Data extraction form

Cyber-Physical Systems Security

Version 0.9

Yuriy Zacchia Lun ⋆
Alessandro D'Innocenzo ⋄
Ivano Malavolta ⋆
Maria Domenica Di Benedetto ⋄

⋄ **University of L'Aquila**
Via Giovanni Di Vincenzo 16/B - 67100 L'Aquila - Italy

⋆ **GSSI Gran Sasso Science Institute**
Viale Francesco Crispi, 7 - 67100 L'Aquila - Italy

DATA EXTRACTION FORM

Cyber-Physical Systems Security

VERSION 0.9, OCTOBER 15, 2015

ABSTRACT

This document describes the parameters of the data extraction activity of a systematic mapping study on cyber-physical systems (CPS) security.

DOCUMENT VERSION CONTROL

Document status	**Version #**	**Date**	**Changes from previous version**
Draft	0.9	October 15, 2015	None

Contents

List of Figures

List of Tables

Abbreviation	Category
STUDY-ID	Study identification
TREND	Publication trends (RQ1)
SEARCH	Search strategy
WHAT	Approach positioning: ”WHAT” (RQ2)
HOW	Approach characterization: ”HOW” (RQ2)
VALID	Approach quality: validation strategies (RQ3)

Table 1: Categories for classifying method or techniques for CPS security

Parameter name	Type	Category	Description
Global identifier	*Int*	STUDY-ID	Unique identifier of the study across all the primary studies.
Internal ID	*Int*	STUDY-ID	Unique identifier of the study across all the potentially relevant studies.
Bibtex identifier	*String*	STUDY-ID	The bibtex identifier used in other reports of this study.
Title	*String*	TREND	Title of the primary study.
Authors	*Comma-separated string*	TREND	List of the authors of the primary study.
Institutions	*Comma-separated string*	TREND	List of the institutions of the primary study (as defined in the article itself).
Countries	*Comma-separated string*	TREND	List of the countries of the institutions of the primary study (as defined in the article itself).
Publication venue	*String*	TREND	The venue in which the study has been published (as defined in the bibtex entry provided by the publisher of the study).
Volume	*Int* or *PP* (for pre-prints)	TREND	The volume in which the study has been published (as defined in the bibtex entry provided by the publisher of the study).
Number	*Int*	TREND	The number of the volume in which the study has been published (as defined in the bibtex entry provided by the publisher of the study).
Month	*String*	TREND	The month in which the study has been published (as defined in the bibtex entry provided by the publisher of the study).
Pages	{*Int*, *Int*}	TREND	The range of pages of the volume in which the study has been published (as defined in the bibtex entry provided by the publisher of the study).
Year	*Int*	TREND	The year of publication of the study.
Publisher	*String*	TREND	The publisher of the study (e.g., IEEE, ACM, etc.).
Year of first appearance	*Int*	TREND	The year of publication of the earliest paper, when a primary study is published in more than one paper.

Parameter name	**Type**	**Category**	**Description**
Publication type	*Set* {*journal, book chapter, workshop, conference*}	TREND	The type of publication venue in which the study has been published.
Research type	*Set*, see Table 3 \ {*Opinion papers, Philosophical papers, Experience papers*}	TREND	Since this facet is general and independent from a specific research area, we reuse the classification of research approaches proposed by Wieringa et al. [3]. We chose this classification because (i) it has been widely used in various systematic mapping studies (e.g., in [4–6]), and (ii) its categories are quite cost-effective to be identified by reading a paper without going into its very details [1]. Table 4 presents a decision table to disambiguate the classification of studies [2]. It worth noting that due to inclusion and exclusion criteria for the primary studies, the *philosophical papers*, *opinion papers* and *experience papers* will never appear.
Source	*Set*, see Table 5 ∪ {*Other*}	SEARCH	The name of the electronic database from which the study has been searched, *other* if the study is coming from an electronic database not included in Table 5.
Search method	*Set* {*automatic, snowballing*}	SEARCH	The search method that the researcher used for obtaining the study.
Main study ID	*String*	SEARCH	A pointer to the Bibtex identifier of another paper counted as a primary study for this publication. This attribute is used only when a primary study is published in more than one paper. For example, if a conference paper is extended to a journal version, only one instance is counted as a primary study, because multiple publications of the same data in data synthesis would seriously bias any results [7].
Application field	*Set*, see Table 9	WHAT	The application field where the proposed approach has been adapted.
Point of view	*Set* {*Attack, Defence*}	WHAT	Indicates whether the study treats approaches for the CPS security breaching (i.e. *attack*) or enforcing via some kind of countermeasures (i.e. *defence*), or both.
Security attribute	*Set* {*Availability , Integrity, Confidentiality*}	WHAT	The primary security attribute [8] tackled by the proposed approach.
System component	*Set* {*Controllers, Sensors, Network, Actuators, Plant*}	WHAT	The cyber-physical system's components considered by an approach.

Parameter name	Type	Category	Description
Plant model	*Set*, see Table 6	WHAT	Mathematical models allow us to reason about a system and make predictions about how a system will behave [9]. The input/output dynamic behaviour is generally described by ordinary differential or/and difference equations.
State estimator	*Set*, see Table 7 $\cup$ {*Novel, Not available*}	WHAT	The concept of state means capturing information about the operation of a system in a set of variables [10]. For many situations, it is highly unrealistic to assume that all the states are measured. In that case, the state can be estimated by using a mathematical model and a few measurements [9].
Anomaly detector	*Set* {*Arbitrary, Performance index test, Largest normalised residual test, CUSUM-type, Novel*} $\cup$ {*Not available*}	WHAT	The bad data detection and (possibly) identification scheme considered by an approach, or *not available*, when there is no such scheme. In power system's community the *performance index test* [11] is also known as $J(\hat{x})$*-test* or χ^2*-test*, and the *largest normalized residual test* is often referred as r^N_{max}*-test* [12].
Controller	*Set*, see Table 8 $\cup$ {*Novel, Not available*}	WHAT	A feedback controller may be viewed as a signal processor that processes the sensor outputs and returns the actuator inputs. Within a broader perspective, a controller can be seen as a law that restricts the behaviour of the interconnection variables [10].
Communication aspects	*Set*, see Table 10 $\cup$ {*Not considered*}	WHAT	The introduction of the communication network in a control loop modifies the external signals of the plant and the controller due to the network-induced imperfections [10], which in turn depend on some communication aspects, such as transmission scheduling and routing.
Process noise	*Set* {*Gaussian, Bounded non-stochastic, Noiseless*} $\cup$ {*Not applicable*}	HOW	The process noise is used to capture any deviation in the plant model from the real dynamics of the controlled physical system [13]; it can be broadly categorized into three classes: *Gaussian*, *bounded non-stochastic*, and *noiseless*. When the study uses the measurement model only, we say that process noise is *not applicable*.

Parameter name	Type	Category	Description
Measurement noise	*Set* {*Gaussian, Bounded non-stochastic, Noiseless*} ∪ {*Not applicable*}	HOW	Depending on the assumptions on the noise, sensor measurement models can be broadly categorized into three classes: *Gaussian*, *bounded non-stochastic*, *noiseless* [14]. We say that the measurement noise is *not applicable* if the work does not consider the measurement model (e.g. when the work is not related to the secure state estimation against sensor attacks).
Time-scale model	*Set*{*Continuous, Discrete*} ∪ {*(Quasi-)static*}	HOW	The dynamic system behaviour can be modelled via different time-scale models, such as *continuous*, *discrete* and *hybrid* (if both continuous and discrete behaviours are considered). In the case of the (quasi-)steady state assumption, the system is treated as *(quasi-)static*, and the time-scale model is named accordingly.
Attack name	*Set*, see Table 11	HOW	The name of the (class of) attacks on a CPS considered in a primary study.
Plant model used by an attacker	*Set*, see Table 6 ∪ {*Absent*}	HOW	A modelling framework used to design an attack on a CPS. Since attacker's knowledge of the control system and plant model can be limited or absent, an adversary may rely on a model of plant, that is different from the the actual model used by a system operator.
Adversary's prior model knowledge	*Set*{*Complete, Limited, None*}	HOW	The amount of *a priori* knowledge regarding the control system is a core component of the adversary model, as it may be used, for instance, to render the attack undetectable [15].
Adversary's disclosure resources	*Set*{*Complete, Limited, None*}	HOW	The disclosure resources enable the adversary to obtain sensitive information about the system during the attack by violating data confidentiality [15]. The disclosure resources alone cannot disrupt the system operation. An example of an attack using only disclosure resources is the eavesdropping attack.
Adversary's disruption resources	*Set*{*Complete, Limited, None*} ∪ {*Above the undetectability threshold*}	HOW	Disruption resources can be used to affect the system operation, which happens for instance when data integrity or availability properties are violated [15].
Attack scheme	*Set*{*Centralized, Distributed, Local only*}	HOW	This dimension looks at whether an attack focuses on the local or global scale of the system. For those approaches at the global scale, this dimension also specifies whether they use centralized or distributed coordination model.

Parameter name	Type	Category	Description
Defence scheme	*Set*{*Centralized, Distributed, Local only*} ∪ {*Not available*}	HOW	This parameter specifies whether an approach focuses on the local or global scale of the system. In case of the global scale, this dimension also specifies whether a defence mechanism uses centralized or distributed coordination model. The defence scheme is *not available*, if the study is only focused on analysis of vulnerabilities from attacks.
Defence strategy	*Set*, see Table 12 ∪ {*Not available*}	HOW	This facet considers the proposed countermeasures against attacks, i.e. actions minimizing the risk of threats. They can be classified as *prevention*, *detection*, and *mitigation* [16]; following the line of the fault diagnosis literature [17], we advocate *isolation* as a further defence strategy extending detection approaches. Moreover, we say that countermeasures are *not available*, if the study uses the attacker's point of view only.
Theoretical foundation	*Set*, see Table 13	HOW	Theoretical background on which a primary study is built upon.
Validation method	*Set*, see Table 14 \ {*Sound argument*}	VALID	The method used for validating the approach being proposed. We apply and extend the classification of research methods in validation research proposed by Petersen et al. [2]. Since all the selected primary studies provide a good line of argumentation (i.e. *sound argument* in Table 14), we are interested in pointing out the works that provide also a mathematical proof of the presented claims.
Simulation model	*Set*, see Table 6 ∪ {*Not applicable*}	VALID	The modelling framework used for the validation via simulation. It can be different from the plant model. We say that the simulation model is *not applicable* if there are no simulations performed in the study.
Simulation test system	*Set*, see Table 15 ∪ {*Other, Not available*}	VALID	The simulation test system used to validate the proposed approach; *not available*, when there are no simulations performed in the primary study; *other* if the simulation is performed on an ad hoc system not included in Table 15.
Experimental testbed	*Set*, see Table 16 ∪ {*Not available*}	VALID	The experimental testbed used for the validation or evaluation of the proposed approach; *not available*, when there are no experiments performed in the primary study.

Parameter name	Type	Category	Description
Repeatability	*Set* $\{High,\ Low\}$	VALID	This parameter captures how a third party may reproduce the evaluation or validation results from the study. In this case we extend the dimension provided in [18] in order to isolate the information concerning the availability of a replication package. Accordingly, repeatability is *high* when the authors provide enough details about (i) the steps performed for evaluating or validating the study, (ii) the developed or used software, (iii) the used or simulated testbed, if any, and (iv) any other additional resource, in a way that interested third parties can repeat the evaluation or validation of the study; *low* repeatability, otherwise.
Availability of replication package	Boolean	VALID	*True* when the underlying platform, tools and/or case studies are publicly available; *false*, otherwise.
Notes	*String*	-	Free field in which the data extractor keeps track of potentially relevant information about the study.

Table 2: Data extraction form

Category	Description
Validation Research	Techniques investigated are novel and have not yet been implemented in practice. Techniques used are for example experiments, i.e., work done in the lab.
Evaluation Research	Techniques are implemented in practice and an evaluation of the technique is conducted. That means, it is shown how the technique is implemented in practice (solution implementation) and what the consequences of the implementation in terms of benefits and drawbacks (implementation evaluation) are. This also includes identification of problems in industry.
Solution Proposal	A solution for a problem is proposed, the solution can be either novel or a significant extension of an existing one. The potential benefits and the applicability of the solution is shown through a small example or a good line of argumentation. We want to point out that often this category corresponds to the results of theoretical research.
Philosophical Papers	These papers sketch a new way of looking at existing things by structuring the field in form of a taxonomy or conceptual framework.
Opinion Papers	These papers express the personal opinion of somebody whether a certain technique is good or bad, or how things should been done. They do not rely on related work nor research methodologies.
Experience Papers	They explain on what and how something has been done in practice. It has to be the personal experience of the author.

Table 3: Research classification (extracted from [1])

	R1	R2	R3	R4	R5	R6
Conditions						
Used in practice	T	•	T	F	F	F
Novel solution	•	T	F	•	F	F
Empirical evaluation	T	F	F	T	F	F
Conceptual framework	•	•	•	•	T	F
Opinion about something	F	F	F	F	F	T
Authors' experience	•	•	T	•	F	F
Decisions						
Evaluation research	✓	•	•	•	•	•
Solution proposal	•	✓	•	•	•	•
Validation research	•	•	•	✓	•	•
Philosophical papers	•	•	•	•	✓	•
Opinion papers	•	•	•	•	•	✓
Experience papers	•	•	✓	•	•	•

Legend: T = True, F = False, • = irrelevant of non applicable, R1-R6 refer to rules.

Table 4: Research type classification decision table (presented in [2]).

Library	**Website**
ACM Digital Library	dl.acm.org
IEEE Digital Library	ieeexplore.ieee.org
ISI Web of Science	apps.webofknowledge.com
ScienceDirect	www.sciencedirect.com
SpringerLink	link.springer.com
Wiley InterScience	onlinelibrary.wiley.com

Table 5: Electronic data sources targeted with search strings

Category	**Description**
AC power flow	Full power flow model of a transmission grid. It considers both real and reactive power, and follows nonlinear mathematical dependencies. The state variables are voltage magnitudes and phase angles of the buses [12, 19].
DC approximation of power flow	Linear approximation of AC power flow. The reactive power is completely neglected, and state variables only consist of voltage phase angles of the buses [12, 19].
Linear time-invariant	Although no real system is either linear invariant or time invariant, many real systems are well approximated by LTI models within the time duration and range of inputs over which they are used [10].
Nonlinear dynamical system	Virtually all physical systems are nonlinear in nature. When a linearized model is inadequate or inaccurate, a nonlinear model is required [20].
Swing equations-based	A model which describes the electromechanical swing dynamics of the synchronous generators in the grid [21].

Table 6: Modelling framework

Category	Description
(Extended) Kalman filter	Linear(-ized) quadratic estimator (LQE) based on the work of R.E. Kalman [22].
(Extended) Luenberger observer	Asymptotic state estimator based on the work of D.G. Luenberger [23].
H_∞ filter	Also called the minimax filter and specifically designed for robustness, it does not make any assumptions about the statistics of the process and measurement noise, and minimizes the worst-case estimation error [24].
Maximum likelihood estimator	Maximizes the probability that the estimate of the state variable is the true value of the state variable vector [19].
Weighted least-square (WLS)	An estimator that minimizes the sum of the squares of the weighted deviations of the estimated measurements from the actual measurements [19].
Minimum variance estimator	Minimizes the expected value of the sum of the squares of the deviations of the estimated components of the state variable vector from the corresponding components of the true state variable vector [19].
Least trimmed squares (LTS)	A typical *robust* estimator that minimizes the sum of the smallest ordered squared residuals up to the rank v [25].

Table 7: State estimators

Category	Description
Event-triggered & self-triggered	Within a scope of control systems where sensing and actuation is performed when needed rather then periodically, event-triggered control is reactive and generates sensor sampling and control actuation when, for instance, the plant state deviates more than a certain threshold from a desired value; self-triggered control, on the other hand, is proactive and computes the next sampling or actuation instance ahead of time [26].
Linear time-invariant feedback	A generic state feedback or output feedback controller with a control law restricted to be linear time-invariant [9].
Linear-quadratic regulator	LQR is one of the most common optimal feedback controllers [9]. In combination with a Kalman filter, it forms a linear-quadratic Gaussian (LQG) controller, which is standard approach to solve control problems in a wide range of application areas, such as the aerospace industry, characterized by physical systems for which it is technically and economically feasible to develop accurate fundamental models [27].
H_∞	A robust controller that addresses the issue of worst-case controller design for plants subject to unknown additive disturbances, including problems of disturbance attenuation, model matching, and tracking [28].
Proportional-integral-derivative	With its three-term functionality covering treatment to both transient and steady-state responses, PID control offers the simplest and yet most efficient solution to many real-world control problems. More than 90% of industrial controllers are implemented based around PID algorithms [29].
Sliding mode	Characterised by a discontinuous nature of the control action whose primary function of each of the feedback channels is to switch between two distinctively different system structures such that a new type of system motion exists in a manifold [30], it can result in systems very robust to parametric uncertainty and external disturbances [31].

Table 8: Controllers

Category	Description
Building automation (e.g. HVAC)	Systems traditionally concerned with automation of heating, ventilation, and air-conditioning (HVAC), as well as lighting and shading, in large functional buildings [32, 33].
Irrigation and water supply	Hydrosystems which rely on automatic control, such as modern open channel flows for irrigation purposes [34] and municipal water supply systems [35].
Linear dynamical systems	Systems modelled by differential (and/or difference) equations are common for different applications [10]. When the application is generic and the model is linear, we speak about linear dynamical system.
Nonlinear dynamical systems	When the application is generic and the model is nonlinear, we speak about nonlinear dynamical system.
Power grid: generation	The generation functionality in a power system primarily involve controlling the generator power output and terminal voltage. The control schemas used here include (local) automatic voltage regulator (AVR) and governor control, in addition to (wide-area) automatic generation control (AGC) [36].
Power grid: transmission	The transmission system normally operates at voltages in excess of 13 KV and the components controlled include switching and reactive power support devices. The control loops involved in transmission systems are power system state estimation, Volt-ampere reactive (VAR) compensation and phasor measurement units (PMU)-based wide-area measurement systems [36].
Power grid: distribution	The distribution system is responsible for delivering power to the customer. With the emergence of the smart grid, additional control loops that enable direct control of load at the end user level are becoming common. They include load shedding schemes and advanced metering infrastructures (AMI) [36].
Power grid: electricity market	Two-settlement system (day-ahead and real-time) based on the concept of locational marginal pricing (LMP) has been widely adopted in the electricity markets [37]. To calculate electricity prices and manage transmission congestion, it uses a real-time information about generation and demand, which is obtained from power grid state estimation.
(Unmanned) aerial systems	Pilotless aircraft in all possible configurations [38], also known as unmanned aerial vehicles (UAV, drones), present a number of challenges in both on-board and remote control. On the supervisory level the air traffic management [39] is also to be considered.
(Unmanned) ground vehicles	The systems dealing the navigation and control of teleoperated and autonomous ground vehicles, together with their supervisory control [40] and vehicle platooning [41] are of the primary interest in this application area.

Table 9: Application fields where the proposed approach has been adapted

Category	Description
Error control coding	To detect whether the received packet contain errors or not, and possibly correct some of the bit errors, error detection codes and error correction codes [42] are used [43].
Transmission scheduling	The competition of multiple nodes (that may correspond to a collection of sensors, actuators, or controllers) accessing network is often referred to as a *scheduling problem* [44]. Within the topic, the analysis and design of appropriate protocols determining which nodes access a network when and how is a major concern. In other words, the focus here is on *medium access control* (MAC) protocols, that define a set of rules for how to share the medium between transmitters to avoid interference and communicate efficiently [43].
Routing	A process of selecting paths along which to send data traffic. Data packets are then forwarded from sources to their final destinations via the intermediate nodes on the selected routes. Most routing algorithms use a single network path between sources and destinations, while multipath routing protocols maintain several alternative paths to improve reliability. Routing protocols are further classified as either reactive (on-demand) or pro-active (table-driven) [43].
Time-varying sampling	For the networked control systems (NCS), the sampling intervals are (preferably) termed as *transmission intervals* [44], since the *sampling jitter* occur not only due to the factors typical in all digital control systems (e.g., clock accuracy), but also to the scheduling of the packet transmissions in the context of multiple sensor nodes.
Variable latency	The *time delays*, which are composed of the computational delays in each component of the system due to the certain processing speed of the digital devices, the network access delay, i.e., the time a queued network packet has to wait before being sent out, and the transmission delay through the network medium [44].
Packet losses & disorder	Due to network traffic congestion and packets transmission failures, packet losses are inevitable in networks, especially in wireless ones. How to determine an adequate lower bound on the packet transmission rate is a major concern in the area. If the network-induced delays are longer than one sampling/transmission interval, the order of the arrival of the packets to the receiver can be lost. The straight way of solving this problem by discarding the old packets if the latest packet has already arrived at the receiver isn't always the best [44].
Limited bandwidth	When shared channels are used by different system components, the data rate of each signal must be counted to ensure that the total is less than the capacity of the communication channel. Effects due to capacity constraints include time delays, losses of data, scheduling of transmissions, and encoding/quantization of signals [43]. The quantization mainly results from the finite word length of the packets. Quite a few opinions in NCS literature insist on that the quantization effect can be ignored since enough number of bits in each transmitted packet can be guaranteed by the current network technologies [44].
Synchronization errors	Errors between the individual clocks at local and remote nodes [44].

Table 10: Communication aspects and network-induced imperfections

Category	**Description**
Bias injection attack	A *deception attack* where the adversary's goal is to inject a constant bias in the system without being detected [15]. The data corruptions may be added to both the actuator and sensor data.
Covert attack	A *deception attack* in which the adversary can gain control of the plant in a manner that cannot be detected by the controller (a covert misappropriation of the plant) [45]. It requires some levels of system knowledge and the ability of attacker to both read and replace communicated signals within the control loop.
Data Framing attack	A *deception attack* on *state estimation* that exploits current bad data detection and removal mechanisms. It purposely triggers the bad data detection mechanism and frames some normally operating meters as sources of bad data such that their data will be removed. After such data removal, although the remaining data appear to be consistent with the system model, the resulting state estimate may have an arbitrarily large error [46].
Denial of Service (DoS) attack	A *disruption attack* that renders inaccessible some or all the components of a control system by preventing transmissions of sensor or/and control data over the network. To launch a DoS, an adversary can jam the communication channels, compromise devices and prevent them from sending data, attack the routing protocols, flood with network traffic some devices, etc. [47].
Eavesdropping	A *disclosure* attack which violates data confidentiality by gathering sequences of data from the real measurements and/or the calculated control actions, in order to obtain a sensitive information about the system during the attack [15].
False Data Injection attack	A specific *deception attack* on state estimation, introduced in the context of electric power grids [48]. An adversary with some knowledge of the system topological information manipulates sensor measurements in order to change the state variables, while bypassing existing bad data detection schemes.
Generic *deception attack*	An attack on data integrity, where an adversary sends false information from (one or more) sensors or/and controllers in order to deceive a compromised system's component into believing that a received false data is valid or true [49]. Usually it is modelled as an *arbitrary additive signal* injected to override the original data.
Leverage point attack	A *deception attack* which creates leverage points within the factor space of the *state estimation* regression model [50]. The residual of the measurement corresponded with the leverage point is very small even when it is contaminated with a very large error. Thus the adversary can freely introduce arbitrary errors into the meter measurements without being detected.
Load altering attack	A *disruption attack* against power grid's demand response and demand side management programs, that can bring down the grid or cause significant damage to the power transmission and user equipment. It consists in an attempt to control and change (usually increase) certain load types in order to damage the grid through circuit overflow or disturbing the balance between power supply and demand. [51]

Category	Description
Load redistribution attack	A special type of *false data injection attack* on electric power grid, in which only load bus power injection and line power flow measurements are attackable [52]. It consists in increasing load at some buses and reducing loads at other buses, while maintaining the total load unchanged.
Packet scheduling attack	A *disruption attack* on the scheduling algorithm that influences the temporal characteristics of the network. It results in time-varying delays and data packets possibly received out-of-order. To remain stealthy, the attacker is not able to delay the packets beyond a maximum allowable delay consistent with the network protocol in place [53].
Replay attack	A *deception attack* (possibly combined with a physical attack), in which an adversary first gathers sequences of measurement and/or control data, and then replays the recorded data while injecting an exogenous signal into the system [15].
Switching attack	A *disruption attack* on power grid, where an opponent remotely controls multiple circuit breakers and employs the local state information to design a state-dependent breaker switching sequence, which destabilizes target synchronous generators [54].
Topology poisoning attack	A *deception attack* in which an adversary covertly alters data from certain meters, network switches and line breakers to mislead the control center with an incorrect network topology [55].
Zero dynamics attack	A *deception attack* based on the perfect (local) knowledge of the plant dynamics, in which an adversary constructs an open-loop policy such that the attack signal produces no output [15].
Attack at physical layer	A good example of the attack through physical layer interactions is an attack on vehicle platoon travelling at a constant speed. It is carried out by a maliciously controlled vehicle, who attempts to destabilize or take control of the platoon by combining changes to the gains of the associated law with the appropriate vehicle movements [56].

Table 11: Attacks

Category	Description
Prevention	Prevention aims at decreasing the likelihood of attacks by reducing the vulnerability of the system [16]. It brings together all the actions performed offline, before the system is perturbed or attacked. As example, during the design of a power network, the risk analysis outcome from computing the measurements' security indices [57] may be used to sort the measurements in terms of their vulnerability and identify those that should be protected.
Detection	Detection is an online approach in which the system is continuously monitored for anomalies caused by adversary actions [16], in order to decide whether an attack has occurred.
Isolation	Attack isolation is one step beyond attack detection, since it distinguishes between different types of attacks [17], and requires also that the exact location(s) of the compromised components(s) be identified [58].
Mitigation	Once an anomaly or attack is detected (and isolated), mitigation actions may be taken to disrupt and neutralize the attack, thus reducing its impact [16]. This approach is related to the resilience aspect of a system, which refers to the system's *ability to recover* online after adversarial events occur [59]. The control systems should be designed to be inherently resilient, to allow them to self-recover from unexpected attacks and failures.

Table 12: Defence strategies

Category	Description
Control theory	In control theory we use a variety of modelling and analysis techniques to capture the essential dynamics of the system and explore possible behaviours in the presence of uncertainty, noise, malicious attacks and component failure. The key issues in designing control logic remain ensuring that the dynamics of the closed loop system are stable (bounded disturbances give bounded errors) and that they have additional desired behaviour (good disturbance attenuation, fast responsiveness to changes in operating point, etc) [9].
Computational complexity theory	The main focus of computational complexity is to asymptotically analyze the intrinsic difficulty of problems and algorithms and to decide which of these are likely to be tractable [60].
Graph theory	Graph theory is a the study of graphs, which are simply a way of encoding pairwise relationships among a set of objects [61], [62].
Information theory	Closely related to the communication theory by answering the fundamental questions on the ultimate data compression (the entropy) and ultimate transmission rate of communication (the channel capacity), the information theory has made fundamental contributions also in statistical physics (thermodynamics), computer science (Kolmogorov complexity), and probability and statistics (error exponents for optimal hypothesis testing and estimation) among others [63].

Category	Description
Formal methods	By providing mathematically based techniques that describe system properties, formal methods present a framework for systematically specifying, developing, and verifying systems [64]. In the CPS domain, the concepts of *signal temporal logic* (STL, which is a rigorous formalism for specifying desired behaviours of continuous signals [65]) and *satisfiability modulo theories* (SMT) [66] are of particular interest.
Machine learning and statistics	The methods of *dimensionality reduction* (such as principal component analysis) and of *latent variable separation* (e.g. independent component analysis) provide a way to understand and visualize the structure of complex data sets [67].
Compressed sensing	A framework for simultaneous sensing and compression of finite-dimensional vectors, that relies on linear dimensionality reduction, compressed sensing predicts that *sparse* high-dimensional signals can be recovered from highly incomplete *measurements* by using efficient algorithms [68].
Dynamic programming	Well suited for the optimization of multi-stage decision problems, it represents or decomposes an N-variable problem as a sequence of N single-variable problems in such a manner, that the optimal solution of the original N-variable problem can be obtained from the optimal solutions of the N one-dimensional problems. Furthermore, the particular optimization technique used for the optimization of the N single-variable problems is irrelevant [69].
Linear programming	Concerned with those optimization problems in which the objective function and the constraints appear as linear functions of the decision variables [69], it is a special case of convex optimization and is solvable in polynomial time [60].
Quadratic programming	Treating nonlinear programming problems with a quadratic objective function and linear constraints [69], in the convex minimization case it is solvable in polynomial time [60].
Semidefinite programming	A class of nonlinear *convex* optimization problems concerned with the optimization of a linear function subject to the constraint that an affine combination of symmetric matrices is positive semidefinite [70]. Although semidefinite programs are much more general than linear programs, they are just as easy to solve. Most interior-point methods for linear programming have been generalized to semidefinite programs.
Convex optimization	If the objective function and the constraint functions are convex, the optimization problem has some important theoretical properties; in particular, any local minimum is a global minimum. These problems have efficient algorithms in general [60].
Integer programming	Involving the optimization of functions over discrete feasible sets, they constitute one of the most challenging classes of optimization problems [60]. When some variables only are restricted to take integer values, the optimization problems are called a *mixed-integer* programming problems [69].

Category	Description
Nonlinear programming	The most general programming problem, in which there is at least one nonlinear function among the objective and constraint functions; all other problems can be considered as its special cases [69].
Stackelberg game	Game in which one player (called the leader) declares his strategy first and enforces it on the other player (called the follower) [71].
Nonzero-sum (differential) game	Continuous-time infinite dynamic games, also known as *differential games* in the literature, constitute a class of decision problems wherein the evolution of the state is described by a differential equation and the players act throughout a time interval [71]. In a nonzero-sum game the sum of the cost functions of the players is not a constant.
Zero-sum (differential) game	In a zero-sum game, as the name implies, the sum of the cost functions of the players is identically zero. A salient feature of two-person zero-sum games that distinguishes them from other types of games is that they do not allow for any cooperation between the players, since, what one player gains incurs a loss to the other player [71].

Table 13: Theoretical foundations

Category	Description
Sound Argument	A valid argument all of whose premisses are true. Clearly the conclusion of a sound argument is true [72]. We remind that an argument is a group of propositions of which one, the conclusion, is claimed to follow from the others, which are premisses.
Mathematical proof	A formal and logical line of reasoning that begins with a set of axioms and moves through logical steps to a conclusion. A proof confirms truth for the mathematician the way experiment or observation does for the natural scientist [73].
Example	An instance illustrating a rule or method, as a mathematical problem proposed for solution. Useful in providing intuition about specific phenomena, it is characterized by a small-to-medium-scale setting and can present a deliberately oversimplified case of a challenging problem.
Case study	An empirical enquiry that draws on multiple sources of evidence to investigate contemporary phenomena in their real-life context, especially when the boundary between phenomenon and context cannot be clearly specified. In some research papers small toy examples claim to be case studies. Those should preferably be termed examples or illustrations [74].
Experiment	A formal, rigorous and controlled empirical investigation. It manipulates one factor or variable of the studied setting, while controls all the other parameters at fixed levels. The effect of manipulation is measured, and based on this a statistical analyses are performed. In cases where it is impossible to randomly assign treatments to subjects, quasi-experiments are used instead, where the assignment of treatments emerges from the characteristics of the subjects or objects themselves. [74].
Simulation	An imitation of the operation of a real-world process or system over time [75]. It is based on a model, that usually takes the form of a set of assumptions expressed in mathematical, logical, and symbolic relationships between the entities of the system. A simulation may be used as a means for conducting an empirical study [74].

Table 14: Validation methods

Category	**Description**
IEEE 4-bus	A 4-bus example. Matpower [76] `case4gs` from [77].
PJM 5-bus system	A modified 5-bus PJM example. Matpower `case5` from [78].
IEEE 9-bus	A 9-bus example. Matpower `case9` from [79].
WSCC 9-bus	Western Systems Coordinating Council's test systems adopted from [80].
IEEE 14-bus	Matpower `case14` represents a portion of the American Electric Power system in the Midwestern United States as of February 1962. See http://www.ee.washington.edu/research/pstca/pf14/pg_tca14bus.htm
IEEE 24-bus RTS / RTS-79 / RTS-96	Matpower `case24_ieee_rts`, also known as IEEE 24-bus reliability test system, is based on IEEE RTS-79 [81, 82].
IEEE 30-bus	Matpower `case30` represents a portion of the American Electric Power system in the Midwestern US as of December 1961. See http://www.ee.washington.edu/research/pstca/pf30/pg_tca30bus.htm
39-bus New England system	Matpower `case39` is obtained from [83] and is available at http://www.pserc.cornell.edu/matpower/docs/ref/matpower5.1/case39.html
IEEE 57-bus	Matpower `case57` represents a portion of the American Electric Power system in the US Midwest as it was in the early 1960's. See http://www.ee.washington.edu/research/pstca/pf57/pg_tca57bus.htm
IEEE 118-bus	Matpower `case118` represents a portion of the American Electric Power system in the Midwestern US as of December 1962. See http://www.ee.washington.edu/research/pstca/pf118/pg_tca118bus.htm
IEEE 300-bus	Matpower `case300` is based on system developed by the IEEE Test Systems Task Force under the direction of Mike Adibi in 1993. See http://www.ee.washington.edu/research/pstca/pf300/pg_tca300bus.htm
Polish system (2383/.../3375)-bus	Matpower cases representing the Polish 400, 220 and 110 kV networks during either peak or off-peak conditions. See http://www.pserc.cornell.edu/matpower/manual.pdf and relevant files.
33-bus / 69-bus RDS	Radial distribution systems from [84] and [85].
Batch reactor process	An unstable batch reactor system as presented by Walsh et al. [86], which is a fourth order unstable linear system with two inputs.
Multi-area LFC	Multi-area load frequency control schemes installed with PI controllers, as described by Jiang et al. [87]
Multipool canal system	An irrigation system consisting of a cascade of a number of canal pools, as presented in [88].
PHANToM Premium 1.5A	A haptic device from SensAble Technologies in the simulation setup, as described in [89]. See also [90].
Rotorcraft in a cruise flight	A model based on flight dynamical equations for a rotorcraft flying at constant altitude and constant speed [91].
Tennessee Eastman challenge	Tennessee Eastman process control system model and associated multi-loop PI control law as proposed in [92].
Two-area Kundur system	A test case from [21], which parameters are provided in `d2asbegh.m` in the Power System Toolbox [93].

Table 15: Simulation test systems

Category	Description
AR.Drone 2.0	A remote controlled flying quadcopter built by Parrot. See http://ardrone2.parrot.com.
Gignac Irrigation canal network	This canal network is located in South France and irrigates about 2800 hectares of agricultural land. The canal is monitored and controlled by the SCADA system which comprises of a centralized base station communicating with the field devices through radio and telephone communication [94].
LandShark	A fully electric unmanned ground vehicle (UGV) developed by Black I Robotics. See http://www.blackirobotics.com/LandShark_UGV_UCOM.html.
Micro grid experimental testbed	A laboratory testbed that consists of three Siemens SENTRON PAC4200 smart meters connected into the network with YanHua Industry control machine, which is used to monitor all traffic of lab network and read the data from all meters [95].
Quadruple-Tank Process	A multivariable laboratory process that consists of four interconnected water tanks [96]. In some testbeds it is controlled through a wireless communication network.

Table 16: Experimental testbeds

References

[1] K. Petersen, R. Feldt, S. Mujtaba, M. Mattsson, Systematic mapping studies in software engineering, in: Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering, EASE'08, British Computer Society, Swinton, UK, UK, 2008, pp. 68–77.

[2] K. Petersen, S. Vakkalanka, L. Kuzniarz, Guidelines for conducting systematic mapping studies in software engineering: An update, Information and Software Technology 64 (2015) 1–18.

[3] R. Wieringa, N. Maiden, N. Mead, C. Rolland, Requirements engineering paper classification and evaluation criteria: a proposal and a discussion, Requirements Engineering 11 (1) (2006) 102–107.

[4] E. Engström, P. Runeson, Software product line testing - a systematic mapping study, Inf. Softw. Technol. 53 (1) (2011) 2–13.

[5] A. Mehmood, D. N. Jawawi, Aspect-oriented model-driven code generation: A systematic mapping study, Information and Software Technology 55 (2) (2013) 395–411, special Section: Component-Based Software Engineering (CBSE), 2011.

[6] K. Petersen, Measuring and predicting software productivity: A systematic map and review, Information and Software Technology 53 (4) (2011) 317–343, special section: Software Engineering track of the 24th Annual Symposium on Applied Computing Software Engineering track of the 24th Annual Symposium on Applied Computing.

[7] B. A. Kitchenham, S. Charters, Guidelines for performing systematic literature reviews in software engineering, Tech. Rep. EBSE-2007-01, Keele University and University of Durham (2007).

[8] A. Avižienis, J.-C. Laprie, B. Randell, C. Landwehr, Basic concepts and taxonomy of dependable and secure computing, Dependable and Secure Computing, IEEE Transactions on 1 (1) (2004) 11–33.

[9] K. Aström, R. Murray, Feedback systems: an introduction for scientists and engineers, Princeton University Press, 2010.

[10] W. S. Levine (Ed.), The Control Handbook, Second Edition, CRC Press, 2010.

[11] A. Teixeira, S. Amin, H. Sandberg, K. Johansson, S. Sastry, Cyber security analysis of state estimators in electric power systems, in: Decision and Control (CDC), 2010 49th IEEE Conference on, 2010, pp. 5991–5998.

[12] A. Abur, A. Exposito, Power system state estimation: theory and implementation, CRC Press, 2004.

[13] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, G. Pappas, Robustness of attack-resilient state estimators, in: Cyber-Physical Systems (ICCPS), 2014 ACM/IEEE International Conference on, 2014, pp. 163–174.

[14] S. Mishra, Y. Shoukry, N. Karamchandani, S. Diggavi, P. Tabuada, Secure state estimation: Optimal guarantees against sensor attacks in the presence of noise, in: Information Theory (ISIT), 2015 IEEE International Symposium on, 2015, pp. 2929–2933.

[15] A. Teixeira, I. Shames, H. Sandberg, K. Johansson, A secure control framework for resource-limited adversaries, Automatica 51 (0) (2015) 135–148.

[16] A. Teixeira, K. Sou, H. Sandberg, K. Johansson, Secure control systems: A quantitative risk management approach, Control Systems, IEEE 35 (1) (2015) 24–45.

[17] I. Hwang, S. Kim, Y. Kim, C. Seah, A survey of fault detection, isolation, and reconfiguration methods, Control Systems Technology, IEEE Transactions on 18 (3) (2010) 636–653.

[18] E. Yuan, N. Esfahani, S. Malek, A systematic survey of self-protecting software systems, ACM Transactions on Autonomous and Adaptive Systems (TAAS) 8 (4) (2014) 17:1–17:41.

[19] A. Wood, B. Wollenberg, Power generation, operation and control, 2nd Edition, John Wiley & Sons, New York, 1996.

[20] M. Vidyasagar, Nonlinear systems analysis, 2nd Edition, Vol. 42 of Classics in Applied Mathematics, SIAM, Phyladelphia, 2002.

[21] P. Kundur, Power system stability and control, McGraw-Hill Professional, 1994.

[22] R. Kalman, A new approach to linear filtering and prediction problems, Journal of Fluids Engineering 82 (1) (1960) 35–45.

[23] D. Luenberger, An introduction to observers, Automatic Control, IEEE Transactions on 16 (6) (1971) 596–602.

[24] D. Simon, Optimal state estimation: Kalman, H_∞, and nonlinear approaches, John Wiley & Sons, 2006.

[25] L. Mili, M. Cheniae, P. Rousseeuw, Robust state estimation of electric power systems, Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on 41 (5) (1994) 349–358.

[26] W. Heemels, K. Johansson, P. Tabuada, An introduction to event-triggered and self-triggered control, in: Decision and Control (CDC), 2012 IEEE 51st Annual Conference on, 2012, pp. 3270–3285.

[27] S. Qin, T. Badgwell, A survey of industrial model predictive control technology, Control Engineering Practice 11 (7) (2003) 733–764.

[28] T. Başar, P. Bernhard, H^∞-optimal control and related minimax design problems: a dynamic game approach, Springer Science & Business Media, New York, 2008.

[29] K. Ang, G. Chong, Y. Li, PID control system analysis, design, and technology, Control Systems Technology, IEEE Transactions on 13 (4) (2005) 559–576.

[30] K. Young, V. Utkin, U. Özgüner, A control engineer's guide to sliding mode control, Control Systems Technology, IEEE Transactions on 7 (3) (1999) 328–342.

[31] J. Hung, W. Gao, J. Hung, Variable structure control: a survey, Industrial Electronics, IEEE Transactions on 40 (1) (1993) 2–22.

[32] W. Kastner, G. Neugschwandtner, S. Soucek, H. Newmann, Communication systems for building automation and control, Proceedings of the IEEE 93 (6) (2005) 1178–1203.

[33] W. Granzer, F. Praus, W. Kastner, Security in building automation systems, Industrial Electronics, IEEE Transactions on 57 (11) (2010) 3622–3630.

[34] X. Litrico, V. Fromion, Modeling and Control of Hydrosystems, Springer-Verlag London, 2009.

[35] J. Burgschweiger, B. Gnädig, M. Steinbach, Optimization models for operative planning in drinking water networks, Optimization and Engineering 10 (1) (2009) 43–73.

[36] A. Ashok, A. Hahn, M. Govindarasu, Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment, Journal of Advanced Research 5 (4) (2014) 481–489.

[37] T. Zheng, E. Litvinov, On ex post pricing in the real-time electricity market, Power Systems, IEEE Transactions on 26 (1) (2011) 153–164.

[38] K. Valavanis (Ed.), Advances in Unmanned Aerial Vehicles: State of the Art and the Road to Autonomy, 1st Edition, Intelligent Systems, Control and Automation: Science and Engineering, Springer Netherlands, 2007.

[39] C. Tomlin, G. Pappas, S. Sastry, Conflict resolution for air traffic management: a study in multiagent hybrid systems, Automatic Control, IEEE Transactions on 43 (4) (1998) 509–521.

[40] D. Gage, UGV History 101: A Brief History of Unmanned Ground Vehicle (UGV) Development Efforts, Unmanned Systems Magazine 13 (3) (1995) 1–9.

[41] D. Swaroop, J. Hedrick, Constant spacing strategies for platooning in automated highway systems, Journal of dynamic systems, measurement, and control 121 (3) (1999) 462–470.

[42] S. Lin, D. Costello, Error Control Coding, 2nd Edition, Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2004.

[43] A. Bemporad, M. Heemels, M. Johansson, Networked control systems, Vol. 406 of Lecture Notes in Control and Information Sciences, Springer, 2010.

[44] L. Zhang, H. Gao, O. Kaynak, Network-induced constraints in networked control systems – a survey, Industrial Informatics, IEEE Transactions on 9 (1) (2013) 403–416.

[45] R. Smith, Covert misappropriation of networked control systems: Presenting a feedback structure, Control Systems, IEEE 35 (1) (2015) 82–92.

[46] J. Kim, L. Tong, R. Thomas, Subspace methods for data attack on state estimation: A data driven approach, Signal Processing, IEEE Transactions on 63 (5) (2015) 1102–1114.

[47] S. Amin, A. Cárdenas, S. Sastry, Safe and secure networked control systems under Denial-of-Service attacks, in: R. Majumdar, P. Tabuada (Eds.), Hybrid Systems: Computation and Control, Vol. 5469 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2009, pp. 31–45.

[48] Y. Liu, P. Ning, M. Reiter, False data injection attacks against state estimation in electric power grids, ACM Trans. Inf. Syst. Secur. 14 (1) (2011) 13:1–13:33.

[49] Y. Mo, B. Sinopoli, Integrity attacks on cyber-physical systems, in: Proceedings of the 1st International Conference on High Confidence Networked Systems, HiCoNS '12, ACM, New York, NY, USA, 2012, pp. 47–54.

[50] S. Tan, Z. Song, W, M. Stewart, L. Tong, LPAttack: Leverage point attacks against state estimation in smart grid, in: Global Communications Conference (GLOBECOM), 2014 IEEE, 2014, pp. 643–648.

[51] A.-H. Mohsenian-Rad, A. Leon-Garcia, Distributed internet-based load altering attacks against smart power grids, Smart Grid, IEEE Transactions on 2 (4) (2011) 667–674.

[52] Y. Yuan, Z. Li, K. Ren, Modeling load redistribution attacks in power systems, Smart Grid, IEEE Transactions on 2 (2) (2011) 382–390.

[53] Y. Shoukry, J. Araujo, P. Tabuada, M. Srivastava, K. Johansson, Minimax control for cyber-physical systems under network packet scheduling attacks, in: Proceedings of the 2Nd ACM International Conference on High Confidence Networked Systems, HiCoNS '13, ACM, New York, NY, USA, 2013, pp. 93–100.

[54] S. Liu, B. Chen, T. Zourntos, D. Kundur, K. Butler-Purry, A coordinated multi-switch attack for cascading failures in smart grid, Smart Grid, IEEE Transactions on 5 (3) (2014) 1183–1195.

[55] J. Kim, L. Tong, On topology attack of a smart grid: Undetectable attacks and countermeasures, Selected Areas in Communications, IEEE Journal on 31 (7) (2013) 1294–1305.

[56] S. Dadras, R. Gerdes, R. Sharma, Vehicular platooning in an adversarial environment, in: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '15, ACM, New York, NY, USA, 2015, pp. 167–178.

[57] J. Hendrickx, K. Johansson, R. Jungers, H. Sandberg, K. Sou, Efficient computations of a security index for false data attacks in power networks, Automatic Control, IEEE Transactions on 59 (12) (2014) 3194–3208.

[58] K. Sou, H. Sandberg, K. Johansson, Data attack isolation in power networks using secure voltage magnitude measurements, Smart Grid, IEEE Transactions on 5 (1) (2014) 14–28.

[59] Q. Zhu, T. Başar, Game-theoretic methods for robustness, security, and resilience of cyber-physical control systems: Games-in-games principle for optimal cross-layer resilient control systems, Control Systems, IEEE 35 (1) (2015) 46–65.

[60] R. Horst, P. Pardalos (Eds.), Handbook of Global Optimization, Vol. 2 of Nonconvex Optimization and Its Applications, Springer US, 1995.

[61] J. Kleinberg, É. Tardos, Algorithm design, Pearson Addison-Wesley, 2006.

[62] J. Bondy, U. Murty, Graph theory with applications, Elsevier Science Ltd/North-Holland, 1976.

[63] T. Cover, J. Thomas, Elements of Information Theory, 2nd Edition, John Wiley & Sons, 2006.

[64] J. Wing, A specifier's introduction to formal methods, Computer 23 (9) (1990) 8–22.

[65] O. Maler, D. Nickovic, Monitoring temporal properties of continuous signals, in: Y. Lakhnech, S. Yovine (Eds.), Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems, Vol. 3253 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2004, pp. 152–166.

[66] C. Barrett, R. Sebastiani, S. Seshia, C. Tinelli, Satisfiability modulo theories, in: A. Biere, M. Heule, H. van Maaren, T. Walsh (Eds.), Handbook of Satisfiability, Vol. 185 of Frontiers in Artificial Intelligence and Applications, IOS Press, Amsterdam, Netherlands, 2009, Ch. 26, pp. 825–885.

[67] J. Lee, M. Verleysen, Nonlinear Dimensionality Reduction, 1st Edition, Information Science and Statistics, Springer-Verlag, New York, 2007.

[68] Y. Eldar, G. Kutyniok, Compressed sensing: theory and applications, Cambridge University Press, 2012.

[69] S. Rao, Engineering optimization: theory and practice, 4th Edition, John Wiley & Sons, 2009.

[70] L. Vandenberghe, S. Boyd, Semidefinite programming, SIAM review 38 (1) (1996) 49–95.

[71] T. Başar, G. Olsder, Dynamic Noncooperative Game Theory, 2nd Edition, Vol. 23 of Classics in Applied Mathematics, SIAM, Phyladelphia, 1999.

[72] I. Copi, Introduction to Logic, Macmillan, 1953.

[73] P. Griffiths, Mathematics at the turn of the millennium, American Mathematical Monthly (2000) 1–14.

[74] C. Wohlin, P. Runeson, M. Höst, M. Ohlsson, B. Regnell, A. Wesslén, Experimentation in Software Engineering, Computer Science, Springer, 2012.

[75] J. Banks, J. Carson, B. Nelson, D. Nicol, Discrete-event System Simulation, Prentice-Hall international series in industrial and systems engineering, Pearson Prentice Hall, 2005.

[76] R. Zimmerman, C. Murillo-Sánchez, R. Thomas, MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education, Power Systems, IEEE Transactions on 26 (1) (2011) 12–19.

[77] J. J. Grainger, W. D. Stevenson, Power System Analysis, McGraw-Hill Education, 1994.

[78] F. Li, R. Bo, Small test systems for power system economic studies, in: Power and Energy Society General Meeting, 2010 IEEE, 2010, pp. 1–4.

[79] J. H. Chow, Time-scale modeling of dynamic networks with applications to power systems, Vol. 46 of Lecture notes in control and information sciences, Springer Berlin Heidelberg, New York, Berlin, Paris, 1982.

[80] P. Sauer, M. Pai, Power System Dynamics and Stability, Stipes Publishing, Champaign, IL, 1997.

[81] C. Grigg, P. Wong, P. Albrecht, R. Allan, M. Bhavaraju, R. Billinton, Q. Chen, C. Fong, S. Haddad, S. Kuruganty, W. Li, R. Mukerji, D. Patton, N. Rau, D. Reppen, A. Schneider, M. Shahidehpour, C. Singh, The IEEE Reliability Test System-1996. A report prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee, Power Systems, IEEE Transactions on 14 (3) (1999) 1010–1020.

[82] J. Pinheiro, C. Dornellas, M. Schilling, A. Melo, J. Mello, Probing the new IEEE Reliability Test System (RTS-96): HL-II assessment, Power Systems, IEEE Transactions on 13 (1) (1998) 171–176.

[83] G. Bills, et.al., On-line stability analysis study, Tech. Rep. RP-90, Edison Electric Institute, Los Angeles (October 1970).

[84] B. Venkatesh, R. Ranjan, H. Gooi, Optimal reconfiguration of radial distribution systems to maximize loadability, Power Systems, IEEE Transactions on 19 (1) (2004) 260–266.

[85] M. Chakravorty, D. Das, Voltage stability analysis of radial distribution networks, International Journal of Electrical Power & Energy Systems 23 (2) (2001) 129 – 135.

[86] G. Walsh, H. Ye, L. Bushnell, Stability analysis of networked control systems, Control Systems Technology, IEEE Transactions on 10 (3) (2002) 438–446.

[87] L. Jiang, W. Yao, Q. Wu, J. Wen, S. Cheng, Delay-dependent stability for load frequency control with constant and time-varying delays, Power Systems, IEEE Transactions on 27 (2) (2012) 932–941.

[88] S. Amin, X. Litrico, S. Sastry, A. Bayen, Cyber security of water SCADA systems – part II: Attack detection using enhanced hydrodynamic models, Control Systems Technology, IEEE Transactions on 21 (5) (2013) 1679–1693.

[89] S. Liu, P. Liu, A. El Saddik, A stochastic game approach to the security issue of networked control systems under jamming attacks, Journal of the Franklin Institute 351 (9) (2014) 4570–4583.

[90] B. Taati, A. M. Tahmasebi, K. Hashtrudi-Zaad, Experimental identification and analysis of the dynamics of a PHANToM Premium 1.5A Haptic Device, Presence: Teleoperators and Virtual Environments 17 (4) (2008) 327–343.

[91] K. Narendra, S. Tripathi, Identification and optimization of aircraft dynamics., Journal of Aircraft 10 (4) (1973) 193–199.

[92] N. L. Ricker, Model predictive control of a continuous, nonlinear, two-phase reactor, Journal of Process Control 3 (2) (1993) 109–123.

[93] J. Chow, K. Cheung, A toolbox for power system dynamics and control engineering education and research, Power Systems, IEEE Transactions on 7 (4) (1992) 1559–1564.

[94] S. Amin, X. Litrico, S. Sastry, A. Bayen, Stealthy deception attacks on water SCADA systems, in: Proceedings of the 13th ACM International Conference on Hybrid Systems: Computation and Control, HSCC '10, ACM, New York, NY, USA, 2010, pp. 161–170.

[95] T. Liu, Y. Sun, Y. Liu, Y. Gui, Y. Zhao, D. Wang, C. Shen, Abnormal traffic-indexed state estimation: A cyber-physical fusion approach for smart grid attack detection, Future Generation Computer Systems 49 (0) (2015) 94–103.

[96] K. Johansson, The quadruple-tank process: a multivariable laboratory process with an adjustable zero, Control Systems Technology, IEEE Transactions on 8 (3) (2000) 456–465.