Analysis of the security of information flow in the Advanced Electric Power Grid using FACTS

Han (Carol) Tang and Bruce McMillin ({ht325,ff}@umr.edu)[†]
Department of Electrical and Computer Engineering and Department of Computer Science
Intelligent Systems Center
University of Missouri-Rolla
Rolla, MO 65409

ABSTRACT:

Confidentiality is a most significant and least understood security issue in cyber-physical systems. Many aspects of the system can jeopardize confidentiality. A great deal of research and effort is spent in integrity and confidentiality through authentication and encryption. However, even with the authentication mechanism working properly, the system's confidential information can be breached through unrestricted information flow or other implicit deducible information channels at the cyber-physical boundary. This paper conducts an information flow analysis using security models of confidentiality at different levels of the advanced electric power grid using cooperating FACTS devices. Taking only the FACTS device's settings and control operations as confidential information, even if the information flow satisfies certain security models, confidential information may still be deducible by observation or inference. The information flow analysis in this paper raises awareness that authentication itself is not enough to protect the confidentiality of a cyber-physical system. The analysis of the architecture of FACTS power system can be extended to many other cyber-physical systems.

KEY WORDS: Security, Critical Infrastructure, Information flow, Security Model

[†] Our prior work described in this paper was supported in part by NSF MRI award CNS-0420869 , CSR award CCF-0614633 and by the UMR Intelligent Systems Center

Analysis of the security of information flow in the Advanced Electric Power Grid using FACTS

ABSTRACT:

Confidentiality is a most significant and least understood security issue in cyber-physical systems. Many aspects of the system can jeopardize confidentiality. A great deal of research and effort is spent in integrity and confidentiality through authentication and encryption. However, even with the authentication mechanism working properly, the system's confidential information can be breached through unrestricted information flow or other implicit deducible information channels at the cyber-physical boundary. This paper conducts an information flow analysis using security models of confidentiality at different levels of the advanced electric power grid using cooperating FACTS devices. Taking only the FACTS device's settings and control operations as confidential information, even if the information flow satisfies certain security models, confidential information may still be deducible by observation or inference. The information flow analysis in this paper raises awareness that authentication itself is not enough to protect the confidentiality of a cyber-physical system. The analysis of the architecture of FACTS power system can be extended to many other cyber-physical systems.

KEY WORDS: Security, Critical Infrastructure, Information flow, Security Model

I INTRODUCTION

Security of critical infrastructures is of paramount importance. The vulnerability of critical infrastructures has been exhibited in the 9/11 terrorist attacks, the Katrina hurricanes, and the 2003 Midwest Blackout as well as other events. Such systems as the electric power transmission and distribution systems, air traffic control, oil/gas pipeline, or the transportation system, are network-centric [4] and control exists at multiple locations and involves multiple security domains. A specific system chosen as a model problem in this paper, representative of these network centric systems, is the Cooperating FACTS power system (CFPS). CFPS has been proposed as installing power electronic flow control FACTS devices on electric power transmission lines to stabilize and regulate power flow to mitigate cascading failures caused by topology changes (such as the 2003 blackout in which critical power lines were lost) or malicious attacks. Coordinating the actions of FACTS devices results in a cyber-physical system in which distributed computing forms a key part of the overall system. The assumption is that distributed decision making among the FACTS devices is confidential. While integrity and availability are vital concerns in operation of the electric power grid, this paper addresses confidentiality of the information used to make operational decisions.

The main contribution of this paper is to address the confidentiality of CFPS by analyzing the information flow of the different level of security entities in the system using security models[1] [6][7][8][9][10][14]. This is a complementary analysis to the traditional authentication approach to provide confidentiality; in a cyber-physical system, such as the CFPS, confidentiality can be compromised even with authentication in place. As shown in Fig. 1, which depicts FACTS device's cooperating message passing over a computer network, the communication in the computer network is secured and the FACTS device is physically secured and internal settings are confidential. However, the settings of the FACTS device are still exposed to the local power network via the actions of the FACTS device on the physical power line. Similar analogies can be made with oil/gas (observing flow in a pipe), aircraft control (observing a physical motion change), or transportation (such as a lane or speed change in an automated vehicle) systems.

The remaining of this paper is organized as: Section II contains background of the FACTS power system; Section III states the problem and the method to conduct the information flow analysis; Section IV is the FACTS power system's information analysis; Section V clarifies the results; Section VI re-emphases the significance of the problem.

[1] Security model is the formal statement of system's confidentiality, integrity and availability requirements. In this paper, the security models refer to confidentiality models only.

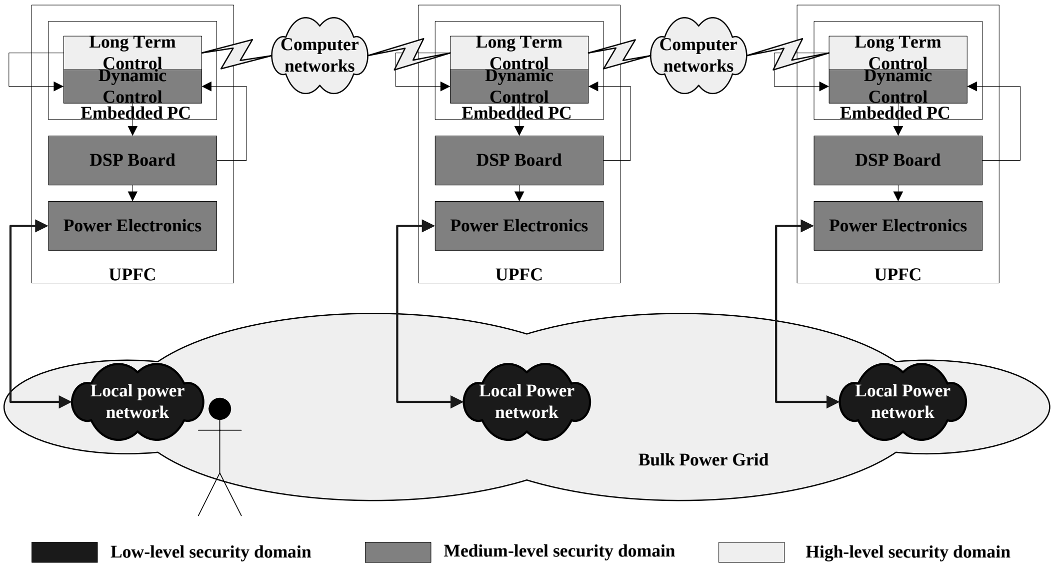


Fig. 1 The vulnerability of cooperative FACTS power networks

II Background

Many network-centric critical infrastructure systems consist of the same elements of a CFPS, an intelligent controller that communicates with other intelligent controllers and makes decisions via distributed decision making. The CFPS is chosen as a tangible model problem, but the results developed here will be applicable to a wide range of other cyber physical systems.

Background on FACTS devices and CFPS

The family of FACTS devices are power electronic-based controllers that can rapidly inject or absorb active and reactive power, thereby affecting the power flow across transmission lines. Put simply, 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. A FACTS device (depicted in Figure 2) consists of power electronics, a control structure, and an embedded computer with a network interconnection.

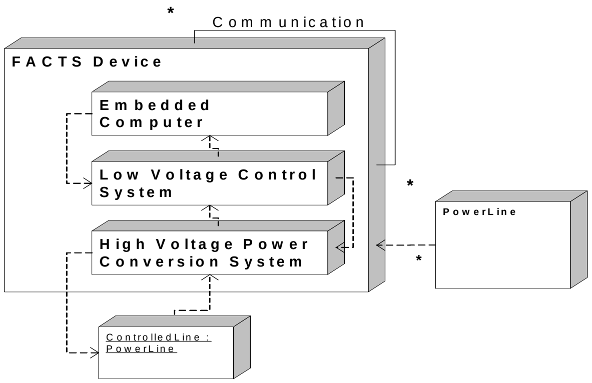

*
Communication
FACTS Device
Embedded Computer
Low Voltage Control System
High Voltage Power Conversion System
*
PowerLine
*
ControlledLine : PowerLine

Fig. 2. 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 one power line (Controlled Line) and multiple FACTS devices interact with each other via exchanging messages over 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 [3][5] that can modify active power flow on a power line. In the analysis of this paper, the FACTS devices refer to the UPFC devices and the power electronics and switch level control interactions are assumed to be those of UPFC devices.

FACTS devices are primarily used when a cascading failure occurs within a power system; one or more lines are lost due to a downed 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. FACTS device coordination is required to prevent cascading failures. 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 contingency. These Cooperating FACTS Devices (CFD) working together in the electric power network form the Cooperating FACTS Power System (CFPS). The FACTS devices behave autonomously, but they depend on information received from their participation in the CFPS to determine their responses.

The CFPS uses a distributed maxflow algorithm[1] to rebalance power flow, which is done in the Long Term Control (LTC), running on different processors that are located in different UPFC devices to compute the decision and manipulate the power network by sending the power settings to Dynamic Control. The Dynamic Control then sets the Power Electronics to enforce the local power flow to an expected value which redistributes power flow at a regional or wider level within the power network. The LTC and Dynamic Control both sit in the Embedded PC as a portion of a FACTS device (shown in Fig. 2). Each FACTS device must continually monitor not only its own behavior in response to system operating changes, but the response of neighboring devices as well. Time scales are seconds to minutes for the LTC and msec for the Dynamic Control.

RELATED WORK

Distributed computing management is different from a traditional centralized power network management system; the CFD manipulate the whole CFPS in a decentralized way, so that new security issues emerge. [5] provides a broad investigation in the operational and security challenges that the CFDs face. A general security analysis of FACTS has been given in the report which includes vulnerability of CFD and some available good practices based on those used for SCADA systems. An agent-based security framework has been suggested, while multiple levels of FACTS devices security issues and the confidentiality, integrity and availability of the electric power grid have been briefly analyzed. However, no approach has been proposed or any concrete example has been described, especially in the confidentiality of CFPS.

The North American Electric Regulatory Commission (NERC) provides a basis to define the permanent cyber security standards [12]. These provide a cyber security framework to identify and assist with the protection of Critical Cyber Assets to ensure reliable operation of the Bulk Electric System. Those requirements, stated in Standard CIP-002-1 – CIP-009-1, address various security issues and require approaches to provide security in the bulk power system. There is no requirement of information flow security, although some requirements of using authentication to achieve confidentiality in CIP-002-1 – CIP-009-1 are defined.

Besides practical work in the security of power systems as shown in [5][12], works on security theory such as security models[6][7][8][9][10][14] were help to provide the theoretic base of the analysis, we will discuss this in later section.

III PROBLEM STATEMENT AND METHODOLOGY

PROBLEM STATEMENT

In the CFPS, the decisions are made cooperatively and distributively. The decision making information is what needs to be kept as confidential. [5] defines the internal settings and control operations of single FACTS device or the CFDs as confidential. This paper will follow their definition of confidential information (as shown in Tab. 1) to analyze the information flow in the CFPS.

Tab. 1 Confidential information in CFPS (adapted from Tab. 2 in [4])

Data	**Type**	**Source**	**Function**
Dynamic Control Feedback	Digital	Dynamic Control	Obtain and pass computed setpoint changes to prevent oscillations
Data Exchange with CFD neighbors	Analog and Digital (Ethernet)	Neighbor CFD	Data necessary to implement distributed max flow algorithm
Control	**Type**	**Source**	**Function**
Control Exchange with CFD neighbors	Digital (Ethernet)	Neighbor CFD	Information necessary for cooperative agreement on CFD changes

The CFPS is made up of 3 security levels (shown in Tab. 2). In the high-level domain, communication is done by the LTC, in the medium-level domain, the Dynamic Control and Power Electronics have implicit communication with other FACTS devices. At the low-level security domain, the settings of the power line cause implicit communication in the power network. The implicit communication is done when the power setting of Controlled Line(s) is changed and the whole system's power flow redistributes correspondingly as shown in Fig. 1. This kind of communication is due to the interconnected nature of power networks. Failure of confidentiality in the system is defined as leakage of higher level (including the high-level and medium-level security domain) information such as internal settings and control operations being leaked to the low-level security domain.

Tab. 2 Security levels in Cooperating FACTS Power System

Security level	Security entities	Reason
High-level	LTC The parameters of whole CFPS	Contains critical information for decentralized control algorithm and calculated settings with a global view of the power grid
Medium-level	Dynamic Control DSP Power Electronics	Contains settings received from high-level security entity and will generate local settings according to local control algorithms
Low-level	Controlled Line Local power network	Easy to gain open access to certain power line or a part of the whole power grid

In order to demonstrate the problem clearly, following assumptions are made:

Assumption 1: This system’s LTC is protected by cryptography, authentication and other security mechanisms to guarantee its confidentiality, integrity and availability.

Assumption 2: The topology of entire power network is secure, although some single power lines can be measured or a local topology is observable.

Assumption 3: The communication network which the LTCs used to pass the maxflow algorithm messages is secure. In other words, the communication between LTCs located in different UPFC devices is considered to be secure.

METHODOLOGY

Inferring confidential information from the observable information flow is a potential source of critical information leakage; the information flow of CFPS need to be carefully analyzed. Various security models [8] that analyze multi-level security system behavior from the access control or execution sequence perspective has been discussed for decades to address the information flow problems of a system. However, most of the related publications [6][7][8][9][10][14] have not been directly applied to cyber-physical systems. Fig. 3 shows a partial taxonomy of the security models discussed in [8]. Those models in grey are what have been used in this paper to analyze the security of CFPS.

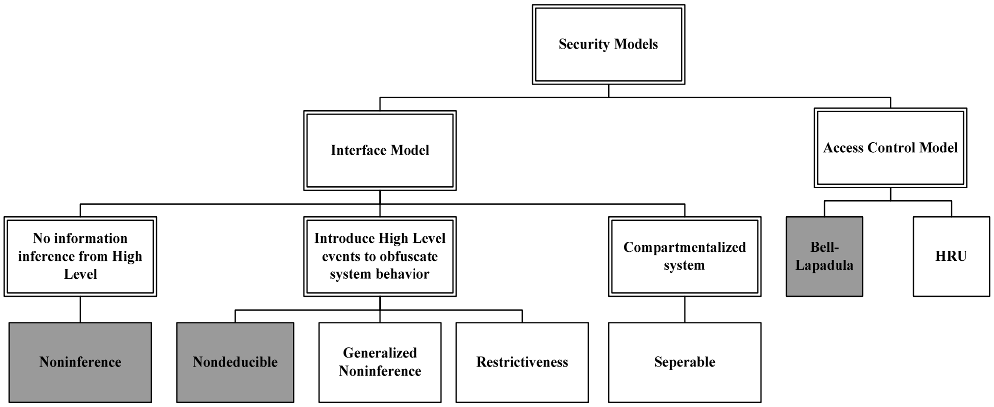


Fig. 3 Partial taxonomy of the security models in [8]

NONINFERENCE MODEL

A system is considered secure if and only if for any legal trace of system events, the trace results from the legal trace purged of all high-level events is still a legal trace of the system [8][10].

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, system is nondeducible secure if the low-level observation is compatible with any of the high-level inputs. [6][8]

BELL-LAPADULA MODEL

Different from the noninference and nondeducible security models, the Bell-Lapadula model is an access control model, which offers more tangible security rules that can be enforced during execution. In the Bell-Lapadula model [2], all entities are divided into subjects and objects. Subjects are active entities, while objects are passive containers for information. The Bell-Lapadula model set up rules for untrusted subjects:

- Untrusted subjects may only read from objects of lower or equal security level
- Untrusted process may only write to objects of greater or equal security level

APPLICABILITY

The CFPS system fits within this multi-level security structure. To analyze the information flow of CFPS more effectively, the security models defined above are used in this paper. The noninference model might be too strong in some systems where the low-level inputs result in high-level outputs. However, we apply the noninference model in our information flow analysis for the principle components of UPFC devices since no low-level input results in high-level outputs in those systems being analyzed. Nondeducible security models are used to analyze the system where high-level outputs are observable. According to [6], if an entire system is nondeducible secure, then no low-level user of that system will ever learn any high-level information through the system. The Bell-Lapadula model is used to illustrate how the vulnerabilities are introduced in other perspectives besides the interface models.

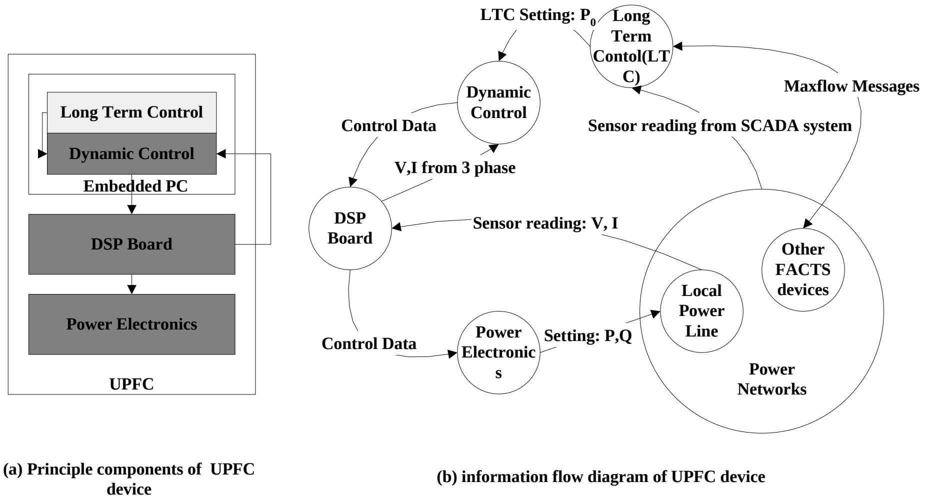
IV ANALYSIS OF CFPS USING SECURITY MODELS

We want to find the appropriate security models where the CFPS will divulge information to the low-level security domain. A bottom-up approach is used to analyze the information flow of CFPS. The CFPS is broken down to the level of single components which is used to build up UPFC device. After investigating the information flow of each component that used to build UPFC device separately, they are composed to build the UPFC device and the information flow is analyzed at this level.

INFORMATION FLOW OF THE COMPONENTS IN THE UPFC

Fig. 4(a) shows the principal components of a UPFC device which include the LTC, Dynamic Control, DSP board and Power Electronics. The information flow of a UPFC device is shown in Fig 4(b), where each component is considered as a security entity. Fig. 5 illustrates the information flow of the principle components building UPFC device

using the pictorial notation for the traces as introduced in [6]. Here, horizontal vectors represent inputs to and outputs from the system. The broken line represents the higher level events and the solid line represents the low-level events.



(a) Principle components of UPFC device

(b) information flow diagram of UPFC device

Fig. 4 Components of UPFC and Internal Information flow of UPFC devices

We now prove a series of lemmas regarding the components of the UPFC device. These are used to prove the property of noninference and other security properties of the composed system in later theorems.

DSP BOARD

Lemma 1, the DSP operation is noninference secure.

Proof: Seen from Fig.5(a), the DSP board is a non-deterministic system which is built up from traces of the following form:{{},e1,e3,e4,e1e2,e1e3,e1e4,e3e4, e1e2e3, e1e2e4,e1e3e4,e1e2e3e4, …} (… stands for any interleavings of listed traces in the system), where e1 is a Low-level Input (LI) event; e2 is a High-level Output (HO) event; e3 is a High-level Input (HI) event and e4 is a HO event. This system satisfies the definition of noninference [8][10][14] because purging any legal trace of events not in low-level security domain, the result will either be e1 or {} which are both legal traces of the system, i.e., DSP Board system itself is a noninference secure system where no information flows from the high level security domain interfere with (the interfere used in this paper refer to the property that events from domains other than the observer belongs to, that can be observed by the observer) the low level security domain. ■

DYNAMIC CONTROL

Lemma 2, the Dynamic Control operation is noninference secure.

Proof: the Dynamic Control system is a non-deterministic system, shown in Fig. 5(b), that contains traces of the following form: {{},e1,e2,e1e3,e1e2,e2e3,e1e2e3, …}, where e1 is a LI event, e2 is a HI event and e3 is a HO event. When we project any legal trace to the low-level security domain or purge any events that not in the low level security domain, the result will be either e1 or {}, which are also legal traces. Therefore, the Dynamic Control system satisfies the noninference security model. ■

LONG TERM CONTROL (LTC)

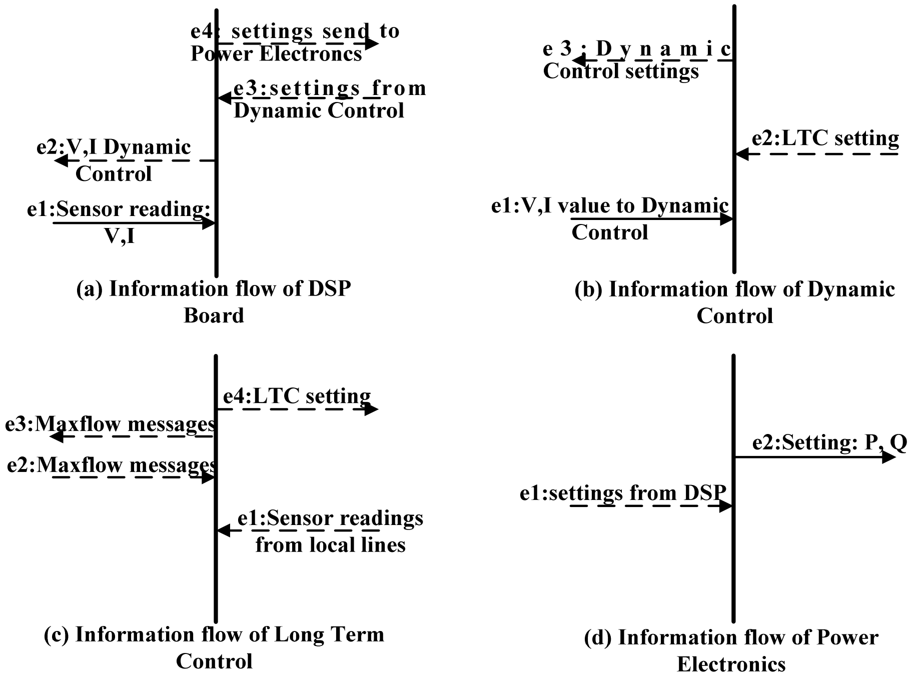
The LTC system, which is a non-deterministic system shown in Fig. 5(c), where all the events are high-level events. It's obvious that there is no interference between high-level security domain and the lower level security domain in LTC system. In other words, there is no information flow out of the high-level security domain. Proving this in the perspective of information flow is trivial.

POWER ELECTRONICS

Lemma 3, the Power Electronics operation is not noninference secure.

Proof: the Power Electronics event system, shown in Fig. 5(d), simply contains traces: {{}, e1, e1e2, …}. When we project any legal traces to the low-level security domain, the result will be either e2 or {}, where e2 is not a legal trace in this system. i.e., the power electronics system is not noninference secure. In this system e1(HI) infers e2(LO), which means if e2 happens e1 must happen before. ■

The causal relationship between e1 and e2 is where the information has been downgraded and passed to the lower security domain. This system is not secure not only in the perspective of interface models, but also in the view of access control models such as the Bell-Lapadula model [2] since there is information classified as higher level has been written to the low level domain, which violates the second rule of the Bell-Lapadula model.


e4: settings send to Power Electroncs
e3:settings from Dynamic Control
e2:V,I Dynamic Control
e1:Sensor reading: V,I
e 3 : D y n a m i c Control settings
e2:LTC setting
e1:V,I value to Dynamic Control
e4:LTC setting
e3:Maxflow messages
e2:Maxflow messages
e1:Sensor readings from local lines
e2:Setting: P, Q
e1:settings from DSP

(a) Information flow of DSP Board

(b) Information flow of Dynamic Control

(c) Information flow of Long Term Control

(d) Information flow of Power Electronics

Fig. 5 Information flow of principle components of UPFC

Information Flow of the Composition of Components into the UPFC

The UPFC device is able to work only when all those components mentioned above compose together and work properly. In this section, the composed UPFC devices will be discussed with and without considering the internal events respectively. After the components are composed to form the UPFC device, the information flows between components inside UPFC device are internal information flows (shown in Fig. 6) and others are externals (shown in Fig. 7).

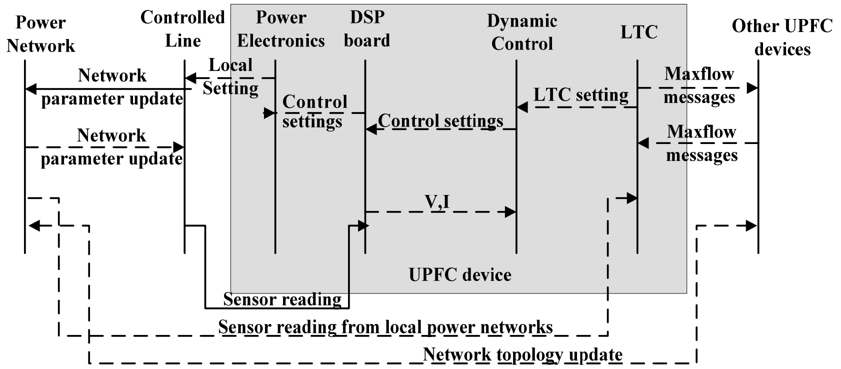


Fig. 6 Information flow analysis at UPFC device level – internal and external flow

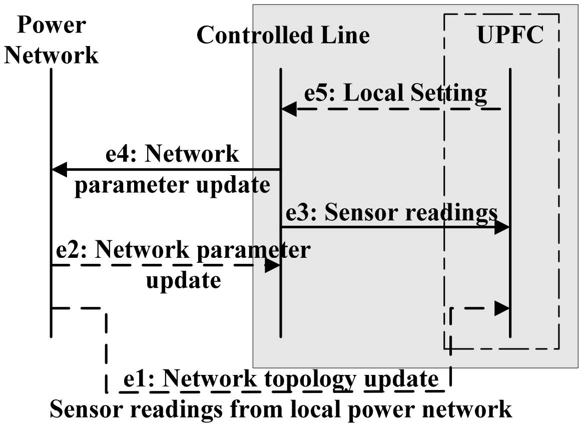

Power Network
Controlled Line
UPFC
e5: Local Setting
e4: Network parameter update
e3: Sensor readings
e2: Network parameter update
e1: Network topology update
Sensor readings from local power network

Fig. 7 Information flow analysis at UPFC device level – external flow only

Theorem 1, The composition of DSP, Dynamic Control, LTC and Power electronics forming the UPFC device is noninference secure considering the external events only.

Proof: From Lemma 1, 2, we can see the DSP and Dynamic Control are noninference secure. Connecting DSP and the Dynamic Control with the LTC, it is still noninference secure. The result of Lemma 3 does not invalidate the noninference secure property of these components composed with power electronics because: observing Fig 7 and taking the UPFC device without considering the internal events, it is a non-deterministic system that contains traces {{},e1,e3,e5, e1e3, e1e5,e3e5,e1e3e5, …} (The composed system's boundary is at UPFC device as shown in Fig. 7). The projection of these external events traces for the UPFC device to the low-level domain is either {} or e3 which are legal traces (the only observable low-level event – the sensor reading event can happen without the occurrence of any higher level events). That means the UPFC device, considering only the external events, is a noninference secure system. The UPFC device is noninference secure so that attackers cannot infer the higher level behavior simply from observing low-level events. ■

This noninference secure property proved in Theorem 1 is achieved without observation of power flow, in other words, the system boundary under consideration is the UPFC device itself but not the Controlled Line linked to the UPFC device. Since the attacker usually will not be able to attack the UPFC device itself due to the physical protection such as those required by CIP-006-1, we force the system boundary to stop at the Controlled Line. Unfortunately, due to the open nature of the physical power network system the Controlled Line is easier to attack.

Theorem 2, the system constructed of the UPFC device connected with the Controlled Line is not noninference secure but it is nondeducible secure.

Proof: Observing the event system at Controlled Line from Fig. 6, the system contains traces {{}, e1e4, e2e4, e1e2e4, …}, where e4 is LO event, both e1 and e2 are HI events. This system is not noninference secure because the projection of the legal trace to the low level domain ({e4}) is not a legal trace. However, the system with the boundary at the Controlled Line satisfies nondeducibility [6][8][14], because every high level input (either e1, e2 or both e1 and e2) are compatible with the low level output (e4). ■

To understand the nondeducibility better, the internal events of UPFC device need to be taken into consideration. As shown in Fig. 6, the changes of Controlled Line can be affected by the local settings from Dynamic Control (internal events) or they could be affected by the other LTC settings (internal events) that propagate through the power network, even more it could also be affected by the topology change of power line (such as line trip), which triggers the redistribution of the power flow for the system. That is to say, only by observing the events interfering with the Controlled Line, no clue of where the information is from can be formed.

That the UPFC device (with the boundary at Controlled Line) satisfies the nondeducible security model seems to be a very favorable result, even during building the UPFC devices, a component which is not secure (as from Lemma 3 where the Power Electronics downgrades the information to a low-level domain), the system is still secure considering the external information flow interference. From the interface model point of view, the system is secure such that no confidential information is exposed through information flow. In the real system, however, the Controlled Line is observable, and this introduces a new vulnerability.

VULNERABILITY OF UPFC VIA OBSERVATION OF CONTROLLED LINES

Given the results of previous section, is this system really secure considering other type of inference; by measuring power flow in or out of the UPFC device, can the high-level actions be deduced (inferred?) Due to the nature of the electric power network, its physical infrastructures are exposed outside and prone to be attacked easily. Take the UPFC device as an example and consider only passive attacks such as attaching meters to measure the line voltage and current parameters, it is possible that these measured data could help to calculate the settings from the control devices of the power system and infer the control operation accordingly. With a passive attack of using meters attached to the Controlled Line and with a reasonable amount of computation that the "settings" of UPFC devices can be calculated with the computation model shown in Fig. 8.

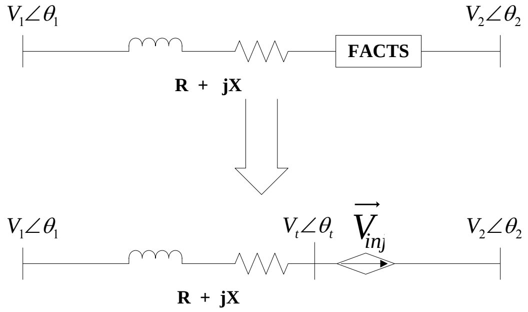


Fig. 8 Computation model of Controlled Line and the FACTS devices

Theorem 3, the UPFC settings can be deduced by computation with the low-level observation.

Proof: In Fig. 8, if take two measurement of three-phase instantaneous voltage and current information at both sides of the UPFC device ($V_t\angle\theta_t$ and $V_2\angle\theta_2$), using Kirchhoff's law, the injected voltage $\overrightarrow{V_{inj}}$ can be solved. The settings of UPFC from the Dynamic Control can be further calculated if $\overrightarrow{V_{inj}}$ is known. This means the local settings can be observed (compromised) even with the information flow analysis that we have done in previous paragraphs. ■

V RESULTS

From the analysis in Section IV, regarding the principle components of UPFC device as the LTC, Dynamic Control and DSP board all individually satisfy the noninference secure model from Lemma 1 and 2. However, Power Electronics, from Lemma 3, has information flow from higher level to low-level which violates confidentiality from the perspective of interface models. Using the Bell-Lapadula model to analyze the Power Electronics, the Power Electronics system fails to satisfy the second rule (no write down policy) of the Bell-Lapadula model. i.e., the Power Electronics is not secure considering the access control model as well.

The result of Section IV also shows the system information flow is noninference secure at the boundary of UPFC device itself (from Theorem 1) and nondeducible secure at the boundary of Controlled Line considering only external events of a UPFC device (from Theorem 2). This means the low-level observer cannot infer nor deduce any information from high-level operations. Also, a not-secure component (Power Electronics) composed with other secure components (LTC, Dynamic Control, DSP board) and/or adding other information flows turn out to be a secure system. This can be explained as the events introduced by other secured components or from other systems which have the same or higher security level obfuscates the system's behavior so that from a low-level observation, no information from the high-level can be inferred. In the CFPS, the obfuscation is brought by the inherited physical nature of power grid, which redistributes power flow through the entire network when there is power flow fluctuation. In another words, any malicious attackers trying to observe the changes of a Controlled Line, they will not be able to infer that the changes are caused by any new setting from the connected UPFC device or are caused by other neighboring UPFC devices or even caused by the dynamics from the power network. However, Section IV also shows that the UPFC settings still are compromised even if the Control of settings is kept secure. The information leak is due to the deducibility from mathematical computation (from Theorem 3).

VI CONCLUSION AND FUTURE WORK

CONCLUSION

This paper analyzed the information flow in the advanced power grid system with FACTS from the level of components that build up the UPFC devices to the level of UPFC devices. Under the Assumptions 1,2 and 3, the UPFC local setting is confidential if we only consider the interface security models, however, it can still be deduced by mathematical computation with enough measurements taken from the Controlled Line(s). Meanwhile, the UPFC control operations such as the Dynamic Control control operation and LTC control operation can not be inferred from observing the low level behavior of CFPS. This is a promising result that shows considering the information flow of the CFPS, the confidentiality of the UPFC data setting and the control operations are not broken by inference or deducing information from information flows. This kind of self-obfuscation ability, which the internal events of certain system can obfuscate the system's behavior so that the external observer will not be able to deduce information from the system, not only appears in the power system but also appears in other critical infrastructure as oil pipeline systems, air traffic control systems and transportation systems.

SIGNIFICANCE

The CFPS using UPFC device is typical of advanced controls that cooperate via distributed computation, where the computation is assumed to be protected, and these devices inherently expose their actions to the public (the lowest security level) by their very actions on the physical system. This is a significant design point in analyzing the security of modern distributed control systems and has extensions to the pipeline industry, air traffic control.

FUTURE WORK

Current analysis of information flow is based on a non-deterministic system with no temporal constraints. However, temporal constraints like the Dynamic Control update rate, Long Term Control update rate and the propagation delay of cooperating FACTS settings will also affect the information flow analysis. Although some temporal constraints have been analyzed for other purpose in the CFPS [13], more work needs to be done to analyze the information flows of CFPS under the temporal constraints.

REFERENCES

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

[2] Bell, D. E. and LaPadula, L. J., "Secure Computer Systems: Mathematical Foundations," MITRE Corporation, 1973

[3] Crow, M., McMillin, B., and Atcitty, S., "An Approach to Improving the Physical and Cyber Security of a Bulk Power System with FACTS," *EESAT Conferences 2005,* http://www.sandia.gov/ess/Publications/pubs.html

[4] IEEE Power Engineering Society FACTS Application Task Force, FACTS Applications, IEEE Publication 96 TP116-0, 1996.

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

[6] McCullough, D., "A hookup Theorem for Multilevel Security," *IEEE Trans. on Software Engineering* 1990

[7] McLean, J., "Security Models and Information Flow," *Procs. of the 1990 IEEE Computer Society Press*, 1990a.

[8] McLean, J., "Security Models," *Encyclopedia of Software Engineering*, 1994

[9] McLean, J., "A general theory of composition for a class of 'possibilistic' security properties," *IEEE Trans. on Software Engineering*, 22(1):53--67, January 1996.

[10] O'Halloran, C., "A calculus of information flow," *Proc. European Symp. Research in Computer Security*, Toulouse, France, 1990

[11] Ryan, M., Markose, S., Liu, X. F. ,McMillin, B. and Cheng, Y., "Structured Object-Oriented Co-Analysis/Co-Design of Hardware/Software for the FACTS Power System," *Procs. of the 29th Annual IEEE International Computer Software and Applications Conference (COMPSAC)*, Edinburgh, Scotland, July 2005

[12] 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

[13] Sun, Y., Liu, X. F. and McMillin, B., "A Methodology for Structured Object-Oriented Elicitation and Analysis of Temporal Constraints in Hardware/Software Co-analysis and Co-design of Real-Time Systems," *Procs. of the 30th Annual IEEE International Conference on Computer Software and Applications (COMPSAC)*, Chicago, Sept. 2006.

[14] Zakinthinos, A. and Lee,E.S., "A General Theory of Security Properties," *Procs. of the 18th IEEE Computer Society Symposium on Research in Security and Privacy*, 1997