Strengthen the Security of Control Model in Substation Automation with Service Tracking

Zhiyong Zhu
College of Information Engineering, Xiangtan University
Xiangtan 411105, Hunan, China
zhuzyxtu@163.com

Bin Duan, *Member, IEEE,* Hanying Yuan，and Mingjie Chen
Collaborative Innovation Center of Wind Power Equipment and Energy Conversion
Xiangtan, China

***Abstract*—Mal-operation brings huge potential security risks to the operation of substation automation system. It is very important to find the mal-operation timely to ensure the security and stability of power system. Addressing the interlocking fault caused by two switches having interlocking relationship operated by different operator at the same time or incorrect power system topology, this paper proposes a new remote control model with interlocking reservation and topology verification for strengthening the security of remote operation, which a control block service tracking technology is used to acquire the control commands by local human-machine interface. The scheme can efficiently help the remote control center to be aware of the mal-operation and strengthen the security of power system operation**.

***Index Terms*--Control Service Tracking, IEC standards, mal-operation, Substation Automation.**

I. INTRODUCTION

Smart grid is a new revolution in the power industry, it's an integrated solution for global energy, environment, climate, economy as well as sustainable development, and it represents the future power research and development direction [1], [2]. Substation is an important constituent part in future smart grid [3]. With the development of substation automation technology, substation automation control has gradually replaced the traditional operating mechanism [4]. However, the automation system may lead to topology omission, false positives and simultaneous operation [5].The mal-operation will bring huge risk to the security and stability of grid.

With the advantages that it can achieve an interoperation among different devices, information sharing, and distribution free of logical nodes which makes it easy for the developed system to integrate and extend, IEC 61850 turns into an internationally accepted standard for substation automation area [6]-[10]. The continuous improvement on IEC 61850 standard brings even greater convenience applying to substation automation [11]-[13]. To effectively strengthen monitoring in real time on control behavior of substation devices and timely discover and avoid mal-operation, this paper take the new proposed control service tracking (CST) in the IEC 61850-7-2 Ed2.0 to implement the control behavior online tracking(If the substation follow the IEC standards, control service tracking function can be achieved.). It helps the monitoring center to grasp and analyze the control operation status in a positive way, thus can improve the function of anti-misoperation interlocking in station level [14].

The rest of this paper is structured as follows. Section II takes a specific substation switching operation for example, illustrates the damages from mal-operations to the grid's security and stability, and proposes ideas to improve the scheme. Section III presents the design based on the control service tracking (CST) and verification in IEC 61850 standard. Section IV is simulation experiment. Concluded with a summary is presented in Section V.

II. DEMAND ANALYSIS

Running Example: A Line Switching Scenario

In allusion to power grid security problem which may be caused by mal-operation, this paper takes line switching as a scenario, to analyze the damage of mal-operation. Fig. 1 is a certain 220KV substation line diagram.

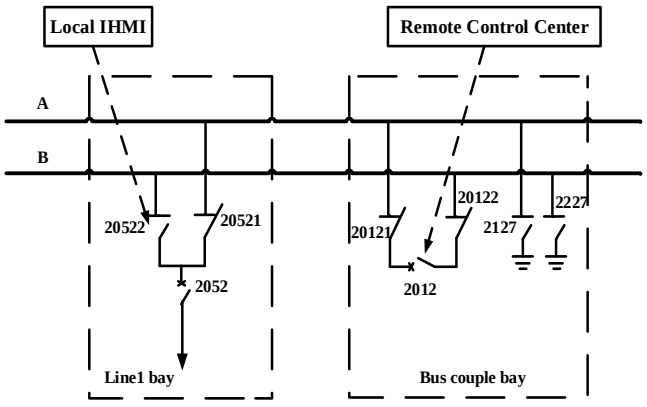

Figure 1. Diagram of 220KV Substation single line

According to interlocking rules of power system, two disconnectors of line bay cannot be closed at the same time[15]. The achievement of interval interlock is to collect reference switch, voltage and current information from process layer, then calculate the interlock group logic, and execute the releasing or closing control operation when the condition is met. At some time, for some reason the remote control center sends remote control command to operate circuit breaker 2012

This research was supported by National Natural Science Foundation of China (NSFC) (No.61170191, 61379063)

open, its simplified interlocking logic expressions meet the equation (1). Here, 1 indicates closing status, 0 indicates opening status.

$$\begin{aligned} Open(2012) = {} & 20121(1)\&20122(1)\&2127(0) \\ & \&2227(0)\&20521(1)\&20522(0) \\ & + 20121(1)\&20122(1)\&2127(0) \\ & \&2227(0)\&20521(0)\ \&20522(1) \end{aligned} \quad (1)$$

Operation commands can be carried out smoothly. Due to the fact that real-time property in remote control process is not very good and status update is not in time. At the same period, if local man-machine interface needs close the disconnector 20522, its simplified interlocking logic expression meets the equation (2).

$$\begin{aligned} Close(20522) = {} & 20121(1)\&20122(1)\& \\ & 2127(0)\&2227(0)\&2012(1) \end{aligned} \quad (2)$$

The action of simultaneous control will cause the dynamic change of topological structure, leading to dynamic change of interlocking result produced by graph theory compute, the failure of interval interlock function. Because the interlock switch information of operation disconnector 20522 that contains 2012 switch status information of breaker. If 20522 switch closes, the 2012 switch's status will change, the interlock result of 20522 is wrong, in the moment, close the 20522 switch is wrong, which may cause electrical accident and seriously harm to the safe and stable operation of power grid.

It is obvious that mal-operation brings potential threat to the safe operation of power grid. However, the service tracking technology proposed in the IEC 61850 Ed2.0, which can implement the real-time tracking of control actions and report the operation conditions of any control service action in real time to the clients that need subscribe. Thus, it provides new ideas for strengthening the control behavior of the station level monitoring and discovering the mal-operation in time. Since the remote control operation needs presetting and executing stage, it takes only millisecond time to generate service tracking report message in preset stage, which is much less than the time interval that operator send control instructions. Thus, the occurrence of simultaneous operation can be avoided effectively.

III. SYSTEM DESIGN

Power topology verification with service tracking

When the station level identifies the topology of entire network, for the protection of real-time property and accuracy, we can adopt distributed identification scheme to implement its design, shown in Fig. 2.

Station level electrical analysis module integrates data sent by the branch and multiple nodes of whole network, completing analysis and verification of power network topology. Control service tracking (CST) server is responsible for the analysis and monitoring of control actions evoked by remote signal and telemetry data change above the branches and nodes, and sending result to the total module of station level electrical topology analysis. At the end, the total module finished the topology analysis and state estimation in local substation, identifying topology faults and bad data, obtaining high-reliability substation topology results and higher accuracy bus voltage, branch power and current data, supplying other advanced applications of station level for utilization.

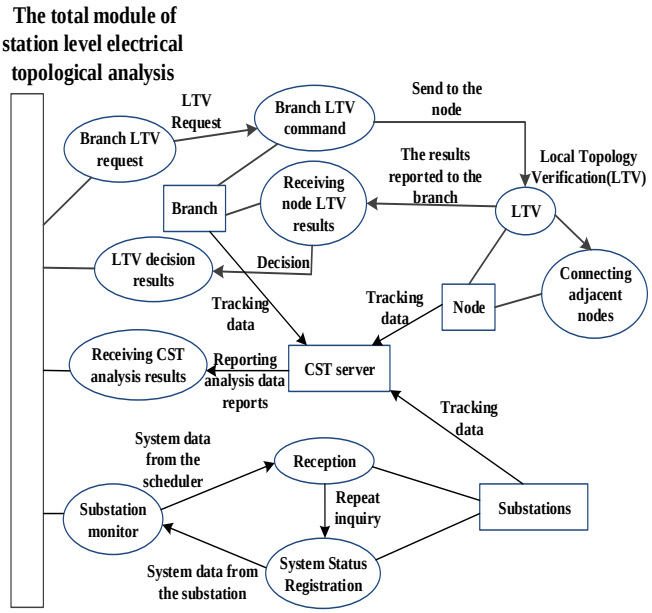

Figure 2. Diagram of Power topology verification with service tracking

Interlocking Reservation with service tracking

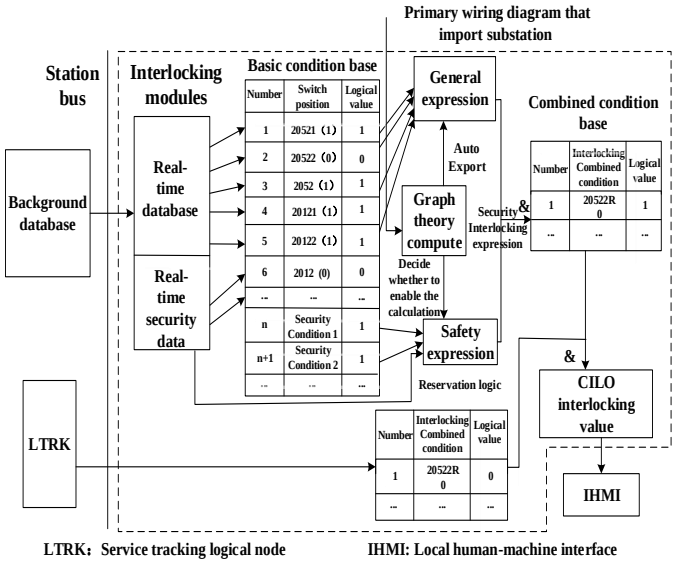

Figure 3. Diagram of Improved CILO model with service tracking

Improved CILO (interlocking logical node) model of station level including service tracking is shown in Fig.3.

Adding reservation logic algorithm in interlocking device model of the substation level, the initial value of reservation logic is "1", does not affect the interlocking device to generate interlocking value. When the substation level needs control operation, in order to doing calculation of interlocking combination condition value, interlocking module obtain real-time data from background monitoring system to obtain an interlocking results, and then detect whether there are other control body are operating and send the service tracking messages to reserving. If it detects the received reservation message, reservation logic value turn to "0", the final interlocking output value is in logical operation (&) between interlocking generated value and reservation logic value "0". On the contrary, the final interlocking output value is in logical operation (&) between interlocking generated value and reservation logic value "1".

Design of remote control model with reservation and verification

1) Remote control process

The remote control execution process based on IEC 61850 standards are illustrated in Fig. 4.

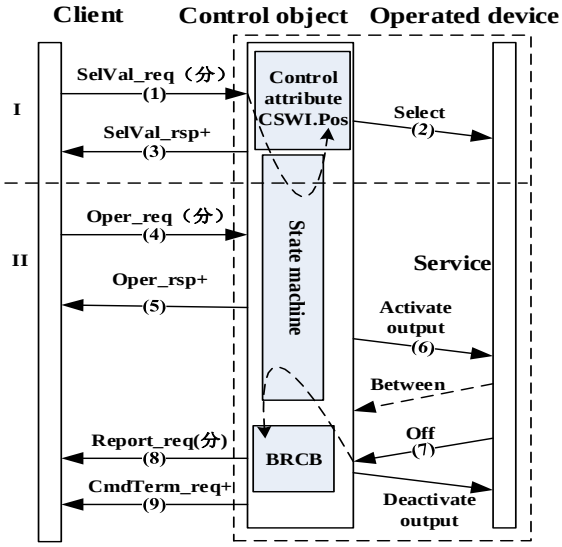

Figure 4. Diagram of select before operate process

In the IEC 61850 standard, the entire remote control execution is completed by defining an enhanced security SBO (select before operate) state machine, and substation remote control process is divided into two stages. Stage I is the preset stage, Stage II is execution stage.

When a client sends a *SelectWithValue* request (SelVal_req), the control object shall determine if the client has appropriate access authority, that the control object is not selected by other client. If the *SelVal* operation is invalid, the control object will issue a negative response (SelVal_rsp-) to the client. If the *SelVal* operation is valid, the control object will issue a positive response (SelVal_rsp+) to the client, shall change the status to ready [12]. If the controls object for this client in a non-ready status, when an operation request is received from the client, the operation will be denied.

When a client sends an *Operate* request, the validity of the control execution will be checked by the control object. If not successful, the control object will issue a negative response (Oper_rsp-) to the client. If successful, the control object will issue a positive response (Oper_rsp+) to the client. Once the control object's status is changed, the control object will report the new status which using the report service of the reporting model [12]. If the status has not been converted to the wanted value after a period of time, once the control object stops activating output, the control object will issue a *ConmandTermination* (*CmdTerm*) negative. If the status has been converted to the wanted value, once the control object stop activating output, the control object will issue a *ConmandTermination* (*CmdTerm*) positive.

The last action is to terminate *ConmandTermination* (*CmdTerm*) the command service.

2) Control service tracking

The essence of remote control is to rewrite data attributes of the controlled object, and the principles of the whole remote control process and the state machines behavior are described detailedly in the above section. The implementation of control service tracking totally applies to the control model in IEC 61850 standards so that the control models do not need any change. The technology can actively track the controlled object performance as long as the object tracking data was defined by the associated data set. When response to a request of the associated control commands, the report behavior would be triggered to report to the clients that need subscribe.

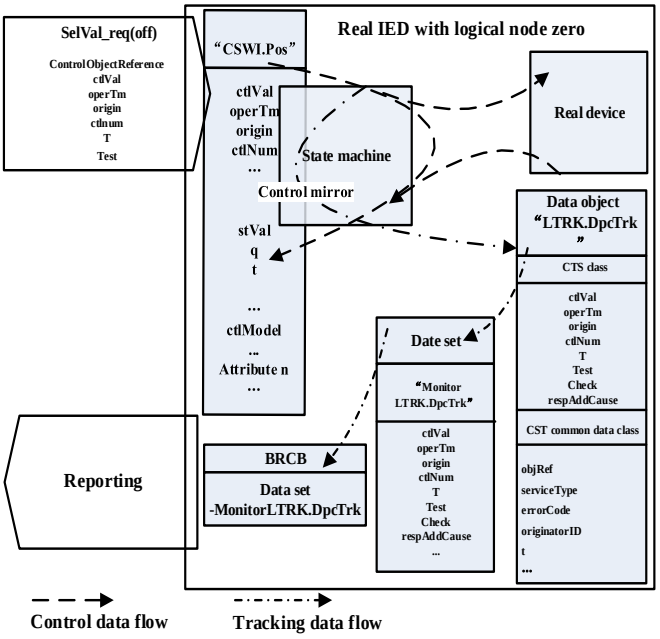

Figure 5. Diagram of Control service tracking

According to the IEC 61850 standard, utilizing logical nodes to model the equipment function, the equipment possesses tracking function of control service tracking (CST), can use logical node LTRK (service tracking logical node) modeling [13]. In the document [16], defining control object type data possess the control mirroring capability. As long as

possesses the relevant data reference path objRef (object reference), LTRK can track the execution of control service in real time. Its implementation principle is shown in Fig. 5.

3) Implementation of reservation and verification

To illustrate how the interactive collaboration of control and control service tracking (CST) realized, we use the line switching scenario instantiation modeling operations, as shown in Fig. 6.

Control commands from the remote control center or integrated human machine interface IHMI use the switch controller CSWI controlling circuit breaker XCBR or disconnector XCWI to be open or close. According to real time state information and interlocking rules, CILO prohibit or allow the execution of control commands; LTRK is used to tracking the control of any tracking service behaviors.

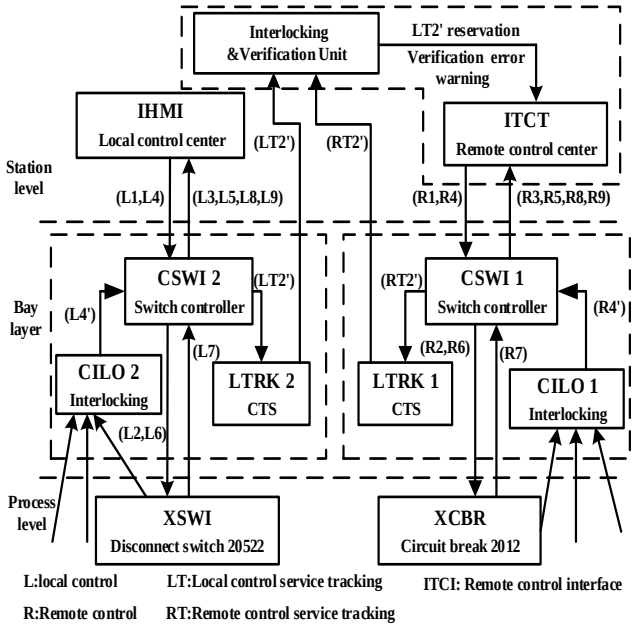

Figure 6. Function block diagram of reservation and verification implementation

Without the application of control service tracking (CST), the control process of disconnector operated by local man-machine interface are shown in icons L1-L9, and remote control center smoothly execute the operation process as shown in icons R1-R9. After addition of the control service tracking (CST) function, regardless of local or remote control center operation, the response of the preset control command parameters will be reported to interlocking & verification unit of the monitoring center by LTRK for on-line analysis and verification, as shown in icons (LT2') and (RT2').

When local operation commands are issued, the interlocking & verification unit online collect control operation situation of entire network controlled equipment in real time for interlocking & verification unit to synchronize on-line analysis. When detected remote operation commands executed, interlocking & verification unit will be performed interlocking logic reservation to local operation commands. When remote operation commands are finished successfully, response message will be tracked by interlocking & verification unit, and then remove the reservation of the local operation commands. Interlocking & verification unit topology verification process is shown in Fig. 2.

The three processes of remote operation commands, including request process, execution process and end of control commands, are shown in Fig. 7.

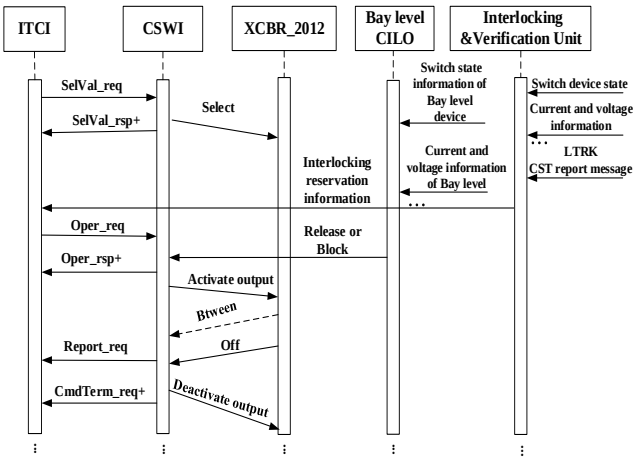

Figure 7. Information interaction diagram of reservation and verification implementation

IV. SIMULATION

This paper uses the Java Agent Development Environment (JADE) software development platform to verify the feasibility of the improved remote control model. Fig. 8 shows the simulation of power system topology verification with control service tracking (CST). Fig. 9 shows the software development of control service tracking agent and event-driven processing.

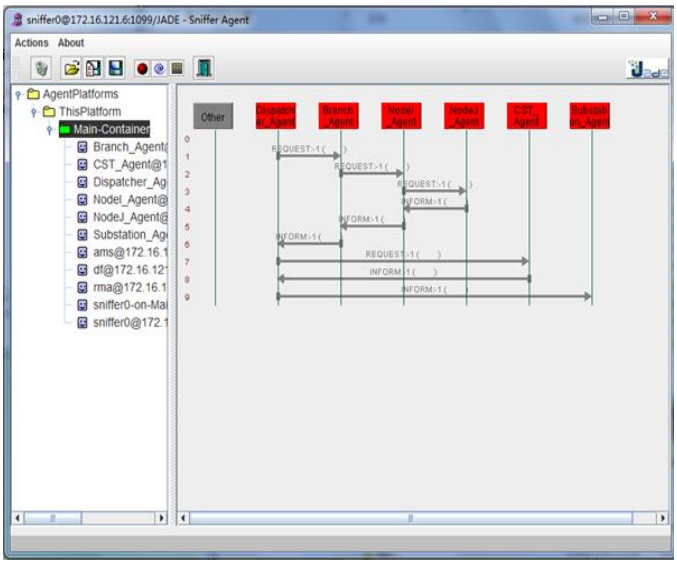

Figure 8. Simulation diagram of power system topology verification

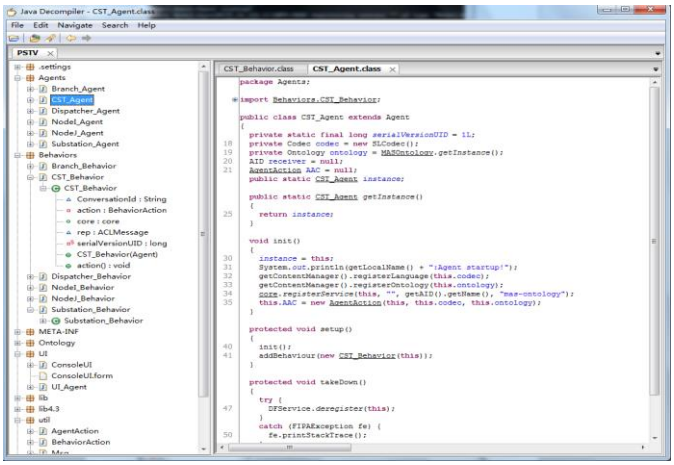

Figure 9. Software development diagram of control service tracking

V. CONCLUSIONS

The continuous improvement of the IEC 61850 standard is more suitable for application to substation automation. The newly revised version proposes the control service tracking (CST) technology, and it can achieve the real-time tracking of any control services, react to changes in the control environment and generate tracking report. This paper explores its implementation mechanism, applies it to the online tracking for substation remote control behavior, and designs the online verification of the control actions. Through the above design, it can effectively reduce the mal-operation behavior and greatly improve the security and stability of the substation, guide the engineering practice, and provide a certain reference value.

ACKNOWLEDGMENT

This research is supported by National Natural Science Foundation of China (NSFC) (No.61170191, 61379063).The authors would like to thank for the Collaborative Innovation Center of wind power equipment and energy conversion.

REFERENCES

[1] H. Farhangi, "A Road Map to Integration: Perspectives on Smart Grid Development," *Power and Energy Magazine, IEEE* 12.3 (2014): 52-66. J. Tan, *Smart Substation Technologies and Its Practice*, vol. II. Beijing: China Electric Power Press, 2010, p. 9.

[2] X. Fang, et al, "Smart grid—The new and improved power grid: A survey," *Communications Surveys & Tutorials, IEEE* 14.4, pp. 944-980, 2012.

[3] J. Tan, "*Smart Substation Technologies and Its Practice*," vol. II. Beijing: China Electric Power Press, 2010, p. 9.

[4] D. Liu, P. Ch. Zhang, and X. L. Li, *The Object-oriented Power System Automation*, vol. II. Beijing: China Electric Power Press, 2009, p. 55.

[5] Y. S. Li, and M. Z. Li, "Analysis and handle of frequent malfunction for unmanned transformer substation remote control," *EI. Power System Protection and Control*, vol. 37. pp. 145-146, Sep. 2009.

[6] V. Shyamala, et al, "Development and operational Experience of Substation Automation System Implementation along with 9–2 LE compliant Process Bus with conventional CTs and PTs," Water and Energy International 57.5, 2014.

[7] F. Clavel, et al, "Integration of a New Standard: A Network Simulator of IEC 61850 Architectures for Electrical Substations," Industry Applications Magazine, IEEE 21.1, pp. 41-48, 2015.

[8] D. V. Dollen. (2009, June.). Report to NIST on the Smart Grid Interoperability Standards Roadmap, Electric Power Research Institute(EPRI).[Online].http://www.nist.gov/smartgrid/upload/InterimSmartGridRoadmapNISTRestructure.pdf.

[9] Z. F. Wang, Y. X, and W. Bao, "*The Smart Grid Safe and Economic Operation of Practical Technology*," vol. II. Beijing: Waterpub, 2011, p. 18.

[10] C. Fan, Y.M. Ni, R.H. Dou, H. Ren, A. G. Zhao, and G. F. Huang, "Discussion on smart substation information model," *EI. Automation of Electric Power Systems*, vol. 36, pp. 15-19, July. 2012.

[11] Y. M. Ren, F. M. Cao, and J. Zhang, "Technical analysis of IEC 61850 Ed 2.0," *EI. Automation of Electric Power Systems.* vol. 37. pp. 1-5, Feb. 2013.

[12] *Communication networks and systems in substations. Ed 2.0: Part 7-2: Basic information and communication structure-Abstract communication service interface (ACSI)*, IEC Std. 61850, Aug. 2010.

[13] *Communication networks and systems in substations. Ed 2.0: Part 7-4: Basic communication structure-Compatible logical classes and data object classes*, IEC Std. 61850, Mar. 2010.

[14] Cui, Mingde, et al. "Research and realization of visual anti-misoperation system of substation based on image recognition technology," *Power System Technology (POWERCON), 2014 International Conference on*. IEEE, 2014.

[15] G. Stranne, "Bay Control IED REC 670," ABB. Rio de Janeiro, Tech.Rep. Apr. 2006.

[16] *Communication networks and systems in substations. Etd 2: Part 7-3: Communication requirements for functions and device models*, IEC Std. 61850, 2010.