Electrical Control Systems – Process control interface design

Paper No. EUR21_13

Alex Waslin CEng, MSc, BEng, MIET
BP Exploration Operating Company Ltd
Chertsey Road, Sunbury on Thames, TW16 7BP
UK

Dibyendu Bhattacharya CEng, FIET
BP Exploration Operating Company Ltd
Chertsey Road, Sunbury on Thames, TW16 7BP
UK

Michael Wilson BSc, MIET
Powell Industries
Ripley Road
Bradford BD4 7EH
UK

Abstract - Adoption of integrated Electrical Supervisory Control and Data Acquisition systems for the operation, control and monitoring of electrical distribution equipment has presented challenges across a global portfolio of projects and operating assets.
The former transition from discrete hardwired to serial interfaces mainly suffered due to interface latency attributed to the hardware and software limitations. The subsequent natural progression to serial interfaces over Internet Protocol network communications has to some degree mitigated the early latency issues. However, this paper outlines the investigations findings as a result of multiple major projects and operating assets, in a global portfolio, suffering process control interface issues, where the majority of those issues impacted the project start-up and early operation. The investigation team established several lines of enquiry encompassing the system interface designs, technology limitations, contractual framework with equipment suppliers and personnel competence.
The work concluded in the development of a technical specification and associated proof of concept testing recommendations of less utilised protocols for process control interfaces.

Index Terms — Electrical equipment instrumentation, On-line Monitoring & Condition, Substation automation and Control. Process Control interfaces. Integrated Control Safety System ICSS, Intelligent Electronic Device IED. Power Management System PMS, Electrical Control System ECS, Electrical Maintenance Network EMN, Electrical Data Monitoring and Control System EDMCS, Modbus, Profibus, IEC 61850, PRP, HSR.

I. Introduction

Contemporary Electrical Control Systems (ECS) have evolved since the advent of microprocessor based electrical protection relays, known as Intelligent Electronic Devices (IEDs), resulting in the ECSs replacing the conventional hardwired control interfaces with electrical equipment such as Switchboards (SWBD) and Motor Control Centres (MCC).

Many features and value adding concepts have been built upon the ECS foundation, enabling remote operation, diagnostics and device parametrisation etc.

Despite the value adding features, ECS's have been tarnished over several system generations due to the performance and reliability of the interface(s) to the Integrated Control and Safety System (ICSS) / Supervisory Control and Data Acquisition (SCADA). The first generation of interfaces mainly utilised two wire serial interfaces directly to local serial to discrete Input/Output (I/O) modules. These interfaces were plagued by latency and bandwidth constraints.

The advent of IED technology installed within each SWBD and MCC outgoing circuit, initially provided a number of benefits, and with the subsequent generations of the technology, communications enabled remote operation, diagnostics and device setting parametrisation. As a result of the network capabilities, process control of electrical equipment evolved to utilise Internet Protocol (IP) networks, which resolved several of the two wire serial interface constraints, however introduced numerous reliability and availability issues which plagued the systems during commissioning, start-up and operations. The situations were greatly exacerbated due to gaps in operations personnel's ability, experience and competence to fault find such systems.
This paper (1) summarises the generic conventional approach to ECS system interfaces for process control for major energy industry assets; (2) summarises subsequent overarching investigation findings as a result of multiple major projects and operating assets suffering process control interface reliability issues, where the majority of the issues impacted the project start-up critical path.
Finally, the paper focuses on a key learning identified during the investigation of the lack of system technology experience and fundamental knowledge, resulting in the development of a bespoke training course for engineer and technicians.

II. Conventional Approach

A. Recent Challenges

Multiple major projects in regions shown in **Erreur ! Source du renvoi introuvable.** have experienced certain availability and performance issues during commissioning and early operation of the process control and monitoring interfaces between the ICSS and electrical systems via the ECS.

Figure 1 outline of asset locations experienced availability and performance issues

The results of a global survey found that almost all the projects surveyed had faced interface issues in one form or other independent of the system Original Equipment Manufacturer (OEM) / system integrator ICSS / ECS combination. All system designs were bespoke for each project, moreover even when the same combination of electrical and ICSS supplier were used on two projects, the engineering design of the interface were very different.
Despite each bespoke project implementation, the overall concept of the interfaces were based on some common principles:

- Communication interface between ICSS and electrical systems;
- Communication bus linking IEDs on the electrical network;
- Data concentrator / protocol convertor used in the interface between ICSS and IED data.

In spite of this, each project developed a different technical solution in terms of the communication protocols used, the detailed physical and logical architecture, along with the hardware specification. These differences attributed to the uncertainty and irregularities observed through the systems sub-optimal performance and unreliability. Specific events include multiple communication losses during the switchover process of the dual redundant interface leading to equipment trips. A reason identified for this is the limited capability of the interface to handle multiple communication sessions concurrently. The second was associated with inadequate firmware Management of Change (MOC) for the key elements of the interface such as firewalls, network switches, interface cards, etc. leading to incompatibility issues post Factory Acceptance Testing (FAT). A further observed behavior was due to the interface becoming unresponsive as a result of unexpected and unassociated high network traffic.

Interface	**Purpose includes** (not limited to)	**Default Protocol / Interface**	**Optional Protocol / Interface**
ECS to ICSS^{M}	Process control and monitoring	Modbus TCP/IP	Hardwired [2, 6] EtherNet IP[1] IEC 61850[1]
ECS^{M} to SWBD (HV/LV distribution)	Control and monitoring	Suppliers standard	Modbus TCP/IP [3] ProfiNet IEC 61850 Hardwired [2, 6]
ECS^{M} to LV MCC/feeders	Control and monitoring	Suppliers standard	Modbus RTU (LV MCC) [3] Profibus Modbus TCP/IP [1] IEC 61850 Hardwired [6]
PMS^{M} (non 3rd party) to SWBD	Sync CB control, FLS, monitoring	Suppliers standard	IEC 61850 Hardwired [2] Modbus TCP/IP [4] ProfiNet [4]
PMS^{M} (3rd party) to SWBD	Sync CB control, FLS, monitoring	Hardwired	IEC 61850 Modbus TCP/IP [4] ProfiNet [4]
PMS^{M} to gen UCP	Control and monitoring	Hardwired	N/A
PMS to ECS^{M}	Monitoring	Suppliers standard	Modbus TCP/IP ProfiNet EtherNet IP [1] IEC 61850 [1]
SWBD to SWBD [7]	Inter-locking, inter-tripping, auto transfer schemes	IEC 61850	Hardwired [2]
ECS^{M} to non-SWBD IEDs. e.g. UPS/DB/Transformer	Control and monitoring	Suppliers standard	Modbus TCP/IP [3] ProfiNet Hardwired [2]
ECS^{M} to SWBD integrated VSD	Control and monitoring	Suppliers standard	IEC 61850 Modbus TCP/IP [3, 5] ProfiNet

B. Investigation

The subsequent in-depth investigation identified a number of root and system causes, these are summarised below:

- Lack of SPA (single point accountability) for the interface management;
- Products / engineering standards have not necessarily kept pace e.g. IEC 61850 is not standard for LV switchgear;
- Engineering capability has not kept pace e.g. electrical engineers / technicians do not traditionally have detailed network / data comms skills;
- Project specification of the interface has tended to lack enough detail;
- Vendors do not yet have mature, standard designs as seen in the variations from project and regions;
- Highly variable levels of off-critical path testing across different projects – often severely compromised due to multiple companies involved, remote locations from design centres, travel constraints and construction schedule pressure etc.;
- Vendor device compatibility even when using the same protocol.

Following the identification of the causes above, the team developed mitigation in response which is outlined within the following section.

C. Intervention

Each of the projects that experienced undesired behavior during commissioning, start-up and early operations, along with those with minimal issues were investigated in an effort to deeply understand the root causes and learnings.
The process depicted in Figure 2 was utilised to develop mitigation for each of the identified root causes.

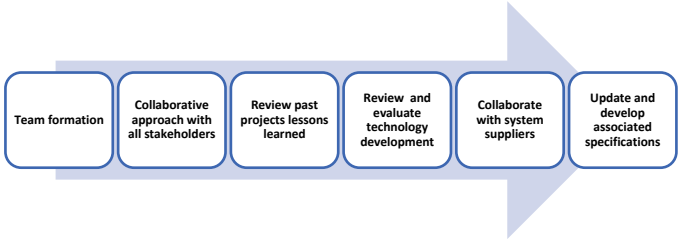

Figure 2 *Process for root cause development*

Ultimately the work concluded in the development of a procurement specification and application requirements, incorporating the mitigation including associated proof of concept testing of less utilised protocols for process control interfaces (see
). The following section summarises the key

enhancements to the approach resulting from the mitigations developed.

III. ENHANCED APPROACH

A. Data Concentrator (DC)

Due to multiple methods of serial communication and protocols in use within an ECS, protocol conversion is often required when interfacing to another system (such as an ICSS for process control). Furthermore, a level of intelligence / signal manipulation is required to manage response to such events as a communication failure.

DCs can provide the required protocol translation, and I/O mapping, along with the required intelligence to manage communications failures and signal consolidation. Other advantages include, the level of abstraction between the controlled device (IED) and the controller (ICSS) so that modifications e.g. an address change, within the electrical equipment does not commonly extend out over the interface, minimising the impact of change.

DCs are generally available in two forms, the first is an industrial Programmable logic controller (PLC) / process controller, with the required optional communications cards. The second is an industrial Personal Computer (PC) / server form, often with a non-Real time operating system (RTOS) such as Unix® or Microsoft® Windows®. As the availability and data integrity of a DC is critical for process control reliability, the selection of both hardware and operating systems is an important factor.

B. OPERATING SYSTEMS

The reliability of devices located in the critical path of process control signals and data are crucial to the reliability of the interface and ultimately the overall system performance. As a result, the performance of any Operating System(s) of a device located in the critical path is fundamental to system reliability.

Most operating systems appear to allow multiple programs to execute at the same time, commonly referred to as multi-tasking. In reality, each processor core can only service a single thread of a program at any given point in time. An operating system will include a scheduler, which is responsible for deciding which program to service when, this provides the illusion of simultaneous execution by rapidly switching between each program.

The type of operating system is defined by how the scheduler decides which program to run when. For example, a multiuser operating system (such as Unix®) uses a scheduler that will ensure each user gets a fair amount of the processing time.

The scheduler in an RTOS is designed to provide a predictable execution pattern, normally described as deterministic. This is particularly of interest in embedded systems as such systems often have real time requirements. A real time requirement is one that specifies that the system must respond to a certain event or events within a defined time. Real time requirement execution can only be guaranteed if the behaviour of the operating system's scheduler can be predicted and is therefore deterministic.

An RTOS uses maximum time and resources to output exact and on time results, there is no difference (beyond jitter) between the results (both outcome and time to execute) when the same program is executed, on different occasions, on same machine/hardware.

Advantages

- Maximum Utilisation: RTOS provide maximum utilisation of the system, giving a greater performance using all the resources of a system;
- RTOS in embedded system: Due to small size of programs, RTOS can also be used in embedded/application specific environments;
- Task Shifting: There is very little time required by these systems to shift between tasks;
- Priority-based scheduling: The separation of non-critical and critical processing;
- Focus on Application: An RTOS focuses on the current application, which is running, rather than other applications waiting for execution. Typically, an RTOS will only be required to run a single application at any one time;
- Easier testing: An RTOS allows for testing of modular tasks, therefore making testing easier.

C. PROTOCOLS

The choice of protocol to be used to facilitate the separate functions of the system at first glance would suggest the same protocol to be used in all instances, but this does not take into account the requirements for functionality, performance, support and cost. Each protocol lends itself to an area of the system giving the best balance of the requirements:

- IEC 61850 GOOSE is used for data/control with a high performance demand;
- IEC 61850 MMS is used for data/control generally related to device data and is recorded as timestamped at source;
- Modbus TCP/IP is commonly used for ICSS interfaces as data is generally high volume with a medium demand on performance. Standard use of protocol does not carry source timestamp;
- Modbus RTU is utilised by the Process RTU for data/control such as IED. It is low cost but maintains the data volume and performance requirements of the system. Standard use of protocol does not carry source timestamp.

Figure 3 below shows the interfaces and protocols utilised by a generic ECS / ICSS interface.

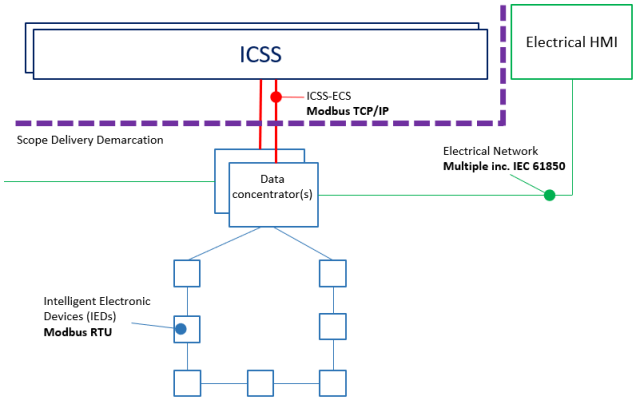

Figure 3 Representation of a generic ECS to ICSS interface including the Electrical network and HMI

D. INTERFACE SPECIFICATION

The importance of the hardware components and associated operating system's along with a deep understanding of the interface and protocol implementation is critical for success, whether it is for simple Power Management System's (PMS) status monitoring or an operational critical process control interface with the ICSS. Historically, ECS procurement specifications regularly failed to fully address the interfaces and specifically failed to appreciate that many and multiple protocols required, along with their limitations. This has resulted in poorly designed systems due to misunderstanding and "blind compliance" by the suppliers.

Following both internal and industry supplier's / OEM consultation,

was developed to detail the specific interfaces, their purpose and preferred protocol for the application. The table also includes options for smaller scale projects, prevision for technology development and the recommended communication 'master' device (see table notes below).

Interface	**Purpose includes** (not limited to)	**Default Protocol / Interface**	**Optional Protocol / Interface**
ECS to ICSS[M]	Process control and monitoring	Modbus TCP/IP	Hardwired [2, 6] EtherNet IP[1] IEC 61850[1]
ECS[M] to SWBD (HV/LV distribution)	Control and monitoring	Suppliers standard	Modbus TCP/IP [3] ProfiNet IEC 61850 Hardwired [2, 6]
ECS[M] to LV MCC/feeders	Control and monitoring	Suppliers standard	Modbus RTU (LV MCC) [3] Profibus Modbus TCP/IP [1] IEC 61850 Hardwired [6]
PMS[M] (non 3rd party) to SWBD	Sync CB control, FLS, monitoring	Suppliers standard	IEC 61850 Hardwired [2] Modbus TCP/IP [4] ProfiNet [4]
PMS[M] (3rd party) to SWBD	Sync CB control, FLS, monitoring	Hardwired	IEC 61850 Modbus TCP/IP [4] ProfiNet [4]
PMS[M] to gen UCP	Control and monitoring	Hardwired	N/A
PMS to ECS[M]	Monitoring	Suppliers standard	Modbus TCP/IP ProfiNet EtherNet IP [1] IEC 61850 [1]
SWBD to SWBD [7]	Inter-locking, inter-tripping, auto transfer schemes	IEC 61850	Hardwired [2]
ECS[M] to non-SWBD IEDs. e.g. UPS/DB/Transformer	Control and monitoring	Suppliers standard	Modbus TCP/IP [3] ProfiNet Hardwired [2]
ECS[M] to SWBD integrated VSD	Control and monitoring	Suppliers standard	IEC 61850 Modbus TCP/IP [3, 5] ProfiNet

Table 1 ECS interface purpose and recommended protocols at interface level.

Table 1 Notes:
[1] Dependant on technology readiness.
[2] Hardwired to be considered for a small-scale process control interface (circa 10 loads or if the I/O is considered critical, such as Fire & Gas related control).
[3] Use of this protocol limits visibility Sequence of Events (SOE) time stamping at source (IED) and therefore require a further protocol in parallel to extract the source SOE to the ECS.
[4] For monitoring only.
[5] Critical hardwired signals directly to ICSS as defined. e.g., tripped on fault, analogue setpoint.
[6] Emergency/Process Shutdown (ESD/PSD) executive action signals are hardwired directly from the ICSS to the electrical equipment.
[7] For information only, to be defined on the SWBD data sheet.
[M] Communications Master device.

E. NETWORKS

The choice of network architecture to be used in an ECS and interfaces is largely dictated by the requirement for reliable and low-latency communications between system components. Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) Protocol are suited for applications that require high availability and short switchover time, the recovery time of commonly used protocols such as the Rapid Spanning Tree Protocol (RSTP) is too long, which would result in a negative impact on the operation of the system.

Most Industrial Ethernet protocols in the IEC 61784 suite can be used with PRP and HSR, as they are independent of the application-protocol. They are network protocols for Ethernet that provides seamless failover against failure of any network component. Both utilise nodes with two network ports, but differ in that HSR utilises the ports as a network bridge which allows arranging them into a ring or meshed structure without dedicated switches, PRP utilises the ports independently and are attached to two separated networks of similar topology. HSR requires specific hardware, PRP can be implemented entirely in software, i.e. integrated in the network driver. Nodes with single attachment (network port) can be used in a HSR topology but only when connected to a dedicated switch, whereas in a PRP network, Redbox devices may be used to maintain the topology.

With either choice it is desirable that all equipment to be connected to the network has the appropriate protocol support to ensure predictable and correct system behaviour. Ideally there should be no single attached nodes to avoid single points of failure, reduce topology complexity, remove the need for extra 'steps' (protocol converters (e.g. Redbox devices)) which will result in increased latency in a network path.

F. INTERFACE PERFORMANCE

As with the protocol specification inadequacies outlined in the previous section, a deep understanding of the overall interface performance (i.e. latency of the communication),

is required. The specification requirements should clearly articulate the overall path of communication, including the components located in the critical path and highlight any specific items such as control commands that should be given priority by the ECS and interrupt lower priority status communications. Along with any non-deterministic components / processes such as a Human Machine Interface (HMI) refresh rate.
An example of the interface performance requirement in its simplest form may be:

- The time from receipt of an ICSS command to verification feedback to the ICSS that the IED has actioned the command shall be no longer than 6 seconds overall 'loop time'.

However, as depicted in Figure 4, further detail is required to clearly define the overall performance requirements for each side of the interface boundary, including;

- The performance requirement shall not be affected by a fully configured ECS system with the specified maximum number of IEDs or high ECS loading e.g. network traffic;
- The performance requirement is exclusive of motor start-up time and "running" status feedback signal being established within the IED.

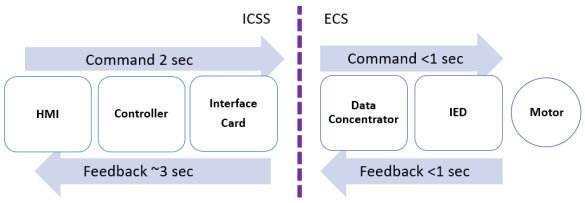

Figure 4 Generic interface performance for key components (excluding IED status update duration)

G. SYSTEM TESTING

There are two main strategies for software testing: 'Positive' and 'Negative' testing. With consideration these strategies can be expanded to validate the operation of multiple 'components' which when combined form the overall ECS.

1) Positive Testing: determines that an ECS works as expected, performing all the prescribed functions, generating the desired outcomes as defined in the project documentation.
2) Negative Testing: ensures that an ECS can gracefully handle invalid input or unexpected behaviour of system components or users. The purpose of negative testing is to detect situations that are outside the specified operation of the ECS and prevent an ECS from crashing or performing/functioning in an undesirable manner. Negative testing also helps to improve the integrity of an ECS and find any weak points.
3) The core difference between positive and negative testing is that generating an exception is not an unexpected event in the latter. When performing negative testing, exceptions are expected – they indicate that the ECS handles improper system component/user behaviour correctly.
4) Negative testing is aimed at detecting possible incorrect operation in the ECS in different situations. These can include:
   - Equipment failure;
   - Incorrect user operation;
   - Network overload;
   - Data bounds and limits.
5) The complexity of negative testing of a ECS is in the scale of the interactions of each of the systems sub-components and the potential cascade effect of seemingly unrelated functions of the system. A positive testing procedure is relatively simple to generate as it will largely be dictated by the functional requirements of a system. In contrast negative testing is very much a product of the design and implementation of a system, it requires a deep understanding of the infrastructure, component relationships and often complex interactions to ensure complete coverage of the operations boundaries.

The balance of minimising test scope on the project critical path with validating system performance is key to successful delivery. As a result of consultation with project discipline engineers, suppliers and system OEM's,
the interface testing is recommended to be broken down into three stages. The testing should encompass a representative sample of the hardware, architecture, and interfaces of the overall project scope at key milestones during the schedule.

H. SYSTEM SUPPLIERS

System suppliers generally fall into two main categories, System Integrators and OEM single source providers. Each supplier brings its own potential risks which need to be carefully assessed against the goals of the project to ensure they are met. A major advantage of an OEM supplier is their tried and tested solution and known interoperability/compatibility of the components within their catalogue. They are also the owners of the components, as such will have ready access to internal support should it be required to assist in issue analysis and resolution; a Systems Integrator can be reliant on third parties for product support, which will require them to have a good relationship with, and strong Management of suppliers to ensure support is provided if required.
A key advantage of a Systems Integrator is their flexibility to meet a projects multi-aspect specification and produce bespoke solutions, utilising the best tools and components available, while an OEM will be largely restricted to their own products which may require compromises to be made in the final solution. The System Integrator will also have the advantage of experience and knowledge gained through the execution of previous projects, using alternative tools and components from multiple manufactures. The key comparisons are outlined within Table 2 and Table 3 below.

System Integrator	OEM System
The ability to produce an unbiased solution using "best of breed" components to satisfy the key client objectives, culminating in the most efficient and reliable solution architecture without compromise.	All components used can be from within the company's catalogue with known interoperability / compatibility.
Able to provide a cost-effective solution to the requirements by selecting components.	OEM Project team should be intimately familiar with each of the components utilised.

Projects generally executed from a single location with all parties familiar will all system components.	If issues are identified during the execution of the project (or when in service) an OEM supplier should not have to rely on a third party for a resolution.
Expertise within the project execution team to perform design and analysis of the complete system.	OEM may have the facilities, the roadmap and the control to develop, test and sell new technologies.
Independent lab component comparison of performance in simulated applications.	Knowledge of issues earlier due to exposure in other industries / markets of their own devices, early workarounds / firmware update.

Table 2 Supplier advantages

System Integrator	OEM System
Reliant on third parties for component issue resolution.	The system design may be compromised to allow the accommodation of OEM components.
System architecture may be unique or contain components that have not been used together previously.	Because of the relative size of OEM system suppliers and the segregation of business units within, a system may be engineered by multiple disparate groups with little knowledge of each other's components.
The system integrator is reliant on what the market has to offer and has little influence on product evolution and upgrade planning.	OEM suppliers may not have subject matter experts within the execution team.

Table 3 Supplier disadvantages

I. PMS

As identified by Mun and Combs [1] in their paper "Distributed Logic Load Shed System Via IEC 61850" distributing the load management decision making operations within a PMS throughout the system, and demanding a higher function of the IEDs in the process, allows for the utilisation of the performance advantages of IEC61850 GOOSE communication over hardwired alternatives. The utilisation of the IEDs in the load management, allows for direct and pre-emptive operations without reliance on the 'main' PMS processors further improving the system performance and availability.

J. CYBER SECURITY

Implementation of cyber security controls is critical in the effort to assure the security and reliability of automation and control systems that enable operations. The cyber security landscape is constantly changing, with new vulnerabilities, threats, and attack vectors identified daily. Therefore, cyber security barriers require maintenance and management throughout the operations life cycle, and barrier strength and risks require regular review to maintain a 'defence in depth' approach.

K. TRAINING

The electrical industry has naturally evolved in the direction of utilising IEDs and data networked solutions. However, practitioners and engineer's technical knowledge has not kept sufficient pace. Electrical engineers / technicians do not traditionally have Information Technology (IT) network / data communication skills, this is considered analogous to the advent of the electronic based control systems in 1970 / 80's, where a generation of instrument mechanics would have had to upskill or become left behind in knowledge to support the technology as it was introduced. The OEM / supplier specific system training offering commonly assumes a basic / fundamental understanding and without this a candidate would not see the full benefit of the training.

In response to this finding identified across numerous major projects and operations assists, the associated competences were identified and established into a training program for technicians and engineers. The program includes existing training / certification offering, such as 3rd party provider online video content, cyber security fundamentals. This is then followed by a suite of bespoke video content covering industry specific protocol implementations such as Network redundancy protocols, two wire serial communications, IEC 61850, Network Time Protocol.

On completion of the training above, the candidates then attend a virtual instructor led training offering learning objectives including, a detailed look at the specific application and lessons learned when implementing or operating an ECS and PMS.

Finally, the training outline above provides the candidate with the fundamental knowledge to attend the OEM / Supplier training offering for their specific system.

NOMENCLATURE

EtherNet IP	Industrial network protocol that adapts the Common Industrial Protocol (CIP) to standard Ethernet
GOOSE:	IEC 61850 - Generic Object-Oriented Substation Event
MMS:	IEC 61850 - Manufacturing Message Specification
Modbus RTU:	Serial data communications protocol
Profibus:	Serial data communications protocol
Redbox:	Provides an PRP interface to a non PRP enabled device
TCP/IP:	Internet protocol suite - Transmission Control Protocol (TCP) and the Internet Protocol (IP).

IV. CONCLUSIONS

The ECS has evolved with the advent of IEDs enabling a shift from traditional hardwired control to communication network type of systems. The ECS foundation has been gradually strengthened with the advent of new technologies enabling several value adding features. However, numerous previous projects have identified gaps in terms of reliability and performance of the ECS / ICSS interface. These gaps had resulted in negative impacts on projects start-up delays and production losses during operation. This paper progresses through the lines of enquiry encompassing the system interface designs, technology limitations, contractual framework with equipment suppliers and personnel competence. The work concluded in the summary of a system specification, including protocol recommendations, and detailing the associated proof of concept testing of the recommended architecture and protocols for process control interfaces summarised.

This paper may be considered as the first step towards standardisation of the interface engineering between ECS and ICSS. Work will need to continue with the aim of

improving the reliability and performance of this critical interface for the energy industry, as the technology further evolves, with respect to technology readiness level and further lessons are learnt from the projects.

V. ACKNOWLEDGEMENTS

The authors would like to thank the management and colleagues of the respective companies, the OEMs and the different project personnel who provided required support.

VI. REFERENCES

[1] Distributed Logic Load Shed System Via IEC 61850 By Jung Mun, Harrison Combs, IEEE PCIC Conference USA, 2019
[2] IEC 61850: Communication networks and systems for power utility automation
[3] IEC 61784: Industrial communication networks
[4] IEC 62439: High availability automation networks

VII. VITA

Alex Waslin started in the oil & gas industry in 1998, joining bp in 2001 where he gained a BEng in Electrical & Electronic Systems and a MSc in Data Networks and Distributed Systems degrees. He is a member of the IOGP, EI and EEMUA committees and of the Institute of Engineering and Technology (IET), UK. This is his first PCIC paper.
pcic2021@ajwaslin.co.uk

Dibyendu Bhattacharya is the Electrical Technical Authority-Projects at bp. He graduated from Jadavpur University, Kolkata, India in 1991 with Bachelor of Electrical Engineering 1st Class Honours degree. He worked with Indian Oil Corporation Limited Refineries division based in India, KNPC in Kuwait, Fluor and KBR in UK before joining bp. He has presented papers at PCIC London and has co-authored seven previous papers. He is a Chartered Engineer and a Fellow of Institute of Engineering and Technology (IET), UK.
d.bhattacharya2005@gmail.com

Michael Wilson graduated from Huddersfield University in 1998 with a BSc (Hons) degree in Electronic Design. He has been the System Applications Engineering Manager at Powell UK since 2012. This is his second external paper.
mwilson.pcic2021@gmail.com