HOW TO ID IOT SOLUTIONS WITHOUT FEELING LIKE AN IDIOT: AN APPLICATION PERSPECTIVE

Paper No. PCIC-

Joseph M. Manahan
Eaton
1201 Wolf Street
Syracuse, NY 13208 USA
joemanahan@eaton.com

Rebecca Templet
Shell Chemicals
7594 Louisiana 75
Geismar, LA 70734 USA
rebecca.templet@shell.com

Carlos Estevez
Schlumberger
23500 Colonial Parkway
Katy, TX 77493 USA
cestevez@slb.com

Dennis Grinberg
Eaton
1000 Cherrington Parkway
Moon TWP, PA 15108 USA
dennisngrinberg@eaton.com

Abstract – The internet of things (IoT) or industrial internet of things (IIoT) has incredible benefits and potential for much more. It promises vast improvements in operational efficiencies and reduction of catastrophic failure. The full benefits of such technology may be limited by incompatibilities due to manufacturer protocol and device differences. These challenges will be passed on to the user resulting in diminished benefits and frustration if not anticipated and mitigated accordingly.

This paper will explore available technologies and address guidelines for future standard and specification development while providing parallels to similar technology introductions in large scale industrial facilities for the review of lessons learned.

Index Terms — Internet of Things, Big Data, Hazardous Area, Connected Devices, Sensors, Network, SCADA

I. INTRODUCTION

The internet of things (IoT) and industrial internet of things (IIoT) promise to revolutionize manufacturing and life itself as we know it. While IoT devices will enhance the lives of many in the form of smart fitness devices or smart coffee makers, for example, providing health and convenience benefits, IIoT devices will improve safety and efficiency for mission critical industrial applications where millions or billions of dollars could be at stake for a single application should the integrity or security of the data IIoT devices transmit be compromised. If you are an engineer responsible for the design, construction or maintenance of complex systems you've inevitably heard these promises and begun assessing how IIoT might impact your role and your business. A quick search of IEEE Xplore® yields some astonishing results in the relevant fields of IoT. For example, a keyword search of "industrial internet of things" cites roughly 1,500 references. Broaden that search to "internet of things" and the references climb to nearly 19,000. Broaden the scope further to something similar to "wireless sensor" and you'll be overwhelmed by nearly 90,000 references. Take these searches to your average web search engine and these numbers increase exponentially. So where does one begin if they seek to be proactive in capitalizing on the promises of a more "connected" business?

If you're reading this paper, there is a likelihood that you think you might be or fear you are the "IDIoT" this paper warns of. The authors of this paper would argue that if one is actively seeking knowledge than those doubts are unwarranted. To help prepare for the inevitability of widespread IIoT, this paper will attempt to help prioritize how to approach a deployment strategy while addressing the most common challenges in highly secure industrial facilities.

While IoT and IIoT are relatively new terms that have evolved over the last decade, the concept dates back to the mid twentieth century where it was identified that any one machine or system can be connected to another machine or system [1]. Since that time, we have witnessed systems grow increasingly more complex while managing the tasks of several interdependent sub-systems in computers, automobiles and air travel to name a few. In the context of a large petro-chemical facility or process, there are no shortage of complex systems already leveraging some level of interdependency through existing supervisory control and data acquisition (SCADA) systems and other networking solutions. The advent of IIoT is poised to strain these existing systems by the sheer volume of data they will produce. The Industrial Internet Consortium suggests the success of IIoT relies on the convergence of operational technology and information technology and is driven by technology advances in ubiquitous connectivity and pervasive computation [2].

It would be short-sighted to look at the impact of IIoT on one business or facility alone. The European Union has emphasized that IIoT promises to blur the lines that traditionally divide the markets including manufacturing, transportation, utility and healthcare. For example, this will be accomplished by leveraging common platforms of data management to coalesce for new insights, services and value creation opportunities [1]. While economic impact estimates of IoT and IIoT may vary greatly, they are none the less staggering. Experts suggest that by the year 2020 over 20 billion devices will be connected, annual spending on IoT related development will approach $16 billion and annual revenue will reach $8.9 trillion [1, 3]. In deploying successful IIoT devices, the challenge remains in bringing the data together in a secure and affordable way that provides the performance, flexibility and scale needed. Table I illustrates the forecasted developments in IIoT by connection type while comparing them with respect to key evaluation criteria [1].

TABLE I

		Wireless access type		
		High power wireless	Low-cost wireless	Low-power wide area (LPWA) wireless
Growth/application	Forecasted connections by 2020	>2 billion	>5 billion	>11 billion
	Sample applications	Driverless cars, video surveil-lance	Smart home	Sensors, utility meters
	Sample technologies	LTE-A Pro, 802.11 ac/ax	LTE, HSPA, Bluetooth, 802.11 n	NB-IoT, EC-GSM, Sigfox, LoRaWAN
Evaluation criteria	Performance	√√√	√	√
	Energy	√	√√	√√√
	Cost	√	√√√	√√√
	Coverage & capacity	Flexible	Flexible	√√√

As the adoption of IIoT devices increases in traditional industrial environments, coupled with the ease and cost effectiveness of these network technologies, the opportunity to partially or fully replace the existing infrastructure will develop [4]. Whether partial or full replacement of the infrastructure is required, there persists the challenge to find the appropriate link layer technologies to bring the network together. In doing so, the same emphasis on security will persist as it has within the traditional infrastructure. As IIoT deployments become more pervasive going beyond monitoring and into the control system, security takes on a new meaning of safety as well. Safety comes in the form of both human lives and catastrophic environmental consequence if not mitigated properly [5].

In addition to the technical challenges impeding mass deployment of IIoT devices, significant challenges in compelling and accepted business models remain. While human safety is paramount to most oil and gas operations, and industrial applications as a whole, it is often the most challenging to create financial models around. Instead, we often focus on the easier models to articulate and justify, such as energy or maintenance savings, which lack sufficient catalyst to promote the technology effectively. Critical to the velocity and success by which IIoT will be eventually mass deployed are the myriad of early adopters who see the potential and financially supplement the industry's development in improved solutions and governing standards [3]. It is likely more critical for a business to consider the right IIoT deployment strategy, with respect to business readiness, infrastructure optimization and future expansion, than it is to consider solutions on the basis of the specific problem it solves at the time.

The remainder of this paper is organized as follows. Section II reviews the results of an oil and gas industry survey across both upstream and downstream businesses to assess perceived IIoT benefits and risks. Section III will highlight some of the obstacles that arise in focusing on solving specific sensing challenges without properly considering the broader network requirements and lessons one has learned from similar technology deployments. Section IV examines the best practices for addressing cybersecurity while Section V highlights opportunities and methodologies for securely leveraging the internet for process functions. Section VI attempts to take the learnings and apply them to a broad deployment strategy in the context of an oil and gas application.

II. WHERE ARE WE NOW? A SURVEY OF TWO OIL AND GAS INDUSTRIALS

If the industry is to address the challenges of widespread IIoT deployment, one must first identify and understand what those challenges are. In an effort to do so, the authors have distributed a survey to a variety of individuals in a large oil and gas refining business (downstream) as well a large services business heavily focused on drilling (upstream) in order to gain perspective on the perceived benefits and challenges of IIoT technology. Of the survey respondents, the results are distributed fairly evenly with approximately 58% of the response coming from upstream businesses and the remaining from downstream businesses as shown in Figure 1.

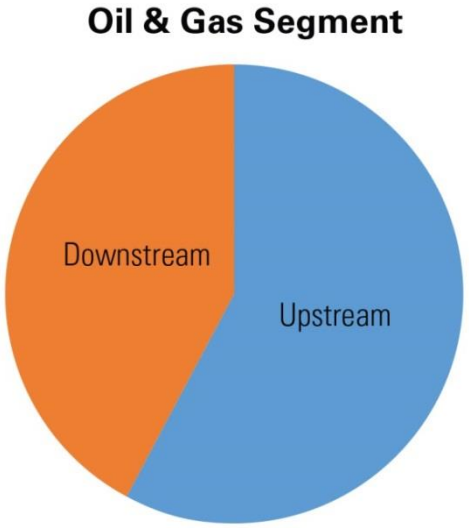

Fig. 1 – Distribution of survey responses by oil and gas industry segment

While it is important to assess the perspective of various business entities within the oil and gas value chain, it is perhaps equally as important to consider the perspectives within each segment by functional role and level of responsibility within the organization. As most would agree, it takes more than a good idea to make change. IIoT inherently will involve an entire organization's resources to successfully specify, procure, provision, analyze and maintain the systems one creates with it. If any one of the functional areas does not execute to the chosen strategy, the results will likely fall short of the intent if deployment can be achieved at all. Figure 2 breaks down the survey responses by functional role, level of influence and industry experience.

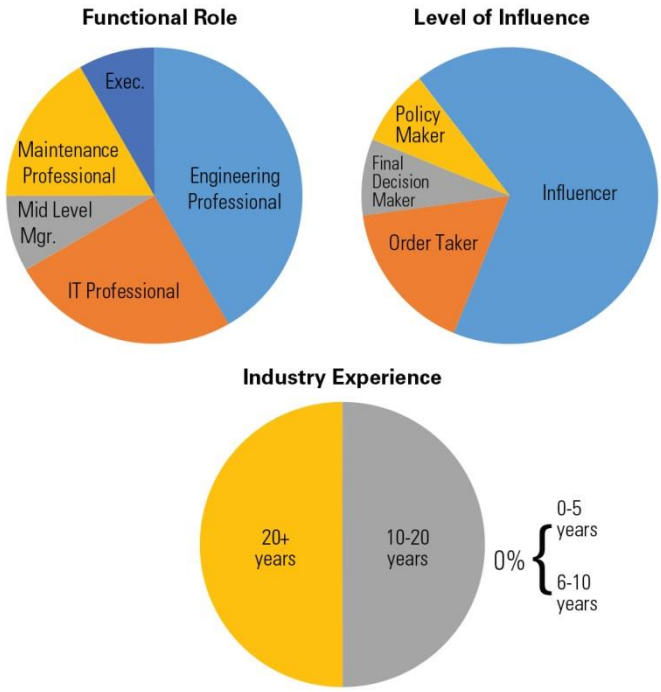

Fig. 2 – Distribution of survey responses by functional role, level of influence and industry experience respectively

Those surveyed were asked a series of questions related to the perceived benefits and challenges IIoT technology would evoke within their businesses. They were also asked questions pertaining to the role the internet and/or third party service providers might play in IIoT deployment along with strategies for aggregating data from multiple OEM equipment and IIoT device suppliers. Lastly, the survey asked a series of questions in an effort to quantify one of the promised benefits of IoT, reduction in equipment failure, by identifying the economics of the downtime presently experienced in these facilities all of which is summarized in Appendix A at the conclusion of this paper.

While the survey asked many questions it is important to be grounded in both the benefits and challenges those surveyed perceived in the future adoption of connected technologies. It is only with this understanding and focus that the industry can respond with targeted solutions having the greatest influence on the rate of adoption and return on investment. Of the ten potential benefits from IIoT provided, those surveyed decisively identified safety and improved operational efficiency as significant benefits with reduced downtime identified as a moderate benefit. All other choices appear to be of modest benefit. Despite predictions that IIoT will bring industries and supply chains closer together [1], those surveyed indicated improved customer relationships and improved supplier products or services were among the lowest perceived benefits. The full comparison of perceived benefits can be seen in Figure 3.

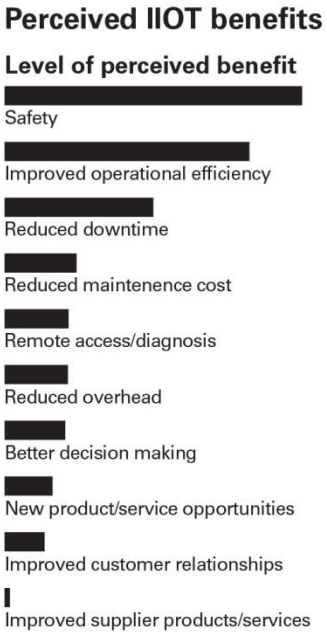

Fig. 3 – Rank order of survey responses by perceived benefit (highest benefit to lowest benefit)

In order to realize any of the perceived benefits that connected technologies can deliver one must acknowlege and mitigate the risks or impediments that preclude successful deployment. Not surprisingly, the survey revealed definitively that perceived security threats and the resulting loss of process control is the most significant challenge of IIoT adoption. Perceived loss of intellectual property and legacy infrastructure should be considered moderate risks and all others appear to be low risks by comparison. Figure 4 summarizes the data in order of perceived risk.

Fig. 4 – Rank order of survey responses by perceived risk (highest risk to lowest risk)

While organizational resistance appeared to be of low risk, it should be noted that 17% of those surveyed perceived that the use of IIoT, or internet connected solutions and services, was unlikely in their business within the next five years. Of those that perceived internet connected solutions were unlikely to impact their business, 50% were in a position of authority (policy and/or decision maker).

The remainder of the paper will focus on the critical risk areas identified in the survey to bring greater awareness to mitigation strategies after first reviewing what lessons one can transfer from other recent technology introductions to industrial facilities.

III. THE PITFALLS OF SHORT-SIGHTED DEPLOYMENT

An entire paper could be dedicated to the lessons learned from deploying a new technology for the first time and only later realizing the compromises unknowingly made in the process. Instead of relenting on the possibilities, this paper will focus on a small group of important points to understand as one endeavors to evolve their corporate policy with respect to IIoT.

1) The perception of new security threats related to IIoT are genuine concerns that are getting much attention from the industry and third party standards bodies such as Underwriters Laboratory (UL). Initiated in 2016, UL created the Cybersecurity Assurance Program with a series of cybersecurity outlines under UL2900 [6]. National Institute of Standards and Technology (NIST) released their own *Framework for Improving Critical Infrastructure Cybersecurity* [7] in 2014. While both provide excellent guidance there is still some work to do for the industry to adopt a standard process.

2) Careful planning and prioritization of the variety of data to be transmitted is necessary to ensure both wired and wireless systems provide the performance desired. Unanticipated latency in the system will drive added cost and likely impede further pursuit of new applications for IIoT by the consumer.

3) Adoption may be most influenced by the ease of provisioning and interoperability between new IIoT devices of competing protocols and the legacy infrastructures they will reside within.

As the race for market position continues for device and service providers, many have raised concerns over the ensuing market fragmentation and ecosystem complexity by the volume of solutions available. Further, it will be those technologies that gain the greatest financial thrust during this period that will prevail due to the inherent economies of scale and not necessarily those that offer superior technological or performance advantages [1]. Successfully leveraging connectivity solutions from competing providers will prove to be a formidable task. It is imperative that each business develop its own strategy accounting for both legacy and new data compatibility and the scale at which the data will evolve over time. Building automation suppliers and system integrators will be forced to solve many of the fragmentation concerns caused by the variety of connectivity technologies such as wired or wireless, short-range or long-range and standard or proprietary protocol along with the middleware needed to facilitate them [1]. While 802.11 (Wifi) is the prevalent wireless technology in the office environments of petro-chemical facilities, 802.15.4 (best known as WirelessHART or ISA100.11a) is the predominant wireless technology in the process areas of those same facilities. Further complicating matters, Modbus, Ethernet and building automation and control network (BACnet) among others provide wired connectivity in these facilities as well. The variety of connectivity solutions poses significant challenges in scale and performance of the network. In a safety critical environment such as those found in petro-chemical facilities, maintaining control and managing latency are of utmost importance. In addition to system performance, specifiers must also consider system flexibility as the differences between devices, the varying quality of the raw data they produce and individual data analysis preferences of the user in order to yield the most value from the system [8].

The closest comparison offering insight in to IIoT adoption in petro-chemical and hazardous area applications may be light emitting diode (LED) lighting. Just over a decade ago, LED lighting for general illumination was introduced to petro-chemical facilities in hazardous locations as defined by the National Electrical Code and NFPA497 [9, 10]. Adoption of LED lighting in non-hazardous applications only preceded this trend by a few years. There is little argument over the benefits of solid state lighting and the improvements that can be gained in energy efficiency, control and safety. However, more than 10 years after the introduction of LED lighting the industry has yet to adopt a common practice for system reliability at the luminaire level, one of the most notable inputs in assessing traditional return on investment calculations. Likewise, while photometry standards exist for assessing lumen output and distribution, the consumer often specifies LED lighting based on perceived equivalency to traditional lighting without appreciation for how the photopic visual response may vary by lighting source [11]. The end result often leads to dissatisfaction with the lighting installation due to excessive light levels and/or diminished economic benefit from the conversion of traditional light sources to LED based technologies.

When comparing LED to IIoT adoption, both will have experienced exponential growth over their first 10 years of deployment. Both require early adopters as catalyst for growth. And the frustrations of that early adoption will create iterative enhancements to industry standards and stricter specifications to address those concerns. Despite these challenges, early adoption will come with the competitive advantage providing new data on the product, process or service along with intangible benefits to the products and services we don't yet understand.

IV. CYBERSECURITY

The survey results of this paper definitively identified cybersecurity as the most significant concern with respect to the future of connected devices and for good reason. In all aspects of life people are confronted with stories of cyber-attack including data breaches in healthcare, banking, merchants and the US presidential elections as a small subset of examples [11, 12, 13, 14]. The NIST *Framework for Improving Critical Infrastructure Cybersecurity* sums up why the petro-chemical industry, a vital contributor to the world economy, must continue to take the topic seriously. "The national and economic security of the United States depends on the reliable functioning of critical infrastructure". By design, IIoT systems will connect machines, sensors and actuators in oil and gas installations where a security breach could result in hazards to on-site personnel, productivity loss or significant financial impact. These risks may be mitigated by accounting for the following

requirements: data and user confidentiality and integrity, user authentication and authorization, service availability, data freshness and nonrepudiation to ensure IIoT devices cannot deny actions in addition to sensors manufactured such that they can only access data during the time they are commissioned [1]. These requirements likely necessitate changes to current security practices for traditional industrial control systems to ensure network stability and integrity. As these systems will employ actuators in some applications, posing greater safety risk, the security schemes should not be over simplified to traditional IT systems either.

The oil and gas industry experienced one of the most significant cyber-attacks in August of 2012. As CNN reported, in a matter of hours 35,000 computers within one major oil and gas company were partially or fully disabled. While oil production remained intact, all other business systems were in a state of chaos. Unable to facilitate procurement, tanker trucks were turned away for 17 days with the corporation finally relenting and *giving oil away* to address demand. While the financial impact has not been published, it can be assumed to be significant not only for the business targeted, but all those depending on the company's supply chain as well [15]. What financial impacts were realized by upstream and downstream supply chain partners? How would the world respond to up to 10% of its oil supply being at risk?

In the oil and gas cyber breach example, it was believed to be orchestrated by individuals from within the facility [15]. Accepting this conclusion, it is important to appreciate each of the areas by which a system is vulnerable. Figure 5 illustrates a cyber-physical production environment architecture and the vulnerabilities within it [5].

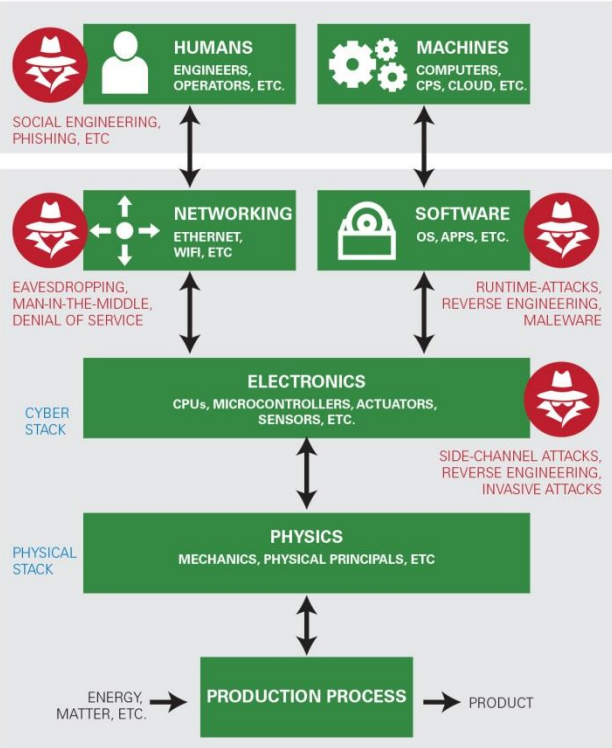

Fig. 5 – Typical cyber-physical production architecture and vulnerabilities

System performance and diversity of system architectures will emphasize the importance of machine-to-machine authentication in lieu of trusting only the protocol by which they communicate [16]. It is equally critical to safeguard the individual devices from malicious modification of their firmware or data to ensure secure operation of IIoT systems. While traditional IT systems may be temporarily disabled to address an attack, availability of process control and automation is of fundamental importance to petro-chemical facilities [5].

The NIST cybersecurity framework previously referenced provides structure for assessing risk in a connected environment. The framework is comprised of three primary parts: the Framework Core, the Framework Profile and the Framework Implementation Tiers. The implementation tiers range from Tier 1 (least) to Tier 4 (most) and denote the level of thoroughness in the risk management practice. The framework provides the criteria needed for consideration in any application. Table II is an abbreviated example illustrating the various functions and categories to be considered. Also included are example controlled unclassified information (CUI) and their descriptions.

Not all responsibility for adherence to cybersecurity best practices should fall on the system owners and specifiers. All parties involved in the supply chain must ensure compliance as well, hence the evolution of the UL2900 series of outlines [6] intended to validate compliance of IIoT devices and products.

TABLE II

Function	Category unique identifier	Category
Identify (ID)	ID.AM-1	Asset management
	ID.BE-1	Business Environment
	ID.GV-1	Governance
	ID.RA-1	Risk Assessment
	ID.RM-1	Risk Management Strategy
Protect (PR)	PR.AC-1	Access Control
	PR.AT-1	Awareness Training
	PR.DS-1	Data Security
	PR.IP-1	Information Protection Processes and Procedures
	PR.MA-1	Maintenance
	PR.PT-1	Protective Technology
Detect (DE)	DE.AE-1	Anomolies and Events
	DE.CM-1	Security Continuous Monitoring
	DE.DP-1	Detection Processes
Respond (RS)	RS.RP-1	Response Planning
	RS.CO-1	Communications
	RS.AN-1	Analysis
	RS.MI-1	Mitigation
	RS.IM-1	Improvements
Recover (RC)	RC.RP-1	Recovery Planning
	RC.IM-1	Improvements
	RC.CO-1	Communications

V. INTERNET VS. INTRANET

As described in the 2012 oil and gas cyber-attack, not all cybersecurity breaches occur with the internet as the primary vehicle to penetrating the network. Whether the preferred network solutions include cloud based services or not, cybersecurity measures need to be strategically planned and provisioned. While some organizations may be evaluating or initiating adoption of cloud based data services it is understood that most petro-chemical operations reside on traditional SCADA networks as illustrated in Figure 6. Procurement and business communications leveraging the internet are partitioned from process control and monitoring networks via the firewall.

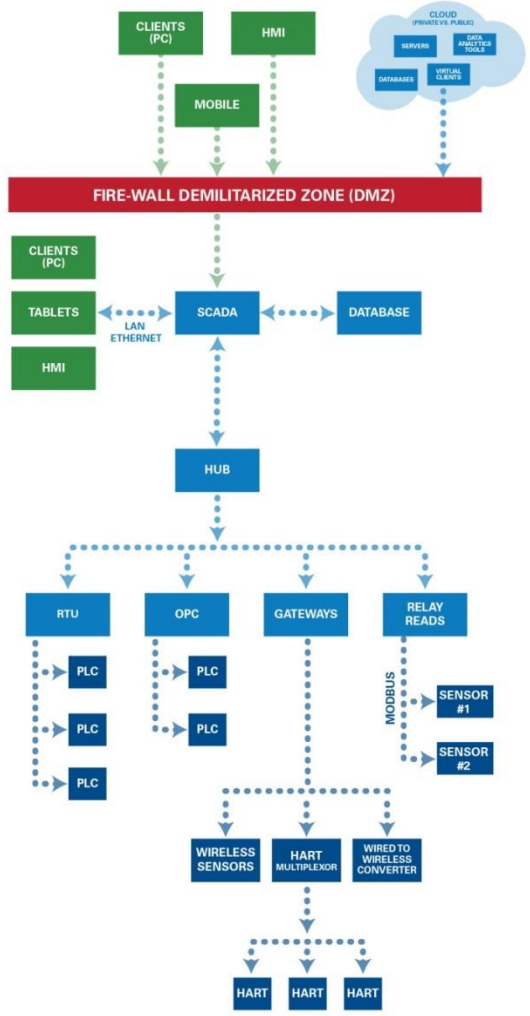

Fig. 6 – Traditional sensor network leveraging SCADA

As the demand for increasing business intelligence grows so will the data that will sustain it. So how does a business effectively utilize human and financial resources to anticipate, capitalize and maintain escalating data storage requirements? Is it practical to recapitalize a business's data center every two to three years as technologies evolve? The answers to these questions may suggest an opportunity to *responsibly* manage the coexistence of on premise and cloud based solutions. Figure 7 illustrates a typical hybrid architecture. Responsibility in this sense means more than simply a mindset, so one can again leverage a framework, similar to that published by NIST, to assist in methodically assessing the business needs and risks associated with each data set transmitted via the network. Some questions to consider may include:

- Should the data be breached, what are the potential ramifications of exposure?
- Does the data set identify personnel or other legally restricted data?
- Is the data directly related to process control?
- What risks are associated with uni-directional data flow from control networks to the cloud?
- What latency can the business accommodate compared with the latency of the chosen network solution?
- Who is the target audience for the data and how do they need it analyzed?
- Is the desired data within the core competence of your business to analyze?

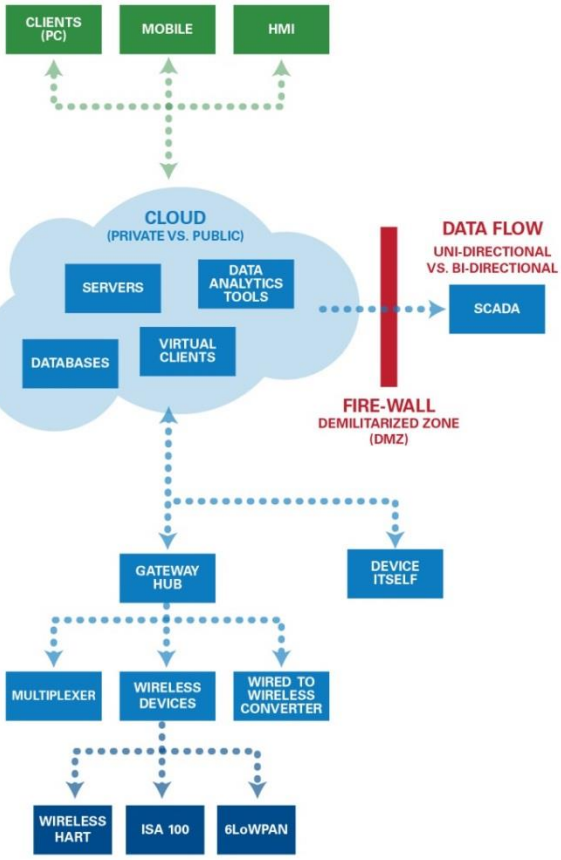

Fig. 7 –On premise & third party based data hosting architecture

Beyond these questions we must also consider how these risks may be mitigated by the devices themselves through fail safe designs including intelligent devices that leverage artificial intelligence (AI) to predict abnormalities or changes in behavior. Safety critical functions should be controlled by the local device regardless of an attack on the software. These provisions will secure remote attack while physical access control may be required to safeguard the system from attack within. An

example scenario in need of a fail-safe solution is a control system where the gateway or server either cannot deliver a data packet to the control valve or the control valve cannot authenticate the packet. In response to this situation, the control valve should reside in a safe state such as normally open or closed based on the process requirements [4]. While performance may not be optimal, provisions such as these will maintain risks at an acceptable level.

As the demand for IIoT devices increases it will become more and more burdensome to commission new devices, manage the data traffic and latency and seamlessly integrate the data into existing or new advanced analytics. To satisfy demand will require highly scalable solutions for data and device management. The sheer volume of data traffic may financially strain an organization's ability to consider cloud based storage, but therein lies an opportunity for equipment manufacturers and contractors to add scale as a function of the services they already provide. Local data management and analytics where necessary will improve latency and security but challenge a business's scalability; therefore, there should not be an either-or consideration but rather there should be a where and when allocation in the overall system architecture [5].

VI. DEPLOYMENT STRATEGY – BRINGING IT ALL TOGETHER FOR AN APPLICATION

The possibilities for improved safety and reduced maintenance resulting from advanced sensor networks and IIoT are nearly endless. It seems fictional to imagine an environment where process equipment systems can be tethered to each other and the humans they interact with to create a new immersive ecosystem that actively prevents catastrophic incidents and autonomously optimizes production, but IIoT is the mechanism by which this is possible. Why can't equipment authenticate an operator's credentials and enable functionality based on this authorization? Why can't that same equipment enable maintenance while validating that the technician adorns the proper personal protective equipment and provide the latest service instructions while also creating real time maintenance logs of the work performed? How can the lighting and other surveillance and safety systems be augmented to respond to changing work or environmental conditions while improving human response to accidents? Figure 8 provides a few examples of different potential IIoT developments that could be used to compliment process monitoring and control. While we may not witness all of these specific solutions, IIoT is poised to bring similar fantasies to fruition within the coming years. In this context, these possibilities are only shared to illustrate the scope by which IIoT could influence the industry and the planning required to capitalize on the solutions when available.

Fig. 8 –Futuristic view of IIoT within a petro-chemical facility

While this paper has addressed some considerations for system latency, there exist some standards for appropriate data delivery times in critical applications. The IEEE1646-2005 standard prescribes requirements for electric power substation automation [17]. While IIoT extends well beyond the substation, the process by which these recommendations were assessed is broadly applicable. Table III and IV, taken from the IEEE1646 standard, demonstrate the data or message types possible in application and the acceptable latency and transport performance criteria for each.

TABLE III

Information types	Internal to substation	External to substation
Protection information, high speed	1/4 cycle	8-12 ms
Monitoring and Control Information, medium-speed	16 ms	1 s
Operations and Maintenace Information, low-speed	1 s	10 s
Text Strings	2 s	10 s
Processed Data Files	10 s	30 s
Program Files	60 s	10 min
Image Files	10 s	60 s
Audio and Video Data Streams	1 s	1 s

TABLE IV

Communication message types	Priority	Criticality	Security	Integrity
Protection Information, high-speed	H	M	H	H
Demand Information, medium-speed	M	H	H	H
Periodic Information, medium-speed	M	M	H	H
Low-speed Operations & Maintenance Information	L	L	M	H
Text Strings	L	L	M	M
Processed Data Files	L	M	H	H
Program Files	L	H	H	H
Image Files	M	L	M	L
Audio and Video Data Streams	L	L	L	L

Comprehensive data models are necessary to account for the variety of data to be exchanged within a system or system of systems and account for the bandwidth available for communication of critical data. Control systems often operate with what is considered five nines, or 99.999%, availability and therefore must prioritize the data holistically [1]. Cost will likely be the biggest challenge in meeting this objective. Many IIoT applications do not require high throughput and low latency data transmission, which will constrict bandwidth and consume significant power. Instead, battery operated sensors can be an affordable deployment alternative in some applications. Further, single gateway solutions with multiple radios have been proven to have lower latency performance and optimal cost over multiple gateway solutions each with a single radio [18].

As previously mentioned, WirelessHART and ISA100.11a are prevalent in many petro-chemical facilities. Cecilio and Furtado demonstrated that the protocol is designed for fluctuating wireless performance yet can achieve 100% data delivery with a node duty cycle as low as 2.48% [4]. Duty cycle is an important consideration for each sensor type and while these protocols are prevalent today, latency can be a significant concern. This factor alone may be significant enough to necessitate development or deployment of alternative protocols for industrial monitoring and control as IIoT networks expand over time. To this extent, it is important to anticipate that the algorithms and data formats may change over time and therefore, organizations must ensure instruction exists for interpreting historical raw data if reformatting is necessary.

Standards development and public policy are likely influencers of IIoT adoption as well. For example, the European Union adopted a 20-20-20 renewable energy directive establishing their climate change goals in 2009 [3]. The 20-20-20 directive specifically targets at least 20% reduction in greenhouse gases, 20% energy consumption from renewable sources and 20% improvement in energy efficiency by the year 2020. Undoubtedly, these requirements will become more aggressive in the near future. How will IIoT enable the significant improvements needed to meet future objectives? How might IIoT address other environmental, political or regulatory pressures to improve waste and air quality, noise pollution, light pollution and energy efficiency? Regardless of those pressures, is one not obligated to exploit every opportunity to improve worker safety and environmental conservation that is financially plausible to ensure future sustainability?

VII. CONCLUSION

The authors have presented survey data from upstream and downstream oil and gas businesses to examine the highest perceived benefits and risks to deploying large scale sensor systems and IIoT. In an effort to help realize the enormous potential of IIoT and address the risks, available standards and accepted planning methodologies have been presented to enhance awareness.

As with any rapidly evolving technology introduction, early adopters of the technology serve as the catalysts for continued development and optimization. IIoT left up to select individuals to solve only specific tactical problems will stifle the potential opportunities and business improvements. Instead, each business requires a collective cross-functional strategy with thoughtful requirements and specifications for data management and system performance in order to ensure the scalability required for the eventuality of IIoT.

VIII. ACKNOWLEDGEMENTS

The authors would like to thank the employees of Schumberger and Shell Chemical who participated in the survey and provided valuable insights into the potential for IIoT deployment in the oil and gas industry. Special thanks are also expressed to Mike DiFlorio for his work on illustrations for the paper.

IX. REFERENCES

[1] D. B. van Lier, "The Indutrial Internet of Things: An ecological and systemic perspective on security in digital industrial ecosystems," in *IEEE International Conference on System Theory, Control and Computing*, Sinaia, 2017.

[2] "Industrial Internet of Things Volume G1: Reference Architecture," Industrial Internet Consortium, 31 January 2017. [Online]. Available: http://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf. [Accessed 19 January 2018].

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet of Things Journal,* vol. 1, no. 1, pp. 22-32, 2014.

[4] J. Cecilio and P. Furtado, "Providing timely actuation guarantees with heterogeneous SAN for industrial process control," in *IEEE Control Automation Robotics & Vision*, Guangzhou, 2012.

[5] A. Sadeghi, C. Wachsmann and M. Waidner, "Security and Privacy Challenges in Industrial Internet of Things," in *IEEE Design Automation Conference*, San Francisco, 2015.

[6] U. L. Inc., *UL 2900 Software Cybersecurity for Network-Connectable Products,* 2016.

[7] "Cybersecurity Framework," National Institute of Standards and Technology (NIST), [Online]. Available: https://www.nist.gov/cyberframework. [Accessed 19 January 2017].

[8] Y. Duan, W. Li, Y. Zhong and X. Fu, "A Multi-network Control Framework Based on Industrial Internet of Things," in *IEEE International Conference on Networking, Sensing and Control*, Mexico City, 2016.

[9] NFPA497, *Recommended Practice for the Classification of Flammable Liquids, Gases or Vapors and of Hazardous (Classified) Locations for Electrical Installations in Chemical Process Areas,* 2017.

[10] NFPA, "Article 501," in *NFPA70 NEC 2017 Edition*, 2017.

[11] A. Jayawardena, D. Duffy and J. Manahan, "Impact of light on safety in industrial environments," in *PCIC*, Houston, 2015.

[12] E. McCann, "Healthcare IT News," 10 September 2015. [Online]. Available: https://www.healthcareitnews.com/news/excellus-bluecross-blueshield-cyberattack-impacts-105m-people. [Accessed 23 January 2018].

[13] M. Snider and K. Whitehouse, "USA Today," 15 February 2015. [Online]. Available: https://www.usatoday.com/story/tech/2015/02/15/hackers-steal-billion-in-banking-breach/23464913/. [Accessed 23 January 2018].

[14] K. McCoy, "USA Today," 23 May 2017. [Online]. Available: https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/. [Accessed 23 January 2018].

[15] "CNN," 31 October 2017. [Online]. Available: https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html. [Accessed 23 January 2018].

[16] J. Pagliery, "CNN," 5 August 2015. [Online]. Available: http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html. [Accessed 19 January 2017].

[17] MacAfee, "2017 Threat Predictions," MacAfee Labs, 2016.

[18] IEEE1646, *Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation,* IEEE, 2004.

[19] J. Banik, R. Arjona, M. Tacca, M. Razo, A. Fumagalli, K. Vijayasankar and A. Kandhalu, "Improving Performance in Industrial Internet of Things Using Multi-Radio Nodea and Multiple Gateways," in *IEEE International Conference on Computing, Networking and Communications*, Santa Clara, 2017.

[20] "National Vulnerability Database," National Institute of Standards and Technology (NIST), [Online]. Available: https://nvd.nist.gov/. [Accessed 19 January 2017].

[21] S. Forsstrom and U. Jennehag, "A Performance and Cost Evaluation of Combining OPC-US and Microsoft Azure IoT Hub into an Industrial Internet-of-Things System," in *IEEE Global Internet of Things Summit*, Geneva, 2017.

[22] P. Lade, R. Ghosh and S. Srinivasan, "Manufacturing Analytics and Industrial Internet of Things," *IEEE Intelligent Systems,* vol. 32, no. 3, pp. 74-79, 2017.

[23] S. Mumtaz, A. Alsohaily, Z. Pang, A. Rayes, K. Tsang and J. Rodriguez, "Massive Internet of Things for Industrial Applications: Addressing Wireless IIoT Connectivity Challenges and Ecosystem Fragmentation," *IEEE Industrial Electronics Magazine,* pp. 28-33, March 2017.

X. VITAE

Joseph M. Manahan is the Manager of Advanced Engineering Development for Eaton's Crouse-Hinds Business. He and his team are responsible for the investigation, development, and validation of all new technologies used throughout the product offering. He has been with Eaton's Crouse-Hinds Business for 17 years in a variety of engineering design and engineering management positions. He has been recognized with forty-four U.S. patents. Previously, he worked in the agricultural and fluidics equipment industry as a Design Engineer. Joe received a Bachelor's degree in Mechanical Engineering from Clarkson University in 1998. This is Joe's fourth PCIC paper since 2012.

Rebecca Templet graduated from Mississippi State University in 1999 with a BSEE degree. She has worked as a design engineer in the electric utility industry, consulting, and petrochemical. She has been a senior electrical engineer with Shell Chemical in Geismar, LA since 2013. Becky is an AEE Certifier Power Quality Professional and is a Products and Services subcommittee member for the IEEE Electrical Safety Workshop. Becky is a code panel member for the NEC (National Electrical Code), 2017 cycle and 2020 cycle. At Shell Chemical, Becky's primary responsibilities are maintenance, troubleshooting, electrical design approval, site electrical safety subject matter expert, and site focal point for electrical design standards, protective relaying, and preventative maintenance guidance.

Carlos Estevez graduated from Simon Bolivar University in Venezuela in 1996 with an Electronics Engineering degree. He joined Schlumberger in 1998 as Drilling Services Engineer working in drilling operations in several countries. In 2001 Carlos graduated from the Politecnic University of Barcelona in Spain with a Masters in Telecommunications and Broadcasting Systems. In 2004 he transferred into the Engineering department to design and support While Drilling Surface Acquisition Systems for Schlumberger Drilling and Measurements until 2010 when he became the first Regulatory Compliance Coordinator in the Houston area. In 2012 he joined the Drilling Automation team where he continues to serve as a Validation and Verification engineer.

Dennis Grinberg received a B.S. and an M.S. in Mathematics and Computer Science from Bar-Ilan University in 1986 and 1990 respectively, and received an M.S. in Computer Science from Carnegie Mellon University in 1993. Dennis is the Director for the Center for Connected Intelligent Solutions at Eaton Corporation where he has been working since 1996. In this role, Dennis is responsible for developing reusable platforms and processes in the embedded, IoT and user experience design disciplines which accelerate Eaton's delivery of numerous connected products and services.

Appendix A - Survey Questions & Results

What function are you part of within your organization?
8% – Executive **8%** – Operations management **17%** – Maintenance professional **25%** – IT professional
42% – Engineering professional **0%** – Procurement, Sales/marketing, Finance & Other

What level of influence do you have in your organization/facility?
67% – Influencer **17%** - Final decision maker **8%** - Policy maker **8%** - Order taker

How many years of experience do you have

Industry experience:	**0%** – 0-5 years, 6-10 years		**50%** – 11-20 years	**50%** – 20+ years
Current function:	**33%** – 0-5 years	**25%** – 6-10 years	**33%** – 11-20 years	**8%** - 20+ years
Existing employer:	**17%** – 0-5 years	**0%** – 6-10 years	**58%** – 11-20 years	**25%** - 20+ years

What are the most impactful benefits of IoT to your role/business in the next 5 years?
High impact – Safety, improved operational efficiency
Moderate impact – Reduced downtime
Low impact – Reduced maintenance, cost, remote access/diagnostics, reduced overhead, better decision making, new products/service opportunities, improved customer relationship, improved supplier products/services

Do you perceive your business will leverage third party internet/cloud based services in the next 5 years?
83% – Yes **17%** – No
100% of respondents who answered "No" perceived there was no benefit to leveraging internet/cloud based services

What are the biggest challenges/threats to your business with IoT?
High impact – Security threat *(loss of process control)*
Moderate impact – Perceived loss of intellectual property, legacy infrastructure
Low Impact – Organizational/technical capability (lack of core competency), interoperability, legal compliance, organizational resistance, specification development, return on investment, deviation from current business model

What strategies do you employ to increase the benefits of aggregate data from multiple suppliers *(equipment manufacturers)*?
25% – Common link layer/connection point **8%** – No solution identified, IoT is the solution **67%** – No reply

What is your typical turnaround schedule (major maintenance overhaul)?
33% - 1-3 years **25%** - 4-5 years **8%** - 6-10 years **8%** - 10+ years **25%** - As required / On demand

On average how many hours of non-productive time (scheduled or unscheduled time when product is not being made or extracted) does your facility incur on an individual process (based on 8760 hours/year)?
58% - 0-1000 hours **8%** - 1001-2000 hours **8%** - 2001-3000 hours **0%** - 3001-4000 hours, 4000+ hours **25%** - I don't know / Did not reply

What percentage of your facility's downtime is unscheduled *(estimate)?*
67% – 0 to10% **0%** – 11 to 50% **25%** – I don't know/no reply

What is the total value of downtime per hour incurred *(estimate in USD)?*
Creditable answers varied between **$12K – $63K per hour** depending on the process affected

Do you have any corporate data management policy (or policies)?
83% – YES **0%** – NO **17%** – I don't know