

University of Southern Queensland

School of Engineering

Industrial Operational Technology Error Detection, Reporting, and the Subsequent Network Performance Impacts

A dissertation submitted by

Clinton Lauriston

in fulfilment of the requirements of

ENG4111 and 4112 Research Project

towards the degree of

Bachelor of Engineering (Honours) (Electrical/Electronic)

Submitted October, 2023

Abstract

As information technology (IT) and operational technology (OT) continue to grow and integrate into networked control systems, the risks associated with both intentional and unintentional cybersecurity and integrity grow. This is of particular concern as it supports many critical systems and infrastructure, maintaining safe and productive operational environments.

The project proposes a method to create a secure process to accurately and rapidly configure OT devices, audit the OT device blueprint, and promptly and autonomously alert the key stakeholders responsible for the integrity of the system, where it addresses the requirements without compromising network vulnerabilities, including performance and security.

This document describes the current shortfalls in information and the lack of technological use at the identified coal mine leaving them susceptible to intentional or unintentional tampering. Key stakeholder engagement was undertaken to gain a thorough understanding of the current situation, followed by bench testing and benchmarking network and device architecture and performance, to determine the feasibility of real-world project execution. The testing monitored the staged reduction in memory and the increased network utilisation with its possible impact on packet accuracy.

Of the advanced authentication testing, the field instrumentation were able to be analysed through the programmable logic controller (PLC) software, however automatic parameter authentication was not possible, due to the inability to access explicit parameters within the data frames. Conversely, the variable speed drives (VSDs) and motor management relay (MMR) were able to return their parameters, thus successfully auditable. Unfortunately they were unable to be configured remotely as the PLC software could not connect successfully through the device type manager (DTM) configuration interface. This testing regime resulted in minimal additional network loading, deeming the increased security measures suitable for implementation site-wide.

There is no information as to whether this method of authentication has been used in industry, so a particularly successful outcome of this dissertation is that with total production loss resulting in \$285,554/hour, the proposed approach has a potential return on hardware investment of 1 hour and 40 minutes.

University of Southern Queensland

School of Engineering

ENG4111 & ENG4112 Research Project

Limitations of Use

The Council of the University Southern Queensland, its Faculty of Health, Engineering and Sciences, and the staff of the University of Southern Queensland, do not accept any responsibility for the truth, accuracy or completeness of material contained within or associated with this dissertation.

Persons using all or any part of this material do so at their own risk, and not at the risk of the Council of the University of Southern Queensland, its Faculty of Health, Engineering and Sciences or the staff of the University of Southern Queensland.

This dissertation reports an educational exercise and has no purpose or validity beyond this exercise. The sole purpose of the course pair entitles “Research Project” is to contribute to the overall education within the student’s chosen degree program. This document, the associated hardware, software, drawings, and any other material set out in the associated appendices should not be used for any other purpose: if they are so used, it is entirely at the risk of the user.

Certification

I certify that the ideas, designs and experimental work, results, analyses and conclusions set out in this dissertation are entirely my own effort, except where otherwise indicated and acknowledged.

I further certify that the work is original and has not been previously submitted for assessment in any other course or institution, except where specifically stated.

Clinton Lauriston

Student Number: XXXXXXXXXX

Acknowledgements

First and foremost, I would like to thank my beautiful wife Anastasia for her support during my dissertation period.

Secondly, I would like to thank Mr John Kilkelly for his amazing guidance, mentoring and patience in helping me obtain the skills required to complete my thesis.

To you both, I will forever be in your debt.

Finally, I would like to thank Dr John Leis for his wisdom and supervision throughout.

Contents

Abstract.....	i
List of Figures.....	viii
List of Tables	ix
Abbreviations	x
1. Introduction.....	1
2. Literature Review	2
2.1 Chapter Overview	2
2.2 Security	2
2.2.1. Integrity.....	2
2.2.2. Availability	2
2.2.3. Confidentiality	2
2.3. Desktop Device Audit.....	2
2.3.1. Programmable Logic Controllers.....	4
2.3.2. Soft Start Drives.....	4
2.3.3. Instrumentation	4
2.3.4. Motor Management Relays.....	5
2.3.5. High Voltage Protection.....	5
2.3.6. Low Voltage Protection	5
2.4. Supervisory Control and Data Acquisition	5
2.5. Change Management Software	5
2.6. Industry Applications.....	5
2.7. Performance Testing	7
2.8. Knowledge Gap	7
2.9. Legislative Requirements.....	8
2.10. Site Requirements	8
2.11. Objectives	8
3. Methodology	10
3.1. Device Audit	10

3.2.	Stakeholder Engagement.....	10
3.3.	SCADA Project Creation.....	12
3.4.	Bench Testing	12
3.4.1.	Benchmarking	12
3.4.2.	Device Addition	13
3.4.3.	Live Plant Testing	13
3.5.	Substation Hardware Audit.....	14
3.6.	Hardware Costs	15
3.7.	Hardware Procurement Feasibility.....	16
3.8.	Schematics	16
3.9.	SCADA Creation	17
4.	Protocol Selection and Utilisation.....	19
4.1.	HART.....	19
4.2.	Modbus TCP/IP	20
4.3.	PLC Communication Configuration	20
4.3.1.	Site Standard Benchmarking.....	20
4.3.2.	Advanced Authentication Mode	21
5.	Results	22
5.1.	Site Standard Benchmarking.....	22
5.1.1.	Memory Usage.....	22
5.1.2.	Network Performance	23
5.2.	Advanced Authentication Mode	24
5.2.1.	Network Performance	25
5.2.2.	Advanced Authentication Functionality	25
5.3.	Loading Comparison Between Modes.....	29
6.	Conclusion	32
6.1.	Project Outcomes	32
6.1.1.	Objective 2.11a Outcome.....	32
6.1.2.	Objective 2.11b Outcome	32

6.1.3. Objective 2.11c Outcome.....	32
6.1.4. Objective 2.11d Outcome	32
6.2. Further Work.....	33
7. References.....	34
Appendix A – Project Specification.....	36
Appendix B – Risk Assessment.....	37
Appendix C – Drawings.....	38
C1 – Site Standard Benchmarking Schematics	38
C2 – Advanced Authentication Mode Schematics.....	41
Appendix D – Cicode	44
D1 – typ_CommsTest	44
Appendix E – Modbus TCP/IP Configurations	55
E1 – Benchmarking Communications DTM Configuration	55
E2 – Advanced Authentication Communications Configuration.....	55
Appendix F – Results	58
F1 – Benchmarking.....	58
F1.1. – Benchmarking Memory Usage	58
F1.2. – Benchmarking Network Performance.....	60
F2 – Advanced Authentication Mode	64
F2.1. – Advanced Authentication Memory Usage.....	64
F2.2. – Advanced Authentication Network Performance	65

List of Figures

Figure 1: eX80 architecture incorporating HART communication with HART compatible instrumentation (Source: Schneider Electric Pty Ltd 2015, p.18).....	6
Figure 2: SCADA main page.....	17
Figure 3: SCADA VSD super genie	17
Figure 4: SCADA MMR super genie.	18
Figure 5: HART protocol digital over analogue superimposition (HART Communication Foundation 2013, p. 11).	19
Figure 6: HART communication data frame (Li & Dong 2018, p. 2222).	20
Figure 7: Modbus TCP/IP data packet structure (Pricop et al. 2017, p. 681).	20
Figure 8: PLC code reading the registers of desired ATV930 parameters.	21
Figure 9: PLC code reading the registers of desired ATV71 parameters.	21
Figure 10: PLC code reading the registers of desired TeSys T parameters.	21
Figure 11: Screenshot of Schneider's Control Expert interface whilst connected to a Vegapuls61 radar.	25
Figure 12: Screenshot of the SCADA mimic page showing alarms pertaining to unauthorised device configuration changes.	26
Figure 13: Vegapuls61 configuration interface within Schneider's Control Expert PLC software.	27
Figure 14: Cerabar S configuration interface within Schneider's Control Expert PLC software.....	28
Figure 15: Cerabar S upload from device page within Schneider's Control Expert PLC interface.	28
Figure 16: ATV930 configuration interface within Schneider's Control Expert PLC software.	29
Figure 17: Network utilisation for benchmarking vs advanced authentication mode.....	30
Figure 18: TCP packet round trip time for benchmarking vs advanced authentication mode.	30
Figure 19: Maximum TCP packet rates for benchmarking vs advanced authentication mode.....	31
Figure 20: PLC memory utilisation comparison for benchmarking vs advanced authentication mode.	31

List of Tables

Table 1: The identified coal mine's list of preferred equipment with high usage numbers (≥ 5).....	3
Table 2: The identified coal mine's list of preferred equipment with low usage numbers (< 5).....	4
Table 3: Stakeholder interview answers.	11
Table 4: Benchmarking and advanced authentication network testing list of activities.	12
Table 5: The identified coal mine's substation Modbus TCP/IP communication hardware audit.	14
Table 6: The identified coal mine's substation HART communication hardware audit.	14
Table 7: Cost estimate of project hardware requirements.....	15
Table 8: OT device connection configuration map.....	22
Table 9: Benchmarking PLC memory consumption.....	23
Table 10: Benchmarking network performance testing.	24
Table 11: Advanced authentication PLC memory consumption.	24
Table 12: Advanced authentication network performance testing.....	25

Abbreviations

ALARP	As Low as Reasonably Practicable
AS	Australian Standards
CHPP	Coal Handling Preparation Plant
CMSHR	Coal Mining Safety & Health Regulation
DTM	Device Type Manager
E&H	Endress & Hauser
HMI	Human Machine Interface
IT	Information Technology
I/O	Input/Output
IROC	Integrated Remote Operating Centre
KPI	Key Performance Indicator
MBAP	Modbus Application Protocol
OPC	Open Platform Communications
OT	Operational Technology
PCN	Process Control Network
PCS	Process Control System
PLC	Programmable Logic Controller
PwC	PricewaterhouseCoopers
SCADA	Supervisory Control and Data Acquisition
SOP	Safe Operating Procedure
SP	Setpoint
VLAN	Virtual Local Area Network
VSD	Variable Speed Drive
VVVF	Variable Voltage Variable Frequency

1. Introduction

Identified as major flaws in industry, field OT devices are easily accessible where parameters may be accessed and altered by anyone, even if by mistake. Changes to OT device configuration settings can prove to be catastrophic, evidenced by an incident in March 2009 where an Emirates Airbus nearly crashed with 275 passengers at Melbourne Airport due to a pilot accidentally implementing the incorrect parameterisation of a setpoint (SP) in an onboard computer (Pietre-Cambacedes et al. 2013, p.2156)

This project idea arose from the increasing emphasis mining operators are placing on blueprint management and cybersecurity. With the complexity of systems employed in heavy industry developing, tampering with a system or device configuration cannot only be dangerous due to the high levels of automation, but extremely difficult to diagnose and rectify due to the intricacies involved and the advanced training required for employees to obtain the required skill level to perform the investigative and rectification tasks. An example of this is evident at the identified coal mine where, by luck, it was discovered that critical protection parameters pertaining to human safety - earth leakage current settings – were disabled to remove the nuisance tripping occurring on multiple operational technology OT devices. This was allowed to happen as there is no monitoring of OT device parameters connected to the site's PCN.

It has also been identified that there are issues with additional processing downtime due to the lack of configuration files being backed-up in the file repository system, meaning every device needs to be configured from the factory default, resulting in reduced plant availability and the possibility of incorrect configurations forming a dangerous scenario.

To effectively mitigate the issues and deliver the project of creating a closed system where only those authorised personnel can configure OT devices, with the system checking the validity of this practice continuously, research into the area of multiple communication protocols being monitored over a multitude of devices will be required. Testing of device and network performance and mutual integration will be a large part, which will require much research, as there is no evidence of the coal industry, or any other with the architecture employed at the identified coal mine producing this system of OT device management.

2. Literature Review

2.1 Chapter Overview

The literature review focuses on closing the knowledge gap of the identified coal mine's control system vulnerabilities, predominantly OT device configuration integrity. This will include the review of assets external to the identified coal mine and their methods of ensuring OT device integrity is sufficiently controlled. The outcome of this section will assist in leading the project down a calculated path and allow for definitive project aims, objectives and deliverables.

2.2 Security

PricewaterhouseCoopers (PwC) (Feinman, et al. 1999, p. 3) formulate the idea that there are three main aspects that should be examined when determining the effective requirements of security pertaining to IT: integrity, confidentiality, and availability. From the PwC report, elements of this project can aim to deliver an uplift in security measures, or ensure they are already being sufficed.

2.2.1. Integrity

The integrity aspect, where an assurance is made that information or configurations cannot be modified in unexpected ways will be the forefront of this project where it has been identified the consequences of inaccurate information can prove to be disastrous. The loss of integrity for a system can be attributed to human error, intentional tampering and events causing corruption (Feinman, et al. 1999, p.4). This project addresses the human error and intentional tampering elements, however, also act to improve device return-to-operation times by creating easy to execute actions to reinstate devices post-corruption.

2.2.2. Availability

Availability, or the lack thereof, can be used to ensure that limitation to devices both physically and via various network topologies and security measures can be used to reduce tampering. This can include the use of gateways to limit access from both internal and external users to only allow certain types of traffic (Feinman, et al. 1999, p.5).

2.2.3. Confidentiality

The use of password protection to ensure information and access is unavailable to people is the most common security element employed as it is low cost, easy to implement and can be dynamic when required. Strong password policies are required to ensure powerful decrypting services find it difficult to unlock the protection (Feinman, et al. 1999, p.5). Tiered approaches can be employed where levels of access depending on stature and position in a company can easily be granted and removed at any stage.

2.3. Desktop Device Audit

With a vast array of OT devices employed at the identified coal mine to monitor and control apparatus within the coal handling preparation plant (CHPP), the importance of understanding the capabilities is

extremely important. Determining which common communication protocol the devices share will help to make the implementation easy and straightforward as it allows for identification as to whether a project has previously been employed with methods and if the subsequent data is available. The coal mine's preferred equipment list (2021, pp. 4-14) declares the devices used, a useful starting point before a widespread audit is undertaken to ensure there is no oversight.

The list of devices at the identified coal mine are outlined in the Preferred Equipment List document which has been tabulated in *Table 1* and *Table 2*, representing the high and low volume devices respectively. Due to experience with the site, it can be identified that some devices are missing. Contemporary radiation gauges have now been installed, phasing out older models documented in *Table 2*.

Safety relays used on site have also not been referenced in the list. These gaps are a concern, as there may undocumented devices installed. Remediation works for this document are external to project scope.

Table 1: The identified coal mine's list of preferred equipment with high usage numbers (≥ 5).

Application	Vendor	Device	Number used
Variable Speed Drives (AC)	Schneider Electric	ATV71	195
		ATV930	7
Soft Starters	Schneider Electric	Altistart	8
Motor Management Relays	Schneider Electric	TeSys T	115
Air Circuit Breakers	Schneider Electric	Masterpact	23
High Voltage Protection Relays	ABB	REF615	18
	Schneider Electric	Sepam	20
High Voltage Power Meters	Schneider Electric	PowerLogic	9
Low Voltage Power Meters	Schneider Electric	PM820	23
Differential Pressure Transmitter	Endress & Hauser	Cerabar S PMC71	8
	Yokogawa	EJX110A	20
Level Transmitter (Ultrasonic)	Endress & Hauser	Prosonic Series	10
Magnetic Flow Meters	ABB	FEP300	12
PLC	Schneider Electric	M580	20
PLC Remote I/O	Schneider Electric	M340	48
		Advantys STB	16
Process Control Network Ethernet Switches	CISCO	IE-3000-8TC	38

Table 2: The identified coal mine's list of preferred equipment with low usage numbers (<5).

Application	Vendor	Device	Number used
Variable Speed Drives (DC)	ABB	DCS800	1
Coriolis Flow Meters	Endress & Hauser	Promass	3
Density Source/ Transmitter	Endress & Hauser	FMG60	4
Density Display and Operating Unit	Endress & Hauser	RIA15	4
Level Transmitter (Radar)	Endress & Hauser	FMR Series	4
	Vega	Vegapuls 61	4
	Rosemount	5600 series	2
Train Weighbridge	Meridian	Application specific	2
Moisture Analyser	Callidan Instruments	MA-500 Series	1

2.3.1. Programmable Logic Controllers

The identified coal mine employs Schneider Electric's Modicon M580 PLC system in all areas to control fixed processing plant. This system also utilises both the Modicon M340 PLC and Advantys STB as remote distributed input and output (I/O) modules for field wiring. The range mentioned all communicate with the process control network (PCN) via Modbus TCP/IP (Schneider Electric Pty Ltd 2022, p.45-46). The M580 and M340 pertain to the X80 form factor which can be integrated with HART 5 protocol, as well as the Advantys STB as prescribed on page 16 of Schneider's document on HART protocol integration (Schneider Electric Pty Ltd 2015, p. 18).

2.3.2. Soft Start Drives

The soft start drives at the identified coal mine are ABB DCS800. The drives are not directly compatible with Modbus TCP/IP Ethernet communication protocol, therefore will need a protocol converter installed as per ABB's manual (ABB Automation Products GmbH 2005, p. 2) for the soft start drives.

2.3.3. Instrumentation

There are varied configurable instruments measuring varied processes from a multitude of manufacturers. All instrumentation by Endress & Hauser (E&H), Emerson Rosemount, Vega and ABB as listed in *Table 1* and *Table 2* are compatible with the HART 5 protocol. The others will need research

into their capabilities as they have been designed by small firms with proprietary communication protocols.

It has been identified that instruments installed that have not been documented in *Table 1* and *Table 2*, which is a gap that will need to be filled external to this project.

2.3.4. Motor Management Relays

The motor management relays at the identified coal mine are Schneider TeSys T. All relays communicate with the PCN via Modbus TCP/IP Ethernet communication protocol as per Schneider's TeSys T LTMR document (Schneider Electric Pty Ltd 2022b, p. 15).

2.3.5. High Voltage Protection

The high voltage protection relays, as listed in *Table 1*, does not specify which model is being used, therefore it cannot be assured as to what communication protocols are available. This is a gap that will need to be filled external to this project.

The REF615 is compatible with Modbus TCP/IP protocol, as per ABB's user manual (ABB Automation Products GmbH 2009, p. 46).

2.3.6. Low Voltage Protection

The low voltage protection relays, as listed in *Table 1*, does not discreetly identify which model is being used, therefore it cannot be assured as to what communication protocols are available. This is a gap that will need to be filled external to this project.

2.4. Supervisory Control and Data Acquisition

The supervisory control and data acquisition (SCADA) system used at the identified coal mine is Vijeo Citect 2023. This will be used to acquire the data from the PLC and display it for operators and maintainers. The level of access to write and read data to and from the end devices will be governed at this level, where a tiered approach will be utilised.

2.5. Change Management Software

Versiondog is the change management system at the identified coal mine, where it has been employed as a file repository, holding all configuration files for OT devices, including but not limited to PLCs, VSDs, MMRs, etc. There is limited information pertaining to automatic comparisons, which is a knowledge gap that will need to be filled.

2.6. Industry Applications

There is no evidence that this task has been undertaken, yet there is evidence that parts of the objective are attainable, predominantly surrounding some parameter acquisition from each device. Schneider (2015) offers a document that steps through the process of integrating HART compatible

instrumentation with the Schneider eX80 architecture. This document covers the wiring requirements for remote I/O to a Schneider M580 PLC, however there is no reference to M340 PLC and Advantys STB I/O modules as per the coal mine's PCN topology. There are also performance characteristics stated for their test instruments, however this is on a micro scale when compared to a real industrial environment, where there are hundreds of OT devices. *Figure 1* is an excerpt from 'How Can I... Integrate HART into eX80 Architecture' (Schneider Electric Pty Ltd 2015) which displays a high-level architecture layout incorporating HART devices

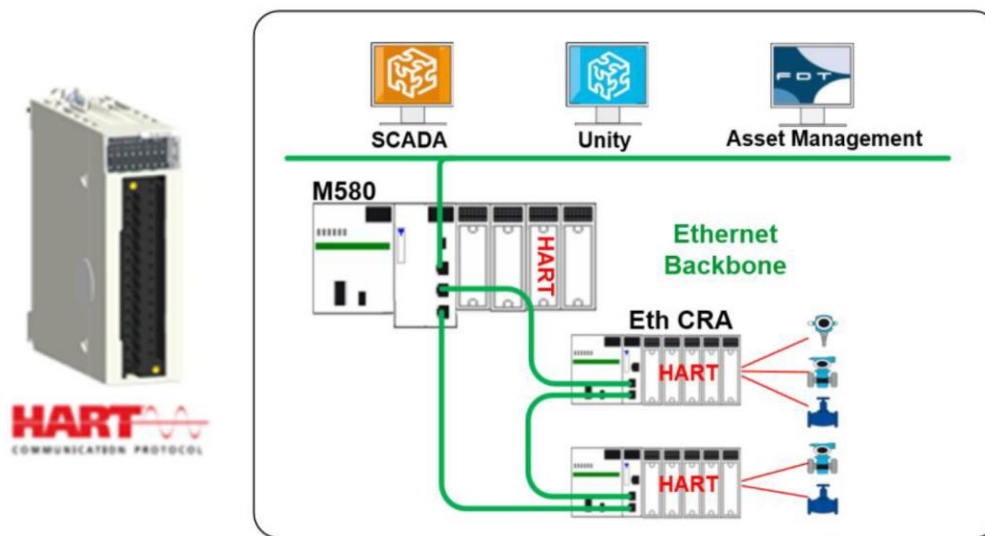


Figure 1: eX80 architecture incorporating HART communication with HART compatible instrumentation (Source: Schneider Electric Pty Ltd 2015, p.18).

There are no precedents in the industry pertaining to HART over Modbus TCP/IP regarding device configuration changes, however other protocols, like Foundation Fieldbus, regularly use this type of instrument integrity checking. An example was made by FieldComm Group (n.d.) where a case study was undertaken on Kaneka Corporation in which the company employed Foundation Fieldbus as their control system communication protocol, giving them the ability to monitor and optimise smart instrumentation and other end-devices remotely and securely. Whilst conversion to Foundation Fieldbus would be an unreasonable task for the coal mine due to the major financial outlay, there are elements from the case study that can be used to assist in idealisation where, possibly outside of this scope, smart algorithms may be created to detect instrument calibration issues and allow a controlled method to modify parameters.

There has been some work undertaken in utilising the Cumulative Sum algorithm where the cumulative summation of the deviations of the differences between the sampled process variables and the process set points are used to alert to tampering as it shows that device outputs are most likely being manipulated manually. This is a good way to identify whether an attack is being made on an output of the OT device,

however due to the fluctuating process characteristics of coal processing and the limited maintenance undertaken on the instrumentation at the identified coal mine, it is not recommended as an intrusion detection method (Ao 2020, p. 3).

No documentation can be found where configuration changes to OT devices pertaining to the coal mine's architecture and hardware can be automatically detected, as all others found employ Foundation Fieldbus.

2.7. Performance Testing

Tang (2017, p. 12) recommends five (5) key performance indicators (KPIs) to derive the performance level of the network, which can be reviewed at each iteration of bench-testing. Depending on the nature of the resultant data, this could lead to the potential for the implementation across the site. These are listed as:

1. Manufacturing process performance: performance of the manufacturing process
2. Network performance: measures the performance of the TCP/IP network
3. Computing resource performance: measures the performance of the computer, hardware and software process
4. Industrial protocol performance: measures the performance of the industrial communication protocol
5. Open platform communications (OPC) data exchange performance: measures the performance of the data exchange mechanism of the system.

2.8. Knowledge Gap

The knowledge gaps pertaining to the question "Is there a way to ensure OT configuration security, automate blueprint verification and report issues?" that have been identified through this literature review are:

1. What is the full device list at the identified coal mine?
2. Can we monitor all parameters, or will this adversely affect the network performance, i.e., can PLC cycle times still be met?
3. What do the end-users (operators, maintainers, engineers) need to fulfill their tasks effectively?
4. Can the system be made tamper-proof?
5. What network topology changes are required to obtain consistent communication with devices that meet the relevant KPIs?
6. Is it possible for the instrumentation to communicate via the Schneider M340 or Advantys STB PLCs as remote I/O drop nodes?
7. What are the impacts of the project on network performance?

8. Which device parameters will be required to be processed and displayed, with minimal network performance impact as priority?
9. Can we upload 'old model' configuration files to 'new model' devices in a bulk upload manner?
10. Can one software application configure multiple OT devices?
11. Will we require additional subnets or virtual local area networks (VLANs)?

2.9. Legislative Requirements

Section 27a of the Coal Mining Safety and Health Regulation (CMSHR) (2017, p. 48) expresses that "A coal mine's safety and health management system must— (a) provide for the security and maintenance of the mine's electrical control system software and control circuits; and (b) control modification of the software and circuits; and (c) provide for records to be kept of any modifications." Currently, the mine does not fully meet this requirement as there are many security issues, predominantly surrounding OT device tampering, as well as recording changes, which is being left to individuals' honesty and integrity, something that should be engineered to ensure compliance.

2.10. Site Requirements

The literature review also identified that the coal mine operator's blueprint management document (2020, p. 6) calls for configuration files to be kept as a blueprint artefact, another issue that must be rectified as part of the site's legislative requirement.

2.11. Objectives

The key objective for this project will be to implement provisions to tamper-proof the OT devices pertaining to the process control system (PCS). This will greatly reduce the ability for any person to change configurations maliciously or accidentally at the coal mine's coal handling and processing plant (CHPP). If unauthorised changes have taken place, an automatically controlled action will be initiated to alert further investigation. The project will aim to communicate directly with the device, monitor the configuration of the device and report if a change to a configuration has been made. Changing configuration settings can only be completed in the SCADA environment, which will be largely write protected and governed by a tiered, password protected authorisation approach. Once updates to device configurations have been completed, a new configuration file will be uploaded to the change management software, which will become the new 'as-built' version. If the security mechanisms have been breached, and there has been an unauthorised change to a configuration file, an alert will be generated where a report will be sent to key stakeholders advising which parameters have been changed and when.

Another key deliverable of the project will be to reduce the downtime caused by OT device failure. Currently, after a failure to a device, some devices are needing to be configured from factory default, in a harsh environment, usually near the process that the device is monitoring or controlling. The

approach from the project will be to utilise the configuration files in the repository to rapidly configure the device, increasing operational and maintenance productivity, as well as greatly improve safety through the removal of technicians from the area, and to greatly reduce or eliminate human error.

To allow for easy qualification, the key objectives are succinctly listed as:

- a) Automatically detect configuration changes for instrumentation and motor control devices.
- b) Configure instrumentation and motor control devices remotely, securely, accurately, and fast.
- c) Determine network and memory loading increases due to advanced methods of monitoring and configuring instrumentation and motor control devices.
- d) Determine suitability of site implementation.

3. Methodology

The approach undertaken was to establish a staged approach to ensure there will be no adverse impacts to the process control network, primarily network performance and PLC memory consumption.

3.1. Device Audit

An audit was undertaken to determine the devices that are required to be networked to the PCN. The main elements taken from each device will be:

1. What OT devices are installed at the coal mine's CHPP?
2. What communication protocol can they use?
3. Can the device be locked from HMI usage?
4. What parameters can be read/ written remotely?
5. Are the configuration files backed up and stored in the change management software?

3.2. Stakeholder Engagement

Stakeholders were engaged to determine which parameters are vital to ensure accurate OT device configuration monitoring and changing, as well as general functionality. This also set the minimum standard, where if the system was not capable of accomplishing the stakeholder requirements, it would be deemed unsatisfactory for site implementation. These answers assisted in qualifying the key aims of the project, listed in 2.11 Objectives.

The primary functionalities that can be derived from the stakeholder interview table, as listed in *Table 3* were:

1. Control access by locking field device HMIs.
2. Use SCADA to configure devices where user access is protected by individual Citect profiles.
3. Automated auditing of configurations incorporating unauthorised parameter change detection.

Table 3: Stakeholder interview answers.

Interviewee	Position	Date	Key Messages
Person 1	Operator/Maintainer (Electrician)	21/03/2023	Identified lack of confidence when using instrument HMIs – easy to corrupt configurations.
			View all available parameters via SCADA.
			Access control using site roles as access levels.
			Automatic auditing of parameters with notifications sent to stakeholders alerting to changes.
			Date of upload for current configuration viewable on SCADA.
			Certain parameters can be accessed individually granted by access level.
			Login required to changed parameter even if logged in to SCADA.
			Default to be shown with colour changes to show non-default values.
Person 2	Control Systems Engineer	21/03/2023	All parameters to be configurable.
			Control Expert (PLC software) to be used to configure parameters.
			All employees to have read-only access.
			Only approved electricians to change parameters.
			Instrument and VSD HMIs locked.
			Automated configuration comparison.
Person 3	Maintenance Electrician	23/03/2023	User-friendly approach.
			All parameters to be visible.
			Parameters stored for easy upload.
Person 4	Process Technician/ Supervisor	23/03/2023	Not too concerned about functionality.
			Fast instrument replacement with minimal impact to production.
			Technicians to be removed from the frontline to reduce risks to safety.
			Alarming upon data corruption.

3.3. SCADA Project Creation

A SCADA system will be needed to interface with the OT devices, where a new project will be created with a graphical interface. This project will aim to contain small genies with links to open the device software-based configuration application and upload the configuration files. This SCADA project will be created in Vijeo Citect 2023 and comply with site standards in terms of genies and layout. This system will allow for a user-friendly form of read/ write access to the OT devices.

3.4. Bench Testing

3.4.1. Benchmarking

A test bench will be constructed containing a large cross-section of the devices obtained in the device audit. This will require a bill of materials to be created and a subsequent procurement of hardware.

Benchmarking will then take place where the network is set up to replicate the current network topology at the coal mine, where tests will then be completed to benchmark the network speed and loading. The tests are listed in *Table 4*, where many tests were derived via the consultation of Tang (2017, pp. 13-6).

Table 4: Benchmarking and advanced authentication network testing list of activities.

Test	Description
Accuracy	Comparing the OT device HMI data vs the SCADA read data
Network utilisation	Measuring the percentage of network capacity being utilised
PLC cycle times	Measuring the cycle times for the PLC
TCP packet round time	Measuring the amount of time for source node to receive acknowledgment of message
Packet rate	Measuring the rate of packets transmitted and received by the OT devices
Packet error rate	Measuring the rate of packets received with errors from the OT devices

By benchmarking the current topology, it will assist in identifying any impacts the project will have on performance, a critical element to the PCN.

Key devices in the benchmarking phase of test benching will be:

- 1 x Cisco IE3000 network switch
- 1 x M580 PLC
- 1 x M340 remote I/O (site standard architecture)
- 1 x Advantys STB I/O (site standard architecture)

- 2 x VSDs (site standard parameter read/write)
- 1 x TeSys T MMR (site standard parameter read/write)

3.4.2. Device Addition

As the bench testing task progresses, the loading of the test network will be increased with the enablement of device specific protocols and the incremental addition of OT devices, where the network performance will be gauged and documented at each change. The addition of devices will cease when the following topology is attained:

- 1 x Cisco IE3000 network switch
- 1 x M580 PLC
- 1 x M340 I/O card with 3 analogue input instruments (HART compatible architecture)
- 1 x Advantys STB I/O with 3 analogue input instruments (HART compatible architecture)
- 2 x VSDs (advanced parameter read/write)
- 1 x MMRs (advanced parameter read/write)

By utilising a test environment, isolated from the active PCN, there will be an assurance that there are no impacts to the PCN, which could potentially result in production loss events or safety issues.

Using stakeholder engagement feedback and the bench testing results, the project will then be able to determine if only critical parameters will be attained from the device, or whether the complete OT device configuration parameters can be used.

3.4.3. Live Plant Testing

Whilst the data will be analysed to determine the suitability of the project to be undertaken on “live plant”, the execution of this will not occur due to time constraints and the risks associated with the advancement of the project. This work may still be undertaken, however not under the banner of this thesis.

3.5. Substation Hardware Audit

The substations have been audited to determine the OT device allocations to assist in determining a good cross-section of devices installed for the project. *Table 5* identifies the OT devices that share Modbus TCP/IP as their communication protocol. The hardware that communicates via HART protocol are represented in *Table 6*.

Table 5: The identified coal mine's substation Modbus TCP/IP communication hardware audit.

Substation	ATV71 (VSD)	ATV930 (VSD)	TeSys (MMR)	T M580 (PLC)	M340 (PLC)	Advantys STB (PLC)
MC101	-	7	32	1	4	-
MC111	7	-	13	1	4	-
MC112	3	2	12	1	2	-
MC121	5	-	8	1	-	8
MC131	8	-	17	1	-	9
MC141	8	-	24	1	5	-
MC404	19	-	57	1	12	2
MC411	4	-	28	1	2	-
MC421	4	-	28	1	2	-
MC471	94	-	35	1	3	3
MC802	6	-	15	1	6	-
MC807	-	-	3	1	-	-

Table 6: The identified coal mine's substation HART communication hardware audit.

Substation	Yokogawa EJX110A (Differential Pressure)	E&H PMC71 (Differential Pressure)	E&H FMG60 (Gamma Density)	E&H FMU90 (Ultrasonic Level)	Vega Vegapuls61 (Radar Level)	ABB FEP630 (Magnetic Flow)
MC101	-	-	-	1	-	-
MC111	-	-	-	1	-	-
MC112	-	-	-	-	-	-
MC121	-	-	-	-	2	-
MC131	-	-	-	-	2	-
MC141	-	-	-	-	-	-
MC404	2	2	3	1	-	2
MC411	4	1	2	2	-	4
MC421	4	1	2	2	-	4
MC471	-	-	3	3	2	3
MC802	-	-	-	-	-	-
MC807	-	-	-	-	-	-

3.6. Hardware Costs

The high-level cost estimate is displayed in *Table 7* below. This cost estimate is primarily focusing on the financial outlay required by the desktop assessment drawn from BMA's Electrical Preferred Equipment List document (2021). This is also assuming that the volume of spares kept are adequate to suffice the testing requirements. There is no added contingency as the parts have been quoted and purchased.

Table 7: Cost estimate of project hardware requirements.

Device Name	Device Description	Total required	Cost per unit	Cost
Cisco IE3000	Network switch	1	\$0 (temp use of spares)	\$0
M580	PLC	1	\$0 (temp use of spares)	\$0
M340	Remote I/O	1	\$0 (temp use of spares)	\$0
Advantys STB	Remote I/O	1	\$0 (temp use of spares)	\$0
Altivar 71	VSD	1	\$0 (temp use of spares)	\$0
Altivar 930	VSD	1	\$0 (temp use of spares)	\$0
TeSys T	MMR	2	\$0 (temp use of spares)	\$0
BMECRA31210	X80 Ethernet Remote I/O drop adapter	1	\$3,410	\$3,410
BMEAHI0812	M340 8-CH HART analogue input card	4	\$2,525	\$10,100
BMEXBP040	4-slot M340 PLC rack	1	\$0 (temp use of spares)	\$0
STBAHI8321KC	Advantys STB 4-CH HART analogue input multiplexer	4	\$1,760	\$7,040
STBAHI8321K	Advantys STB 4-CH HART analogue input card	1	\$0 (temp use of spares)	\$0
TEESTBNIP2311	Remote IO Ethernet module	2	\$1,240	\$2,480
SHNSTBPDT3100K	PDM Standard Kit connection base	2	\$221	\$442
SHNBMXFTB2010	20 point screw terminal strip	4	\$102	\$408
Total				\$23,880

3.7. Hardware Procurement Feasibility

At the date 2/09/2023, using the current spot price of coking coal at \$117US per ton (Business Insider 2023a), an exchange rate of 0.6462 (Business Insider 2023b) and the average yield of the coal mine at 55% for an hourly feed rate tonnage of 2750tph, the cost per hour of downtime can be calculated by first determining the hourly financial loss (3.1), calculating the hardware cost (3.2), which then allows the feasibility of the project's hardware procurement to be calculated (3.3).

$$\text{hourly financial loss} = \frac{\text{spot price} \cdot \text{yield} \cdot \text{feed rate}}{\text{exchange rate} \cdot \text{hours}} \quad (3.1)$$

$$\text{hourly financial loss} = \frac{\$122 \cdot 0.55 \cdot 2,750}{0.6462 \cdot 1}$$

$$\therefore \text{hourly financial loss} = \$285,554/\text{hr}$$

Now, assuming this is 5% of the required hardware cost for a full CHPP upgrade project,

$$\text{total hardware cost} = \frac{\text{total with contingency}}{\text{percentage completed}} \quad (3.2)$$

$$\text{total hardware cost} = \frac{\$23,880}{0.05}$$

$$\therefore \text{total hardware cost} = \$477,600$$

If 100% production is ceased due to an OT device issue, the payback time can be calculated as:

$$\text{payback time} = \frac{\text{total hardware cost}}{\text{hourly financial loss}} \quad (3.3)$$

$$\text{payback time} = \frac{\$477,600}{\$285,554/\text{hr}}$$

$$\text{payback time} = 1.67 \text{ hours}$$

$$\therefore \text{payback time} \approx 1 \text{ hour } 40 \text{ minutes}$$

The hardware procurement payback time in lost production gives a payback time of 1 hour and 40 minutes, however costs to install, etc., will need to be accounted for if a large-scale feasibility study is to be undertaken. This is the least important figure, however when one considers the safety uplift from the removal of personnel from the frontline and ensuring OT devices contain the correct and safe configurations, as well as ensuring compliance to the CMSHR.

3.8. Schematics

Schematics have been devised using AutoCAD, ensuring a structured approach to the electrical wiring and communication patching. Schematics may be viewed in *Appendix C – Drawings*.

3.9. SCADA Creation

The SCADA project was created from scratch and named *ThesisSCADA*. This was to reduce the overheads from the site project that could suppress elements key to testing, primarily OFS communications. *Figure 2* shows the SCADA project's main page with *Figure 3* and *Figure 4* being the super genies for the VSDs and MMR respectively during testing.

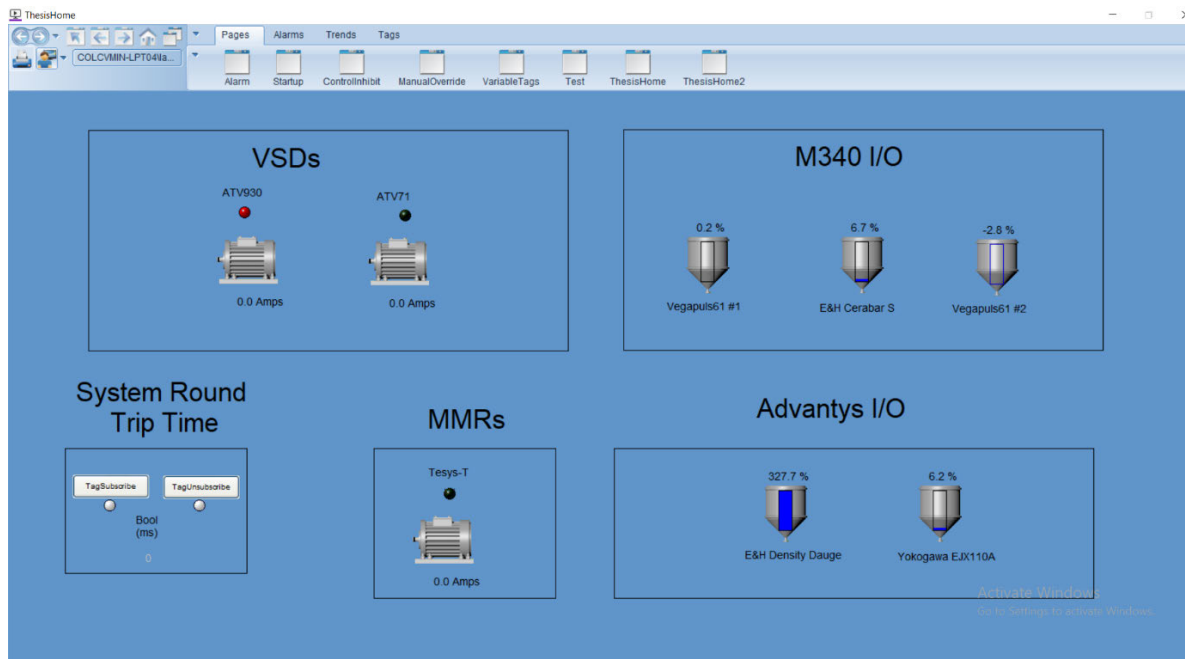


Figure 2: SCADA main page

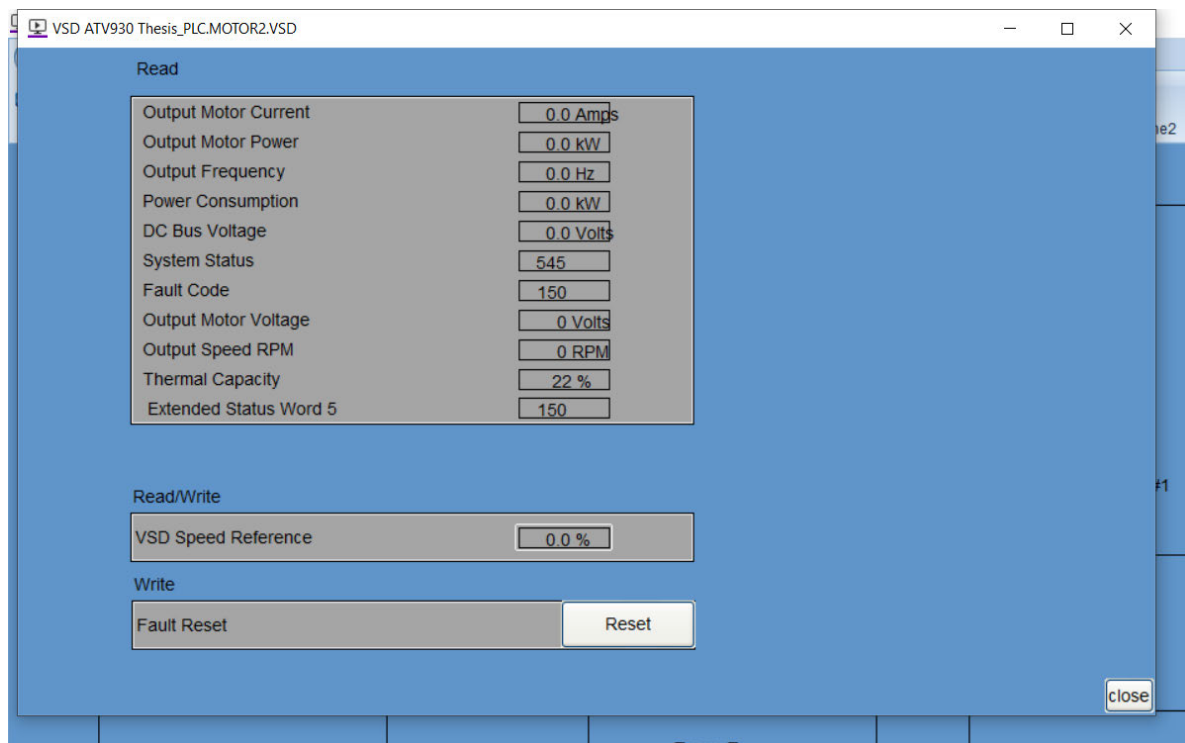


Figure 3: SCADA VSD super genie

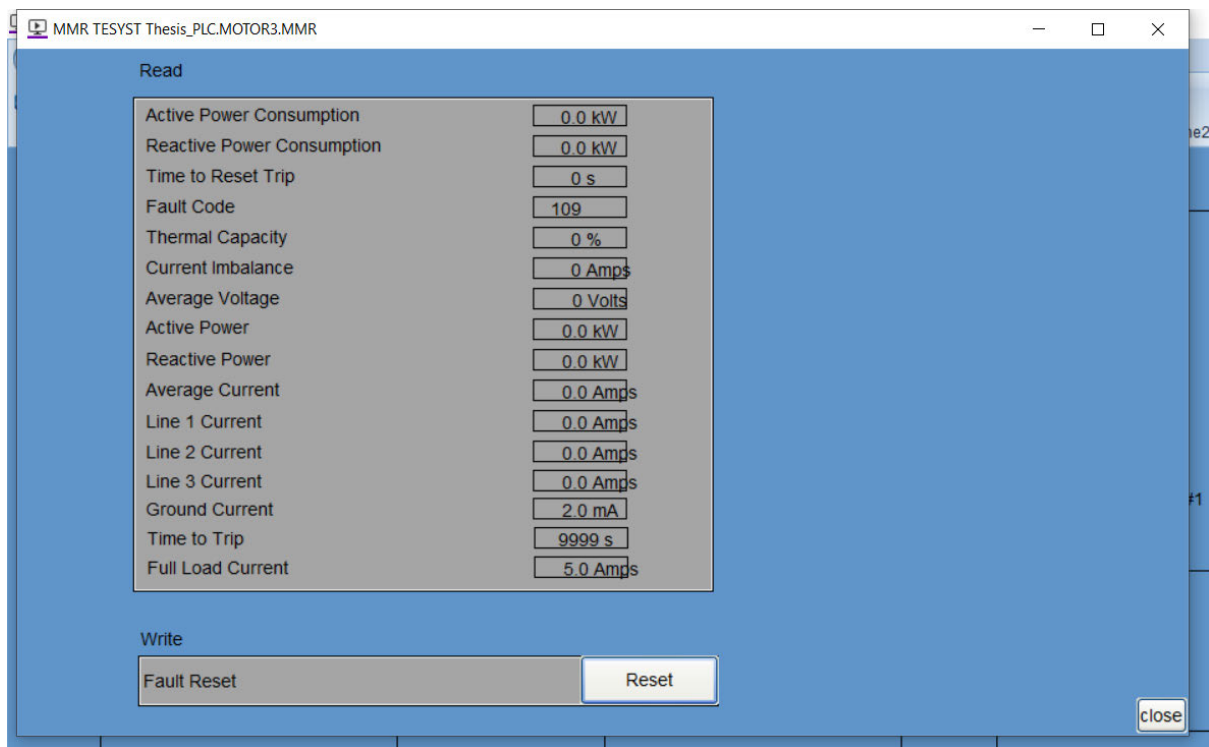


Figure 4: SCADA MMR super genie.

4. Protocol Selection and Utilisation

As prescribed by Pricop et al. (2017, pp. 679-80), the most common attacks on industrial control systems (ICS) are man-in-the-middle attacks. This occurs when the attacker physically installs a device, (USB, hardware containing malware, etc.) within the control system network, simulating data from a field device. This requires a form of authentication to detect and mitigate the impacts from the violation – a unique “fingerprint”.

4.1. HART

The HART protocol, through the employment of digital signalling superimposed onto the 4-20mA analogue signal, as shown in *Figure 5*, is an extremely common measurement method in industrial instrumentation (Sasaki & Ueda 2007, p. 1) and may give data which can be reviewed against the system information gathered during the controlled installation and commissioning of the device. This will allow for serial numbers, plant identifiers and parameterisation sets to be reviewed periodically.

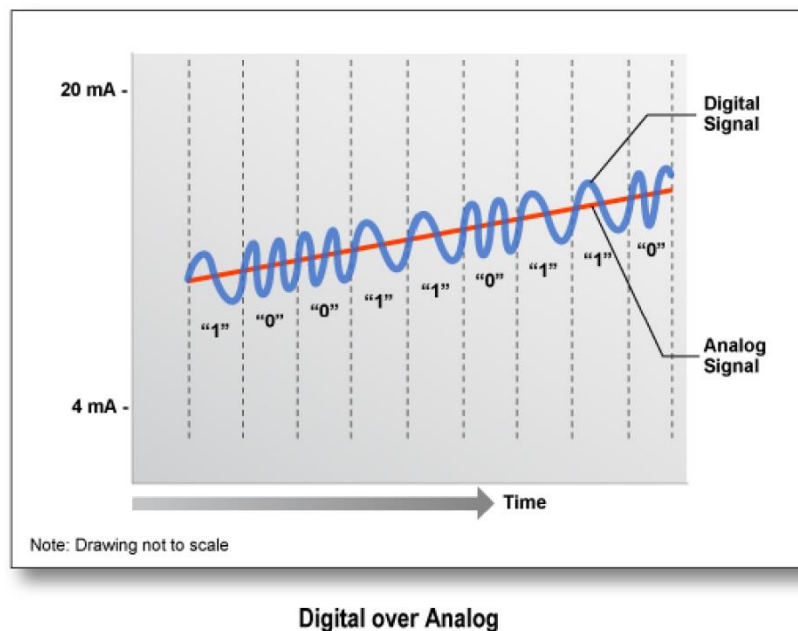


Figure 5: HART protocol digital over analogue superimposition (HART Communication Foundation 2013, p. 11).

Figure 6 documents the standard HART data frame, where extractions can be made to ensure identity and parameterisation data integrity is maintained.

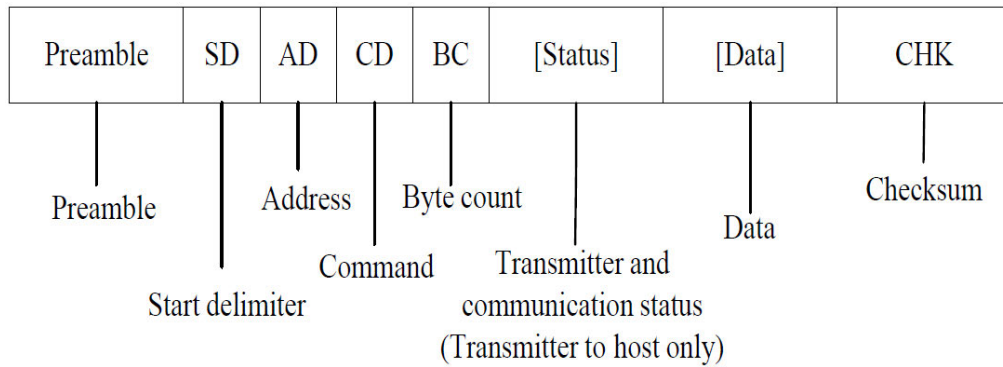


Figure 6: HART communication data frame (Li & Dong 2018, p. 2222).

4.2. Modbus TCP/IP

Communications via the Modbus TCP/IP protocol offers the same type of system checking ability. The Modbus Application Protocol packet (MBAP) shown in *Figure 7* displays the packet structure of Modbus TCP/IP, identifying components that may be extracted to authenticate the integrity of the data (Pricop et al. 2017, p. 681).

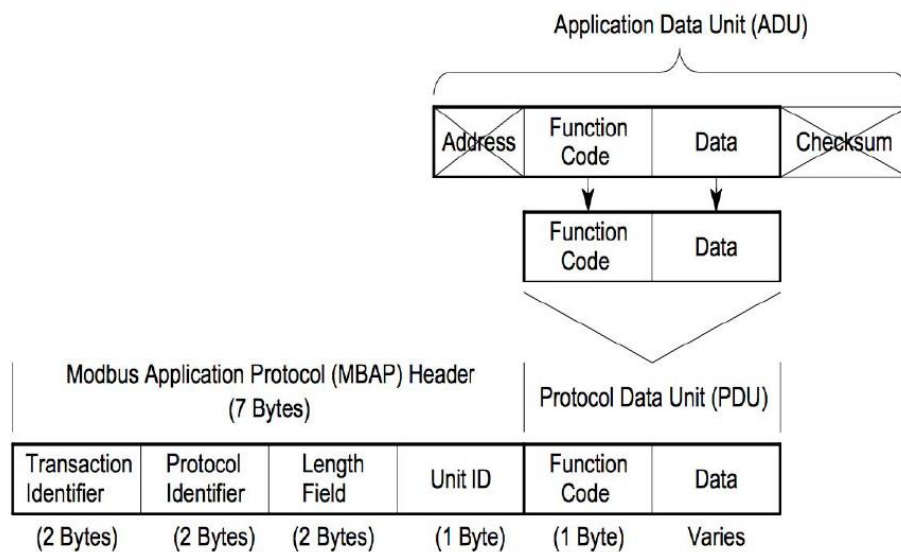


Figure 7: Modbus TCP/IP data packet structure (Pricop et al. 2017, p. 681).

4.3. PLC Communication Configuration

4.3.1. Site Standard Benchmarking

To ensure validity to site standard, Modbus DTM settings were taken from an installed PLC and placed into the benchmarking configuration. The data loading from configurations are listed in the table in appendix *E1 – Benchmarking Communications DTM Configuration*.

4.3.2. Advanced Authentication Mode

The advanced system, in conjunction with the DTM settings, used PLC derived function blocks (DFBs) to read explicit Modbus registers. As the ATV930 and ATV71 used the same Modbus address tables, their code was mirrored allowing for reading of the key parameters. The table in appendix E2 – *Advanced Authentication Communications Configuration* outlines the addressing used, where each “read” function block was enabled individually and sequentially.

Figure 8 to Figure 10 are excerpts from the PLC code which reflect the table in appendix E2 – *Advanced Authentication Communications Configuration*.

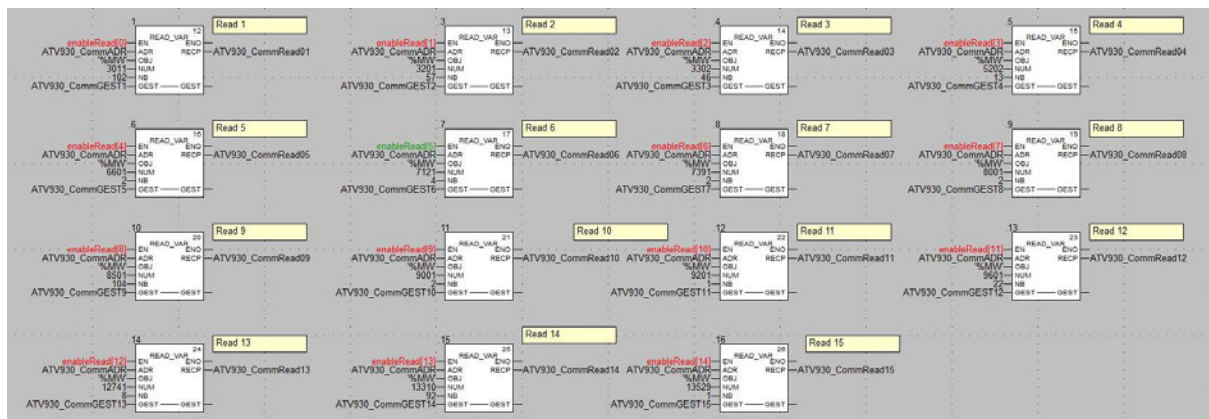


Figure 8: PLC code reading the registers of desired ATV930 parameters.

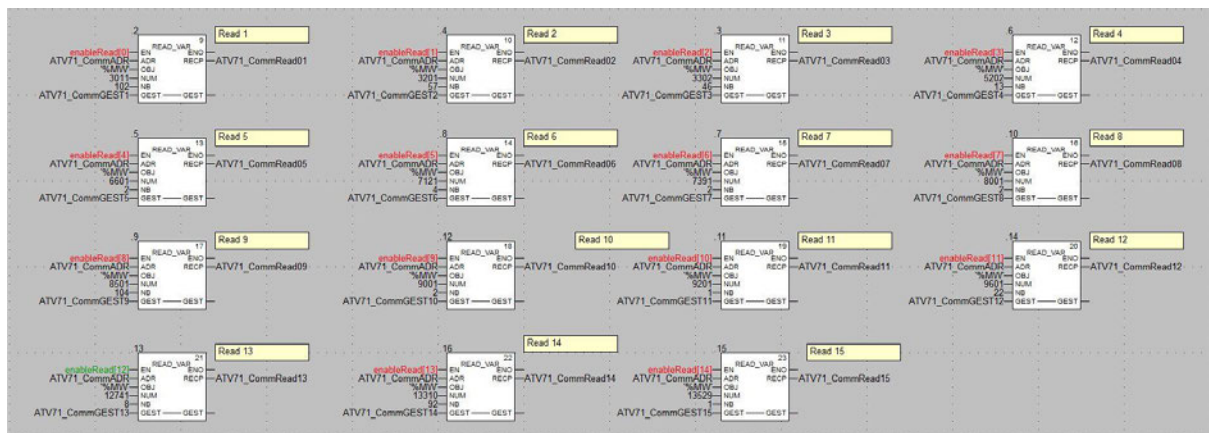


Figure 9: PLC code reading the registers of desired ATV71 parameters.

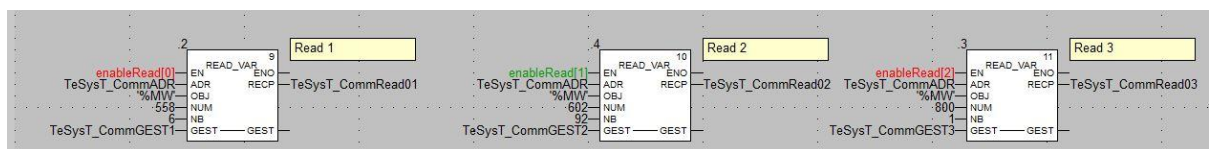


Figure 10: PLC code reading the registers of desired TeSys T parameters.

5. Results

The testing was split into two phases, “benchmarking” and “authentication applied” (AA). Each step in the two phases started at the minimal hardware, working up to the point where all hardware was connected. This is displayed in *Table 8*, where the “x” represents the use of an OT device, designated accordingly from configuration 1 to 9.

Table 8: OT device connection configuration map.

Configuration	M340 analogue input 1	M340 analogue input 2	M340 analogue input 3	STB analogue input 1	STB analogue input 2	ATV71	ATV930	TeSys T
1	-	-	-	-	-	-	-	-
2	x	-	-	-	-	-	-	-
3	x	x	-	-	-	-	-	-
4	x	x	x	-	-	-	-	-
5	x	x	x	x	-	-	-	-
6	x	x	x	x	x	-	-	-
7	x	x	x	x	x	x	-	-
8	x	x	x	x	x	x	x	-
9	x	x	x	x	x	x	x	x

5.1. Site Standard Benchmarking

The test bench was created where the mine’s current topology was replicated. Drawings were created to ensure a structured approach was taken and mitigate any wiring issues. The benchmarking drawings may be seen in appendix *C1 – Site Standard Benchmarking Schematics*.

Due to the minimal hardware available for testing, resulting from procurement costs, the results will need to be scaled when suitability for the mine implementation is means-tested.

5.1.1. Memory Usage

Table 9 displays the PLC memory usage between configuration 1 and 9. There is no great increase in memory consumption, where, through the full scale, there is an additional 20kB used, leaving more than 65MB free. The graphs pertaining to the memory data collection are in appendix *F1.1. – Benchmarking Memory Usage*.

Table 9: Benchmarking PLC memory consumption.

Configuration	User Data (kB)	Declared Data (kB)	Constants (kB)	Executable Code (kB)	Information (kB)	Upload (kB)	System (kB)	Data Dictionary (kB)	Free Memory (MB)	Program Data Utilisation	Saved Data Utilisation
1	20.59	19.31	512.0	138.54	174.70	27.68	1604.51	11.55	65.15	2.90%	1.30%
2	20.59	19.81	512.0	139.63	180.00	28.18	1604.51	11.55	65.14	2.90%	1.40%
3	20.59	19.79	512.0	139.79	180.05	28.18	1604.51	11.55	65.14	2.90%	1.40%
4	20.59	19.81	512.0	139.92	180.10	28.18	1604.51	11.55	65.14	2.90%	1.40%
5	20.59	19.97	512.0	141.62	183.62	28.83	1604.51	11.55	65.14	2.90%	1.40%
6	20.59	19.98	512.0	141.76	183.68	28.83	1604.51	11.55	65.13	2.90%	1.40%
7	20.59	20.10	512.0	145.17	193.12	29.44	1604.51	11.55	65.13	3.00%	1.40%
8	20.59	20.16	512.0	148.02	194.26	30.02	1604.51	11.55	65.12	3.00%	1.40%
9	20.59	21.31	512.0	150.13	199.55	30.53	1604.51	11.55	65.11	3.00%	1.40%

5.1.2. Network Performance

Table 10 displays the network performance, where it can be seen by the graphs in appendix F1.2. – *Benchmarking Network Performance*, that once the field motor control devices are introduced into the network, there are elements of instability added, mainly noted in the TCP packet round trip time (RTT) and TCP packet rate. This instability begins at configuration 7 until testing conclusion at configuration 9 and can be attributed to by the mismatch in device poll rates. Appendix E1 – *Benchmarking Communications DTM Configuration* shows the poll rates of the PLC remote I/O devices are set at 250ms, however the VSDs and MMR have varying poll rates of 300ms and 1500ms, depending on data priorities. This creates dynamic and competing timeslots that the devices must be polled at, instead of the semi-static 250ms from the I/O devices, which can cause issues due to the master-slave nature of Modbus communications. In saying this, added loading is extremely small across the board, with network utilisation, where the difference between the network utilisation from configuration 1 to configuration 9 increases from 0.15% to 0.98%. This proves that the benchmarking topology is creating a largely underloaded network. The poll rates are reasonably slow at ~500ms because the OFS poll rates are set at 250ms, as per site standard, cascading onto the PLC poll rates of 250ms. This will be altered during the advanced authentication process to speed up intrusion detection.

The TCP packet RTT was measured by subscribing or setting a SCADA Boolean tag equal to 1, sending it through OFS to the PLC changing a corresponding tag to the value of 1 then sending it back to SCADA where the Cicode mirrored the value. The duration of this was timed and visually represented on the SCADA page. The Cicode for this can be viewed in appendix D1 – *typ_CommsTest*.

Table 10: Benchmarking network performance testing.

Configuration	Accuracy	Network Utilisation	TCP Round Trip Time (ms)	TCP Packet Rate (packets/s)	TCP Packet Error Rate	PLC Processor Scan Times (ms)	OPC Success Rate
1	100%	0.03%	492	12	0%	1	100%
2	100%	0.15%	487	65	0%	1	100%
3	100%	0.15%	515	75	0%	1	100%
4	100%	0.15%	510	76	0%	1	100%
5	100%	0.58%	483	74	0%	1	100%
6	100%	0.58%	438	78	0%	1	100%
7	100%	0.98%	586	65	0%	1	100%
8	100%	0.87%	436	61	0%	1	100%
9	100%	0.98%	554	67	0%	1	100%

5.2. Advanced Authentication Mode

The schematics for the authentication applied topology may be viewed in appendix C2 – Advanced Authentication Mode Schematics.

Memory Usage

Table 11 displays the PLC memory usage between configuration 1 and 9. There is no great increase in memory consumption, where, through the full scale, there is an additional 28kB used, leaving approximately 64.87MB free. The graphs pertaining to the memory data collection are in appendix F1.1. – Benchmarking Memory Usage.

Table 11: Advanced authentication PLC memory consumption.

Configuration	User Data (kB)	Declared Data (kB)	Constants (kB)	Executable Code (kB)	Upload Information (kB)	Configuration (kB)	System (kB)	Data Dictionary (kB)	Free Memory (MB)	Program Data Utilisation	Saved Data
1	20.59	19.31	512.0	138.54	174.70	27.68	1604.51	11.55	65.15	2.90%	1.30%
2	20.59	21.26	512.0	150.56	222.05	47.02	1605.25	10.53	65.07	3.00%	1.40%
3	20.59	21.26	512.0	150.56	259.95	47.09	1605.62	10.53	65.04	3.10%	1.40%
4	20.59	21.42	512.0	151.50	266.59	47.78	1605.25	10.58	65.02	3.10%	1.40%
5	20.59	21.49	512.0	151.50	301.78	48.43	1605.25	10.58	64.99	3.20%	1.40%
6	20.59	21.52	512.0	151.63	317.52	48.48	1605.25	10.59	64.97	3.20%	1.40%
7	20.59	23.68	512.0	182.72	349.76	48.62	1605.23	12.43	64.91	3.30%	1.40%
8	20.59	25.94	512.0	194.38	363.10	49.34	1605.23	13.66	64.88	3.30%	1.50%
9	20.59	30.94	512.0	199.70	366.85	49.87	1605.62	14.70	64.87	3.30%	1.60%

5.2.1. Network Performance

Table 12: Advanced authentication network performance testing.

Configuration	Accuracy	Network Utilisation	Time (ms)	TCP Round Trip	TCP Packet Rate (packets/s)	TCP Packet Error Rate	PLC Processor Scan Times (ms)	OPC Success Rate
1	100%	0.03%	492	12	0%	1	100%	
2	100%	0.15%	638	66	0%	1	100%	
3	100%	0.15%	640	73	0%	1	100%	
4	100%	0.15%	688	76	0%	1	100%	
5	100%	0.58%	550	76	0%	1	100%	
6	100%	0.55%	689	64	0%	1	100%	
7	100%	0.58%	681	200	0%	1	100%	
8	100%	0.73%	488	243	0%	1	100%	
9	100%	0.84%	733	433	0%	2	100%	

5.2.2. Advanced Authentication Functionality

The image in *Figure 11* is a screenshot of the configuration interface within Schneider's Control Expert PLC software connected to the Vegapuls61 using the HART communication protocol.

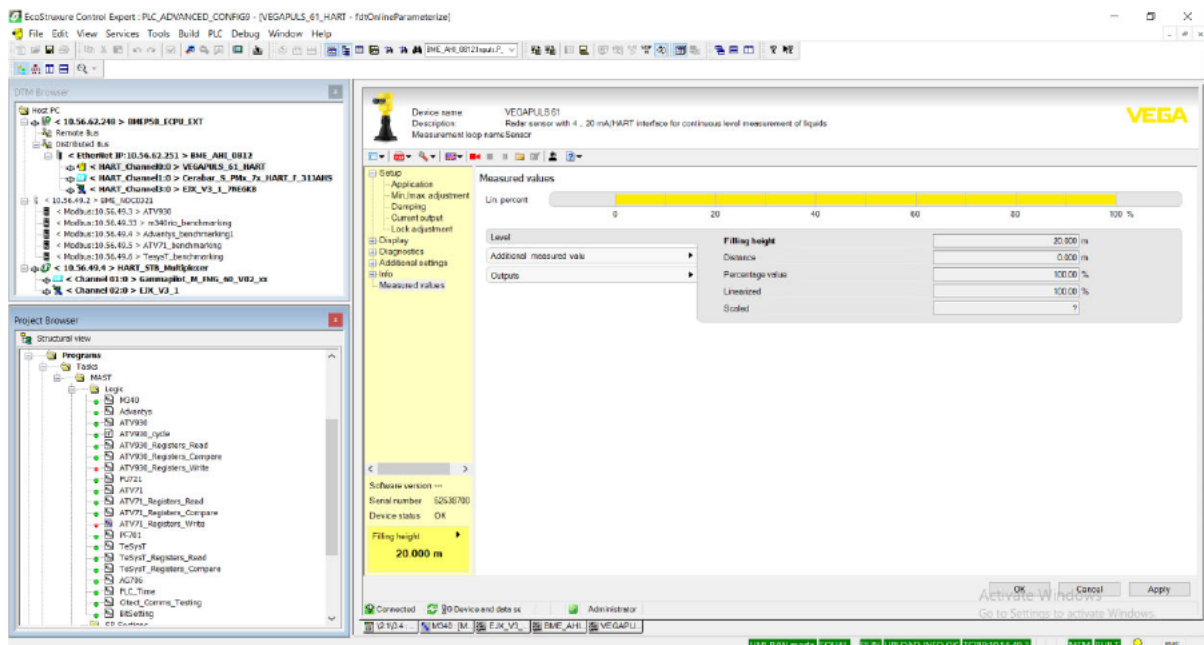


Figure 11: Screenshot of Schneider's Control Expert interface whilst connected to a Vegapuls61 radar.

Figure 12 exhibits the authentication actively detecting non-authorised changes to the ATV930, ATV71 and TeSys T MMR configurations. This activates an alarm on the SCADA and displays the parameter that has been changed, alerting the processing operator to the issue.

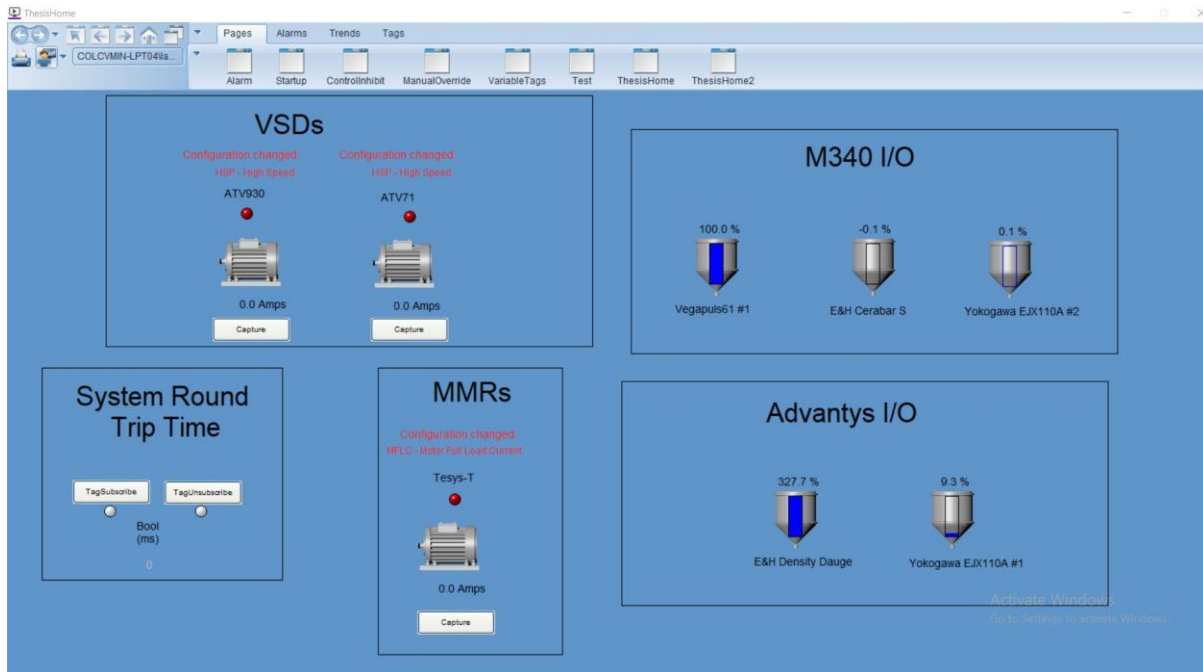


Figure 12: Screenshot of the SCADA mimic page showing alarms pertaining to unauthorised device configuration changes.

5.2.2.1. HART Instrumentation

Whilst the instrumentation using HART offered the capability of online parameterisation via the Control Expert PLC software, the DTM did not allow for the interrogation of individual registers pertaining to words associated with any parameters. This deemed the protocol unable to fulfill the automatic authentication required for auditing purposes. The online access to the instrument proved to be an extremely easy way to calibrate and configure the instrument online, removing the technicians from the vicinity of the process mediums that the instruments are employed to measure. The image in Figure 13 shows the interface where the Vegapuls61 may be configured remotely within the PLC program.

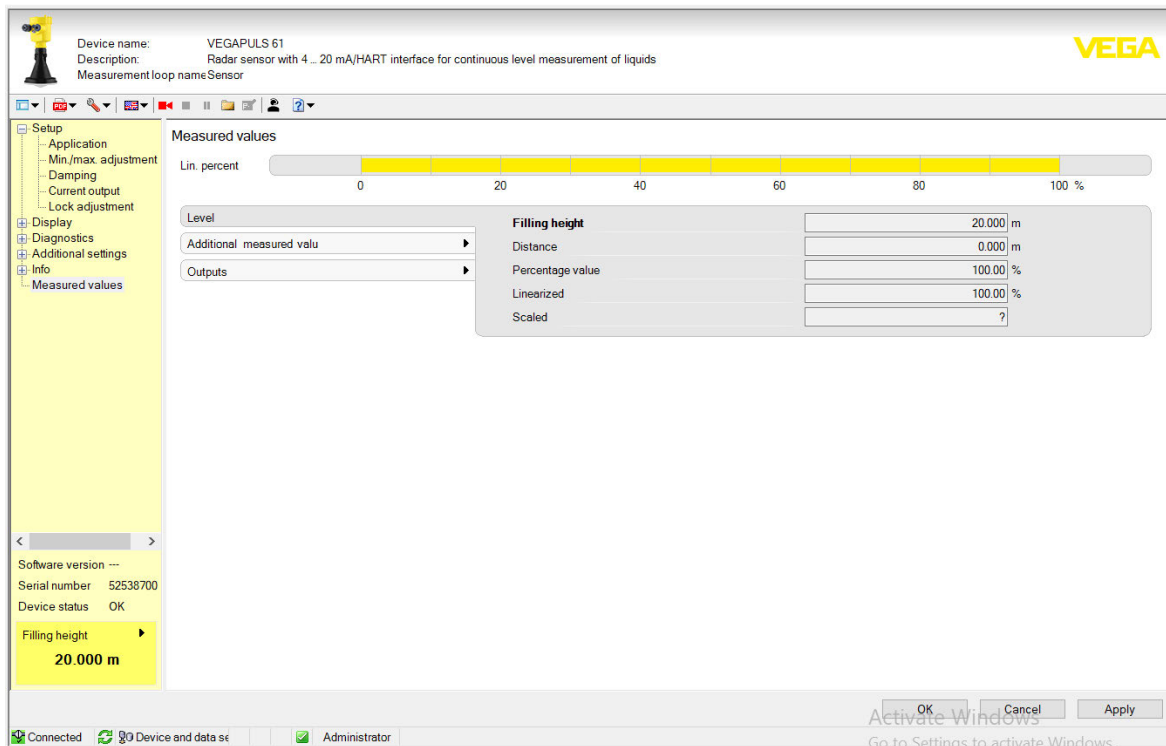


Figure 13: Vegapuls61 configuration interface within Schneider's Control Expert PLC software.

Another benefit of the system interfacing with the instrumentation is the ability to download and restore pre-configured parameter files, greatly reducing the duration of parameterisation activities. Timed upload of a configuration file took 1 minute and 2 seconds, compared to the 25 minutes for a technician to configure the instrument from factory default. *Figure 14* and *Figure 15* display screenshots, giving an understanding to the ease of downloading a configuration file from the Cerabar S device. The red circles represent where to execute mouse-clicks.

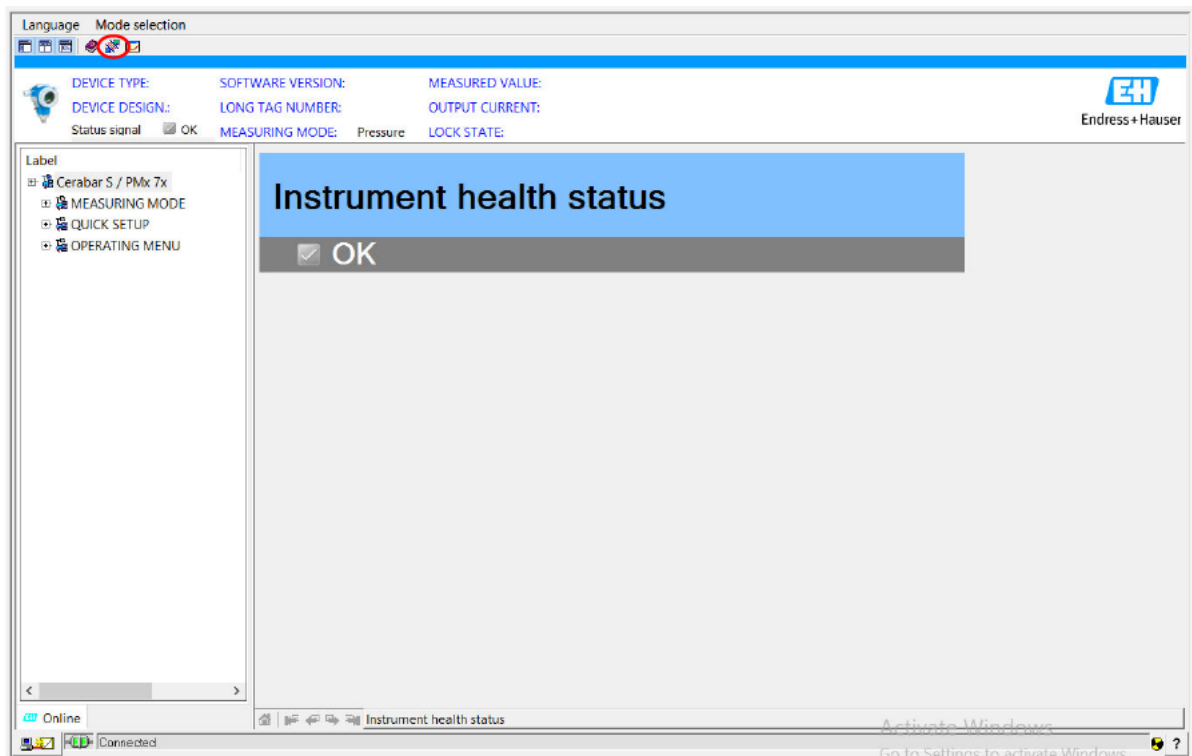


Figure 14: Cerabar S configuration interface within Schneider's Control Expert PLC software.

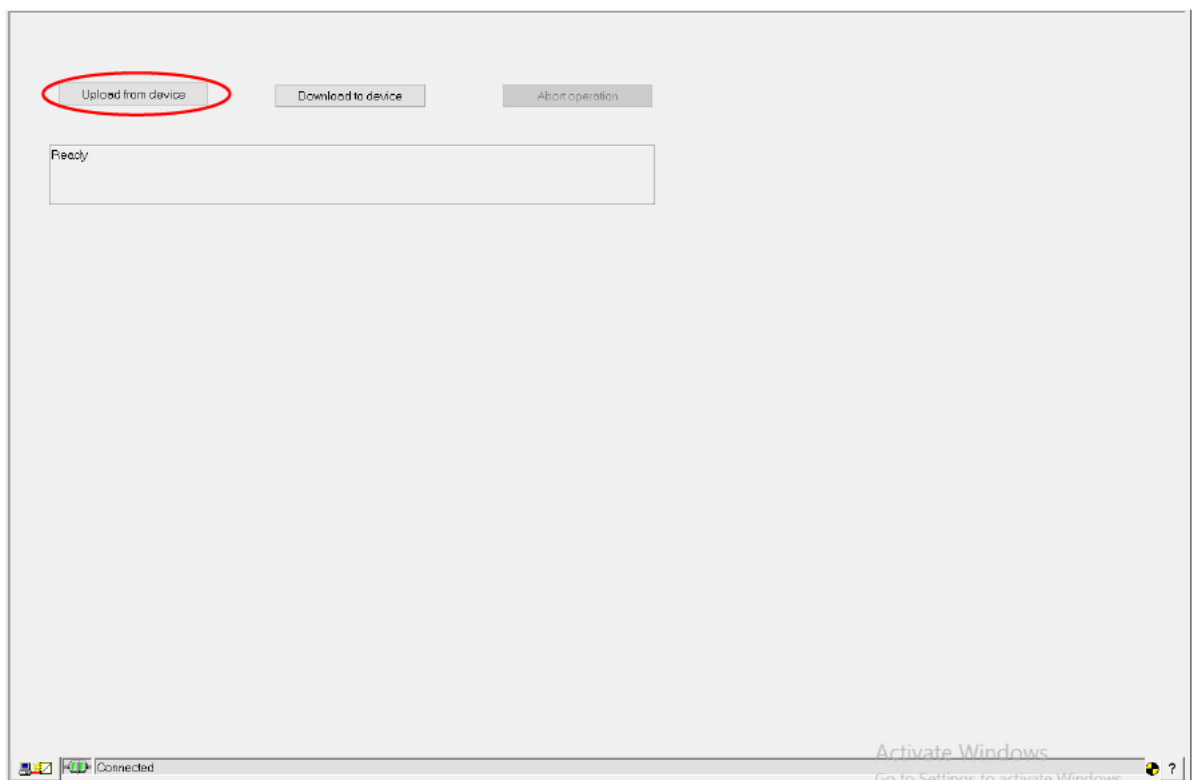


Figure 15: Cerabar S upload from device page within Schneider's Control Expert PLC interface.

5.2.2.2. Modbus TCP/IP Devices

The automatic detection of non-authorised configuration changes was a success. This led to the ability for operators and maintenance personnel to be alerted to parameter tampering via the site SCADA.

Unfortunately, issues with the PLC DTMs meant that the drives and MMR were unable to be connected to, as can be seen in *Figure 16*, where the configuration interface within Schneider's Control Expert PLC software is shown. The red circle highlights the disconnection message. Due to this deficiency, the drives and MMR were unable to be configured remotely using the interface, making it impossible to transfer configuration files to the devices, unlike the HART compatible instrumentation.

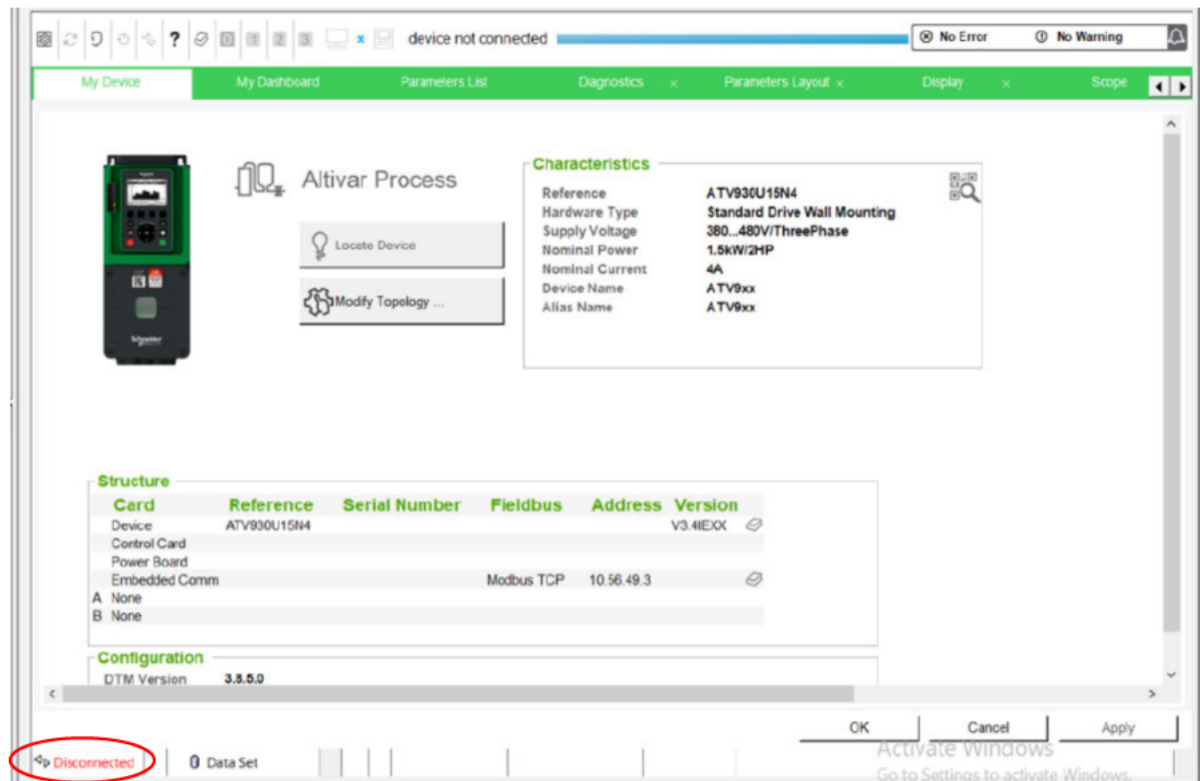


Figure 16: ATV930 configuration interface within Schneider's Control Expert PLC software.

5.3. Loading Comparison Between Modes

The plots from *Figure 17* to *Figure 20* display the comparisons in results from the testing obtained in *F1 – Benchmarking* and *F2 – Advanced Authentication*, where the yellow bar at configuration 6 marks the final test before the motor control devices were added to the network.

Only the comparisons where there are noteworthy changes have been shown, as other comparison results gave negligible disparities. These plots show that whilst there are increases in loading to the network, there are no concerns with the system deteriorating to a point of failure – the system is extremely underloaded. It is understandable that with the increase in parameter reading for the Modbus TCP/IP devices and the addition of a new protocol, there are increases between the two modes.

Figure 17 shows that once the motor control devices were added, those which employ the Modbus TCP/IP communication protocol, the results increased marginally between the two modes.

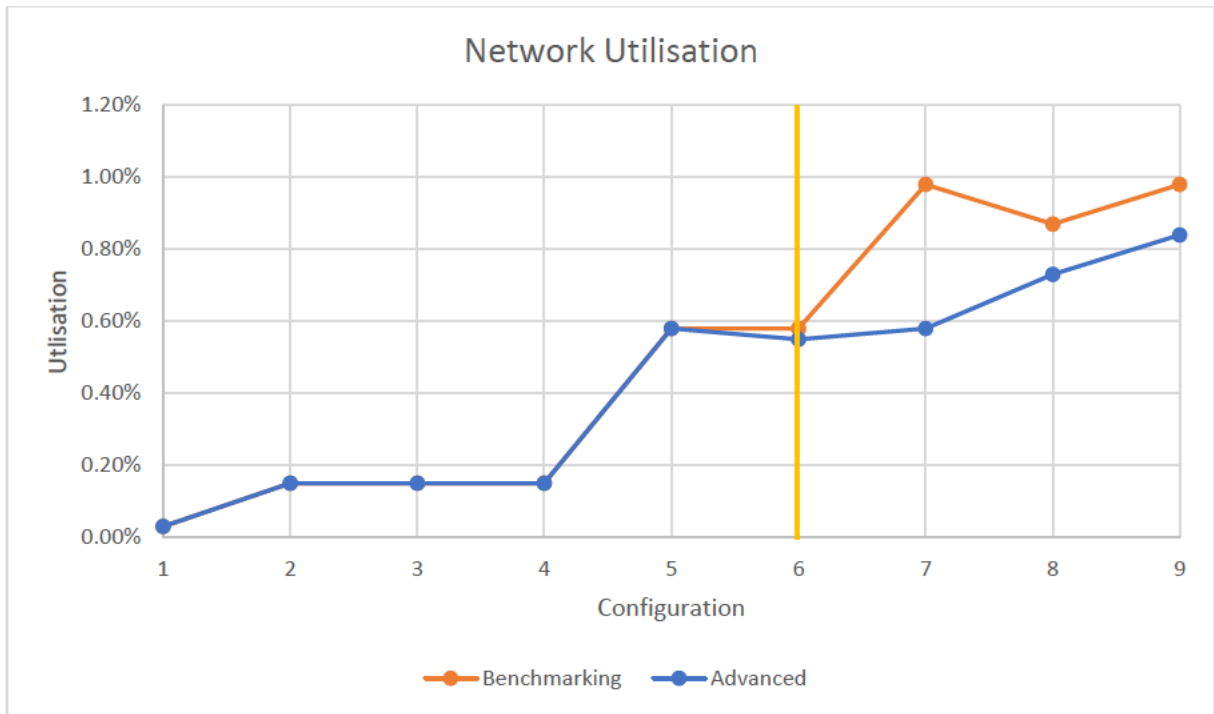


Figure 17: Network utilisation for benchmarking vs advanced authentication mode.

The TCP packet round trip time (RTT), is elevated from the advanced mode to benchmarking as soon as devices are connected to the system (configuration 2 onwards). Due to the extra loading on the system communications, this is to be expected as the test bool that is being sent around from the SCADA, through the OPC, into the PLC and back must be prioritised, therefore with more packets of data comes delayed positioning. This can be viewed below in *Figure 18*.

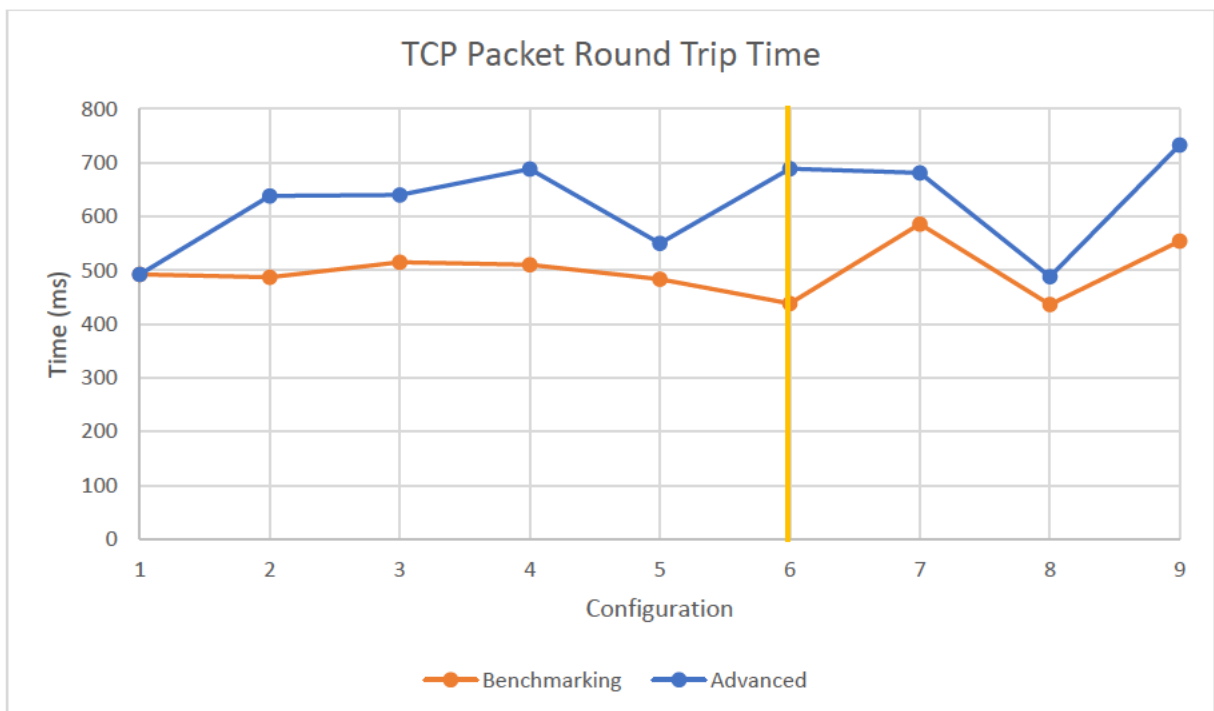


Figure 18: TCP packet round trip time for benchmarking vs advanced authentication mode.

Once the motor control devices using Modbus TCP/IP were added, the TCP packet rate greatly increased immediately, then reduced over time. Shown in *Figure 19* is the maximum packet rates detected through the network communications card. This is of minimal concern as the increase was fleeting and is swamped by the 5,500 packets per second capacity of the PLC's communications card.

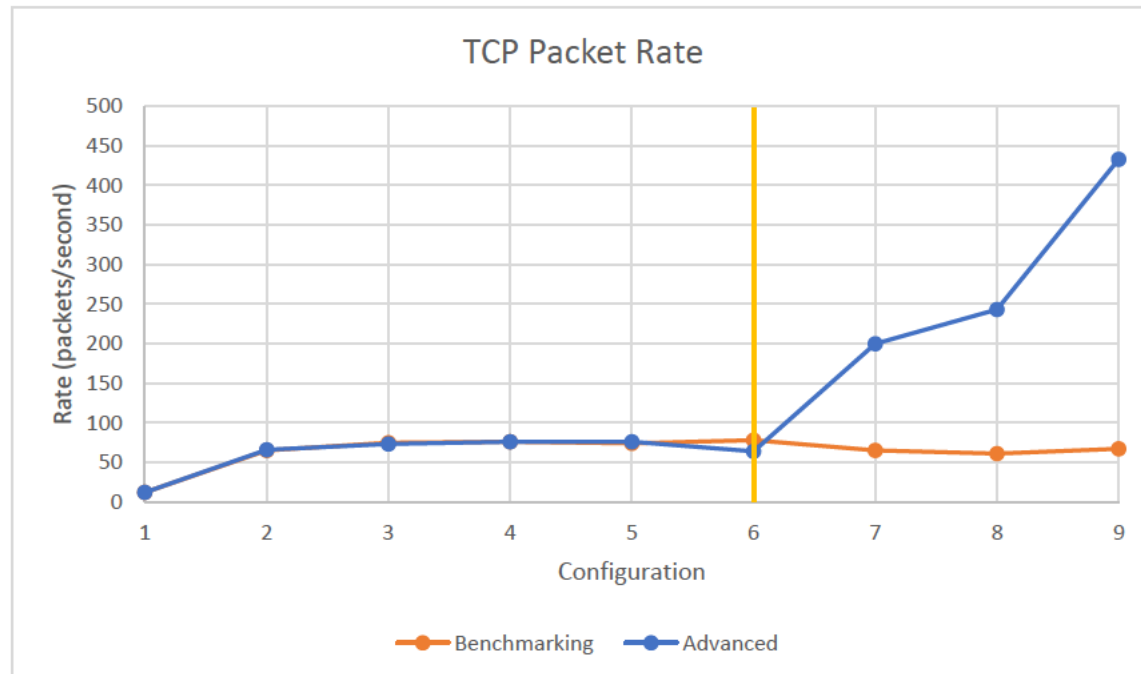


Figure 19: Maximum TCP packet rates for benchmarking vs advanced authentication mode.

As can be seen in *Figure 20*, the memory consumption is barely affected. Whilst there are minor differences between the benchmarked and advanced mode testing, this is negligible.

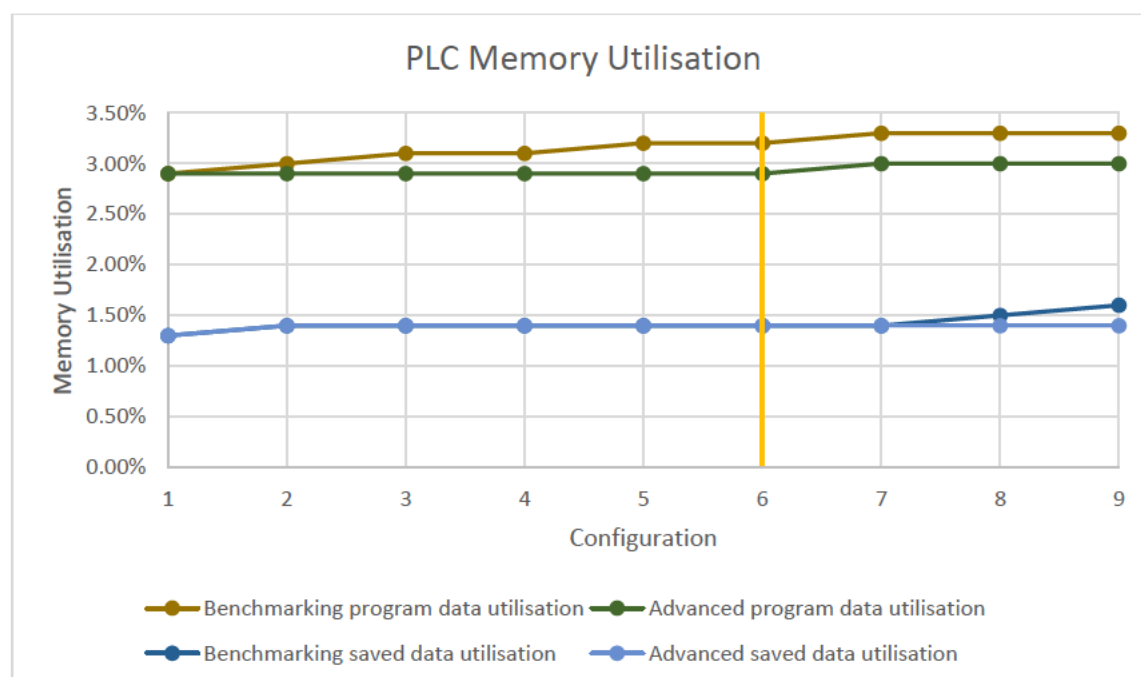


Figure 20: PLC memory utilisation comparison for benchmarking vs advanced authentication mode.

6. Conclusion

6.1. Project Outcomes

The project outcomes are listed below. Most project objectives were achieved, where technical and time limitations prevented the full implementation of the project.

6.1.1. Objective 2.11a Outcome

Automatically detect configuration changes for instrumentation and motor control devices:

Automatic detection of configuration changes was achieved on the motor control devices using Modbus TCP/IP; however, the same functionality with the instrumentation communicating via the HART protocol was unattainable. This was due to the inability to access registers along the data frames pertaining to their particular parameters.

6.1.2. Objective 2.11b Outcome

Configure instrumentation and motor control devices remotely, securely, accurately and fast:

The instrumentation communicating via the HART protocol was successful in all elements of the objective. Effective configuration ability was attained using Schneider's Control Expert interface remotely, securely, accurately, and fast. Configuration files were able to be employed, ensuring repeatable parameters were used regarding elements like tank profiles, etc., with the ability to calibrate for any small discrepancies between the old and new instrument component characteristics. This increased the speed of configuration from approximately 25 minutes to 1 minute and 2 seconds when comparing manual configuration to configuration file upload. Implementing the same system for the motor control devices using Modbus TCP/IP, was unsuccessful due to the inability to enter "online mode" within Schneider's Control Expert configuration interface.

6.1.3. Objective 2.11c Outcome

Determine network and memory loading increases due to advanced methods of monitoring and configuring instrumentation and motor control devices:

The impacts to the network and PLC memory consumption were negligible, where utilisation remained extremely low throughout the testing regime, with large memory capacity remaining.

6.1.4. Objective 2.11d Outcome

Determine suitability of site implementation:

The results of the testing regime prove favourable for site implementation, where no adverse effects to the network appear to be present. This would greatly improve turnaround times of instrumentation replacements and ensure tamper-proofing of motor control device parameters.

6.2. Further Work

It is suggested that attempts be made to incorporate the configuration interface of the instrumentation into SCADA, as its access is currently limited to within the Control Expert software, where there is currently very restrictive user access. This will require some research to determine if it is required for DTMs to be installed on all Citect client computers throughout site. There may be an opportunity to modify this to improve flexibility of the system.

There may also be further opportunities to write parameters to the drives with additional PLC programming. With that, refinement of the PLC code is also possible, aimed to improve speed of network and PLC computing. This will require a testing regime to ensure the impacts on the network are also negligible.

Within industry, this information may also be made available, where the company can look at implementing these methods across various assets that utilise the same PCN architecture. Conversely, it may give external companies the framework for employing this methodology for their unique process control networks.

Email notifications of changed parameters will be a key functionality to transpire from this project, where we can actively monitor key parameters, alerting the key stakeholders of unauthorised changes.

7. References

- ABB Automation Products GmbH 2005, *DCS 800 - Hardware Manual*, Lampertheim, Germany, viewed 7/10/2022, <<https://library.e.abb.com/public/354318dff16891cbc1257b0c00545df7/3ADW000194R0201%20DCS800%20Hardware%20Manual%20e%20b.pdf>>.
- ABB Automation Products GmbH 2009, *615 series Technical Manual*, Vaasa, Finland, viewed 7/10/2022, <https://library.e.abb.com/public/0bf06cb26c50628cc1257b130056c974/RE_615_tech_756887_ENb.pdf>.
- Ao, Q 2020, 'An intrusion detection method for industrial control system against stealthy attack', *2020 7th International Conference on Dependable Systems and Their Applications (DSA)*, IEEE, pp. 157-61.
- BMA 2020, 'CVM Standard - Blueprint Management', Engineering, 09/2021, CVM-STD-15758741, viewed 7/10/2022, <internal>.
- BMA 2021, 'CVM Standard - Electrical Preferred Equipment List', Engineering, 06/2021, CVM-STD-0029, viewed 7/10/2022, <internal>.
- Business Insider 2023a, *Coal Price*, viewed 2/09/2023, <<https://markets.businessinsider.com/commodities/coal-price>>.
- Business Insider 2023b, *Australian Dollar - United States Dollar*, viewed 2/09/2023, <<https://markets.businessinsider.com/currencies/aud-usd>>.
- Feinman, T, Goldman, D, Wong, R, Cooper, N & PricewaterhouseCoopers, L 1999, *Security basics: a whitepaper*, Unpublished Paper, Resource Protection Services, PricewaterhouseCoopers, London, viewed 1/10/2022, <<https://www.networkdls.com//Articles/security101.pdf>>.
- FieldComm Group n.d., 'Kaneka Employs FOUNDATION Fieldbus in Demanding Chemical Plant Applications', viewed 1/10/2022, <https://www.fieldcommgroup.org/sites/default/files/imce_files/technology/documents/kaneka_case_study.pdf>.
- HART Communication Foundation 2013, 'HART Communication Application Guide', Austin, TX, USA, viewed 7/06/2023, <http://fieldcommgroup.org/site/default/files/imce_files/technology/documents/HART_ApplicationGuide_r7.1.pdf>.

Li, T & Dong, Z 2018, 'Design and implementation of field bus device management system based on hart protocol', *2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, IEEE, pp. 2221-5.

Pricop, E, Fattahi, J, Parashiv, N, Zamfir, F & Ghayoula, E 2017, 'Method for authentication of sensors connected on modbus tcp', *2017 4th International Conference on Control, Decision and Information Technologies (CoDIT)*, IEEE, pp. 679-83.

Queensland Government 2017, *Coal Mining Safety and Health Regulation 2017*, Do Resources, viewed 5/10/2022, <<https://www.legislation.qld.gov.au/view/pdf/asmade/sl-2017-0165>>.

Sasaki, H & Ueda, K 2007, 'Design and deployment of wireless monitoring system for 4-20mA current loop sensors', *2007 Fourth International Conference on Networked Sensing Systems*, IEEE, pp. 73-6.

Schneider Electric Pty Ltd 2015, *How can I... Integrate HART into eX80 Architecture?*, Rueil-Malmaison, France, viewed 1/10/2022, <<https://ckm-content.se.com/ckmContent/sfc/servlet.shepherd/document/download/0691H00000DwEXBQA3>>.

Schneider Electric Pty Ltd 2022a, *Modicon M580 Hardware Reference Manual*, Rueil-Malmaison, France, viewed 7/10/2022, <https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=EIO0000001578.12.pdf&p_Doc_Ref=EIO0000001578&_ga=2.1077363.313262203.1665089790-138762825.1664079627>.

Schneider Electric Pty Ltd 2022b, *TeSys T LTMR Motor Management Controller User Guide*, Andover, MA, USA, viewed 7/10/2022, <https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=DOCA0127EN_02.pdf&p_Doc_Ref=DOCA0127EN&_ga=2.62888046.313262203.1665089790-138762825.1664079627>.

Tang, C 2017, *Key performance indicators for process control system cybersecurity performance analysis*, US Department of Commerce, National Institute of Standards and Technology.

Appendix A – Project Specification

ENG4111/4112 Research Project

Project Specification

For: Clinton Lauriston

Title: Industrial Operational Technology Error Detection, Reporting and the Subsequent Network Performance Impacts

Major: Electrical/Electronics

Supervisors: John Leis

Enrollment: ENG4111 – EXT S1, 2023

ENG4112 – EXT S2, 2023

Project Aim: Develop a method to centrally maintain and automatically audit industrial operational technology parameters via an easy to use and user-protected interface. Investigate the impacts of the subsequent communication speed and data volume loading on the identified coal mine's process control network to determine capacity.


Programme: Version 5, 24th February 2023

1. Conduct initial background research of previously undertaken projects/technology.
2. Conduct interviews with key stakeholders.
3. Undertake an audit on the operational technology devices at the identified coal mine
4. Assess hardware requirements and costs, selecting hardware and suitable software.
5. Construct a test environment using the site standard process control network architecture and topologies to determine loading baseline of current system and collect baseline data.
6. Conceptualise a suitable topology and network architecture for the proposed system.
7. Augment PLC function block code and SCADA Cicode projects to test functionality of the newly proposed system and incrementally add devices – document results
8. Implement PLC code to undertake compliance checks and report unauthorised parameter changes and test.
9. Test configuration speed – technician local vs technician using PLC/SCADA
10. Determine suitability of new system to be rolled out to site.

If time and resource permit:

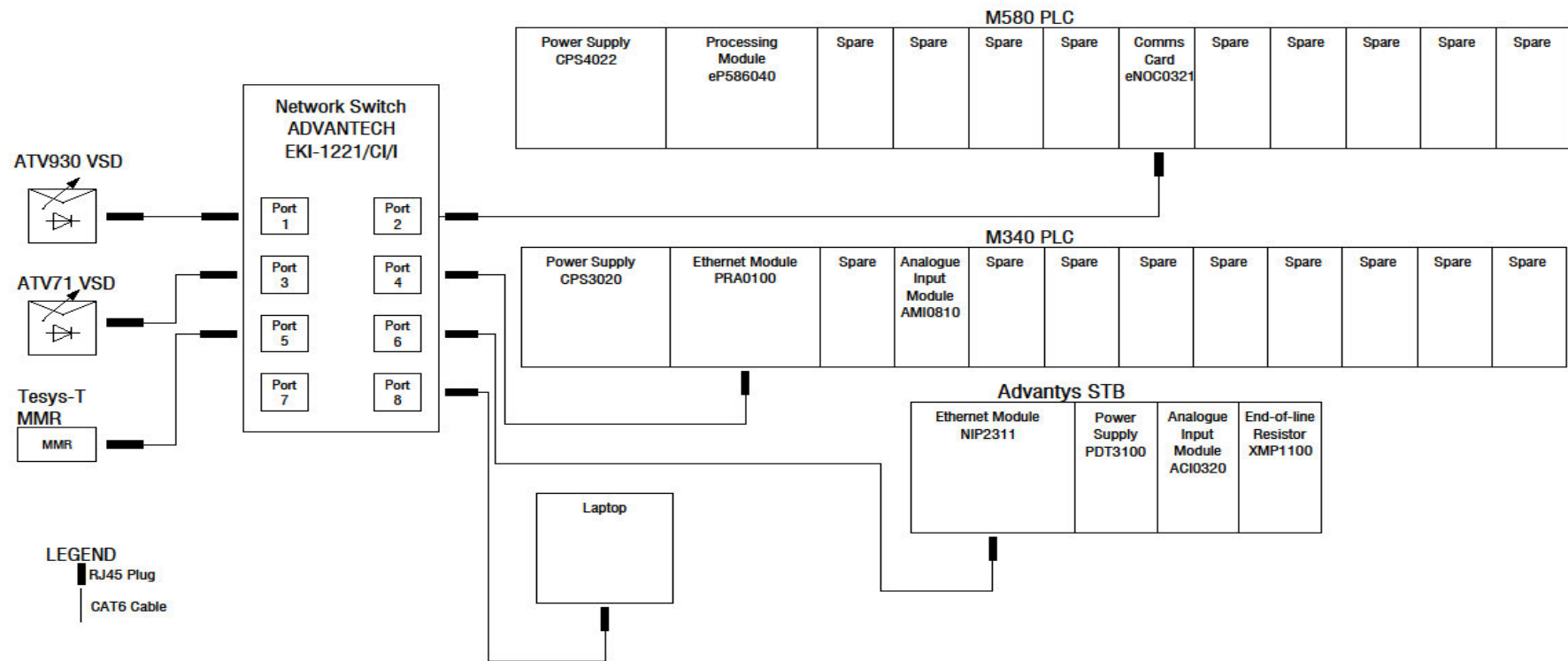
11. Add new architecture to live-plant non-production critical area.
12. Change “live” PLC and SCADA project with new functionality to become active in the area.
13. Test to determine if successful in live plant and monitor performance.

Appendix B – Risk Assessment

2997	RISK DESCRIPTION		STATUS	TREND	CURRENT	RESIDUAL
	Lauriston_Clinton_DissertationRA		Live		Low	Not Assessed
RISK OWNER		RISK IDENTIFIED ON	LAST REVIEWED ON		NEXT SCHEDULED REVIEW	
Clinton Lauriston		26/08/2023	26/08/2023		26/08/2024	
RISK FACTOR(S)	EXISTING CONTROL(S)	CURRENT	PROPOSED CONTROL(S)	TREATMENT OWNER	DUE DATE	RESIDUAL
Installing equipment	Control: Buddy system when carrying large instruments - group lift Control: Wear gloves unless unsafe to do so	Low				
Installing equipment	Control: Isolations when LV conductors accessed, including verification of de-energised state. Control: 30mA RCDs used on circuits. System complies to AS/NZS3000 standards Control: Licensed electrician to undertake electrical work	Low				
Theft of hardware	Control: Work area locked to reduce accessibility of thesis hardware Control: Area labelled to advise that parts are not to be taken for any other tasks.	Very Low				
Hot weather exposure trying to find spare parts	Control: Take regular breaks. Follow site processes. Wear hat. Limit time in direct sun exposure. Share task with other person. Maintain buddy system to	Low				

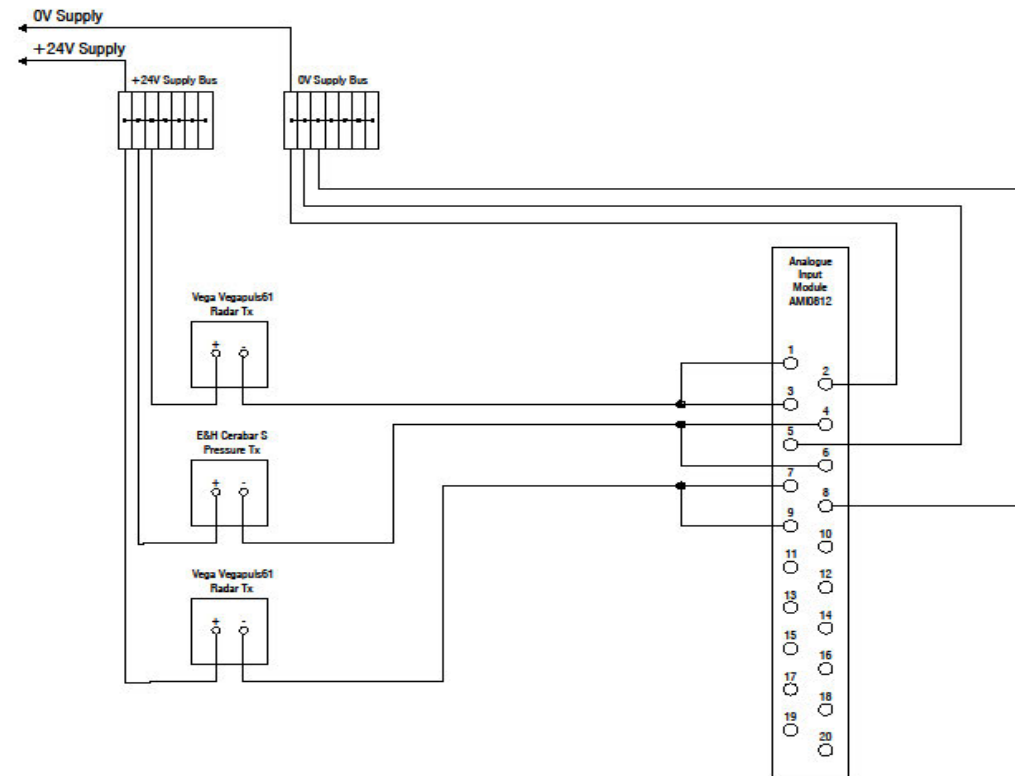
Appendix C – Drawings

C1 – Site Standard Benchmarking Schematics



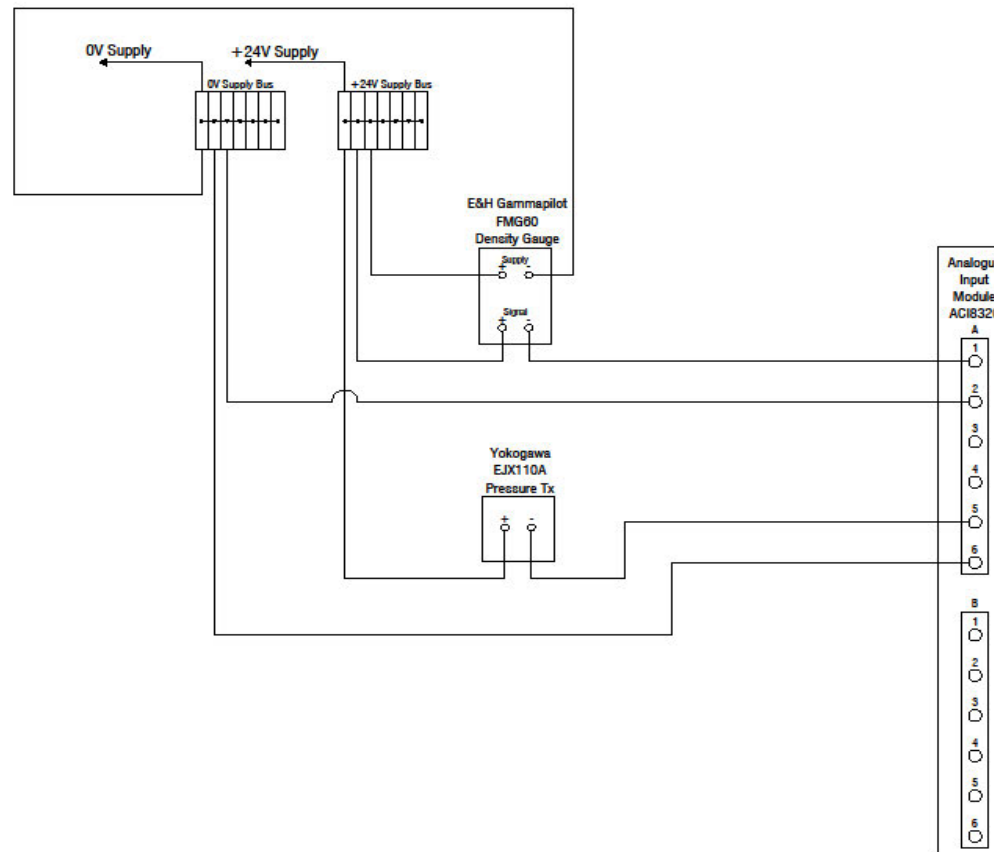
BENCHMARKING - COMMUNICATIONS TERMINATION DIAGRAM

Drawing # - B1



BENCHMARKING - M340 PLC I/O WIRING DIAGRAM

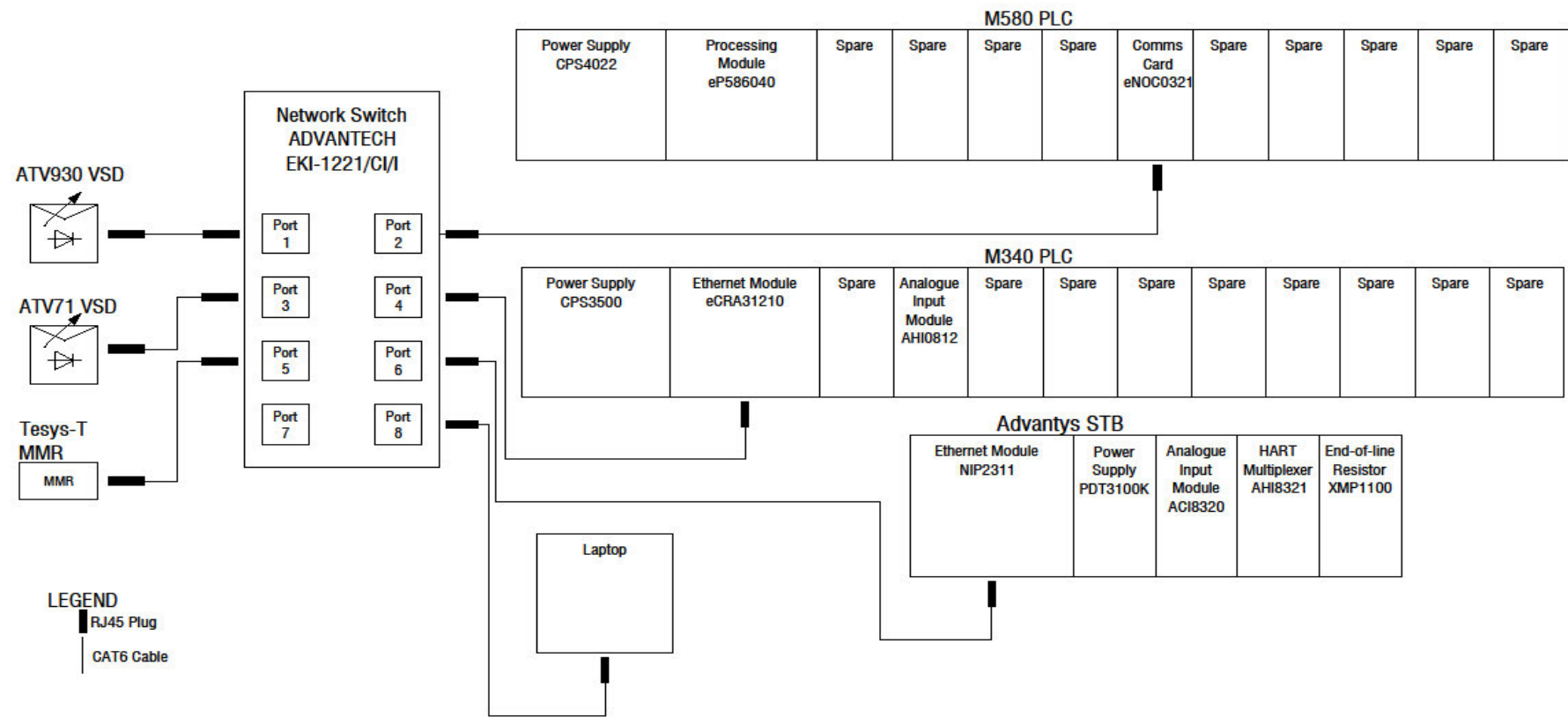
Drawing # - B2



BENCHMARKING- ADVANTYS STB PLC I/O WIRING DIAGRAM

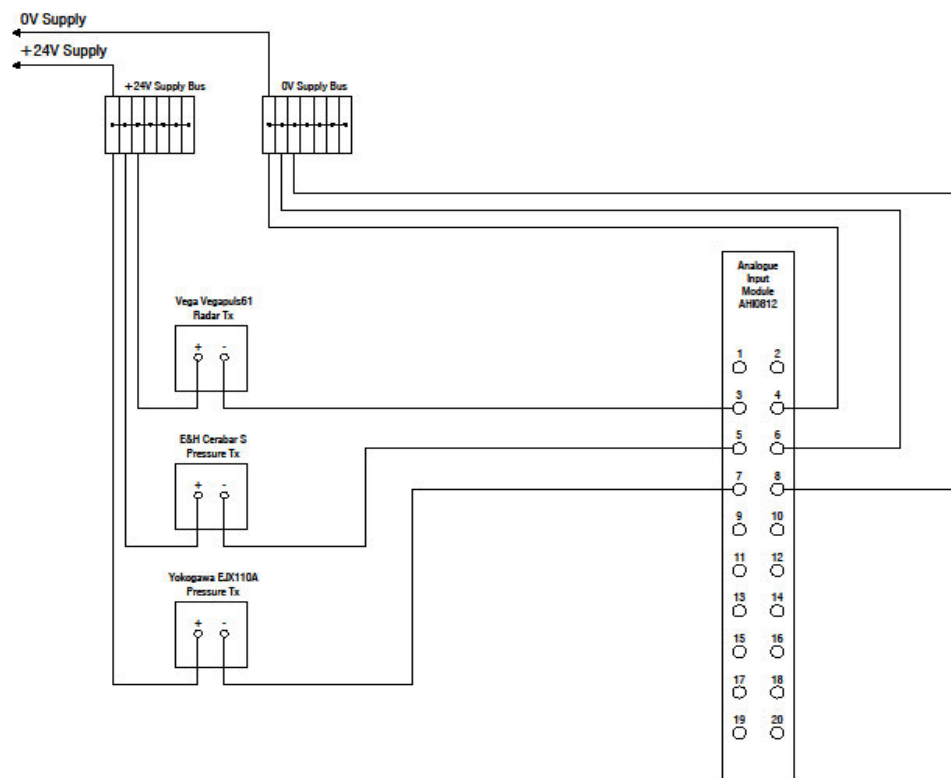
Drawing # - B3

C2 – Advanced Authentication Mode Schematics



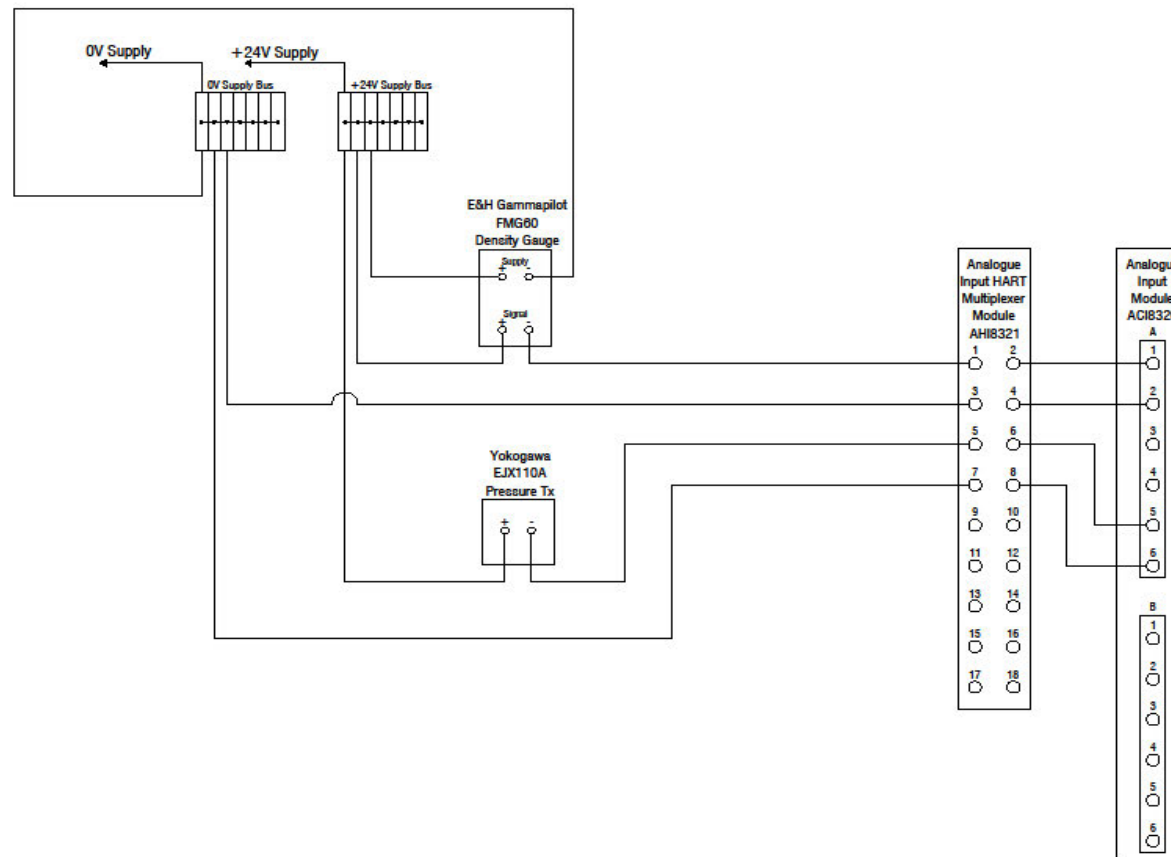
ADVANCED AUTHENTICATION - COMMUNICATIONS TERMINATION DIAGRAM

Drawing # - A1



ADVANCED AUTHENTICATION - M340 PLC I/O WIRING DIAGRAM

Drawing # - A2



ADVANCED AUTHENTICATION - ADVANTYS STB PLC I/O WIRING DIAGRAM

Drawing # - A3

Appendix D – Cicode

D1 – typ_CommsTest

```

/*****

*

* File:          typ_CommsTest.ci

*

*****/

/*****

*

* Functions:

*               typ_CommsTest                      -
1.0

*               typ_CommsTestCallback              - 1.0
*               typ_CommsTestReport                - 1.0
*               typ_CommsTestClearTags              - 1.0
*

*****/

// Define module variables

!-----
-----

! Function:      typ_CommsTest

!

! Author:        Clinton Lauriston,                - 1.0

!

! Date/Revision: 31 July      2023,                - 1.0

!

! Description:   Copys file from server to local folder

!

!

! Parameters:    sTagPrefix The name of the tag eg Thesis_SCADA_Citect_Real

!               iMode
```

```

!                                     1 TagSubscribe
!                                     2 TagUnsubscribe
!
!

```

! Returns: 0 (zero) if successful, otherwise an error is returned.

```

!
!-----
-----

```

INT FUNCTION

```

    typ_CommsTest(STRING sTagPrefix , INT iMode)
    INT    iReturn = 0;

    //TagSubscribe(STRING TagName [, INT PollTime] [, STRING ScaleMode] [, REAL
Deadband] [, STRING Callback] [, INT Lightweight])
    INT    iHandle = 0;
    STRING    sTagName    = "";
    INT    iPollTime      = 250;
    STRING    sScaleMode   = "Eng";
    REAL    rDeadband      = -1.0;
    STRING    sCallback     = "typ_CommsTestCallback";
    INT    iLightWeight = 0; //For a client to retrieve quality and value timestamps for a tag, you
should explicitly specify that a full tag value is required by setting this option to 0.
    INT    errorcode       = 0;
    INT    convValue       = 0;
    INT    convQual        = 0;
    INT    convTime        = 0;

    //DebugMsg("TagSubscribe ----- " + ErrMsg(IsError()));
    //DebugMsg(sTagPrefix + " " + IntToStr (iMode));

    SELECT CASE iMode
        CASE 1 // TagSubscribe
            iHandle = TagRead("lv" + sTagPrefix + "_H");
                                TagWrite("lv"      +      sTagPrefix      +
"_T1",SysTime());//Gets the Vijeo Citect internal system millisecond counter.

```



```

        IF iHandle = 0 THEN
            iHandle = TagSubscribe(sTagPrefix + "_I",
iPollTime, sScaleMode, rDeadband, sCallback, iLightweight); //Subscribes a tag so that Cicode
functions can be called when a tag's value changes.

            TagWrite("lv" + sTagPrefix + "_H",iHandle);

            iReturn = iHandle;

        END

        TagWrite(sTagPrefix + "_Y",1);
        //errorcode = TagWrite(sTagPrefix + "_Y",1);

        //DebugMsg("TagWrite ----- " + ErrMsg(errorcode));

CASE 2 // TagUnsubscribe
    iHandle = TagRead("lv" + sTagPrefix + "_H");
    iReturn = TagUnsubscribe(iHandle);
    typ_CommsTestClearTags(sTagPrefix);

CASE ELSE
    RETURN -1;

END SELECT

RETURN iReturn;

END

!-----
!-----
! Function:          typ_CommsTestCallBack
!
! Author:             Clinton Lauriston,                - 1.0
!
! Date/Revision:      31 July        2023,                - 1.0
!
! Description:        Record tag update times
!
!
! Parameters:          iHandle is the subscription that raised the event.  this  is  passed  to  function
when callback is called.

```

!

!

! Returns: None.

!

!-----

FUNCTION

 typ_CommsTestCallBack(INT iHandle)

 TIMESTAMP vtValueTimeStamp; // The value timestamp, which will access the
timestamp of when the value last changed.

 QUALITY qQuality; // The quality, which will access the quality
quality of the value, either GOOD, UNCERTAIN or BAD.

 INT vValue; // The value, which will access the data value
of the tag or element.

 STRING sTagName;

 STRING sTagPrefix;

 INT iT1;

 INT iT2;

 INT iTd;

 STRING sTimeStamp;

 STRING sQuality;

 STRING sIO;

 sTagName = SubscriptionGetInfo(iHandle, "TagName");

 vtValueTimeStamp = SubscriptionGetTimestamp(iHandle,
"ValueTimestamp"); // The timestamp when value of the tag last changed.

 qQuality = SubscriptionGetQuality(iHandle);
// The quality for a subscribed tag. On error, QUAL_BAD.

 vValue = SubscriptionGetValue(iHandle);
// Returns a value of a subscribed tag.

 // Thesis_PLC_Citect_Real_I

 sTagPrefix = StrLeft(sTagName,22); // PC404_Citect_Real

 iT1 = TagRead("lv" + sTagPrefix + "_T1");

```

iT2 = SysTime();
TagWrite("lv" + sTagPrefix + "_T2",iT2);

iT2 = SysTime();
iT2 = iT2 - iT1;
TagWrite("lv" + sTagPrefix + "_TD",iT2);

sTimeStamp = TimestampFormat(vtValueTimeStamp , "dd/MM/yyyy
hh:mm:ss.fff");
TagWrite("lv" + sTagPrefix + "_VT",sTimeStamp);

sQuality = QualityToStr(qQuality , -1, 0);
TagWrite("lv" + sTagPrefix + "_Q" ,sQuality);

sIO = "TODO"
TagWrite("lv" + sTagPrefix + "_IO",sIO);

DebugMsg( sTagName + " - Tag update time was " + IntToStr(iTD) + "ms");
Prompt(IntToStr(iTD) + "ms " + sTagPrefix);

// Thesis_PLC_Citect_Real
// Log Data to CSV file
// typ_CommsTestReport(sTagPrefix);
END

```

```

!-----
!
! Function:          typ_CommsTestReport
!
! Author:            Clinton Lauriston,          - 1.0
!
! Date/Revision:     31 July      2023,          - 1.0
!
! Description:       Record data to file

```

```

!
!
! Parameters:      sPC      The name of the PLC eg PC404
!
!
! Returns:         0 (zero) if successful, otherwise an error is returned.
!
!-----
-----

```

INT

FUNCTION typ_CommsTestReport(STRING sTagPrefix)

INT iReturn = -1; // 0 (zero) if successful, otherwise an error code is returned.

INT hFile;

STRING sDate;

STRING sTime;

STRING sPage;

STRING sUser;

STRING sIP;

STRING sPC;

STRING sMsgLog;

REAL rTag_Y;

REAL rTag_I;

INT iTag_T1;

INT iTag_T2;

INT iTag_TD;

INT iTag_H;

STRING sTag_VT;

STRING sTag_Q;

STRING sTag_IO;

STRING sTagName;

// Get Date

sDate = Date(9);

```
sDate = StrPad(sDate," ",13);// (Date,14) DD/MM/YYYY (Date, n) The date (in short format)
when the command was issued (dd:mm:yy).
```

```
// Get Time
```

```
sTime = StrPad(TimeToStr(TimeCurrent(),1), " ",11);
```

```
sTime = StrPad(sTime," ",15);// (TimeLong,16) HH:mm:ss (TimeLong,n) The time (in long
format) when the command was issued (hh:mm:ss).
```

```
// Get User name
```

```
//sUser = typ_UserFullName();
```

```
sUser = UserInfo(1); // need to use same format as command buttons
```

```
sUser = StrPad(sUser," ",17);// (UserName,18)
```

```
// Get the name of this PC from the INI file
```

```
sPC = ParameterGet("CVM", "PC", "PC Name Error");
```

```
sPC = StrPad(sPC," ",16);
```

```
// Get the IP Address of this PC from the INI file
```

```
sIP = ParameterGet("CVM", "IP", "PC IP Error");
```

```
sIP = StrPad(sIP," ",16);
```

```
// Open a file to write
```

```
//[DATA1]:
```

```
// check if file exists
```

```
IF FileExist("[DATA1]:typ_CommsTestReport.csv") THEN
```

```
hFile = FileOpen( "[DATA1]:typ_CommsTestReport.csv", "a+");// Exists open it
```

```
ELSE
```

```
hFile = FileOpen( "[DATA1]:typ_CommsTestReport.csv", "a+");// Create file and add
```

```
header
```

```
FileWriteLn(hFile,"Date" + "," + "Time" + "," + "User" + "," + "PC Name" + "," + "IP
Address" + ","
```

```
+ "Value to PLC" + "," + "Value from PLC" + "," + "Time write" + "," + "Time Read" +
"," + "Time Delta" + "," + "Handle" + "," + "Timestamp" + "," + "Quality" + "," + "Tag Name" + "," + "IO
Server");
```

```
END
```

```

IF hFile = -1 THEN
    Message("ERROR", "Failed to open [DATA1]:typ_CommsTestReport.csv file.", 0);
    RETURN 0;
END

// Log Data to CSV file

rTag_Y = TagRead(sTagPrefix + "_Y");
rTag_I = TagRead(sTagPrefix + "_I");
iTag_T1 = TagRead("lv" + sTagPrefix + "_T1");
iTag_T2 = TagRead("lv" + sTagPrefix + "_T2");
iTag_TD = TagRead("lv" + sTagPrefix + "_TD");
iTag_H = TagRead("lv" + sTagPrefix + "_H");
sTag_VT = TagRead("lv" + sTagPrefix + "_VT");
sTag_Q = TagRead("lv" + sTagPrefix + "_Q");
sTag_Q = TagRead("lv" + sTagPrefix + "_Q");
sTag_IO = TagRead("lv" + sTagPrefix + "_IO");

//FileWriteLn(hFile,"Date" + "," + "Time" + "," + "User" + "," + "PC Name" + "," + "IP
Address" + "," + "Y" + "," + "I" + "," + "T1" + "," + "T2" + "," + "TD" + "," + "H" + "," +
"VT" + "," + "Q");

sMsgLog = sDate + "," + sTime + "," + sUser + "," + sPC + "," + sIP + ","
+ RealToStr(rTag_Y,2,0) + "," + RealToStr(rTag_I,2,0) + "," + IntToStr(iTag_T1) + ","
+ IntToStr(iTag_T2) + "," + IntToStr(iTag_TD) + "," + IntToStr(iTag_H) + ","
+ sTag_VT + "," + sTag_Q + "," + sTagPrefix + "," + sTag_IO;

FileWriteLn(hFile,sMsgLog);

iReturn = FileClose(hFile);

RETURN iReturn;

END

!-----
-----

```

```

! Function:          typ_CommsTestClearTags
!
! Author:            Clinton Lauriston,                      - 1.0
!
! Date/Revision:    31 July      2023,                      - 1.0
!
! Description:      Clear all tags
!
!
! Parameters:       sTagPrefix
!
!
! Returns:          0 (zero) if successful, otherwise an error is returned.
!
!-----
-----

INT
FUNCTION typ_CommsTestClearTags(STRING sTagPrefix)
    INT    iReturn = 0; // 0 (zero) if successful, otherwise an error code is returned.

    // Clear all tags
        iReturn = TagWrite(sTagPrefix + "_Y",0);
        iReturn = TagWrite(sTagPrefix + "_I",0);
        iReturn = TagWrite("lv" + sTagPrefix + "_T1",0);
        iReturn = TagWrite("lv" + sTagPrefix + "_T2",0);
        iReturn = TagWrite("lv" + sTagPrefix + "_TD",0);
        iReturn = TagWrite("lv" + sTagPrefix + "_H",0);
        iReturn = TagWrite("lv" + sTagPrefix + "_VT","");
        iReturn = TagWrite("lv" + sTagPrefix + "_Q","");
        iReturn = TagWrite("lv" + sTagPrefix + "_IO","");

RETURN iReturn

END

```

```

!-----
!
! Function:          typ_CommsTestAll
!
! Author:            Clinton Lauriston,                - 1.0
!
! Date/Revision:     31 July      2023,                - 1.0
!
! Description:       Subscribe
!
!
! Parameters:        sMode
!
!                                iMode
!
!                                1 TagSubscribe
!                                2 TagUnsubscribe
!
!
! Returns:           0 (zero) if successful, otherwise an error is returned.
!
!-----

```

INT

FUNCTION typ_CommsTestAll(STRING sMode, INT iMode)

INT iReturn = 0; // 0 (zero) if successful, otherwise an error code is returned.

INT iSleepMS = 2500;

sMode = StrUpper(sMode);

IF sMode = "ALL" THEN

 // 1 TagSubscribe

 // 2 TagUnsubscribe

 //Thesis_PLC

 SleepMS(iSleepMS);

 typ_CommsTest("Thesis_PLC_Citect_Bool",iMode);

 SleepMS(iSleepMS);


```
        typ_CommsTest("Thesis_PLC_Citect_Real",iMode);
ELSE
    //1 PLC
    SleepMS(iSleepMS);
    typ_CommsTest(sMode + "_Citect_Bool",iMode);
    SleepMS(iSleepMS);
    typ_CommsTest(sMode + "_Citect_Real",iMode);
END

RETURN iReturn

END
```

Appendix E – Modbus TCP/IP Configurations

E1 – Benchmarking Communications DTM Configuration

Connection	Setting	ATV930	ATV71	M340	Advantys STB	TeSys T
1	Read (words)	12	11	125	60	32
	Write (words)	6	5	93	0	3
	Total (words)	18	16	218	60	35
	Poll rate (ms)	300	300	250	250	300
2	Read (words)	8	8	0	1	0
	Write (words)	0	0	0	0	0
	Total (words)	8	8	-	1	-
	Poll rate (ms)	1500	1500	0	250	0
3	Read (words)	0	0	0	2	0
	Write (words)	0	0	0	0	0
	Total (words)	0	0	0	2	0
	Poll rate (ms)	-	-	-	250	-
Total	Read/write (words)	26	24	218	61	35

E2 – Advanced Authentication Communications Configuration

Read Block	Setting	ATV930	ATV71	TeSys T
1	First read register	3011	3011	558
	Last read register	3112	3112	563
	Total words read	102	102	6
	Poll duration (ms)	50	50	50
2	First read register	3201	3201	602
	Last read register	3257	3257	693
	Total words read	57	57	92
	Poll duration (ms)	50	50	50
3	First read register	3302	3302	800
	Last read register	3347	3347	800
	Total words read	46	46	1
	Poll duration (ms)	50	50	50
4	First read register	5202	5202	-

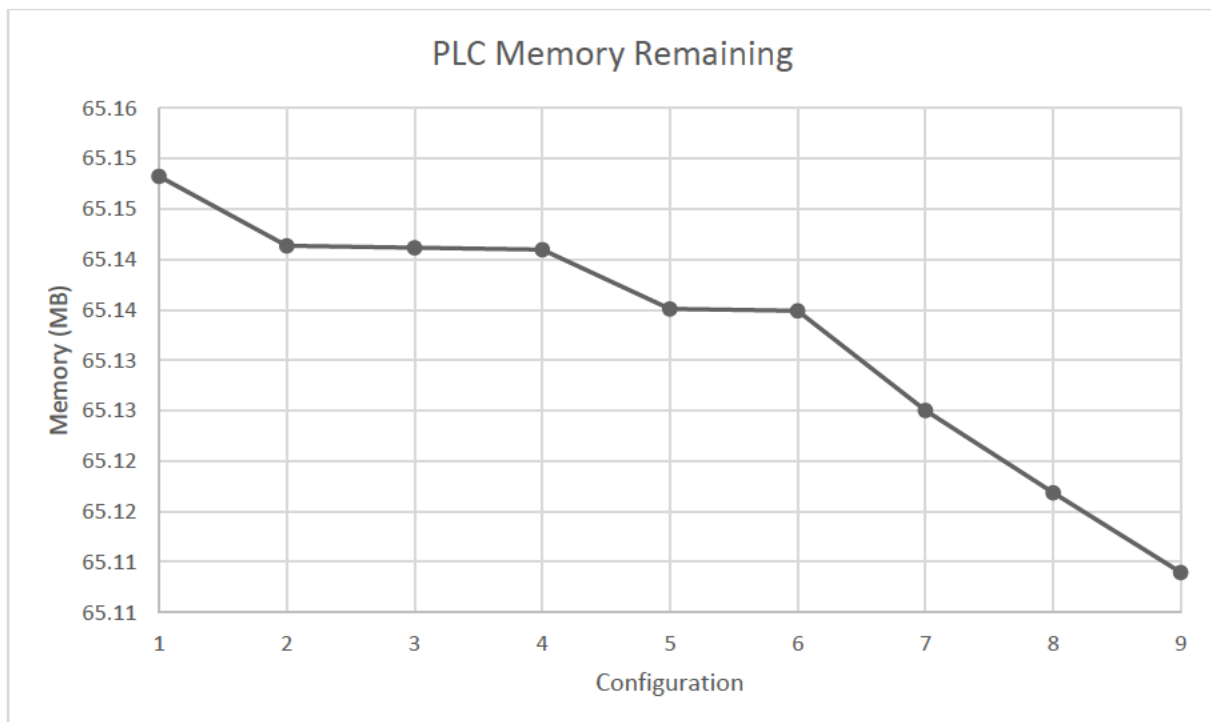
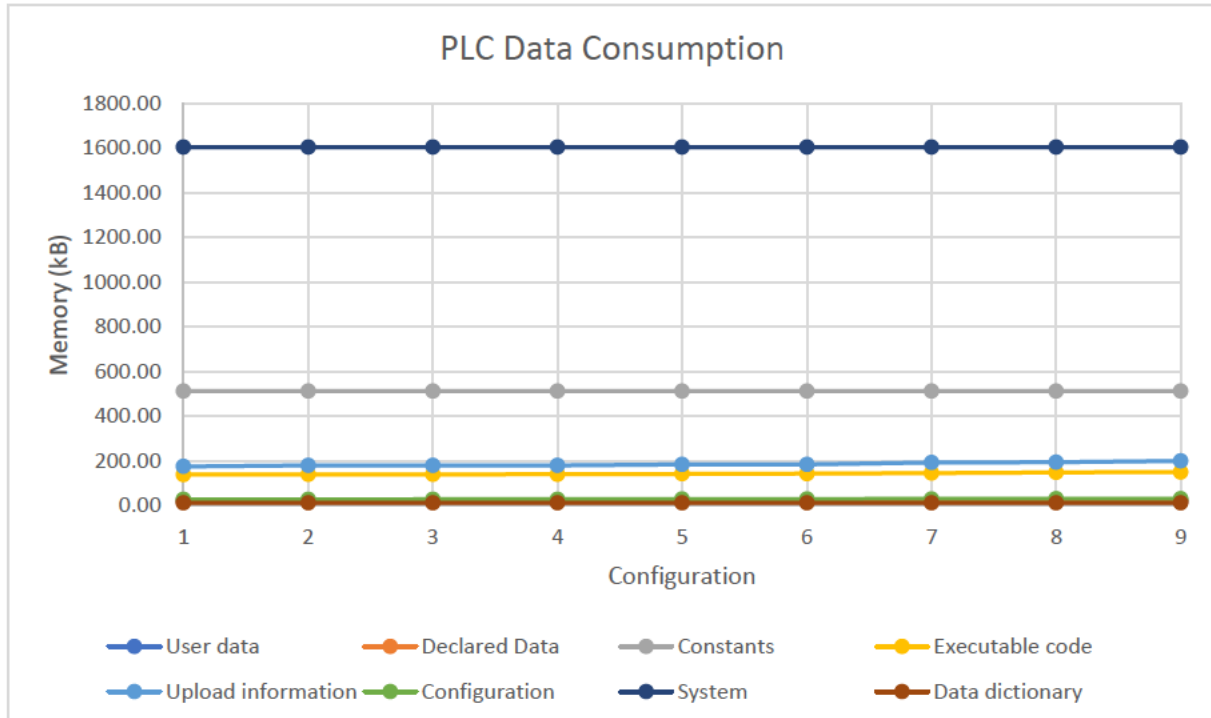
	Last read register	5204	5204	-
	Total words read	13	13	-
	Poll duration (ms)	50	50	-
5	First read register	6601	6601	-
	Last read register	6602	6602	-
	Total words read	2	2	-
	Poll duration (ms)	50	50	-
6	First read register	7121	7121	-
	Last read register	7124	7124	-
	Total words read	4	4	-
	Poll duration (ms)	50	50	-
7	First read register	7391	7391	-
	Last read register	7392	7392	-
	Total words read	2	2	-
	Poll duration (ms)	50	50	-
8	First read register	8001	8001	-
	Last read register	8002	8002	-
	Total words read	2	2	-
	Poll duration (ms)	50	50	-
9	First read register	8501	8501	-
	Last read register	8604	8604	-
	Total words read	104	104	-
	Poll duration (ms)	50	50	-
10	First read register	9001	9001	-
	Last read register	9002	9002	-
	Total words read	2	2	-
	Poll duration (ms)	50	50	-
11	First read register	9201	9201	-
	Last read register	9201	9201	-
	Total words read	1	1	-
	Poll duration (ms)	50	50	-
12	First read register	9601	9601	-
	Last read register	9622	9622	-
	Total words read	22	22	-
	Poll duration (ms)	50	50	-

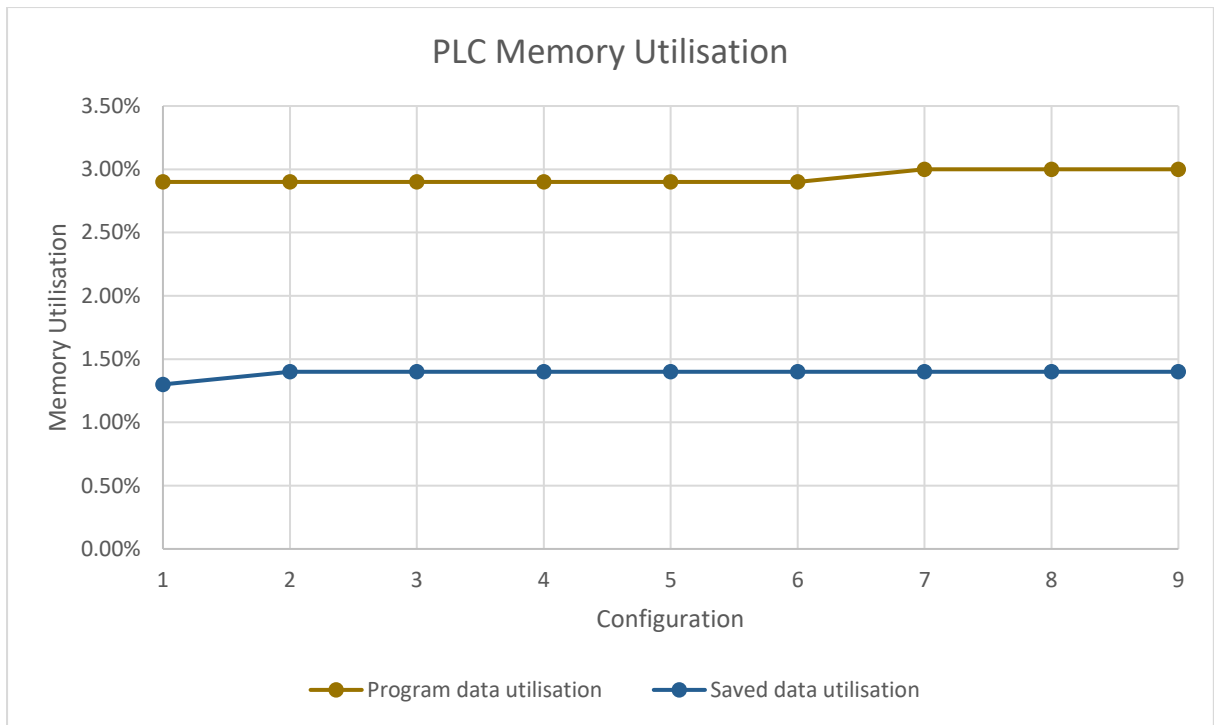
13	First read register	12741	12741	-
	Last read register	12748	12748	-
	Total words read	8	8	-
	Poll duration (ms)	50	50	-
14	First read register	13310	13310	-
	Last read register	13401	13401	-
	Total words read	92	92	-
	Poll duration (ms)	50	50	-
15	First read register	13529	13529	-
	Last read register	13529	13529	-
	Total words read	1	1	-
	Poll duration (ms)	50	50	-
Total	Total words read	458	458	99
	Poll duration (ms)	750	750	150

Appendix F – Results

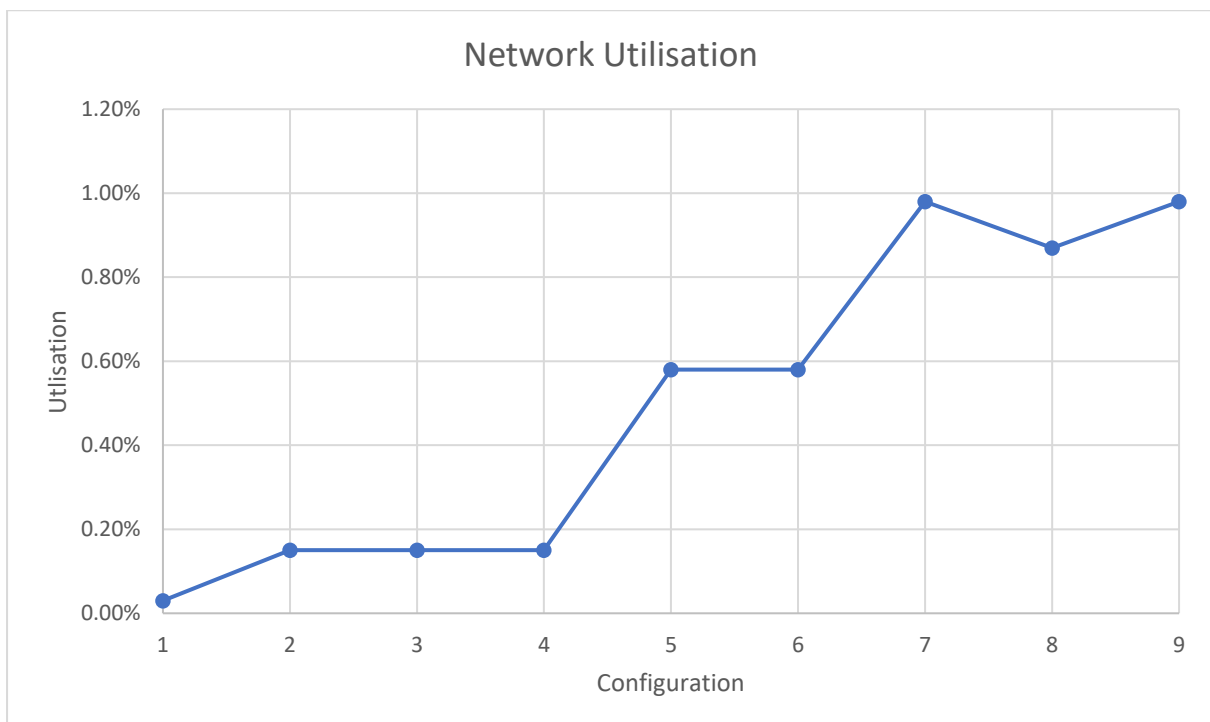
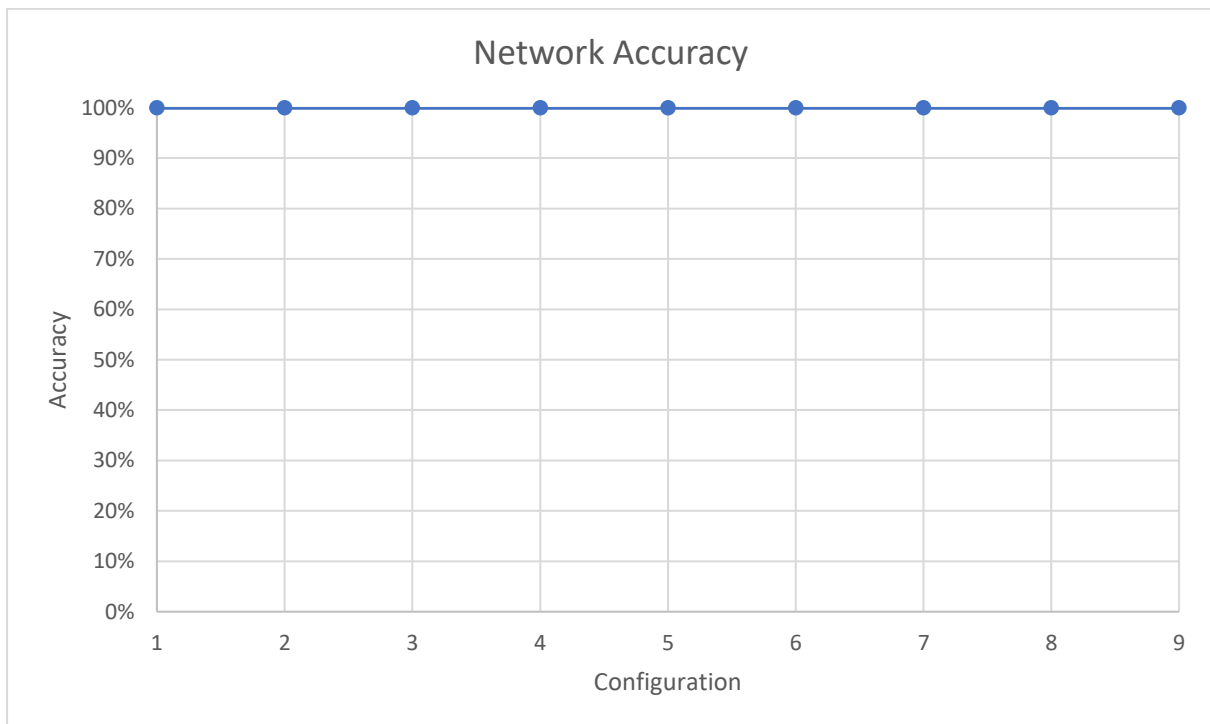
F1 – Benchmarking

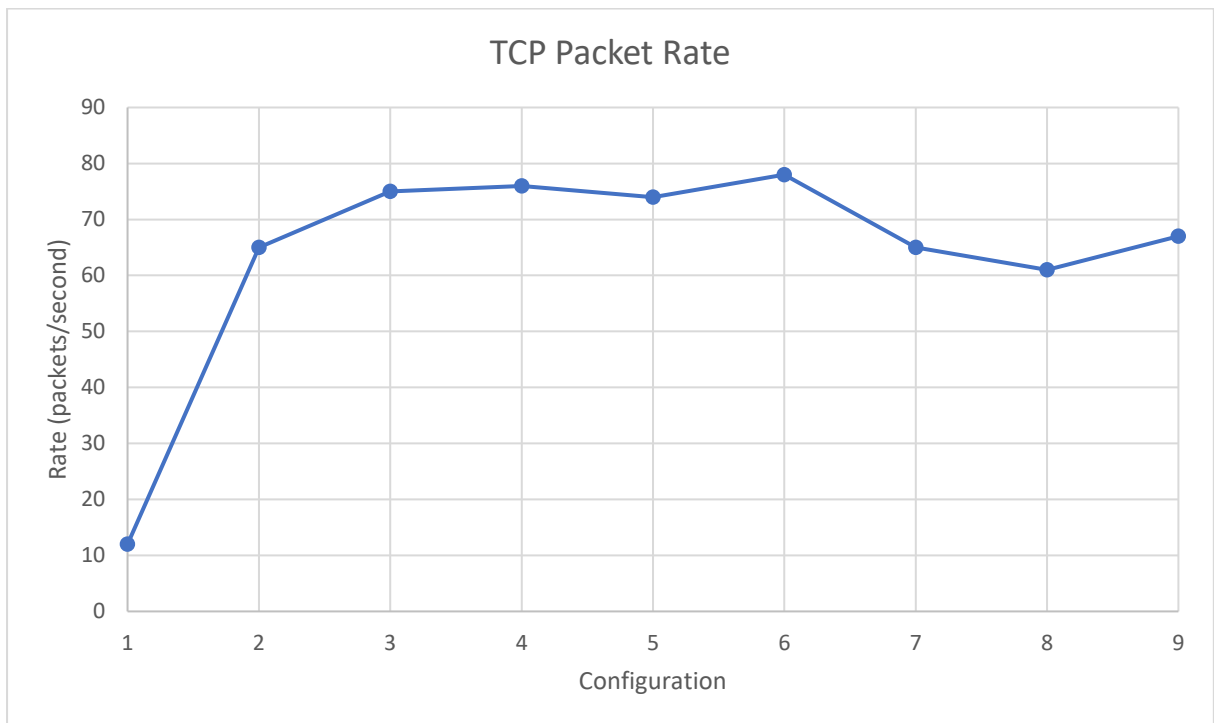
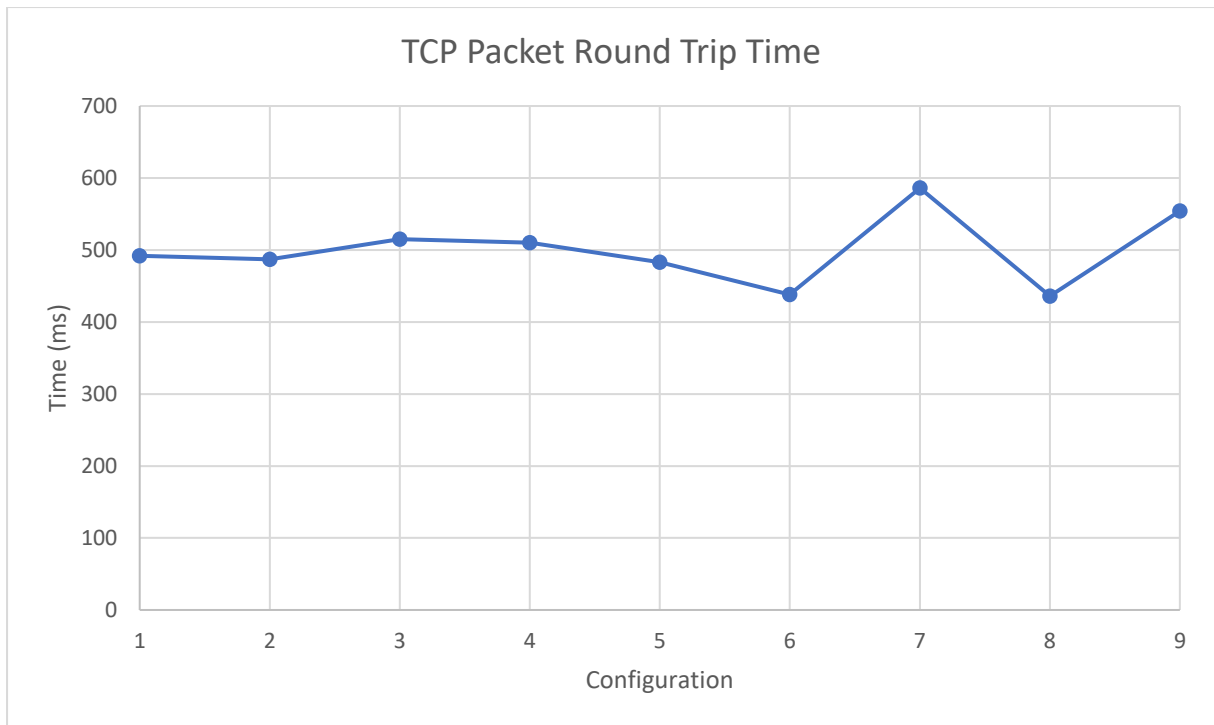
F1.1. – Benchmarking Memory Usage

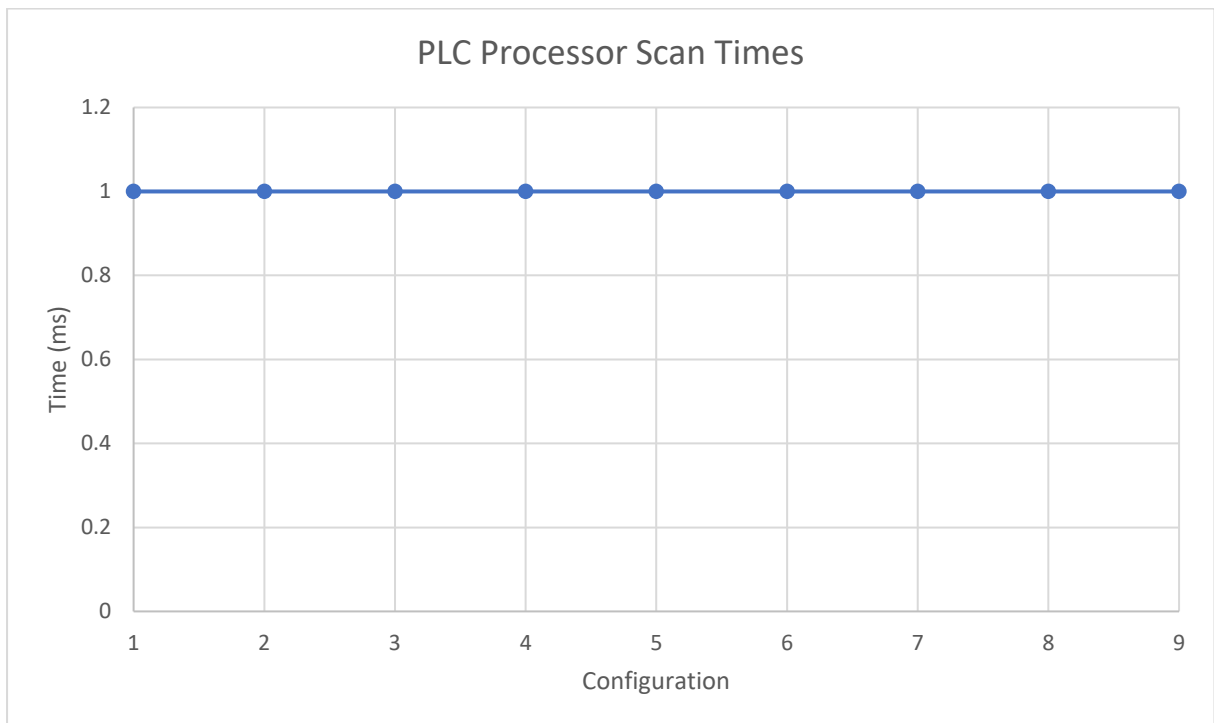
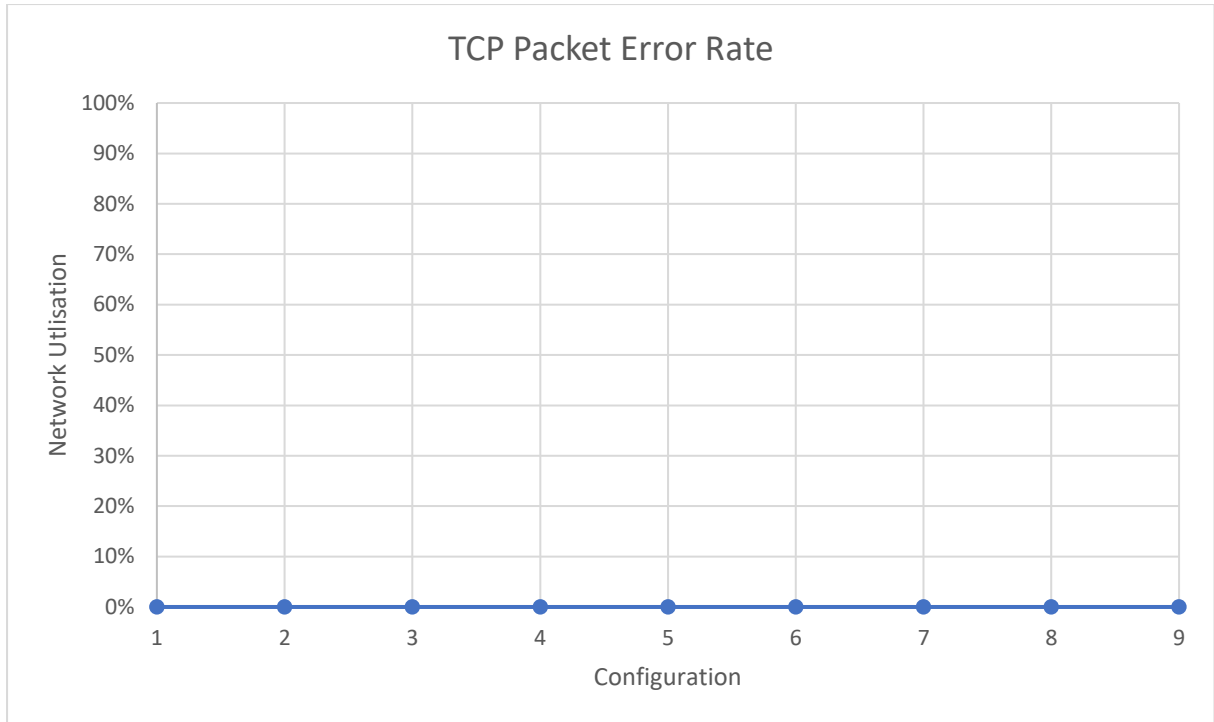


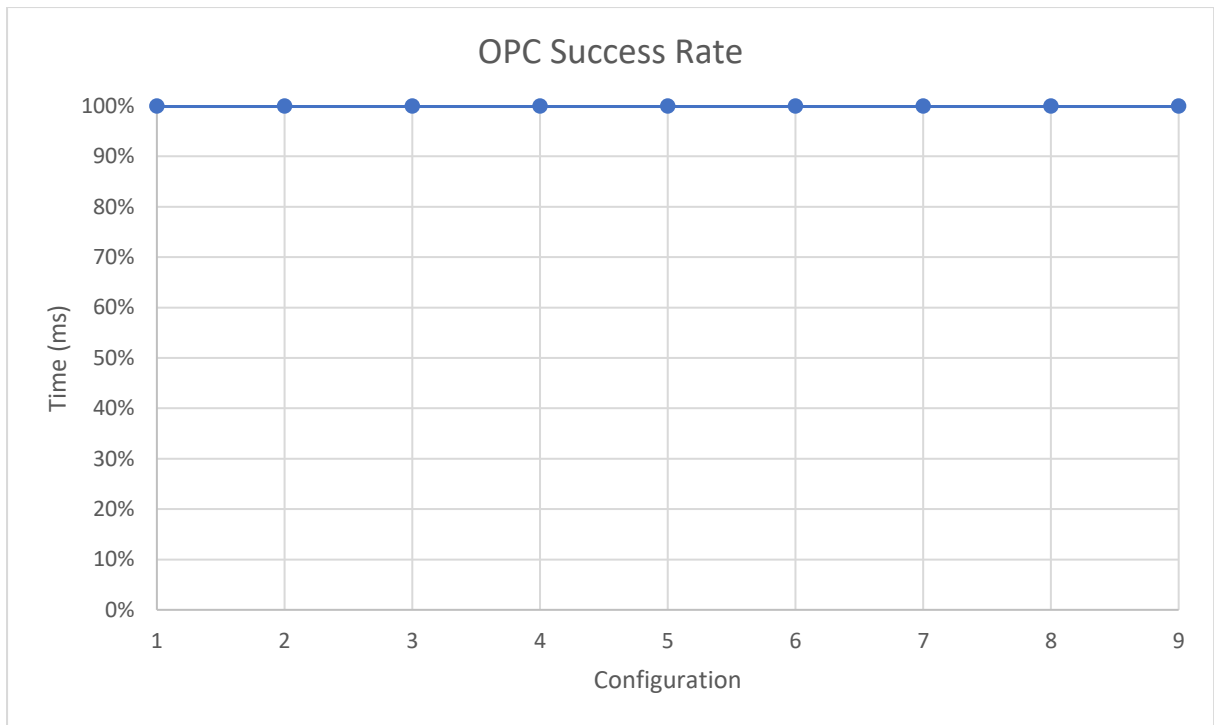


F1.2. – Benchmarking Network Performance



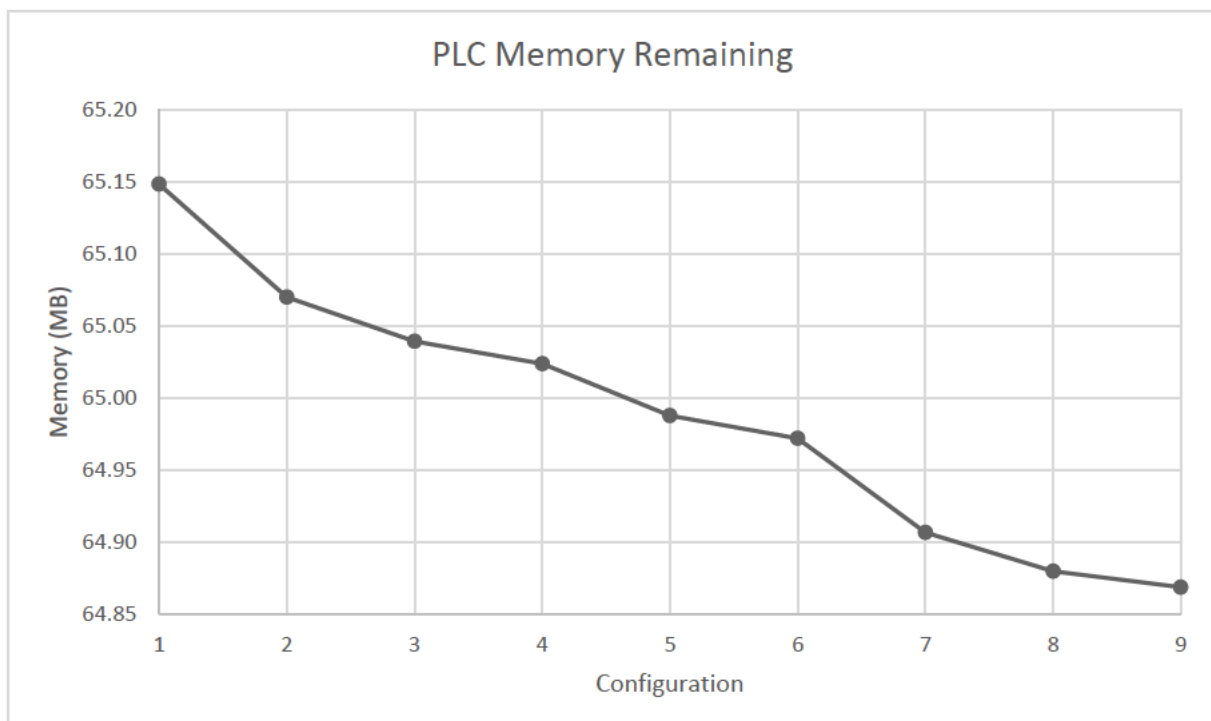
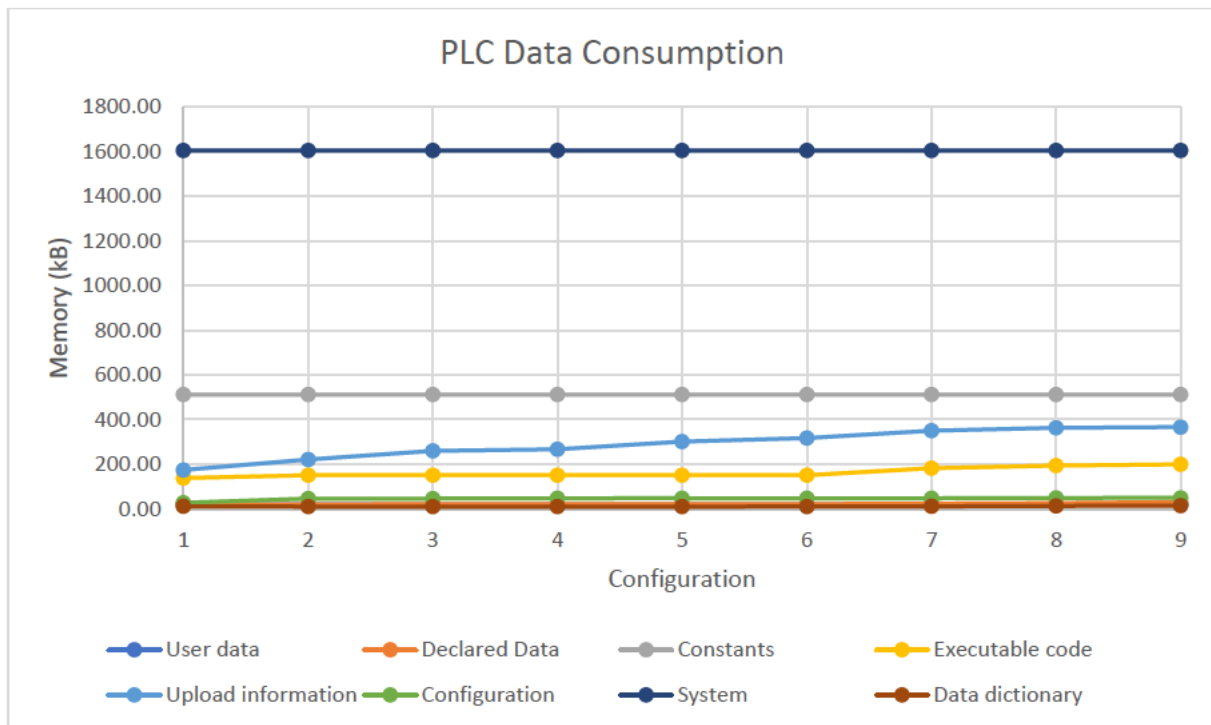


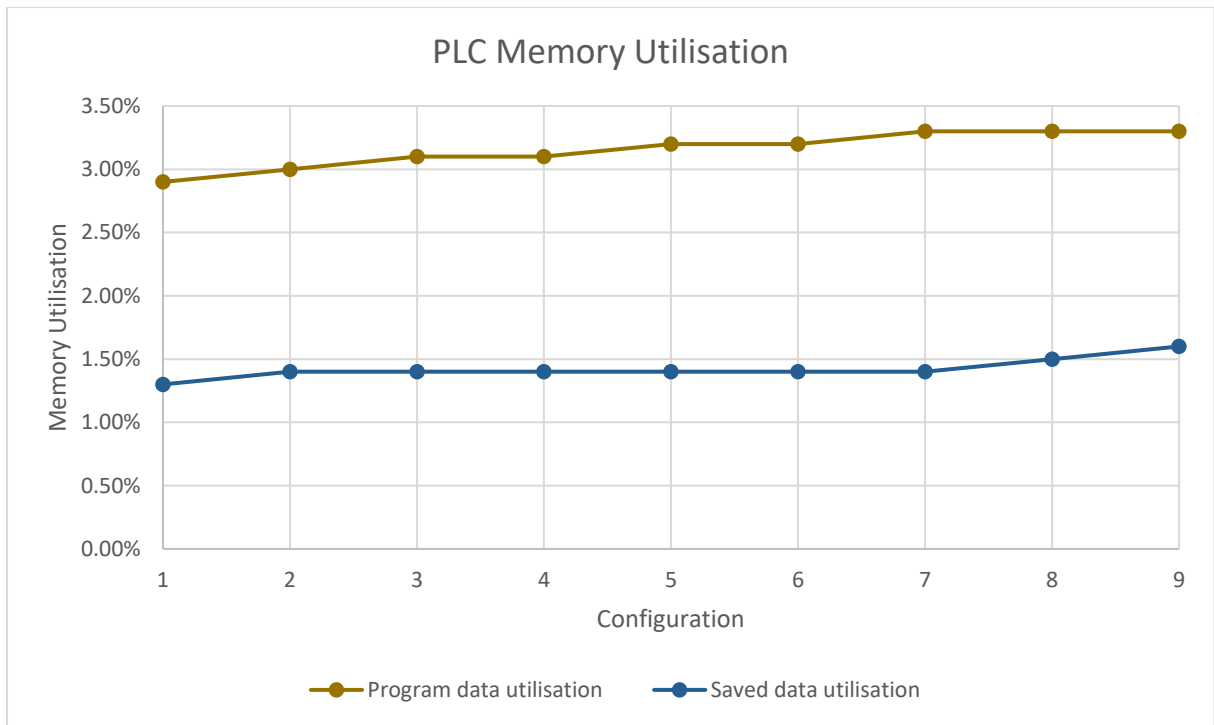




F2 – Advanced Authentication Mode

F2.1. – Advanced Authentication Memory Usage





F2.2. – Advanced Authentication Network Performance

