1e_3, e_1e_5, e_3e_5, e_1e_3e_5, \ldots\}$. (Note that the composed system's boundary is at the UPFC device as shown in Figure 7.) The projection of these external event traces for a UPFC to the low-level domain is either $\{\}$ or e_3, which are both legal traces. This means that a UPFC device, considering only external events, is a non-inference secure system. Because a UPFC device is non-inference secure, an attacker cannot infer higher-level behavior simply by observing low-level events.

The non-inference property proved in Theorem 1 holds for a UPFC device itself but not when a controlled line is linked to a UPFC device. Since a UPFC device has physical protection as stipulated by Standard CIP-006-1 [10], the system boundary is forced to stop at the controlled line.

Theorem 2: The system consisting of a UPFC device connected to a controlled line is non-deducible secure.
Proof: Upon examining the events in the controlled line in Figure 6, we see that the system contains the traces: $\{\{\}, e_1e_4, e_2e_4, e_1e_2e_4, \ldots\}$, where e_4 is an LO event, and e_1 and e_2 are HI events. This system is not non-inference secure because the projection of a legal trace to the low-level domain ($\{e_4\}$) is not a legal trace. However, a system with a boundary at the controlled line is non-deducible secure [6, 8, 14] because every high-level input (either e_1 or e_2 or both) is compatible with the low-level output (e_4).

As shown in Figure 6, changes to a controlled line can be affected by: (i) local settings of the dynamic control subsystem, or (ii) other LTC settings that propagate through the power network, or (iii) topology changes of power lines (e.g., line trips), which trigger the redistribution of power flow in the system. Therefore, it is not possible to determine the source of the information only by observing events interfering with a controlled line.

The fact that a UPFC device (with a boundary at the controlled line) satisfies the non-deducible property is a very favorable result. Even when a UPFC device is constructed from components that are not secure (e.g., a power electronics device according to Lemma 3), the UPFC is still secure based on external information flow. In a real system, however, the controlled line is observable, and this introduces a new vulnerability.

4.3 Observation of Controlled Lines

Given the results of the previous section, the question is whether or not a UPFC device is really secure considering other types of inference. For example, can the UPFC settings be deduced by measuring the power flow in or out of the device? This is an important issue because many electric power network components are exposed and, therefore, can be physically accessed by an attacker. Consider a passive attack involving the use of meters to measure line voltages and current parameters. In such a situation, it is important to determine if the measured data could be used to compute control device settings in the bulk power grid, which could then be used to infer information about control operations. We use the computation model in Figure 8 to show that a passive attack using meters attached to a controlled line can be used to compute UPFC device settings.

Theorem 3: UPFC settings can be deduced by computation along with low-level observations.
Proof: In Figure 8, if two measurements of the three-phase instantaneous voltage and current information are taken at both sides of a UPFC device ($V_t\angle\theta_t$

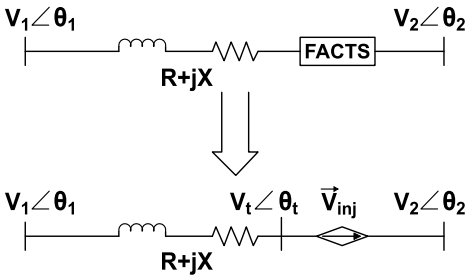

Figure 8. Computational model of a controlled line and FACTS devices.

and $V_2\angle\theta_2$) using Kirchhoff's law, the injected voltage V_{inj} can be computed. Since V_{inj} is known, the UPFC settings can be computed from the dynamic control subsystem. This means the local settings of the UPFC can be observed and high-level information is compromised despite the fact that the system satisfies the security properties related to information flow described in the previous sections.

5. Results

The analysis in Section 4 shows that the principal components of a UPFC device (DSP board, LTC and dynamic control subsystems) individually satisfy the non-inference property (Lemmas 1 and 2). However, according to Lemma 3, the power electronics subsystem permits the flow of information from a higher level to a lower level, which violates confidentiality from the perspective of the interface models. The power electronics subsystem also does not satisfy the "no write down" rule of the Bell-LaPadula model; therefore, the power electronics subsystem is not secure from the access control perspective as well.

The analysis also shows that, in terms of UPFC control operations, information flow is non-inference secure at the boundary of a UPFC device (Theorem 1) and non-deducible secure at the boundary of the controlled line considering only external events of a UPFC device (Theorem 2). This means a low-level observer can neither infer nor deduce any high-level or medium-level control messages by only observing the controlled line. Also, when a component that is not secure (e.g., power electronics subsystem) is composed with secure components (DSP board, LTC and dynamic control subsystems), the addition of other information flows yields a secure system. The events introduced by other secure components or by other systems that have the same or higher security levels obfuscate the system's behavior so that no high-level information can be inferred by observing only low-level information. In a CFPS, this obfuscation arises from the inherent physical characteristics of the power grid. In another words, a malicious attacker attempting to observe the changes to a controlled line cannot infer if the changes are caused by a new setting from the connected UPFC device or by neighboring UPFC devices or by the dynamics of the power network. However, Theorem 3 shows that UPFC settings could nevertheless be

deduced using mathematical computations along with low-level observations of the electric power grid.

6. Conclusions

The analysis of information flow in a CFPS from the component level to the UPFC device level verifies that UPFC control operations cannot be inferred by observing low-level CFPS behavior. However, UPFC settings can be deduced using mathematical computations along with low-level observations of a CFPS.

A CFPS with UPFC devices is a typical advanced distributed control system where the computations of the control devices are assumed to be protected. However, the actions of these devices on observable physical systems inherently expose their behavior at the lowest security level. This is a significant issue that should be considered when designing modern distributed control systems used in critical infrastructure components such as the power grid, oil and gas pipelines, vehicular transportation and air traffic control systems.

Our analysis of information flow assumes a non-deterministic system and ignores temporal considerations. However, timing issues such as those involved in interactions between the dynamic control and LTC subsystems can affect the information flow analysis. Although some research has been undertaken in this area (see. e.g., [13]), much more work needs to be done to analyze information flow in a CFPS based on temporal constraints.

Acknowledgements

This research was supported in part by the National Science Foundation under Grants CNS–0420869 and CCF–0614633, and by the Intelligent Systems Center at the University of Missouri at Rolla.

References

[1] 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.

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

[3] B. Chowdhury and S. Baravc, Creating cascading failure scenarios in interconnected power systems, *Proceedings of the IEEE Power Engineering Society General Meeting*, 2006.

[4] M. Crow, B. McMillin and S. Atcitty, An approach to improving the physical and cyber security of a bulk power system with FACTS, *Proceedings of the Electrical Energy Storage Applications and Technologies Conference*, 2005.

[5] E. Lee, Cyber-physical systems: Are computing foundations adequate? presented at the *NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*, 2006.

[6] D. McCullough, Hookup theorem for multilevel security, *IEEE Transactions on Software Engineering*, vol. 16(6), pp. 563–568, 1990.

[7] J. McLean, Security models and information flow, *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 180–189, 1990.

[8] J. McLean, Security models, in *Encyclopedia of Software Engineering*, J. Marciniak (Ed.), John Wiley, New York, pp. 1136–1144, 1994.

[9] 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.

[10] North American Electric Reliability Corporation, Reliability standards (Standard CIP-002-1 through Standard CIP-009-1), Princeton, New Jersey (www.nerc.com/∼filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection), 2007.

[11] L. 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, Technical Report SAND2005-730, Sandia National Laboratories, Albuquerque, New Mexico, 2005.

[12] M. Ryan, S. Markose, X. Liu, B. McMillin and Y. Cheng, Structured object-oriented co-analysis/co-design of hardware/software for the FACTS power system, *Proceedings of the Twenty-Ninth International Conference on Computer Software and Applications*, vol. 2, pp. 396–402, 2005.

[13] Y. Sun, X. Liu and B. McMillin, A methodology for structured object-oriented elicitation and analysis of temporal constraints in hardware/software co-analysis and co-design of real-time systems, *Proceedings of the Thirtieth International Conference on Computer Software and Applications*, pp. 281-290, 2006.

[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.