

EXPERIENCES OF A GLOBAL ELECTRICAL MANUFACTURING ENTERPRISE: THE JOURNEY TO BECOME INDUSTRY 4.0 READY

David B. Durocher
Senior Member, IEEE
Eaton Corporation
26850 SW Kinsman Road
Wilsonville, OR 97070
USA
DavidBDurocher@eaton.com

Lyle Sprinkle
Member, IEEE
Eaton Corporation
1000 Cherrington Parkway
Moon Township, PA 15108
USA
LyleESprinkle@eaton.com

Abstract - One challenge for electrical system design engineers in the process industries is assuring real time information is accessible to plant operators who need this to assure mill processes run safely, reliably and efficiently. Network enabled process systems offer an abundance of available data, but most data rarely qualifies as useful information. This paper will present a case study outlining the experience of a global electrical power distribution and control manufacturer that recently made significant investments to upgrade electrical systems at existing circuit breaker manufacturing and assembly factories with a focus on leveraging emerging applications for the Industrial Internet of Things (IIoT). The paper will outline details of the capital investment, decisions on systems and processes selected in the planned facility upgrade, and technologies deployed in the manufacturing environment to assure systems were IIoT ready. Metrics outlining operational improvements following the IIoT upgrade and lessons learned after project completion will be reviewed. Finally, based on practical experience from the case study and understanding of industry processes, a review of ideas on how IIoT can be scaled-up to apply in a process industry environment will be discussed.

Index Terms – Industry 4.0, digital transformation, process control, digital factory, operational efficiency, cybersecurity, predictive maintenance

I. INTRODUCTION

It seems nearly every industry conference and periodical are now actively promoting Digital Transformation and focusing on Industry 4.0. One recent industry conference offered participants technology updates on a broad array of topics including smart sensors, artificial intelligence, robots and drones, augmented and virtual reality, cybersecurity, and additive manufacturing. According to the World Economic Forum, by 2025, digitalization in one industry will reduce emissions of CO₂ by 610 million tons, allow data collection usage increase between 1-5 percent and prevent 44,000 injuries, saving as many as 1,000 lives. It sounds like wonderful things are just around the corner for global industry applications, but what do these changes really mean and how can the industry execute to take advantage of this paradigm shift?

Don't feel badly if you missed the first three revolutions – most of us were not around back when these took place. For the record: The first industrial revolution was in the late 18th century when steam engines and hydraulic power offered

power generation that drove early gains in productivity and industrialization. The second revolution was early in the 20th century when the commercialization of electricity transformed manufacturing – the assembly line came of age and electrical energy drove staggering gains in productivity. The third industrial revolution began in the 1970's and ended around the year 2000 when computers and the internet enabled automation, delivering instant access to information used for enhanced decision-making. Today's fourth industrial revolution is characterized by a transition from the manual, sequential value chain in manufacturing to an information rich digital core enabled by new developments in smart sensors, cloud computing and the Industrial Internet of Things

II. IT'S NOT THAT SIMPLE

Clearly, the world has now entered our fourth industrial revolution, and in fact many businesses are advertising that they have already arrived. Regretfully, it's not that simple. Many users in the industry are working hard to find a way to leverage a wealth of readily accessible digital data to extract the right information that can then be used to improve operations. This is not just about adding technology to the existing model. True digital transformation will involve the much more difficult task of rethinking the current business model and applying this to a new platform supported by 21st century technologies. And what of the issue regarding the upgrade of existing systems that are compatible with the new world of digitalization?

Today's electrical infrastructure across all industries includes machines supported by power distribution and control assemblies that were installed decades ago. These are the backbone of manufacturing systems and they were built to last. There is no easy business case to be made to replace functioning legacy systems simply for the sake of installing new technology. However, as described in this paper, there are case studies where new technology has assisted plant owners in extending the life of older electrical systems through retrofit with new sensors and condition monitoring. Well planned and executed life extension retrofits of electrical systems of existing facilities deliver access to a wealth of data, supported by software and communications that accurately extracts the right information to track the health and performance of assets to allow predictive maintenance schedules to be implemented.

III. CASE STUDY OF ONE MANUFACTURING PLANT

The authors' employer is a power management company with a global manufacturing footprint in the electrical, hydraulic,

digital meter to function as a network enabled data historian by leveraging on-board memory. High-end digital meters installed at the point of service can be combined with lower cost digital submeters to establish “energy owners” in various process areas of the production facility. These together with a user interface can serve as a facility wide energy management system as outlined in [1]. Where possible, existing current and voltage transformers serving legacy analog meters were reused to support network enabled multifunction digital meters.

2) *Variable Frequency AC Motor Drives:* As explained previously, energy efficiency was the primary driver in selecting the subject circuit breaker assembly plant as one of the first across the company enterprise for Industry 4.0 implementation. Several of the larger electrical loads in the plant were low-voltage AC motors with centrifugal fans and pumps as the driven load. The project team identified several applications where flow modulation was accomplished using dampers and valves. These mechanical devices could easily be replaced by variable frequency AC motor drives (VFDs). For the identified centrifugal loads, the energy in consumed horsepower (HP) using VFDs would be reduced by the speed cubed as defined by well-known and understood Affinity Laws [2]. Several articles have documented application of VFDs in controlling the speed of centrifugal fans and pumps as a method to save energy. Legacy systems including mechanical flow control devices were replaced with variable speed control, allowing for more accurate flow management at a greatly reduced energy footprint. The site electrical upgrade included the addition of over 30 variable frequency drives. In most cases, a wall-mounted drive was installed near the driven motor load and upstream circuit protection was from a circuit breaker in an existing motor control center making this a low installed cost retrofit. EtherNet/IP™ network communication cards were included in all drives added to the system. Even for smaller horsepower ratings, the latest designs of this product include a host of functionality such as monitoring (voltage, current, power), protection (overcurrent, under load, under voltage) and health (run time, trip logs) that were not available in legacy systems installed when the plant was first commissioned. An opportunity for plant operators to gather more data as a part of the Industry 4.0 initiative.

3) *Motor Management Relays:* For induction motors requiring fixed speed control, legacy across the line motor starters consisting of an electro-mechanical contactor and thermal sensing relay for motor overload protection were upgraded by replacing the thermal sensing relay. Legacy motor protection at the plant included relays that detected a higher temperature of a resistive element in the motor current circuit to detect a possible motor overload condition. Historically, thermal sensing motor overload relays have included a melting eutectic alloy or bi-metal device for motor protection. These were replaced in 54 locations with a current design motor management relay, coupled with the existing electro-mechanical contactor which was reused. As shown in Fig. 2, this consisted of a measurement module that includes on-board functionality to collect real-time phase current and voltage measurements. Integral current transformers allow for three-phase power conductors to simply connect between the switching contactor and three-phase motor terminals. Voltage terminations are also made at the measurement module. A base control module monitors system voltage and current parameters at the measurement module using an on-board

microprocessor responsible for multifunction motor monitoring plus control/protection and network enabled connectivity. An optional user interface module can also be applied if local control and monitoring is desired. Like the variable frequency drive, retrofit installation of the motor management relay into existing control panels at the plant was a straightforward system upgrade. Modification of existing motor control centers required additional consideration due to applicable industry standards including UL 845 [3]. A detailed review of considerations regarding low-voltage motor control center replacement versus upgrade decisions can be found at [4]. The newly installed motor management relays added the capability to monitor a host of electrical system values, along with protective operational data and equipment health functionality in a small, network communication ready package. Available real time data beyond legacy motor protective relays including under-voltage, under-load and pump cavitation with metering of phase voltages, amperes and power in Watts and Vars is considered a positive. Multiple communication network options were available. The site selected EtherNet/IP™ so easy connections could be made to Ethernet switches and newly installed network gateways.

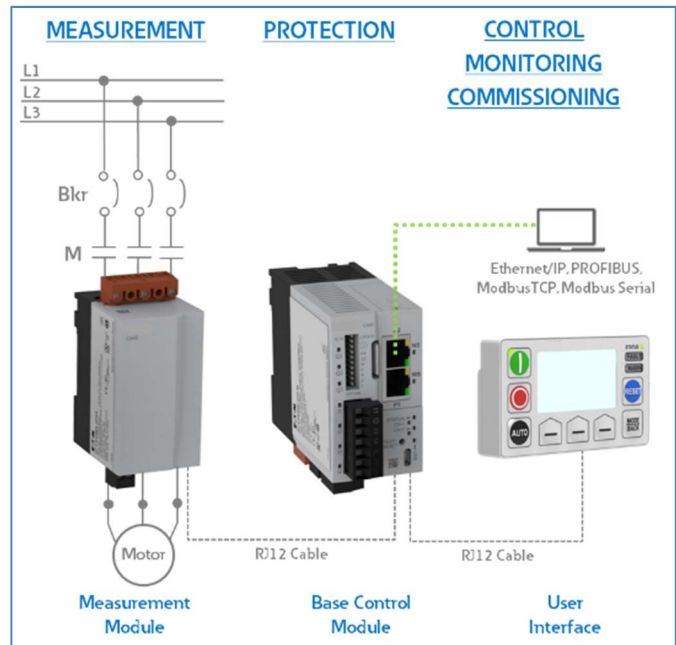


Fig. 2: Block diagram of a new motor management relay

4) *Integral Circuit Breaker Racking:* In some cases, decisions to install site electrical upgrades are inspired by factors other than improved energy or operational efficiency. Recent changes in electrical workplace safety standards including the NFPA70E-2018 [5] outline new requirements regarding the need to perform an onsite risk assessment prior to performing energized electrical work. Because the risk assessment includes a review of both the likelihood and severity of injury from an arc flash event, manual racking of medium voltage circuit breakers is quickly becoming an unaccepted practice, now being replaced by stand-alone universal racking devices or integral motorized remote racking. Today, some commercially available offerings are designed as

a retrofit able to replace manual racking circuit breaker cell parts with an updated integral motor operator. This allows operators to work from outside the calculated flash protection boundary as defined in NFPA70E-2018 during breaker racking, connecting or disconnecting the breaker from the energized bus. Racking is accomplished from a pendant station or remotely via a network connection. Newer remote isolation systems applied for overland conveyors tested to Functional Safety Standard IEC-61506 based on Safety Integrity Level 2 (SIL 2) can now be installed using legacy medium voltage switchgear and a motorized racking retrofit [6]

B. Case Study Results & Lessons Learned

New equipment including multi-function point of service meters and submeters, variable frequency drives, soft-start motor controllers, motor management relays and Ethernet gateways collecting real time data from 73 areas on the factory floor were installed. The factory wide area network (WAN) was also upgraded to support the additional data. Results from this effort were promising with over US \$815,000 in first year savings obtained – less than a 2-year payback on the original investment which was in line with the business return on investment targets. Most savings were attributed to energy reduction on the order of 12% in the plant molding production line, 15% in the punch press and plating line and nearly 30% in the building HVAC systems. Perhaps more important than the energy savings was a positive step change in process operational efficiency. Business metrics that were previously hand recorded were replaced by flat screen monitors that displayed machine availability, manufacturing performance and component quality. These three metrics multiplied together deliver an Overall Equipment Effectiveness performance measure as shown in Fig. 3. The facility, which was once presumed to be operating at efficiencies well above 70 percent

was at times operating well below these efficiency levels. The root cause of most efficiency loss was attributed to machine availability. Several months after Industry 4.0 implementation, a purchase requisition to add an additional punch press at the facility was put on hold. Collected operational data showed availability of existing plant machines was the issue, so purchasing a new machine was not necessary.

Lessons learned by the company in completing pilot site implementation of Industry 4.0 were many. First, up-front preparation time prior to implementation was a critical element in success of the project. Also, planned production scheduling conflicts were anticipated, but the scope of work and time for commissioning was extensive due to the 24/7 operation of the plant which impacted the project schedule. Deployment of a multi-disciplined team from the business assured there was little ramp-up time that would have otherwise been necessary by an outside contractor not familiar with the business manufacturing disciplines, people and processes. It was also advantageous to deploy talent from outside the plant operations organization as a large mix of skills were required for effective implementation, and necessarily these resources needed to be de-coupled from plant daily operations. Because virtually all system upgrades involved network connected products, a robust plan to upgrade firewalls and network security with installed systems that were tested to UL Standard 2900-2-2 [7] was a necessary component of success. The issue of cybersecurity is discussed in a following section of this paper.

For the initial project, all operational data was uploaded to a secure cloud computing service provider providing fault protection, unlimited storage for analytical study, and disaster recovery. After a year of operation, most members from both the project team and operations leadership agreed that future

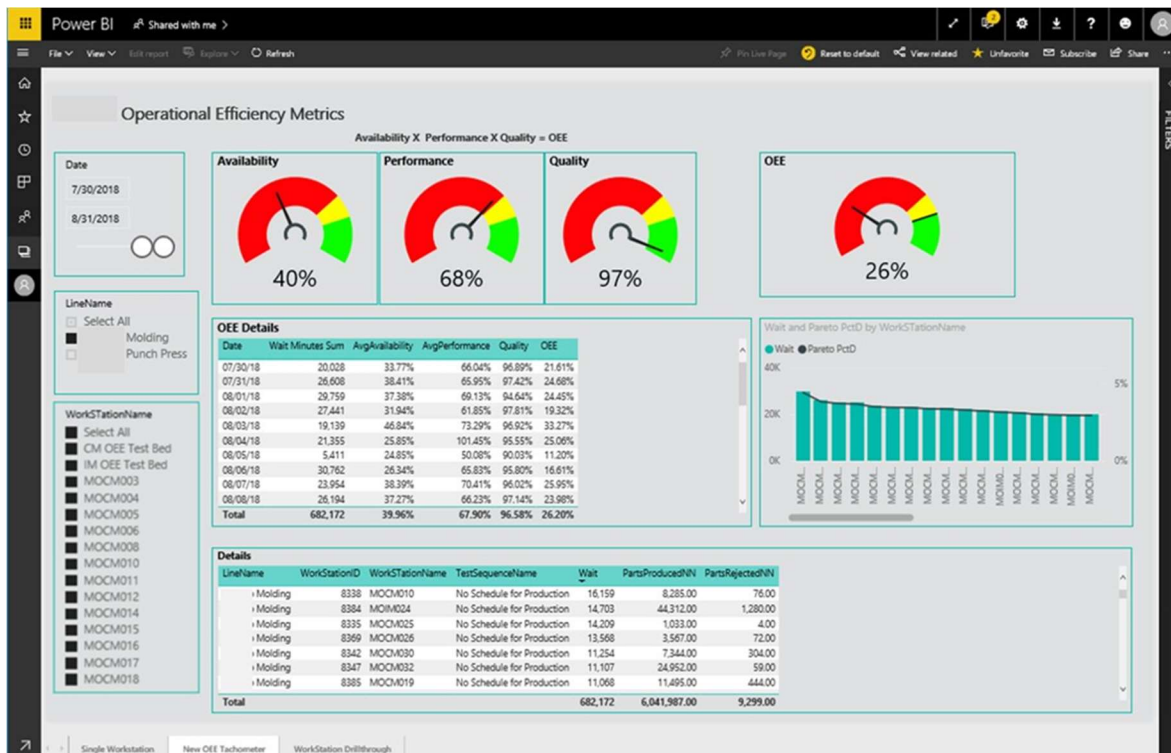


Fig. 3: Factory floor display showing real time Operational Efficiency metrics

roll-outs could be just as successful through edge-processing to provide real-time analytics and real-time action/response information to operators and plant management while still allowing long-term data analytics, enterprise integration and storage to be completed in the cloud [8].

IV. A NOTE CONCERNING CYBERSECURITY

In the authors' opinion, an important issue related to the successful implementation of Industry 4.0 in a new or existing industrial facility is cybersecurity. Perhaps one of the most famous security breaches in recorded history took place on December 23, 2015 when three independent electrical distribution companies in the country of Ukraine were subjected to cyber-attacks. Over the course of just a few hours, over 225,000 Ukrainian residents lost power. The attackers demonstrated a variety of capabilities beginning first with phishing emails, ultimately manipulating Microsoft Office documents that contained necessary malware to gain a foothold into the Information Technology (IT) business networks of the target utility companies. From there, user credentials were harvested to hack into system, ultimately using virtual private networks (VPNs) to gain access to the industrial control system (ICS) network. The VPNs into the ICS from the business network lacked two-factor authentication, allowing the adversary to use remote access capability of the native systems to gain administrative privileges to the ICS environment. The attackers also used telephone systems to generate thousands of calls to the utility call centers, denying access to customer incoming calls to report outages. Details of the cyber-attack in Ukraine are included in a March 2016 report issued by the Electricity Information Sharing and Analysis Center (E-ISAC) in Washington D.C. [9].

Perhaps the most significant learning from this well-orchestrated large scale cyber-attack in the Ukraine was the relative ease in which the attackers gained access to the ICS network. Where IT business networks have historically relied on robust encryption and data security to protect systems from attack, ICS networks have traditionally been configured with a focus on operational efficiency including availability, reliability and safety. Neither the system components nor the ICS networks were designed with robust firewalls that prevent unauthorized access to the system.

Although the proliferation of networks exponentially elevates the risk of cyber-attack, any product with embedded logic is vulnerable. The product may not be connected to a network, but it could be protecting an asset. A stand-alone laptop computer with a USB connected device is one example. Recognizing this risk is a first step toward users understanding that before buying any product, one aspect in considering product quality is cybersecurity.

Cybersecurity incidents present increased business risk. As a result, process industry users are now requiring that suppliers provide evidence that the products sold comply with industry cybersecurity standards. Today, most major suppliers including the authors' company recognize that one aspect of product quality is cybersecurity. To greatly reduce the risk that the integrity is compromised, strict procedures are maintained as a part of the product development process, assuring cybersecurity features are embedded as a part of the design. Although cybersecurity industry standards are still somewhat new, in mid-2017 one globally recognized testing organization,

Underwriter's Laboratories (UL), first published standard 2900 focused on *General Requirements for Software Cybersecurity for Network-Connectable Products*. Guidelines outlined in the Standard include processes to test and certify network-connected products meet the Standard's cybersecurity criteria. This Standard includes UL 2900-1 Software Cybersecurity for Network Connectable Products, UL 2900-2-1 Cybersecurity for Healthcare Products and UL 2900-2-2 Cybersecurity for Industrial Control Systems. The authors' company first collaborated with UL in 2018 and during that year, an in-house lab was constructed and approved as a part of a UL Client Lab Validation Program. Conformance to the program requires demonstration via lab tests to assess products for security software weaknesses, vulnerabilities and malware prevention before achieving listing by the UL Cybersecurity Data Acceptance Program. The lab includes the capability to test products with intelligence or embedded logic to key aspects of the UL 2900-1 and UL 2900-2-2 Standards, assuring that all tested components are compliant with industry cybersecurity requirements before being installed in critical field systems.

Electrical products installed at datacenters, utilities and process industrials need to be hardened. The expectation of any buyer purchasing a product should be that one of the most relevant aspects of quality should be cybersecurity. Product manufacturers must embed cybersecurity by design and include this in any new product development. It is important to realize that not just network connected products are at risk, but any product with embedded logic is vulnerable. The product may not be connected to a network, but it could be protecting an asset. UL cybersecurity standards and manufacturer collaboration to establish UL approved vendor in-house testing labs are new to the industry. One additional cybersecurity standard of note is IEC 62443 [10] which was originally introduced by the International Society of Automation (ISA). As of this writing, the IEC62443 has only has 3 standards with schemes for independent assessment including:

- IEC 62443-2-4 (requirements for Service Providers)
- IEC 62443-3-3 (requirements for Systems)
- IEC 62443-4-1 (requirements for Product Development)

Unlike the UL Standard, vendors can claim conformance via self-certification or as an option, with third-party testing. Cybersecurity System conformance based on IEC 62443-3-3 does not require that all components of the system be tested for compliance if an element of the system, such as a firewall, demonstrates total system compliance. No doubt that cybersecurity standards from both UL and IEC will one day be harmonized to support what appears to be continuous and exponential growth of network connected products across the global industries.

V. FUTURE TRENDS FOR THE INDUSTRY

The case study plant was able to successfully plan and execute Industry 4.0. One key element of the success was deployment of a multi-disciplined project team that carefully considered the many limitations associated with installing network enabled upgrades in an existing manufacturing facility. In an active production environment, it is often not practical to install technology via a wholesale changeout of the electrical systems. In the case study, a primary business driver to reduce

operating costs based on improving energy efficiency pushed the project implementation plan toward installation of variable frequency drives: a proven and well understood energy solution. Most process industries have already “done their homework” around energy efficiency. The next frontier in driving improvements in operational productivity based on reduced maintenance costs.

The current maintenance model deployed across many process industry users would best be described as preventive maintenance. This involves a routinely scheduled rotational outage when existing electrical assets are de-energized, cleaned, tested and repaired. Fig. 4 shows a diagram of the hierarchy of maintenance strategies regarding both efficiency and effectiveness. This begins with Reactive or run to failure. There are some applications where this approach is acceptable, but typically this does not apply in an operating process environment. Preventive maintenance is shown as a more efficient and effective approach, but there are significant limitations. Recent studies including [11, 12] have demonstrated that 82% of assets that fail during operation, fail randomly. This suggests that maintaining every electrical asset in a manufacturing facility would be an effective strategy only 18% of the time. Condition Based maintenance can be implemented manually based on equipment operators making the rounds to check on-line sensors on given machinery, but the approach is both cost prohibitive and ultimately not effective because the collected data will not be real time. The confluence of advancements in big data, low-cost cloud computing, and advanced analytics has enabled a new era where analytics can first be used to effectively implement condition based maintenance whereby assets are serviced only when they need to be. From there, advanced analytics allow for systems to “learn” a known good state and this will drive operations toward a Predictive maintenance model where impending failure can be predicted in advance. Finally, Prescriptive maintenance strategies are in place when operators focus maintenance activities on the asset projected to soon fail, performing this maintenance at a prescribed schedule that does not disrupt production.

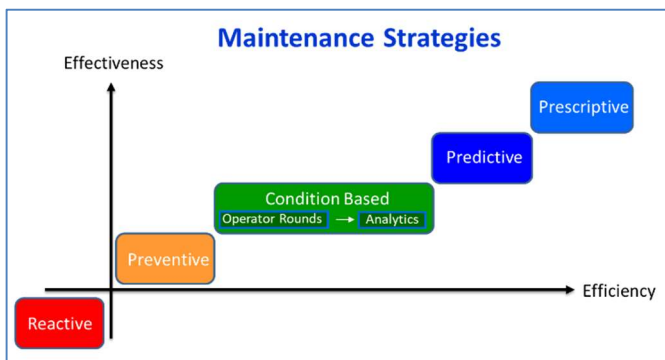


Fig. 4: Hierarchy of Maintenance Strategies

Of course, the use of analytics to predict machine failure is nothing new to most process industries. Today’s paper machine drives system or steel rolling mill includes hundreds of on machine sensors supported by a distributed control system, making decisions in real time to assure operational efficiency, reliability and safety. The use of analytics to support the

electrical infrastructure of power distribution and control systems that support these processes is something new.

One example of best practices in deploying available technologies in this area is described in [13]. This outlines a case study involving on-line partial discharge (PD) monitors installed on two 49 megawatt (MW), 13.8 kilovolt turbine generators at a paper mill in Alberta, Canada. The on-line monitor measured low level discharges in millivolts and picocoulombs, effectively used as a measure of the machine’s winding insulation. High levels of phase resolved partial discharges in phase C of one generator stator winding caused site maintenance to pull the rotor of the suspect machine during a scheduled outage. A manufacturing defect of the stator where the phase A and C conductors were routed with insufficient clearance was causing corona build-up and insulation breakdown. The area was cleaned and repaired, and the machine was then returned to service following the scheduled outage. Partial discharge levels returned to normal as shown in Fig. 5. Though this case study is an example of a well-executed prescriptive maintenance practice that was implemented well in advance of the Industry 4.0 era, this serves as one of many

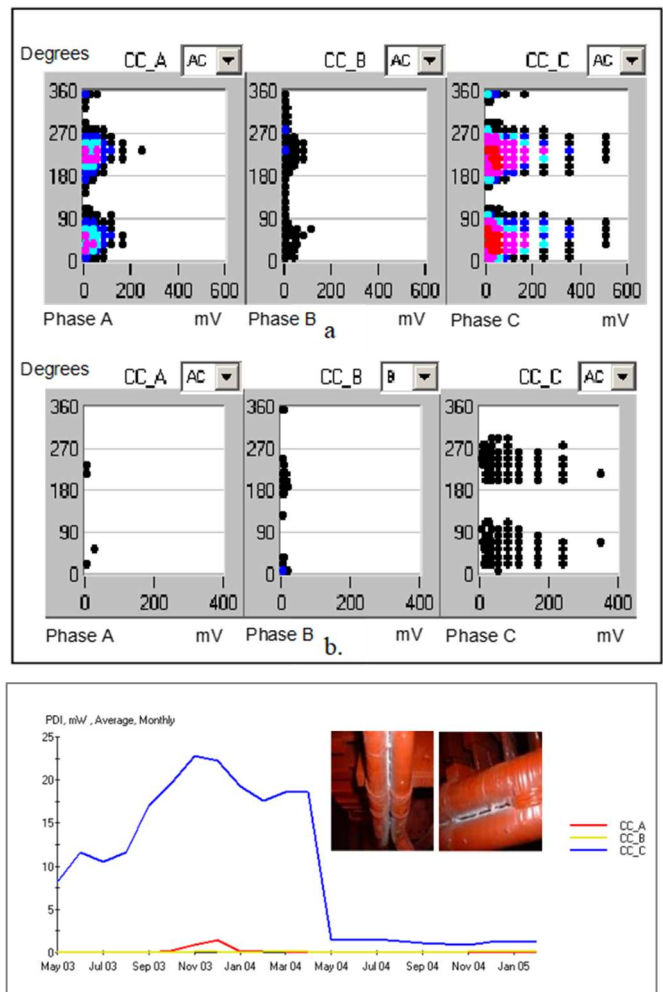


Fig 5: Above; before and after PD pulse count. Below; stator winding corona and PD activity return to normal after repair

excellent examples. The installed technology collected PD data via an on-board memory card. This device includes network connectivity, so PD data could have been aggregated to a mill server or to the cloud, but this was not a necessity. One business driver for the installation was the very high value of the asset. If the 49 MW stator winding had failed, a stator rewind would have taken 3 months for completion. The cost of the repair plus the lost opportunity in generating electrical energy to support the mill was estimated at over U.S. \$4 million.

One additional example where technology has shifted significantly, opening the door for application of Industry 4.0 in plant electrical systems is around circuit protection. As discussed in previous sections of this paper, motor overload protection for legacy systems generally included a mechanical sensor that used the heat produced by the resistance of a conductive element in the current path as a measure of a possible motor overload. Legacy circuit breakers that also used similar methods have been replaced with microprocessor-based protection offering a host of data points that can be used for health monitoring and predictive diagnostics. Electronic trip units applied in both molded-case and low-voltage power circuit breakers have seen significant advancements [14] in the past few years. Fig. 6 shows a recently introduced molded case circuit breaker, tested to global standards with a host of data recorded in real time while the breaker is in operation. This circuit breaker could be applied in a typical distribution switchboard manufactured and tested to UL891, or its low-voltage power circuit breaker counterpart that would be applied in a low-voltage switchgear assembly manufactured and tested to UL1558. The common component for all ratings is the electronic trip unit (ETU). This offers new protective features such as multiple load alarms and ground fault alarms with IloT-ready embedded communications and onboard metering. A breaker health algorithm is included as part of the standard offering. This algorithm tracks and records the number and

magnitude of circuit interruptions, operating temperature, run time and other parameters to determine the estimated remaining life of the circuit breaker before it is recommended to be replaced. The manufacturer's instructions suggest a threshold level of remaining life before replacement. Perhaps more important than the breaker health algorithm is the wealth of real-time electrical information available from a protective device serving a single load. In a typical industrial plant, literally thousands of these devices are applied as in the power distribution system. It would be cost prohibitive for any business to replace legacy systems across an existing facility with these new devices, but as legacy systems approach their end of life and are replaced, newer devices offer great promise for any business beginning a journey to an Industry 4.0 future. VI.

VI. CONCLUSIONS

Demographic studies suggest that the world is becoming more urban, more connected and more electrified. Today, many traditional manufacturing industries are working hard to find a way to leverage a wealth of now readily accessible digital data to extract and use the right information to improve operations. This is not just about adding technology to the existing model. True digital transformation will involve the much more difficult task of rethinking the current business model and applying this to a new platform supported by 21st century technologies. This transformation offers great opportunity. It is an exciting time for us all.

The path forward in many cases will not require a wholesale replacement of existing systems which is both cost prohibitive and simply impractical. Instead, a carefully planned program to upgrade existing systems is a good beginning course providing new insights on how to more intelligently manage power. Investment in a facility with a well-defined business case and a high probability of success led to a successful financial payback. The case study site of the global electrical manufacturer described in this paper was a good Industry 4.0 implementation site for these reasons. Users should also look to high value assets where making a transition toward predictive or prescriptive maintenance strategies will generate the highest business value. Selecting a site with solid and well understood business systems is a prerequisite before beginning any project. Finally, choosing suppliers and partners with extensive technology-based product portfolios and experience of Industry 4.0 execution in their own manufacturing facilities is a must, assuring they are both qualified and capable to assist any user toward their digitalization transformation future. Those who do not start, will not have a chance to learn.

VII. REFERENCES

- [1] Young, H.R, Newell, B., Durocher, D.B., "Energy Management at a Mineral-Processing Plant", IEEE Industry Applications Magazine, Sept/Oct 2014, pgs. 14-23.
- [2] Karassik, I.J, Messina, J.P., Cooper, P., Heald, C.C., "Pump Handbook", McGraw-Hill Professional; 3rd Edition
- [3] Underwriter's Laboratories UL 845; "Motor Control Centers", Northbrook, IL U.S.A., 2005
- [4] Durocher, D.B., Hussey, M.R., "Vintage Low-Voltage Motor Control Centers – Replace or Upgrade", IEEE IAS/PCA Cement Industry Conference, 2019.
- [5] National Fire Protection Agency NFPA70E; "Standard for Electrical Safety in the Workplace", 2018

BREAKER HEALTH	CURRENT and STATUS
Health % left	IA Real / Min / Max
INST/SDT count	IB Real / Min / Max
LDT/GFT count	IC Real / Min / Max
Operations count	IG Real / Min / Max
Short Delay Trip count	IN Real / Min / Max
Inst Delay Trip count	Breaker Position status
Long Delay Trip count	Trip condition status
Ground Fault Trip count	Alarm status
Total Trip count	Maintenance Mode status
Test Trip count	Long delay pickup status
Open by Comm count	Manual status
Manual Open count	Zone Interlock status
Time of Last Operation	Ground status
Temperature Real / Min / Max	Diagnostic status
Time of Max Device Temp	Cause of status
Run Time: Min / Hour / Day	VOLTAGE and POWER
OPTIONS	VAB Real / Min / Max
Ground Slope/Pickup/Time	VBC Real / Min / Max
Ground Fault Type	VCA Real / Min / Max
Ground Fault Pre Alarm	VAN Real / Min / Max
Neutral Protection Ratio	VBN Real / Min / Max
Maint Mode: Remote Control	VCN Real / Min / Max
ARMS Level	Power Factor
BREAKER CONTROL	Real / Apparent / Reactive Energy
Enable maintenance mode	Real / Apparent / Reactive Power Demand
Disable maintenance mode	Real / Apparent / Reactive Power Peak
Open Breaker	Demand
Activate relay output 1/2/3	FWD / REV / Total Energy
De-activate relay output 1/2/3	




Fig 6: New design molded case circuit breaker with electronic trip unit.

- [6] Durocher, D.B., Koepke, M., Fisher, D., "Advancing Workplace Safety Through Vintage Equipment Upgrades", IEEE IAS Electrical Safety Workshop, 2019
- [7] Underwriter's Laboratories UL 2900; "Standard for Software Cybersecurity for Network-Connectable Products", 2017
- [8] Yu, W., Liang, F., He, X., Hatcher, W.G., Lu, C., Lin, J., Yang, X. "A Survey on the Edge Computing for the Internet of Things", IEEE Access, Nov 2017, pgs. 6900-6919
- [9] Electricity Information Sharing and Analysis Center E-ISAC; "Analysis of the Cyber Attack on the Ukrainian Power Grid", March 2016.
- [10] International Electrotechnical Commission IEC 62443 "International Industrial Security Standard, 2018
- [11] Price Waterhouse Cooper; "Predictive Maintenance 4.0 - Predict the Unpredictable", 2017
- [11] Rio, R. "Improve Asset Uptime with Industrial IoT and Analytics", Arc Advisory Group, <https://www.arcweb.com/blog/improve-asset-uptime-industrial-iot-analytics>, Aug 7, 2015
- [12] Astasiewicz, R. Kane, C., Patterson, C., "Experiences of Monitoring Partial Discharges in a Pulp and Paper Mill" IEEE IAS Pulp & Paper Industry Conference, 2005.
- [13] Lagree, J., Griffin, R. "Molded Case and Low-Voltage Power Circuit Breaker Health" WP012010EN at www.eaton.com
- [14] Walther, T. "Digital Transformation of the Global Cement Industry", IEEE IAS/PCA Cement Industry Technical Conference, 2018, pgs. 1-8
- [15] Mielli, F., Bulanda, N. "Digital Transformation: Why Projects Fail, Potential Best Practices, and Successful Initiatives", IEEE IAS Cement Industry Technical Conference, 2019

I. AUTHORS' INFORMATION

David B. Durocher (SBM '77 M '97-SM '99) received BSEE at Oregon State University, serves as a Global Mining, Metals, and Minerals Industry Manager with Eaton. He has authored numerous technical papers presented and published in the IEEE Transactions on Industry Applications, Plant Engineering, and EC&M Magazine. He serves on IEEE Standards Working Groups IEEE1584 and IEEE1458 and is an active member of the IEEE IAS Mining Industry Committee, Cement Industry Committee, Pulp & Paper Industry Committee and Association of Iron & Steel Technology. He served as President of IEEE IAS 2015-2016 and as Division II Director - IEEE Board of Directors 2019-2020.

Lyle Sprinkle received his Electrical Engineering degree from the Georgia Institute of Technology and an MBA with an International Marketing focus from the University of Texas at Dallas. He is Director of Meters, Relays and IoT Solutions in the Power Components Division at Eaton, leading plans for the advancement of new IoT solutions to dramatically improve power system monitoring and reporting for industrial manufacturing and commercial businesses. Previously, he has authored content within the "Classic Guide to Mobile Commerce", spoken at the CCBN China Digital Summit, and held product management, marketing and engineering roles at Honeywell, Vocollect - an industrial speech-recognition start-up, Harris Corporation and Alcatel.