An Integrated Solution for Developing SCADA System towards Smart Electric Grid

Yahia Bahaa Hassan
Computer Department
Wadi Technical College-TVTC
Kingdom of Saudi Arabia
Email: yhassan [AT] tvtc.gov.sa

Ashraf Aboshosha
Radiation Eng. Dept., NCRRT
Atomic Energy Authority
Cairo, Egypt

Nabil Litayem
Wadi College of Science
Setam University
Kingdom of Saudi Arabia

Yahia ElSaid
Electrical Engineering Dept.,
Menya University
Menya, Egypt

Abstract— **this paper presents a proposed strategy to embed the reactive power compensation system into Supervisory Control and Data Acquisition (SCADA) systems for advanced smart grid. To connect the suggested regulator of power factor to SCADA system, the ordinary regulators will be replaced by new power factor regulators usingMSP430 microcontrollers as a Remote Terminal Unit (RTU). A case study will be showed for SCADA's project of the Middle Egypt Electricity Distribution Company (MEEDCO) that actually has been implemented since 2005. This paper also introduces quark hashing algorithm for MSP430 microcontroller to achieve a secure smart grid.**

***Keywords- power factor regulators; MSP430; RTU, hash-based authentication*.**

I. INTRODUCTION

Electricity distribution companies provide the infrastructure to connect customers to the electric grid. The grid of these distribution companies suffer from poor power quality problems like high reactive power burden, unbalanced load excessive neutral current and voltage distortion [1]. To optimize the control of reactive power compensation, the power factor regulator with variable capacitor banks are designed. For better control, SCADA systems have been implemented by many electric utilities for years[2]. SCADA can provide information in a real-time environment that identifies problems as they occur and can take corrective action when assistance is needed [3]. As the SCADA system of MEEDCO works so far and coupling the Intelligent Electronic Devices (IED) with SCADA provide a wealth of useful information. Therefore, for better performance, the proposed regulator of power factor (IED) using MSP430 microcontroller should be monitored and controlled by SCADA system. Extending a power factor regulator at the end user to the SCADA system leads to an improvements for grid reliability and provides visibility into information of critical load, asset management, reduced costs of operations and maintenance and customer satisfaction. The remainder of the paper is organized as follows. Section 2 shows a background for MEDDCO's SCADA system, MSP430 microcontroller, security for smart grid and hashing algorithms. Section 3 presents the suggested strategy to embed the new reactive power compensation systems into MEEDCO's SCADA system.

II. BACKGROUND

A. MEDDCO's SCADA system

Various voltage levels of the distribution grid are used: High Voltage (HV 66kV), Medium Voltage (MV11kV to 22kV) and Low Voltage (LV 400V or 230V). The majority of customers are connected to the LV network with single phase or three-phase connections. MEEDCO covers five governorates in upper Egypt. MEEDCO is providing almost 9682 [MWh/year] for approximately 3151860 customers through 21212 km of medium voltage lines and 35114 km of low voltage lines. The company provides power supply coming from the Transmission Company to subscribers and make connections for them. MEEDCO is continually making an effort to improve the performance of the distribution network through benefiting from advanced technologies. In 2002, the company moved to implement a SCADA project to cover Menya governorate and Assiut governorate. The implementation of the project took 3 years to finish and it is still working so far. The total number of measured, monitored and controlled points by the control center is 29661 points. The SCADA system of MEEDCO includes some of the transformer stations of Transmission Company, some of the distribution transformers (kiosks) and most of the distribution panels that include incoming feeders, outgoing feeders, bus tie, digital relays, digital meters and charger. In the SCADA project of MEDDCO, The data from remote locations like kiosks, distribution panels and transformer stations of Transmission Company are collected by RTUs and sent to the LAN of control center. The control center consists of servers, workstations, routers, switches, printers and large displays. The previous components of the control center are connected and organized in the star topology form.

TABLE I. DATA OF SCADA PROJECT FOR MENYA SECTOR.

List	Distribution Panels	Transformer Stations	kiosks	Total
Numbers	27	10	119	-
Incoming feeders	102	22	-	124
Outcoming feeders	287	160	-	447
Monitored Points	12862	2596	1190	16648

The servers and workstations of control center use UNIX as an operating system. MEEDCO consists of five sectors for electricity distribution. Our case study will focus on Menya sector, which is the supplier of electricity in Menya governorate that contains nine large cities with an area of 32279 km2. Table 1 illustrates the data of SCADA project for Menya sector.

B. MSP430 MICROCONTROLLER

Known for its low cost and low-power consumption, MSP430 from Texas Instruments (TI) is a family of 16-bit microcontrollers commonly used in wireless sensors/actuator networks and metering applications [4]. The utilization of this Microcontroller Unit (MCU) becomes too broad due to the introduction of new innovative features apart from low-cost and low power. Texas Instrument has a wide range of MSP430 flavors designed for diverse applications such as smart metering, wireless communication, motor control, personal health care, etc. For each application of MSP430 flavor Texas Instrument has a development or evaluation board.The most successful development boards are MSP-EXP430F5529, eZ430 Chronos [5] and MSP430 Launchpad [6].

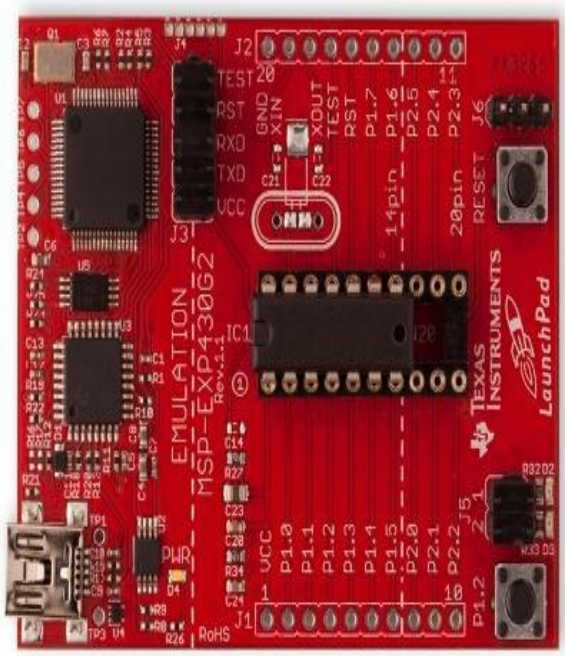

Figure 1. MSP-EXP430G2 LaunchPad

MSP430 has the advantage of the complete software ecosystem that ranging from powerful development environment such as IAR, Code Composer Studio and Energia to very appropriate software stack such as SimpliciTI [7] or Capacitive Touch sense library. On the other hand, solutions of TI MCU are also very cost effective and scalable. The wide variety of available TI MCU offers the possibility to switch between various TI MCUs. In2010, Texas Instrument has expanded MSP430 portfolio by introducing MSP430 Value Line. This new low cost family starting at 0.25$, is essentially intended to replace the old 8-bits MCU. To promote this new family, TI has introduced the MSP-EXP430G2 LaunchPad as seen in figure 1. This evaluation board is a low cost, very valuable evaluation platform. Launchpad can be used to develop applications for the overall Value Line MSP430 microcontrollers.

C. SECURITY FOR SMART GRID

Given the recent paradigm shift towards rapid and large-scale deployment, the attack surface is rapidly increasing [8]. A cyber-attack is an attempt by hackers to damage or destroy a computer network or system. As the power grid evolves the smart grid, smart grid components will have to be secured against cyber-attacks to prevent fraud, unauthorized access, the corruption of data or to counter threats to network operation [9]. The basic security requirement is to guarantee the secure exchange of messages between the nodes in the system. The power system has suffered from many attacks which have raised the question regarding the security vulnerabilities and its large scale impact on the critical power system infrastructure [10]. Earlier SCADA system was based on an event-driven operating system and basic serial communications. This kind of solution does not have any security threats because complete physical isolation SCADA devices from any external intrusion. Thanks to Moor Law, SCADA applications become cost effective and ubiquitous. Such solution is based on standard hardware, open source software and open protocols. Any compromise in SCADA system security can have serious consequences [11]. During this last decade, many research works have studied the security of such system and proposed innovative solutions, [12], [13], and [14]. In this paper, we introduce an authentication solution using a hashing algorithm for MSP430 microcontroller as a SCADA RTU. In our application, hashing algorithm will be used to protect the authenticity of transmitting information and to offer a reliable authentication mechanism between MEEDCO's control center and the suggested power factor regulators. Hashing algorithms [15] are commonly used in computing, their main purpose is to map a variable message length to a fixed length message. The hashing algorithms are available to adopt appropriate implementation as an integrity check and authentication solution for our SCADA system. Our system is regarded as a practical example of the physical platform for doing just proof

of concepts. In fact, integrity verification and authentication are a common need for all modern smart objects. Several academic studies have produced a respectable number of hash algorithms from various different research schools and having various qualities and characteristics. Each hash algorithm may be appropriate for a specific application and a particular implementation platform. On the other hand, the choice of this algorithm is guided by the quality of the reference implementation, the available profiles, the associated resources and scientific publications. During the first phase of investigation, we found the large number of hash algorithms. However, much suffering intolerable weakness in the associated facilities is sometimes limited to implementations in C or Pascal. In [16] we have grouped the most interesting hashing algorithms available with a free implementation. In our study Photon, Spongent and QUARK are very interesting for our application. In fact, these three algorithms can meet the needs of our application while respecting the constraints of the choosing platform. The algorithms of Photon [17] and Spongent [18] are largely inspired by the QUARK algorithm which was published for the first time in [19]. According to the results of [17] and [20], QUARK is most suitable for software implementation. On the other hand, the QUARK algorithm has a very good documentation of a software and hardware implementation and a respectable number of academic publications. Furthermore, QUARK is a lightweight hash algorithm with four profiles that can be suitable for different levels of performance and safety. This prompted us to investigate the levels of performance and memory footprints of different profiles for QUARK algorithm.

III. THE PROPOSED STRATEGY TO EMBED THE NEW REACTIVEPOWER COMPENSATION SYSTEMS INTO MEEDCO'S SCADA SYSTEM

1. IMPLEMENTING THE POWER FACTOR REGULATOR IN LOW VOLTAGE NETWORKS

The Menya sector provides electricity to a very large number of participants. A slice of those participants nominates senior participants as an indication of their large consumption of electricity, such as factories, stations of lifting water, sewage plants, hospitals and great business shops. These loads are mostly inductive in nature and they create serious power quality problems for senior participants like low power factor, increased load current and reduction in voltage. To solve these problems, Menya sector has applied a control system for power factor compensation. The next figure presents common power factor compensation arrangement used in commercial power systems. The scheme consists of one or more breaker switched capacitor units along with an intelligent controller for power factor correction and transformers of current (CT)

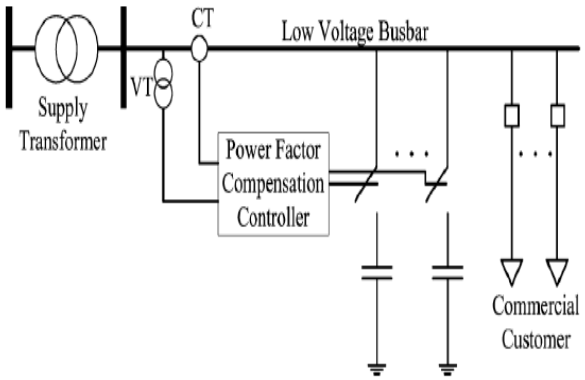

Figure 2. The arrangement of power factor compensation system for low voltage power systems

and voltage (VT) which are connected at the low side of the supply transformer. These banks often include three to nine capacitor units connected in three-phase grounded-wye, ungrounded-wye, or delta configurations [21].The regulator automatically responds to changing power factor by closing or opening the internal relays of contractors who add or subtract capacitor banks on the line. In Menya sector, many power factor regulators have been installed in various locations. But these regulators up till now use ordinary microcontrollers and still not connecting to the control center of Menya sector. With advances in integrated circuit technology, MCUs now has higher processor speeds as well as greater quantities of on-board ROM and RAM, which combine to increase the newer MCUs computational capabilities of complex algorithms and signal processing routines. These advancements can be taken to produce a more effective controller for reactive power compensation. This paper suggests a replacement process of the existing power factor regulators with new regulators using MSP430 microcontrollers as effective MCUs for communication with SCADA system.

2. THE COMMUNICATION OF THE PROPOSED REGULATORS WITH THE CONTROL CENTER OF MENYA SECTOR

As mentioned before, factories are senior participants in Menya sector. In figure3, the proposed system illustrates the chosen architecture to connect many regulators who located in two factories in the supervision center. Each node in the factory has its own power factor regulator. This regulator has a CC110L BoosterPack offers a local wireless communication with others power factor regulators. This local ad-hoc network has a main role to achieve supervision, data to the collection node based on an MSP430 board with CC3000 BoosterPack. The collection node is mainly used to connect the local factory network to the external internet network in order to offer professional supervision, home supervision or mobile supervision. In fact, all the data collected from the node inside the factory can be acceded anywhere across the globe.

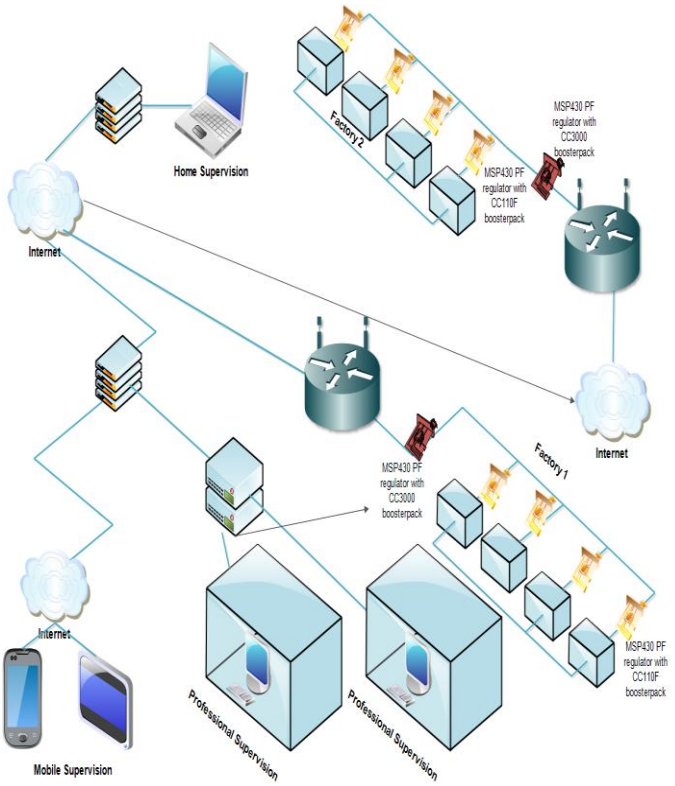

Figure 3. The architecture proposed system

3. *Implementation of a Secure Smart Grid*

3.1 Quark Hashing Algorithm for MSP430G2553 Microcontroller

As stated in [22], the designers of lightweight cryptographic algorithms and protocols must choose between two opposing design philosophies. The first is to create new programs from scratch, while the second is to reuse the available algorithms adapting to the constraints of the system. This second approach has the advantage of guaranteeing a certain level of compatibility with existing algorithms by offering tailored implementations of the proposed systems. Moreover, the approach of producing an algorithm specifically designed for a certain application has the advantage of taking into account the specific constraints of these systems. These considerations can be introduced from the first steps of the design flow. This kind of approach provides a better match between the software and the hardware components, especially in limited resources environments. The main feature of QUARK is the separation of the message in fixed lengths for working with shift registers. This fact can minimize the complexity of such algorithm, which facilitates its widespread adoption for very limited applications in computing power. In our SCADA system, the execution of the hashing algorithm is just used during new supervision node connection, then this algorithm can have a middle complexity level. Our target platform is the MSP430G2553 microcontroller with 16 KB of flash memory, 512 bytes of RAM and cannot go over 16MHz in frequency. The target platform is a limited platform for traditional hash algorithms. On the other hand, the level of security required is much lower than that of conventional computer applications given the existence of physical barriers and behavioural darkness of equipment involved.

3.2 Performance Evaluation of Various Quark Profiles Running on the Proposed RTU

After adapting the different profiles of QUARK algorithm for MSP430G2553, we conducted the measurement of the execution time and memory footprint of each algorithm profile. All adaptation and compilation phases were carried out on the environment of Code Composer Studio 5. On the other hand, the measured time were carried out through the measurement of an external signal on an oscilloscope (set to a beginning of execution of the algorithm and to zero at the end of the execution). On the other hand, the memory footprint is recovered through the compiler after executing compiler phases and linking. It should be noted that the code optimization settings were disabled for all profiles of the algorithm. The obtained results in figure 4 and figure 5 summarize the execution time and memory footprints of different variants of the QUARK algorithm. We would like to emphasize that this outcome is obtained with 1 MHz MCU frequency, which can be easily improved by increasing the frequency of the MCU since the adopted MCU can run up to 16 MHz or by switching to higher MCU family as in the next section.

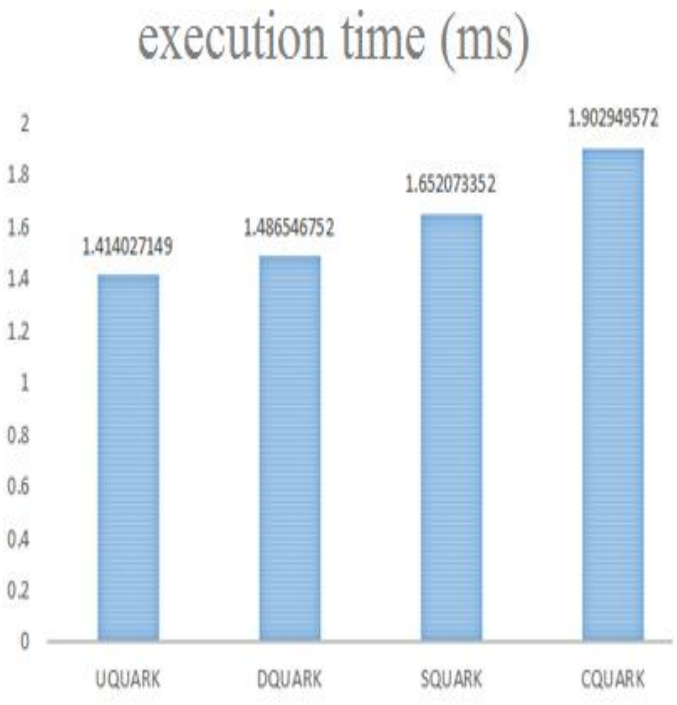

Figure 4.Execution time for various profiles of Quark algorithm

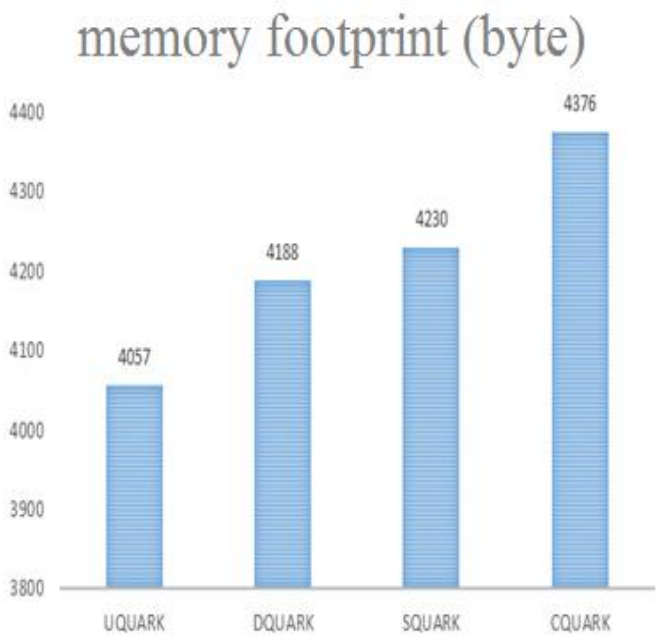

Figure 5. Footprint for various profiles of Quark algorithm

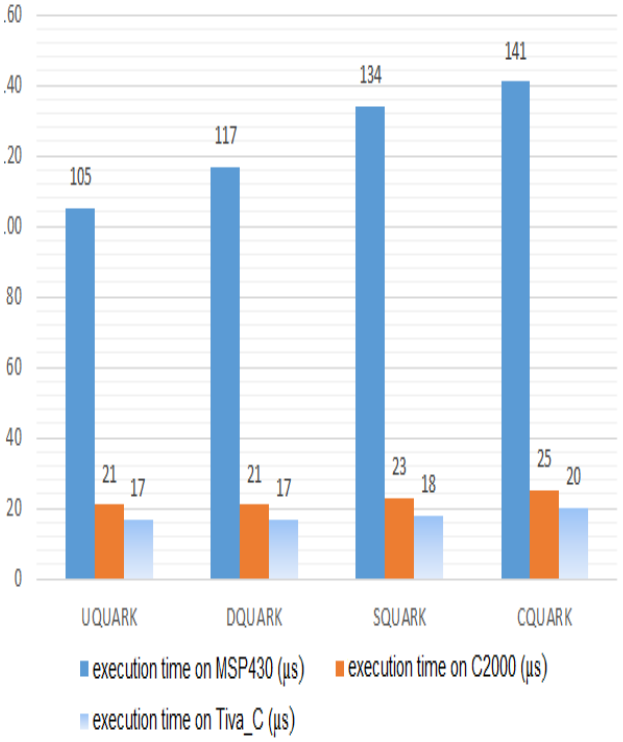

Fig. 5. Execution time on MSP430, C2000 and Tiva_C

3.3 Performance evaluation of the different profiles of the QUARK hash algorithm at alternative platforms on MCUs

To improve the performance of QUARK hash algorithm, we have to increase the frequency of the studied processor or by substitution of the MSP430 platform with more efficient platforms such as Tiva_C and C2000 Piccolo microcontroller. We proceeded with the implementation of the different profiles of Quark algorithm on the previous two platforms and a change in the frequency of the MSP430 microcontroller. The main features of Tiva_C,C2000 and MSP430 microcontroller are shown in table 2. The Tiva_C,C2000 and MSP430 microcontroller are configured at respective frequencies 80 MHz, 60 MHz and 16 MHz, which are the maximum frequency of these platforms. After increasing the working frequency, the results are taken as an average of 1000 iterations of each profile of the algorithm. The obtained results of the execution time and memory footprint are illustrated in figure 6 and figure 7.

TABLE 2. MAIN FEATURES OF THE USED MICROCONTROLLERS

List	MSP430	Tiva_C	C2000 Piccolo
CPU	MSP430	ARM Cortex-M4 (32 Bit)	TMS320C28x (32 Bit)
Flash	16kB	256 KB	64KB
SRAM	512B	32 kB	12KB
Max Speed (MHz)	16	80	60

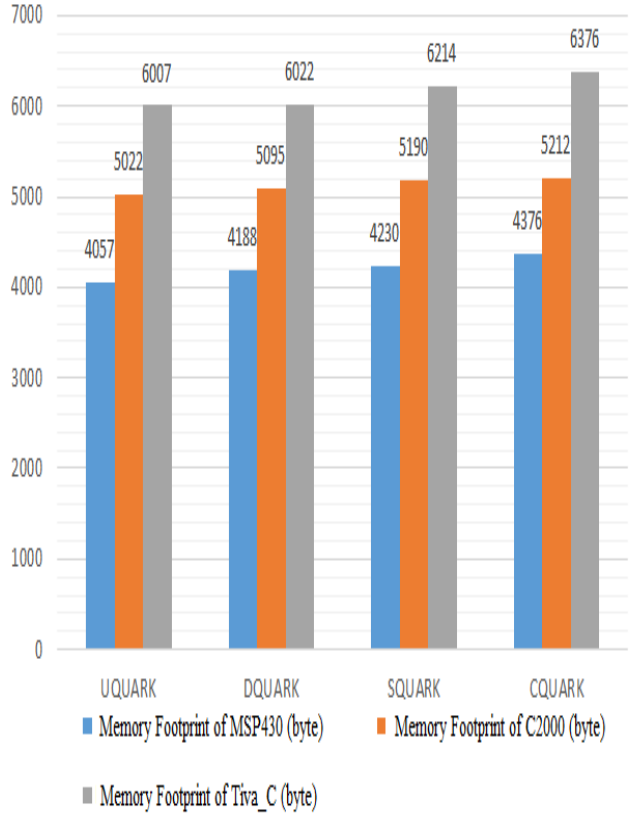

Figure 7. Memory Footprint for different profiles of the Quark algorithm on MSP430, C2000 and Tiva _C

3.4 Analysis of Results

In this section, we explored various possibilities of Texas Instruments MCUs and their usability in our application field. Through this study we get some interesting results that can be used as a reference for various node of a smart grid system. In fact, the obtained results by the u Quark can encourage its adoption in low cost low power node using the MSP430 MCU, while c Quark can be easily adopted in some complex application especially in those requiring higher level of security with some overhead of cost and power consumption.

V. Conclusion

Smart grid is developing a more sophisticated electricity delivery infrastructure that requires embedding intelligence and communications at every node of the electric-power delivery system. This paper proposes an integrated solution for embedding the reactive power compensation systems of low voltage power grids into MEEDCO's SCADA system. New power factor regulators (IDE) using MSP430 microcontrollers have been presented instead of the traditional compound regulators. Data transfer between the control center of MEEDCO and power factor regulators has been introduced efficiently and in a secure way. This work can be valid for many applications in the smart grid to include efficiently every node on the electric-power delivery system.

Acknowledgment

The authors thank too much the engineer, Alaa Abdel Fattah, manager of MEEDCO's control center for giving us information about MEEDCO and its SCADA system.

References

[1] Jianguo, Zhou, et a, “Load balancing and reactive power compensation based on capacitor banks shunt compensation in low voltage distribution networks."Control Conference (CCC), ” 2012 31st Chinese. IEEE, 2012.

[2] Lippincott, Colin, “Secure wireless data communications for distribution automation in the Smart Grid, ”Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES. IEEE, 2012.

[3] Endi, Mohamed, Y. Z. Elhalwagy, and Attalla Hasha, “Three-layer plc/scada system architecture in process automation and data monitoring. ” Computer and Automation Engineering (ICCAE), 2010 The 2nd International Conference on. Vol. 2. IEEE, 2010.

[4] Aumasson, Jean-Philippe, et al. “Quark: A lightweight hash,”Cryptographic Hardware and Embedded Systems, CHES 2010. Springer Berlin Heidelberg, 2010. 1-15.

[5] Yoo, Seong-eun, “A Wireless Sensor Network-Based Portable Vehicle Detector Evaluation System. ”Sensors 13, no. 1 (2013): 1160-1182.

[6] Chernbumroong, Saisakul, Anthony S. Atkins, and Hongnian Yu, “Activity classification using a single wrist-worn accelerometer, ” Software, Knowledge Information, Industrial Management and Applications (SKIMA), 2011 5th International Conference on. IEEE, 2011.

[7] Nikitin, Pavel V., Shashi Ramamurthy, and Rene Martinez, “Simple Low Cost UHF RFID Reader,”

[8] Foreman, J. Chris, and DheerajGurugubelli. “dentifying the Cyber Attack Surface of the Advanced Metering Infrastructure." The Electricity Journal 28.1 (2015): 94-103.

[9] Donohoe, Michael, Brendan Jennings, and Sasitharan Balasubramaniam. “Context-awareness and the Smart Grid: Requirements and Challenge, ”Computer Networks (2015).

[10] Anwar, Adnan, and Abdun Nase rMahmood, “Cyber security of smart grid infrastructure. ” arXiv preprint arXiv:1401.3936 (2014).

[11] Vulnerability Assessment of Cyber security for SCADA Systems, Chee-Wooi Ten, Student Member, IEEE, Chen-Ching Liu, Fellow, IEEE, and GovindarasuManimaran, Member, IEEE, IEEE TRANSACTIONS ON POWER SYSTEMS, VOL. 23, NO. 4, NOVEMBER 2008

[12] Wang, Yongge, “sSCADA: Securing SCADA infrastructure communications. ”arXiv preprint arXiv:1207.5434 (2012).

[13] A Testbed for Secure and Robust SCADA Systems, AnnaritaGiani, Gabor Karsai, Tanya Roosta, Aakash Shah, Bruno Sinopoli, Jon Wiley

[14] Secure SCADA framework for the protection of energy control systems, Cristina Alcaraz1, Javier Lopez1, Jianying Zhou2 and Rodrigo Roman1, Concurrency Computat.: Pract. Exper. 2011; 23:1431–1442

[15] Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). “Security issues in SCADA networks”. Computers & Security, 25(7), 498-506.

[16] Yahia Bahaa Hassan1, Nabil Litayem, Mohyi el-din Azzam, “ Recent Trends in SCADA and Power Factor Compensation on low Voltage Power Systems for Advanced Smart Grid”.Website: ijrdet. ISSN 2347-6435. Volume 3, Issue 1, July 2014

[17] Guo, Jian, Thomas Peyrin, and Axel Poschmann, “The PHOTON family of lightweight hash functions.” Advances in Cryptology–CRYPTO 2011. Springer Berlin Heidelberg, 2011. 222-239.

[18] Bogdanov, Andrey, et al. “SPONGENT: A lightweight hash function. »Cryptographic Hardware and Embedded Systems–CHES 2011. Springer Berlin Heidelberg, 2011. 312-325.

[19] Aumasson, Jean-Philippe, et al. “Quark: A lightweight hash. ” Journal of cryptology 26.2 (2013): 313-339.

[20] Balasch, Josep, et al. “Compact implementation and performance evaluation of hash functions in a tiny devices. ”Smart Card Research and Advanced Applications. Springer Berlin Heidelberg, 2013. 158-172.

[21] IEEE Guide for Application of Shunt Power Capacitors, IEEE Std. 1036-1992, 1992.

[22] Bogdanov, A., Knežević, M., Leander, G., Toz, D., Varıcı, K., &Verbauwhede, I. (2011). SPONGENT: “ A lightweight hash function, ” In Cryptographic Hardware and Embedded Systems–CHES 2011 (pp. 312-325). Springer Berlin Heidelberg.