Towards Threat of Implementation Attacks on Substation Security: Case Study on Fault Detection and Isolation

Chattopadhyay, Anupam; Ukil, Abhisek; Jap, Dirmanto; Bhasin, Shivam

2017

Chattopadhyay, A., Ukil, A., Jap, D., & Bhasin, S. (2018). Towards Threat of Implementation Attacks on Substation Security: Case Study on Fault Detection and Isolation. IEEE Transactions on Industrial Informatics, in press.

<https://hdl.handle.net/10356/88768>

<https://doi.org/10.1109/TII.2017.2770096>

© 2017 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [<http://dx.doi.org/10.1109/TII.2017.2770096>].

Downloaded on 26 Apr 2023 20:53:19 SGT

Towards Threat of Implementation Attacks on Substation Security: Case Study on Fault Detection and Isolation

Anupam Chattopadhyay, *Senior Member, IEEE*, Abhisek Ukil, *Senior Member, IEEE*,
Dirmanto Jap, *Member, IEEE*, and Shivam Bhasin, *Member, IEEE*

Abstract—Modern and future substations are aimed to be more interconnected, leveraging communication standards like IEC 61850-9-2, and associated abstract data models and communication services like GOOSE, MMS, SMV. Such interconnection would enable fast and secure data transfer, sharing of the analytics information for various purposes like wide area monitoring, faster outage recovery, blackout prevention, distributed state estimation, etc. This would require strong focus on communication security, both at system level as well as at embedded device level. Although communication level security is dealt in IEC 62351, implementation attack on embedded system is not considered. Since embedded system makes the core of smart grid, in this paper, we take a deeper look into impact of implementation attacks on substation security. An overview of potential exploits is first provided. This is followed by a case study, where implementation attacks like malicious fault injection attacks and hardware Trojan are used to compromise a substation level intelligent electronic device (IED). The studied scenario extend implementation attacks beyond its usual exploit of confidentiality to affect power grid integrity and availability.

Index Terms—Implementation attack, distribution automation, GOOSE, IEC 61850, IEC 62351, power system communication, smart grid, SMV, substation automation.

NOMENCLATURE

<i>IED</i>	Intelligent Electronic Device
<i>Fault_m</i>	Temporary fault/error introduced for malicious purpose [45]
<i>FIA</i>	Malicious Fault (<i>Fault_m</i>) Injection Attack
<i>GPS</i>	Global Positioning System
<i>T_x</i>	Transient event
<i>I</i>	Measured current
<i>I_{set}</i>	Nominal current

I. INTRODUCTION

THE advances in technology is paving the path from traditional power grid to smart grid. Smart grid exploits digital technology to achieve goals like energy saving, reduce cost, increase quality of service and transparency. With various components of a smart grid communicating seamlessly, new features are proposed. However, a well connected network

from central power grid to consumer end also brings in security and privacy threats. The most obvious threat in this scenario is the cyber-security with Stuxnet being a relevant example [1]. Nevertheless, cyber-security does not only apply to network security vulnerabilities but can also be used to trigger other attacks. Referring back to prime example of Stuxnet, a cyber attack was eventually used to launch a component level threat. Such attack motivates the need for security of the whole chain rather than mere secure access control.

Connected embedded systems will form the *smart* component of the smart grid. Therefore, it is important that these embedded devices are also secure. Implementation attacks on embedded devices have been well studied over the last two decades. [20]. However, in the context of smart grid, these attack are only considered relevant for applications like Advanced Metering Infrastructure (AMI), which is at the consumer end [3]. Historical examples of age-old tampering of mechanical and electromechanical meters by consumer have been for the basis for this assumption. This assumption is rather pessimistic when one is assuming a well connected network. In this paper, we look into critical embedded devices, e.g., protective relays, installed at the substation level under implementation attacks. The main idea is to demonstrate the importance of embedded security for a secure smart grid. Moreover, we demonstrate the implications of implementation attacks beyond the usual target of confidentiality and extend it towards other threats like availability and integrity.

A. Smart Substations

Protection plays a key role in reliable and secure power delivery. Application of the digital recording technology, e.g., digital fault recorders (DFRs), digital protective relays (DPRs), intelligent electronic devices (IEDs) etc. result in high quality and huge quantity of data [4], during the normal and the transient events in power system. Modern and future substations are aimed to be more interconnected. Communication standards like IEC 61850-9-2 [5] are expected to enable fast and secure instantaneous data (from current and voltage transformers, etc.) transfer, sharing of the analytics information at process and bay level. Substation equipment, transient and normal events data would be structured by the abstract data models like SMV (Sampled Measured Value), abstract communication service interface like, GOOSE (Generic

A. Chattopadhyay (corresponding author) is with School of Computer Science & Engineering, Nanyang Avenue, Nanyang Technological University, 639798, Singapore (email: anupam@ntu.edu.sg, tel: +65 6790 6092).

A. Ukil (corresponding author) is with Dept. of Electrical & Computer Engineering, 20 Symonds Street, University of Auckland, Auckland, New Zealand (email: a.ukil@auckland.ac.nz, tel: +64 9 923 4035).

D. Jap and S. Bhasin are with Temasek Laboratories, Nanyang Technological University, Singapore (email: {djap,sbhasin}@ntu.edu.sg).

Object Oriented Substation Event), specific communication service mapping like MMS (Manufacturing Message Specification) [5]. Besides standard Internet-based communication, potential utilization of the wireless LAN with IEC 61850 [6] for SA and distribution automation (DA) applications is under investigation. IEC 62351 [7] is a recent standard developed by IEC for addressing the security challenges for future digital substations. With the envisioned connected, digital substations, security will also play a significant role in applications like wide area monitoring, faster outage recovery, blackout prevention, distributed state estimation, etc.

B. Related Work: Security of Power Substation

Detection and mitigation model for cyber-attacks in an IEC 61850 enabled substation is a growing area of research [8]–[11]. Different attack models, e.g., data isolation attack [16], data integrity attack [17], time-synchronization attack [18], automation system cyber-attack [19], etc. are also discussed for various operations. Recently, attack on IED devices were presented [43], [44] using malicious network communication, followed by application of data mining approach to differentiate cyber attacks from power system faults. However, in power systems, the security aspects are two-fold, both at embedded device level as well as at system level communication. Power systems protection involves many such embedded devices as well as system level communication. State-of-the-art studies on the power substation automation [8]–[15] assumes a pure computer network security model, which significantly underestimates the potential range of attacks that can happen in any of these devices and simply assumes a classic network security model supported by standardized protocols. This is insufficient to tackle the security challenges for a modern system where the threat model has evolved significantly. Note that, for such security incidents to occur, a malicious attacker need to access the devices, albeit for a short while. Alternatively, the devices could be contaminated with hardware Trojan [24]. Given the proliferation of smart grids in user-centric manner, such risks will grow manifold in near future. Indeed, in the recently released cyber threat and intelligence report for US Electric Sector [2], it is mentioned that, protecting hardware and ensuring a trustworthy supply chain is one of the key challenges.

While the earlier model of security assumed that each of these devices are, so-called, black-boxes, i.e., only the input and output are visible, modern security systems exploit diverse sources of information leakage [20] in the physical implementation of a device, network and storage. Recent investigations have shown, for example, it is possible to get complete knowledge of the secret security keys of a computer by recording the electrical potential of it, merely by touching the computer. In view of the severity of a failure in power substation, modern cyber-attacks, e.g., side-channel attacks and hardware Trojan viruses, cannot be ignored anymore. Clearly, it is important to perform a holistic security assessment of substation protection at network-level as well as the device-level. While some network level attacks are previously presented, the lack of analysis at device-level forms the core motivation of this paper.

C. Contributions

The contributions of this paper are as following. *Firstly*, we give an overview of threat of implementation security at substation level to highlight the gap in the security analysis of the modern smart grid standards. A non-exhaustive but representative list of attack surfaces are identified, and the impacts are discussed. *Secondly*, we show relevant case studies of implementation attacks on substation level IED to substantiate our claim. While IED have been target of cyber attacks before, the attacks demonstrate how implementation attack can impact the integrity and availability of the power grid. The two case studies demonstrate the impact of malicious fault injection attacks and hardware Trojan on the IED and corresponding exploit.

D. Organization

The remainder of the paper is organized as follows. Section II describes the background information on the substation, its data and communication architecture and process flow with relevant standards. Security aspects of smart grid and potential security issues are briefly reviewed in section III. Practical case study to demonstrate impact of implementation attack on IED, leading to the violation of integrity and availability is presented in section IV, followed by conclusions in section V.

II. GENERAL BACKGROUND

A. Substation Architecture

Modern substation architecture can be structured roughly in three-levels: process, bay and station, as shown in Fig. 1. Process level has different power devices like transformers, current/voltage transformers (CT/VT), circuit-breakers (CB), switch-gears, surge arresters, etc., which are all essentially analog devices. Therefore, merging units (MU) are required to convert the analog signals, acquired/generated by the process level equipments, into digital signals. These information are transferred to the bay level, which comprises of the protection and control devices, which are embedded devices like DFRs, DPRs, IEDs, etc. The bay level embedded devices control and interact with the process level equipments. The station level gathers information from the bay level devices for real-time supervision, monitoring and intervention by human experts. The future interconnection between the substations, and for centralized operation with network control centers, should be handled from the station level.

B. Data and Communication Architecture

The IEDs at process and bay level devices typically use IEEE COMTRADE (Common Format for Transient Data Exchange) format to store the disturbance data for grid fault analysis. The standard files are ASCII files. Each event has three types of files associated with it, header (*.HDR), configuration (*.CFG) and data (*.DAT) [4]. Transient and normal events are typically captured for 3–5s. The sampling frequency varies from about 1 kHz to 4–8 kHz, up to about 15.36 kHz (corresponding to maximum allowed 256 samples/cycle for 60 Hz nominal frequency [5]). All the digital data files

Fig. 1: Substation architecture at process, bay and station level.

could be susceptible to be compromised in future, e.g. wrong information could be written, or event data could be erased, etc. This could particularly happen in future digital substation, described in following sections.

C. Substation Process Flow

In this subsection, we describe the flow of information in a power substation and how it is envisioned to be part of a smart grid.

1) *Disturbance & Fault Analysis in Substations:* The first disturbance recording systems in electrical power systems were based on electromechanical and analogue technology. The measurements were recorded on metallic or photosensitive papers or magnetic tapes. The accuracy, the number of signals, the recording time and the number of data records per paper roll or magnetic tape were highly restricted. Eventually electromechanical relays were used. However, all of these devices had little or no communication. The device level communication was done using copper cables.

Modern substations use variety of digital recording devices, DFRs, DPRs, IEDs, etc. However, most of the different protection devices are now increasingly being merged into the DFRs (also referred as IEDs), which are installed on the feeder bays, as well as on the static var compensator (SVCs). The digital recording of the events are done as per the IEEE COMTRADE standard, described in the previous section.

Typical disturbance analysis architecture employed at the substations is shown in Fig. 2. The substations are typically connected to the utility network control (NC) centers. After a transient (Tx) event, e.g., temporary/permanent faults, power swing, etc. in the network, the DFRs trigger and record the event. The substation receives the information via a SCADA (Supervisory Control And Data Acquisition) network, and the protection/restoration units provide a 24-hour support through the analysis of the records. It is possible to download the fault record via the X.25 communication network. The dotted lines in Fig. 2 represent the items that are not yet fully realized. For example, after downloading the fault records, the analysis is semi-automatic, not fully automated, which is shown as dotted. The analysis and the fault records would go to the database 'Transient Information Post Processing System' (TIPPS). At transmission level, the DFRs employ GPS as well,

in order to accurately time-stamp the measurements. GPS is not yet applied at distribution level substations. Thus, given the importance of DFR or IED in the whole process flow, it becomes a single point of failure in event of attack.

Fig. 2: Architecture for disturbance and fault analysis at substations.

2) IEC 61850 Standard for Substation Automation:

SCADA and sometimes X.25 form current choice for communication protocol in modern substations. However, both are rather slow. In future, communication standards like IEC 61850-9-2 [5] are expected to enhance the communication, data availability more flexibly. Fig. 3 shows the architecture of the utilization of IEC 61850 standard at a particular substation. Also, one of the key features for the IEC 61850 enabled digital substations would be interconnection of the different substations, as shown in Fig. 3. Digital substation with IP-enabled devices is a key step in the smart grid initiative. This is because of easier interoperability of the substations, which will facilitate better inter-connection of multiple grids, e.g., main grid with different micro grids, etc. Remote and easier access to the devices is a main driver as well. This would facilitate applications like easier fault zone identification, quicker outage recovery, faster and robust power system state estimation, blackout prevention etc. Potential utilization of the wireless LAN with IEC 61850 [6] for substation and distribution automation are also under considerations. However, all these schemes would require enhanced security.

As seen from Fig. 3, the most vulnerable access points prone to electronic intrusions would be the connection between the substation and the control center, substation to substation, as well as substation to remote operator, as these will carry the information over the internet. Within a substation, the most vulnerable points would be the 'merging units', which collects the channel data from CT/VT to line data, which would be shared. Hence, the merging units could be compromised for injecting wrong information digitally. Also, it is very dangerous because the compromised merging units could result in mal-operation of critical field devices like circuit-breaker, transformer, creating extreme events like blackouts, etc. The substation ethernet bus could also be a vulnerable point to get compromised.

3) *IEC 62351 Standard for Substation Security:* IEC 62351 is a recent standard [7] developed by IEC for addressing the security challenges for future digital substations. The subsections of the 62351 standard, namely, IEC 62351-3 to

62351-6 covers the protocol IEC 61850, and other protocols like IEC 60870 IEC 61970, IEC 61968. IEC 62351-7 covers the network management related topics. IEC 62351-8 covers the remote users and role-based operations, which would play an important role in future microgrids. IEC 62351-9 describes the correct and safe usage of security-critical parameters, e.g. passwords, encryption keys. The security architecture is described in IEC 62351-10 and IEC 62351-11 covers security for XML files, which would be extensively used in digital substation communication. In general, IEC 62351 cover data security, communication security and access control. The threat of implementation attacks on embedded system is not covered, even though it is emerging as a crucial threat to embedded security as observed in other domains, for example, in automotive.

Fig. 3: IEC 61850 standard for substation automation.

III. SECURITY ISSUES OF SMART GRID

Classic information security is based on the core assumption that the information remains secret (*confidentiality*), unaltered (*integrity*), accessible (*availability*) and comes from a reliable source (*authenticity*). In the following, a brief overview of attack interfaces and security issues are discussed with the perspective of smart grid.

A. Attack on Data Communication

In the general sense, for a connected computing system, the security threats can originate from the *computing* devices, *storage* devices and *communicating* channels. For example, any of the process buses coming from the bay-level IEDs, either carrying a digital or analog signal, can be corrupted by external devices (by an electro-magnetic field) to convey tampered information to the process-level IEDs. This indicates that every communication happening in the substation must have data authentication to ensure integrity and possibility of packet re-transmission to ensure smooth operation. While authentication ensures that the data integrity is maintained, further encryption modes are required to provide confidentiality. COMTRADE communicates sensitive information in plain ASCII format with no authenticity, leaving a huge scope for tampering data. Such data tampering is already addressed to a great extent in IEC 62351. Thankfully, modern embedded devices [35] are equipped with high-performance security accelerator engines that can enable the protection modes without violating the COMTRADE real-time requirements. The same security features are extended by IEC 62351 for inter-substation and substation to grid communication.

B. Implementation Attacks on Embedded Devices

Implementation attacks are not well studied in the context of smart grid, even though there are potentially malicious activities through unauthorized and stealthy hardware modification as well as Trojan insertion through unreliable equipment supply chain. In principle, every computation, storage or communication, could leak information in form of power dissipation, electromagnetic, acoustic, etc. By correlating these leakages with the transmitted or received data, it is possible to fully recover the sensitive data and/or damage the critical operations. Physical vulnerabilities can also be synchronized with remote attacks, as exemplified with recent attacks on memory devices through Rowhammer bug [33]. We highlight some key implementation security issues, including both *passive* and *active* attacks, which can be exploited in a smart grid. The threats exist at the IED level in a substation or inter-substation and grid level. Furthermore, we point out several sources, so called *attack surfaces*, that can be exploited by a malicious attacker to cause catastrophic consequence.

1) *IED-level Security Issues*: At device/circuit level, it is assumed that an off-the-shelf microcontroller is deployed. For that, the following security threats can occur.

- Passive security threats are prevalent, where the goal is simply to breach the confidentiality. A task running at the device can contain confidential information, e.g., user-level key, which can be revealed through passive side-channels. These include, information leakage of any form, such as, power consumption variation [20] of the device and electrical potential of the device [23]. Such information leakage eventually results in the breach of confidentiality.
- Timing error can be caused by underfeeding the supply voltage or simply regulating the clock frequency or supply voltage downward. Dynamic voltage and frequency control is provided in several modern microcontroller to achieve low-power operations [21]. This attack compromises the functionality of a device, thus affecting the availability of the device.
- Functional error can be caused by $fault_m$ attack. $Fault_m$ attacks attempt to modify a computing/storage element by flipping its value. It is possible to mount a $fault_m$ attack with very high precision by using laser, optical or electromagnetic sources [27]. This will cause a violation of data integrity.
- Off-the-shelf microcontroller undergoes a detailed design, verification and manufacturing flow that may not necessarily secure could be compromised by hardware Trojan [24]. Hardware Trojan can be used for many different purposes, including selective malfunctioning of critical operations.

2) *System-level Security Issues*: In addition to the IED-level threats that can escalate to system-level, there are independent security threats emerging from the following issues at the level of substation.

- For obtaining the system state across the substation, Global Positioning System (GPS) modules are used for accurate time-stamp of a measurement. It is shown that the GPS signals can be spoofed, thus leading to false timestamps [18]. This is an integrity breach, which can result into erroneous

functionality. Reliance on the GPS modules does further expose the substation to potential jamming attacks, which is essentially an attack to undermine availability [36].

- Intra-substation communication via process bus and station bus relies on Ethernet switches, which is essentially a protocol operating on datalink layer and is regarded as insecure network technology [22].

Similar to substation-level security issues, GPS and Ethernet gateway can lead to breach of confidentiality, availability and integrity at the grid-level as well. From an alternative viewpoint, it can be observed that all the attacks either originate at a sensor/storage (e.g., memory corruption), computing (e.g., integrity violation), communication (e.g., GPS jamming), or actuation of the control (e.g., Automatic Gain Control attack [37]). The distribution of attacks in different levels of power substation design is shown in the following Table I.

TABLE I: Security Issues in Power Substation

Location	Exemplary Attack Mode	Security Issue
IED	Differential Power Analysis (DPA)	Confidentiality
	Voltage/Frequency Scaling	Integrity, Availability
	$Fault_m$ Injection	Integrity
	Malware, Trojan	Integrity, Availability
Substation/ Grid	GPS Spoofing	Integrity
	Ethernet Switch Attack	Integrity, Availability
	SCADA Attack (Database, Sync.)	Integrity, Availability
	WLAN Attack (DoS, Spoof)	Integrity, Availability

IV. CASE STUDY

We will show that user-controlled voltage/frequency scaling [21] can lead to the miss of real-time deadlines, causing protection failure in a substation. Essentially, this is an integrity attack, where an event of potential concern is not reported accurately. In the following, we first present a preliminary coverage of fault detection followed by the experiment. A prolonged attack of this nature can also lead to blackout, thus extending to availability.

A. Fault Detection at Distribution Level

Accurate fault detection and isolation is very critical in reliable power systems operation. Failure or delay in fault detection can create large damage at network level, and eventually create blackout situation. Depending on the type of the fault, the commonly used protection techniques like instantaneous overcurrent, non-directional time overcurrent, directional instantaneous and/or time overcurrent, step time overcurrent, inverse time distance, zone distance, pilot relaying are used.

At distribution level (< 35 kV), typically non-directional time overcurrent and instantaneous overcurrent protection schemes are used. A typical fault signal is shown in Fig. 4, which was measured in a real distribution network [38]. In Fig. 4, the current is measured at 2.5 kHz sampling frequency, and the fault inception happens around the 80th sample. After that, due to the fault, there is overcurrent (over than nominal) in the system. However, the relay has to differentiate between overcurrent due to fault and due to load change. This is required for robust fault detection without any false alarm.

The principle for fault detection is that load change is temporary, but during fault, overcurrent would occur for long duration. Therefore, for accurate detection, one has to judge overcurrent vs time (see Fig. 4 [38]). From the fault inception point, i.e., 80th sample to about 1 cycle (in 50 Hz system, 1 cycle is 20 ms), the relay monitors the overcurrent. As the overcurrent is persistent, it recognizes it as fault, and issues a ‘trip’ command to the circuit-breaker in the next cycle. The circuit-breaker, which waits for the relay’s instruction, starts opening at around 200th sample, after receiving the ‘trip’ command. It successfully isolates the whole system in about 10 ms (half cycle).

Fig. 4: Overcurrent signal and fault detection in power systems.

B. Standard & Operation for Overcurrent Fault Detection

The fault detection principle is implemented in the ‘Inverse Definite Minimum Time (IDMT)’ curve, covered by the IEC 60255 standard [29]. This is shown in Fig. 5. Equation (1) is the corresponding mathematical description, where t is operating time, K is the time multiplier, I , I_{set} are the measured and nominal current, α and β are two parameters. Typical values of the α and β for the different types of IDMT curves are given in Table II. By changing the α and β values, different IDMT curves (see Table II) with different slopes could be incorporated. This is typically configured as required by the utilities for faster or slower protection operation.

For this case-study, very inverse type curve is used, with $\alpha = 1.0$, $\beta = 13.5$. These parameters, critical for estimating the time duration i.e., for fault duration, are typically user configurable parameters in the microprocessor-based relay.

$$t = \frac{K\beta}{\left(\frac{I}{I_{set}}\right)^\alpha - 1}. \quad (1)$$

TABLE II: Values of α , β in IDMT Curves

Type of curve	α	β
Normal Inverse	0.02	0.14
Very Inverse	1.0	13.5
Extremely Inverse	2.0	80.0
Long-time Inverse	1.0	120.0

Using the equation (1), and Fig. 5, and time-multiplier $K = 0.1$, for an overcurrent magnitude of 10, i.e., 10 times fault, we get the operating time as 0.15s. However, for the same setting, if the overcurrent magnitude is lower, e.g., 5 times, the

Fig. 5: Time-Overcurrent curve for overcurrent fault detection.

operating time would be longer, 0.34s. Similarly, the attacker might change the curve types (see Table II) by changing the α and β values, causing the protection failure.

C. Relay Compromise for Protection Failure

Microprocessor-based numerical relays are used at transmission and distribution levels. However, at the transmission level (typically $> 35kV$), the computational requirement is higher with synchronized measurements of voltage, current, GPS signals, requiring a faster processing. Hence, typically FPGA, GPU, etc. are used in the transmission level relays by the major manufacturers. However, at the distribution level, typically only current is used, with not so much fast processing requirement. Cost is also a significant factor at the distribution level. Therefore, the cost of the distribution relays are typically 5-10 times lower than the transmission level ones. Typically the relays use 2-3 kHz of sampling frequency for the measuring the current signals, and for executing the logic decision, typically 60 MHz range clocks are used [30]. All modern microprocessor-based relays provide digital ‘trip command signal’ to the CB.

It is essential that the CB opens the circuit in correct time. For large overcurrent fault, CB should trip as quickly as possible, while for low overcurrent, it should take longer time, and should not trip in case fault is temporary. The relay’s decision is critical, which depends on the time evaluation, as discussed above. Thus, by compromising the microprocessor-based relay, this decision could be altered, e.g., in case of a critical large overcurrent fault, the trip command could be delayed, causing the CB not to trigger, creating large physical damage to the power substation and grid. Otherwise, unwanted trip commands can be created to wrongly open the CB, thereby creating artificial power outage. Such events if created in a chain fashion could lead towards artificially created power blackout, which could have devastating consequence for the whole grid.

D. Case Study on $Fault_m$ Injection Attacks

Fault detection and isolation is a time crucial task in any power system. The brain of this fault detection system is the aforementioned relay. A relay is typically composed of a microcontroller and supporting analog-digital converter

circuitry. Few relays can contain FPGA or dedicated ASIC. In the following, we consider a microcontroller based monitor, typically an ARMv7, type of processor used in the distribution relays which are much lower in cost than transmission level relays [30]. Nevertheless, such attacks on desktop and server level processors is also known [33].

The microcontroller monitors the overcurrent values in a digital format and reacts with a trip signal if abnormal conditions are sensed. The ratio of overcurrent to reaction time is defined in IEC 60255 standard. The microcontroller should react before the worst-case reaction time. In this context, the reaction time is computed by a static piece of software which is flashed into the microcontroller. The software which implements the defined standard is not usually updated during the lifetime of the relay. To meet the required deadline of reaction time, the natural choice of a designer is a look-up table (LUT) based implementation. In such a LUT-based implementation, the reaction time is pre-computed based on parameters and stored in the memory. An example of such LUT based code is shown in Tab. III. The example code assumes that the parameters are predefined and static for a given application. For sake of simplicity, α is assumed to be unity.

Fig. 6: Malicious $Fault_m$ Injection setup for ARM based smartcard by underfeeding

Malicious FIA is a class of implementation attacks which are performed by injecting computation errors in the target. The computation error can be done by invasive or non-invasive techniques. Note that $fault_m$ injection in a device should not be confused with the faults in a power system. For sake of clarity, we interchangeably use the term error and $fault_m$ to define error injected for a FIA. FIA can be global or local in nature and can involve invasive or non-invasive intervention. Global errors are easy to mount, require rather cheap equipment, however, they lack precision. For precise FIA, local methods like laser-based injection or electromagnetic pulse injection are used. These methods can inject precise errors and require high expertise and expensive equipment. In the following, we consider low-cost injection technique which is non-invasive and does not require strong assumption on the adversary capabilities.

Typical low-cost techniques to inject errors in a device are underfeeding (lower supply voltage) or overclocking or glitch on voltage/clock line. Such techniques are even previously demonstrated to work on commercial applications like pay-TV smart cards. Such FIA were widely demonstrated on microcontroller [31], [32], FPGA and ASIC [34].

Specifically the work presented in [31], [32] is demonstrated on ARM i.e. our target of interest. When an ARM microcon-

TABLE III: ARM7 Assembly pseudocode for *LUT-based IDMT*. Instructions in **Bold** denotes memory access.

#	Instruction
1	VLDR S0, [input]
2	VLDR S1, [I]
3	VDIV S0, S0, S1
4	VMOV S1, # (16 * 2 ⁻⁴) // $\alpha = 1$
5	BL [power(S0,S1)]
6	VSUB S0, S0, S1
7	VLDR S1, [K]
8	VLDR S2, [b]
9	VMUL S1, S1, S2
10	VDIV S0, S1, S0
11	VSTR S0, [output]

Fig. 7: Fault Injection Attack Experiments on ARM executing IDMT code

troller is subjected to low-cost FIA methods like underfeeding, the instructions involving memory access are most prone to errors. This means any software involving **LOAD** or **STORE** instruction to program memory, are worst hit by such FIA. The main cause of such errors is that memory access in a typical microcontroller requires much higher power than arithmetic or logical operations. When the microcontroller is underfed, these memory access are the worst hit and would lead to errors. A typical setup for such FIA is shown in Fig. 6. Now coming back to the example code in Tab. III. This code is composed of 11 instructions out of which 6 are either **LOAD** (**VLDR**), **STORE** (**VSTR**) or **Branch** (**BL**). Therefore, over 54.5% of the code is vulnerable to such low-cost FIA. This ratio further increases for a stronger adversary. For instance,

with precise methods like laser injection, where the adversary has the capability to either skip instruction execution or change values in the register, the whole code becomes vulnerable. In the following, we focus on low-cost techniques as it can be performed by a less equipped adversary.

We demonstrate the impact of these low-cost FIA by code analysis. In particular, we observe the impact of FIA on the IDMT curve (from Fig. 5). The first analysis is done under data change $fault_m$ model by underfeeding. As previously stated, when the core of the microcontroller is underfed, the memory operations are worst hit. Actually, the core is unable to provide enough power (current) to the memory decoder, which result in a wrong address decoding. Thus, the instruction would load or store from/to a wrong address i.e. further operations are performed on wrong data. Although with underfeeding, the latched address will always be lower than the correct address, i.e. only bit resets can occur on the address, however, the content of the memory at the wrongly latched address can be considered random. Thus we assume that a random wrong value is loaded from or stored in the memory under FIA.

The code analysis under this $fault_m$ model is shown in Fig. 7a. The result is obtained after averaging results of 100 independent experiments. Similarly, the underfeeding can also impact the instruction decoder. If the ARM core is fed with lower power voltage, the instruction decoder may not be able to draw enough current, resulting in wrong decoding. Wrong decoding of the instruction would lead to execution of a wrong instruction i.e. a different operation is performed on the given data. This $fault_m$ model is commonly known as instruction change $fault_m$ model. As the instruction code for different operations will be different on different processors, we randomly modify the underlying instruction for this code analysis. This code analysis averaged over 100 experiments is shown in Fig. 7c. Similarly, the instruction decoding may result in skipping instruction (i.e., wrong instruction decoding leading to NOP operation). Similar experimental result is shown in Fig. 7e.

Observing Fig. 7a, Fig. 7c, and Fig. 7e, the impact of a low-cost error FIA is evident in causing a shift in IDMT curve. Under the current analysis, the results observe an increase in the reaction time, which can cause serious damages to the power substation. For example in Fig. 7a, an overload which should have caused the relay to cut-off in 10 seconds, under FIA, reacts in 16 seconds. This exposure of extra 6 seconds to over-current can cause serious damage to the system. In fact, instruction change $fault_m$ model can also cause false positives for certain over-current cases. The impact is even serious for smaller value of $K = 0.1$ as shown in Fig. 7b, Fig. 7d and Fig. 7f. Besides the overall time delay, the time-multiplier K in eq. (1) also plays a significant role. Lower value of K is used for invoking faster protection operation, and vice versa, which generally depends on the utility practice. Therefore, the impact is even serious for sensitive applications with smaller value of $K = 0.1$.

In order to protect from such attacks, the underlying countermeasures are based on redundancy which incurs a computation time overhead $3 \times$ [32]. However, such overhead can not be suitable owing to strict requirement on the reaction

time. Protecting against data change $fault_m$ requires use of error correction encoding. However, as reported in [40], such countermeasures incur huge overhead of $\approx 8 - 10\times$, we consider it out of scope for such time critical applications.

We further study one of the main countermeasure proposal against instruction skip attacks as proposed in [39]. The protection is achieved by instruction redundancy and use of idempotent as well as separable instructions. For idempotent instructions, the destination of the operand is independent of the source operand which allow easy duplication at the instruction level without affecting the flow like *VLDR*, *VMOV*, *VSTR* etc. For separable instructions, the source and destination register are the same, but it can be simply changed to idempotent instructions like *VMUL*, *VSUB* etc. We implemented the same code to resist single instruction skip using idempotent and separable instructions. The performance overhead was reported between $2.5-3\times$ depending on the chosen parameter. This high performance overhead (or computation time) can have serious bottlenecks in time critical real time systems like the underlying IED.

Fig. 8: $Fault_m$ Injection Attack Experiments on ARM executing IDMT code with countermeasure

Figure 8a, 8b and 8c show the results of FIA on the protected code. As the protection is designed to resist single instruction skips, the protected code show no penalty in the reaction time which is always correctly reported. However, in terms of data change and instruction change attack, the proposed protection only works marginally, while still increasing reaction time. While protection against data change are known (even though at high overhead), protections against instruction change $fault_m$ s is an open problem. Alternative protection approaches require use of physical sensors [41] to prevent FIA while keeping the reaction time in acceptable limits. Such countermeasure will increase the cost of microcontroller and thus also the IED.

E. Case Study on Malicious Hardware Attacks

Fig. 9: Malicious Trojan Attack

Hardware Trojans [24], [25] are threats originating from the outsourcing trend adopted in semiconductor industry. Here, the industry might introduce several untrusted players in the supply chain leading to birth of hardware Trojans. Any unauthorized modification of the physical hardware to realize a potential malicious function falls under this category. The malicious function can be in the form of information leakage, malfunction, denial of service, diminished reliability etc. Hardware Trojan can be introduced at each step right from initial specification phase to final fabrication and testing. Owing to its wide variety, it is not possible to find a unique solution which detects all kind of Trojans.

In this case study, we assume that the IEDs are based on embedded devices which might be maliciously modified. A typical hardware Trojan has two components: *trigger* and *payload*. While trigger activates a dormant hardware Trojan, payload realises the malicious function. Based on the kind of trigger, payload and insertion point, there are several classes of Trojans [25]. We assume the trigger to be a *time-bomb* i.e. the dormant hardware Trojan that activates itself sometime during the lifetime of the product. This is indeed a valid assumption, as IEDs are designed to stay several years in function and updates/patches are very rare. The hardware Trojan payload is a malicious instruction set extension (ISE) [26]. When activated, a processor instruction will be changed to a malicious one, by swapping (unused) opcode, leading to a wrong computation. The functioning of the present hardware Trojan case study is oriented towards FIA, however, the scope can be much beyond and extend to several applications.

For the exploit, we refer to Table III. The attack target is statement 5 i.e. *VMOV* instruction. Based on the documentation, the *VMOV* operation could only support loading some set of numbers (within the range of $\pm n \cdot 2^{-r}$ for $16 \leq n \leq 31, 0 \leq r \leq 7$). In this case, the hardware Trojan could simply modify the value being loaded to the register, and based on Eq. (1), the attacker can modify the value α . On the physical level, such modifications require simple wiring and can be easily passed undetected. The attack results (averaged over 100 independent executions) is highlighted in Fig. 9. The Trojan is smartly designed to have minimal impact at lower/regular load and deviate largely for higher load. This could slowly degrade the performance over time while being hard to detect.

Protection against hardware Trojan is even harder than protection against FIA. As the Trojans are designed to be

mostly dormant, their existence is not known and thus harder to detect. Nevertheless, some methods can be applied for detections, like [42], [25] etc. Upon detection, the simplest method is to replace the malicious component. Currently, run-time solutions to bypass a Trojan in a malicious device are not widely known.

V. CONCLUSION

Modern and future substations are aimed to be more interconnected, leveraging standards like IEC 61850-9-2, and abstract data models like, GOOSE, MMS, SMV [5], for wide area monitoring, faster outage recovery, blackout prevention, distributed state estimation, etc. This would require strong focus on information security, both at system level as well as at embedded device level. While IEC 62351 solves several security issues, however, no emphasis is given on physical security. In this paper, we have focused on impact of implementation attacks on smart grids, specially on substation level. A general overview of the threats is provided followed by two distinct case studies to highlight the impact of these threats. The impact of any of the exploit is shown to affect integrity and availability of the smart grid. Countermeasures to implementation attacks are also studied. In the future, it will be an interesting topic, to design efficient countermeasures in context of IED and substation protection.

REFERENCES

- [1] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon." *IEEE Security & Privacy*, 9(3), 49-51, 2011.
- [2] Idaho National Laboratory, "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector." August, 2016.
- [3] P. McDaniel, S. McLaughlin, "Security and privacy challenges in the smart grid." *IEEE Security & Privacy*, 7(3), 2009.
- [4] A. Ukil, R. Zivanovic, "Automated Analysis of Power Systems Disturbance Records: Smart Grid Big Data Perspective," *IEEE Innovative Smart Grid Tech. Conf.-ISGT ASIA*, Kuala Lumpur, Malaysia, 2014.
- [5] Int. Elet. Comm. (IEC), "Communication networks and systems in substations Part 9-2: Specific communication service mapping (SCSM) Sampled values over 390 ISO/IEC 8802-3," IEC 61850-9-2:2004(E), 2004.
- [6] P. Parikh, T. Sidhu, A. Shami, "A Comprehensive Investigation of Wireless LAN for IEC 61850 Based Smart Distribution Substation Applications," *IEEE Tr. Industrial Informatics*, vol. 9, no. 3, pp. 1466-1476, 2013.
- [7] Int. Elet. Comm. (IEC), "Power systems management and associated information exchange - Data and communications security," IEC 62351, 2016.
- [8] B. Moussa, M. Debbabi, C. Assi, "A Detection and Mitigation Model for PTP Delay Attack in an IEC 61850 Substation," *IEEE Tr. Smart Grid*, 2017. (10.1109/TSG.2016.2644618)
- [9] M. Cheminod, A. Pironti, R. Sisto, "Formal Vulnerability Analysis of a Security System for Remote Fieldbus Access," *IEEE Tr. Industrial Informatics*, vol. 7, no. 1, pp. 30-40, 2011.
- [10] T. Vollmer, M. Manic, "Cyber Physical System Security With Deceptive Virtual Hosts for Industrial Control Networks," *IEEE Tr. Industrial Informatics*, vol. 10, no. 2, pp. 1337-1347, 2014.
- [11] J. Hong, C. C. Liu, M. Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations," *IEEE Tr. Smart Grid*, vol. 5, no. 4, pp. 1643-1653, 2014.
- [12] Y. Zhang, L. Wang and Y. Xiang, "Power System Reliability Analysis With Intrusion Tolerance in SCADA Systems," *IEEE Tr. Smart Grid*, vol. 7, no. 2, pp. 669-683, March 2016.
- [13] J. Hu and A. V. Vasilakos, "Energy Big Data Analytics and Security: Challenges and Opportunities," *IEEE Tr. Smart Grid*, vol. 7, no. 5, pp. 2423-2436, Sept. 2016.
- [14] I. K. Song, S. Y. Yun, S. C. Kwon and N. H. Kwak, "Design of Smart Distribution Management System for Obtaining Real-Time Security Analysis and Predictive Operation in Korea," *IEEE Tr. Smart Grid*, vol. 4, no. 1, pp. 375-382, March 2013.
- [15] Y. Liu, H. Xin, Z. Qu and D. Gan, "An Attack-Resilient Cooperative Control Strategy of Multiple Distributed Generators in Distribution Networks," *IEEE Tr. Smart Grid*, vol. 7, no. 6, pp. 2923-2932, Nov. 2016.
- [16] K. C. Sou, H. Sandberg and K. H. Johansson, "Data Attack Isolation in Power Networks Using Secure Voltage Magnitude Measurements," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 14-28, Jan. 2014.
- [17] S. Tan, W. Z. Song, M. Stewart, J. Yang, L. Tong, "Online Data Integrity Attacks Against Real-Time Electrical Market in Smart Grid," *IEEE Tr. Smart Grid*, 2017. (10.1109/TSG.2016.2550801)
- [18] Z. Zhang, S. Gong, A. D. Dimitrovski and H. Li, "Time Synchronization Attack in Smart Grid: Impact and Analysis," *IEEE Tr. Smart Grid*, vol. 4, no. 1, pp. 87-98, March 2013.
- [19] D. Wei, Y. Lu, M. Jafari, P. M. Skare and K. Rohde, "Protecting Smart Grid Automation Systems Against Cyberattacks," *IEEE Tr. Smart Grid*, vol. 2, no. 4, pp. 782-795, Dec. 2011.
- [20] P. C. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis," In Proceedings of CRYPTO, pp. 388-397, 1999.
- [21] A. Mallik, B. Lin, G. Memik, P. Dinda, R. P. Dick, "User-Driven Frequency Scaling," *IEEE Comp. Arch. Let.*, vol. 5, no. 2, pp. 16, 2006.
- [22] E. Vyncke, C. Paggen, *LAN Switch Security: What Hackers Know About Your Switches*. Cisco Press, 2007.
- [23] D. Genkin, I. Pipman, E. Tromer, "Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs. Cryptographic Hardware and Embedded Systems," *Lecture Notes in Computer Science*, vol. 8731, pp. 242-260, 2014.
- [24] G. T. Becker, F. Regazzoni, C. Paar, W. P. Burleson, "Stealthy dopant-level hardware trojans. In Proceedings of CHES, pp. 197-214, 2013.
- [25] M. Tehranipoor, M., F. Koushanfar, A survey of hardware trojan taxonomy and detection. *IEEE Design & Test of Computers*, 27(1), 2010.
- [26] S. T. King, J. Tucek, A. Cozzie, J. Grier, W. Jian, Y. Zhou, "Designing and Implementing Malicious Hardware. LEET, 8, 1-8, 2008.
- [27] N. Moro, A. Dehbaoui, K. Heydemann, B. Robisson, E. Encrenaz, "Electromagnetic Fault Injection: Towards a Fault Model on a 32-bit Microcontroller," In proc. workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), pp. 77-88, 2013.
- [28] IEEE, "IEEE Standard Common Format for Transient Data Exchange," Std. 37.111-1991, ver. 1.8, 1991.
- [29] Int. Electrotechnical Commission (IEC), "Standard for Measuring Relays and Protection Equipment," no. 60255, 2008.
- [30] A. Ukil, V. H. Shah, B. Deck, "Fast Computation of arctangent Functions for Embedded Applications: A Comparative Analysis," 20th IEEE Int. Symposium Industrial Electronics ISIE'11, Gdansk, Poland, Jun. 2011.
- [31] A. Barenghi, G. Bertoni, L. Breveglieri, M. Pellicoli, and G. Pelosi, "Low voltage fault attacks to aes and rsa on general purpose processors," *Cryptology ePrint Archive*, Report 2010/130, 2010.
- [32] A. Barenghi, L. Breveglieri, I. Koren, G. Pelosi, and F. Regazzoni, "Countermeasures against fault attacks on software implemented AES: effectiveness and cost," In Proc. 5th Workshop on Embedded Systems Security (WESS), pp.7, ACM 2010.
- [33] M. Joye and M. Tunstall, "Exploiting the DRAM rowhammer bug to gain kernel privileges," Black Hat 2015.
- [34] N. Selmane, S. Bhasin, S. Guille, J. L. Danger, "Security evaluation of application-specific integrated circuits and field programmable gate arrays against setup time violation attacks," *IET Information Security*, vol. 5, no. 4, pp. 181-190, 2011.
- [35] G. Panic, O. Stecklina, and Z. Stamenkovic, "An Embedded Sensor Node Microcontroller with Crypto-Processors," In *Sensors*, vol. 16, no. 5, pp. 607, Basel, 2016.
- [36] GPS Jamming, Available Online. <http://www.gps.gov/spectrum/jamming/>
- [37] R. Tan et al., "Optimal False Data Injection Attack against Automatic Generation Control in Power Grids," *International Conference on Cyber-Physical Systems (ICCPS)*, 2016, pp. 1-10.
- [38] A. Ukil, B. Deck, V. H. Shah, "Current-Only Directional Overcurrent Protection for Distribution Automation: Challenges and Solutions," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1687-1694, 2012.
- [39] S. Patranabis, A. Chakraborty, and D. Mukhopadhyay, "Fault Tolerant Infective Countermeasure for AES," In *SPACE 2015*: 190-209
- [40] J. Breier and X. Hou, "Feeding Two Cats with One Bowl: On Designing a Fault and Side-Channel Resistant Software Encoding Scheme," in *CT-RSA 2017*: 77-94
- [41] W. He, J. Breier, and S. Bhasin, "Cheap and Cheerful: A Low-Cost Digital Sensor for Detecting Laser Fault Injection Attacks," in *SPACE 2016*: 27-46
- [42] Y. Jin, and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *HOST 2008*: 51-57

- [43] S. Pan, T. Morris and U. Adhikari, "Classification of Disturbances and Cyber-Attacks in Power Systems Using Heterogeneous Time-Synchronized Data.," in IEEE Transactions on Industrial Informatics, vol. 11, no. 3, pp. 650-662, June 2015.
- [44] U. Adhikari, T. Morris and S. Pan, "Applying Hoeffding Adaptive Trees for Real-Time Cyber-Power Event and Intrusion Classification.," in IEEE Transactions on Smart Grid, vol. PP, no. 99, pp. 1-1.
- [45] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall and C. Whelan, "The Sorcerer's Apprentice Guide to Fault Attacks.," in Proceedings of the IEEE 94(2): 370-382 (2006).

Anupam Chattopadhyay (S'97-M'10-SM'14) received his B.E. degree from Jadavpur University, India, MSc. from ALaRI, Switzerland and PhD from RWTH Aachen in 2000, 2002 and 2008 respectively. From 2008 to 2009, he worked as a Member of Consulting Staff in CoWare R&D, Noida, India. From 2010 to 2014, he led the MPSoC Architectures Research Group in RWTH Aachen, Germany as a Junior Professor. Since September, 2014, he is appointed as an assistant Professor in SCSE, NTU

and also holds an honorary adjunct appointment at SPMS, NTU. In the past, he was visiting Professor at EPFL, Switzerland and Indian Statistical Institute, Kolkata.

His research advances has been reported in more than 100 conference/journal papers (ACM/IEEE/Springer), multiple research monographs and edited books (CRC, Springer) and open-access forums. Together with his doctoral students, Anupam proposed novel research directions like, domain-specific high-level synthesis for cryptography, high-level reliability estimation flows for embedded processors, generalisation of classic linear algebra kernels and multi-layered coarse-grained reconfigurable architecture. Anupam's research in the area of emerging technologies has been covered by major news outlets across the world, including Asian Scientist, Straits Times and The Economist. Anupam received Borchers's plaque from RWTH Aachen, Germany for outstanding doctoral dissertation in 2008 and the nomination for best IP award in DATE 2016.

Abhisek Ukil (S'05-M'06-SM'10) received the B.E. degree in electrical engineering from the Jadavpur Univ., Kolkata, India, in 2000 and the M.Sc. degree in electronic systems and engineering management from the Univ. of Bolton, Bolton, UK in 2004. He received the Ph.D. degree from the Pretoria (Tshwane) University of Technology, Pretoria, South Africa in 2006, working on automated disturbance analysis in power systems.

Currently, he is Senior Lecturer in the Dept of Electrical and Computer Engineering, at University of Auckland, New Zealand. From 2006-2013, he was Principal Scientist at the ABB Corporate Research Center, Baden-Daettwil, Switzerland, where he led several projects on smart grid, protection, control, condition monitoring, including first world-wide prototype of directional protection relay using only current for smart grid applications. From 2013-2017, he was Assistant Professor in the School of EEE, Nanyang Technological University, Singapore, where he led a group of 20 researchers with several industrial collaborations. He is inventor of 10 patents, and author of more than 130 refereed papers, a monograph, 2 chapters. His research interests include smart grid, DC grid, protection & control, energy efficiency, renewable energy & integration, energy storage, condition monitoring.

of machine learning and data mining approach for enhancing side-channel analysis, as well as for effective hardware trojan detection.

Dirmanto Jap is currently a Research Scientist in Temasek Laboratories, Nanyang Technical University Singapore. He previously received his B.Sc. in Mathematics from NTU in 2011, and his PhD in Mathematics, focusing on physical attacks on block cipher, from NTU in 2016. His main research interests are in the area of analysis of leakage detection and leakage modelling for side-channel attacks, analysis and investigation of fault attacks, including practical EM/laser fault injection, and application

Shivam Bhasin is a Senior Research Scientist in Temasek Laboratories, Nanyang Technical University Singapore since 2015. His research interests include embedded security, trusted computing and secure designs. He received his PhD from Telecom Paristech in 2011, Master's from Mines Saint-Etienne, France in 2008 and Bachelor's from UP Tech, India in 2007. Before NTU, Shivam held position of Research Engineer in Institut Mines-Telecom, France. He was also a visiting researcher at UCL, Belgium (2011) and Kobe University (2013). He has co-authored several publications at recognized journals and conferences. Shivam served in TPCs of several conferences, regularly reviews journal/ conference articles and presented multiple invited seminars/tutorials in prestigious venues. Some of his research now also forms a part of ISO/IEC 17825 standard.