# Poster: Specification-Based Process Control Attack Detection in Substation Automation

Muhammad Nouman Nafees
*Computer Science and Informatics*
*Cardiff University*
Cardiff, United Kingdom
nafeesm@cardiff.ac.uk

Neetesh Saxena
*Computer Science and Informatics*
*Cardiff University*
Cardiff, United Kingdom
saxenan4@cardiff.ac.uk

Pete Burnap
*Computer Science and Informatics*
*Cardiff University*
Cardiff, United Kingdom
burnapp@cardiff.ac.uk

***Abstract*—High capability adversaries use sophisticated strategies to stealthily target control processes of critical infrastructure such as the smart grid. Monitoring the "physics" of such process control loops from the cyber-attacks perspective is a growing area of research. However, the existing attack detection strategies have limitations such as requiring correlation techniques for the detection of process control attacks in multiple process loops of a system. To mitigate these issues, we propose a semi-automated specification-based data-driven approach, grounding on a set of programmable logic control invariant information, to detect stealthy attacks in substation automation of the smart grid. Towards this end, we consider a dynamic trust model for our process control attack detection approach. We model IEEE 12-bus system in the PowerWorld simulator to realize the impact and feasibility of such process control attacks. In particular, we study the efficacy of our detection approach on the simulated power system case. We find that our proposed detection approach is capable to detect process control attacks in substation automation with high precision.**

***Index Terms*—Process control attack, Stealthy Attack, Smart Grid, IDS.**

## I. Introduction

Substation automation system, a critical entity of Smart Grid (SG), consists of many physical control processes such as transmission of electricity and conversion of one voltage level to another. High capability adversaries can cause tangible damage to the underlying power and control systems by maliciously performing process control attacks to stealthily manipulate sensors and control data in the substation automation systems. For instance, attackers can alter the temperature of the transmission transformer reported by the sensors which can trigger over-temperature protection logic [1]. As a consequence, protection relays may falsely open circuit breakers to trip several transmission lines. To address these security issues, there is an emerging need to develop an Intrusion Detection System (IDS) with a defined set of rules to detect stealthy attacks against the substation automation systems.

Most of the existing detection approaches use machine learning models to detect cyber-attacks in substation automation systems [2]. However, high capability attackers with advanced power system knowledge can bypass the attack detection systems by performing a stealthy attack that imitates the expected behavior of the physical processes. Other works do not address the trust model of their IDS with high precision and implicitly assume that two or more components such as Programmable Logic Controllers (PLCs) and sensors are trusted [3]. However, a compromised actuator can completely ignore the control signals from the PLC to continue maliciously affecting the system. None of these works develops a specific approach to detect stealthy attacks targeted at the process control loops of the substation automation by considering the dynamic trust model of control processes.

**Contributions.** We propose a specification-based data-driven approach to detect process control attacks where an adversary is able to circumvent a traditional IDS. In so doing, we contribute to semi-automate the specification mining process by utilizing the Substation Configuration Language (SCL) files. We also leverage this documentation to store additional information describing process control logic for various scenarios. As proof of concept, we perform the attack on the IEEE 12-bus system using the PowerWorld simulator to validate the impact of the attack and implement our detection approach on the power system.

## II. Attack Model

We consider a sophisticated adversary, who has gained remote access to protection relays and PLCs in transmission substations. On one hand, the attacker modifies the relay logic so that the fault on one transmission line is detected and responded to by the other relay in the neighboring transmission line. On the other hand, an attacker can replay the normal relay logic to the PLC's process-image input table. Note that the supervisory control layer reads the readings from the process-image input table. The attacker can then opportunistically wait for a stressed load or a line fault on the transmission line which can result in tripping of more transmission lines in the transmission substation.

## III. Approach

We focus our specification-based detection system on the components involved in the process control loops such as PLCs, actuators, and sensors. The first step in creating our detection system is to parse the critical component and function specifications that are available within the SCL file, which is part of IEC 61850 standard. SCL files usually contain formal representations of modeled substations and communication

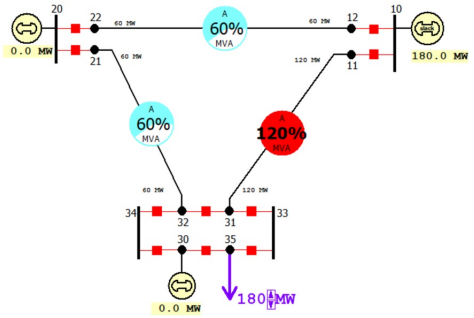


Fig. 1. IEEE 12-bus system.

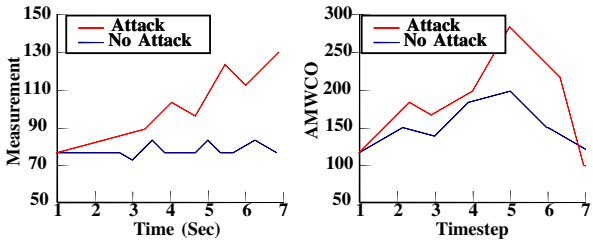


Fig. 2. Process control attack detection with control invariant measurement and AMWCO metric.

data. We leverage this documentation for our IDS to store additional information describing process control logic for various scenarios. Towards this end, time-series data of the power system logs along with voltage measurements are used to derive the state estimation model for control operations. Once information about the functions and components is retrieved, a rule definition is applied to define the actual specification rules.

To detect attacks on the PLCs and relays, we create a temporal state-based model, where we correlate the pre-defined control rules in the PLC. By doing so, we map the process-image input table with a programmed input/output table. Note that the attacker cannot forge the record of the actual commands issued during an attack which are stored in the programmed input/output table of the PLC. This incurs strong relation of the control invariants between the aforementioned two tables. When a process control attack is performed, the correlation of control invariant is matched to verify if an attacker has sent malicious control signal commands or changed any settings. The actual commands and settings are looped back as feedback to the control logic. The control logic actions will record the parameters relevant to the control operations (e.g., opening or closing of circuit breakers). To detect malicious command attacks in the process control loop, we utilize the power system security metric System Aggregate Megawatt Contingency Overload (SysAMWCO). The SysAMWCO is a reliable metric that always indicates the presence of the attack and the value increases with respect to the contingency on transmission lines.

## IV. Validation

We perform the process control attacks on the IEEE 12-bus system using the PowerWorld simulator as shown in Figure 1. We study the impact of process control attacks using simulated attack scenarios. We demonstrate and compare the effectiveness of our detection system on simulated power system datasets from a scaled-down version of substation automation systems. We show that how our specification-based detection algorithm detects stealthy attacks by correlating process control logic. In particular, we show that how the relation of control invariants in PLCs and AMWCO metric can detect attacks targeted at physical operations of the substation automation systems, as shown in Figure 2. One of the observations from our attack detection results indicates that the SysAMWCO metric always increases even if there is a disruption in the process control for other reasons, for example, a faulty transmission line. However, the correlation of control invariants with timesteps can strongly indicate the presence of cyber-attacks in the process control of substation automation system. By doing so, we can ascertain the validity of the applicability of our detection approach to a wide range of process control attacks in the settings of substation automation.

## V. Challenges and Future Work

While the preliminary results of our detection system indicate the efficacy of the system in detecting stealthy and process control attacks, different challenges need to be tackled in the next phase of this work. Firstly, the current validation is performed using a simulated environment, which does not have fidelity to the real physics of the system. Secondly, much of the specification rules are extracted using the SCL files, however, many process control logic and invariants are stored manually for different scenarios of cyber-attacks by considering various trust models in the process control loops. Thirdly, experimenting with attacks targeted at all components of the system in the process control of substation automation was not considered, because a significant amount of human effort is required to craft all the rules for each control process logic in the system. In the next step, we will explore the efficacy of our detection approach by conducting experiments on the physical testbed. In this direction, we will analyze the feasibility of multiple attack scenarios along with adding more control logic algorithms for the detection of process control attacks.

## References

[1] M. M. Roomi, P. P. Biswas, D. Mashima, Y. Fan, and E.-C. Chang, "False data injection cyber range of modernized substation system," in *IEEE SmartGridComm*, 2020.

[2] A. Valdes, R. Macwan, and M. Backes, "Anomaly detection in electrical substation circuits via unsupervised machine learning," in *17th international conference on information reuse and integration (IRI)*, IEEE, 2016.

[3] J. Nivethan and M. Papa, "A scada intrusion detection framework that incorporates process semantics," in *Proceedings of the 11th Annual Cyber and Information Security Research Conference*, 2016.