Proceedings of GPPS Forum 18
Global Power and Propulsion Society
Montreal, 7th-9th May 2018
www.gpps.global

GPPS-2018-0149

CLOUD BASED IMPLEMENTATION OF A GAS TURBINE REMOTE MONITORING SYSTEM

Sunit Oliver
Vericor Power Systems, LLC
sunit.oliver@vericor.com
Alpharetta, GA,USA

Dr. Martin Engber
Vericor Power System, LLC
martin.engber@vericor.com
Alpharetta, GA, USA

Ryan Mich
Microsoft Corporation
rmich@microsoft.com
Wrightstown, NJ, USA

Deep Bohra
Microsoft Corporation
deep.bohra@microsoft.com
Alpharetta, GA, USA

ABSTRACT

Vericor Power Systems is introducing remote performance monitoring capabilities for their aero-derivative commercial marine and industrial gas turbine product lines. Historically, Vericor has been focused primarily as an OEM of military marine engines and is now looking to expand their footprint into non-military markets. The expectation from industrial customers is that remote performance monitoring is not only a desired feature, but a necessary minimum capability. Vericor has provided custom remote monitoring solutions on an as needed basis in the past. However, in order to stay competitive, the need was identified to provide a standardized remote performance monitoring offering. A development program was initiated with the intent to rapidly bring to market a robust, quick to deploy solution. During the conceptual design phase, existing technologies were evaluated for suitability as a platform for data storage and analytics. Traditional solutions relied on the incorporation of a network server housed within Vericor's corporate IT infrastructure for field data collection. A data historian software package would be used for analytics and reporting functions. Recent trends in the internet technology space have made cloud computing more prevalent than ever. Cloud based platforms were evaluated during the conceptual design phase and were found to have several advantages over corporate based servers. Ultimately Vericor elected to proceed with the development of a cloud based platform for their remote performance monitoring system. This paper dives into the selection process, reviewing the relative strengths and weaknesses of each platform type in the areas of availability, maintainability, analytic capability and cybersecurity.

BENCHMARKING BEST PRACTICES

The power generation industry has a rich history of turbine performance monitoring and diagnostics. Power plants have long made use of data historians to gather and archive data for long term storage and performance analysis. A data historian is typically a software package, such as OSI PI® running on a server connected to the plant's equipment network. Data is collected from various plant assets through the network using industry standard protocols such as Modbus, DNP3, EtherNet IP, EGD, OPC, etc. Since the network is dedicated to plant equipment and is located inside the plant's firewall, the data is usually transmitted unencrypted to the data historian.

Remote access to the data historian and/or other plant equipment can be established through the use of a dedicated private network or a virtual private network. This allows the utility's central office and/or equipment OEMs the ability to view and analyze data from remote locations. A depiction of this type of architecture is included in the block diagram of Figure 1.

For smaller power generation units used in distributed generation, Supervisory Control and Data Acquisition (SCADA) systems are often used for both remote monitoring as well as remote control of assets (Boyer, 2010). SCADA equipment is varied in form factor but typically is a software package running on a server. The SCADA can be paired with a data historian, colocated with the SCADA or located remotely from the SCADA. SCADA packages can also have integral data historian features. For portable equipment (e.g. diesel gen sets) OEMs can provide SCADA edge devices to communicate with a central server through a LAN or cellular connection.

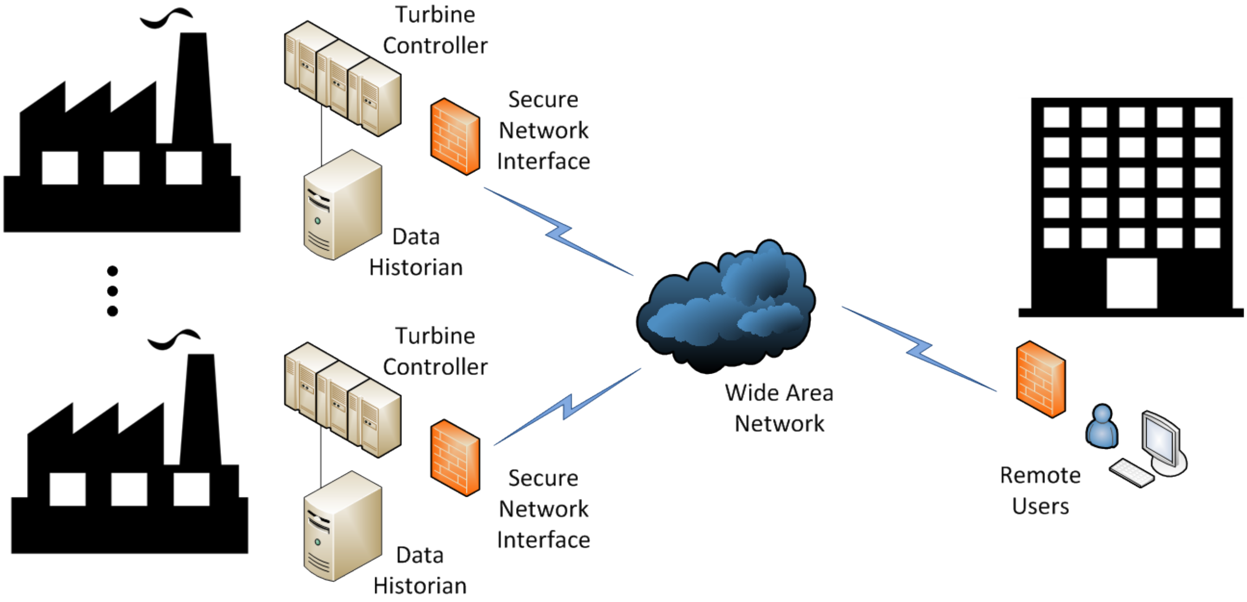

FIGURE 1 TYPICAL POWER PLANT DATA HISTORIAN REMOTE ACCESS

THE CYBERSECURITY THREAT

For years, cybersecurity threats were thought to be limited to devices using PC based operating systems. Industrial controllers were thought to be immune since they often run on proprietary operating systems. This strategy of security through obscurity was thought to be adequate.

That all changed when the details of the Stuxnet cyber-attack were fully understood (Broad, et al, 2011). This was the first major incident in which an industrial control system was successfully exploited. Stuxnet demonstrated the ability to gain access to a control system, modify control parameters, manipulate reported data and issue commands for malicious intent.

This spurred the industry to formalize standards for cybersecurity, adopting best practices, such as the ISA/IEC 62443 series, commonly referred to as ISA99 (ISA, 2009). Additional best practices are described in documents from the US Dept. of Commerce (Stouffer, et al, 2011) and the US Dept. of Homeland Security (CPNI, 2011). These guidelines were used in the development of Vericor's remote performance monitoring system.

The best practices involve developing a defense in depth strategy in which there are multiple layers of security, such as:

- Physical security of the equipment
- Physical and logical network separation through the use of firewalls
- Network isolation of equipment in a Demilitarized Zone (DMZ)
- Encryption of data transmission using IPSec standards
- Establishment of virtual private networks to keep traffic isolated from public networks
- Remote distribution of equipment security patches
- Managed user privileges and the use of multi-factor authentication.

VERICOR'S CHALLENGES

Vericor has specific challenges in deploying a remote monitoring system for their gas turbine product line. Vericor's commercial marine and industrial engines are rated in the 4,000 to 5,500 horsepower range (roughly 3 to 4 MW). The compact, lightweight design of these engines allows them to be used in smaller commercial marine craft that have limited space and accessibility in the engine rooms and/or bridge. Industrial engines of this size can also be trailer mounted for portable applications. As such, they are often operated in remote locations without manned control rooms. In both cases, the infrastructure does not exist to allow the kind of networked data historian scheme used in larger power plants.

A SCADA based scheme using small form factor edge devices colocated with each engine controller is a viable solution. The SCADA software would reside on a server located within the OEM's IT infrastructure, behind the corporate firewall. This method can present challenges for some organizations in which there are limited resources for maintenance and administration of specialized IT equipment such as the SCADA server. IT expertise is required to establish the network security configuration, such as the DMZ. Additionally, the maintenance of user profiles along with user access restrictions and account authentication are typically outside the core expertise of a gas turbine OEM, but are necessary for a robust, secure solution.

CLOUD COMPUTING EVALUATION

Over the years a convergence of technologies has led to the emergence of the IoT (Internet of Things) and the pervasive use of cloud computing. All the major cloud service providers offer similar features that are useful for deploying a remote monitoring system.

- Integration with IoT devices
- Data cleansing and filtering

- Long term data storage
- Visualization tools
- Computing platform for data modelling
- Predictive analytics
- Machine learning
- User account administration
- Platform security

This feature set made the usage of cloud services very appealing over the establishment of an in house SCADA server. However, the relative advantages/disadvantages of a cloud platform vs. an on premises server needed to be understood to make a sound judgement for the architecture to be used for the remote monitoring system. The platforms were evaluated for system availability, maintainability, analytic capability and cybersecurity.

Availability

A robust and reliable remote monitoring system depends upon a hosting platform with high availability. This aspect is important since it impacts the customer experience directly and reliability issues could potentially damage the OEM’s reputation. The availability of an on premises server is dependent upon hardware reliability, environmental controls and the skill of IT professionals to limit down time. As such, availability can vary, but it can be expected to be similar to that of a cloud based platform (Ward, 2012).

The top cloud providers all specify a minimum guaranteed availability. If availability falls below this threshold, the service provider will extend a service credit. As such, they are incentivized to maintain a highly reliable platform.

Maintainability

Maintainability refers to the overall life cycle effort required to sustain the operation of the platform. This includes the need to maintain a secure climate controlled physical installation, perform routine server maintenance and address server downtime. From the perspective of the OEM, outsourcing these responsibilities to the cloud services provider is beneficial since it eliminates that burden from the internal organization.

An additional aspect of this attribute pertains to licensing. With an on premises server, software license agreements are required for the operating system, data historian software, analytical tool software, etc. In many cases, each license agreement may be with individual companies. One strong benefit for cloud solutions is that all the major cloud services providers can include each of these features under a common license agreement. An entire set of features are available, but only those that are required for the remote monitoring system are enabled.

Scalability is also a key consideration for maintainability of the system. As more and more engine data is collected, the system needs to be able to expand to handle the increasing capacity. With an on premises model, the peak demand needs to be known in order to acquire a server and equipment to handle the forecasted load. If the forecast is too high, or if the service is slow to be adopted, the system will be oversized with unused capacity. If the system is undersized, or growth is faster than expected, the server may have to be replaced with a larger server with more capacity. Cloud services are meant to scale out as opposed to scaling up. In addition, pricing is consumption based, not capacity based, wherein the OEM pays for what is used.

From both a software and hardware perspective, platform upgrades are also pertinent to the maintainability of the system. Hardware becomes obsolete and software, especially in regards to look and feel, can become dated. Hardware upgrades have obvious cost implications. Depending on the licensing agreement, software upgrades may include additional fees. For either type of upgrade, a disruption in service can be expected while the transition takes place. Since cloud service providers are in competition, they are incentivized to continually upgrade their systems and expand their feature sets. When upgrades are made, they appear seamless to the end user. When new features are made available, they can be added to the remote monitoring system at the discretion of the OEM.

Analytic Capability

One of the necessary features of the remote monitoring system is the ability to perform analytics on the engine data and drive alerts when anomalies are detected. Modelling allows for the implementation of a Digital Twin that is used to determine engine performance degradation long before a control system alarm or trip threshold is reached. The digital twin can be implemented as a physics based model (Kraft and Kuntzagk, 2017), or can use other Machine Learning techniques such as Advanced Pattern Recognition (APR).

Most data historian packages include long term data storage and the ability to configure alert thresholds. Advanced modelling is generally left to other software packages. All the major cloud service providers include computational capabilities for implementation of an OEM specific physics based model. They all also have available advanced analytic capabilities including machine learning that can be used to implement predictive maintenance models to increase engine uptime and performance.

Cybersecurity

The most critical aspect of implementing a remote monitoring system is ensuring that it incorporates robust cybersecurity protection. A cybersecurity breach could have a direct negative impact on engine operations. Even a benign attack that resulted in no physical harm, but only a breach of engine data, could negatively impact the OEM’s reputation.

With an on premises server, the responsibility of maintaining cybersecurity protections resides in house. This includes the design of the network architecture to implement best practices, such as a DMZ. There is also the need to continuously monitor for security breaches and stay abreast of the latest known security exploits, rolling out patches as needed. One aspect that should not be neglected is the need to restrict physical access to the server.

Because cloud service providers have numerous customers, they are incentivized to ensure security breaches do not impact their operability. They are also staffed with cybersecurity experts that are aware of the latest threats and often have patches in place before the exploits become public knowledge (Schilling, 2017). In addition, cloud service providers have tools in place to monitor for suspicious system activity that could indicate a security issue.

Another aspect of cybersecurity pertains to the flow of data from the edge device to the main platform, whether that is an on premises server or a cloud platform. One of the best practices described in the industry guidance is the use of encrypted data transmission. With an on premises server running a data historian package, encryption is a feature that can be enabled but is the responsibility of the platform owner to implement. The major cloud service providers that support IoT connections require transmissions to be encrypted using TLS/SSL protocols (part of the IPSec standards). Additionally, initiation of the edge device connection to the cloud must be secured using an X.509 certificate or an SAS token for authentication. These features secure the transmission of data by only allowing authorized devices to transmit and keep the edge device traffic isolated from other internet traffic.

Users of the system require authentication as well. With traditional data historian packages this is accomplished through standard username and password confirmation at the local level. Newer packages also include remote authentication over a network. One common feature of cloud based platforms is the ability to enable multi-factor authentication on a user by user basis. This feature reduces the opportunity of unauthorized access to the system.

SELECTED SYSTEM ARCHITECTURE

After considerable evaluation, the selected system architecture was structured around a cloud based platform. A block diagram is included in Figure 2. The two major components of the system are the edge device and the cloud platform, both highlighted in blue.

The edge device is referred to as the Engine Data Manager (EDM). It communicates directly with the Gas Turbine Controller (GTC), which exists for every installation, to gather engine data. The EDM is an IoT device that includes a cellular gateway and an integral firewall to limit communication only to authorized devices. The EDM transmits data through the cellular connection using a standard IoT protocols, such as MQTT and AMQP. The transmission is encrypted using TLS/SSL protocols and X.509 authentication between the EDM and the cloud platform. In the event that cellular communications are unavailable, the EDM can fail-over to use hardwired, Ethernet or WiFi communications.

The other primary component of the system is the cloud based platform that is referred to as the Fleet Data Manager (FDM). The FDM is Vericor’s designation for the collection of cloud based tools and apps that together produce the specified functionality. Vericor partnered with Microsoft to execute and host the FDM. All user interaction with the remote monitoring system is through the FDM.

Data from the EDM is ingested and then filtered and aggregated based on information linked to the engine serial number. Data is retained in long term storage and kept segregated by engine serial number to limit customer access to data for only those engines that they own.

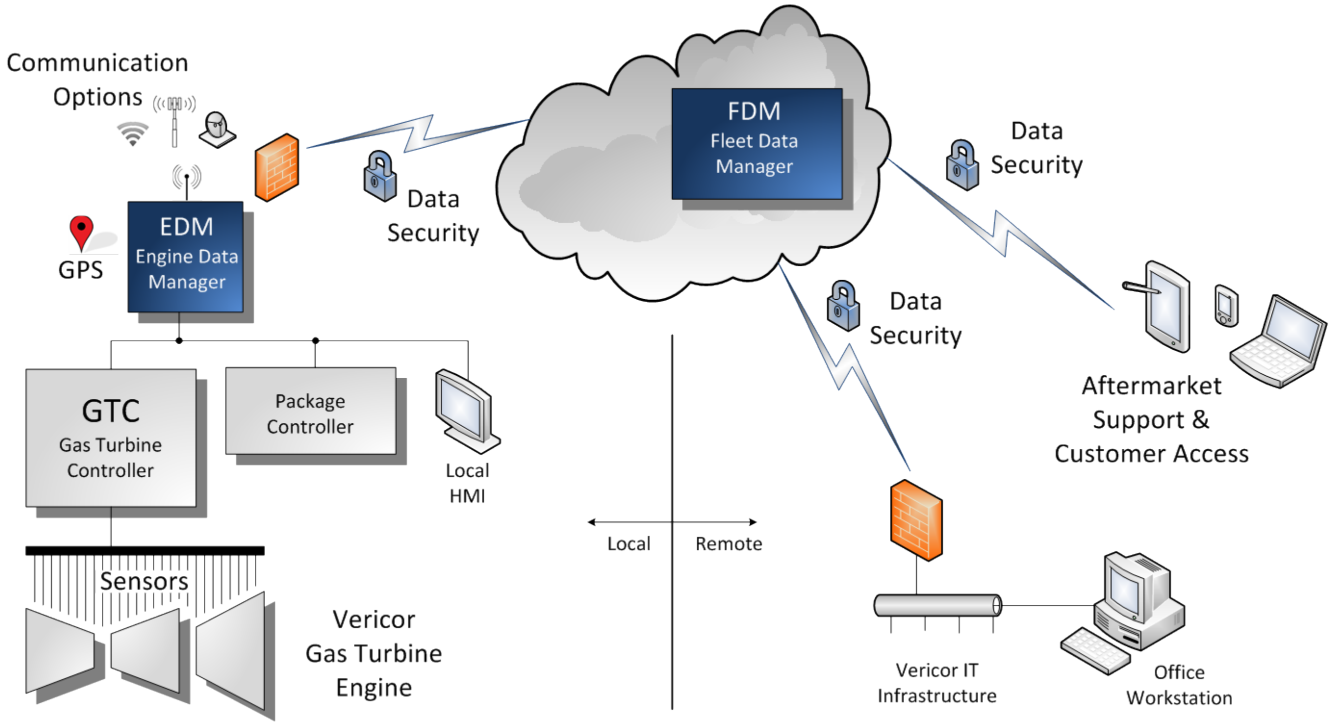

FIGURE 2 CLOUD BASED IMPLEMENTATION

The digital twin performance calculations are also executed within the FDM on a realtime basis as the data is ingested. User access and authentication are handled from within the cloud based platform. The cloud based platform also provides the tools for quickly implementing dashboards and reports to visualize engine data. The dashboards and reports are easily shared between those users authorized for the system. Screenshots of the system user interface are included in Figure 3 for various form factors.

As described in the previous section, there are several key criteria that are important considerations for a remote monitoring system; availability, maintainability, analytic capability and cybersecurity. The final architectural solution precipitated out of the process of analyzing each of these criteria.

Availability is important to Vericor since the remote monitoring capability is needed to provide the data necessary to evaluate fielded engine performance. This allows Vericor to offer enhanced aftermarket support and extended warranties. An outage resulting in the loss of data hampers the ability to execute these services and could result in the loss of revenue. Both an on premises server and a cloud based platform were evaluated to offer similar availability. However, the contractually guaranteed availability of the cloud platform pushed the design in that direction.

Vericor places a high value on system maintainability. As described in the previous section, this includes ease of implementation, ability to scale out and consistent system upgrades. While an on premises server can allow direct control over the asset, the utilization of a cloud based platform is more attractive to Vericor since it requires fewer resources for system maintainability and can seamlessly grow as the business grows.

Analytic capability allows Vericor to have greater insight into engine performance. The evaluation showed that implementation of the digital twin would be easier on a cloud based platform than with an on premises server. An added benefit of the cloud based platform is that the available visualization tools allow the system to incorporate a rich user experience. This is an important aspect for Vericor since it spurs customer adoption of the system and can help keep them engaged for the long term. The analytic and visualization advantages of a cloud based system, gave it a clear advantage over an on premises server.

Early in the design evaluation, it was recognized that cybersecurity would be of paramount importance and would need to be considered in all aspects of the system architecture. As described in the previous section there are numerous cybersecurity advantages when using any of the major cloud services providers. In addition to the

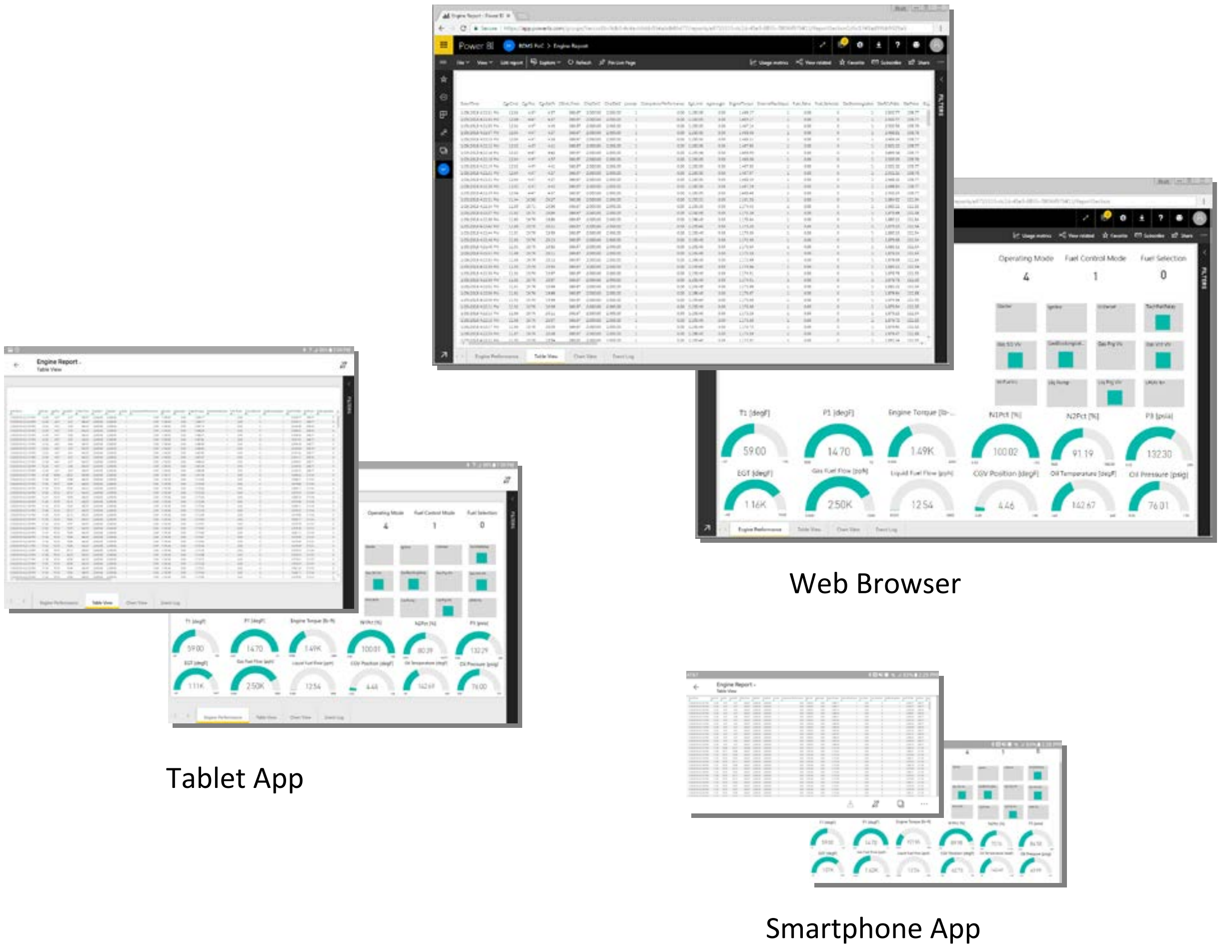

Figure 3 System User Interface in Various Form Factors

cybersecurity best practices described in the previous section, the decision was made to limit communication to one way only, from device to cloud (EDM → FDM). Cloud to device communications are disabled as an added cybersecurity feature. Another key aspect to the system architecture is that all user interaction takes place with the FDM only. At no point does an end user connect directly to any of the fielded EDMs. This separation is a key cybersecurity feature of the architecture that limits exposure to the EDM. With the typical power plant scheme depicted in Figure 1, system users have direct access to the data historian which is on the same network as the turbine controller. This exposure could lead to a potential exploit by malicious actors. These cybersecurity considerations heavily influenced the design decision to use a cloud based platform for the FDM.

SUMMARY

In order to remain competitive in the industrial markets, it was imperative for Vericor to quickly implement and deploy a remote monitoring system. The recent emergence of IoT technology and cloud services provided new tools to allow Vericor to quickly introduce this capability, greatly reducing the resources needed to design and deploy the system. The remote performance monitoring system adds value for external customers to understand the performance of their engines, as well as internally for Vericor to understand how customers utilize their engines.

While there are many legitimate concerns for hosting a remote monitoring system on a cloud based platform, the assessment presented in this paper demonstrates that these concerns can be adequately addressed. Cybersecurity concerns especially need to be considered from the beginning of the program. Vericor's research has shown that many of these concerns have already been considered by cloud service providers with solutions built into the platform. A cloud based remote monitoring system is shown to be a viable solution with no greater risks than that of an on premises based system.

As of the writing of this paper, Vericor's system is in the beta phase of the development program, and is only deployed to a few users. The system has demonstrated promising capabilities providing insight to engine operation for Vericor Aftermarket services and Performance Engineering. The system development is progressing rapidly with the expectation of commercial readiness by the beginning of 2019.

NOMENCLATURE

APR	Advanced Pattern Recognition
DMZ	DeMilitarized Zone
EDM	Engine Data Manager
FDM	Fleet Data Manager
IT	Information Technology
IoT	Internet of Things
SAS	Shared Access Signatures
SCADA	Supervisory Control And Data Acquisition
WAN	Wide Area Network
X.509	type of public key certificate

ACKNOWLEDGMENTS

The authors would like to acknowledge the numerous contributions made in the field of remote asset monitoring, cloud computing and the Internet of Things. Without these prior efforts, the task of developing and deploying a remote monitoring solution would have been monumental.

REFERENCES

[1] Boyer, Stuart A. (2010). SCADA – Supervisory Control and Data Acquisition – 4th Edition. ISA – International Society of Automation, Research Triangle Park

[2] Broad, William J., Markoff, John and Sanger, David E. (2011) Israeli Test on Worm Called Crucial in Iran Nuclear Delay. The New York Times (15 January 2011). http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

[3] ISA/IEC 62443-2-1 (99.02.01) (2009). Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program. International Society of Automation / International Electrotechnical Commission

[4] Stouffer, Keith., Falco, Joe and Scarfone, Karen. (2011). NIST Special Publication 800-82 – Guide to Industrial Control Systems (ICS) Security – Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) – Recommendations of the National Institute of Standards and Technology. US Department of Commerce (June 2011)

[5] CPNI Paper (2011). Configuring & Managing Remote Access for Industrial Control Systems – Centre for the Protection of National Infrastructure – U.S. Department of Homeland Security – Control Systems Security Program – National Cyber Security Division (April 2011)

[6] Ward, Jenny (2012). Cloud Software vs. On-Premises: System Availability. DSD Inc. Blog (23 August 2012) https://www.dsdinc.com/2012/08/23/cloud-software-vs-on-premises-system-availability/

[7] Kraft, Joern and Kuntzagk, Stefan (2017). Engine Fleet Management – The Use of Digital Twins From an MRO Perspective. Proceedings of the ASME Turbo Expo 2017. American Society of Mechanical Engineers.

[8] Schilling, Jeffery (2017). When Shifting to the Cloud Offers More Security. Forbes Magazine. 15 August 2017. https://www.forbes.com/sites/forbestechcouncil/2017/08/15/when-shifting-to-the-cloud-offers-more-security/

[9] McLaughlin, Pete and McAdams, Rohan. (2016). The Undiscovered Country: The Future of Industrial Automation. Honeywell Process Solutions White Paper (January 2016). https://www.honeywellprocess.com/en-US/online_campaigns/IIOT/Documents/The-Undiscovered-Country.pdf

[10] Microsoft (2017). Drive Digital Transformation of Your Business with Microsoft Azure. Microsoft White Paper (April 2017). https://www.microsoftpartnerserverandcloud.com/_layouts/download.aspx?SourceUrl=/Hosted%20Documents/Azure%20Digital%20Transformation%20Whitepaper.docx