IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 8, 2016, accepted November 22, 2016, date of publication January 17, 2017, date of current version September 19, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2654685

A Standardised Modular Approach for Site SCADA Applications Within a Water Utility

ALEX D. L. GRAY[1,2], IOANA PISICA[1], GARETH A. TAYLOR[1], AND LOUISA WHITEHURST[2]
[1]Smart Power Networks Theme, Energy Futures Institute, Brunel University London, Uxbridge UB8 3PH, U.K.
[2]Thames Water Limited, Reading RG1 8DB, U.K.

Corresponding author: Ioana Pisica (ioana.pisica@brunel.ac.uk)

ABSTRACT Any large water treatment/production utility that employs autonomous plant as part of its processes will utilize supervisory control and data acquisition systems. These systems will generally be isolated from each other and will exist solely to serve the site they control and visualize. More often, they are delivered and developed organically through cost driven maintenance regimes that prioritize on process risk rather than asset lifecycles. In some cases, this has led to variations in installed software and hardware applications, not only across a business enterprise, but also down to a site level. This is usually based on favored products at the time of supply, and in turn requires a broader range of engineering skills to maintain and update. The previous adoption of a ''fit and forget'' model has also led to large areas of unsupported computer assets within an organization that further introduces ''data risk.'' As regulatory bodies start to impose stricter compliance measures on the water industry, so to the suppliers become more reliant upon their process data. This paper presents how a water utility has employed a modular approach and has set to standardize its SCADA assets across all business sectors. It reviews the hardware the systems are installed on, the software applications used to deliver the integration, and discusses how the software devices have been modeled and tagged in search of a common information model. All in line with their respective field assets. It also discusses some of the human factors surrounding the replacement of control systems.

INDEX TERMS SCADA, control systems, human factors, water utility, regulators, process, common information model (CIM), standardisation.

I. INTRODUCTION

The ever increasing availability of faster processing power at more affordable prices is providing water utilities with more robust computational platforms, further enabling access to improved data resolution and efficacy. This increase in data efficacy provides process analysts with a more reliable foundation to base their modelling algorithms. Thus, increasing the value the data brings to the enterprise and the efficiency with which it is stored, accessed and retrieved [1].

From this, utilities are becoming more and more driven towards a common information model (CIM) across all business areas, with a realisation that asset lifecycles can be further extended through an improved understanding of mining techniques and analysis rules. These can be applied to the vast quantities of operational, as well as customer based data they hold [3].

For many years the centralised visualisation of process plant, including the storage of critical infrastructure data variables, has centred on supervisory control and data acquisition (SCADA) systems, where controllers can monitor and manipulate the interaction of a system and its process assets [4].

SCADA systems, as a rule, are generally deployed with a centralised datacentre [5], however, water company estates comprise large physical asset bases, spatially distributed across varying population equivalents (PE). Including regions of mixed topography, geology and land use and therefore site SCADA systems can sometimes become isolated from the central historians, with only the local machine providing access to the historical data.

Providing a better connection mechanism to these isolated sources of data, will ultimately improve the key components of the water companies' data challenges [3]. This will provide faster links to the data, permit real-time trending and event handling, (through remote control), which goes towards being able to operate the asset base in an improved way. For example, if a waste water site was receiving an influx of influent during an antisocial period, on a site that is not 24hr manned, there could be a process risk that leads to an environmental consent breach. These breaches cost water companies large amounts in fines each year [6].

The Thames Water annual report and financial statement for 2014/15 provided pollution information, which suggested it was still exceeding the upper control limit set by The Water Services Regulatory Authority (OFWAT) [7]. This results in the below ground asset performance being categorised as deteriorating, and has huge commercial impact on the company.

A. MOTIVATION AND CONTRIBUTIONS

Improvement of the SCADA architecture and connection mechanisms allow remote connections, which can permit users to monitor and make control decisions, thus deploying reactive mitigation actions, which then go towards preventing critical events.

Just as processing is becoming more reliable, networked control systems (NCS) are becoming more robust and can provide larger bandwidth, thus permitting larger data packet transfer rates [8]. This, coupled with an increase in available fieldbus enabled actuators, sensors and controllers permits higher resolution information to be distributed over the network, without the need for an increase in direct electrical connections [9]. Where an older variant of flowmeter may have comprised a single discrete 4-20mA output, with an 8-bit array of digital outputs, needing cabling segregation through electromagnetic compatibility (EMC) requirements, the fieldbus NCS infrastructure enables multiple devices, with large analogue and digital information data bundles, to all simultaneously connect over one cabling system (not considering auxiliary power supplies per specific device), due to each device having its own node address.

This dramatically reduces the requirement for signal infrastructure, including input/output (I/O) cards and cable marshalling cabinets, thus reducing the control panel real-estate. Other advantages include the distances between instrument and control system that can be achieved with low frequency communication and easy integration in the field [10].

The contributions of this paper include the utilisation of a **common object template library** developed by a utility company for standardising the approach to SCADA applications. This library provides **standardised building blocks for asset configuration and visual interfaces**. It also contributes towards an **understanding of human factors associated with adversity towards change** within control rooms across multiple demographics.

B. ORGANIZATION

This paper is organised as follows. Section II describes existing SCADA configuration and process types within a UK water utility. Section III details the new system architecture employed within the delivery of an upgrade project, including the standardised software templates used. After which, Section IV discusses the challenges associated with aligning the systems to a CIM. Section V includes human factors and their challenges with the conclusions of the research presented in Section VI.

II. EXISTING SCADA CONFIGURATION

Within any water utility company there are a number of different process types. Where it is easy to split out the 2 primary types; clean water production and waste water treatment, these two processes also comprise huge variance between their internal inter-stage processes. This, coupled with the technology available at the time of system installation and a limited governance model in place for ensuring alignment, leads to a wide diversity across the different site SCADA types in the utilities estate.

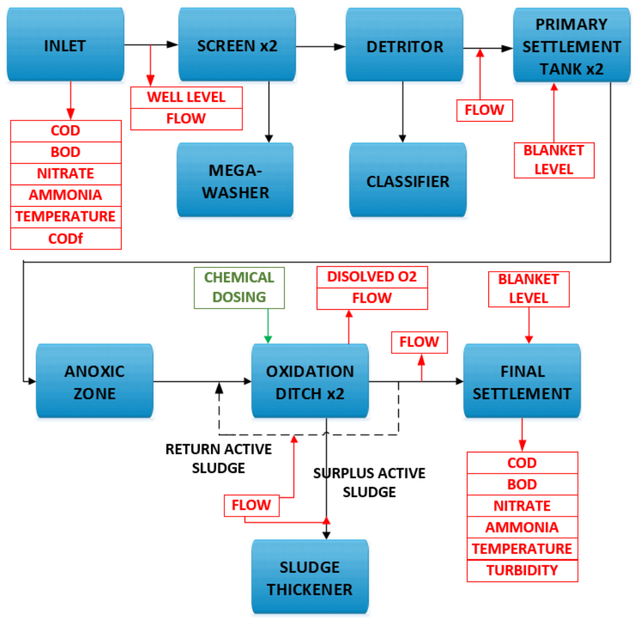

FIGURE 1. Typical sewage treatment process block diagram.

An example sewage treatment application, as per the process block diagram (PBD) shown in Figure 1 will take the effluent from small towns with a PE of approx. 10,000 people.

These sites typically comprise basic primary/secondary filtration and oxidation techniques. Each process area may have a designated programmable logic controller (PLC) and could have a couple of hundred I/O per device. The items coloured red in Figure 1 indicate control system analogue inputs.

For this type of site an operator may use the SCADA for around 20 minutes per day.

Whereas, an example large scale clean water production facility, as per the PBD in Figure 2 below, supplies clean water to large urban areas with PE's in the hundreds of thousands. These sites comprise highly complex processes and control systems, typically with 1000's of I/O per process area. These sites are permanently manned with the shift controllers using the SCADA 24h/day as their primary control interface.

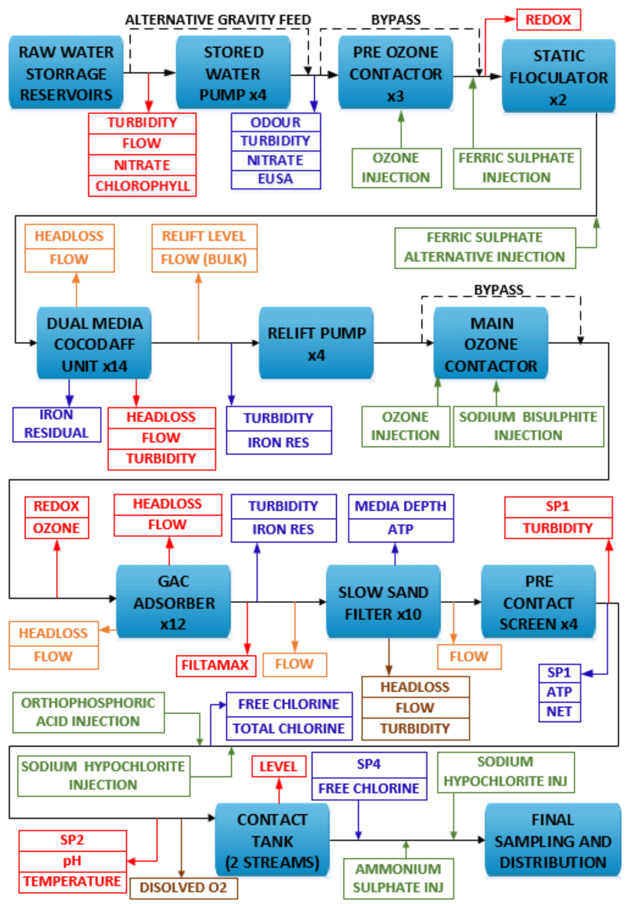

FIGURE 2. Large london clean water process block diagram.

SCADA systems can use several protocols; Object Linking and Embedding for Process Control (OPC), Inter-Control Centre Protocol (ICCP), MODBUS, Distributed Network Protocol version 3 (DNPv3), IEC 870.

The platforms currently in use on site systems vary in design and functionality based upon the age or location of the system, and are generally not integrated from a control or data perspective. This non standardised and bespoke approach leads to issues surrounding the serviceability of the SCADA system, with a requirement for many of the company's operational maintenance teams being divided into their own 'areas of expertise' leading to an increasing reliance upon external resource. For example, one team will need to service a Genesis 32 Iconics™ platform, which utilises Simple Network Management Protocol (SNMP) for system monitoring and management, direct graphical animation tagging via Open Platform Communications (OPC) for plant floor device communication and enterprise infrastructures business objects, such as SAP™ and Oracle™ [11]. Another team will be required to maintain a General Electric Intelution FIX32™ system that utilises indirect database management for I/O control and separate drivers for interfacing to the plant floor devices. When there is a lack of expertise 'on shift', this leaves the enterprise systems exposed during fault events, which in turn could lead to, at the worst case, costly pollution events.

The local engineering resource may comprise an older demographic, which over time reduces through retirement, thus removing that particular knowledgebase and skill set, leaving the area exposed to increased risk.

Many of the SCADA applications are obsolete, running on end of life operating systems and hardware, much of which is no longer supported by the manufacturer. The extraction of business critical data for reporting purposes from these systems is therefore, difficult, and limited to pockets of sites on the newer application types. Or it is undertaken via a labour intensive, manual extraction process, through special requests to the companies technical support teams. Thus the wealth of information and data becomes unavailable from other business stakeholders. Furthermore, when it does become available, is not relied upon due to inconsistencies in database terminologies. A lack of governance on asset tag naming conventions has also made data collection within a central service more complex.

Under the Y2K remit, there was an adoption of central standards, which gave rise to greater consistency in the delivery of new systems. However, even these systems are now classed as legacy applications with most of the hardware and operating systems failing to meet the integration requirements of the utilities operational management centre (OMC).

The current site SCADA systems within the utility comprise a number of products that include; RSView, Paragon, Fix32 and Iconics. Different operator client workstations exist providing different data sets and access methods across the utilities estate. In addition, these legacy systems do not always follow the internally regulated standards. Asset tagging is not applied consistently, which leads to data mining constraints when trying to analyse centrally managed datasets that have propagated from the site historians up to the corporate historians.

III. NEW SYSTEM ARCHITECTURE

A programme to replace the various legacy systems aimed to provide a standardised approach was deployed. This was achieved through the use of a single technology, Wonderware System Platform, which can be scaled to fit systems of varying size. In addition, the utilities internal governing SCADA standards have been applied across all new replacement projects, aiming to provide consistent database construction and visualisation across the estate.

All hardware is standardised on Dell servers with redundant disks, PSUs and monitored by Enterprise Integrated Dell Remote Access Controller (iDRAC). To consolidate the different variants of hardware within the utility, only two types of server have been used. For large and medium sites Dell Poweredge R700 series servers have been utilised and for small sites the Dell Poweredge R300 series servers are specified, although as technology progresses, so to the spec will improve.

The server architecture is a virtual solution using VMware ESXi™. The use and reliance upon virtualisation techniques are discussed and presented in [12]. These techniques permit the use of one or more virtual machines (VM) within a single physical host, enabling multi-platform deployment. The layer responsible for providing the virtual computer abstraction is the virtual machine monitor. Within industry this is known as a hypervisor. Typically, there are two types of hypervisor, Type 1 and Type 2. Type 2 comprises an operating system installed on the physical hardware, with the hypervisor running as an application over on this. Type 1, which is what has been used in the this project, is where a single hypervisor executes directly on the hardware. Type 1 eliminates the need for an additional master operating system, which is then subject to additional costs and updates.

This method was adopted for all new application, historian and terminal server combinations of which make up the different Wonderware system platform site architectures. The advantage of these virtual servers is that they provide the company with the ability to manage them both remotely and securely from one central platform. This can be done securely by an internal resource pool. Virtualising the infrastructure further reduces the number of physical servers and permits 'virtual guests' (operating systems) to run on the same virtual host (hardware). This better utilises the hardware by reducing administration overhead, physical space required in the datacentres and also reduces power and cooling requirements for each site. Using a virtualised environment also allows for the deployment of the Veeam™ backup and recovery utility, which provides enhanced resilience through the provision of recovery times and point objectives of <15 minutes for all virtual applications [13].

The operating system software is based on the Microsoft technology. Windows Server 2008R2 was installed for all server operating systems, with Windows 7 images installed on the client workstations. These workstations are used as 'thick clients' and connect to a remote desktop terminal server.

The SCADA software uses the System Platform's; Application, Galaxy Repository (GR), Terminal, and Historian Servers. These are installed onto the VM's and host the object/scanning engines, database configuration (known as a 'Galaxy'), visualisation applications and historical databases respectively. The database component is provided by Microsoft SQL server 2012. The terminal servers use the InTouch client application to provide mimic visualisation to the operator which is presented when connecting through the terminal server.

Virtual machine templates were created to provide a consistent configuration. These included guest operating systems and associated corporate software. As part of the machine templates, batch files were written to provide the installer with a predefined, governed, installation methodology. Thus, local specific configuration was kept to a minimum which reduced risk through the different supplier's interpretation of how the systems should be setup.

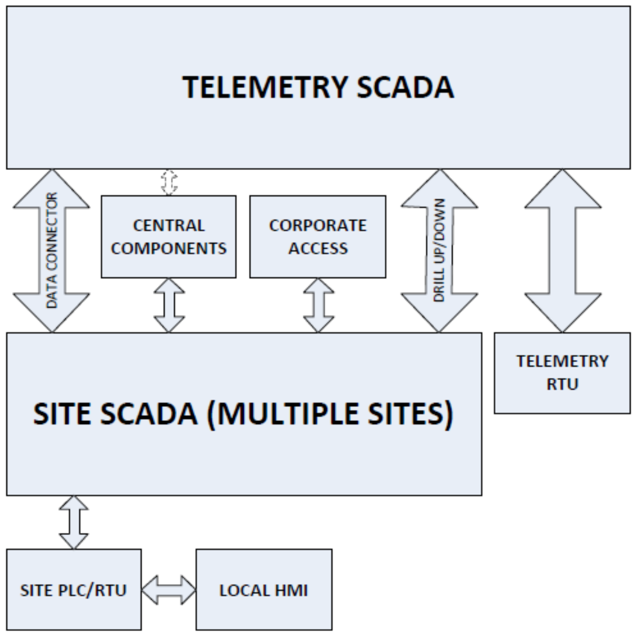

FIGURE 3. High level SCADA estate architecture.

As well as the local site SCADA, most of the process sites within the utility also contain a separate telemetry outstation to regional SCADA system, which provides alarming and visualisation of process critical data to the Operational Management Centre (OMC). Although the technologies of the two systems are different, they interact with each other using data connections OPC and Distributed Component Object Model (DCOM). Figure 3 shows the high level overview of the site data's lifecycle which starts its journey as local field instrumentation and continues up the chain, via either the site SCADA, or telemetry outstation, or both, and ends up in the overarching corporate telemetry SCADA system.

Above the site SCADA systems, this corporate visualisation layer exists, which permits non-operational users access to the system in a controlled manner and provides data for regulatory reporting purposes. This may be disconnected or otherwise controlled when required in order to protect the operational systems.

Each site system replaced was allocated into one of three categories, with each having a standardised architecture. They were classified as small, medium or large systems. This classification was not solely based on I/O count but more on the criticality of the processes being captured. For example, on sewage systems, if advanced processes exist, such as; thermal hydrolysis plant (THP) with high throughput to combined heating and power (CHP) systems, and where the site can generate megawatts in power, then the system was installed under the large architecture. This was due to the increase in redundancy resilience available for both hardware and software. Similarly, in clean water applications, if specialist complex treatment, such as ozone, was a process employed on site, then this full system redundancy was also required.

A. SERVER ARCHITECTURE

All system architectures use an RODC, which is essentially a read only copy of the master domain controller (DC). This master DC is deployed centrally within the enterprise and is the management agent for the SCADA.Net domain. All SCADA servers are integrated on this .Net domain. There is also a Linux virtual management agent (vMA) used for handling the uninterruptible power supply (UPS) status commands and controlling the safe shutdown of the ESXi virtual host.

Small site systems employ a single physical server with virtual machine and operating system, containing an all-inclusive repository, application, historian and terminal server. The RODC and vMA are included as standard.

Medium sites consist of a pair of dual redundant application servers and a terminal server running on a single virtual host. One of the application servers is a combined historian with GRNode server. Again, the RODC and vMA are included as standard.

Large sites consist of a standalone GRNode, dual redundant Application Servers and a pair of terminal servers. The data historian is dual redundant with the primary historian on the GRNode. The backup historian has its own guest operating system located on the other virtual host.

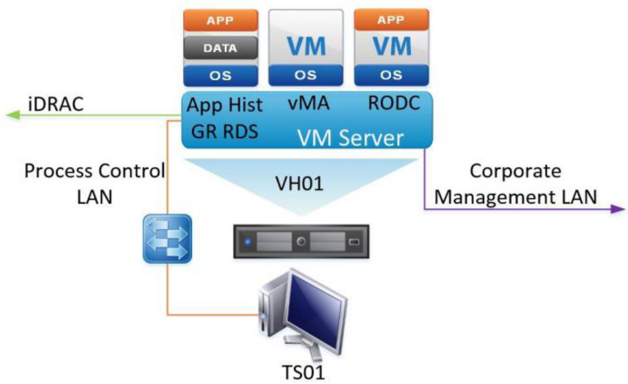

FIGURE 4. Small site architecture.

Figures 4-6 show an overview for each of the three site architectures available. The following acronyms are used within the figures and are listed below for ease of reference.

- VM = Virtual Machine
- OS = Operating System
- APP = Application Component
- DATA = Historian Component
- vMA = Virtual Management Agent (Linux)
- iDRAC = Integrated Dell Remote Access
- GR or GRNode = Galaxy Repository (Wonderware ArchestrA central configuration area)
- TS = Terminal Server
- LAN = Local Area Network
- RDS = Remote Desktop Session
- VH = Virtual Host
- RODC = Read Only Domain Controller

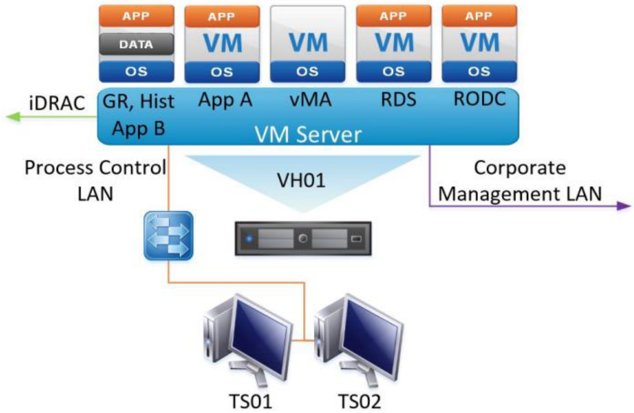

FIGURE 5. Medium site architecture.

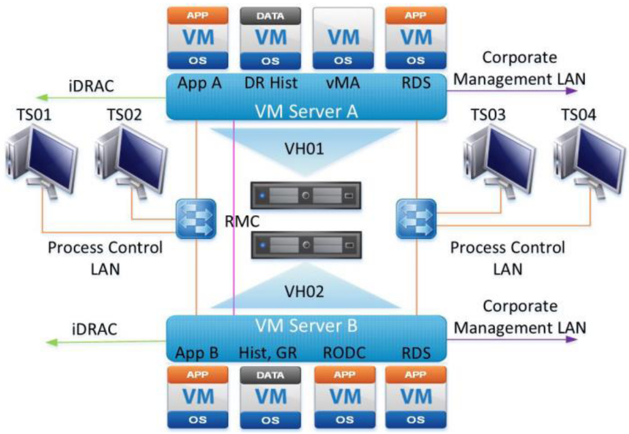

FIGURE 6. Large site architecture.

B. SCADA APPLICATION ARCHITECTURE

Within the new SCADA's development environment, there are application objects. These objects are domain specific [14] and are used to represent field equipment such as flowmeters, valves and pumps. Additional integration objects are used for communicating with the sites OPC servers and providing accessible data points to the application objects. The software used for this project comprises an add-on to Microsoft's Visual Studio that enabled the utilities software developers to create custom application objects in C#, providing a framework to create business specific templates.

C. SYSTEM UPDATES AND PATCHING

The asynchronous and/or sporadic nature of system patches, including Windows updates and antivirus upgrades provide system owners with critical real-time constraints [15]. Automated application of these updates is often difficult and can present unacceptable risks and delays to production processes, and networks. To help address this, the utility controls all Windows updates via the Windows Server Update Services (WSUS), patch management software tool. This provides a systematic, accountable, and documented system for managing exposure to vulnerabilities through the timely deployment of patches.by automating the process of acquiring, testing, and applying the patches [16] to the system servers around the estate.

IV. STANDARDISATION

As part of the SCADA delivery strategy, a standardisation model was developed and employed. The approach was to take elements of different SCADA system naming and graphical visualisations, combining them to find a common approach to apply to all systems. As previously discussed, the existing SCADA estate had been left to organically mature, with a supply chain of multiple systems integration experts, all whom of which brought their own best practices to their specific system installations. This led to differences across the site systems.

A. GRAPHICS

A typical SCADA screen presents dynamic graphics in a way that represents the sites process piping and instrumentation diagram (P&ID). The basic building blocks consist of pumps, valves, analogue and digital instrument displays. However, within clean and waste water systems, there are also some non-standard devices that require visualisation. These can include, but are not limited to, screens, aerators, grit removal, chemical dosing, filtration systems and dewatering equipment.

Generally, process operators are required to cover multiple sites and sometimes regions. The more experienced can also be expected to transfer between disciplines, (i.e. cover both clean and waste applications), although they generally work from a base location. The base location is the site they are primarily responsible for and most accustom to. If an operator from one part of the utility was familiar with his/her SCADA's operating system principles, then it may become confusing to have to use another SCADA application that doesn't follow the same operating principles. This introduces risk and could potentially lead to error. This would certainly require further training and impact the businesses operational expenditure (OPEX) budget. When considering the amount of operators and the amount of legacy system variances, this soon equates to large costs.

1) DYNAMIC GRAPHICS

Dynamic graphics comprise any asset based graphical object that changes state based on site conditions. For example, a pump that is failed in the field may have a red flashing box around it. Or the same pump may change colour when the filed device is running. An example of how existing dynamic graphical devices may differ across the legacy SCADA estate is shown in Figure 7.

From inspection of the varying pump graphics in figure 7, it appears most are similar in overall appearance. The issues manifest with the introduction of a perceived impeller in the middle of the pump housing. To an operator who knows the site, this isn't an issue, however, this 'star graphic' inside the casing may be how another site represents an air blower or fan.

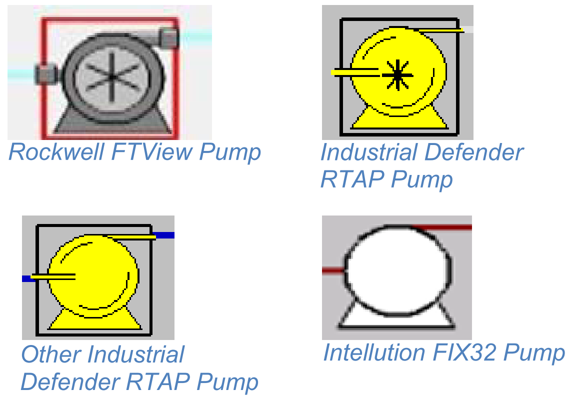

FIGURE 7. Different legacy pump graphics.

In a more extreme case, the overall graphical design of a sludge screenings system presents complete ambiguity between two variants. Figure 8 shows how one site uses a circular device to represent a surplus activated sludge (SAS) screening system, with another sludge screen using what appears as an electric motor graphic. In both cases, the physical plant on site utilises similar techniques for sludge screening and therefore, should also comprise visual commonality when displayed on SCADA, in order for operators to easily identify plant when covering multiple sites.

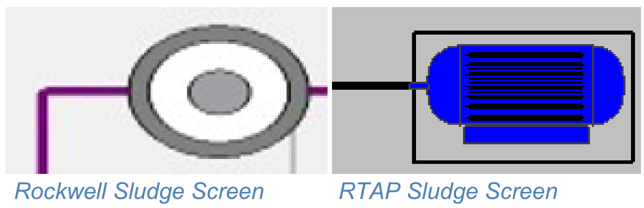

FIGURE 8. Interpretations of screening plant graphics.

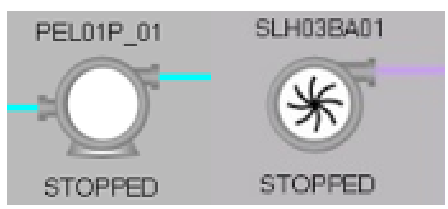

FIGURE 9. New graphic library pump and blower.

The delivery of a standardised graphical library ensures consistency is met across all sites. The new library delivered contains multiple graphic templates, capturing all standard water treatment process. Figure 9 below defines a pump and blower graphic.

2) PROCESS COLOURS

As well as standard graphics for a templated design, the standardisation also defines the coloration for each process area

TABLE 1. Process colour standards.

Process Area	Colour	Colour	R	G	B
Air/Oxygen		Lavender	204	153	255
Digesting sludge		Brown	153	51	0
Ozone		Pink	255	0	255
RAS / SAS		Violet	128	0	128
Sludge screenings		Lime	153	204	0
Storm water		Green	0	128	0
Polyelectrolyte		Turquoise	0	255	255
11Kv		Signal Red	187	64	57
6.6Kv		Blue	0	0	255
3.3Kv		Dark Violet	109	79	115
2.2Kv		Magenta	102	0	51
< 1Kv		Black	0	0	0

when applied to the visualisation of process lines on a monitor screen. These are defined within the utilities internal standards and are detailed, along with their RGB colour space coordinates. For the purpose of this paper, not all coordinates will be presented, however, table 1 below shows some of the most common colours used.

B. OBJECT BUILDING BLOCKS

Within the industry there are multiple iterations of the same device, whether this is a pump, valve, level instrument, per site, per catchment or estate wide. Frameworks exist to ensure replacement assets can be procured quickly and cost effectively, with minimal resource effort required for swap-over. This approach was also a key driver in the development of SCADA asset database devices.

The Wonderware System Platform package used in the delivery of this project utilises a developer interface called ArchestrA Object Toolkit (AOT). AOT is a Microsoft Visual Studio add-on and allows developers to create their own application specific object templates in the C# language.

The project team created a set of 6 high level application object templates, that were designed to cover most of all the available plant items across the waste and clean water estate. These were:

- $STR – Starter Device. Pumps, motors, conveyors, screens etc.
- $POS – Positioner. Folomatic valves, Penstocks etc.
- $AI – Analogue Instrument. Any device that provides a variable feedback. Level, pressure, flow, temperature etc.
- $DI – Digital Instrument. A single instrument such as a level or pressure switch with a Boolean output.
- $Ctrl – Blank canvas. This was created to allow SCADA engineers to create bespoke control objects that otherwise would not be configurable via any of the above templates.
- $UI - Blank canvas. This was created to allow SCADA engineers to create bespoke user interfaces, as long as there was no associated control.

$AI and $DI were for singular devices and not associated with larger plant items. I.e. a pumps integral pressure device would be integrated within the $STR device. A penstock torque over-pressure signal would be an extension attribute within a $POS object.

Developers who use the AOT can create complex custom Application Objects that represent specific types of equipment. They support various events that allow the execution of custom config time and run time code.

Once a template is available, multiple iterations can be created. These iterations are known as instances. An instance inherits all config and runtime code from its parent template, which allowed for the quick creation of multiple assets. An example could be a site that comprises 20 rapid gravity filters (RGF's). Once the specific template of an RGF drain down pump has been created, from the $STR high level template, then the 20 instances can be created. They are all exact copies and all inherit then same configurable attributes. Therefore, the engineer only needs to point the instance to the relevant device integration object tag (such as an OPC data point) and the object is complete. Any change to the template propagates through to all instances, which eliminates the need for individual updates.

C. DATABASE STRUCTURES

1) EXISTING SYSTEM CONSTRAINTS

Legacy system databases contain all configuration data; I/O integration, point scaling, alarms, trend information and associated identification tags. A mixture of old standards, non-compliance with standards and limited governance mechanisms has led to a multitude of different interpretations in how to formally identify application objects and their attributes. This nonstandard approach has meant that analysists who receive critical data via tier 2 historians, and require it for driving efficiencies within the sustainability sectors, have a near impossible data mining task when it comes to cross site analysis.

For example, a raw water valve that throttles flow between a reservoir and a receiving treatment plant may be tagged as follows at one site; RWT1VLV1, with another site comprising the same type of valve and being tagged as RW1MV1. Where local site knowledge permits an understanding of what each tag relates to; when these are presented to a wider audience via a remote tier 2 historian, (which in the case of the water company is the telemetry SCADA database, as shown in figure 3), there is ambiguity between the tag codes. This will ultimately require further investigation, at an increased resource cost, to be able to satisfy the data modellers that they have identified the correct signal and asset.

It is worth highlighting that when data is presented via tier 2 data historians and used for analysis purposes, the people inspecting the data do not have the 'visual aide' in the form of the SCADA process screens. It is presented in standard database format. The other constraint with ungoverned tagging and string lengths is that autonomous inspection rules that utilise specific string lengths for identifying common components within a tag cannot be applied. By taking the previous example of the two raw water valves above; if the local asset tag is prefixed with a site functional location code (FLOC) and a simple inspection rule was required to determine the raw water valves process group and ID, this would not be a simple autonomous rule;

- TEST1SITE_RWT1VLV1
- TEST2SITE_RW1MV1

The strings above represent the two raw water valves at two separate clean water sites. They both provide the same physical interaction with their site process. The colour codes are detailed as follows.

- Functional Location Code – Unique Site Identifier
- Process Code- in this example – Raw Water
- Process numeric code
- Plant code – In this example - Valves
- Plant numeric code

If a database contained multiple valves from varying sites and analysis required the raw water valves in process 1, then for test site 1 above, the excel command =MID('Cell-Ref',14,1) could be used to extract this. However, for test site 2, in order to extract the same component, the following command would be required; =MID('Cell-Ref',13,1). This therefore eliminates the ease of use of a template set of autonomous extraction tools for data manipulation and leads to increased resource effort when trying to interrogate the big data repositories and silos.

2) NEW APPROACH

Within the delivery of a modular standardised SCADA platform, the approach to employ a tagging standard used process, plant and signal codes. It was used to provide statements of ownership of these, and rules for constructing formal identifiers. These new codes have been used for identification of operational processes and plant, signals and associated data. The identification scheme given here for process plant allows visibility of; 1) the area/site, 2) the main process and number, 3) the plant/instrument and number, 4) the signal [17].

All plant that was subject to the SCADA redesign within this research project was assigned a process related unique identifier. These identifiers are assembled to comprise the following attributes; FLOC, process, and plant/instrument codes. To save on SCADA screen real estate, the FLOC codes were omitted for the use within the on screen displays, however, in some rare cases where ambiguity resulted, these were reintroduced. For example, where two sites share a single reservoir or borehole. The FLOC code is utilised throughout the business to identify assets associated with individual sites and is intended to line up with other corporate systems, such as SAP^{TM} business objects.

The utilities SCADA data standards were published and used by the project, which set out mandatory tagging structures and process/plant codes. The following structures were used.

Plant items associated with main process units shall be given identifiers as follows:

- LLLLLLLL_PPPBBCCDD

With LLLLLLLL comprising an 8-character FLOC code, PPP being a 3 character process code, BB is a 2 character process numeric code, CC is the 2 character plant code and DD is a 2 character plant numeric code.

By considering the previous raw water valve tagging issue, the new standardised approach would now see the two valves tagged as follows.

- TSTSITE1_RWT01MV01
- TSTSITE2_RWT01MV01

The components that construct the full tag now align across the SCADA estate and therefore inspection rules for data comparison can be employed.

D. SUMMARY

By following the standardisation procedures detailed in this section, it has allowed the project to deliver a common information platform when visualising process control systems. From the two assets in figure 9, any site SCADA operator, regardless of site, would now be able to immediately know what the devices are from the dynamic graphic, the process colour and the asset tag.

- PEL01P_01 = Polyelectrolyte Stream 1, Pump 1
- SLH03BA01 = Sludge Holding Tank, Stream 3, Air Blower 1

This would be applicable at any site across the estate, and is common all the way through the data's lifecycle, from site, the high level historians and analytics packages.

V. HUMAN FACTORS

When the new SCADA systems became the primary control systems onsite, users had to familiarise themselves with new functionality. The mimics follow site process and replacement ones were presented in a similar style to the old system, these were accepted by operational teams without issue. The trending package however, was presented with a different user interface and received comments on the usability. Following this, targeted training was arranged to familiarise operators with the enhanced functionality.

A. DOMAIN AUTHENTICATION

The new site systems utilise the Microsoft Server Active Directory architecture, which allows for a centrally located domain controller (DC), with individual sites having a standby Read Only Domain Controller (RODC). The RODC will become the primary should the corporate offsite communication link be lost, thereby continuing to provide user authentication on site.

Individual user authentication was introduced as part of the standardised SCADA strategy. It provides an enhanced level of system security, thus protecting the asset base and enabling event handling and traceability. Each user within the company has their own account, which can be used to access any centrally authenticated SCADA application to which they are permitted access.

At a strategy and systems security level, this was an approved way forward, however, at an operational level, it presented challenges. For a user to gain access to the SCADA runtime application, he/she would need to first log into the client workstation, which requires entering the domain credentials. Once in the client operating system, a remote desktop session is then required to be able to open a client to one of the terminal servers. Again, domain authentication is required and therefore, the entering of credentials. Once in the terminal server session, the application can be started. The time it takes to log on fully to the runtime application varies as a result of the operator's different computer literacy skills. However, with a proficient user, this will take approx. 1-2 minutes from start to finish, due to the operating system loading the user profile and the application. The old legacy SCADA systems did not utilise domain authentication. Users typically accessed the application using one of two accounts; 1) operator (default) and 2) engineer, where the operator account could navigate and change the process and the engineer account was for the systems team to maintain, add, modify functionality etc. The operating systems were always logged on to a default account and the SCADA application was permanently logged on to the operator account. What this meant previously; is that an operator could enter a control room, touch the mouse pointer, which exited the screen saver and the application was immediately available.

Stakeholder engagement was crucial in understanding user needs and led to a deeper knowledge of the main issues. The engagement with operations found that the change in approach was receiving user push back, as it was deemed to be an unacceptable increase in the time required to view the SCADA application. This was perceived as a probable risk under event conditions. Further to this, under domain policy, the users were set to be automatically logged off after a 15minute period of inactivity on the application. Considering the perceived risk and points raised in the introduction of this paper, regarding the varying degrees of reliance on a SCADA system across different sizes of site, and within the clean and waste communities, there was a clear understanding that domain policy required modification.

In order to alleviate the operational concern, the users were split within the active directory and a new policy was written for critical process systems. For a 24-hour, manned site that comprised a secure control room, a 12-hour account was created and qualified users assigned to it. It came with a 2 hour inactivity screen saver that required a single password entry to get back to the runtime application. This eliminated the need to login to the workstation client device and then on to the terminal server. All other sites were left as per the original design and extended training was offered to operators that required it.

B. TAGGING ACCEPTANCE

As part of the migration from old to new, the legacy system databases were extracted and analysed. The conversion dictated that old legacy asset tags would be aligned to the standardisation model as detailed in this paper, and in line with the utilities asset standards tag code dictionary. In some cases this introduced ambiguity in how an asset was labelled pre and post upgrade. As per the example, in the standardisation section of this paper, RWT1VLV1 became RWT01MV01. In some more extreme cases, a valve PV30 became MV06, which deviated from the 'as is' tag in the field. Mitigation steps were developed to reduce risk through ambiguity. All dynamic graphics had associated faceplates/popups, which, when called, provided information tabs, these provided the historical 'legacy' SCADA tag for inspection where required. A lookup utility was also provided that enabled users to enter a new asset tag, which would then show the equivalent legacy tag ID and any associated mimics where the device is presented.

Consultation with senior company health & safety engineers and operational production managers ruled against these steps as appropriate mitigation, as the risk ultimately concerned the introduction of the new tag structures as the primary identifier visible on the SCADA mimic back cloths. This decision was primarily formed based upon control room behaviours during event/crisis management. I.e. during an event that introduces a heightened sense of urgency for a shift controller, the need for the known asset tag to be available immediately, and not through mitigation measures, was a mandatory requirement.

This decision came at a cost to the project, however due to the object orientated programming structures, that included graphical hierarchies, only a minor change was required at the highest level, that modified a small script to point at the legacy tag metadata field, as opposed to the new asset tag. Database work was also required to prefix the legacy tag to all trend and alarm descriptions, ensuring consistency remained.

C. RESISTANCE TO CHANGE

A key component in acceptance of systems when delivering new operational technologies, is the individuals who will use them. A water company's estate will generally span multiple counties and could comprise large metropolitan cities at one end of the spectrum, with untouched rural areas at the other end. This wide spectrum introduces variance in user demographics, which in turn presents variance in an understanding and acceptance of the technology being delivered. A lot of this was due to the perceived ease of carrying out daily tasks using existing systems and that change contributes to making tasks harder. This inevitably leads to a lack of trust in what is new

From an organisational perspective, there is a strong correlation between the resistance to change and the implementation success [18]. This resistance has been witnessed at every level throughout the lifecycle of this project. It requires sensitive management, at an individual level in some cases, and should always be considered when planning wholesale change to user interactive technologies. Early engagement should always be sought, with the inclusion of the end user at the design stages. This has started to be employed in some more recent capital programmes, along with a move towards left shift.

D. BEHAVIOURAL STUDIES

SCADA control room performance is like any other area of a business. The behaviour within it is a function of its environment.

Within the construction industry, the use of behavioural techniques for improving safety is becoming more commonplace. It primarily focuses on the behaviours that lead to incidents and injuries, however, the author believes that further research in the analysis of behaviour related to technological changes in the workplace environment could lead to a better understanding of how integration could be delivered more effectively, and without such resistance to change.

VI. CONCLUSIONS

The standardisation of utility wide SCADA systems brings huge potential and value in aligning database structures. It provides a common information model that is scalable and transferable across all business areas. It also goes towards reducing analytical resource burdens when driving through business efficiencies in highly regulated industries.

When standardisation rules are applied correctly to 'greenfield' installations, they provide a solid platform for system development, including a sound governance model. A user will not have any comparison to make between an old operating system, and acceptance across all business stakeholders is more forthcoming. However, when migrating an old system that has been in place for decades, then applying a new standardisation model to the output will, in certain cases, change the core functionality of the product an end user is accustom to. As a result, this may require a paradigm shift in operational behaviours, which must introduce additional thinking in the planning phase of a project. Training in the product, pre-delivery should also be considered.

With a deeper understanding of operational control room behaviours, this research would recommend that human factors are studied in depth prior to any major operational technology change.

REFERENCES

[1] M. H. Zack, "Managing codified knowledge,," *Sloan Manage. Rev.*, vol. 40, no. 4, pp. 45–58, 1999.
[2] P. Kulkarni and T. Farnham, "Smart city wireless connectivity considerations and cost analysis: Lessons learnt from smart water case studies," *IEEE Access*, vol. 4, pp. 660–672, 2016.
[3] D. M. Jones, *Digging Deeper: Big Data Dilemma*. accessed on Jan. 10, 2016. [Online]. Available: http://wwtonline.co.uk/features/big-data-dilemma#.VpJQiFk2W7I
[4] A. M. Grilo, "An integrated WSAN and SCADA system for monitoring a critical infrastructure," *IEEE Trans. Ind. Informat.*, vol. 10, no. 3, pp. 1755–1764, Aug. 2014.
[5] P. J. May and C. Koski, "Addressing public risks: Extreme events and critical infrastructures," *Rev. Policy Res.*, vol. 30, no. 2, pp. 139–159, 2013.
[6] C. H. See *et al.*, "A Zigbee based wireless sensor network for sewerage monitoring," in *Proc. Asia–Pacific Microw. Conf. (APMC)*, Dec. 2009, pp. 731–734.
[7] T. Water, *Annual Report and Financial Statements 2014/15*. 2015, pp. 23–26. [Online]. Available: https://corporate.thameswater.co.uk/About-us/Our-investors/-/media/BA8CF4ED58B84808983A570ABB4A980A.ashx?bc=White&db=web&la=en&thn=1&ts=0af872f5-9fb5-45fc-9b72-56296ae450f6.pdf
[8] P. Gaj, J. M. Jasperneite, and M. Felser, "Computer communication within industrial distributed environment—A survey," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 182–189, Feb. 2013.
[9] K. C. Lee, S. Lee, and M. H. Lee, "QoS-based remote control of networked control systems via Profibus token passing protocol," *IEEE Trans. Ind. Informat.*, vol. 1, no. 3, pp. 183–191, Aug. 2005.
[10] G. Shoshani and S. S. Mitschke Stephan, "Industrial Fieldbus technology and Fieldbus cable overview—Cable standards and electrical qualifications," in *Proc. 57th Annu. Petroleum Chem. Ind. Conf. Rec. Conf. Papers Ind. Appl. Soc. (PCIC)*, Sep. 2010, pp. 1–10.
[11] *GENESIS 32—Product Brief for GENESIS32 V9.4 November 2015*, Iconics, GENESIS 32, Iconics Inc, 2015.
[12] P. Gaj, M. Skrzewski, J. Stój, and J. Flak, "Virtualization as a way to distribute pc-based functionalities," *IEEE Trans Ind. Informat.*, vol. 11, no. 3, pp. 763–770, Jun. 2015.
[13] *Veeam Backup Enterprise Manager Version 9.0 User Guide February, 2016*, in User Guide, Veeam Software, 2016, pp. 38–39.
[14] Invensys Wonderware, *ArchestrA Object Toolkit Developer's Guide*, Wonderware, 2009. [Online]. Available: http://platforma.astor.com.pl/files/getfile/id/6820
[15] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 277–293, Feb. 2013.
[16] M. A. Badawy and N. A. O. El-Fishawy Elshakankiry, "Using patch management tools to enhance the signature customization for IDS based on vulnerability scanner," in *Proc. 11th Int. Conf. Inf. Technol., New Generat. (ITNG)*, Apr. 2014, pp. 529–533.
[17] *Instrumentation & Process Plant Identification Specification*, Standard AM-DES-SCADA-F24 Section 05, 2014.
[18] O. Nov and C. Ye, "Personality and technology acceptance: Personal innovativeness in IT, openness and resistance to change," in *Proc. 41st Annu. Hawaii Int. Conf. Syst. Sci.*, Jan. 2008, p. 448.

ALEX D. L. GRAY received the B.Eng. degree in power engineering from the University of West London in 2013. He is currently pursuing the Ph.D. degree with Brunel University London, sponsored by Thames Water Limited, which is focused on optimising sewer networks for improved energy utilisation, by applying improved automation to satellite pumping systems. He is currently a Chartered Engineer with the Institution of Engineering and Technology. Whilst studying part-time, he was a Consultant within the water industry and specialises in the delivery and commissioning of control and instrumentation and software systems.

IOANA PISICA received the M.Sc. degree in information systems from the Academy of Economic Studies, Bucharest, and the Ph.D. degree in intelligent energy networks from the University Politehnica of Bucharest. She is currently a Lecturer of Power Systems with the Department of Electronic and Computer Engineering, Brunel University London. Her research interests include modern optimization techniques for energy systems, machine learning for power systems control, power quality, smart metering, and ICT infrastructures for future power networks and energy efficiency.

GARETH A. TAYLOR received the B.Sc. degree from the University of London, London, U.K., in 1987, and the M.Sc. and Ph.D. degrees from the University of Greenwich, London, in 1992 and 1997, respectively. He was the National Grid U.K. Post-Doctoral Scholar with Brunel University London, Uxbridge, U.K., from 2000 to 2003, where he is currently a Professor and the Director of the Brunel Institute of Power Systems. His current research interests include transmission system operation, smart grids, and power system modeling and analysis.

LOUISA WHITEHURST received the M.Eng. degree in civil engineering from the University of Exeter in 2012. She has been involved in the control and instrumentation sector of the water industry since 2013. She has authored several internal technical governance documents that focus on virtualised SCADA platforms. She has also contributed towards internal governing standards. She is a member of the Institution of Engineering and Technology.