Industrial Control System Applications go Mobile in the Cloud

Dr. Jeff Daniels
Lockheed Martin Corporation
jeff.daniels@lmco.com

Dr. Ben Amaba, PE, CPIM®, LEED® AP BD+C
IBM Corporation
baamaba@us.ibm.com

Dr. Arman Sargolzaei
PLC International Inc.
arman.sargolzaei@plcpower.com

Abstract
Industrial control systems are increasingly becoming interconnected with local area networks, wide area networks, extranet networks, and cloud computing environments. Cloud and mobile technologies provide a competitive advantage for global companies. In this research, a DevOps approach to cloud-based applications development was used to create a capability for industrial control systems management and reporting. The research demonstrates a secure method to connect to industrial controls systems using cloud-based, yet open platform mobile technologies leading to cognitive technology or artificial intelligence systems, addressing one of the most challenging issues in cloud computing systems. Data access control and security connectivity from mobile to cloud to control systems are addressed.

Categories and Subject Descriptors
Cybersecurity, information technology, manufacturing

General Terms
Cybersecurity, cloud computing, industrial control systems, applications development

Keywords
Cybersecurity, cloud computing, cloud services, Industry 4.0, control systems, devops

1. Introduction

Industrial control systems (ICSs) have many applications in the industry. An innovation in control systems is the cloud based control system, which is used to monitor and control systems in wide areas, enabling engineers to more easily configure, monitor and control devices through cloud and mobile devices worldwide. In recent years, the security of industrial control systems has been an important challenge for many researchers. Industrial Control Systems (ICSs) include Networked Control Systems (NCSs), Supervisory Control and Data Acquisition (SCADA), Process Control Systems (PCSs), Distributed Control Systems (DCSs), Load Frequency Control (LFC) and Programmable Logic Controllers (PLCs). Security of the abovementioned ICSs plays an important role in the successful performance of industrial and critical infrastructures. Energy and power sectors, transportation system sectors, water and wastewater system sectors, healthcare and public health sectors are examples of industries facing a high probability of attacks on their performance. Along with the development and advancement of security schemes for ICSs during the past several years, there have also been many cyber attacks [1-5]. This is evidence that ICS are not very secure in light of cyber-attacks.

Here we contributed to solve this need by interconnecting ICSs to IP telephony and Simple Network Management Protocol (SNMP). Also we used security communication protocols to address this issue and have a secure connection. RS-M2M series developed by PLC International Inc. (PLCI) helps to support communications on Internet-enabled industries efficiently, professionally and effortlessly.

2. Related Work

2.1 Industry 4.0

Industry 4.0 is term that refers to the digitization of manufacturing driven by disruptive technologies including big data, advanced analytics capabilities, human-machine interaction, and enhancements to manufacturing work instructions such as 3-D printing.

Industry 4.0 is referred to as "Industrie 4.0" in Germany where it originated as a strategic manufacturing initiative; in the United States, it is called the "Industrial Internet." The Industry 4.0 approach often overlaps with the "Internet of Things" (IoT) concept which refers to interconnected devices such as watches, appliances, and automobiles. It also encompasses cyber-physical systems (CPS) such as smart machines, intelligent storage devices, and production facilities such as "smart" factories.

An estimated 90% of manufacturing systems are based on information and communications technology (ICT) that has been implemented over the past 30 years. The Industry 4.0 concept taps into these interconnected devices capable of creating, processing, and transmitting critical manufacturing data across the enterprise.

A 2013 study on Industry 4.0 identifies key features that should be considered for implementation:

1. Horizontal integration through value networks
2. End-to-End digital integration of engineering across the entire value chain
3. Vertical integration and networked manufacturing systems

This research embraces the Industry 4.0 approach of end-to-end digital integration through the use of development methodologies (DevOps), information technology (Cloud Computing), and cybersecurity to analyze information and remotely manage industrial controllers using mobile-based cloud systems.

2.2 DevOps

The industrialization of information technology (Weinman, 2012) has similarities and benefits that the agricultural, construction, and industrial age delivered to society by connecting people, harvesting best practices and integrating technology. The Toyota Production System and the DevOps principles leverage concepts and ideas in producing better products faster by optimizing resources. Terms like software factory, quality, security, reliability, maintainability, open standards, agility, collaboration, risk analysis, defect prevention, defect removal and engineering methods has allowed us to reuse concepts and knowledge learned from earlier disciplines and transformations. Like modern manufacturing, DevOps is bringing groups of people together to collaborate and communicate on critical information through the life cycle of a product and service. Although new job titles or terms like developer, coder, tester, programmer, cyber-security, and SCRUM have been created, the community of participants and/or actors understand by improving communications across the life cycle brings higher benefits to the group, organization, industry and market. Best practices and methods still are symbiotic to the product or service success of the endeavor or initiative especially if one expects to improve and gain economies of scale to the new industrial controls systems and applications.

Technical tools and automation becomes an enabler for the concepts of DevOps. The tools allow us to codify, audit and clarify our work break down structure and represent a model that can be stored, modified, transmitted, and reused over an extended time horizon. An important milestone exemplifying the importance and maturation of the use of DevOps in industrial control systems is the Software

Professional Engineering license as of 2013. With public health, safety, security and environmental protection as a priority, licensing bestows accountability and liability to those developing and operating digital control systems. The DevOps approach can leverage the principles espoused in the minimum standards represented in software professional licensure. Licensure is the process by which a federal, state or local governmental agency grants an individual permission to practice in a particular occupation or profession that is subject to regulation under the government's authority and to refer to oneself as "licensed" or authorized to practice. Within the practice acts are mandates for practitioners to become licensed, usually based upon requirements such as education, examination, experience and moral character. Obtaining a license in order to practice a profession is mandatory, and state laws may provide for criminal or administrative penalties for unlicensed practice. Several studies point to a growing trend of DevOps as a foundation.

A recent IBM's Business Value (IBM, 2014) study based on insights from 435 executives in 58 countries, spanning 18 industries where organizations self-reported the following:

- 85% respondents realize and reported it is important to critical
- Almost 70 percent of the companies currently leveraging software development for competitive advantage outperform their peers from a profitability standpoint

A 2013 study analyzed several development teams and found that the group, on average, went from delivering 10 projects in Year 1 before implementing DevOps, to 20 projects in Year 2, to 30 projects in Year 3 — all without having to add additional developer headcount (Forrester, 2013).

And the developers were happy; less stressed, and had a greater feeling of accomplishment.

2.3. Cloud Computing

Author and technology prognosticator George Gilder has called today's cloud data centers, 'information factories." Since the cloud can be viewed in part as a representing the industrialization of IT and the end of the era of artisanal boutiques, many of the lessons learned in the evolution of manufacturing and the industrial age are being applied – consciously or not – via the cloud. Damon Edwards explained the business context of Cloud and DevOps very eloquently in a blog post:

"The most fundamental business process in any company is getting an idea from inception to where it is making you money ... The whole point of DevOps is to enable your business to react to market forces as quickly, efficiently, and reliably as possible."

This fits in with the 'jump in and iterate' mojo of cloud application development and the commensurate expectations of line-of-business managers, who are looking for product delivery cycles to shorten months down to weeks (Wainewright, 2011).

Cloud computing is the fast emerging business model regarding the use of information systems to support the business. According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." The NIST definition lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. It also lists three "service models" (software, platform and infrastructure), and four "deployment models" (private, community, public and hybrid) that together categorize ways to deliver cloud services. The definition is intended to serve as a means for broad

comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing (NIST).

Originally driven by an economical justification, the Cloud model for information systems is led by customer intimacy, product differentiation, operational excellence, agility, and risk reduction (Weinman, 2012). What use to take years to acquire several thousand customers and the information about a market, now takes weeks where the use of Cloud technologies are integrating data, computational power, networks, memory and devices have been coming together on open standards, common infrastructure and robust governance models that improves reliability, accessibility, availability, location independence, on-demand resources, utility pricing, and security. Like the industrial revolution where core competency was the focus and other aspects like logistics, warehousing, payroll, etc.; certain parts of the business would be outsourced or contracted out allowing the organization to focus and build on their core competencies. Cloud computing for information technology has taken a similar journey. For example, the Infrastructure as a Service (IaaS) can provide pay-per-utility pricing, dynamic scaling, security control, faster provisioning and guaranteed performance levels. Platform as a Service (PaaS) can deliver lower operational cost, faster development, and seamless integration. Software as a Service (SaaS) improves upgrade cycle times, automated backups, and location independence. These services can be delivered privately, publically or as part of a community, but more importantly, a hybrid model can be used to customize the right configuration or resources with agility. In “Architecting the Cloud” by Michael J. Kavis he presents two scenarios depicting the opportunity.

Scenario A (On-premise): Buy three different servers at roughly $3000 to $5000 each, plus software, shipping and installation

- Elapsed time to procure and implement likely to range between one and three months.
- Outcome: Decide on which server to keep, buy more, get rid of the other two

Scenario B (Cloud model): Developer creates three different virtual computing resources within minutes at $0.50/hour, using one at a time for two hours each (total $3.00).

- Complete testing and make a decision in one day
- Outcome: Complete the entire scenario in one day of work for just $3.00 plus one person's salary. No wasted assets.

The cost, speed and quality in modern day Cloud technologies and models are enabling companies, industries, and other stakeholders to take advantage of economies of scale and expert knowledge which was once left only to specialty groups of artisanal resources confined to certain geographical locations. The common infrastructure and open standards have provided rapid adoption and growth, but governance will then play a more vital role moving forward to include security, risk, availability, reliability, and backup/recovery analysis to sustain performance.

2.4 Cybersecurity

As part of the discussions at the 2013 VSAE Annual Conference, data and currency have similar challenges. Data may be a more important asset than money in certain scenarios. Money and other valuables such as jewelry can be kept under your mattress – a premises solution – or in a bank – a cloud solution. Which has the better security? The bank can afford stronger security in terms of vaults with foot think hardened steel walls, and can have a security team made up of security professionals and one or more people on payroll who stay abreast of new burglary strategies and determine and implement counterstrategies. The platforms and components were chosen to ensure a robust framework on the

prevention, isolation and remediation of cyber-security breaches. For example, the IBM Bluemix platform leverages the security API (application programming interface) to secure workloads against the latest threats and comply with regulatory requirements efficiently. The platform is used to simplify the management of who can sign in to cloud applications, and scan those applications for vulnerabilities, embed security controls into data management and big data services. Protect access to apps and workloads, scan apps for vulnerabilities, and protect the data are very important as part of the security control and vulnerability analysis. With the platform, we can easily add user authentication and single sign-on capabilities into web and mobile apps, deploy policy-based authentication interfaces to allow quick creation of multi-factor authentication, assess web and mobile applications for vulnerabilities, strengthening both security and regulatory compliance efforts by scanning apps before deployment, you can identify issues, generate reports, and make recommended fixes. To protect the data, the platform approach will utilize built-in security and privacy controls within big data and data management services, including data masking, discovery, and audit. Taking the API approach, we can then combine the security API with other APIs including IoT (Internet of Things), DevOps, Cloud Integration, Mobile and Business Analytics. Another aspect that we had to consider was we had to place the API platform on a secure infrastructure, which supports deployment of regulated workloads through extensive compliance and clear delineation of roles and responsibilities. The project was able to reuse important best practices and patterns to insure success of the industrial control system and the life cycle from end to end for the project.

3.0 The Project

In this demonstration, we used the RSM2M PLCI Gateway [6] and IBM Bluemix cloud [7] platform to create a secure and robust connection between ICSs and mobile and cloud. The RS-M2M talks in MODBUS through serial RS485/RS232 or TCP with industrial devices and transfers information to the cloud platform using MQ Telemetry Transport (MQTT) protocol and to the SNMP manager. One of the advantages of RSM2M gateway is that it provides firewall between the cloud and the mobile connection and ICSs. Also the RSM2M gateway provides relay outputs, OPTO inputs, A/D, ZigBee, Sensors and TTL I/Os for other industrial applications. This practical demonstration consisted on reading information stored on the RS-M2M gateway such as its configuration, ModBus registers, inputs and outputs. Besides reading and analyzing the information remotely on the cloud, we controlled the equipment using mobile based cloud solution. On top of all these connections, this module is also interacting with Industrial Module (IM), a piece of software that is part of the IUC (Industrial Unified Communications). With the unified messaging system in place, this demonstration is able to generate text messages (SMS), email and voice calls when any emergency event occurs. The diagram of this demonstration can be shown in Figure 1.

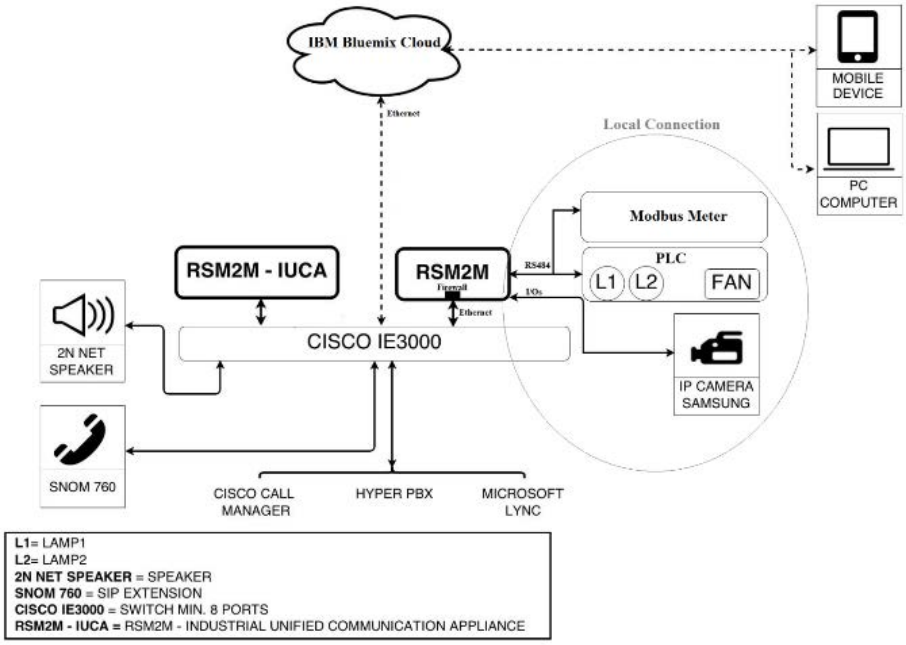

Figure 1. Diagram of proposed demonstration

Security Approaches

In this demonstration, data has been transferred to the cloud using MQTT protocol. The objective of this protocol is to deliver a really lightweight communication protocol for the internet of things. So this is the reason that this protocol has only a few security mechanisms. But in this implementation and all common demonstrations, other security standards are used, such as IPsec tunnel or SSL/TLS for transport security.

MQTT security is divided in multiple layers. Figure 2 shows different levels briefly.

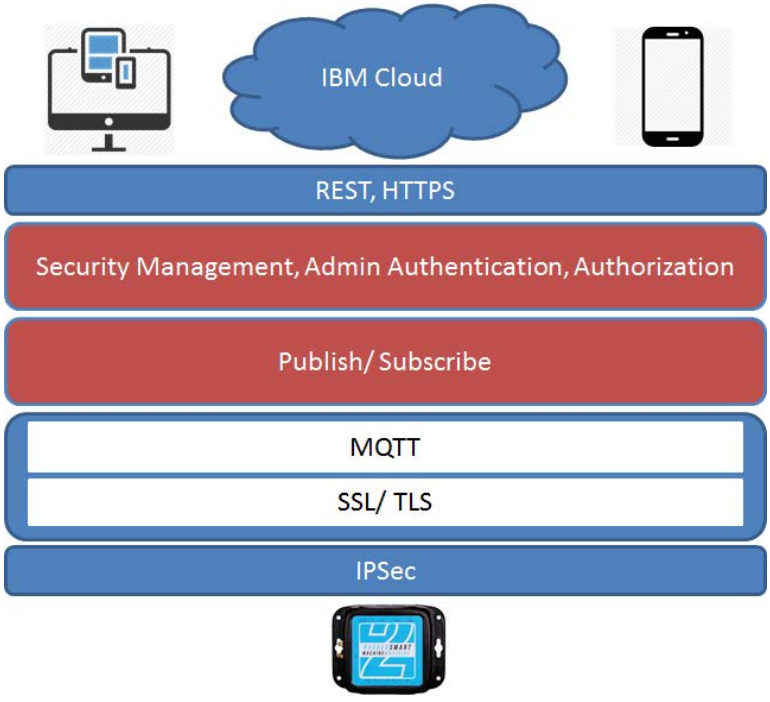

Figure 2. Different layers of communication protocol

Network Level

A physically secure network or virtual Protocol Network (VPN) can be used as foundation for any client/ broker communication which is one way and provides a secure and trustworthy connection. For gateway applications, where the gateway is a converter between devices and the broker, VPN is suitable. Here we used Internet Protocol Security (IPsec) tunnel to create appropriate secure connection (Black, 2000).

The IPsec adds security to Internet Protocol that enhances communications using packet encryption and authentication. IPsec protocols establish Mutual authentication and cryptographic keys between the authorized agents at the beginning of the session. IPsec protects flow of data between pair of hosts (host-to-host), multiple security gateways (network-to-network), and a security gateway and a host (network-to-host).

Cartographic security services of IPsec protect data sharing over IP networks. IPsec supports end-to-end security and provides integration, confidentiality (encryption), and replay protection. More information about implementing IPsec tunnel can be found in [Kent, S.; Atkinson, R. (November 1998). IP Encapsulating Security Payload (ESP). IETF. RFC 2406.].

Transport Level

While VPN provides security for the network level, Transport Layer Security (TLS)/Secure Shell (SSL) can be used for transport level encryption. It delivers a secure approach to guarantee nobody can read along and even authenticate both sides, when using client certification authentication (IETF RFC 4252, 2006).

SSL is the older version of TSL. TSL is a secure and cryptographic protocol that provides security to communication. This protocol encrypts the data and checks for integrity to prevent snooping and tampering. This technology uses for securing access to websites such as internet banking.

While using TLS, the client validates the server certificate to certify that it is linked to a trusted server. After a linked is establishes, the server and client interchange necessary information to build an encrypted, secure connection between each other. This secure connection is used to transport MQTT packets.

Application Level

With the mentioned techniques, it is ensured that the communication is secure, encrypted on the transport level. Also it certifies that the identity is authenticated. The MQTT protocol includes username and password credentials and also a client identifier that is used for authenticating devices and applications on the application level. Based on the user specification, the broker will implement accessibility, policies and authorization for different application. The payload encryption can be added to add more security to the application level. This ensures security on the transmitted information even if there is no encryption on transport level.

Authentication

Authentication is used to confirm identity of applications and devices to the cloud and gateway. As mentioned earlier, the MQTT client provides a username and password when connection stablished. The

username and password is checked by the server. It is possible to use the supplied identity for the authorization process. We can act as a certificate authority (CA) to use mutual authentication and create certificates by ourselves to make the MQTT network very constricted. In this case, each client has its own identity as part of its certificate. In this circumstance, the adversary can impersonate a client hardly and in case of success, can only impersonate that specific client.

In some cases, MQTT is implemented with OAuth 2.0 which is an authorization framework. OAuth 2.0 is a centralized checking which separates the authorization server from a resource MQTT server. This framework allows the user to grant access to the resource without sharing the credentials to the resource server. Figure 3 shows all steps that should take place to give authorization to publish and subscribe a connection.

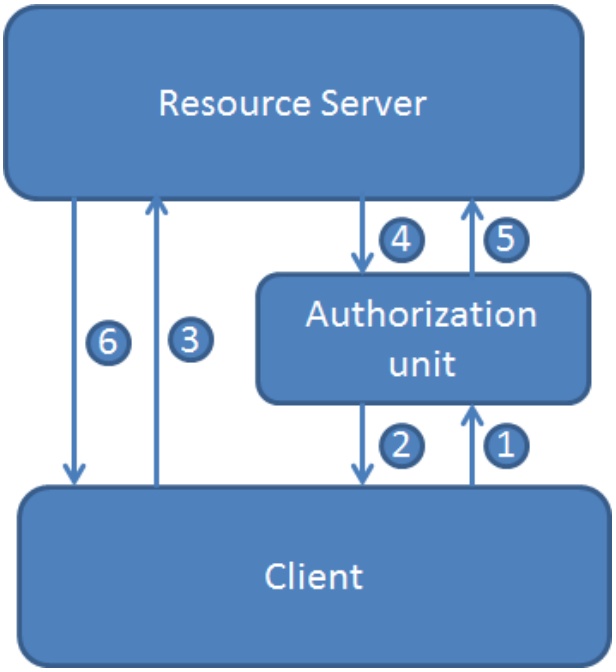

Figure 3. OAuth 2.0 framework

The following cybersecurity services were demonstrated in this research:

- Encrypted Storage with FIPS 140-2
- Data synchronization: Synchronize data items accessed or modified offline against REST services. The local store may be encrypted
- App security framework: Cross application SSO, authenticity checking, etc.
- App management: Remote disable and direct update

3.1 Designing the Application with Platform-as a Service (PaaS) using DevOps

Platform as a service (PaaS) offerings allow companies to move quickly, while incorporating the third platform technologies, in order to develop impactful applications utilizing cloud computing. PaaS is a cloud development platform that provides services and compute options for developers, allowing them to truly devote their time to coding without being concerned about the infrastructure or resource constraints.

When infrastructure abstraction is combined with robust set of DevOps tools and services, teams can follow agile development best practices, services, and reusable patterns including:

- DevOps
- Big Data
- Mobile
- Cloud Integration
- Security
- Internet of Things
- Watson
- Data Management
- Web and Application
- Business Analytics

To develop these disruptive applications it is crucial for the platform to be committed to the open source community. This ensures interoperability because the foundation is built on industry standards and that the platform will be at the forefront of innovation with the community. Critical characteristics of a PaaS include multi-tenancy, reusable patterns, open integration protocols (APIs), application development tools including Software Development Kits (SDKs) and analytics. Enterprises and start ups are competing on a leveled battlefield for building successful applications since the emergence of Platform as a service offerings that enforce cloud computing, agile development, governance, and are devoted to the open source community (Rowe, 2015). In order to reuse assets including code and process, Bluemix uses Docker Container technology, an open platform for building distributed applications for developers and system administrators, enabling the movement of solutions to different platforms. Containers are lightweight with no need to install an operating system; uses less CPU, memory and storage; can deploy more containers than virtual images and has greater portability flexibility. Bluemix is an open standard, cloud-based platform for building, running, and managing applications by IBM Corporation. As the development model rapidly evolved toward cloud, agile, and highly elastic, available web services, our customers needed a new way to consume and deliver technology and services. IBM built Bluemix to help customers address the desire and need to innovate, and in the process changed the way we build and operate software. Bluemix originally began with public cloud, our hosted deployment of the open source project, Cloud Foundry. Since that time it has evolved into a much broader cloud platform, supporting an ever-increasing variety of apps, workloads, and services across a combination of public and private cloud. Technologies continue to be improved in the design, build and manage of cloud technologies including Urban Code, Gravitant and IBM Cloud Orchestrator to incorporate best practices and processes in an asset based portfolio.

A list of DevOps tools used in the project is below:

IBM BlueMix Service supports several programming languages and services as well as integrated DevOps to build, run, deploy, and manage applications on the cloud. Bluemix runs on SoftLayer infrastructure. Bluemix supports several programming languages including Java, Node.js, Go, PHP, Python, Ruby Sinatra, Ruby on Rails and can be extended to support other languages such as Scala through the use of build packs.

IBM Rational Test Virtualization Server - IBM® Rational® Test Virtualization Server enables the deployment of virtualized services, software, and applications for simplified, efficient testing. It accelerates the delivery of complex test environments and enables you to complete integration testing earlier and more frequently in the development cycle. Rational Test Virtualization Server helps you

eliminate application test dependencies and reduce setup time and infrastructure costs. Simulate real system behavior to accelerate software development and testing. Update, reuse and share virtualized test environments to gain efficiency and keep pace with changes in the underlying systems and data. Customers benefit from integration with other tools to improve performance and quality management.

4. Conclusion

Industrial control systems are improving rapidly with the technologies available. The new cloud and mobile technologies are providing rapid and secure deployments by reusing best practices and processes, which can be stored, modified, improved and deployed effectively and efficiently using a cloud platform. No longer are cloud technologies proprietary or isolated to only community, private or public clouds. The future of data, artificial intelligence and cognitive computing will be based on open platforms that can create, build and manage hybrid configurations or hybrid clouds. No longer will systems will be isolated, but composed of legacy and new technologies, which will continue to be invented and improved. The project exemplifies the integration and connection of ICSs to IP telephony and Simple Network Management Protocol (SNMP) combining DevOps, Industry 4.0, and Cyber security best practices on the Bluemix Cloud platform to leverage robust data, compute, storage and networking infrastructures. We used security communication protocols with an RS-M2M series developed by PLC International Inc. PLCI helps to support communications on Internet-enabled industries efficiently, professionally and effortlessly.

References

[1] Gorman, S. "Electricity grid in US penetrated by spies," The Wall Street Journal, vol. 8, 2009.

[2] Pidd, H. "India blackouts leave 700 million without power," The Guardian, vol. 31, 2012.

[3] Slay, J. and M. Miller. Lessons learned from the maroochy water breach: Springer, 2008.

[4] Quinn-Judge, P. "Cracks in the system," TIME Magazine (January 9, 2002), 2002.

[5] Leyden, J. "Polish teen derails tram after hacking train network," The Register, vol. 11, 2008.

[6] http://www.power-line-carrier.com/PLCI_Uploads/Brochure-rs-m2m_print-Gen.pdf

[7] http://www.ibm.com/cloud-computing/bluemix/

[8] IBM Business Value Study: http://www-935.ibm.com/services/us/gbs/thoughtleadership/

[9] Weinman, Joe. “Cloudonomics: The Business Value of Cloud Computing.” Wiley Publishing, September 4, 2012

[10] Forrester, 2013

[11] Kavis, Michael J. “Architecting the Cloud”

[12] Black, David L. "Differentiated services and tunnels." 2000.

[13] NIST. http://www.nist.gov/itl/csd/cloud-102511.cfm

[14] Network Working Group of the IETF, January 2006, RFC 4252, The Secure Shell (SSH) Authentication Protocol

[15] Rowe, Deanne. “Bluemix.” IBM Cloud Technology Conference, Dallas, Texas, 2015

[16] Wainewright, Phil. Software as Services, September 12, 2011)

[17] Kent, S.; Atkinson, R. (November 1998). IP Encapsulating Security Payload (ESP). IETF. RFC 2406

[18] Recommendations for implementing the strategic initiative Industrie 4.0. April 2013. Found on 22 August at: http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf