**QUEEN'S
UNIVERSITY
BELFAST**

A Seamless Cloud Migration Approach to Secure Distributed Legacy Industrial SCADA Systems

Khan, R., McLaughlin, K., Kang, B., Lavery, D., & Sezer, S. (2020). A Seamless Cloud Migration Approach to Secure Distributed Legacy Industrial SCADA Systems. In *IEEE Innovative Smart Grid Technologies (ISGT) North America 2020 17/02/2020 → 20/02/2020 Washington DC, United States: Proceedings* (IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT): Proceedings). Institute of Electrical and Electronics Engineers Inc.. <https://doi.org/10.1109/ISGT45199.2020.9087760>

Published in:

IEEE Innovative Smart Grid Technologies (ISGT) North America 2020 17/02/2020 → 20/02/2020 Washington DC, United States: Proceedings

Document Version:

Peer reviewed version

Queen's University Belfast - Research Portal:

[Link to publication record in Queen's University Belfast Research Portal](#)

Publisher rights

Copyright 2020 IEEE. This work is made available online in accordance with the publisher's policies. Please refer to any applicable terms of use of the publisher.

General rights

Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy

The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

A Seamless Cloud Migration Approach to Secure Distributed Legacy Industrial SCADA Systems

Rafiullah Khan, Kieran McLaughlin, BooJoong Kang, David Lavery and Sakir Sezer

Queen's University Belfast, Belfast, United Kingdom

Email: {rafiullah.khan, kieran.mclaughlin, b.kang, david.lavery, s.sezer}@qub.ac.uk

Abstract—Currently deployed legacy industrial systems were not designed with the future industry 4.0 vision in mind and lack advanced, and often even basic, security features. Further, the presence of legacy systems not only introduces security and data privacy challenges but is also a barrier for the adoption of emerging cloud technologies. This paper proposes an approach for seamless and secure migration of legacy industrial control systems to the cloud. It investigates whether the cloud can meet the real-time requirements for control operations without compromising system safety. The proposed approach is designed to cause no or minimal interruption to industrial processes during cloud migration and offers a generic framework to be applied for different industrial sectors. As a use case, this paper presents the design and validation for synchrophasor technology in smart grid using the Amazon AWS cloud. Experiments on a real laboratory-based cyber-physical tested concluded that proposed cloud migration approach is promising for time-critical systems such as synchrophasor technology.

I. INTRODUCTION

The fourth industrial revolution is inevitable due to numerous societal and economic benefits [1]. However, security and reliability are major hindrances for such a paradigm shift due to the critical nature of industrial processes [2]. Unlike IT devices, industrial devices have high deployment complexity and are cost-prohibitive to upgrade. Specifically, the smart grid contains a large quantity of legacy equipment. For example, synchrophasor technology was proposed in the 1980s and since then, power companies have deployed a large number of expensive phasor devices. Most phasor devices (i.e., Phasor Measurement Units (PMUs) and Phasor Data Concentrators (PDCs)) are IEEE C37.118 compliant and lack even basic security features [3]. In short, legacy technologies and devices are critical assets of power companies and emerging cloud technologies must support them. Thus, a seamless and secure cloud migration approach needs to be investigated.

A. Related Work

Over the last few years, several cybersecurity incidents have been reported on critical industrial operations such as Stuxnet and the Ukraine blackout [4], [5]. The presence of legacy systems is normally considered as the root cause for such security incidents [6]. Similarly, legacy devices in power systems have weak or no security as identified in [3], [7]. Thus, industry modernization is a difficult job unless security is assured for legacy systems [8].

Authors in [9] proposed a middleware to equip legacy devices with advanced security features. It runs on both, the

control application and the legacy device to ensure mutual authentication and communication integrity. Authors in [10] proposed a security gateway that bridges the gap between legacy and latest technologies. It is a low-cost gateway attached to the legacy device which acts as the protocol translator. However, the presented work does not address the migration of legacy systems to the cloud.

Several researchers have identified challenges in migrating industrial control systems to the cloud [11], [12]. Authors in [13] proposed Windows Communication Foundation (WCF) framework and Azure IoT Hub to control industrial operations from the cloud. A local PC with Windows OS is used in the middle between Programmable Logic Controller (PLC) and the cloud. The presented approach lacks plug & play feature and raises cost and scalability concerns for attaching a windows PC to each industrial device. Authors in [14] presented cloud-based control for manufacturing industry. Each manufacturing site is equipped with a local server that receives instructions from the cloud when a customer places an online order. The presented work does not migrate control of each individual device to the cloud. Authors in [15] presented access control models for the integration of cloud technologies. However, presented work assumes the latest devices communicating directly with the cloud and does not address security issues arising due to legacy devices.

B. Paper Motivation and Contributions

In general, the current research trend focuses on developing SCADA systems specifically for the cloud [14], [15]. However, solutions still need to be investigated which can allow adaption of legacy SCADA devices while ensuring security and data privacy in the cloud migrated system. This paper investigates a new cloud migration approach that can be applied to most legacy industrial control systems. The proposed approach is a step beyond relevant previous work [13] with the following considerations in its design: (i) a low-cost and seamless cloud migration strategy that causes no or minimal interruption to industrial operations, (ii) cloud migration architecture that is inherently secure, (iii) support legacy devices with obsolete communication technologies without risking entire system security, and (iv) improve resilience and infrastructure-wide system visibility/control compared to local on-site deployment.

This paper presents the architectural design for the proposed cloud migration approach. For validation, it considers distributed generation in power systems as a use case sce-

Figure 1. Proposed secure cloud migration approach for a typical heterogeneous industrial system.

nario. Implementation details are provided for synchrophasor technology which plays a vital role for real-time control and monitoring in distributed generation systems. This paper analyzes necessary features for key architectural components for ensuring safe and secure cloud migration of legacy industrial equipment. It provides a walk-through demonstrating the cloud migration of a real micro-grid testbed facility. Synchrophasor technology has a higher data rate and stricter low-latency requirements than many ICS applications. The successful cloud migration of synchrophasor's control validates the suitability of proposed approach for real-time industrial applications.

II. PROPOSED CLOUD MIGRATION APPROACH

A typical industrial system has many applications, SCADA servers, historian and HMI located locally, or accessed via a remote SCADA system as depicted in Fig. 1. Due to the presence of legacy devices and protocols with no or weak security, ICS operations are susceptible to cyber-attacks if any of the internal network device is compromised by a malware. To avoid the risk of breaking system, devices typically have several decades long life cycle and often receive no software updates/patches. Therefore, the proposed cloud migration approach is designed to be secure and tackle with challenges emerging due to co-existence of new and legacy technologies. It consists of two main components as shown in Fig. 1: (i) Cloud Connectivity Kit (CCK), and (ii) Cloud platform.

A. Cloud Connectivity Kit (CCK)

For enabling secure cloud migration of legacy equipment, a low-cost small device, the CCK, is attached to the industrial device (PLC, RTU, actuator, sensor, etc). The CCK offers localized security for the ICS device as depicted in Fig. 2. Once connected to the ICS device, the CCK establishes an encrypted end-to-end VPN tunnel with the cloud. VPN tunnel secures the network traffic between ICS device and the cloud.

It can be observed in Fig. 2 that the ICS device is only accessible through CCK. After successful cloud migration,

CCK blocks access and control of ICS device from the local network and only allows from the cloud over the secure VPN tunnel. Most legacy ICS protocols have weak or no security. The proposed cloud migration strategy overcomes this limitation by using end-to-end encrypted VPN tunnel.

Figure 2. CCK offers localized end-point security to the ICS device.

The CCK consists of three functional blocks as depicted in Fig. 3: (i) a Firewall/VPN which is managed from the cloud, (ii) a network switch for connecting ICS devices, and (iii) traffic monitoring and storage. The CCK is capable of supporting advanced firewall and VPN tunnel with VLAN segregation capability to ensure end-point (i.e., ICS device) security. It is equipped with a minimum of two Ethernet ports (i.e., to connect one ICS device) as depicted in Fig. 2. It can also log activities and capture network traffic data for analytics.

B. Cloud Platform

Cloud platform securely integrates ICS operations and offers effective APIs for integration of control/monitoring software and third-party services. The basic architectural components are depicted in Fig. 4 for a distributed power system scenario. The cloud is responsible for secure data acquisition and orchestration of ICS devices. This is achieved through the CCK,

Figure 3. Functional blocks of the CCK.

Figure 4. Power systems scenario.

uniquely identifiable and controllable from the cloud. The cloud acts as the trusted Certificate Authority (CA) and issues a security certificate for each CCK. These digital certificates verify the identity and security credentials of the CCKs and can be pre-configured on them before they are supplied to industrial integrators. The cloud manages certificates validity, VPN tunnels as well as ensuring segregation using VLAN technology. If a CCK has been compromised, its certificate can be revoked from the cloud. Once a certificate is revoked, the specific CCK is disconnected and can no longer connect to the cloud. Based on the requirement, different Virtual Machines (VMs) can be created in the cloud for each legacy application. The cloud also needs network management functionality offered by most public clouds (e.g., Amazon AWS and Microsoft Azure) and private clouds (e.g., OpenStack) to control inter-VM communication. The networking feature can be used for creating segregated virtual networks within the cloud and assigning different security/firewall rules for each VM.

III. USE CASE: DISTRIBUTED POWER GENERATION

This paper demonstrates cloud migration for synchronous islanding that deals with distributed generation in smart grid. It relies on synchrophasor technology to ensure safe integration of distributed generation sources (e.g., micro-grids) into the main grid. Synchrophasor technology is several decades old and first introduced in the 1980s. For real-time control and monitoring in power systems, a large number of expensive and legacy phasor devices (PMUs, PDCs) have been deployed which use obsolete insecure communication protocols. Over time, synchrophasor technology has evolved and several wide-area control and monitoring applications have been proposed including synchronous islanding. Synchronous islanding technology is still in the laboratory validation stage and faces communication security as a major concern for deployment in the real grid. Replacement of insecure legacy phasor devices is cost prohibitive. Thus, security and resilience are of paramount significance for reliable and trustworthy operations. The proposed cloud migration approach can address these challenges paving the way for the modernization of power systems.

A. Communication Protocols

The first synchrophasor communication standard was IEEE 1344, published in 1995. It was improved and replaced by IEEE C37.118 in 2005. IEEE C37.118 was limited to address

Figure 5. Synchronous islanding use case.

requirements only for steady state condition. It was replaced by IEEE C37.118.2 in 2011 that also takes into account dynamic power system conditions. All these IEEE standards lack security features and are vulnerable to cyber attacks [16]. A new standard, IEC 61850-90-5 emerged in 2012 with support for optional encryption but its use in power systems is still very limited. Its adoption is hindered due to interoperability issues with the existing legacy IEEE C37.118 compliant devices. Due to cost and deployment complexity involved, it is usually not a feasible option to replace legacy phasor devices [6].

B. Synchronous Islanding

A microgrid is a certain geographical area where electricity generation (e.g., wind farms, solar panels, etc), storage and load/consumers are in close proximity. Generators in a microgrid normally produce enough electricity for the local load and can also contribute to the main grid. A microgrid can be in three different operational states: (i) connected to the main grid, (ii) disconnected from the main grid, and (iii) transitional state i.e., going to connect or disconnect from the main grid. The disconnected state is also known as the islanded state. The transitional state is most volatile. If going to disconnect, a microgrid must fulfill local demand to avoid blackout. If going to connect, the microgrid must be synchronized with the main grid to avoid any physical damage. The process of synchronizing an islanded microgrid with the main grid before the connection is known as synchronous islanding.

A basic synchronous islanding system is depicted in Fig. 5. A PMU device is connected to both, microgrid and the main grid. It measures electrical quantities in real time, timestamps them with the GPS time and transmits them to the PDC using IEEE C37.118.2 protocol. PDC aggregates data from both PMUs and provides it to the controller. Based on the received data, the controller decides if a microgrid is synchronized with the main grid. If controller observes any difference in the voltage magnitude, phase angle or frequency, it sends a feedback signal to the microgrid to make necessary adjustments. Once synchronization is achieved, the circuit breaker can be closed and microgrid can be safely connected to the main grid.

IV. TEST-BED AND EXPERIMENTAL VALIDATION

This section validates the proposed cloud migration approach by migrating a real synchronous islanding testbed

Figure 6. Cloud migration of synchronous islanding testbed.

facility. The testbed components are connected according to Fig. 5. The microgrid consists of a generator set and 3 phase transmission load. The generator set is comprised of an alternator which is driven by a prime mover. The prime mover is a DC machine which is coupled to the alternator drive shaft. To increase/decrease electrical power output in the microgrid, the prime mover receives feedback from the controller and then increases or decreases torque on the alternator drive shaft. The PMUs used in the testbed are the OpenPMUs [17]. They communicate the state of main grid (i.e., utility supply) and microgrid (i.e., generator set) to the controller which then adjusts the phase angle of the microgrid with the main grid. Once synchronized, the circuit breaker can be safely closed.

A. AWS Cloud Migrated Testbed

Amazon AWS is used as the cloud platform. The objective is to migrate control, monitoring, data analytics, and archival systems to the cloud except field devices. Thus, the PDC and controller in Fig. 5 need to be migrated to the cloud. Four VMs were created in AWS with different necessary configurations to run the PDC, controller, VPN server and data analytics (see Fig. 6). A private network is created between VMs for internal communication. The external access to cloud VMs is restricted and allowed only through a VPN server after successful authentication. The data analytics VM is used for logging activities, analyzing and alerting based on events happening in the system. The pictorial view of testbed components is shown in Fig. 7 which are connected according to Fig. 6.

B. OpenVPN Setup

For VPN setup, an open-source and scalable VPN solution is used i.e., OpenVPN. A cloud VM is configured with ‘OpenVPN Access Server’ that acts as the gateway for external access. It also acts as the trusted Certificate Authority (CA) and issues a security certificate for each CCK. These digital certificates verify the identity and security credentials of CCKs and are pre-configured on them before they are shipped/installed in the testbed. Certificate-based authentication has several advantages including the ability to revoke a certificate whenever necessary (e.g., if a CCK is compromised).

(a) Microgrid and 3-Phase Transmission Load

(b) PMUs connected to CCK

(c) Local Controller

(d) AWS Cloud VMs

(e) Cloud Controller

Figure 7. Pictorial view of the testbed components.

Certificates for OpenVPN can be generated using OpenSSL. However, some systems are configured to block such certificates if detected from an untrusted CA. To avoid such issues, SSL certificates were generated using LetsEncrypt. LetsEncrypt is a trusted CA that provides free and secure SSL certificates with the aim of securing the Internet.

C. Security Groups

Each cloud VM is configured with a different security group which allows or blocks access to specific protocols and devices. E.g., OpenVPN access server is configured to allow only ports TCP:443 (HTTP over TLS/SSL) and TCP:943 (admin web UI). This ensures that only devices part of the VPN network are able to access the cloud. Security groups for other VMs are configured to block external access. Traffic monitoring along with enforcing strict access control using TLS security and certificate management features ensure cloud security and make it nearly impossible to perform an undetected malicious activity.

D. Data Analytics

For synchrophasor traffic and log analytics, Splunk tool is configured on a cloud VM that receives log messages from PDC over a UDP port. Splunk offers intuitive log search features and various visualization options on a highly customizable dashboard. Traffic analytics is useful for analyzing data patterns, diagnosing problems, maintaining QoS and identifying security threats. In current implementations, Splunk analyzes only IEEE C37.118.2 traffic logs. For meaningful analysis, logs are plotted using different visualizations on a customized dashboard as shown in Fig. 8.

Figure 8. Synchrophasor traffic analytics.

Table I

OBSERVED COMMUNICATION LATENCIES AVERAGED OVER 100 TRIALS.

	Latency (ms)			
	Min	Avg	Max	Mean Dev.
Local system	0.35	0.46	1.51	0.143
Cloud-migrated system	13.52	13.84	20.67	0.886

E. Communication Latencies

Latencies can severely impact real-time control operations. Like many industrial control systems, synchronous islanding testbed under consideration has a 100 ms limit for receiving synchrophasor data. In the cloud migrated testbed, communication latencies depend on the ISP and access technology. Table I presents communication latencies considering both, local and cloud deployment of synchronous islanding operation. It can be observed that communication latencies in the cloud migrated system are much lower than 100 ms limit. This validates the proposed cloud migration approach for time-critical synchrophasor technology.

V. CONCLUSIONS

Cloud migration is a challenging task for dispersed critical industrial systems due to security and strict real-time control requirements. Legacy systems are critical assets of industry and their adoption in the cloud migration strategy is essential. Recent research works primarily focus on developing industrial SCADA systems specifically for the cloud [14], [15] and use a cloud migration strategy [13] that raises concerns about scalability and use of legacy systems with no or weak security.

In contrast to previous works [13], [15], the proposed cloud migration approach is equally useful for legacy equipment and modern devices with secure technologies. The design can migrate devices using heterogeneous technologies without risking system security. Moreover, the proposed approach operates as plug & play and causes no or minimal interruption to industrial operations during the cloud migration process.

For the validation of the proposed concept, this paper presented implementation details for synchrophasor-based distributed generation in power systems. It successfully migrated the synchronization and microgrid control capabilities to the cloud using secure VPN technology. The use of VPN tunnels ensured secure and trustworthy communication between the cloud and end-point legacy phasor devices. Certificate-based authentication and VPN encryption prevent the risk of eavesdropping and malicious packet modifications in transit. It is identified that the cloud connectivity kit software is lightweight, has low resource requirements and suitable to be deployed on a low-cost device. This significantly reduces the cost involved in an industry modernization. It is experimentally validated that the incremental communication latencies introduced by the cloud are very low and do not impact real-time synchrophasor operations. Successful validation for synchrophasor technology with high data rate and strictly low latency requirements proves that the proposed cloud migration approach could be widely applicable to similar industrial cyber-physical systems.

REFERENCES

- [1] J. M. Müller, D. Kiel, and K.-I. Voigt, "What drives the implementation of industry 4.0? the role of opportunities and challenges in the context of sustainability," in *Sustainability*, 2018.
- [2] T. Pereira *et al.*, "Network and information security challenges within industry 4.0 paradigm," in *Procedia Manufacturing*, vol. 13, 2017.
- [3] R. Khan, K. McLaughlin, J. Hastings, D. Lavery, and S. Sezer, "Demonstrating cyber-physical attacks and defense for synchrophasor technology in smart grid," in *Privacy, Security and Trust (PST)*, 2018.
- [4] R. Khan, K. McLaughlin, D. Lavery, and S. Sezer, "Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid," in *4th ICS-CSR*, August 2016.
- [5] I. Stelios *et al.*, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys Tutorials*, 2018.
- [6] R. Khan, K. McLaughlin, J. Hastings, D. Lavery, and S. Sezer, "Inter-technology bridging gateway: A low cost legacy adaptation approach to secure industrial systems," in *IEEE PES-GM*, 2018.
- [7] C. Tu, X. He, X. Liu, and P. Li, "Cyber-attacks in pmu-based power network and countermeasures," *IEEE Access*, 2018.
- [8] V. Kumar Singh *et al.*, "Stealthy cyber attacks and impact analysis on wide-area protection of smart grid," in *NAPS*, 2016.
- [9] T. A. Rizzetti *et al.*, "Cyber security and communications network on scada systems in the context of smart grids," in *UPEC*, 2015.
- [10] R. Khan, K. McLaughlin, D. Lavery, and S. Sezer, "Design and implementation of security gateway for synchrophasor based real-time control and monitoring in smart grid," *IEEE Access*, 2017.
- [11] A. Ibrahim, M. Zubaida, and H. Yahaya, "Information security factors in the implementation of industrial control system into cloud environment," *Advanced Science Letters*, Vol. 24, No. 7, 2018.
- [12] H. P. Breivold, "Towards factories of the future: migration of industrial legacy automation systems in the cloud computing and internet-of-things context," *Enterprise Information Systems*, 2019.
- [13] P. Papcun *et al.*, "Cloud based control of industrial cyber-physical systems," in *CIE48 Proceedings*, 2018.
- [14] X. Liu *et al.*, "Cyber-physical manufacturing cloud: Architecture, virtualization, communication, and testbed," *Manufacturing Systems*, 2017.
- [15] J. Lopez and J. E. Rubio, "Access control for cyber-physical systems interconnected to the cloud," *Computer Networks*, vol. 134, 2018.
- [16] R. Khan, K. McLaughlin, D. Lavery, and S. Sezer, "IEEE C37.118-2 Synchrophasor Communication Framework - Overview, Cyber Vulnerabilities Analysis and Performance Evaluation," in *ICISSP*, 2016.
- [17] D. M. Lavery *et al.*, "The OpenPMU Project: Challenges and Perspectives," in *IEEE PES-GM*, 2013.