Strathprints Institutional Repository

Baker, PC and Catterson, VM and Judd, MD (2015) Standards-based wireless sensor networks for power system condition monitoring. HubNet Position Papers. ,

This version is available at http://strathprints.strath.ac.uk/54479/

HubNet Position Paper Series

Standards-Based Wireless Sensor Networks for Power System Condition Monitoring

Title	Standards-Based Wireless Sensor Networks for Power System Condition Monitoring		
Authors	PC Baker, VM Catterson and MD Judd		
Author Contact			
Version Control	Version	Date	Comments
	1.0 1.1 2.0	05/12/2014 17/08/2015 11/09/2015	Version for peer review Edited in response to peer review comments Final version for publication
Status	Final		
Date Issued	11/09/2015		
Available from	www.hubnet.org.uk		

About HubNet

HubNet is a consortium of researchers from eight universities (Imperial College and the universities of Bristol, Cardiff, Manchester, Nottingham, Southampton, Strathclyde and Warwick) tasked with coordinating research in energy networks in the UK. HubNet is funded by the Energy Programme of Research Councils UK under grant number EP/I013636/1.

This hub will provide research leadership in the field through the publication of in-depth position papers written by leaders in the field and the organisation of workshops and other mechanisms for the exchange of ideas between researchers, industry and the public sector.

HubNet also aims to spur the development of innovative solutions by sponsoring speculative research. The activities of the members of the hub will focus on seven areas that have been identified as key to the development of future energy networks:

- Design of smart grids, in particular the application of communication technologies to the operation of electricity networks and the harnessing of the demand-side for the control and optimisation of the power system.
- Development of a mega-grid that would link the UK's energy network to renewable energy sources off shore, across Europe and beyond.
- Research on how new materials (such as nano-composites, ceramic composites and graphene-based materials) can be used to design power equipment that is more efficient and more compact.
- Progress the use of power electronics in electricity systems through fundamental work on semiconductor materials and power converter design.
- Development of new techniques to study the interaction between multiple energy vectors and optimally coordinate the planning and operation of energy networks under uncertainty.
- Management of transition assets: while a significant amount of new network equipment will need to be installed in the coming decades, this new construction is dwarfed by the existing asset base.
- Energy storage: determining how and where storage brings value to operation of an electricity grid and determining technology-neutral specification targets for the development of grid scale energy storage.

The HubNet Association is a free-to-join grouping of researchers and research users. Join via the “HubNet Registration” tab at www.hubnet.org.uk to get access to working document versions of positions papers, an archive of workshop and symposium presentations and to receive notification of future events.

Standards-Based Wireless Sensor Networks for Power System Condition Monitoring

1 Introduction

Central to the smart grid vision is the need for increased observability of the electrical network through the addition of sensing and metering technology. In substations, one key area of development is online condition monitoring (CM) which, replacing physical inspections, aims to provide engineers with timely information on electrical plant health that can be used to inform maintenance decisions and avoid unplanned outages. Through the application of online monitoring and diagnostics, system reliability can be maintained and the operational lifetime of plant can even be extended beyond the original design lifetime, leading to an overall reduction in ongoing operational costs and deferred capital expenditure on replacement assets.

To implement an online condition monitoring system, a robust communication platform is required to convey data from monitoring sensors in the field back to engineers in the control room. In a high-voltage environment such as a substation this can become a barrier to deployment due to both operational issues and the cost of running multiple cables to a central location. For this reason, wireless sensor networks (WSNs) have become an attractive option for substation condition monitoring architectures, offering a low-cost approach that circumvents the typical constraints associated with the installation of wired monitoring systems. Also, as the price of implementation decreases it becomes increasingly cost-effective to deploy condition monitoring sensors onto a wider range of assets.

There have been several studies in the literature detailing research into WSNs for industrial applications, including the fundamental performance of WSNs in industrial environments [1, 2], theoretical schemes for wireless sensing applications [3, 4], and reports on the performance of field deployments of WSNs in both the power [5] and oil and gas domains [6]. Industrial support of WSN technologies has led to two industrial wireless sensor network (IWSN) standards emerging in recent years, which are designed to support monitoring and control applications in harsh industrial environments.

This paper assesses the industrial needs motivating interest in wireless monitoring within the power industry, and reviews applications of WSN technology for substation condition monitoring (Section 2). A key contribution is the identification of a set of technical requirements for substation-based WSNs, focused around security requirements, robustness to RF noise, and other utility-specific concerns (Section 3). Section 4 comprehensively assesses the suitability of various IWSN protocols for substation environments, using these requirements. A case study implementation of one standard, ISA100.11a, is reported in Section 5, along with deployment experience. The paper concludes by describing future research challenges for WSN protocols which are specific to this domain.

2 Background

2.1 Substation Condition Monitoring

Condition monitoring enables utilities to progress from periodic maintenance, where plant is taken out of service for maintenance on a periodic basis or based upon its operational lifetime, towards predictive- or condition-based maintenance (CBM), where plant maintenance is scheduled based upon the ongoing health of the asset.

CBM aims to reduce costs for maintenance through removing unnecessary outages and discovering and managing incipient defects. Through these measures, reliability can also be increased enabling the operational lifetime of plant to be extended past factory specifications.

Han and Song [7] define a condition monitoring system as having four components:

1. **Sensors**: converting physical parameters to a form that can be measured electronically. For substation condition monitoring, useful sensing applications could include: transformer oil and winding temperature, online dissolved gas sensing, partial discharge monitoring and SF_6 gas density sensing.

2. **Data Capture**: incorporating analogue-to-digital conversion and, optionally, digital signal processing and/or data preprocessing.
3. **Defect Identification**: using techniques such as anomaly detection, pattern recognition or AI methods (including data-driven, model-based or knowledge-based classifiers).
4. **Diagnostics**: determining the specific problem and appropriate course of maintenance action to take.

Within this model, research tends to focus on new types of sensor and defect identification. However, a key challenge is to integrate all four aspects into a system which helps engineers to manage their assets, by offering enhanced diagnosis based on multiple sensors and defect identification techniques. Whatever technology is chosen to integrate the four components of a monitoring system, it must also have a communications network through which monitoring data is transmitted. Since installing new cabling in substations is a significant undertaking, there are practical and financial motivations for using wireless technology to circumvent associated costs.

2.2 Wireless sensor networks

Wireless sensor networks are comprised of discrete, spatially distributed and (ideally) self-organising nodes which form an ad-hoc communications network with redundant links. They are a key enabling technology for ‘smart environments’, providing the sensing, communication and first-stage processing platform for a range of applications. They have already seen deployments in a wide range of application domains including environmental monitoring, home automation, industrial process control, transport and military applications. Wireless sensor nodes usually have five principal components [8]:

1. **Microprocessor**: to host sensing and diagnostic applications, and provide control functions to other device components.
2. **Data storage**: in the order of megabytes of RAM and megabytes of flash for program and data storage. This can be extended through the addition of on-board flash memory if required for a particular application.
3. **Sensing**: either on-board or externally connected sensors, connected to the processor via an input/output (I/O) interface through digital or analogue-to-digital converters.
4. **Wireless radio**: providing data communication between nodes, encapsulating all network functions and inevitably connecting the remote node to a base station for data archival and dissemination.
5. **Power**: either from a fixed-capacity primary battery or from an energy harvesting device (with or without a secondary battery or alternative energy storage such as a supercapacitor).

2.3 WSN Deployments in the power domain

To date, there are a limited number of power system WSN deployments reported in the literature, with most publications describing modelling and simulation results.

Applications in this area include that of Leon *et al.* [3], where a wireless sensor network was proposed for mechanical health monitoring of transmission lines to allow operators to schedule preventative maintenance and aid in the analysis of post-fault conditions. A diagnostic model was built using strain, vibration, tilt and temperature measurements to determine the mechanical health of transmission towers, which was tested successfully under simulation.

At the distribution level, WSN models have been applied to both operational monitoring, and plant condition monitoring. In [4], results of modelling a wireless sensor system for electrical distribution networks is presented, which uses phase current characteristics to estimate fault locations. In [9], a fully-customised wireless sensor network was designed for busbar joint temperature monitoring. Both of these installations were proof-of-concept systems rather than generic approaches to wireless substation condition monitoring.

In terms of industrial deployments, the most substantial to-date has been part of an EPRI-funded project of a wireless temperature sensor network for substation monitoring [10]. This installation measured transformer tank surface and circuit breaker temperature, utilizing photovoltaic energy harvesting to extend the operational length of the battery-powered sensor network system. In [11], the study was expanded to consider the design of large-scale wireless condition monitoring networks. A 122-node WSN monitoring transformers was deployed to evaluate energy performance and battery lifetime using the following monitoring applications:

1. Temperature monitoring of oil-filled circuit breakers and oil-filled transformers.
2. Vibration monitoring of oil-filled transformers to monitor transformer activity and fan and pump health [11].
3. Ambient temperature.
4. SF_6 circuit breaker gas density monitoring (using a Trafag 8774 gas density sensor).

A recent US Department of Energy study investigated a suite of wireless technologies for the electric power system [12], including WSN protocols. The study found that, as may be expected, out of all of the wireless technologies surveyed, industrial wireless sensor network protocols were the best suited for power system monitoring applications based on security and latency features.

3 Requirements for a wireless substation condition monitoring network

Gungor *et al.* [2] highlight the major challenges to smart grid wireless sensor networks' operation as including harsh environmental conditions (such as RF noise from switching and transients), reliability and latency requirements, variable link capacity, and resource constraints (e.g. sensor node measurement acquisition speed, processing and memory capabilities and energy usage). These challenges have, in part, been met by investigations into the performance of WSN technology in industrial environments and advances in wireless sensor network standards. Key challenges relating to wireless substation CM systems are considered below.

3.1 Security

Security is paramount in any industrial system to mitigate against intrusions and to maintain data confidentiality and integrity. Security presents an additional challenge in WSNs as the network uses a wireless broadcast medium. While monitoring data may not immediately present itself as being confidential in nature, the communications channel between the sensor and the control room must still be secure; for instance, to stop injection of spurious measurements which would misrepresent the condition of a unit, which in turn could potentially require a site visit to investigate. Akyol *et al.* [12] have specified that, for this reason, industrial wireless sensor networks must use data encryption in multiple network layers to validate data and mitigate against eavesdropping, and 2-way, mutual authentication of nodes to mitigate against malicious nodes joining and participating in the network. In addition, application-level security and validation in addition to network and data-level encryption schemes is recommended.

3.2 Performance in the presence of RF noise

Industrial wireless sensor networks can be subject to a number of environmental factors which can degrade the quality of wireless links. The primary factor, RF interference, can be caused by electrical plant switching, partial discharge (PD), and other sources of wireless communication. A study into RF noise pollution from energized electrical plant found that noise from switching and PD is predominantly confined to the sub-1 GHz range [13] so, in practice, wireless communications operating above this range (i.e., in the 2.4 GHz range) are not generally affected by impulsive noise. This has been demonstrated under laboratory conditions for a number of wireless protocols operating in the 2.4 GHz ISM band [1] [14], and suggests that protocols operating below 1 GHz, such as the 868 MHz and 915 MHz ISM bands, could be more susceptible to impulsive noise, depending on local conditions of the deployment environment.

In the 2.4 GHz range, there are other potential narrowband sources of RF which may interfere with WSN operation, including other WSNs, WiFi, and 'walkie-talkies'. The optimal method of addressing narrowband noise in this range is by employing *frequency diversity*, where the transmission channel frequency changes in a pseudorandom sequence. In addition to this technique, a multichannel wireless protocol with suitable support can employ either manual or automatic channel blacklisting so noisy channels are avoided.

3.3 Network management and integration

Substation condition monitoring networks must support the addition of new nodes transparently, securely and automatically without operator intervention by the underlying sensor network protocol. Monitoring information may be provided from a number of other sources which may each use different protocols (for example: IEC 61850, DNP3 and MODBUS), therefore protocol adaption at the sensor network basestation is required to integrate wireless protocols with field protocols used within the wired network.

3.4 Time synchronisation

The ability to synchronise geographically dispersed nodes is critical within all distributed systems so that each node has an accurate reference with which to timestamp sensor data, and (depending on the wireless protocol method) synchronise transmission and reception slots between nodes. Factors including voltage fluctuations, age and temperature cause all digital clocks to accumulate clock error, where local time at the sensor node deviates from the atomic time. To correct these errors, a clock synchronisation scheme can be employed by the sensor network protocol [15].

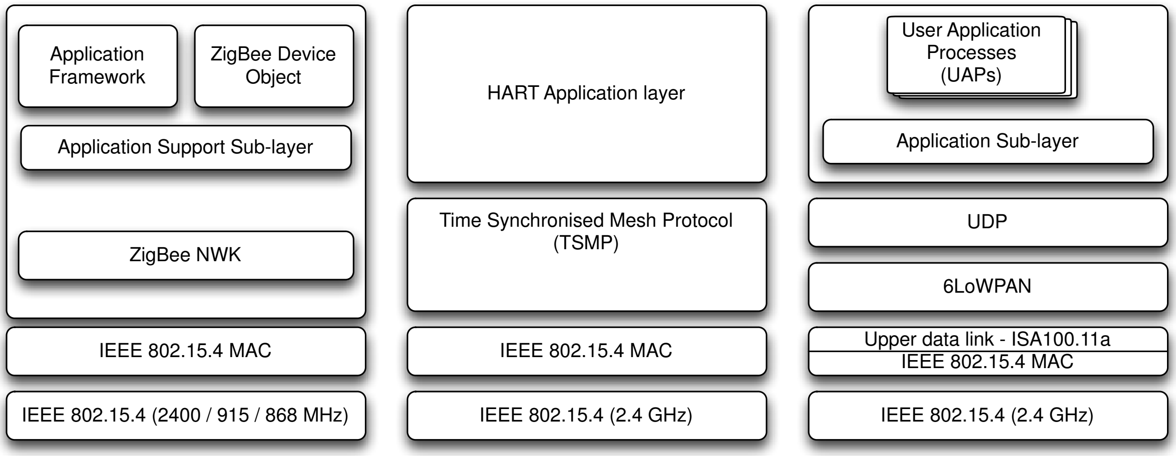
3.5 Power

Power availability within a wireless sensor network governs the behaviour and performance of all aspects of the system. For every wireless sensing application, it is necessary to analyse the energy profile of all components—both hardware and software—so that optimisations can be made [16]. For substation applications, sensor nodes must operate continuously for many years, requiring sensing hardware and applications to be designed accordingly.

There are two potential approaches to powering CM sensors. Firstly, using a primary (non-rechargeable) battery with a fixed lifespan, which needs to be replaced after a certain length of time. The second approach is to use an energy harvesting device with or without a secondary (rechargeable) battery or supercapacitor. Solar panels were employed to power condition monitoring sensors in [11], and energy harvesting from the latent electromagnetic fields has been demonstrated for substation environments in [17].

4 Wireless Sensor Network Standards for Power System Condition Monitoring

A standards-based approach to building industrial wireless sensor networks offers interoperability, ease of integration between different vendors, and a well documented security model. This section describes the most relevant WSN standards applicable to power system condition monitoring, based upon investigations into the literature and the state-of-the-art in WSN technology. The relevant protocol stacks (layers of communications network standards) are shown in Figure 1.



(a) Zigbee stack [18] **(b) WirelessHART stack [19]** **(c) ISA100.11a stack [20]**

Figure 1: OSI reference model for Zigbee, WirelessHART, and ISA100.11a protocol stacks

4.1 IEEE 802.15.4

IEEE standard 802.15.4 defines the physical (PHY) and media access control (MAC) layer specification for low-data rate, low-power wireless personal area networks (WPANs) [21]. The standard has three physical layers, operating in 3 unlicensed bands (868 MHz, 915 MHz and 2.4 GHz), with the most recent (2006) revision of the standard supporting over-the-air data rates of up to 250 kbit s^{-1} in each band. In the 2.4 GHz band, the standard operates in 15 discrete channels (11-25). By default, the MAC layer employs Carrier Sense Multiple Access (CSMA) and supports clear channel assessment (CCA) to mitigate against transmission collisions. Both star and peer-to-peer (mesh) topologies are supported, along with multiple addressing schemes. Cryptographic primitives are defined for building higher-level encryption and authentication features.

Gungor *et al.* [2] investigate the performance of wireless sensor networks for smart grid applications through deployments of IEEE 802.15.4-based wireless networks within three power-system environments: a 500kV substation, a power control room and an underground distribution substation, characterising the wireless link in each location in terms of packet reception rates. The study focuses on the IEEE 802.15.4 protocol, so the results are applicable to all 802.15.4-based protocols. However, as 802.15.4 only defines the lowest layers of the protocol stack, higher level network functions included in IWSN protocols serve to increase reliability well beyond the capabilities of a simple 802.15.4 network link.

IEEE 802.15.4 is a key technology for standards-based wireless sensor networks, as it is the root from which all other open WPAN standards grow. From a practical standpoint, the PHY and MAC layers provide basic peer-to-peer messaging capabilities, however, these two layers alone do not meet requisite industrial requirements such as multi-layer encryption and data reliability. These functions are deferred to higher layers, and implemented by other protocols that incorporate IEEE 802.15.4 technology.

4.2 Zigbee

ZigBee, governed and published by the ZigBee Alliance [22], builds upon the IEEE 802.15.4 protocol defining the network layer to provide tree and mesh networking, multi-hop routing and route discovery, and providing upper layers to support specific sensing applications. Multi-layer security mechanisms are included to ensure the integrity of the network. The latest iteration of the protocol, ZigBee Pro, offers channel-hopping functionality [23] (described later).

The main application area for ZigBee networks are non-industrial monitoring and control applications, using ‘application profiles’ which target specific applications. These profiles are designed to enforce interoperability between devices from different vendors. Example profiles include ‘Home automation’, ‘Smart energy’, ‘Health care' and 'Device remote control'. ZigBee is in continuous development, and up-to-date information on available ZigBee application profiles can be found on the ZigBee Standards website [24].

ZigBee was the first 802.15.4-based full-stack protocol to be released, therefore it has seen significant interest from potential industrial adopters. A study of the performance of ZigBee in substation environments has found that in laboratory conditions it is not affected by PD and other impulsive noise sources [1]. However, Akyol *et al.* [12] find that ZigBee has security concerns that deem it inappropriate for power application usage outside the home. This view is echoed in [25], which suggests that Zigbee is not suitable for most industrial applications. Another critical reason, highlighted in a recent EPRI report [26], is that, as yet, there is no industrial application profile for ZigBee therefore its proper operation within industrial settings has not been specified. Consequently, performance and vendor interoperability cannot be guaranteed. This evidence suggests that, despite Zigbee having been trialled in industrial environments, it has not gained any traction due to its shortcomings in the industrial domain, and there are specific recommendations against its use for power system monitoring.

4.3 Time-synchronised Mesh Protocol

The Time Synchronised Mesh Protocol (TSMP) [27], while itself not being a standalone ratified wireless standard, has become a *de facto* standard for industrial wireless sensor network protocols due to its incorporation in both WirelessHART and ISA100.11a, described later. Built on top of the 2.4 GHz IEEE 802.15.4 PHY and MAC layers, TSMP specifies extended MAC and network (NWK) layer functionality, providing temporal, frequency, and spatial network diversity. These are achieved through five key features:

1. **Redundant mesh networking**: TSMP supports automatically configured mesh networking, using advanced scheduling and routing algorithms to optimally decide where and when packets should be sent. Time Division Multiple Access (TDMA) is employed in place of CSMA to remove device contention, as each node is assigned specific timeslots within which it is permitted to transmit and receive data.
2. **Time synchronisation**: One key requirement for TDMA-based systems is an accurate shared sense of time between nodes. Nodes are automatically synchronised to sub-millisecond accuracy against International Atomic Time (TAI). This ensures that nodes enable their transmitters and receivers for the minimum amount of time possible to conserve energy.
3. **Channel hopping**: As stated previously, TSMP is built on the 802.15.4, 2.4 GHz PHY specification which operates in 16 discrete frequency channels. To mitigate against RF interference, Frequency Hopping Spread Spectrum (FHSS) is used where nodes dynamically switch between communication channels in a predetermined pseudorandom sequence. Channel noise assessments and blacklists are also supported to block specific channels in use by other RF sources in the same band such as WiFi and Bluetooth.
4. **Security**: Multi-layer encryption and authentication provides node-to-node and link-to-link security, ensuring message validity and integrity by stopping 3rd party nodes from joining the network and preventing routing nodes between the sender and receiver from eavesdropping or injecting spurious data.

TSMP is a key technology for IWSN standards, forming the cornerstone of both WirelessHART and ISA100.11a protocols, supporting industrial-grade wireless monitoring networks without the constraints associated with wired systems, while maintaining a focus on network resilience and security.

4.4 WirelessHART

In September 2007, the WirelessHART standard was released as a wireless evolution of the ubiquitous HART protocol used in process field networks [28]. This standard became the first for WSNs to be ratified by the IEC (in April 2010) as IEC 62591 [29].

The HART standard extends the 4-20mA analogue process loop standard with a multiplexed digital channel for sensor interrogation, configuration and diagnostics. WirelessHART extends this further with a robust and secure network stack for industrial monitoring and control applications, with native application layer support for existing HART-compliant sensors [30]. The WirelessHART protocol stack is shown in Figure 1b.

In [31], Kim *et al*. investigate the WirelessHART standard from an industrial user's point of view, describing each of the core components of the WirelessHART standard and the requirements for deploying a WirelessHART network. Petersen and Carlsen [6] give a performance evaluation of WirelessHART for factory automation, where nine temperature and pressure sensors are deployed within a noisy RF environment, close to large metal structures and with limited line-of-sight between the sensors and the base station. Three operational scenarios were tested: normal operation, coexistence with 802.11 WiFi networks, and operation under a simulated denial-of-service attack using a 2.4 GHz chirp jammer device. To quantify the relative performance of each of the scenarios, packet loss, reliability and latency were measured. Under normal conditions, packet loss was around 1%, however 100% reliability was maintained at the expense of latency and channel capacity. WiFi networks were found to degrade the performance of the WirelessHART network, but network reliability was maintained at 100%. This was without channel planning and although WirelessHART supports channel blacklists, they must be defined manually rather than being set automatically by nodes using channel noise assessments. The denial of service (DoS) attack used the chirp jammer 1m from the basestation, reducing the network reliability to zero. However, in an operational setting an attack like this would primarily be an issue of physical security which should ideally be monitored by a surveillance system.

WirelessHART has had limited but successful deployments within the industrial sector [32] [33]. Despite it having been the first industrial WSN standard to be ratified, its primary focus on being an extension of the HART protocol renders it unsuitable for most applications in the power domain as it is incompatible with other process bus standards and does not support application layer extensibility for generic monitoring and diagnostic applications. Nevertheless, results from initial trials in the oil and gas sector may be informative, as this is an industry that is just as operationally rigorous, safety-driven and cautious to disruptive technologies as the power industry.

4.5 ISA100.11a

The International Society of Automation (ISA) standard ISA100.11a is a recent addition to the 802.15.4-based IWSN protocol family, designed for wireless process control and monitoring [20]. ISA100.11a is currently under consideration as an ANSI standard, having been approved by the IEC as a ‘publicly available specification’, en route to future ratification as IEC 62734 [34].

The protocol augments the 802.15.4 MAC layer with support for the 6LoWPAN standard for IP version 6 enabled wireless sensor networks. Sensor nodes in an ISA100.11a network can take on multiple roles, either as routing nodes, sensing nodes or both. This allows for flexible deployments where sensors can be specifically configured with or without mesh routing functions, and additional non-sensing routing nodes can be added to the network to increase spatial diversity and hence network reliability. An example of how this feature could be effectively utilized in a substation environment is where routing nodes could be placed in regions with high magnetic flux powered by inductive energy harvesters such as the one developed in [17]. These nodes would be powered from the latent magnetic field, potentially offering a robust routing network with which to connect adjacent sensor nodes.

ISA100.11a supports adaptive blacklisting, where individual nodes can use clear channel assessment (CCA) to contribute to a network-wide channel occupancy survey which can mandate that certain channels are blacklisted from use, for instance if a WiFi network is co-located on the same site.

The ISA100.11a standard is not limited to the transmission of process bus sensors. In fact, it is possible to layer any application on top of ISA100.11a through protocol-level support for IP-like data communication. This type of communication allows standards-based process bus sensors to be used in parallel with advanced sensing and detection techniques that require message-based communications. In this way, any application can be built on top of an ISA100.11a network, gaining the benefits of rugged network performance and low power consumption combined with the flexibility of a generic communications platform.

ISA100.11a also specifies the Gateway Service Access Point (GSAP) protocol which gives access to sensor network services, configuration, and auditing features to wired clients outside of the sensor network. GSAP supports protocol translators through the definition of a set of communication and control primitives. Each ISA100.11a basestation runs a GSAP service, offering GSAP clients logical access to remote sensor nodes for polling, configuration, and updating. This offers a flexible approach to sensor network management that can be integrated into existing distribution automation systems.

4.6 Discussion

All of these technologies stem from the IEEE 802.15.4:2006 specification for personal area networks. For power system use, despite being the first protocol to market, ZigBee has gained little traction and, in its current form, has been recommended for power system use only within the home [12].

Both WirelessHART and ISA100.11a fill a common application space, competing for early industry adoption. [35] compares WirelessHART and ISA100.11a for process automation and manufacturing applications, finding that for process control and monitoring networks, WirelessHART may be an attractive option especially where HART-enabled sensors are already in place. However, WirelessHART's exclusive support for HART-enabled sensors forces vendor lock-in, not to mention restricting system flexibility. ISA100.11a provides extensible support for arbitrary application protocols, including WirelessHART, making it a more attractive choice as a platform for substation CM networks.

As ISA100.11a is in its infancy as a standard there have not yet been conclusive studies of its performance in power system monitoring applications. However, as it employs the IEEE 802.15.4 MAC and shares the Time Synchronised Mesh Protocol features with WirelessHART, the performance of these protocols in industrial environments is a direct indication of the performance of ISA100.11a. Adaptive blacklisting support also suggests that ISA100.11a may perform better than WirelessHART in an evolving operational setting. Field testing of ISA100.11a networks is critical if ISA100.11a is to be adopted for power system condition monitoring.

5 Case study deployment of ISA100.11a for substation condition monitoring

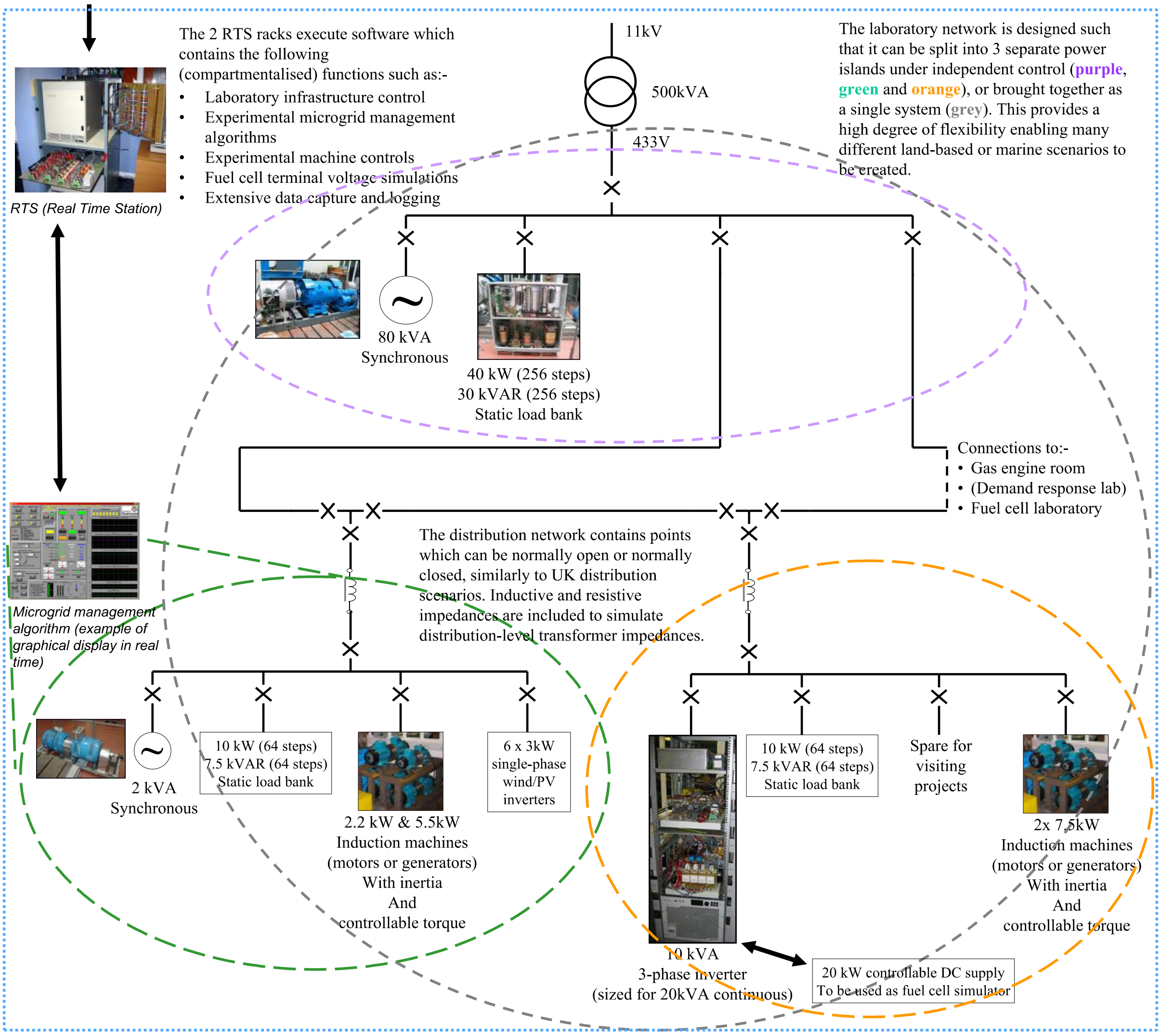
In order to test the features of ISA100.11a within a power system environment, a condition monitoring installation was deployed within the University of Strathclyde's 400V 3-phase microgrid laboratory [36]. It should be noted that the aim of this case study was not to test the data transmission limits of the network or the processing capabilities of the sensor nodes. The case study aims to show some of the design considerations revealed by using off-the-shelf hardware for the ISA100.11a network, and to explore the effects of transient and continuous sources of noise as may be encountered within a power system environment. To that end, a relatively small network of three sensor nodes was deployed within the LV microgrid laboratory.

The network (Figure 2) includes four generators:

1. An 80 kVA motor-generator (M-G) set
2. A 2 kVA M-G set
3. 23 kVA of PV inverters
4. A 10 kVA inverter.

The network can operate as an island, as three separate islands, or grid connected through a 500 kVA 11 kV / 400 V transformer. The loads include a mixture of variable loadbanks, induction motors, and single phase loads. This facility is used for many experimental purposes, including testing of equipment behaviour under unusual transient conditions, replaying of large network disturbance scenarios in order to validate control, and active network management system testing.

While the network is LV, the close proximity of all plant produces the type of electrically noisy, space-constrained environment representative of an MV substation. The requirements placed on a condition monitoring deployment within this environment are very similar to those detailed in Section 3, including the need to limit cabling, simplify deployment and sensor management, be robust to noise (both from electrical sources and a co-located WiFi network), and to ensure the security of sensor data.



The 2 RTS racks execute software which contains the following (compartmentalised) functions such as:-

- Laboratory infrastructure control
- Experimental microgrid management algorithms
- Experimental machine controls
- Fuel cell terminal voltage simulations
- Extensive data capture and logging

The laboratory network is designed such that it can be split into 3 separate power islands under independent control (**purple**, **green** and **orange**), or brought together as a single system (**grey**). This provides a high degree of flexibility enabling many different land-based or marine scenarios to be created.

The distribution network contains points which can be normally open or normally closed, similarly to UK distribution scenarios. Inductive and resistive impedances are included to simulate distribution-level transformer impedances.

Figure 2: Schematic of the microgrid lab network. Dashed lines show the areas which can operate as islands.

In addition, the control architecture for the microgrid network is similar to the smart grid substation environment, allowing manual or automated reconfiguration, load shedding, and the ability to curtail generation under thermal constraints. Consequently, the challenges of creating and deploying the condition monitoring system detailed below are relevant to condition monitoring within the substation.

5.1 System architecture

The monitoring system architecture comprised three wireless sensor nodes and one basestation. Wireless nodes were deployed at the 80 kVA M-G set, at an induction motor, and on the plant room wall for ambient monitoring. Past experience with utility condition monitoring installations suggested that satisfactory timescales for data collection could range from every five minutes [37] up to once per day [38], depending on the specific application. For this installation a SCADA-type timescale of 10 minutes was selected, with each node reporting data to the wireless gateway at 10 minute intervals.

The wireless basestation is an ISA100.11a-compliant Nivis VersaRouter VS900, configured by way of a web-based interface. This ruggedised device includes a monitoring host which concentrates sensor node data, and MODBUS server support to transform physical sensor node tags to logical MODBUS registers which can be interrogated by wired MODBUS clients.

The substation-level data concentrator is a Subnet SEL ruggedised substation computer. The SEL performs protocol translation, in this case translating from MODBUS to OPC format for data archival. Within a substation deployment, this data concentrator would translate to whichever standard fits most appropriately into the utility's existing data architecture.

5.2 Sensor platform architecture

Each wireless sensor node comprises two hardware parts: the ISA100.11a radio, and the microcontroller board. The hardware package can be seen in Figure 3.

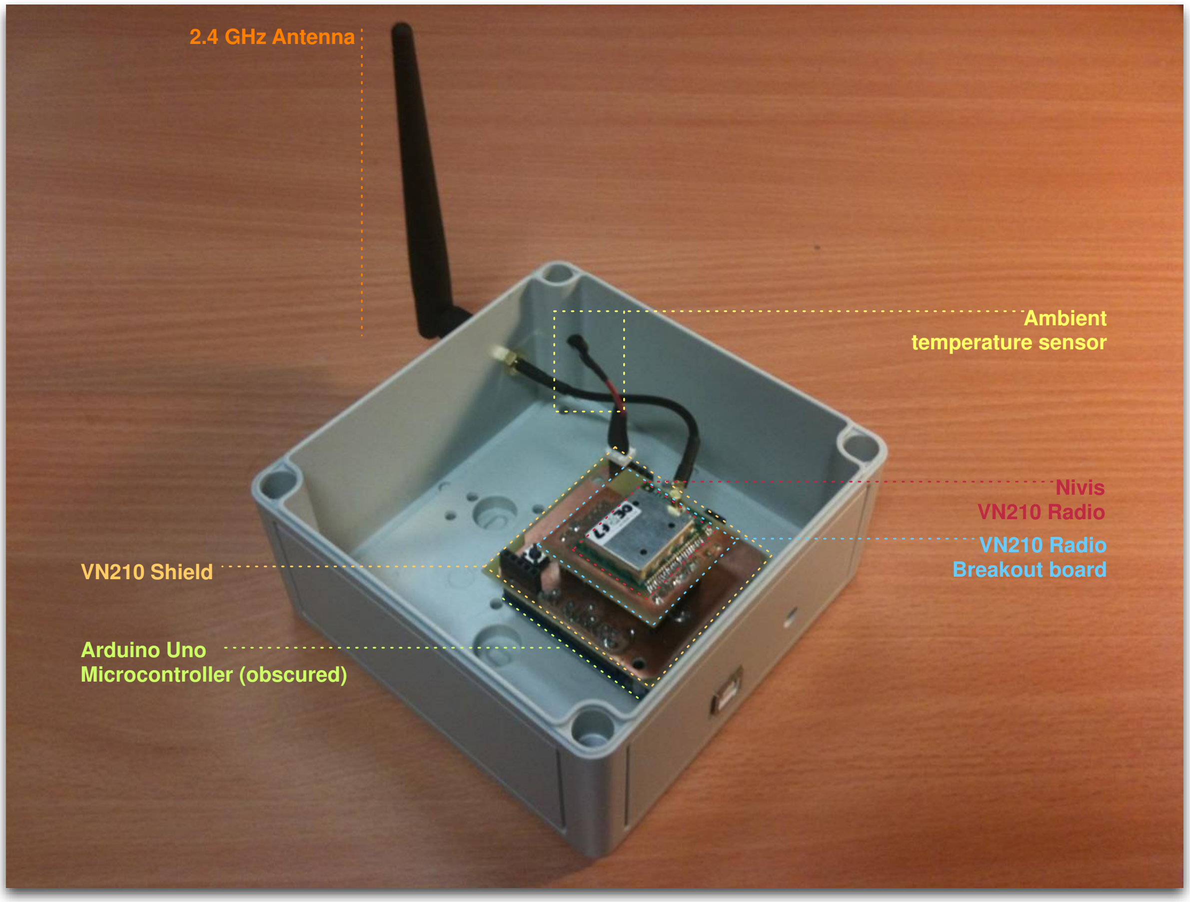


Figure 3: The hardware package for a sensor node

For flexibility, ease of programming, and future application extensibility, the microcontroller board chosen was the Arduino UNO. This platform can be programmed in the C-like Wires language with key functions provided by the Arduino API. Many open-source 3rd party libraries provide additional sensor driver support and utility functions such as timer abstraction. The microcontroller is an Atmel ATmega328: a 16 MHz processor with 32 kB of flash memory and 2 kB of RAM. While it is not initially power-optimised, there are various options for programmatically reducing power usage. The full software and hardware stack is shown in Figure 4.

Each sensor node incorporates a Nivis VN210 ISA100.11a radio, which connects to the Arduino via an adaptor 'shield' interface ("VN210 Shield" in Figure 3). ISA100.11a device functions are managed by the VN210 stack, with a SPI-based software driver providing the interface between the Arduino application processor and the radio board.

The VN210 shield hardware schematic and VN210 radio driver developed for this study are released under Creative Commons 4.0 Sharealike and MIT licences, respectively [39]. Combined with the Arduino hardware and software platform, this provides an open development platform for Nivis-based ISA100.11a industrial WSNs.

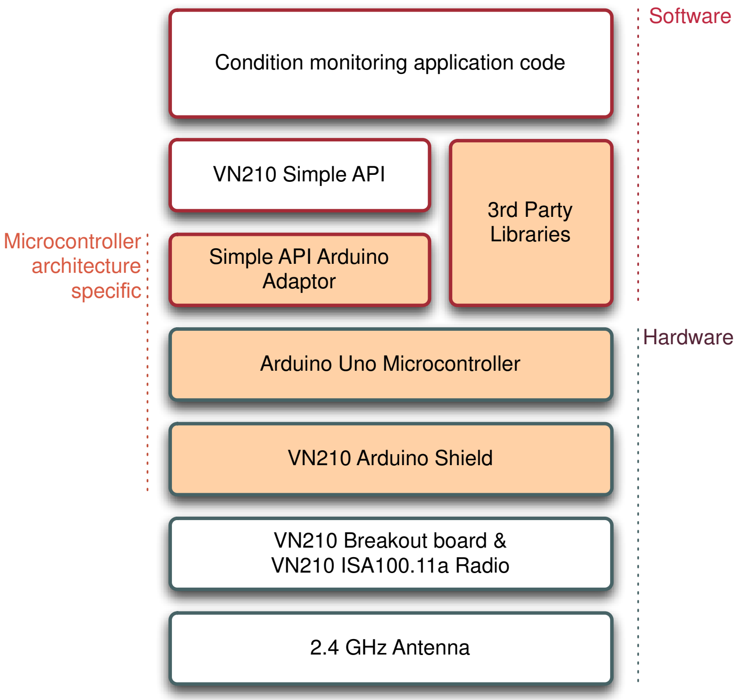


Figure 4: Software and hardware stack of a wireless sensor node

5.3 Monitoring applications

The three sensor nodes monitor the following:

- Ambient temperature within the plant room
- Temperature of a 5.5 kW induction motor
- Vibration of the 80 kVA M-G set.

The ambient node uses a Maxim DS18S20 digital thermometer to sample temperature every 1 s. The sensor node stores the maximum, minimum, and average temperatures during the monitoring period, which are updated as appropriate when a new sample is taken. Every 10 minutes these values are transmitted before being reset for the next period. In this way, SCADA-like 10 minute averaged data is collected.

The second node is very similar to the first, incorporating a LabFacility K-type thermocouple with an M6 screw termination that is screwed directly into an induction motor ground tap (Figure 5). The use of the ground tap ensures a robust thermal bond without the use of epoxy. The thermocouple interfaces with a MAX6675 thermocouple amplifier whose open source hardware schematic and driver are available online at [40]. As before, 10 minute maximum, minimum, and average temperatures are reported over the radio to the basestation.

Figure 5: Node 2 in situ (bottom), with base station visible (top)

The 80 kVA M-G set node (the most complex of the three) interfaces with an ADXL345 three-axis accelerometer, mounted using a magnetic base to a point on top of the machine-side casing. The three axes are oriented with *x* axially along the length of the machine, *y* radially across it, and *z* being vertical.

Standard machinery diagnostics practice is to monitor key vibration frequencies, including 0.5x, 1x, 2x, and 3x rotational frequency. Changes to the amplitudes of these components can highlight common fault types, such as out of balance faults, misalignment, and mechanical looseness [41].

In this application, the accelerometer is sampled every 4 ms for a Nyquist frequency of 125 Hz. The M-G set rotates at 25 Hz, so this captures up to the 5th harmonic at most. An 8-bit Fast Fourier Transform (FFT) is performed on-board the Arduino (LSB equal to an acceleration of 0.1248 g), and for initial testing, this was transferred by serial connection to a computer for storage.

In this application it is not practical for the raw data or the full frequency spectrum to be transmitted wirelessly, due to the amount of data and therefore time and power required. Even calculating four harmonics for all axes gives 12 values to report, while the default ISA100.11a radio firmware forwards only four 32-bit floating point registers to the basestation. Development of a fully customised ISA100.11a sensor which supports an arbitrary number of registers is non-trivial and was outside of the scope of this study; therefore the vibration signature of the machine had to be characterised to focus on the most important four values.

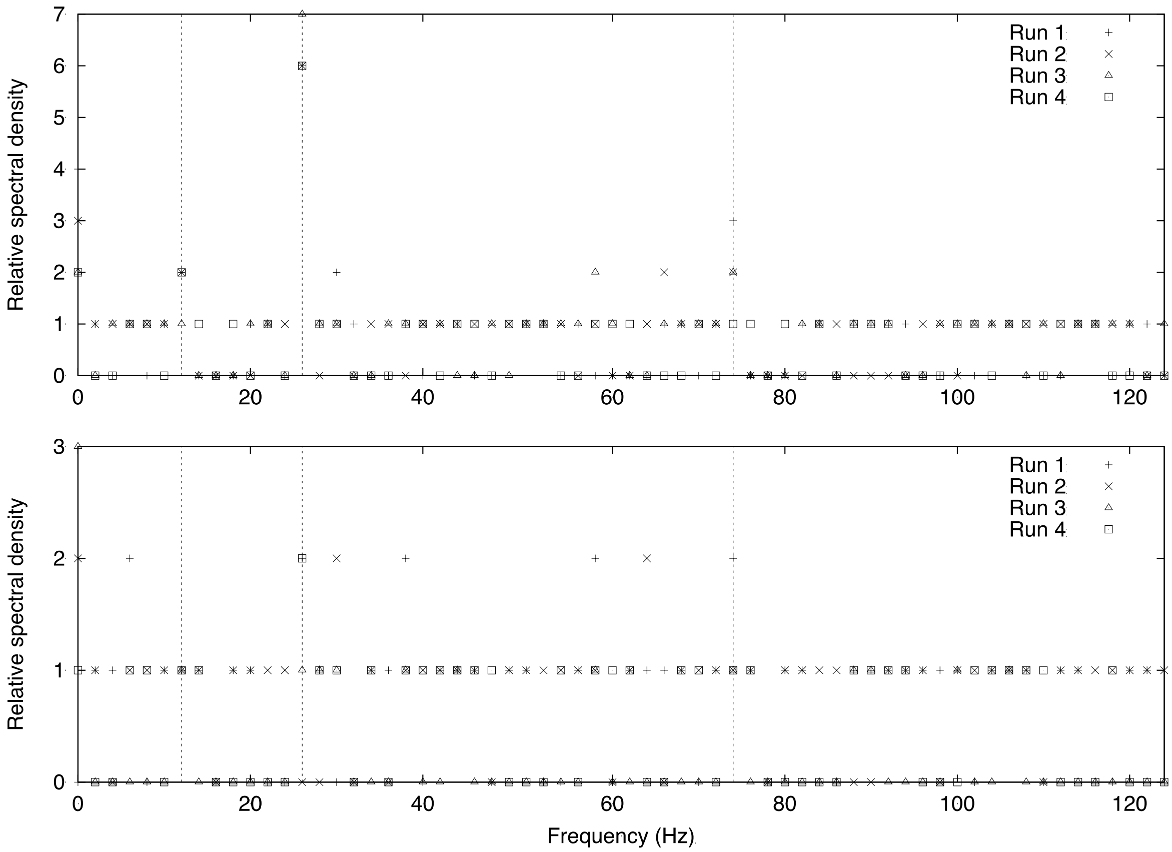


Figure 6: Frequency spectra of the axial (above) and radial (below) vibration. 0.5x, 1x, and 3x rotational frequencies are marked with dashed lines.

To do this, four runs of 512 ms of data were captured under normal operating conditions, and the FFTs calculated. The results are overlaid in Figure 6, which shows slight variations between runs. The axial vibration shows clear peaks at 1x and 3x rotational frequency (25 Hz and 75 Hz), as well as 0.5x and frequencies with no harmonic relationship. The radial direction has a lower amplitude of vibration generally, but peaks can be seen at many of the same frequencies as the axial plot. The *z* axis sensor showed no significant peaks, so its data was not included in the wireless transmissions. The values chosen for wireless transfer were 0.5x, 1x, and 3x rotational frequency in the axial direction, and 1x in the radial direction.

5.4 Network results

The system has been operational for over 12 months while day-to-day work has continued in the laboratory. The WSN is co-located alongside an IEEE 802.11(b/g) WiFi network, which occupies 2.4 GHz channel 9. While this is below the 802.15.4 channel range of 11–25, a WiFi network will infringe upon two adjacent channels on both sides of the main channel, therefore affecting channel 11.

The channel blacklist comprises channels 11 (as expected), 13, 14, 15, 16, 17, 19, and 22. This leaves the list of clear channels as 12, 18, 20, 21, 23, 24, 25, which are predominantly at the upper end of the available spectrum.

Testing revealed that start-up of plant within the microgrid can cause strong transient interference on particular channels. Start-up of the 2 kVA M-G set causes severe packet loss on channels 20 and 23 (one test showing 12% and 25% loss respectively). Start-up of the 10 kVA inverter impacts channel 20 only, with two consecutive tests causing 50% and 75% packet loss on this channel. These effects are short-lived, with channel statistics returning to under 2% loss within 5 minutes of plant energisation.

Since these start-ups occur relatively infrequently (even busy periods seeing under 10 per day) it is appropriate that these channels are not blacklisted. The transient effects do not lead to high packet loss when averaged over hours, and therefore these channels need not be avoided. In contrast, the relatively high number of channels which are blacklisted are due to more constant sources of noise and interference.

6 Future research challenges for substation adoption

The case study deployment demonstrated that ISA100.11a is suitable for use within a substation-type environment, with certain features such as automatic channel blacklisting being particularly useful. This section considers areas where any new standard, including ISA100.11a, could be enhanced for substation-specific deployments.

6.1 ISA100.11a and IEC 61850 Integration

ISA100.11a supports arbitrary application-layer protocol tunnelling, which has the potential to simplify condition monitoring system deployments (for instance by supporting IEC 61850 or the IEEE 1451 Smart Transducer standard [42]). Devices compliant with a particular standard would require a corresponding adaptor that translated the native protocol to an ISA100.11a User Application Process. As yet, this remains to be addressed, but its solution could pave the way for more flexible, wireless distribution automation and CM systems in the future.

6.2 Phase-resolved power system monitoring

The Time Synchronised Mesh Protocol (TSMP) which underpins ISA100.11a and WirelessHART specifies that each sensor node must have an accurate shared sense of time to support communication slot synchronisation. For any time-synchronised system, remote clocks inevitably have some timing offset from the atomic time (TAI). This timing error, t_e, is caused by ageing and thermal effects which cause a difference in clock frequencies (skew, ε), plus latencies caused by the synchronisation process (t_s). To guard against these, TSMP defines a value for the guard time, t_g, which is the maximum tolerated clock error for slot synchronisation, where:

$$-t_g < t_e < t_g$$

The guard time for TSMP-based systems is 1 ms, but in real systems the clock error on a node will be significantly less [27]. An empirical study on clock synchronisation errors [43] found that in a practical wireless sensor network, the clock error is normally distributed around a mean value of zero with the maximum observed error approximately equal to the PHY layer symbol length, t_P. This timing jitter is caused by the receiver having to synchronise its clock with the first bit of a received packet at time t_{b0}, where:

$$t_{b0} < \pm t_P$$

For an IEEE 802.15.4-based protocol, the symbol rate is 62.5 k symbol s^{-1} with 4 bits per symbol, resulting in a symbol length, $t_P = 16\mu s$, and bitrate of 250 k bit s^{-1}.

Assuming that this holds true for a TSMP-based protocol, under optimal conditions for a node synchronised at time t_0 [44]:

$$t_e < \varepsilon(t - t_0) + 16\ \mu s$$

Assuming that modern digital clocks would limit ε to under 10 ppm, for a sync time of 30 s this would result in a clock error of less than 316 μs. There may be additional latencies in the synchronisation channel that need to be accounted for, which could be determined experimentally. This presents a significant opportunity for diagnostic applications that resolve sensor measurements against the electrical phase, such as phase-resolved partial discharge (PD) diagnostics. Relying upon timing information from the sensor network rather than from an electrical phase measurement would simplify deployment and could potentially lead to novel CM diagnostic methods specifically designed for wireless sensor network operation.

6.3 Power system monitoring and Big Data

The case study presented above is intended to be representative of a small-scale test deployment which a utility may initiate as a forerunner to a larger wireless deployment. With only three nodes it is fairly limited in its capabilities, although the network can be extended over time with further nodes monitoring additional parameters.

In general, the trend in the power industry is towards increased volumes of data representing multiple parameters from various assets. This trend is driven by decreasing costs of sensor hardware and data storage, as well as technologies such as WSNs which simplify practical issues of deployment and cabling. The smart grid concept, where networks become more self-managing and self-healing, is enabled by increased visibility of the power network and assets, achieved through increased monitoring.

At the same time, many industries are facing similar shifts and challenges of dealing with constant volumes of data. So-called 'Big Data' can be seen in sectors such as the finance industry, which handles millions of transactions per day.

Big Data can be defined according to the Gartner 3 Vs model [45]: where the dataset demonstrates velocity (the speed at which the data can be processed), volume (the volume of data that is being stored or analysed), and variety (the different types of data that are being stored or analysed). When these three traits combine, the complexity of analysing such a dataset in real time becomes extremely challenging with conventional hardware and software solutions.

Within the power industry, there has been some investigation into the applicability of Big Data techniques to power system operation [46] and condition monitoring [47]. Broadly speaking, the velocity and volume of data typically being captured from power networks is not sufficiently great to be considered Big, although extensive deployment of Phasor Measurement Units (PMUs) in the future would start to change this. While not a pressing need at the moment, it is worthwhile watching developments in Big Data research for approaches which may benefit the power industry in the future.

The main tool in the Big Data toolbox is parallelisation, where the processing of data is distributed across multiple computers to improve throughput. Software design paradigms such as MapReduce can support this approach [48], with specialist platforms such as Hadoop simplifying the deployment of such software across the cluster of computers.

One possibility would be to use a WSN as the computing platform for Big Data-type analysis, where each node performs local computation before sending smaller batches of higher level data to a central point. Indeed, the nodes in the case study above display this pattern of behaviour by taking measurements every second, but sending only the 10 minute-averaged data to the basestation. This allows the WSN to reduce the volume and velocity of data that engineers need to deal with. While convenient at current sizes of dataset, this pattern may become essential in future deployments.

7 Conclusion

This paper has presented a review of recent standardisation efforts in the field of industrial wireless sensor networks and discussed their applicability to substation condition monitoring systems. Of the standards discussed, ISA100.11a has emerged as the most suitable for substation applications, offering robust security, network diversity, time synchronisation and integration facilities capable of supporting arbitrary monitoring applications. A case study demonstrated the use of ISA100.11a technology for a smart grid laboratory condition monitoring network, incorporating both temperature and vibration sensors installed on operational plant. An open source platform was developed for this deployment, which has been made available online for other researchers and industrialists to build their own IWSN monitoring systems. Some further research and technical challenges have been outlined, which the authors believe must be met to deliver fully integrated, autonomous wireless sensors for the smart grid.

8 Acknowledgments

Dr P. Baker was supported by National Grid (UK) research funding under contract number TAO/22009.

The authors would like to thank Mr Frank Cox and Mr Gordon Jackson for their technical skills and guidance through the development and deployment of the laboratory-based wireless condition monitoring network.

9 References

[1] Q. Shan, I. A. Glover, P. J. Moore, I. E. Portugues, R. J. Watson, and R. Rutherford, "Performance of Zigbee in Electricity Supply Substations," *Int. Conf. Wireless Communications, Networking and Mobile Computing (WiCom 2007)*, no. pp. 3866-3869, 2007.

[2] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid," *IEEE Transactions on Industrial Electronics,* vol. 57, no. 10, pp. 3557-3564, October 2010.

[3] R. A. Leon, V. Vittal, and G. Manimaran, "Application of sensor network for secure electric energy infrastructure," *Power Delivery, IEEE Transactions on,* vol. 22, no. 2, pp. 1021-1028, 2007.

[4] M. M. Nordman and M. Lehtonen, "A wireless sensor concept for managing electrical distribution networks," in *Power Systems Conference and Exposition, 2004. IEEE PES*, ed: IEEE, 2005, pp. 1198-1206.

[5] A. Nasipuri, R. Cox, J. Conrad, L. Van der Zel, R. Zel, and M. Bienvenido Rodriguez, "Design considerations for a large-scale wireless sensor network for substation monitoring," in *5th IEEE Int. Workshop on Practical Issues in Building Sensor Network Applications*, ed. Denver, Colorado, 2010, pp. 866-873.

[6] S. Petersen and S. Carlsen, "Performance evaluation of WirelessHART for factory automation," in *IEEE Conf. Emerging Tech. & Factory Automation*, ed, 2009, pp. 1-9.

[7] Y. Han and Y. Song, "Condition monitoring techniques for electrical equipment-a literature survey," *IEEE Trans. Power Del.,* vol. 18, no. 1, pp. 4-13, 2003.

[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks,* vol. 38, no. 4, pp. 393-422, 2002.

[9] Q. Gao and H. Wang, "WSN design in high-voltage transformer substation," in *Intelligent Control and Automation*, ed: IEEE, 2008, pp. 6720-6724.

[10] A. Nasipuri, R. Cox, H. Alasti, L. Van der Zel, B. Rodriguez, R. McKosky, and J. A. Graziano, "Wireless Sensor Network for Substation Monitoring : Design and Deployment," in *Proc. 6th ACM conf. Embedded network sensor systems*, ed, 2008, pp. 365-366.

[11] A. Nasipuri, H. Ala, P. Puthran, R. Cox, J. Conrad, L. Van der Zel, B. Rodriguez, R. McKosky, and J. Graziano, "Vibration sensing for equipment's health monitoring in power substations using wireless sensors," *Proc. IEEE SoutheastCon 2010*, no. pp. 268-271, March 2010.

[12] B. Akyol, H. Kirkham, S. Clements, and M. Hadley, "A Survey of Wireless Communications for the Electric Power System," US Department of Energy Tech Rep PNNL-19084, 2010.

[13] P. Moore, I. Portugues, and I. Glover, "Pollution of the radio spectrum from the generation of impulsive noise by high voltage equipment," in *IEE Seminar Digests* vol. 37, ed, 2002.

[14] S. Bhatti, I. Glover, R. Atkinson, Q. Shan, Y. Yang, and J. da Rocha Neto, "Vulnerability of Bluetooth to impulsive noise in Electricity transmission substations," in *IET Int. Conf. Wireless Sensor Network*, ed, 2010, pp. 53-58.

[15] F. Sivrikaya and B. Yener, "Time synchronization in sensor networks: a survey," *Network, IEEE,* vol. 18, no. 4, pp. 45-50, 2004.

[16] V. Raghunathan, C. Schurgers, S. Park, and M. B. Srivastava, "Energy-Aware Wireless Microsensor Networks," *IEEE Sig. Proc. Mag.*, no. March 2002.

[17] N. M. Roscoe and M. D. Judd, "Harvesting Energy From Magnetic Fields to Power Condition Monitoring Sensors," *IEEE Sensors Journal,* vol. 13, no. 6, pp. 2263-2270, June 2013.

[18] D. Gislason, *Zigbee wireless networking*: Newnes, 2008.

[19] D. Chen, M. Nixon, and A. Mok, *WirelessHART: Real-Time Mesh Network for Industrial Automation*: Springer Verlag, 2010.

[20] International Society of Automation, "Wireless Systems for Industrial Automation: Process Control and Related Applications," ISA100.11a-2011, 2009.

[21] IEEE Computer Society, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)," IEEE 802.15.4-2006, September 2006.

[22] Zigbee Alliance, "Zigbee specification," *ZigBee Document 053474r06, ,* vol. 1, no. pp. 1-378, 2005.

[23] P. Baronti, P. Pillai, V. Chook, S. Chessa, A. Gotta, and Y. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," *Computer Communications,* vol. 30, no. 7, pp. 1655-1695, May 2007.

[24] Zigbee Alliance. (2012). *ZigBee Standards Overview*. Available: http://www.zigbee.org/Standards/Overview.aspx

[25] T. Lennvall, S. Svensson, and F. Hekland, "A comparison of WirelessHART and ZigBee for industrial applications," in *IEEE Int. Workshop on Factory Communication Systems*, ed, 2008, pp. 85-88.

[26] EPRI, "Wireless Connectivity for Electric Substations," EPRI, Palo Alto, CA Tech Rep 1016145, 2008.

[27] Dust Networks, "Technical Overview of Time Synchronized Mesh Protocol (TSMP)," Dust Networks, 2007.

[28] HART Communication Foundation. Available: http://hartcomm.org

[29] IEC. (2010). *IEC 62591: Industrial comms. networks: Wireless communication network and communication profiles: WirelessHART*.

[30] HART Communication Foundation, "WirelessHART Technical Data Sheet," Tech Rep HCF_LIT-98, 2007.

[31] A. N. Kim, F. Hekland, S. Petersen, and P. Doyle, "When HART goes wireless: Understanding and implementing the WirelessHART standard," in *Emerging Technologies and Factory Automation, IEEE International Conference on*, ed: IEEE, 2008, pp. 899-907.

[32] S. Petersen, P. Doyle, S. Carlsen, J. H. van der Linden, B. Myhre, M. Sansom, A. Skavhaug, E. Mikkelsen, and D. Sjong, "A Survey of Wireless Technology for the Oil & Gas Industry," in *Intelligent Energy Conference and Exhibition*, ed, 2008.

[33] M. R. Akhondi, A. Talevski, S. Carlsen, and S. Petersen, "Applications of Wireless Sensor Networks in the Oil, Gas and Resources Industries," in *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, ed: Ieee, 2010, pp. 941-948.

[34] International Society of Automation. (2011). *ISA100 Wireless Standard Receives IEC Approval*.

[35] S. Petersen and S. Carlsen, "WirelessHART versus ISA100.11a. The Format War Hits the Factory Floor," *Industrial Electronics,* vol. 6, no. 4, pp. 23-34, December 2011.

[36] A. J. Roscoe, A. Mackay, G. M. Burt, and J. R. McDonald, "Architecture of a Network-in-the-Loop Environment for Characterizing AC Power-System Behavior," *IEEE Transactions on Industrial Electronics,* vol. 57, no. 4, pp. 1245-1253, April 2010.

[37] V. M. Catterson, S. D. J. McArthur, and G. Moss, "Online Conditional Anomaly Detection in Multivariate Data for Transformer Monitoring," *Power Delivery, IEEE Transactions on,* vol. 25, no. 4, pp. 2556-2564, 2010.

[38] S. Rudd, V. M. Catterson, S. D. J. McArthur, and C. Johnstone, "Circuit Breaker Prognostics Using SF6 Data," IEEE Power and Energy Society General Meeting, 2011.

[39] P. C. Baker and V. M. Catterson. (2012). *Open VN: An Industrial Wireless Sensor Network R&D platform*. Available: https://github.com/cowlet/open-vn

[40] LadyAda.net. *LadyAda Thermocouple Sensor Tutorial*. Available: http://www.ladyada.net/learn/sensors/thermocouple.html

[41] P. Girdhar, *Practical machinery vibration analysis and predictive maintenance*: Newnes, Elsevier, 2004.

[42] K. Lee, "IEEE 1451: A standard in support of Smart Transducer Networking," in *Proc. 17th IEEE Instrumentation and Measurement Tech. Conf.*, ed. Baltimore, Maryland, 2000, pp. 525-528.

[43] J. Elson and L. Girod, "Fine-Grained Network Time Synchronization using Reference Broadcasts," *SIGOPS Oper. Syst. Rev.,* vol. 36, no. Winter 2002, pp. 147--163, December 2002.

[44] K. S. J. Pister and L. Doherty, "TSMP: Time Synchronized Mesh Protocol," in *IASTED Distrib. Sensor Networks*, ed, 2008, pp. 391--398.

[45] M. Beyer. (2011). *Gartner Says Solving 'Big Data' Challenge Involves More Than Just Managing Volumes of Data*. Available: http://www.gartner.com/newsroom/id/1731916

[46] M. Kezunovic, L. Xie, and S. Grijalva, "The Role of Big Data in Improving Power System Operation and Protection," IREP Symposium: Bulk Power System Dynamics and Control, Rethymnon, Greece, 2013.

[47] D. Ferguson and V. M. Catterson, "Big Data Techniques for Wind Turbine Condition Monitoring," European Wind Energy Association (EWEA 2014), 2014.

[48] J. Dean and S. Ghemawat, "MapReduce: a flexible data processing tool," *Communications of the ACM,* vol. 53, no. 1, pp. 72-77, 2010.