Quantifying Observability in State Estimation Considering Network Infrastructure Failures

Victor Meza, *Member, IEEE*, Xiomara Gomez and Ernesto Perez, *Member, IEEE*

***Abstract*—Smart grid integrates electrical network, communication systems and information technologies, where increasing architecture interdependency is introducing new challenges in the evaluation of how possible threats could affect security and reliability of power system. While cyber-attacks have been widely studied, consequences of physical failures on real-time applications are starting to receive attention due to implications for power system security. This paper presents a methodology to quantify the impact on observability in state estimation of possible disruptive failures of a common transmission infrastructure. Numerical results are obtained by calculating observability indicators on an IEEE 14-bus test case, considering the simultaneous disconnection of power transmission lines and communication links installed on the same infrastructure.**

***Index Terms*—Observability, power systems, state estimation, cyber-physical security.**

I. Introduction

Smart grid is defined as a system of systems, based on the interaction of three foundational layers: Power and energy system, information technology and communications [1]. This collaborative integration is defined as a cyber-physical system (CPS), whose communication and computing capabilities allow improving monitor, control and protection functionalities of power systems. However, interaction of different infrastructures, introduce additional complexity in modeling, assessing vulnerability and quantifying the impact of attacks and disruptive failures of CPS.

In recent years, there have been an increasing concern about cyber attacks in the smart grid context, encouraging the development of security standards, as IEEE 1686-2013 Standard for Intelligent Electronic Devices (IEDs) Cyber Security Capabilities, North American Electric Reliability's (NERC) Critical Infrastructure Protection in the electric grid and National Institute of Standards and Technology's (NIST) guidelines for smart grid cyber security, NISTIR7628.

Due to the most of the installed infrastructure is evolving to more complex cyber-physical systems that have not been initially planned to operate under these new paradigms of security, vulnerability to threats and the impact of attacks and failures should be assessed for securing both the networks and the application running on them.

These power and communication networks used to support the applications and tools for monitoring, supervisory and controlling the power grid, have been usually installed on the same transmission towers to make maximum use of the infrastructure. This bidirectional dependency of two infrastructures is denominated interdependency [2]. More complex interdependencies lead to increased risks and greater requirements for security [3].

CPS risk assessment is made by taking into consideration four elements: Asset identification, threat identification, vulnerability and damage [4]. On the other hand, CPS security requirements for the power grid focuses on the functional composition of the following: Physical components and control applications, cyber infrastructures required, the impacts of attacks and countermeasures to mitigate risk [5].

In this CPS framework both the risk assessment and the security assessment entail the identification of physical components and the estimation of the consequences of the materialization of a possible threat to those components.

While the most of the power networks components are typically located at substations and the communication networks components are installed at indoor locations that facilitate implementation of surveillance and access control policies, the electric and communication transmission infrastructures span regions and countries, exposed to natural hazards and vulnerable to deliberate attacks (sabotage, terrorism or military).

Several research works have studied how attacks and failures on CPS affect real-time functionalities and the security of the power system [6] [7] [8] [9]. However, the impact of failures and attacks against an interdependent transmission infrastructure are not clearly quantified in terms of the observability in state estimation.

This paper focuses on establishing a methodology that allows quantifying the risk of unobservability in state estimation when common-cause disruptive failures or attacks affect both power grid topology and availability of measurements.

The definition of an interdependency model and its considerations for this paper are described in Section 2. State estimation principles and numerical observability indicators are described in Section 3. In Section 4, a study case using an IEEE 14-bus test case with a communication system integrated to its infrastructure is shown. The conclusions are summarized in Section 5.

X. Gomez and V. Meza are with XM S.A. E.S.P, Colombian independent system operator. (e-mail: {xagomez}{vmmeza}@xm.com.co).
E. Perez iswith Universidad Nacional de Colombia, Medellin, Colombia. (e-mail: eperez@unal.edu.co).

978-1-4673-6605-2/15/$31.00 ©2015 IEEE

II. Electricity and Communication Infrastructure Interdepencies

Communication networks interconnect wide areas through high-speed links in which data are transmitted to the users via switching and routing nodes. While interconnection allows data to be routed through multiple paths of different lengths, network redundancy enables system to deliver data regardless of a link failure. However, in several cases, these high speed connections are travelling under the same physical transportation medium, constituting a single point of failure. For instance, in January 2015, vandalism against two fiber optic cables at the northern and western part of Colombia causes a disruption in the ring topology of one of the biggest internet service provider, affecting thousands of users as well as the availability of some measurements at the independent system operator's control center [10]. Military escort was required to perform to repairing operations in the area where the attack took place to return to the ring topology.

Additionally, in many power grids, carrier links are physically installed on top of the electrical transmission network, based on optical ground wire (OPGW), and exposed to different threats and adverse conditions. In this case, an attack or a natural hazard that affects the transmission infrastructure is a common cause for a failure, affecting simultaneously both communication and power systems. As an example, the risk of transmission towers collapsing due to landslides in the Peruvian Amazonia region in 2015 which attempted to interrupt energy supply and the internet service [11] clearly illustrates infrastructure interdependency on power grids and the importance of considering the current topology of network to assess vulnerability of systems.

In order to properly consider how systems are affected by disruptive failures and attacks, it is necessary to identify architecture dependency on several different dimensions and. Architecture interdependencies are classified by four different types: Physical, geographic, cyber and logical [3].

A mutual dependency of architectures on the physical output(s) of each other is denominated physical interdependency. Cyber interdependency is the bidirectional relation established by the information transmitted from architectures. Geographic interdependency is the relation derived from spatial proximity of architectures. Logical interdependency implies a bidirectional relation between infrastructures that is not a cyber, physical or geographical connection.

According to definitions of types of interdependency, it is possible to define the interaction of systems based on the facts that the transmission infrastructure has been designed to exchange data in a hierarchical architecture, where most of the data flow from substations to control center and the measurements data serve as input to support supervisory, control and protection functionalities, as well as decision making tools at control center, by processing topology and estimating the state of the power system.

An input-output diagram as shown in Fig. 1, summarize possible interactions between power and communication networks in both level cyber and physical.

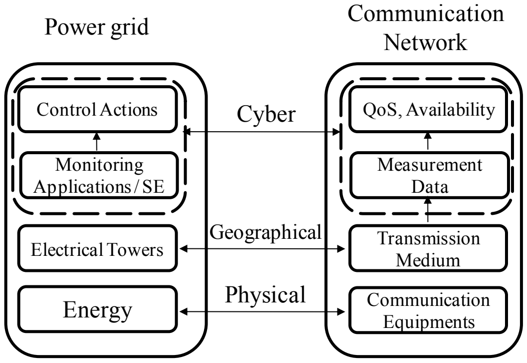

Fig. 1. Interactions between interdependent architectures.

The physical interdependency, at the bottom of the diagram, describes how a power outage could shut down communication equipments. In this paper, no effects on data were considered due to existing robust redundancy schemes (in equipments and energy supply).

Geographical interdependency, the second layer of the diagram, describes a CPS where the transmission infrastructure is shared at some geographical points, this means that damages to transmission towers could lead to simultaneous disconnections of power lines and communication links, thus a possible massive data loss. In this paper, single contingency of line was considered to generate disruption on one or more communication links, according to the communication system topology. Other geographical interdependencies, such as those in which facilities are shared by communication and electrical equipments, were not considered in this paper.

Cyber interdependency is relying on the information transmitted through communication channels, physically affected by the geographical interdependency. The effect of an event on the information could be established around the concepts of confidentiality, integrity and availability, as well as the attributes associated to protocols and systems. For this paper, unavailability of measurements was the only characteristic considered. Considerations associated with the low quality of service (QoS) levels were not taken into account, as they affect mostly control applications rather than observability in state estimator.

III. Observability Analysis and Indicators

Supervisory and control functionalities at control centers are centralized in SCADA/EMS, supervisory control and data acquisition/energy management systems, that provide valid information in real time to the operator to support decision making by the estimation of system states.

State estimator is a tool that allows determining the power system operating point by processing topological information and measurement with high confidence. The topological information is related to location and interconnection of system components and the measurements are usually associated with the variables of voltage, power and angles.

Measurements, control signals and the states of equipments are collected at substations by the SCADA systems, and transmit it to the control center through remote unit terminals (RTU) or programmable logic controllers (PLC), via communication channels, usually dedicated for this exclusive purpose. Measurements and the equipments states serve as input for the state estimator [12].

The state estimator's performance relies on the quality and availability of measurements and data, which in turn means reliance on the communication systems and on the sensing devices at substation. Regularly, the sensing devices belong to the utility company and their failure affects a few data, whereas communication infrastructure belongs to different service providers and its failure involves major consequences.

Usually, state estimators include the following functionalities used to validate the quality and availability of the required input information [13]: Topology processor, Observability Analysis, State estimation solution, Bad data processing, Parameter and structural error processing.

Observability analysis allows to check whether the availability of measurements is enough to estimate the power system state, which in this case, the network is considered observable [14]. When the system is unobservable, determination of observable islands and pseudo-measurements injections are required to restore observability.

There are primarily two approaches to carrying out an observability analysis in state estimation: Topological analysis and numerical analysis. Numerical analysis has been widely employed because of its simplicity and the ease of its implementation in any process [15].

A. *Observability Numerical Analysis*

The problem of observability in state estimation has a structural nature, based on an interdependence between states variables and measurements, which are conditioned by the configuration of the grid [14]. This non-linear relation between the measurements and the state variables can be linearized, taking into account the variables to be estimated: voltages and angles at each bus.

The following considerations, described in [16], allow to simplify the numerical observability analysis:

- To use a linearized network model, P-θ (active power-angle) model, shown in the Equation (1).

  $$\mathrm{z} = \mathrm{H}\theta + \mathrm{v} \tag{1}$$

  Where, z is the active power measurement vector at each transmission line; H is the decoupled Jacobian matrix of the active power flows and injections; θ is the bus voltage phase angle vector; v is the measurement error vector.

- Only the branch reactances are considered and set at one ($b_{ik} = 1$).

- Jacobian matriz elements are defined as:

  $$P_{ik}:\ H(l,i) = b_{ik};\ H(l,k) = -b_{ik} \tag{2}$$

  $$P_i:\ H(l,i) = \textstyle\sum_k b_{ik}\ ,\ i \neq k\ ;\ H(l,k) = -b_{ik} \tag{3}$$

  i and k denote power system buses. Equation (2) allows for the calculation of power flow through line *i-k*. Equation (3) allows for the calculation of power injections at node *i*.

An example of how the matrices z and H are formed from Equations (2) and (3) is presented as follow.

$$z = \begin{bmatrix} P_i \\ P_n \\ \vdots \\ P_{ij} \\ P_{nj} \\ P_{in} \\ \vdots \\ P_{ik} \end{bmatrix} \quad ; \quad H = \begin{bmatrix} 3 & -1 & \dots & -1 & -1 \\ 0 & 1 & \dots & -1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & -1 & \dots & 0 & 0 \\ 0 & -1 & \dots & 1 & 0 \\ 1 & 0 & \dots & -1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & 0 & & 0 & -1 \end{bmatrix}$$

Jacobian matrix dimensions are lxn, where l are the measurements of the active power flows and injections from the model *P*-θ and n is the number of buses in the system.

A system will be considered observable if the gain matrix G, calculated by the Equation (4), is not singular, verified by triangular factorization or whether H is a full rank matrix; this means, that the rank of H must be at least equal to the number of variables to be estimated.

$$G = H^T R^{-1} H \tag{4}$$

Where, G is the gain matrix; H is Jacobian matrix; R is covariance matrix, assumed equal to identity matrix.

B. *Observability Indicators*

The results of conventional observability analysis are one of the two possible states: system is observable or not. Nevertheless, this answer does not present quantitative information that allows for the determining of the unobservability risk.

In [17] some indicators are presented to quantify the unobservability risk, based on the probability of unavailability of a single measurement, and graded according to the number of critical measurements in the power system. Critical measurement is a measurement that once it is removed from the group of measurements, makes system unobservable [18].

The existence of critical measurements and critical measurements sets is inherently given by the configuration network and not by the parameters of the equipments or the value of the measurements, thus this considerations simplify critical measurements identification. In literature several algorithms have been developed for this purpose [19][20][21][22][23][24]. In this paper the algorithm used is proposed in [25], which is based on residual analysis.

Vulnerability of measurement system could be quantified as follows:

$$C_1 = \frac{N_{C_{meas}}}{m}.100\% \tag{5}$$

where,

$N_{C_{meas}}$: Number of critical measurements

m : Total number of system measurements

C_1 is the unobservability risk, assuming that all the measurements have the same probability of unavailability.

A critical set of measurements could be defined as a group of redundant measurements, in which the unavailability of any of its elements, causes the other measurements of the set to be considered as critical measurements [17]. Normalized residuals and correlation coefficients are calculated for the identification of measurements that belong to the same critical set.

$$C_2 = \frac{M_{C_{sets}}}{m} x100\% \qquad (6)$$

Where:

$M_{C_{sets}}$: Number of measurements belonging to the critical measurement sets C_{sets}

m : Total number of system measurements

This indicator quantifies in terms of observability the system's ability to withstand the contingency of a single measurement.

C. Proposed Methodology

Power systems are planned so that they can operate in order to fulfill the *N-1* reliability criteria, in which the security must be guaranteed despite of disconnection of single network element. However, a contingencies assessment mainly focuses on the electrical impact on a system, without taking into account the others effects. According to the described interdependency before, it is possible to quantify transmission line contingency effects in terms of observability when a communication disruptive failure occurs on high capacity links that share the same transmission infrastructure.

Proposed methodology relies on the fact that some line contingency (*N-1*), could cause the unavailability of measurements (*m-k*), where the set of unavailable measurements will depend on networks topology that are not always operating in physical ring topology due to failures, maintenances and attacks. Once identified the impact of infrastructure damage, it is necessary to quantify the risk in terms of the unavailable measurements derived from this possible condition.

The following methodology is proposed to quantify unobservability risk associated with transmission network events in which common transmission infrastructure is affected.

- Calculate the base case indicators with the current topology (C_{Base_1} and C_{Base_2}).
- Read input data: Fiber links and RTU maintenances, transmission lines, available measurements and topological changes.
- Upgrade available measurements and topological changes.
- Calculate gain matrix and verify whether system is observable or not.
- Calculate indicators and percentage change and compare to the base case indicators, as shown in following equation.

$$\Delta_i = \frac{C_{Base\_i} - C_i}{C_i} . 100\% \qquad (7)$$

Where i denotes the indicators C_1 and C_2.

- Compare results to admissible thresholds and display warning signals to operator, if so.

Thresholds for the unobservability risk indicator and the percentage change Δ_i are summarized in the following table, where warning colors are associated with the possible topological scenarios.

TABLE I. THRESHOLDS AND WARNING SIGNALS

	Percentage Change			
Risk	0 to -20 %	-21 to -30%	-31 to -50%	<-50%
0 to 20%	🟩	🟩	🟩	🟩
21 to 30 %	🟩	🟨	🟧	🟧
31 to 50%	🟧	🟧	🟥	🟥
> 50%	🟥	🟥	🟥	🟥

While the unobservability risk indicators quantify how close is the system of being unobservable, the percentage change expresses how C_1 and C_2, in comparison to the current topology, are being affected by transmission infrastructure disruptive failures or attacks.

These warning signals allow to users of this methodology a quickly identification of critical topological scenarios. For instance, warning signals could be displayed at control center to aware operator about possible risks derived from topological changes that could lead to massive loss of data by communication link disruption.

IV. NUMERICAL RESULTS

The method described in this paper is tested on an IEEE 14-bus case, as illustrated at Fig.2. A 11 RTU, 20 measurements (6 injections and 14 power flows) and 12 links communication system (dotted line), in a ring topology, is used along with the test case. The system is assumed to be fully observable. Additionally, it was assumed that each bus with available measurements had a working RTU attached for data gathering and transmission.

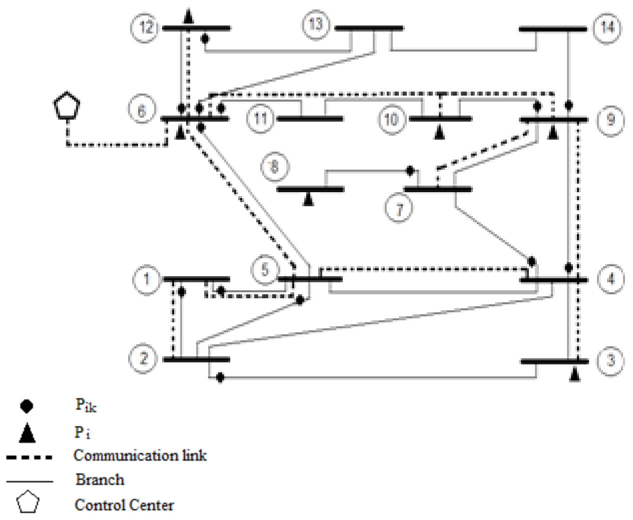

Fig. 2. IEEE 14-bus test case.

All contingencies were evaluated and most relevant results were summarized in Table I. *m* is one or a set of unavailable measurements in case of link disruption. Indicators are shown in columns C$_1$% and C$_2$% (for simultaneous contingency and communication link disruption) and C'$_1$% and C'$_2$% (for single contingency). Percentage change is denoted by Δ_1 and Δ_2. Negative percentage values express an increasing of unobservability risk. Due to the definition of the C_1% and C_2% indicators, a positive change in one indicator always represents a negative change in the other.

TABLE I I. NUMERICAL RESULTS

Failed line	***m***	**C_1 %**	**C_2 %**	**C'$_1$ %**	**C'$_2$ %**	Δ_1	Δ_2
Base case		0	50	0	50	N/A	N/A
1-2	$\boldsymbol{P_{2-3}}$	**22**	**56**	**5**	**47**	**-100**	**-10.7**
1-5	$\boldsymbol{P_{1-2}}$ $\boldsymbol{P_{2-3}}$	***Unobservable***		**5**	**47**	**N/A**	**N/A**
2-3		11	68	11	68	-100	-26.4
3-4	P_3	11	68	11	68	-100	-26.4
5-6		16	63	16	63	-100	-20.6
6-11		16	63	16	63	-100	-20.6
9-10		16	63	16	63	-100	-20.6

Traditionally, the single contingency of 1-2 line would result in an expected value of 5 for the C_1% indicator calculation. However, when an integrated effect of the contingency is considered, the new value of the indicator C_1% is 22, showing a higher risk of unobservability than the conventional approach, where the architecture interdependencies is not taking into account. Due to the contingency of 1-2 line causes a decreasing of 100% of indicator C_1% in comparison to the base case indicator, a new alert level could be displayed at control center, turning the initial green signal into a yellow one for this contingency.

In the same way, the single contingency of 1-2 line shows an increasing unobservability risk value that changes from 47 to 56, when interdependencies described before are considered. However, in this particular case, the change of this indicator would not imply a new warning signal as it does not surpass the proposed threshold.

For the single contingency of 1-5, the loss of two power flow measurements, related to 1-2 and 2-3 lines, made the system unobservable, assuming that the measurement data associated with P_{1-2} and P_{2-3} are gathered and transmitted to control center, via the RTU located at node 5. In contrast, conventional approach shows tolerable values for indicators (denoted as C'$_1$% and C'$_2$%) that indicate a low unobservability risk.

Results obtained by applying the proposed methodology remain the same as in the conventional approach for the rest of contingencies, which means the warning signals and the indicators have the same values.

V. CONCLUSIONS

In this paper is proposed a methodology to quantify risk derived from the impact of disruptive failures caused by attacks or natural hazards that affect a common transmission infrastructure, making possible to achieve *N-1* criteria while is taking into account an unobservability risk evaluation under topology changes.

Information related to communication architecture is considered in contingency analysis to estimate unobservability risk. RTU and high-speed OPGW-based links maintenances information could be part of data inputs, in order to give a more realistic approach to operators at control center where communication systems topology changes can take place.

Suggested architecture interdependencies between power and communication networks are validated against numerical results obtained by considering interdependency-related failures that increase values of critical measurements-based indicators. Additional risk scenarios were identified when methodology was applied to test case.

Percentage change and base case indicators values could be used to aware operator about criticality of contingencies in terms of availability of measurements. Main advantage of this methodology is that provides early signals to power system operators of how severe is the unobservability risk under contingency, before materialization, when preventive actions to mitigate risk could be taken.

Implementation of this methodology implies a good knowledge of the communication network, especially of the current topology and the configuration of communication channels; this information is not always available for the power system operator.

Future works could focus on determining how degradation of quality of service could affect control and protection functionalities centralized at control center.

REFERENCES

[1] C. Lima, "Smart Grid Communications: Enabling a Smarter Grid," presented at the 2010 IEEE SCV ComSoc Monthly Meeting, Silicon Valley, 2010.

[2] J.-C. Laprie, K. Kanoun, and M. Kaâniche, "Modelling Interdependencies between the Electricity and Information Infrastructures," presented at the 26th International Conference on Computer Safety, Reliability and Security (SAFECOMP'2007), Nuremberg, 2007, vol. LNCS 4680–0054.

[3] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *Control Syst. IEEE*, vol. 21, no. 6, pp. 11–25, Dec. 2001.

[4] Yong Peng, Tianbo Lu, Jingli Liu, Yang Gao, Xiaobo Guo, and Feng Xie, "Cyber-physical System Risk Assessment," *Intell. Inf. Hiding Multimed. Signal Process. 2013 Ninth Int. Conf. On*, pp. 442–447, Oct. 2013.

[5] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–Physical System Security for the Electric Power Grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[6] Gu Chaojun and P. Jirutitijaroen, "Impacts of communication failure on power system operations," *Power Energy Eng. Conf. APPEEC 2013 IEEE PES Asia-Pac.*, pp. 1–5, Dec. 2013.

[7] A. Ashok and M. Govindarasu, "Cyber attacks on power system state estimation through topology errors," *Power Energy Soc. Gen. Meet. 2012 IEEE*, pp. 1–8, Jul. 2012.

[8] Jingwen Liang, O. Kosut, and L. Sankar, "Cyber attacks on AC state estimation: Unobservability and physical consequences," *PES Gen. Meet. Conf. Expo. 2014 IEEE*, pp. 1–5, Jul. 2014.

[9] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid," *Smart Grid IEEE Trans. On*, vol. 6, no. 5, pp. 2444–2453, Sep. 2015.

[10] J. Pérez and J. Rojas, "Vandalismo causó caída local de internet en la noche del sábado," *El Colombiano*, Medellin, Colombia, 12-Jan-2015.

[11] RPP Noticias, "San Martín: torres de energía eléctrica a punto de colapsar," *RPP Noticias*, Perú, 14-Feb-2015.

[12] O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, "Network-Aware Mitigation of Data Integrity Attacks on Power System State Estimation," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1108–1118, Jul. 2012.

[13] E. A. Blood, B. H. Krogh, and M. D. Ilic, “Electric power system static state estimation through Kalman filtering and load forecasting,” in *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, 2008, pp. 1–6.

[14] A. Abur and A. Gómez Expósito, *Power system state estimation: theory and implementation*. New York, NY: Marcel Dekker, 2004.

[15] M. Gol, A. Abur, and F. Galvan, “Metrics for Success: Performance Metrics for Power System State Estimators and Measurement Designs,” *IEEE Power Energy Mag.*, vol. 10, no. 5, pp. 50–57, Sep. 2012.

[16] Brown Do Coutto Filho, M, Stacchini de Souza, J.C, and M. T. Schilling, “Handdling Critical Data and Observability,” *Electr. Power Compon. Syst.*, vol. 35, pp. 553–573, 2007.

[17] M. Brown Do Coutto Filho, J. C. Stacchini de Souza, and J. E. Villavicencio Tafur, “Quantifying Observability in State Estimation,” *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2897–2906, 2013.

[18] A. Monticelli and F. F. Wu, “Network Observability: Theory,” *IEEE Power Eng. Rev.*, vol. PER-5, no. 5, pp. 32–33, May 1985.

[19] J. B. A. London, L. F. C. Alberto, and N. G. Bretas, “Network observability: a fast topological approach to identify critical measurements,” *Power Syst. Technol. 2000 Proc. PowerCon 2000 Int. Conf. On*, vol. 2, pp. 583–588 vol.2, 2000.

[20] K. A. Greyson and A. Oonsivilai, “Identification of critical measurements in the power system network,” *Power Syst. Conf. Expo. 2009 PSCE 09 IEEEPES*, pp. 1–6, Mar. 2009.

[21] M. Gol and A. Abur, “Identifying vulnerabilities of state estimators against cyber-attacks,” *PowerTech POWERTECH 2013 IEEE Grenoble*, pp. 1–4, Jun. 2013.

[22] J. B. A. London, L. F. C. Alberto, and N. G. Bretas, “Analysis of measurement-set qualitative characteristics for state-estimation purposes,” *Gener. Transm. Distrib. IET*, vol. 1, no. 1, pp. 39–45, Jan. 2007.

[23] M. Brown Do Coutto Filho, J. C. S. de Souza, F. M. F. de Oliveira, and M. T. Schilling, “Identifying critical measurements & sets for power system state estimation,” *Power Tech Proc. 2001 IEEE Porto*, vol. 3, p. 6 pp. vol.3, 2001.

[24] Kin Cheong Sou, H. Sandberg, and K. H. Johansson, “Computing Critical -Tuples in Power Networks,” *Power Syst. IEEE Trans. On*, vol. 27, no. 3, pp. 1511–1520, Aug. 2012.

[25] M. Brown Do Coutto Filho, J. C. Stacchini de Souza, and J. E. Villavicencio Tafur, “Quantifying Observability in State Estimation,” *Power Syst. IEEE Trans. On*, vol. 28, no. 3, pp. 2897–2906, Aug. 2013.