

MS22 - 5GTT Final Closure Report

CONTENTS

1. Executive summary
2. Introduction, including objectives of the Testbed and Trial(s)
3. Description of what the project did
4. Description of the results - Impact of the results including benefits
5. Key learnings

1. Executive summary

The UK port industry is the second largest in Europe, handling almost 500 million tonnes of freight each year. The Port of Felixstowe is Britain's biggest and busiest container port, handling more than 4 million containers. It plays a pivotal logistical role in keeping the UK's trade moving, delivering real benefits to customers, the wider economy and community and directly employing over 3000 staff.

The bridge cranes availability and efficient operation are a key factor in port logistics productivity. Crane failures have a significant impact on both operational capability, flexibility, and financial outcomes.

This Trial project aimed to bring together the technological advances in the fields of 5G, Internet of Things (remote control, remote sensing, and condition monitoring) and Predictive Data Analytics to test the application of new types of technology that require significantly higher throughput for CCTV and control over **latency, security and reliability** that cannot be realised through today's 4G. This includes exporting know-how, 5G expertise and Condition Monitoring and Predictive Maintenance solutions internationally; create sustainable growth with highly scalable and repeatable solutions for all UK ports.

Although the trial encountered a number of issues with the stability of 5G at site critical operations taking priority, it did provide greater understanding of the technical design, coverage, availability and speed of the network. The learnings will form more robust requirements when procuring network uplift to support the collection of Predictive Analytics, driving insight into Predictive Maintenance.

In summary, the trial acknowledged that there were some disturbances to availability which were attributable to the lack of redundancy and operational management of the trial

configuration, while noting the pioneering status of 5G Standalone System and multi vendor aspects of the Port deployment.

Key findings from the trial found issues with 5G stability on site, generated profisafe alarms concluding that this does not operate consistently enough to be used in a live environment. Some Data was collected on predictive maintenance (Refer to Appendix B for more evidence) but is not representative or consistent due to intermittent availability issues.

What it did provide is greater knowledge and closer understanding of the restrictive nature of industrial crane software whose parameters for safe operation are not friendly to modern wireless technology methods. The trial established a more accurate specification of requirements which will be invaluable in future procurement exercises for a network that will support new autonomous technologies in an industrial port setting; learnings in terms of speed needed to be achieved, coverage and capacity levels as well as technical design needed to integrate port's software and equipment.

2. Introduction

The project led by Port of Felixstowe had three consortium members:

- Hutchison 3G UK Ltd
- Cambridge University
- BlueMesh Solutions Limited

The consortium, along with key subcontractors Ericsson and Siemens provided a 5G testbed deployment, one of the earliest 5G Core Standalone trials globally and introduced several innovations from Ericsson intended to evaluate the 5G technology for Industrial use cases.

The objective of the trial was to tackle two main uses cases :- (Refer to Appendix A for more detail)

• Use Case 1 – Predictive maintenance using IOT sensors and Cambridge AI

Providing access to information on discords (i.e., unusual patterns that we detect on monitored parameters in comparison to normal operational behaviour of the component). Success or failure rate in identifying "real" faults.

• Use Case 2 – Remote control of cranes using 5G network and HD Cameras.

Demonstrating automated operations using 5G can overcome the capacity and latency constraints associated with the wired system.

Proving the ability to run multiple streams of traffic with different Quality of Service*

3. Description of what project did (including scope, security approach)

Scope

This entailed deploying a 5G private network on site to cover **six cranes**, 5G enabled **sensors were fitted** to detect shocks, vibrations and stresses imposed on the cranes to identify early warning signals of wear and tear and failure.

The 5G radio access network was served by a 5G SA core deployed on site, providing data backhaul for the Remote-Control Yard Crane system and the Quayside Crane Preventative Maintenance system.

Outline Plan

The Trial ran from March 2021 to September 2022. Key Dates included:

- Project Kick-Off: March 2021

- Pre-Staging (CKH-IOD Labs): June 2021
 - End-to-End Application Testing: August-September 2021

- Site Deployment (Port of Felixstowe): October 2021
 - Field Test [3] and Acceptance [1]: 29th November 2021
 - Support - Period of Support Dec 202 to September 2022

Security strategy and approach

The implementation of IoT devices using 5G networks is a relatively new concept and the cyber security risks may not be well understood. Moreover, any risks to the cranes at the UK's busiest container port could have a far-reaching and detrimental effect on the UK supply chain and economy, and for this reason the system could be defined as critical national infrastructure. A strategy document was created to address a concern from stakeholders that security needed to be considered within the project and handled appropriately. Although the trial is not considered to be critical national infrastructure (CNI), in the future the expanded trial and any industrialisation would be CNI. Refer to Appendix C for more detail.

Trial Design

In high level terms, the data from the cranes was captured by sensors, the data is then removed and transmitted by WiFi devices across the crane, into the crane's fibre network, where a 5G WNC device then backhauls the data via 5G into the port data processing environment.

In slightly more detail, the Predictive Maintenance Use Case has connected sensors to strategic (high energy) parts of the cranes to measure various parameters such as vibration and acceleration. These data are then transferred to a sensor gateway (Raspberry Pi)

where the data is then sent into a Wi-Fi access point and then finally into a 5G CPE device. The Wi-Fi access points are used to remove direct cabling and to give the 5G CPE Wi-Fi capability, as it does not come with this feature.

The data is then sent in a raw format to the Relay Server, then it is processed on the Data Server, then returned to the Relay Server for transport to University of Cambridge using MQTT. The data are then 'unpacked' and prepared for analysis in the AI – Discord Detection developed by Cambridge.

Each sensor creates raw data of around 20,000 bytes which per 6 minute data reading session is around 720MB per sensor, or around 4GB per crane per session. So M20 asks the question, can this amount of data be delivered successfully over 5G?

Data is then delivered to the Data Processing service inside the PoF Data Centre, cleaned, filtered and then presented for analytic analysis.

Once analytic analysis via Cambridge University is complete the data is then stored and presented via the BlueMesh reporting tools.

The Predictive Maintenance Reporting Tool has a scope in two parts.

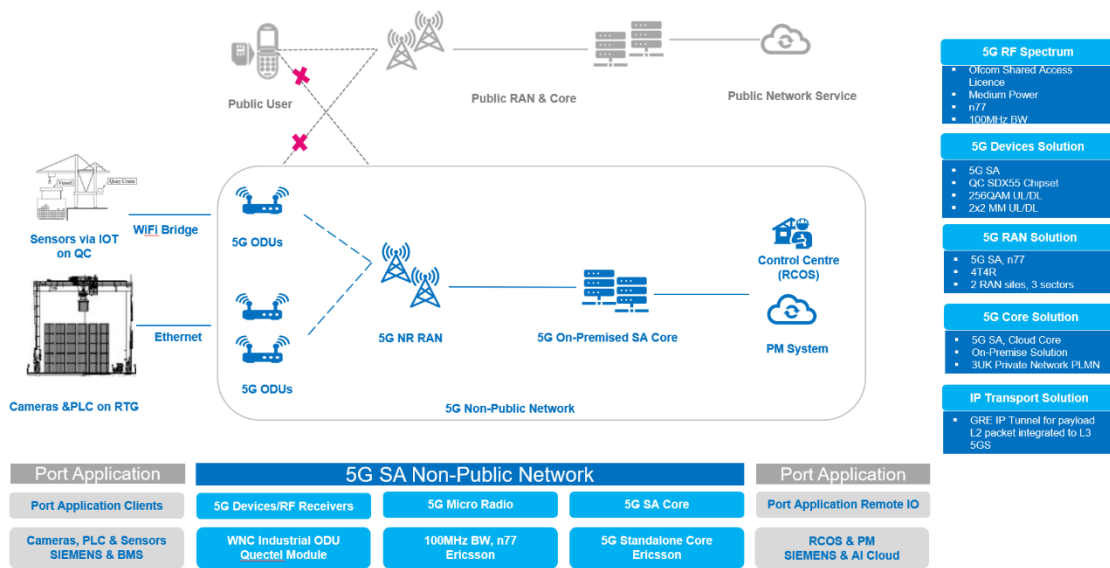
Part 1 is a Condition Monitoring tool that allows the engineers to review data from sensor targets on each crane and examine events on a date / time basis.

Part 2 is a Predictive Maintenance tool, which takes the data feed from the sensors and then reviews the data using a Machine Learning statistical model to identify anomalous features within the data, known as discords. The Discord Detection system is explained in section 24.3 below.

The idea of the reporting design is that it combines two methods of reviewing crane data, the first is a human review of crane activity using self generated charts, the alternative is a Machine based system that reviews all of the data for discord events.

Our idea is that by combining both human and machine methods we can provide the best review of the crane's operational data.

So in summary – the system collects both sensor data and PLC data and combines them into one data set and then the data is available as a Condition Monitoring toolset and a Predictive Maintenance – Discord Detection toolset.



Communications, Collaboration and Dissemination

Given the wider sector interest and immediate Partner stakeholders a communication plan and tracker were established (Appendix G and L). An intent to engage, collaborate and share knowledge including lessons was a key success factor to maturing understanding of 5G experiences, best practices, and requirements within a working Port. Refer to appendix G and H for more detail.

4. Description of the results and impact of Benefits

(refer to Appendix A for details results / outcome)

For the **predictive maintenance use case (CR 15)**, this aimed to put in place a predictive maintenance system based on the data that we are collecting (e.g., vibration and temperature of the motors). In other words, the AI system needs to be informed of vibration/temperature patterns leading to and when a fault is occurring. The monitored components of the Quay Cranes did not materialise any mechanical faults or breakdown during the monitored period within the project. This resulted in a lack of data/information on how a fault manifests resulting in the inability to predict the occurrence of faults in advance.

However, a **discord detection** algorithm was developed detecting the 'discords' identifying abnormal patterns within monitored parameters (e.g., vibration, temperature) and reporting the (i) time stamps and (ii) location of their occurrence will provide engineering team to manually access against the maintenance and operational logs to judge if they are early indicators of a potential fault. This translates to informing inspection strategies at individual crane/component level. It provides engineers with potential discords that might need early intervention (before a disruption occurs). A number of interruptions during the monitoring phase such as wider Operational critical issues, network availability affected collecting a representative set of data on how a fault comes to fruition means difficulty in predicting the occurrence of future faults. It is therefore intended to continue collecting data, re-using the

discord algorithms developed under this use case but analyse using 4G network - Phase 2 and not in scope for this trial which was to prove 5G could support. (Refer to CR15).

For the **Remote Control use case, (CR16)** Programmable Logic Controllers (PLC) which controls the crane itself requires very low latency to work effectively and smoothly, if it senses that it is dipping below a safe threshold it will stop working. It also requires a stable connection with no disconnects or lost packets. As we got into the live testing of the project it became apparent that whilst the network could achieve the original parameters set at the start of the project, it couldn't achieve them consistently to safely move to the final stage of testing. This final stage was the actual operation of the RTG using the 5G network. Due to the inconsistent performance affecting the latency and the inconsistent stability of the network leading to outages and lost packets, it was not deemed safe to operate the RTG, due to health and safety concerns.

The work done on the 5G network showed that it was operable with the parameters required, but it could not consistently achieve these parameters and operate within them. Considerations were made to accommodate Ericsson kit in a later release that potentially offered a resolve to the consistency challenge; but this was not possible to implement with non-GA (accredited) equipment nor in good time to reconvene the project use case original objectives.

Overall up to 12 months has been gained with enough knowledge about the core and the RAN / UE to be confident that an accurate specification of requirements can be produced in future for remote control of RTGs.

The operational performance of the 5G network was also benchmarked when the network was working optimally. The radio optimisation carried out in the planning stage also successfully delivered knowledge of how the radio antenna needs to be deployed to maximise coverage and also circumvent the issues which the containers cause in a harsh port environment

Another use case to prove **IOT Enhance security** resulted in a technology and commercial collaboration agreement which was signed between BMS and Arqit. New software has been created to deliver Quantum Cloud based symmetric keys in a trustless state to end points. Enhanced IOT / MQTT data pipes have been created to test the concept. A list of large enterprises are now engaged and reviewing the technology, BMS currently estimate that commercial activity will be seen in 2023. 1 FT job position has been created at Arqit to promote the technology. One PT job position in software engineering has been created at BMS.

5. Key Learnings

(Refer to Appendix A and D, E and F for more detail)

Overall concerns about 5G coverage remain. Where ports deploy their own private network, there may be a large area of land to be covered with 5G and this leads to the need for significant investment. For some ports, a public or hybrid (public/private) network may be an alternative, but these then depend upon the coverage available. Solutions to overcome security concerns around public networks are now becoming available. 5G networks are currently more focused on urban areas, whereas ports are often away from these. There needs to be flexibility in the deployment of 5G networks with ports, so that they can adapt and expand over time. It is clear that a 'bi ban' approach is challenging to adopt for ports and therefore using technology that has both 4G and 5G capabilities offers a progressive evolution. This applies to both the radio network and the hardware, the latter being a constraint on adoption. This also enables ports to explore different use case possibilities and acquire a deeper understanding of how 5G should be best deployed to maximise its value. This then informs later, large-scale deployments.

What is seen as a way forward is to adopt a **hybrid approach**, whereby radio masts can support both 4G and 5G, with a switch towards the latter over time as required.

Another enabler for 5G investments to **align with wider asset renewal cycles**. Much port infrastructure predates the internet era and therefore telecommunications equipment needs to be retrofitted. By contrast, new build facilities can include the physical infrastructure for 5G connectivity and may need wireless communication methods to be installed. In these situations, the justification for 5G can be stronger.

Another common observation remains in relation to current **technology readiness** being a barrier to wider adoption. Off the shelf solutions are not widely available and, given the complexities of 5G deployment, operators lack confidence that a network can be set up to deliver what is expected. There are also issues with the availability of devices able to connect to 5G networks. Over time, this barrier should reduce as availability improves.

Conversely, **collaborative working** and knowledge sharing between a wide range of stakeholders was seen as an enabler for 5G deployment. This includes network providers, use case developers, government (both national and local) and, particularly for smaller ports, the wider community. In doing so, a better understanding of 5G capabilities and opportunities can be developed, increasing the likelihood of successful deployment. Equally, sharing experiences within the port sector more widely further enhances this.

Several other areas were identified where government support would benefit the deployment of 5G:

- **Standardisation**: this will be required to enable use cases to work with each other and with existing systems. While the government can play a supporting role here, there are also opportunities for port industry bodies to facilitate this.
- **Spectrum availability**: ensuring that ports can get licences for private 5G networks in a timely manner.

• **Skills development:** as noted above, workforce issues are a challenge for and government support to people into the ports industry would be welcomed.

One challenge identified with this is where responsibility lies within government departments as the issues cut across a range of responsibilities, and with national, devolved, and local administrations.

IoT deployments often face challenges associated with sourcing, installation, calibration, and communication of sensors. Sensors' location in spaces, position in the assets, and calibration must be considered to interpret data similarly across all devices. Communication or power drops will occur during their lifetime. After these drops, the sensors may require to be restarted and communication with the IoT network may need to be restored. Even for fully working sensors, it is vital to have a timestamp alongside every data reading. If the moment when an event or measurement happened at the source is unknown, data is meaningless. Additionally, clocks in IoT sensors tend to drift because of the power and communication losses or because they live in a local network without access to a common time server. Thus, ensuring a **common time reference for all sensing data** becomes one of the most important challenges, as it directly impacts the levels of **data quality**. High sampling rates affect the data ingestion process in terms of concurrency, and storage. Having to **deal with high-volume, high velocity of data is at the heart of most IoT deployments**. Additionally, the variety of sensors becomes a variety of data streams, even if they are from the same provider, and thus, they require different pre-processing. Feeding real-time applications demands a **good understanding of technology** and the **assurance of an acceptable end-to-end latency**, from the edge — sensors — to the user — applications.

Ongoing work is focusing to develop a decision support system powered by artificial intelligence to analyse the data collected from the IoT deployment and predict any faults before they compromise crane operations.

The market for IOT devices is growing with **potential of commercial interest** and is estimated by some market commentators to reach US\$1 Trillion by 2028. Protecting IOT devices used on strategic assets is very important because interference with data can have technical and economic impacts. IOT devices increase the performance of engineering assets but can also increase the risk of hacking and organised attacks. By combining QuantumCloud with MQTT, Arqit and BMS have a potential product with global potential. In February 2022 Arqit and BMS signed a technical collaboration agreement. In May 2022 Arqit and BMS signed a commercial agreement to exploit the Quantum Secure MQTT idea in collaboration. Both parties have had High Level discussion on how to create a product that customers may purchase, probably on a platform as a service model.

Appendix for Part 1:

- **20220914 Final Security Strategy pages 9 - 82**
- **20221024 DCMS 5GTT 5G Ports Sustainability v4 page 83**
- **20220914 Master Knowledge Comms, Dissemination 5G Ports Tracker V7 page 84**
- **20220914 Master Redraft Benefits Realisation 5G Ports Tracker_V7 pages 87 - 99**

- Asset register - Blue Mesh (1) pages 100 - 104
- Asset register - MASTER COPY_14Sept pages 105 -108
- 20221024 5G Smart Ports Collaboration Report pages 109 - 127

Part 2 - Risk Management and Information Security Controls

Three UK – PoF 5G IoT Trial

07 September 2022

CONFIDENTIAL INFORMATION – FOR INTERNAL USE ONLY

This document is the property of Three UK. It contains information that is proprietary, confidential, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Trustwave and Three UK.

Copyright © 2022 Trustwave Holdings, Inc. All rights reserved.

Document Control

0.1 Initial release Rob Horne 26/07/2022

0.2 Revised release Rob Horne 01/09/2022

1.0 Final release Rob Horne 07/09/2022

Table of Contents for Part 2 of this report

1. BACKGROUND	11
2. SECURITY TERMS OF REFERENCE	12
3. SECURITY STRATEGY.....	13
Trail Design.....	6
Compliance to Information Assurance Standards	8
Gap analysis	8
4. SECURITY IMPLEMENTATION	17
Governance.....	17
Risk management	17
Asset management	18

Supply chain.....	18
Service protection policies and processes	19
Identity and access control.....	19
Data security	20
System security.....	21
Resilient networks and systems.....	21
Staff awareness and training.....	22
Security monitoring	22
Proactive security event discovery.....	23
Response and recovery planning.....	24
Lessons learned.....	24
5. FUTURE ACTIONS.....	25
6. CONCLUSION	26
Appendix A. POF 5G TRIAL – GAP ANALYSIS.....	27
Appendix B. SECURITY WORKING GROUP TERMS OF REFERENCE	77
Appendix C. IOT SECURITY SCOPE EXPANSION MILESTONE 31 REPORT.....	79

1.BACKGROUND

This 5G trial at the Port of Felixstowe (PoF) is being carried out under a DCMS funding grant to investigate the use of 5G to control a Remote-Control Yard crane and collect data for the preventative maintenance of Quayside cranes. A 5G private network will be deployed on site with two 5G base stations to cover twelve cranes for preventative maintenance and one crane for remote control operation. The 5G radio access network will be served by a 5G SA core that will be deployed on site, providing data backhaul for the Remote-Control Yard Crane system and the Quayside Crane Preventative Maintenance system.

The trial encompasses two use cases:

- Use Case 1 – Predictive maintenance using IOT sensors and Cambridge AI
- Use Case 2 – Remote control of cranes using 5G network and HD Cameras.

2.SECURITY TERMS OF REFERENCE

The implementation of IoT devices using 5G networks is a relatively new concept and the cyber security risks may not be well understood. Moreover, any risks to the cranes at the UK's busiest container port could have a far-reaching and detrimental effect on the UK supply chain and economy, and for this reason the system could be defined as critical national infrastructure.

Such a designation mandates a high level of security control and management is implemented. This document seeks to demonstrate how the security requirements were managed, ensuring should the trial move into operation in a production environment, a sufficient level of security control and management would be in place to protect the systems in scope, or a clear path to achieving the level had been documented and accepted.

During the trial, the requirement for an experienced information security SME was recognised. Rob Horne, principal consultant at Comissum and more recently at Trustwave was brought on to the project to fill this requirement. He has many years of experience, having worked in both the private and public sector, most lately for the UK Home Office from 2015 to 2018, is an ISO/IEC 27001 Lead Auditor and was previously a SIRA at Senior Practitioner level.

Copyright © 2022 Trustwave Holdings, Inc. All rights reserved.

3.SECURITY STRATEGY

The strategy document was created to address a concern from stakeholders that security needed to be considered within the project and handled appropriately. Although the trial is not considered to be critical national infrastructure (CNI), in the future the expanded trial and any industrialisation would be CNI.

The initial strategy was to divide the trial into three domains and assign a domain owner with the technical and physical responsibility for the security of the components within that domain. In addition to the domain security strategy, an end-to-end approach was layered across all domains to secure and monitor the trial against any security breach. The strategy was reviewed and determined to be fit for purpose.

However, as the design has evolved, this approach has changed and is now aligned to the data flows.

Trial Design

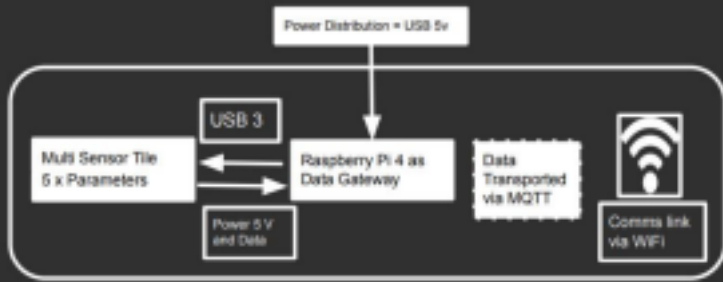
In high level terms, the data is captured by sensors, the data is removed and transmitted by WiFi devices across the crane, into the crane's fibre network, where a 5G WNC device then backhauls the data via 5G into the port data processing environment.

Data is then delivered to the Data Processing service inside the PoF Date Centre, cleaned, filtered and the presented for analytic analysis.

Once analytic analysis is complete the data is then stored and presented via the BlueMesh reporting tools.

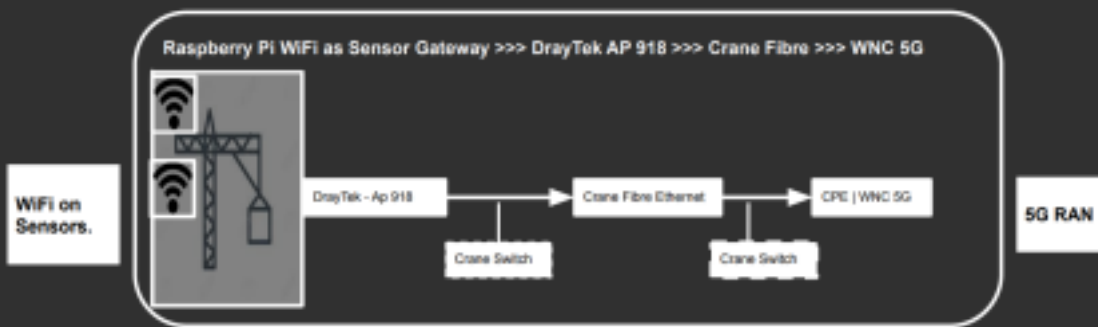
Sensors - Data Creation & MQTT

Sensors generate data. Sensors include: accelerometer (x,y,z) + Audio + Temperature + Magnetic Field. The sensors are powered via USB 3 cable providing a 5V PD. Data and power via USB cable. The USB is in turn powered from a Raspberry Pi board, this includes a WiFi transceiver for short range data transfer over the air. The Linux operating system on the Raspberry Pi also includes an MQTT data communication service, this prepares the data as MQTT 'packets' and sends the data over WiFi.



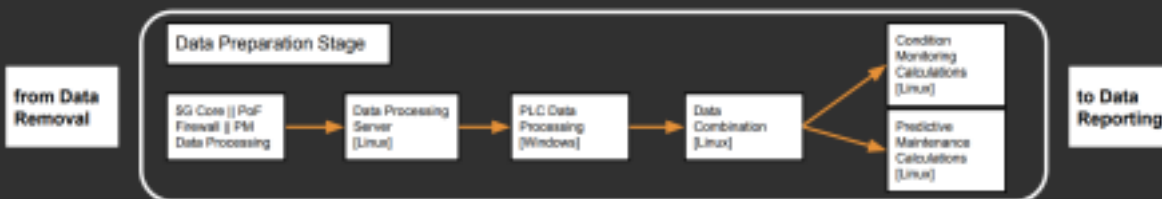
Data Removal - WiFi to 5G

The data is removed from each crane via a 5G access point that connects to the port's 5G network. Before that the data is collated via a high power DreyTek router and then transferred via the crane's own fibre channel into a 5G access point.



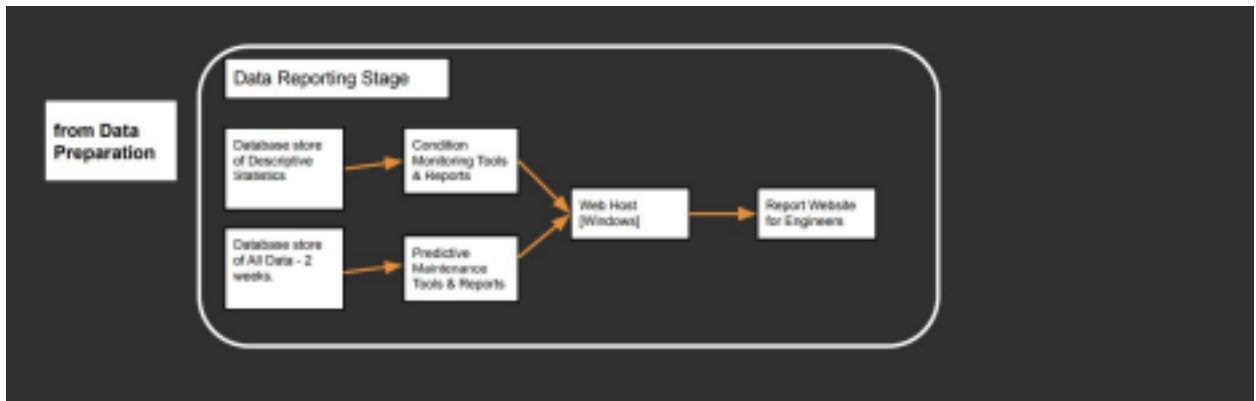
Data Processing

Data Preparation stage takes the data pipe from the cranes on the sensors and cleans the data stream of unnecessary data, it then creates a second data structure based on the PLC data. Once collected the data is then concatenated into blocks of data that represent each individual sensor and then the vibration etc data from the Cranes aligned with the PLC data events. The data is then processed via two systems; 1. A Condition Monitoring system and 2. A Predictive maintenance system.



Data Reporting

Data Reporting is based on two data sets within the same Mongo.DB; 1. All Data collected over the previous 2 weeks informs the AI model and allows engineers to review in detail any event during a 2 week timeframe. However, the data storage requirements are high, and so 2. Longer Term data is abstracted into a set of Descriptive Statistics for longitudinal tracking / deterioration of the crane by increased vibration



Compliance to Information Assurance Standards

A number of security assurance standards were considered with the choice of the NCSC Cyber Assessment Framework (CAF) chosen for the following reasons:

- Recommended framework for NIS-D Operators of Essential Services which closely aligns to CNI
- The Three Private Network Security Framework used to form the security strategy is based on the CAF.

The fourteen principles of the CAF contain in total, 180 objectives. These have all been assessed for relevance and 168 have been identified as in scope.

Gap analysis

A gap analysis was carried out against the requirements of the CAF.

Principle	No. of objectives	No. in scope
1. Governance	11	9
2. Risk Management	15	14
3. Asset Management	5	5
4. Supply Chain	6	6
5. Service Protection Policies and Processes	10	10

Principle	No. of objectives	No. in scope
6. Identity and Access Control	19	19
7. Data Security	19	17
8. System Security	18	18
9. Resilient Networks and Systems	9	8
10. Staff Awareness and Training	10	4
11. Security Monitoring	31	31
12. Proactive Security Event Discovery	6	6
13. Response and Recovery Planning	13	13
14. Lessons Learned	8	8

All fourteen principles were identified as within scope.

Information on the NCSC Cyber Assessment Framework (CAF) which further explain and expand on the cyber security principles can be found here:

<https://www.ncsc.gov.uk/collection/caf> More information and the results of the analysis are recorded in Appendix A.

4.SECURITY IMPLEMENTATION

Governance

Principle implementation status:	
Requirements:	
<ul style="list-style-type: none">• Identify who has overall responsibility for security; create a forum for top-level discussions on security with a Terms of Reference, agenda, and schedule• Identify and record all security-related roles and responsibilities, ensuring those that fulfil the roles have the capabilities to do so• Publish key risk decisions to appropriate stakeholders, ensuring they understand their responsibilities to make decisions.	

A Security Working Group was created to review and address any security issues and design changes. The SWG Terms of Reference are included in Appendix B. The SWG meets virtually every two weeks, and all stakeholders are represented at a suitable level.

Security related roles and their responsibilities have been identified and assigned to named individuals. These persons participate in the SWG.

Decision-making is a function of the SWG with input from relevant stakeholders and recorded outcomes.

Locally, there is a PoF monthly security group which addresses incidents, policy updates and risk reviews.

Risk management

Principle implementation status:	
Requirements:	
<ul style="list-style-type: none">• Implement a robust and effective information security risk management process• Identify and record an appropriate assurance methodology.	

The existing risk management process is project focused but does cover elements of security, such as supplier risk. An ISO 27005 methodology has been proposed for information security assessments; a risk management policy and procedure for this has been provided.

A high-level risk assessment has been carried out as part of a policy and procedure review to identify any areas where extant policies and related procedures are not in evidence. The outcome has been embedded into this document. A risk register is in place and is reviewed appropriately.

Asset management

Principle implementation status:	
Requirement:	
• Implement an asset register and a process to keep it up to date.	

An asset register for the trial has been created and all parties have contributed to the content. The asset register can be used as input to any risk assessment.

The PoF maintains its own asset register for physical, software and information assets but as most trail assets aren't owned by PoF they are not included in this, including data assets for preventative maintenance which are managed by BlueMesh.

Supply chain

Principle implementation status:	
Requirement:	
• Implement a supply chain risk management process, to include data sharing and incident management.	

The existing risk assessment process covers supplier risk, and the issues are very well understood. Each party has responsibility for the suppliers within their particular scope.

Service protection policies and processes

Principle implementation status:	
Requirements:	
<ul style="list-style-type: none"> • Document the security governance and risk management approach, technical security practice and specific regulatory compliance • Ensure policies and processes are integrated with others where needed, followed, their correct application and security effectiveness is evaluated, they are communicated, and breaches are handled appropriately. 	

The Three UK security policy framework has provided an overarching approach to security. With the majority of the data processing and security systems the responsibility of the PoF, their policies and procedures have been leveraged to provide a documentation set and processes for security operations.

PoF policy areas that cover the trial to some extent include:

- Access management
- Physical security
- Data security
- OT network security.

Identity and access control

Principle implementation status:	
Requirements:	
<ul style="list-style-type: none"> • Implement access control, including privileged access • Implement restricted device usage for privileged access, certificate-based device access, independent assurance of third-party devices or networks, device identification scanning • Implement specific access controls for privileged access, record activity for analysis • Implement RBAC, least privilege, and logging and monitoring of activity. 	

As stated above, the PoF policies and procedures cover the requirements for access management.

Prior to being provided with an identity credential, background checks are done for new staff. While all PoF employees are subject to comprehensive controls, external parties, such as BlueMesh, are required to conform to the PoF remote access and acceptable use

policies. Each external user is provided with an account after their request has been approved, which must then be enabled by the Service Desk when it's required and access to the trial equipment and data is via VPN

Normal users do not have privileged access and cannot install or modify applications.

Data security

Principle implementation status:	
Requirements:	
<ul style="list-style-type: none"> • Identify and catalogue all relevant data, including its location, quality, quantity, methods of transmission and users with access • Understand and document all data transfers, protective measures and alternative routes • Understand and document all data storage and its protective measures • Record and track all devices that contain data and implement procedures to sanitise devices before disposal or reuse. 	

The 5G standalone non-public network used for the trial has all expected security controls in place. The data was originally stored in the Google Cloud platform for processing, but the design has changed, and data is now stored on site.

All external communications are encrypted to industry standard.

All storage media used in the trial is subject to the PoF data removal and disposal process which will ensure data sanitization takes place.

The trial does not process personal data as defined in UK law, therefore, a Data Protection Impact Assessment is not necessary.

System security

Principle implementation status:	
Requirements:	

- Design a secure network with appropriate segregation and simple data flow, with content-based attack mitigation
- Use and maintain secure configurations, employ change control and patch management, only use permitted software that standard users cannot reconfigure
- Bastion hosts or similar are used for administration; network diagrams are maintained; malware protection is implemented
- Only supported software is used, vulnerability scanning is implemented together with a patching process.

Comprehensive solution designs have been created and compliance with these is closely monitored. Systems are built to agreed templates with the latest patches installed before being used in production. As part of the vulnerability management process all production systems are patched weekly, with any exceptions managed to ensure they are brought up to date within a month. The installation status is monitored, and alerts are investigated manually.

Resilient networks and systems

Principle implementation status:	
Requirements:	
<ul style="list-style-type: none"> • Testing of BC/DR plans takes place, and security awareness and threat intelligence sources are used to make temporary changes where needed • Networks and systems are designed to ensure resilience with the service not accessible from the Internet • Automatic backups are taken, tested, secured, documented, reviewed and made accessible should an event occur. Key roles are duplicated, and knowledge is shared. 	

Backups of systems used in the trial and taken regularly, integrity checked and securely stored.

Given the temporary nature of the trial, the stakeholders had agreed there was not a requirement for a full business continuity capability.

Staff awareness and training

Principle implementation status:	
Requirement:	
<ul style="list-style-type: none">• Security is seen as important to all those involved in the project with open communication and management commitment.	

All PoF staff complete security awareness training as part of their induction, covering physical and logical security. Online training is provided on a regular basis thereafter.

Security monitoring

Principle implementation status:	
Requirements:	
<ul style="list-style-type: none">• Monitoring data must have enough detail to reliably detect security incidents, this should include user activity, systems and networks; new systems must be in scope• The integrity and confidentiality of logs is maintained, with access controls and only copies used for analysis• Logs are reviewed continuously in real time, alerts can be tracked to network assets, alerts are tested, additional data and knowledge is used to enrich log information• Relevant threat intelligence feeds are used and new signatures and IoCs are received and applied• Suitably experienced monitoring staff are in place to analyse, investigate, prioritise and report alerts covering both security and performance; tools make use of all available data.	

Monitoring of the trial infrastructure is the responsibility of the PoF and they have deployed Darktrace as the monitoring solution (<https://www.darktrace.com/en/>). The application is monitored by IT Operations with alerts sent via SMS.

Logs from PoF systems are collected, collated and stored securely.

Proactive security event discovery

Principle implementation status:	
Requirements:	
<ul style="list-style-type: none">• System behaviour understood, and is used to detect and identify malicious activity• System abnormalities are searched for and generate alerts.	

The system and network monitoring in place detects events and alerts the relevant PoF staff. The PoF also employs its own police department in order to conform to the International Ship and Port Facility Security (ISPS) Code; they monitor the port for physical security events and the port is protected by a range of rigorous security controls.

Response and recovery planning

Principle implementation status:	
Requirements:	
<ul style="list-style-type: none">• A comprehensive incident response plan is in place, documented, integrated with other areas of the service, communicated and understood• Response activities are understood and resourced, have backup mechanisms in place, with team members having the skills and knowledge needed, and specialist support is available• Suitable exercise scenarios are documented, run, regularly reviewed, and validated.	

The PoF incident response plan contains extensive and detailed playbooks, incident drills are carried out and these are supported by crisis simulations exercises.

Lessons learned

Principle implementation status:	
Requirements:	

- A comprehensive root cause analysis is conducted following an incident
- An incident review process/policy is in place to ensure lessons learned from each incident are identified, captured, prioritised and acted upon, with the results used to inform risk management information.

All incidents affecting the PoF are investigated, and a root cause analysis completed. Any lessons to be learned are incorporated into a process of continual improvement.

5. FUTURE ACTIONS

The trial, at least in its current state, is not expected to continue. However, in the future a further trial leading to operationalisation of the infrastructure and processes could be put into place. If that were the case, there are a number of recommended actions necessary to ensure security:

- A full risk assessment of the trial should be completed and consider typical threat actors for CNI
- Penetration testing of the infrastructure should take place to identify vulnerabilities
- Security processes for the trial should become part of the PoF managed policy document set.

6. CONCLUSION

The 14 principles of the Cyber Assessment Framework provide a holistic approach to cyber security management and controls, by working towards the attainment of compliance with the requirements all stakeholders have demonstrated commitment to and acceptance of security as an integral part of the project.

The opinion of the report author is that, providing the future actions listed above are carried forward and there is no lessening of the security controls or their management detailed within this report, there should be no reason the security scope should prevent the trial from moving to an operational status.

APPENDIX A. POF 5G TRIAL – GAP ANALYSIS

Executive Summary

This report is the results of a gap analysis of the Port of Felixstowe 5G Trial Project following on from the review of the security strategy, against the objectives of the NIS Directive for Operators of Essential Services (OES). OES will be required to meet a set of fourteen NIS cyber security principles written in terms of outcomes i.e., specification of what needs to be achieved rather than exactly what needs to be done, which have been derived from the NCSC Cyber Assessment Framework (CAF) and includes all the good practice controls.

The fourteen principles of the CAF contain in total, 180 objectives. These have all been assessed for relevance and 168 have been identified as in scope.

For all those in scope, an assessment has been made of their priority, dependencies, what is in place now and what needs to be done.

The remainder of the report is in three sections:

The fourteen NIS Cyber Security principles with the objectives under each and showing which are in scope

A summarised version of the objectives with a priority, status references to any dependencies or related principles, a description of the current measures in place to meet the objectives requirements and suggested initial actions • A summary of the current status.

The Fourteen NIS Cyber Security Principles

The fourteen principles are:

Principle	No. of objectives	No. in scope
15. Governance	11	9
16. Risk Management	15	14
17. Asset Management	5	5
18. Supply Chain	6	6
19. Service Protection Policies and Processes	10	10
20. Identity and Access Control	19	19
21. Data Security	19	17

22. System Security	18	18
23. Resilient Networks and Systems	9	8
24. Staff Awareness and Training	10	4
25. Security Monitoring	31	31
26. Proactive Security Event Discovery	6	6
27. Response and Recovery Planning	13	13
28. Lessons Learned	8	8

All fourteen principles were identified as within scope.

Information on the NCSC Cyber Assessment Framework (CAF) which further explain and expand on the cyber security principles can be found here:

<https://www.ncsc.gov.uk/collection/caf>

Objectives in and out of scope The table below lists all the objectives together with their applicability., Where an objective is deemed not applicable the reason is given.

Note the reference numbering does not match that used within the CAF as this method will be more easily followed going forward.

Ref	Control	Requirements	Applicable
A	Governance Principle: The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.		
A1	Board direction: You have effective organisational security management led at board level and articulated clearly in corresponding policies.	The approach to security is owned and managed at the top level	Yes
A2		Regular top-level discussions on security take place, based on timely and accurate information and informed by expert guidance	Yes
A3		There is a top-level individual who has overall accountability for security and drives regular discussion at the most senior level	Yes
A4		Direction set at the top level is translated into effective organisational practices that direct and control security	Yes
A5	Roles and responsibilities: Your organisation has established roles and responsibilities for the security of networks and information systems at all levels,	Necessary roles and responsibilities for the security of networks and information systems supporting your essential service have been identified. These are reviewed periodically to ensure they remain fit for purpose.	Yes

Ref	Control	Requirements	Applicable
A6	with clear and well-understood channels for communicating and escalating risks.	Appropriately capable and knowledgeable staff fill those roles and are given the time, authority, and resources to carry out their duties.	Yes
A7		There is clarity on who in your organisation has overall accountability for the security of the networks and information systems supporting your essential service.	Yes
A8	Decision-making: You have senior-level	Senior management have visibility of key risk decisions made throughout the organisation.	Yes
A9	accountability for the security of networks and information systems, and delegate decision-making authority appropriately and effectively. Risks to network and information systems related to the delivery of essential services are considered in the context of other organisational risks.	Risk management decision-makers understand their responsibilities for making effective and timely decisions in the context of the risk appetite regarding the essential service, as set by senior management.	Yes
A10		Risk management decision-making is delegated and escalated where necessary, across the organisation, to people who have the skills, knowledge, tools, and authority they need.	No; within the scope of the trial there will not be others to delegate or escalate to.
A11		Risk management decisions are periodically reviewed to ensure their continued relevance and validity	

B	Risk Management		
	Principle: The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the delivery of essential services. This includes an overall organisational approach to risk management.		
B1	Risk Management Process: Your organisation has effective internal processes for managing	Your organisational process ensures that security risks to networks and information systems relevant to essential services are identified, analysed, prioritised, and managed.	Yes

Ref	Control	Requirements	Applicable
B2	risks to the security of network and information systems related to the delivery of essential services and communicating associated activities.	Your approach to risk is focused on the possibility of disruption to your essential service, leading to a detailed understanding of how such disruption might arise as a consequence of possible attacker actions and the security properties of your networks and information systems.	Yes
B3		Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your essential service.	Yes
B4		Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to date understanding of security threats to your essential service and your sector.	Yes

B5		The output from your risk management process is a clear set of security requirements that will address the risks in line with your organisational approach to security.	Yes
B6		Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals.	Yes
B7		You conduct risk assessments when significant events potentially affect the essential service, such as replacing a system or a change in the cyber security threat.	Yes

24

Copyright © 2022 Trustwave Holdings, Inc. All rights reserved.

Ref	Control	Requirements	Applicable
B8		Your risk assessments are dynamic and updated in the light of relevant changes which may include technical changes to networks and information systems, change of use and new threat information.	Yes
B9		The effectiveness of your risk management process is reviewed periodically, and improvements made as required.	Yes
B10		You perform detailed threat analysis and understand how this applies to your organisation in the context of the threat to your sector and	Yes

		the wider CNI.	
B11	Assurance: You have gained confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services.	You validate that the security measures in place to protect the networks and information systems are effective and remain effective for the lifetime over which they are needed.	Yes
B12		You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential services.	Yes
B13		Your confidence in the security as it relates to your technology, people, and processes can be justified to, and verified by, a third party.	No; there is no requirement for third party assurance
B14		Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied, when necessary, in a timely and effective way.	Yes

Ref	Control	Requirements	Applicable
B15		The methods used for assurance are reviewed to ensure they are working as intended and remain the most appropriate method to use.	Yes
C	Asset Management Principle: Everything required to deliver, maintain or support networks and information systems for essential services is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).		

C1	Asset management	All assets relevant to the secure operation of essential services are identified and inventoried (at a suitable level of detail). The inventory is kept up to date.	Yes
C2		Dependencies on supporting infrastructure (e.g., power, cooling etc.) are recognised and recorded.	Yes
C3		You have prioritised your assets according to their importance to the delivery of the essential service.	Yes
C4		You have assigned responsibility for managing physical assets.	Yes
C5		Assets relevant to essential services are managed with cyber security in mind throughout their life cycle, from creation through to eventual decommissioning or disposal.	Yes
D	Supply Chain Principle: The organisation understands and manages security risks to networks and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used. Regardless of your outsourcing model the OES remains responsible for the security of the service and therefore all the requirements that come from the NIS Directive.		

Ref	Control	Requirements	Applicable
D1	Supply chain	You have a deep understanding of your supply chain, including sub contractors and the wider risks it faces. You consider factors such as supplier's partnerships, competitors, nationality and other organisations with which they sub-contract. This informs your risk assessment and procurement processes.	Yes
D2		Your approach to supply chain risk management considers the risks to your essential services arising from supply chain subversion by capable and well-resourced attackers.	Yes
D3		You have confidence that information shared with suppliers that is essential to the operation of your service is appropriately protected from sophisticated attacks.	Yes
D4		You can clearly express the security needs you place on suppliers in ways that are mutually understood and are laid in contracts. There is a clear and documented shared-responsibility model.	Yes
D5		All network connections and data sharing with third parties is managed effectively and proportionately.	Yes
D6		When appropriate, your incident management process and that of your suppliers provide mutual support in the	Yes

		resolution of incidents.	
E	Service Protection Policies and Processes Principle: The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support delivery of essential services.		

Ref	Control	Requirements	Applicable
E1	Policy and process development: You have developed and continue to improve a set of service protection policies and processes that manage and mitigate the risk of cyber security-related disruption to the essential service.	You fully document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance. Cyber security is integrated and embedded throughout these policies and processes and key performance indicators are reported to your executive management.	Yes
E2		Your organisation's service protection policies and processes are developed to be practical, usable and appropriate for your essential service and your technologies.	Yes
E3		Essential service protection policies and processes that rely on user behaviour are practical, appropriate and achievable.	Yes
E4		You review and update service protection policies and processes at suitably regular intervals to ensure they remain relevant. This is in addition to reviews following a	Yes

		major cyber security incident.	
E5		Any changes to the essential service or the threat it faces triggers a review of service protection polices.	Yes
E6		Your systems are designed so that they remain secure even when user security policies and processes are not always followed.	Yes
E7	Policy and process implementation:	All your service protection policies and processes are followed, their correct application and security effectiveness is evaluated.	Yes

Ref	Control	Requirements	Applicable
E8	You have successfully implemented your security policies and processes and can demonstrate the security benefits achieved.	Your service protection policies and processes are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness.	Yes
E9		Your service protection policies and processes are effectively and appropriately communicated across all levels of the organisation resulting in good staff awareness of their responsibilities.	Yes
E10		Appropriate action is taken to address all breaches of service protection policies and processes with potential to disrupt the essential service including aggregated	Yes

		breaches.	
F	Identity and Access Control		
	Principle: The organisation understands, documents and manages access to systems and functions supporting the delivery of essential services. Users (or automated functions) that can access data or services are appropriately verified, authenticated and authorised.		
F1	Identity verification, authentication and authorisation: You robustly verify, authenticate and authorise access to the networks and information systems supporting your essential service.	Only authorised and individually authenticated users can physically access and logically connect to your networks or information systems on which your essential service depends.	Yes
F2		User access to all your networks and information systems supporting the essential service is limited to the minimum necessary.	Yes
F3		You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, for privileged access to all systems that operate or support your essential service.	Yes

Ref	Control	Requirements	Applicable
F4		You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, when you individually authenticate and authorise all remote user access to all your networks and information systems that support your	Yes

		essential service.	
F5		The list of users with access to networks and systems supporting and delivering the essential service is reviewed on a regular basis, at least every six months.	Yes
F6	Device management: You fully know and have trust in the devices that are used to access your networks, information systems and data that support your essential service.	Dedicated devices are used for privileged actions (such as administration or accessing the essential service's network and information systems). These devices are not used for directly browsing the web or accessing email.	Yes
F7		You either obtain independent and professional assurance of the security of third-party devices or networks before they connect to your systems, or you only allow third-party devices or networks dedicated to supporting your systems to connect.	Yes
F8		You perform certificate-based device identity management and only allow known devices to access essential services.	Yes
F9		You perform regular scans to detect unknown devices and investigate any findings.	Yes
F10	Privileged user management: You closely manage privileged user access to networks and	Privileged user access to your essential service systems is carried out from dedicated separate accounts that are closely monitored and managed.	Yes

Ref	Control	Requirements	Applicable
F11	information systems supporting the essential service.	The issuing of temporary, time-bound rights for privileged user access and external third-party support access is either in place or you are migrating to an access control solution that supports this functionality.	Yes
F12		Privileged user access rights are regularly reviewed and always updated as part of your joiners, movers and leavers process.	Yes
F13		All privileged user access to your networks and information systems requires strong authentication, such as two-factor, hardware authentication, or additional real-time security monitoring.	Yes
F14		All Privileged user activity is routinely reviewed, validated and recorded for offline analysis and investigation.	Yes
F15	Identity and Access Management (IdAM):	Your procedure to verify each user and issue the minimum required access rights is robust and regularly audited.	Yes
F16	You assure good management and maintenance of identity and access control for your networks and information systems supporting the essential service.	User permissions are reviewed both when people change roles via your joiners, leavers and movers process and at regular intervals - at least annually.	Yes
F17		All user access is logged and monitored.	Yes

F18		You regularly review access logs and correlate this data with other access records and expected activity.	Yes
F19		Attempts by unauthorised users to connect to your systems are alerted, promptly assessed and investigated.	Yes

Ref	Control	Requirements	Applicable
G	Data Security		
	Principle: Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause disruption to essential services. Such protection extends to how authorised users, devices and systems access critical data necessary for the delivery of essential services. It also covers information that would assist an attacker, such as design details of networks and information systems.		
G 1	Understanding data: You have a good understanding of data important to the delivery of the essential service, where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would impact the service. This also applies to third parties storing or accessing data important to the delivery of essential services.	You have identified and catalogued all the data important to the delivery of the essential service, or that would assist an attacker.	Yes
G 2		You have identified and catalogued who has access to the data important to the delivery of the essential service.	Yes
G 3		You maintain a current understanding of the location, quantity and quality of data important to the delivery of the essential service.	Yes
G 4		You take steps to remove or minimise unnecessary copies or unneeded	Yes

		historic data.	
G 5		You have identified all mobile devices and media that may hold data important to the delivery of the essential service.	Yes
G 6		You maintain a current understanding of the data links used to transmit data that is important to your essential service.	Yes
G 7		You understand the context, limitations and dependencies of your important data.	Yes

Ref	Control	Requirements	Applicable
G 8		You understand and document the impact on your essential service of all relevant scenarios, including unauthorised data access, modification or deletion, or when authorised users are unable to appropriately access this data.	Yes
G 9		You validate these documented impact statements regularly, at least annually.	Yes
G1 0	Data in transit: You have protected the transit of data important to the delivery of the essential service. This includes the transfer of data to third parties.	You have identified and protected (effectively and proportionately) all the data links that carry data important to the delivery of your essential service.	Yes

G11		You apply appropriate physical or technical means to protect data that travels over non-trusted or openly accessible carriers, with justified confidence in the robustness of the protection applied.	Yes
G1 2		Suitable alternative transmission paths are available where there is a significant risk of impact on the delivery of the essential service due to resource limitation (e.g., transmission equipment or service failure, or important data being blocked or jammed).	Yes
G1 3	Stored data: You have protected stored data important to the delivery of the essential service.	You have only necessary copies of this data. Where data is transferred to less secure systems, the data is provided with limited detail and/or as a read-only copy.	Yes
G1 4		You have applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion.	Yes

Ref	Control	Requirements	Applicable
G1 5		If cryptographic protections are used you apply suitable technical and procedural means, and you have justified confidence in the robustness of the protection applied.	Yes

G1 6		You have suitable, secured backups of data to allow the essential service to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies.	Yes
G1 7		Necessary historic or archive data is suitably secured in storage.	Yes
G1 8	Mobile Data: You have protected data important to the delivery of the essential service on mobile devices.	You catalogue and track all devices that contain data important to the delivery of the essential service (whether a specific storage device or one with integral storage).	No; it is understood mobile devices will not be used
G1 9		All data important to the delivery of the essential service is sanitised from all devices, equipment or removable media before disposal.	No; it is understood mobile devices will not be used
H	System Security Principle: Network and information systems and technology critical for the delivery of essential services are protected from cyber-attack. An organisational understanding of risk to essential services informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.		
H1	Secure by design:	You employ appropriate expertise to design network and information systems.	Yes

Ref	Control	Requirements	Applicable
H2	You design security into the network and information systems that supports the delivery of essential services. You minimise their attack surface and ensure that the delivery of the essential service should not be impacted by the exploitation of any single vulnerability.	Your networks and information systems are segregated into appropriate security zones, e.g., operational systems for the essential service are segregated in a highly trusted, more secure zone.	Yes
H3		The networks and information systems supporting your essential service are designed to have simple data flows between components to support effective security monitoring.	Yes
H4		The networks and information systems supporting your essential service are designed to be easy to recover.	Yes
H5		Content-based attacks are mitigated for all inputs to operational systems that effect the essential service (e.g., via transformation and inspection).	Yes
H6		Secure configuration: You securely configure the network and information systems that support the delivery of essential services.	You have identified, documented and actively manage (e.g., maintain security configurations, patching, updating according to good practice) the assets that need to be carefully configured to maintain the security of the essential service.
H7		All platforms conform to your secure, defined baseline build, or the latest known good configuration version for that environment.	Yes

H8		You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.	Yes
----	--	--	-----

Ref	Control	Requirements	Applicable
H9		You regularly review and validate that your network and information systems have the expected, secured settings and configuration.	Yes
H10		Only permitted software can be installed and standard users cannot change settings that would impact security or business operation.	Yes
H11		If automated decision-making technologies are in use, their operation is well understood, and decisions can be replicated.	Yes
H12		Secure management: You manage your organisation's network and information systems that support the delivery of essential services to enable and maintain security.	Your systems and devices supporting the delivery of the essential service are only administered or maintained by authorised privileged users from dedicated devices that are technically segregated and secured to the same level as the networks and systems being maintained.
H13		You regularly review and update technical knowledge about networks and information systems, such as documentation and network diagrams, and ensure	Yes

		they are securely stored.	
H14		You prevent, detect and remove malware or unauthorised software. You use technical, procedural and physical measures as necessary.	Yes
H15	Vulnerability management:	You maintain a current understanding of the exposure of your essential service to publicly known vulnerabilities.	Yes

Ref	Control	Requirements	Applicable
H16	You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.	Announced vulnerabilities for all software packages, network equipment and operating systems used to support your essential service are tracked, prioritised and mitigated (e.g., by patching) promptly	Yes
H17		You regularly test to fully understand the vulnerabilities of the networks and information systems that support your essential service and verify this understanding with third-party testing.	Yes
H18		You maximise the use of supported software, firmware and hardware in your networks and information systems supporting your essential service.	Yes
I	Resilient Networks and Systems Principle: The organisation builds resilience against cyber-attack and system failure into the design, implementation, operation and management of systems that support the delivery of essential services.		

I1	Resilience preparation: You are prepared to restore your essential service following disruption.	You have business continuity and disaster recovery plans that have been tested for practicality, effectiveness and completeness. Appropriate use is made of different test methods, e.g., manual fail-over, table-top exercises, or red-teaming.	Yes
I2		You use your security awareness and threat intelligence sources, to make immediate and potentially temporary security changes in response to new threats, e.g., a widespread outbreak of very damaging malware	Yes

Ref	Control	Requirements	Applicable
I3	Design for resilience: You design the network and information systems supporting your essential service to be resilient to cyber security incidents. Systems are appropriately segregated, and resource limitations are mitigated.	Your essential service's operational systems are segregated from other business and external systems by appropriate technical and physical means, e.g., separate network and system infrastructure with independent user administration. Internet services are not accessible from operational systems.	Yes
I4		You have identified and mitigated all resource limitations, e.g., bandwidth limitations and single network paths.	Yes

15		You have identified and mitigated any geographical constraints or weaknesses. (e.g., systems that your essential service depends upon are replicated in another location, important network connectivity has alternative physical paths and service providers.)	No; given the physical constraints this is not relevant; however, the objective below will be used to assess any changes
16		You review and update assessments of dependencies, resource and geographical limitations and mitigation's when necessary.	Yes
17	Backups: You hold accessible and secured current backups of data and information needed to recover.	Your comprehensive, automatic and tested technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event.	Yes
18		Key roles are duplicated, and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential service.	Yes

Ref	Control	Requirements	Applicable
19		Backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.	Yes

J	Staff Awareness and Training Principle: Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the delivery of essential services.		
J1	Cyber security culture: You develop and pursue a positive cyber security culture.	Your executive management clearly and effectively communicates the organisation's cyber security priorities and objectives to all staff. Your organisation displays positive cyber security attitudes, behaviors and expectations.	No; within the scope there is no wider organisation
J2		People in your organisation raising potential cyber security incidents and issues are treated positively.	Yes
J3		Individuals at all levels in your organisation routinely report concerns or issues about cyber security and are recognised for their contribution to keeping the organisation secure.	No; within the scope there is no wider organisation
J4		Your management is seen to be committed to and actively involved in cyber security.	Yes
J5		Your organisation communicates openly about cyber security, with any concern being taken seriously.	Yes
J6		People across your organisation participate in cyber security activities and improvements, building joint ownership and bringing knowledge of their area of expertise.	Yes

Ref	Control	Requirements	Applicable
J7	<p>Cyber security training:</p> <p>The people who operate and support your essential service are appropriately trained in cyber security. A range of approaches to cyber security training, awareness and communications are employed.</p>	All people in your organisation, from the most senior to the most junior, follow appropriate cyber security training paths.	No; this would be the responsibility of individual organisations
J8		Each individuals' cyber security training is tracked and refreshed at suitable intervals.	No; this would be the responsibility of individual organisations
J9		You routinely evaluate your cyber security training and awareness activities to ensure they reach the widest audience and are effective.	No; this would be the responsibility of individual organisations
J10		You make cyber security information and good practice guidance easily accessible, widely available and you know it is referenced and used within your organisation.	No; this would be the responsibility of individual organisations
K	<p>Security Monitoring</p> <p>Principle: The organisation monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.</p>		

K1	Monitoring coverage: The data sources that you include in your monitoring allow for timely identification of security events which might affect the delivery of your essential service.	Monitoring is based on an understanding of your networks, common cyber attack methods and what you need awareness of in order to detect potential security incidents that could affect your essential service. (e.g., presence of malware, malicious emails, user policy violations).	Yes
K2		Your monitoring data provides enough detail to reliably detect security incidents that could affect your essential service.	Yes

Ref	Control	Requirements	Applicable
K3		You easily detect the presence or absence of Indicators of Compromise (IoCs) on your essential services, such as know malicious command and control signatures.	Yes
K4		You have timely access to the data you need to use with IoCs.	Yes
K5		Extensive monitoring of user activity in relation to essential services enables you to detect policy violations and an agreed list of suspicious or undesirable behaviour.	Yes
K6		You have extensive monitoring coverage that includes host-based monitoring and network gateways.	Yes

K7		All new systems are considered as potential monitoring data sources to maintain a comprehensive monitoring capability.	Yes
K8	Securing Logs:	The integrity of logging data is protected, or any modification is detected and attributed.	Yes
K9	Logging data should be held securely and read access to it should be granted only to accounts with business need. No employee should ever need to modify or delete logging data within an agreed retention period, after which it should be deleted.	The logging architecture has mechanisms, processes and procedures to ensure that it can protect itself from threats comparative to those it is trying to identify. This includes protecting the service itself, and the data within it.	Yes
K10		Log data analysis and normalisation is only performed on copies of the data keeping the master copy unaltered.	Yes
K11		Logging datasets are synchronised, using an accurate common time source, so separate datasets can be correlated in different ways.	Yes

Ref	Control	Requirements	Applicable
K12		Access to logging data is limited to those with business need and no others.	Yes
K13		All actions involving all logging data (e.g., copying, deleting or modification, or even viewing) can be traced back to a unique	Yes

		user.	
K14		Legitimate reasons for accessing logging data are given in use policies.	Yes
K15	Generating alerts: Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.	Logging data is enriched with other network knowledge and data when investigating certain suspicious activity or alerts.	Yes
K16		A wide range of signatures and indicators of compromise are used for investigations of suspicious activity and alerts	Yes
K17		Alerts can be easily resolved to network assets using knowledge of networks and systems.	Yes
K18		Security alerts relating to all essential services are prioritised and this information is used to support incident management.	Yes
K19		Logs are reviewed almost continuously, in real time.	Yes
K20		Alerts are tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms.	Yes

Ref	Control	Requirements	Applicable
.			

K21	<p>Identifying security incidents:</p> <p>You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response.</p>	<p>You have selected threat intelligence feeds using risk-based and threat informed decisions based on your business needs and sector (e.g., vendor reporting and patching, strong anti-virus providers, sector and community-based infoshare).</p>	Yes
K22		<p>You apply all new signatures and IoCs within a reasonable (risk-based) time of receiving them.</p>	Yes
K23		<p>You receive signature updates for all your protective technologies (e.g., AV, IDS).</p>	Yes
K24		<p>You track the effectiveness of your intelligence feeds and actively share feedback on the usefulness of IoCs and any other indicators with the threat community (e.g., sector partners, threat intelligence providers, government agencies).</p>	Yes
K25	<p>Monitoring tools and skills:</p> <p>Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential services they need to protect.</p>	<p>You have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance.</p>	Yes
K26		<p>Monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process.</p>	Yes
K27		<p>Monitoring staff follow process and procedures that address all governance reporting requirements, internal and</p>	Yes

		external.	
K28		Monitoring staff are empowered to look beyond the fixed process to investigate and understand non standard threats, by developing their own investigative techniques and making new use of data.	Yes

Ref	Control	Requirements	Applicable
K29		Your monitoring tools make use of all logging data collected to pinpoint activity within an incident.	Yes
K30		Monitoring staff and tools drive and shape new log data collection and can make wide use of it.	Yes
K31		Monitoring staff are aware of essential services and related assets and can identify and prioritise alerts or investigations that relate to them.	Yes
L	Proactive Security Event Discovery Principle: The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the delivery of essential services, even when the activity evades standard signature-based security prevent/detect solutions, or when it is not possible to use signature-based detection, for some reason.		
L1	System abnormalities for attack detection: You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is	Normal system behavior is fully understood to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity. (e.g., You fully understand which systems should and should not communicate and	Yes

	otherwise hard to identify.	when.)	
L2		System abnormality descriptions from past attacks and threat intelligence, on yours and other networks, are used to signify malicious activity.	Yes
L3		The system abnormalities you search for consider the nature of attacks likely to impact on the networks and information systems supporting the delivery of essential services.	Yes

Ref	Control	Requirements	Applicable
L4		The system abnormality descriptions you use are updated to reflect changes in your networks and information systems and current threat intelligence.	Yes
L5	Proactive attack discovery: You use an informed understanding of more sophisticated attack methods and of normal system behavior to monitor proactively for malicious activity.	You routinely search for system abnormalities indicative of malicious activity on the networks and information systems supporting your essential service, generating alerts based on the results of such searches.	Yes
L6		You have justified confidence in the effectiveness of your searches for system abnormalities indicative of malicious activity.	Yes

M	Response and Recovery Planning		
	Principle: There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential services in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.		
M 1	Response Plan: You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential service and covers a range of incident scenarios.	Your incident response plan is based on a clear understanding of the security risks to the networks and information systems supporting your essential service.	Yes
M 2		Your incident response plan is comprehensive (i.e., covers the complete lifecycle of an incident, roles and responsibilities, and reporting) and covers likely impacts of both known attack patterns and of possible attacks, previously unseen.	Yes
M 3		Your incident response plan is documented and integrated with wider organisational business and supply chain response plans.	Yes

Ref	Control	Requirements	Applicable
M 4		Your incident response plan is communicated and understood by the business areas involved with the supply or maintenance of your essential services.	Yes
M 5	Response and recovery capability: You have the capability to enact your incident response plan, including	You understand the resources that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.	Yes

M 6	effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.	You understand the types of information that will likely be needed to inform response decisions and arrangements are in place to make this information available.	Yes
M 7		Your response team members have the skills and knowledge required to decide on the response actions necessary to limit harm, and the authority to carry them out.	Yes
M 8		Back-up mechanisms are available that can be readily activated to allow continued delivery of your essential service (although possibly at a reduced level) if primary networks and information systems fail or are unavailable.	Yes
M 9		Arrangements exist to augment your organisation's incident response capabilities with external support if necessary (e.g., specialist cyber incident responders).	Yes
M1 0	Testing and exercising: Your organisation carries out exercises to test response plans,	Exercise scenarios are based on incidents experienced by your and other organisations or are composed using experience or threat intelligence.	Yes

46

Copyright © 2022 Trustwave Holdings, Inc. All rights reserved.

Ref	Control	Requirements	Applicable
M1 1	using past incidents that affected your (and other) organisation, and scenarios	Exercise scenarios are documented, regularly reviewed, and validated.	Yes

M1 2	that draw on threat intelligence and your risk assessment.	Exercises are routinely run, with the findings documented and used to refine incident response plans and protective security, in line with the lessons learned.	Yes
M1 3		Exercises test all parts of your response cycle relating to particular services or scenarios (e.g., restoration of normal service levels).	Yes
N	Lessons Learned Principle: When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.		
N1	Incident root cause analysis: Your organisation identifies the root causes of incidents you experience, wherever possible.	Root cause analysis is conducted routinely as a key part of your lessons learned activities following an incident.	Yes
N2		Your root cause analysis is comprehensive, covering organisational process issues, as well as vulnerabilities in your networks, systems or software.	Yes
N3		All relevant incident data is made available to the analysis team to perform root cause analysis.	Yes
N4	Using incidents to drive improvements: Your organisation uses lessons learned from incidents to improve your security measures.	You have a documented incident review process/policy which ensures that lessons learned from each incident are identified, captured, and acted upon.	Yes

N5		Lessons learned cover issues with reporting, roles, governance, skills and organisational processes as well as technical aspects of networks and information systems.	Yes
----	--	---	-----

47

Copyright © 2022 Trustwave Holdings, Inc. All rights reserved.

Ref	Control	Requirements	Applicable
N6		You use lessons learned to improve security measures, including updating and retesting response plans when necessary.	Yes
N7		Security improvements identified as a result of lessons learned are prioritised, with the highest priority improvements completed quickly.	Yes
N8		Analysis is fed to senior management and incorporated into risk management and continuous improvement.	Yes

48

Copyright © 2022 Trustwave Holdings, Inc. All rights reserved.

Gap ANALYSIS OUTPUT

The 168 objectives in scope have been summarised to a more manageable list of 37. Each has a priority and status assigned, a reference to any dependencies or related principles, a description of the current measures in place to meet the objective requirements and initial actions to take forward.

You will note some of the low priority objectives do not have an initial action against them, this is because changes in the controls and processes implemented for the higher priority

objectives will have a bearing upon what will be needed and until they are agreed it is not possible to define what the action should be.

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
A. Governance						
Top level direction	High	In progress	Identify who has overall responsibility for security; create a forum for top-level discussions on security with a Terms of Reference, agenda, and schedule		Richard Noyau as the senior stakeholder is the person most likely to have overall responsibility. Can we confirm this, or should it be the DCMS technical lead? No forum in place, suggest we use existing regular PMO and/or technical design meetings	Agree and document the outcome of the decision Richard N in charge Look at what's required and see if it can be part of an existing meeting ToR and agenda – need to be done

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
---------	----------	--------	---------------------	---------------------	---------------------------------	-------------------

Roles and responsibilities	Medium	Not started	Identify and record all security-related roles and responsibilities, ensuring those that fulfil the roles have the capabilities to do so			Discuss, agree and document the stakeholders who hold relevant roles and their responsibilities Dan @ PoF – small number, expand on security strategy -RN
Decision-making	High	In progress	Publish key risk decisions to appropriate stakeholders, ensuring they understand their responsibilities to make decisions	Risk management	Publish to forum proposed above	Implement a process for regular security discussions, which could be part of an existing meeting

B. Risk Management

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
---------	----------	--------	---------------------	---------------------	---------------------------------	-------------------

Risk management process	High	Not started	Implement a robust and effective information security risk management process			Develop, document and agree the process (see full objectives list for detail) and carry out a risk assessment As above
Assurance	High	In progress	Identify and record an appropriate assurance methodology		Use of NIS-D for OES which aligns with the Three Private Network Security Framework	Agree and formally sign off the use of the NCSC CAF, the UK implementation of NIS D for OES Agreed
C. Asset Management						
Asset management	High	Unknown	Implement an asset register and a process to keep it up to date	Risk management	A list of physical and logical assets can be inferred from the project documentation	Create an asset register for all asset types and populate it All will have separate lists – RH to supply template

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
---------	----------	--------	---------------------	---------------------	---------------------------------	-------------------

D. Supply Chain

Supply chain	High	Unknown	Implement a supply chain risk management process, to include data sharing and incident management		BlueMesh responsible for IoT devices	<p>Confirm who has responsibility for all supplies, risk assess the suppliers and take forward any actions that arise from the results</p> <p>Will come out of asset management</p>
--------------	------	---------	---	--	--------------------------------------	---

E. Service Protection Policies and Processes

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
---------	----------	--------	---------------------	---------------------	---------------------------------	-------------------

Policy and process development	High	Not started	Document the security governance and risk management approach, technical security practice and specific regulatory compliance	Governance Risk management	Reference 3UK security policy framework	Review any applicable 3UK and PoF policies and procedures, create and document references to those which are relevant Create new policies where gaps are identified Find out what policies are being followed and see if they're fit for purpose plus any gaps
--------------------------------	------	-------------	---	-----------------------------------	---	--

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
Policy and process implementation	High	Not started	Ensure policies and processes are integrated with others where needed, followed, their correct application and security	Lessons learned		Assess and, if necessary, align the policies and procedures above with other relevant 3UK and PoF

			effectiveness is evaluated, they are communicated, and breaches are handled appropriately			policies and procedures
--	--	--	---	--	--	-------------------------

F. Identity and Access Control

Identity verification, authentication and authorisation	High	Unknown	Implement access control, including privileged access		The PoF Engineering Team - senior engineering team responsible for maintenance and operation of Quayside Cranes, PoF IT Operations - IT engineering team responsible for IT systems and solutions, and Cambridge University Engineering and AI Department are in scope	Document any processes currently in place and check for gaps and alignment with PoF policies and procedures Ask Dan and BlueMesh for info
---	------	---------	---	--	--	--

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
---------	----------	--------	---------------------	---------------------	---------------------------------	-------------------

Device management	High	Unknown	Implement restricted device usage for privileged access, certificate-based device access, independent assurance of third-party devices or networks, device identification scanning	Asset management	OAuth for devices using key pair (part of Google Cloud IoT Management System)	Check what is in place and document the outcome, then compare against the requirements Ask BlueMesh for info
Privileged user management	High	Unknown	Implement specific access controls for privileged access, record activity for analysis	Security monitoring		Check what is in place and document the outcome then compare against the requirements. Also, Review in respect of Darktrace monitoring to confirm whether privileged user activity is captured
Identity and Access Management (IdAM)	High	Unknown	Implement RBAC, least privilege, and logging and monitoring of activity	Security monitoring		Check what is in place and document the outcome then compare

						against the requirements
--	--	--	--	--	--	--------------------------

G. Data Security

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
Understanding data	High	In progress	Identify and catalogue all relevant data, including its location, quality, quantity, methods of transmission and users with access	Asset management Identity and access control	Physical Sensors (analogue), 5G, AI analytics, Siemens Weather/Operations inputs	This objective can be including as part of the asset management requirements See template above
Data in transit	High	In progress	Understand and document all data transfers, protective measures and alternative routes	Systems security	Solution designs expected to cover this 5G Standalone Non public Network - using 5G security and resilience components Remote control crane traffic to be secured and isolated TLS 5G data converted, then sent through firewall via VPN into	Review and confirm the solution designs properly meet the requirement, then create dataflow maps to include the protective measures in place

					PoF, to relay server then to public cloud	
--	--	--	--	--	---	--

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
Stored data	High	In progress	Understand and document all data storage and its protective measures	Supply chain	AI analytics in Tensor Flow hosted in Google Cloud Raw data in Cloud storage bucket then into Integrated Data Storage (Cloud SQL, Cloud Storage bucket, Firestone)	This objective can be addressed as part of the one above, by recording data storage and associated protective measures
Media / equipment sanitisation	Medium	Unknown	Record and track all devices that contain data and implement procedures to sanitise devices before disposal or reuse	Asset management		This objective should be included within the asset management requirement as media / equipment sanitisation forms part of the lifecycle of data storage assets

H. System Security

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
Secure by design	High	In progress	Design a secure network with appropriate segregation and simple data flow, with content-based attack mitigation		Solution designs	Review the solution designs and record any gaps against the requirements of the objective PoF and BlueMesh to provide info
Secure configuration	High	Not started	Use and maintain secure configurations, employ change control and patch management, only use permitted software that standard users cannot reconfigure	Asset management Security monitoring	5G Standalone Non public Network - using 5G security and resilience components 3GPP	Check whether PoF policies and procedures are relevant and applied, then consider whether there is a need to create a trial-wide process
Secure management	High	In progress	Bastion hosts or similar are used for administration; network diagrams are maintained; malware		Relay Server in DMZ separates the PoF network from the Sensor Data	Check and confirm the status of the bastion host in use

			protection is implemented		Note: where is the 5G network management GUI system?	
--	--	--	---------------------------	--	--	--

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
Vulnerability management	High	Not started	Only supported software is used, vulnerability scanning is implemented together with a patching process	Supply chain		<p>Review and confirm whether there is any vulnerability management conducted by PoF which covers the systems and networks in scope of the trial; if not, consider whether it can be extended, or a new process is required</p> <p>What is used? BlueMesh use Qualys for continuous scanning -</p>

						scope
						Pen tests under discussion

I. Resilient Networks and Systems

Control	Prior ity	Statu s	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
Resilience preparation	Low	Not started	Testing of BC/DR plans takes place, and security awareness and threat intelligence sources are used to make temporary changes where needed			No immediate action as this is dependent on the outcome of other actions
Design for resilience	Medium,	In progress	Networks and systems are designed to ensure resilience with the service not accessible from the Internet	System security	Reliable and high Uplink throughput data connectivity 5G Standalone Non public Network - using 5G security and resilience components	Review the solution designs and record any gaps against the requirements of the objective

Control	Prior ity	Statu s	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
----------------	----------------------	--------------------	--------------------------------	--------------------------------	--	------------------------------

Backups	Medium	Unknown	Automatic backups are taken, tested, secured, documented, reviewed and made accessible should an event occur. Key roles are duplicated, and knowledge is shared			<p>Check whether a backup process is in place and is applied, or if not, can a PoF process be extended to cover the trial or will a new process be required</p> <p>PoF – all backed up and resilience built in (firewalls in HA pair)</p> <p>3 - ?</p> <p>BlueMesh - ?</p>
---------	--------	---------	---	--	--	--

J. Staff Awareness and Training

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
---------	----------	--------	---------------------	---------------------	---------------------------------	-------------------

Cyber security culture	Medium	Not started	Security is seen as important to all those involved in the project with open communication and management commitment	Governance	The involvement of Commisum will help to drive a security culture going forward	No immediate action as this is dependent on the outcome of other actions, particularly under Governance which should keep in mind this objective Ask all what is in place – 3 and PoF have it in place
------------------------	--------	-------------	--	------------	---	---

K. Security Monitoring

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
Monitoring coverage	High	In progress	Monitoring data must have enough detail to reliably detect security incidents, this should include user activity, systems and networks; new systems must be in scope	Asset management	Status is based on the use of Darktrace	Gain an understanding of the Darktrace implementation and any other logging or monitoring activity, then document and check against the

						objective requirements It's a managed service, PoF responsible
Securing Logs	High	Unknown	The integrity and confidentiality of logs is maintained, with access controls and only copies used for analysis	Service protection policies and processes Identity and access control		Gain an understanding of the Darktrace implementation and any other logging or monitoring activity, then document and check against the objective requirements

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
Generating alerts	Medium	In progress	Logs are reviewed continuously in real time, alerts can be tracked to network assets, alerts are tested, additional data and knowledge is used to enrich log information		Status is based on the use of Darktrace	Gain an understanding of the Darktrace implementation and any other logging or monitoring activity, then document and check

						against the objective requirements
Identifying security incidents	Medium	Unknown	Relevant threat intelligence feeds are used and new signatures and IoCs are received and applied			Gain an understanding of the Darktrace implementation and any other logging or monitoring activity, then document and check against the objective requirements

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
Monitoring tools and skills	Medium	In progress	Suitably experienced monitoring staff are in place to analyse, investigate, prioritise and report alerts covering both security and performance; tools make use of all available data		Status is based on the use of Darktrace	Gain an understanding of the Darktrace implementation and any other logging or monitoring activity, then document and check against the objective requirements

						Monitored by Darktrace and PoF staff – DT have a SOC
--	--	--	--	--	--	--

L. Proactive Security Event Discovery

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
System abnormalities for attack detection	Low	In progress	System behaviour understood, and is used to detect and identify malicious activity	System security	Status is based on the use of Darktrace	Gain an understanding of the Darktrace implementation and any other logging or monitoring activity, then document and check against the objective requirements. Note that given the low priority this action can take place later in the project lifecycle

Proactive attack discovery	Low	Unknown	System abnormalities are searched for and generate alerts			Gain an understanding of the Darktrace implementation and any other logging or monitoring activity, then document and check against the objective requirements. Note that given the low priority this action can take place later in the project lifecycle
----------------------------	-----	---------	---	--	--	--

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
M. Response and Recovery Planning						

Response Plan	Medium	Not started	A comprehensive incident response plan is in place, documented, integrated with other areas of the service, communicated and understood			<p>Review any relevant PoF or other applicable policies and procedures to confirm if the trial is in scope, if not, consider extending existing processes or creating new ones</p> <p>PoF have own plans which should cover project – need to check (3 and PoF to discuss)</p>
Response and recovery capability	Medium	Not started	Response activities are understood and resourced, have backup mechanisms in place, with team members having the skills and knowledge needed, and specialist support is available			<p>Review any relevant PoF or other applicable policies and procedures to confirm if the trial is in scope, if not, consider extending existing processes</p>

						or creating new ones
--	--	--	--	--	--	----------------------

Control	Priority	Status	Requirement summary	Dependency /related	Description of current measures	Initial action(s)
Testing and exercising	Low	Not started	Suitable exercise scenarios are documented, run, regularly reviewed, and validated			No immediate action as this is dependent on the outcome of other actions

N. Lessons Learned

Incident root cause analysis	Low	Not started	A comprehensive root cause analysis is conducted following an incident	Security monitoring Proactive security event discovery		Review any relevant PoF or other applicable policies and procedures to confirm if the trial is in scope, if not, consider extending existing processes or creating new ones
Using incidents to drive improvements	Low	Not started	An incident review process/policy is in place to ensure lessons learned from each incident are identified, captured,	Response and recovery planning		No immediate action as this is dependent on the outcome of other actions

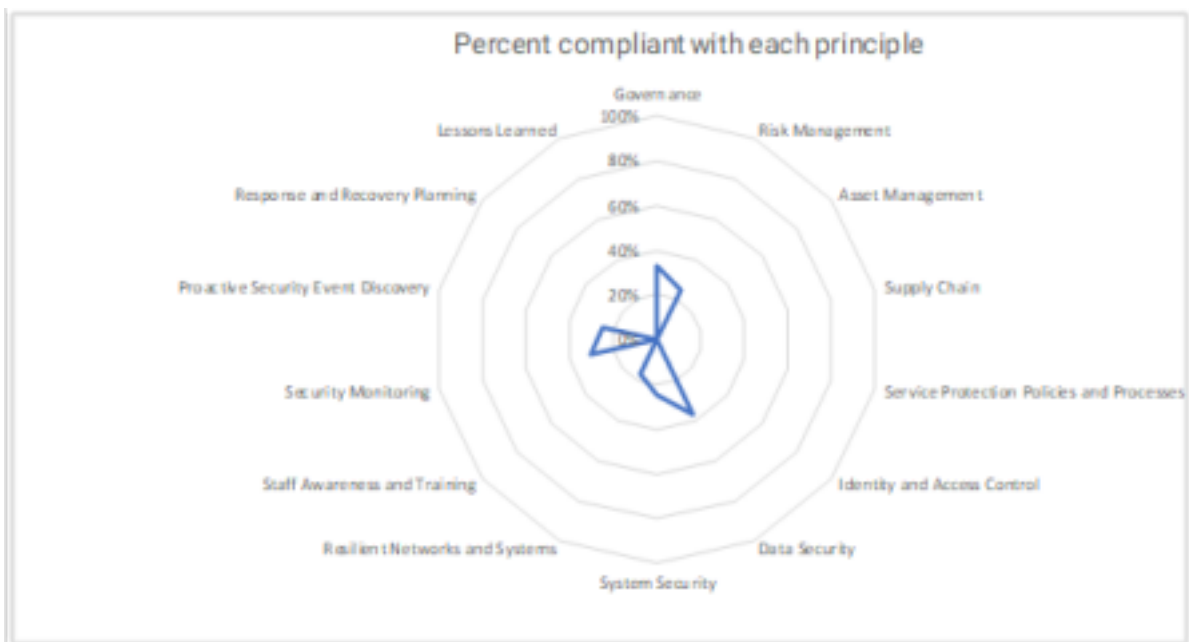
			prioritised and acted upon, with the results used to inform risk management information			
--	--	--	---	--	--	--

Current Status Summary

The priority and status of the 37 summarised objectives is shown below:

Priority		Status	
High	20	Implemented	0
Medium	11	In progress	13
Low	6	Not started	13
Total	37	Unknown	11
		Total	37

The radar chart below shows the estimated compliance with each principle; note this is based on what is known and confirmed at this time and it is expected, once progress has been made on the actions, it is likely the chart will show an increase in compliance.



APPENDIX B. SECURITY WORKING GROUP TERMS OF REFERENCE

Security Working Group for PoF 5G Trial

Overview

The PoF 5G Trial will collect and analyse data generated by crane operations at the UK's busiest port. The operation is likely to be seen as part of the UK's Critical National Infrastructure (CNI) and, as such, requires a high level of information security to be in place for protection.

The purpose of the Security Working Group (SWG) is to provide an active level of governance and assurance to the trial, establishing one of the primary building blocks of good security practice and meeting one of the requirements of NIS-D as encapsulated within the NCSC Cyber Assurance Framework.

Objective

The objective of the SWG is to provide oversight and advice throughout the trial to ensure the data, infrastructure, software and people operate securely.

Membership

The core membership of the SWG will be:

- Security Lead
- Representatives from all major stakeholders

Other parties will be invited to attend SWG meetings as required.

If any of the core membership cannot attend a deputy should be nominated. The SWG will be chaired by the Security Lead or nominated deputy.

Responsibilities

The responsibilities of the SWG are:

1. Ensure security measures in place are effective and remain effective throughout the trial;
2. Act as a point of contact and resource for any security issues raised;
3. Coordinate security activities affecting the trial;
4. Assess, prioritise and remediate any security deficiencies;
5. Escalate any risks or other issues as required;
6. Create and update relevant trial documentation;
7. Maintain and regularly review a register of risks to the trial;

8. Review the assurance methods used, ensure they are working as intended and are the most appropriate.

Meetings

The SWG will meet every two (2) weeks either separately or as part of a regular project meeting.

In the event of a major incident or other urgent requirement the SWG may be convened as required.

All meeting will be minuted and records maintained.

Meeting Agenda

1	Outstanding actions	Security Lead
2	Review of progress against requirements	Security Lead
3	Notable incidents	All
4	Planned changes	All
5	New and notable risks	All
6	Risk register review	All
7	AOB	All

APPENDIX C. IOT SECURITY SCOPE EXPANSION MILESTONE 31 REPORT

Provided by Blue Mesh Solutions and Arqit. Copyright Blue Mesh Solutions 2022

Introduction

This is the Milestone 31 report for the IoT Security workstream for the scope expansion on the 5G Ports Project.

M31 is a Project Close report to describe the project in high level terms and then to give a narrative of the outcomes and potential future benefits. The Acceptance Criteria is to complete the DCMS Excel based Benefits Realisation Template. In addition we have created the narrative below to document the main stages of the project.

Deliverables	Acceptance Criteria
---------------------	----------------------------

<ul style="list-style-type: none"> • Milestone 31: Benefits, Reporting and Close. • Milestone Target Date: 31 March 2022 • Milestone Grant Value: £4,850 	
<ul style="list-style-type: none"> • 31.1 Report benefits realised by the workstream, in the project's benefits realisation spreadsheets (DCMS template). 	<ul style="list-style-type: none"> • Acceptance Criteria: Benefits realisation outcomes accepted by DCMS, via email.

Background

Arqit contacted BMS in September 2021 and due to our involvement in the Port of Felixstowe project suggested we review their technology to add a very high level of data security to protect asset data.

The technology proposed was QuantumCloud (QC). Based on Symmetric encryption keys, and the AES256 Symmetric Algorithm which uses them, are known to be secure against quantum attack. Arqit has developed a secure way to use them at scale.

Project Proposal and Funding

A technology validation project was agreed and a proposal for grant assistance made to DCMS as an extension to the 5G Ports project. The value of the grant was £46,452 at 60% grant and the total value ex VAT £77,420.

The proposal had seven stages;

1. Project Set Up
2. QuantumCloud testing on Linux Stack into Google CLoud
3. Extraction of Linux Stack into cloud based Lambda code - serverless. a. Proof of concept to create MQTT service using QuantumCloud.
4. Market awareness - planning stage
5. Market awareness - survey and analysis stage
6. Press release of findings
7. Project Close and Benefits Realisation

During stage three we discussed the possibility of creating an MQTT version of the QuantumCloud service, as an alternative to the Lambda based test. This was agreed and instead we pivoted the project towards this new idea. The idea was selected as it has a better commercial potential in our opinion.

The technology tests were successful and the market awareness engagement discovered that industry has a potentially strong interest in Quantum Secure MQTT.

Quantum Secure Encryption of MQTT data

Incorrect implementation of MQTT deployments can lead to severe security implications for IoT deployments such as the control of devices by bad actors, accessing device data and tracking the location of end users and violating privacy requirements.

Quantum Secure MQTT is an enhanced data encryption method that is considered as unbreakable using current standard and quantum computer technology. This has great potential for ensuring that Internet of Things data used in industrial measurement and control systems are given the highest level of protection.

The global market for industrial Internet of Things (IIoT) was sized at over 263 billion U.S. dollars in 2021. The market is expected to grow to one trillion U.S. dollars by 2028.

MQTT is the chosen data transport method for IoT data because it has a smaller use of computer resources to transport data than for other methods such as HTTPS. MQTT therefore is a ubiquitous method for publishing (sending) data into a server for data manipulation.

Blue Mesh Solutions is an IoT solution developer and Arqit a quantum secure system developer, and when the two companies worked together, they shared their skills to create the first Quantum Secure MQTT data service for IoT.

Based upon a PaaS cloud self-service model, low computation burden, low cost, and high interoperability delivering the trustless and computationally secure benefits of symmetric encryption keys to all and any connected device. It is a scalable, policy based service that is quick to deploy and requires no infrastructure.

Commercial Potential

The market for IOT devices is growing and is estimated by some market commentators to reach US\$1 Trillion by 2028. Protecting IOT devices used on strategic assets is very important because interference with data can have technical and economic impacts. IOT devices increase the performance of engineering assets, but can also increase the risk of hacking and organised attacks.

By combining QuantumCloud with MQTT, Arqit and BMS have a potential product with global potential.

In February 2022 Arqit and BMS signed a technical collaboration agreement.

In May 2022 Arqit and BMS signed a commercial heads of agreement to exploit the Quantum Secure MQTT idea in collaboration. Both parties have had High Level discussion on how to create a product that customers may purchase, probably on a platform as a service model.

Benefits Realisation

It is probably too soon to make any high probability benefits realisation predictions as the project only started in December 2021 and only six months have elapsed. It is also worth mentioning that it was originally intended to run some trials inside the Port of Felixstowe on the experimental Condition Monitoring / Predictive Maintenance system we are testing.

However, given the extreme difficulties caused by COVID, then supply chain and logistics backlogs, then certain weather events, plus the underwhelmed reception from the port's technical team for more experimentation, we decided it was better to undertake development in our lab.

That said, when we started to test the Arqit encryption method it was very obvious to us that an MQTT version for IOT (and possibly PLC control) over MQTT was a positive way forward and one that could have significant demand from industry.

In exchange for working in the port, we instead created 4 sensor devices by combining an industrial (4 core) Raspberry Pi with a range of environmental sensors, we then protected these using the Arqit software and after some programming sprints, tested the Quantum Secure MQTT communication method on devices very similar to those in the port. So although the test was a lab test, it was a reasonable proxy for the in-situ sensors and sensor gateways.

The outcome was that we tested as a proxy for in port operation a very similar sensor + gateway + Quantum Secure MQTT system and so we have confidence it would work in field tests, in the port, or in other settings.

The Benefits Realisation spreadsheet has been completed and we can make the following observations.

However we can report the following:

1. Technology collaboration agreement signed.
2. Commercial Heads of Terms to commercially collaborate signed.
3. Probable visit to Oman to present to the oil and gas industry.
4. Possible link with Hutchinson Group and Three telecom.
5. Presentation at a senior level to Accenture, global IoT consulting team.
6. Presentation to procurement lead for BP.
7. Visit to Smart Ports conference in Rotterdam May 2022 to network.

Closing Comments

The IoT Security project has some exciting possibilities, as it could possibly create the highest level of IOT data security available over MQTT globally, putting the Arqit BMS collaboration into the highest technology quartile.

If we can get some traction, one or two early customers, then we will probably raise funding on this basis and invest in commercial exploitation. The grant has been an enabler for a technology sharing project that has combined slightly different skill sets to create a potentially global product.

Its very early days, however, the economic potential is very exciting.



a statement addressing how the grant recipient (lead partner) and project consortium plans to handle assets from the project; state any further delivery outputs after the grant funding period ends;

Upon the commencement of the trial, the 5G network had known constraints particularly on latency and hardware required to support it was in its infancy. The Trial has concluded reporting at much higher latency than expected, thus affecting the collection of data consistently. Despite these constraints, Hutchison learnings have provided highly valuable insight,

- 1) bringing more accurate specifications for procurement of future 5G network and remote operation of RTGs for the whole of the port.
- 2) when running multiple streams of traffic, the ability to classify the prioritisation of different traffic types across the network

ability to optimise control RTGs by increasing the number of CCTV cameras using the Port's wireless network, thus enabling there to be remote vision of the surroundings of the cranes, higher frame rates and increased picture resolution and enabling OCR capabilities. Something that Hutchison would look to possibly pick up, post 5g network successful deployment.

Hutchison also remains committed to the concept of predictive maintenance and plan to use 4G network over the next 6 months, partnered with Cambridge and Bluemesh to drive a commercially viable product.

The market for IOT devices is growing and is estimated by some market commentators to reach US\$1 Trillion by 2028. Protecting IOT devices used on strategic assets is very important because interference with data can have technical and economic impacts. IOT devices increase the performance of engineering assets but can also increase the risk of hacking and organised attacks. By combining QuantumCloud with MQTT, Arqit and BMS have a potential product with global potential. In February 2022 Arqit and BMS signed a technical collaboration agreement. In May 2022 Arqit and BMS signed a commercial head of agreement to exploit the Quantum Secure MQTT idea in collaboration. Both parties have had High Level discussion on how to create a product that customers may purchase, probably on a platform as a service model.

Master Knowledge Comms

Tab Purpose: It is a key aim of the 5G Testbeds and Trials Programme to share knowledge/findings with the 5G ecosystem. This tab captures project activity related to disseminating knowledge and findings from the project.
Update Frequency: To be updated quarterly.

Knowledge dissemination activity	Q1 - 2021	Q2 - 2021	Q3 - 2021	Q4 - 2021	Q1 - 2022	Q2 - 2022	Q3 - 2022	Q4 - 2022
1 Research outputs (e.g. patents applications/granted; prototypes; research publications; patent/publication citations)		0 Cambridge Academic Paper	ifm bun talk 0 Cambridge Uni			Enhanced Security for Strategic Assets White Paper.		
2 Number and type events (including attendance rates)	Be Better Connected conference x 3 attendees	5G Realised event, hosted table, round table discussion	None	5G World Presentation Wireless Port network Conference presentation Multimodal Conference with 5G Logistics	5GT&T Webinar Roundtable	SmartPorts conference in May – 4 5G ports attendees.		
3 Other communications activities	BMS at least 15 meetings held with sensor / electronics suppliers.	BMS website rewrite ifm insights web article	3600 Twitter impressions on a Port related Tweet Faces of 5G video with Cambridge Uni	Potential press release for 5G go live (TBC) BMS - COP26 Regional Roadshow East Midlands [11th November 2021] Manu S speaker at 5G Transport & Logistics Webinar Series Freight & Ports & Promotional Tweet (29th November 2021) Cambridge centre for Smart Infrastructure and Construction sent out their annual review and 5G ports was a highlight [Cambridge]	Press Release of First 5G data packet from Quay Cranes sent - Dec/Jan the 5G Showcase - 22nd and 23rd March BMS in attendance, Cambridge joined remotely, CKHH attended Industrial 5G Uncovered webinar series 18th/19th January; Loretta and Richard presented	AMEST Bogata 2022 conference in July 28th to 29th (remote/Manu)		
4 Increased revenue from knowledge transfer (e.g. licensing)		0		0	0			
5 Attraction and retention of qualified personnel	BMS = 2			0	0			
6 Staff training (no. staff/spend)		0		0	0			
7 Number of new Master/PhD graduates in the specialised fields		0		0	0			
8 Number of spin-offs generated		0		0	0			
9 Use Case 2						This will be run for a further 6 months and then disseminated if successful.		
10 IoT					Arqit press release sent out for IoT scope extension with BMS BMS to join the UK5G Security working group Cambridge CSIC BMS engagement moved to March.	MS30 for IoT – press release with Arqit – aiming to publish May – DCMS comment awaited UK5G showcase, attendance and presentation – 6 different relevant businesses engaged on IoT security case including BAE BMS and CKHIDD attending Smart Ports conference in Rotterdam 10th May – spoke to Alcatel about 5G IoT security. Also spoke about Fender condition monitoring with Port of Rotterdam. Press release for Arqit and BMS IoT work published	IoT Security - this is being demonstrated and disseminated in September / October 2022.	
11 What do these relate to?	University of Cambridge have published and presented 3 papers at international conferences and currently drafting a paper for submission to a high-impact journal.							
Collaboration					Collaboration report May 2022 between two projects under the DCMS 5G Testbed and Trials programme, 5G Logistics and 5G Ports. The aim of this report to identify requirements for ports and their stakeholders to enable the wider deployment of 5G within the UK port sector.			
5G lessons					Digital Catapult Industrial 5G Uncovered webinar - Industrial 5G: Technical lessons learned; ThreeUK Presenting [18th January 2022]			
Showcase (Webinar/Conferences)								

Master Re-draft Benefit Realisation



Department for
Digital, Culture,
Media & Sport

5G Testbeds and Trials Programme Benefits Realisation Record Sheet Cover Page

This sheet contains information about: the document purpose, important notes, contacts, and an index of the contents

Document Purpose:

The aim of this spreadsheet is to capture essential information about projects funded as part of the 5G Testbeds and Trials Programme run by the Department for Digital, Culture, Media & Sport. The sheet is to be filled out and updated every quarter during the timeperiod which the project is running.

Important Notes:

- 1) **Do not distribute this list without prior consent from DCMS and the project lead.** It contains information subject to the Data Protection Act 2018.
- 2) Throughout the document there are notes attached to the headings in the tables. Keep your cursor in the top right hand corner of the cell in order to see the notes.
- 3) The 5G Testbeds and Trials team are happy to discuss issues in filling out the spreadsheet. Your first port of call should be the project manager responsible for the

Contacts:

If you have any further questions about the spreadsheet please contact the document authors:
robert.carlsson@culture.gov.uk or richard.palfery@culture.gov.uk

Index

Project Information & Employment Effects: This tab captures the impact of Government funding on employment and enables follow up with partners during the programme's evaluation.

Investment Stimulation: This tab captures investment and collaborations stimulated by the project

TRLs: This tab captures the progress with innovation and time to market. Technology Readiness Levels to be chosen by projects in consultation with DCMS project managers.

Testbed Monitoring: This tab captures the characteristics of the testbed.

Use Case Monitoring: This tab captures evidence to track the project benefits, their progress, support overall findings and impact evaluation, feeds into the Programme Success Measure on contributing to improved business cases for 5G and will be useful for future partner business cases.

Knowledge Creation & Dissemination: This tab captures the knowledge/findings shared with the 5G ecosystem. This includes any project activity related to disseminating knowledge and findings from the project.

Lessons Learnt: This tab captures lessons learnt. Both process and findings lessons should be included e.g. barriers to deployment and solutions identified; best practices; new business models identified; issues with managing the project.

The Purpose: This information helps to establish the spread of Government funding on employment and enables follow up with partners during the programme's evaluation.
Update Frequency: To be filled in at the beginning of the project, to include significant suppliers as well as partners, and reviewed at the end of the project, with any changes highlighted.

Overall Project Information:		
Project Information Type	Answer	Further Comments
Lead partner	Port of Felixstowe	
Total project funding (£)	£3,483,778.86	
Total infrastructure investments (£)	£318,268	
Type of infrastructure	Core and R&D, note this is total for only with no ongoing capital value	
Business-to-business - New collaborations	One	POF and BMS.
Business-to-business - Collaborators within	Two	POF and Three, Three and BMS
Business-to-academia - New collaborations	Three	BMS and Three with University of Cambridge
Business-to-academia - Collaborators within	One	POF and Cambridge
Location(s) of Testbed(s)/Trial(s)	IP11 3SY	Port of Felixstowe

Where an academic institution is involved (insert extra rows if required. Reason for collection given as note for each header):

Name of institution	Address of institution	Appropriate project contact name and details (e-mail, phone etc)	Named contact consents to share contact details with third party evaluation consultants? Yes/No	Type of institution	Number of departments working on the project (excluding administrative)	Type of involvement	Further Comments
University of Cambridge	The Old Schools, Trinity Lane, Cambridge, CB2 1TN	Dr Aith Parkash, aip2@cam.ac.uk Mob: 245 2021	Yes	FE	1	Research	
		To understand link between place and project impact					
		From imported document					

Where a business is involved in the project: (insert extra rows if required. Reason for collection given as note for each header)

Business Name	Address of main place(s) of operations	Business details			Turnover (if trading)	Type of involvement	Contact details		Named contact consents to	Staff FTE				Additional Information Previously received funding from
		Companies house Company number	Type of business	Contact name and details (e-mail, phone etc)			Total staff	Number of staff allocated to project		Number of staff allocated to project	Number of staff allocated to project reallocated			
Blue Mesh Solutions	Unit 13, 51 Portland Road, London K11 2SH	12452317	IoT / Electronics	£500k, 2021 estimated	Collaboration Partner	Richard Brooks richard@bluemeshsolutions.com 07971 613184	Yes	5 FTE	1	1	0	0	Yes	
Port of Felixstowe	The Docks, Tomline House, Felixstowe	2990042	Port Operator	£307,122,000	Lead Partner	Karen Poulter poulter@pof.co.uk 07948015154	Yes	2524	0	0	0	0	No	
Hutchison 3G UK Ltd	Great Brighthelm Mead, 1 Vastern Road, Reading, Berkshire RG1 8DJ	3885486	Telecoms	£2,379,281,000	Collaboration Partner	Steve Wylie steve.wylie@three.co.uk 07764811000	Yes	4558	34	0	0	0	No	

Where a public body is involved: (Reason for collection given as note for each header)

Name of public body	Address of public body	Appropriate project contact name and details	Named contact consents	Type of public	Number of staff (FTE)	Type of involvement

Investment simulation

Tab Purpose: To capture additional investment/collaborations stimulated by the project

Update Frequency: To be updated quarterly, especially columns E and F. Explanations for each column are given as notes in the heading cells.

Partner organisation (name)	Original expected R&D investment levels (5G related)	Final expected R&D investment levels (5G related)	Public funding received for this project	Additional £ spent on R&D due to the funded project	Third party investment attracted (domestic/foreign)	Further investment/collaborations building on project's research outputs	Additional notes/comments
Port of Felixstowe	0	434,312	173,724.80	280,587.20	0	c. £2,000,000	5G to be extended across PoF replacing 4G and extending operations if trial is proved
Three UK	Cannot be provided	1,548,947.30	618,778.92	928,168.38	0	0	Research costs across the organisation are too vast and dispersed to be able to quantify any meaningful value
University of Cambridge	0	476,352.01	381,081.61	95,270.40	0	0	Research costs across the organisation are too vast and dispersed to be able to quantify any meaningful value
Bluemesh Solutions Ltd	0	408,693.44	245,216.07	163,477.38	None Yet	None Yet	We have 2 venture capital companies we are planning to contact once we have reached the first installation on
Blue Mesh Solutions IoT	100,000	485,173.44	48488	30992	None Yet - Planning	None Yet - Planning	Product and project collaborations emerging - we will use these to build an investment round in 2022.

Testbed Moinitoring

Tab Purpose: To determine the characteristics of the testbed. We are particularly interested in properties that demonstrate how '5G' the testbed is (e.g. latency, throughput), so baselines may be current 4G levels. Testbed properties to

Update Frequency: To be updated quarterly with the Current column values reflecting those achieved most recently.

Testbed property type	Specific Property Metric Title	Baseline	Current	Target	LAB	Description/Notes
Uplink time	Uptime service level agreement	99.90%	99.90%	99.90%		This is the service availability metric required
Download	Throughput	5Mb	5Mb	1Gbps	530 Mbps	Max capability of 4G 100Mb due to throttling, 5Mb per device
				37Mbps-100Mbps	400 Mbps	Throughput measured using a single device
Upload	Throughput	5Mb	5Mb			Throughput measured using a single device
Ping	Latency	50ms	50ms	<15ms	18ms	Load: 100Bytes, with L2TP tunnelling

TRLs

Tab Purpose: To capture progress with innovation and time to market. Technology Readiness Levels to be chosen by projects in consultation with DCMS project managers. Further explanations given as notes in column headings.

Update Frequency: Progress should be updated quarterly in the Current TRL column

EU TRL Definitions

Application/Use Case (product/service)	Description	Original TRL	Current TRL	Target TRL	Expected time to market without funding	Target time to market	Actual time to market	Sales/revenues in the UK (£)	Sales/revenues in the UK (% of total revenues)	Sales/revenues outside the UK (£)	Sales/revenues outside the UK (% of total revenues)
1	Condition Monitoring over 5G	TRL2	TR7	TRL8 (by March 2023)	Not Possible	2 years					
2	Remote control crane operations over 5G	TRL1	TRL4	TRL7	3 plus years	2 years					
3	Vibration sensors (RB)	TRL 8	TR7	TRL8 (by March 2023)	Not Possible	12 months	12 months - guess				
4	Google AI Tensaflow. Environment for AI and IoT quite advanced. In 5G Ports the cloud part is TRL 7, to develop to 8 or 9	TRL 7	TRL7	TRL8/9	Not Possible	12 months	12 months - guess				
3	Adding Quantum Security Layer to IoT Sensor Gateways and Cloud Services.	TRL 2	TRL4	TRL 4	Not possible as Blue Mesh (SME) does not have the R&D budget.	18 months					
3	Predictive Maintenance / Discord Detection AI system deployed	TRL4	TRL4	TRL 8/9 by March 2023							
3	Data Processing Centre to combine PLC and Sensor Data	TRL 7	TRL 7	TRL 8 by March 2023							

User Case Monitoring

Use Case 1: The information provided outlines 3 trial programs against remote control and typical activities. Based on comments from the SC and will be used to follow further business cases. (Minorance to be followed by Projects to use the information provided. And to be a benefit of the remote control operation. However, not to be considered as a specific Update frequency to be updated quarterly.

Use Case 2: Measures on contributing to improve the Port Managers. Further organisations given opportunities to be used monthly.

Use Case Number	Use Case Name	Use Case/Trial Information			How the benefit will be measured										Measurement data				Additional information						
		Use Case Description	Use Case Location	Number of Use Case/Trial and users	Benefit Description/Title	Benefit Owner	Metric short description	How is it measured	Unit of measure	Baseline or current performance	Date of Baseline (or time from go-live)	Target start date	Target end date	Full target value	Measure Start Date	Measure End Date	Measured Data/Values	Measured benefit per user	Cash value (£)	Is this Cash recovery? Yes / Part / No	Is this a recurring benefit?	SC Dependence	Further comments/notes		
1	SC enabled remote rubber tyred gantry (RTG) crane operation	Enabling the remote operation of RTG cranes, used in intermodal operations to ground or stack containers with the dock over SC	Port of Felixstowe	1 Crane	Enabling the accurate specifications for procurement of a production SC network for remote operation of RTG as a port	Port	"Eight first time" specification and procurement of future production SC network as a port	Time Gained	Months	12 months	29/1/2021	1/1/2022	30/9/2022	N/A	1/1/2022	30/9/2022	N/A	N/A	N/A	N/A	N/A	N/A	High dependence - SC network control in a production environment, and further technology releases are required; enough knowledge has been gained about the design and operation of the SC network to produce a specification. It is not clear if more efficient to lay fibre to RTG, therefore a SC network would be essential.	Although the trial showed that currently SC is not sufficiently stable in its performance to support remote control in a production environment, and further technology releases are required; enough knowledge has been gained about the design and operation of the SC network to produce a specification. It is not clear if more efficient to lay fibre to RTG, therefore a SC network would be essential.	
11	SC enabled remote rubber tyred gantry (RTG) crane operation	Enabling the remote operation of RTG cranes, used in intermodal operations to ground or stack containers with the dock over SC	Port of Felixstowe	1 Crane	Ability to run multiple streams of traffic with different Quality of Service across a SC network	Port	Number of different types of data traffic, each having its own priority level - the tool used to measure this is Wireshark	Number of different types of data traffic, each having its own priority level - the tool used to measure this is Wireshark	Number	5	29/1/2021	1/1/2022	30/9/2022	3 separate streams (PLC, CCTV and OT) of SC and OTCP	1/1/2022	30/9/2022	3 separate streams (PLC, CCTV and OT) of SC and OTCP	N/A	N/A	N/A	N/A	N/A	N/A	High dependence - It is not clear if more efficient to lay fibre to RTG, therefore a SC network would be essential.	
13	SC enabled remote rubber tyred gantry (RTG) crane operation	Enabling the remote operation of RTG cranes, used in intermodal operations to ground or stack containers with the dock over SC	Port of Felixstowe	1 Crane	The end to end design of a SC network to successfully run in a container port environment	Port	SC integration to remote control platform (PROT) and CCTV and ability to control an RTG under optimal conditions	Uplink speed and latency and PROT/CCTV integrated success	Uplink - Mbit/s Best performance latency - ms Passes traffic - yes/no	Uplink - Mbit/s Best performance latency - ms Passes traffic - yes/no	28/1/2021	1/1/2022	31/12/2022	Uplink - 10Mbps Latency - 15ms, but not consistent Passes traffic - yes	1/1/2022	30/9/2022	Uplink speed - 10Mbps Latency - 15ms, but not consistent Passes traffic - yes	N/A	N/A	N/A	N/A	N/A	N/A	High dependence - It is not clear if more efficient to lay fibre to RTG, therefore a SC network would be essential.	The project was able to demonstrate that at peak performance, a SC network was able to meet the latency requirements of PROT/CCTV, but the project was not able to demonstrate that this could be consistently achieved at this stage of the technology cycle.
30	SC enabled predictive asset maintenance - Access to information on discards (in-advance patterns that we detect on monitored parameters in comparison to normal operational behaviour of the component).	The discard detection system that is currently being deployed to the Port has the potential to work as a detection support mechanism that the engineering team could use to inform their inspection strategies (i.e. more planned inspections than unplanned). This is currently under development and will be tested by the Engineers before we can report a quantitative benefit. The discard detection system that is currently being deployed to the Port has the potential to work as a detection support mechanism that the engineering team could use to inform their inspection strategies (i.e. more planned inspections than unplanned).	Port of Felixstowe	6 cranes	Success or failure rate in identifying "real" faults.	Port	% of True Positives of the hot-motor related discards	The sensor and PLC data features (for April-June) are utilised and run through the discard detection system that supports time storage of discards (abnormal operational behaviour from a data perspective). These discard time-stamps are compared with the discards logs that the Port of Felixstowe holds to identify the True Positives	% of True Positives					We are analysing the April-June 2022 period. Engineers at the Port do not have access to such a system before and hence we can consider the baseline as pre-April (or post-April if would still show a performance as we are comparing to this).									Note from Maria (05/08): Please note that the system is live at the moment but we are reporting our data and not comparing our data and not comparing our data and not comparing our data. We will be reporting but that won't be reported until the benefit realisation part of the project as it is still being tested in a port environment. This is due to the issues on SC and drives that we see the whole of August		
2	SC enabled predictive asset maintenance	SC connected IoT sensors to deliver data into the AI model predicting failures and optimising maintenance	Port of Felixstowe	13 Cranes	Reduction in critical failures of fault types covered in the trial	Port	Number of failures due to monitored faults	Months	Number	5000	22/12/2020	1/1/2022	31/12/2022	500 approximately (Total)											
21	SC enabled predictive asset maintenance	SC connected IoT sensors to deliver data into the AI model predicting failures and optimising maintenance	Port of Felixstowe	13 Cranes	Reduction in downtime attributed to failures of monitored components	Port	Downtime of crane due to monitored faults	Months	Hours	1000	22/12/2020	1/1/2022	31/12/2022	100 hours approximately (Total)											
22	SC enabled predictive asset maintenance	SC connected IoT sensors to deliver data into the AI model predicting failures and optimising maintenance	Port of Felixstowe	13 Cranes	Increased number of lifts by monitored quay cranes	Port	Number of lifts (moved) per hour	SC Terminal operating systems statistics	Moves per hour	100	29/1/2021	1/1/2022	31/12/2022	100 mph											
30	IoT Enhanced Security	End to end Quantum Security on IoT data	Cambridge Science Park	One IoT based Smart Parking Solution based on Google Cloud	Port - Blue Mesh Solutions	Increases IoT security inside strategic assets - ports, refineries, etc.	Port - Blue Mesh Solutions	Number of devices protected with enhanced IoT security type	Count of devices protected	Number	27/06/2021	1/10/2021	11/03/2021	30											
31	IoT Enhanced Security	End to end Quantum Security on IoT data	Cambridge Science Park	One IoT based Smart Parking Solution based on Google Cloud	Port - Blue Mesh Solutions	Increases IoT security inside strategic assets - ports, refineries, etc.	Port - Blue Mesh Solutions	Number of other strategic asset manager contacted with results of demonstration	Count of Asset managers contacted	Number	27/06/2021	1/10/2021	11/03/2021	30											
32	IoT Enhanced Security	End to end Quantum Security on IoT data	Cambridge Science Park	One IoT based Smart Parking Solution based on Google Cloud	Port - Blue Mesh Solutions	Increases IoT security inside strategic assets - ports, refineries, etc.	Port - Blue Mesh Solutions	Commercial Agreement to share expedition signed with Apple	Number	3 Parties	27/06/2021	1/10/2021	11/03/2021	Don't know yet											

SUGGESTION FROM USERS TO ADD IN THE ORIGINAL USE CASES - WITH CONTEXT PROVIDED IN ADDITIONAL COMMENTS COLUMN - NOT DONE AS AT 28 OCTOBER 2022 (WAS ADDED FOR NEW PROJECTS)

Use Case Number	Use Case Name	Use Case Description	Use Case Location	Number of Use Case/Trial and users	Benefit Description/Title	Benefit Owner	Metric short description	How is it measured	Unit of measure	Baseline or current performance	Date of Baseline (or time from go-live)	Target start date	Target end date	Full target value	Measure Start Date	Measure End Date	Measured Data/Values	Measured benefit per user	Cash value (£)	Is this Cash recovery? Yes / Part / No	Is this a recurring benefit?	SC Dependence	Further comments/notes	
1.1	Original use case for RTG Crane (now change to)	SC enabled remote rubber tyred gantry (RTG) crane operation	Port of Felixstowe	1 Crane	Reduction in failures of remote yard cranes through communication issues	Port	Number of failures due to communication faults on Remote Yard Cranes	Maximum?	Number	0	29/1/2021	1/1/2022	31/3/2022	0										We have not been able to achieve the original Benefits realisation due to the instability of the trial SC network. It has not managed to successfully achieve the operational parameter required to safely operate an automated remote crane and therefore we have not been able to attempt the realisation of operating a crane remotely and gathering how many moves can be achieved in comparison to the existing network. What we have achieved over the trial period is a greater knowledge and understanding of some of the constraints to operating in a port environment. Please see trial report for further explanation and details.
1.2	Original use case for RTG Crane (now change to)	SC enabled remote rubber tyred gantry (RTG) crane operation	Port of Felixstowe	1 Crane	Increase in the number of moves per hour of SC remote yard crane compared to fixed power line cranes	Port	Maximum Number of lifts (moves) per hour	nGen Terminal operating systems statistics	Number	6.9 moves per absolute hour 6.8 moves for idle and service hours only	29/1/2021	1/1/2022	31/3/2022	7.66 moves per absolute hour 6.46 moves for idle and service hours only										As above.

1.3 Original use case for RTG Crane (row change 6)	5G enabled remote rubber tyred gantry (RTG) crane operation	Enabling the remote operation of RTG cranes, used in intermodal operations to ground or stack containers with the dock over 5G	Port of Felixstowe	1 Crane	5G Powered RTG's provide a more consistent productivity than standard yard cranes	PoP	Number of moves per hour average over a 24 hour period	Non-terminal operating systems statistics	Average	£7	29/1/2021	1/1/2022	31/3/2022	7.54									As above.	
1.4 New use case for RTG Crane	5G enabled remote rubber tyred gantry (RTG) crane operation	Enabling the remote operation of RTG cranes, used in intermodal operations to ground or stack containers with the dock over 5G	Port of Felixstowe	1 Crane	Enabling the accurate specifications for procurement of a production 5G network for remote operation of RTGs at a port	PoP	"Right first time" specification and procurement of future production 5G network at a port	Time Gained	Months	12 months	29/1/2021	1/1/2022	30/9/2022	N/A	1/1/2022	30/9/2022	Enough knowledge has been gained about the design and operation of the 5G network to produce a specification.	N/A	N/A	N/A	N/A	N/A	High dependence - 4G networks cannot perform this function due to limitations on throughput and latency.	Although the trial showed that currently 5G is not sufficiently stable in its performance to support remote control in a production environment, and further technology releases are required, enough knowledge has been gained about the core and the RAN and UE networks cannot perform this function due to limitations on throughput and latency.
1.2 New use case for RTG Crane	5G enabled remote RTG crane operation	Enabling the remote operation of RTG cranes, used in intermodal operations to ground or stack containers with the dock over 5G	Port of Felixstowe	1 Crane	Ability to run multiple streams of traffic with different Quality of Service across a 5G network	PoP	Number of different types of data traffic, each having its own priority levels	Number of different types of data traffic, each having its own priority levels - the tool used to measure this is Wireshark	Number	Zero	29/1/2021	1/1/2022	30/9/2022	3 separate streams (PLC, CCTV and IOT) of 5G and DSCP	1/1/2022	30/9/2022	3 separate streams (PLC, CCTV and IOT) of 5G and DSCP	N/A	N/A	N/A	N/A	N/A	High dependence - it is not cost or time efficient to lay fibre to RTGs, therefore a 5G network would be essential.	
1.3 New use case for RTG Crane	5G enabled remote RTG crane operation	Enabling the remote operation of RTG cranes, used in intermodal operations to ground or stack containers with the dock over 5G	Port of Felixstowe	1 Crane	The end to end design of a 5G network to successfully run in a container port environment	PoP	5G integration to remote control platform (PROFINET and CCTV) and ability to control an RTG under optimal conditions	Uplink speed and latency and PROFINET integration success	Uplink - Mbps Best performance latency - ms Passes traffic - yes/no	Zero	29/1/2021	1/1/2022	31/3/2022	Uplink - 40Mbps Latency - 15ms Passes traffic - yes	1/1/2022	30/9/2022	Uplink speed - 50Mbps Latency - 15ms, but not consistent Passes traffic - yes	N/A	N/A	N/A	N/A	N/A	High dependence - it is not cost or time efficient to lay fibre to RTGs, therefore a 5G network would be essential.	The project was able to demonstrate that at peak performance, a 5G network was able to meet the latency requirements of PROFINET, but the project was not able to demonstrate that this could be consistently achieved at this stage of the technology cycle.

Knowledge Creation

Tab Purpose: It is a key aim of the 5G Testbeds and Trials Programme to share knowledge/findings with the 5G ecosystem. This tab captures project activity related to disseminating knowledge and findings from the project.									
Update Frequency: To be updated quarterly									
Knowledge dissemination activity		Q1 - 2021	Q2 - 2021	Q3 - 2021	Q4 - 2021	Q1 - 2022	Q2 - 2022	Q3 - 2022	Q4 - 2022
1	Research outputs (e.g. patents applications/granted, prototypes; research publications, patent/publication citations)	0	Cambridge Academic Paper	ifm bun talk 0 Cambridge Uni			Enhanced Security for Strategic Assets White Paper.		
2	Number and type events (including attendance rates)	Be Better Connected conference x 3 attendees	5G Realised event, hosted table, round table discussion	None	5G World Presentation Wireless Port network Conference presentation Multimodal Conference with 5G Logistics	5GT&T Webinar Roundtable	SmartPorts conference in May – 4 5G ports attendees.		
3	Other communications activities	BMS at least 15 meetings held with sensor / electronics suppliers.	BMS website rewrite ifm insights web article	3600 Twitter impressions on a Port related Tweet Faces of 5G video with Cambridge Uni	Potential press release for 5G go live (TBC) BMS - COP26 Regional Roadshow East Midlands [11th November 2021] Manu S speaker at 5G Transport & Logistics Webinar Series Freight & Ports & Promotional Tweet [28th November 2021] Cambridge centre for Smart Infrastructure and Construction sent out their annual review and 5G ports was a highlight [Cambridge]	Press Release of First 5G data packet from Quay Cranes sent - Dec/Jan tba 5G Showcase - 22nd and 23rd March BMS in attendance, Cambridge joined remotely. CKHH attended Industrial 5G Uncovered webinar series 18th/19th January, Loreta and Richard presented	AMEST Bogata 2022 conference in July 26th to 29th (remote/Manu)		
4	Increased revenue from knowledge transfer (e.g. licensing)	0		0	0	0			
5	Attraction and retention of qualified personnel	BMS = 2		0	0	0			
6	Staff training (no. staff/spend)	0		0	0	0			
7	Number of new Master/PhD graduates in the specialised fields	0		0	0	0			
8	Number of spin-offs generated	0		0	0	0			
9	Use Case 2						This will be run for a further 6 months and then disseminated if successful.		
10	IoT					Arquit press release sent out for IoT scope extension with BMS BMS to join the UK5G Security working group Cambridge CSIC BMS engagement moved to March.	MIS30 for IoT – press release with Arqit – aiming to publish May – DCMS comment awaited UK5G showcase, attendance and presentation – 6 different relevant businesses engaged on IoT security case including BAE BMS and CKH/OD attending Smart Ports conference in Rotterdam 10th May – spoke to Alcatel about 5G IoT security. Also spoke about Fender condition monitoring with Port of Rotterdam. Press release for Arqit and BMS IoT work published	IoT Security - this is being demonstrated and disseminated in September / October 2022.	
11	What do these relate to?	University of Cambridge have published and presented 3 papers at international conferences and currently drafting a paper for submission to a high-impact journal.							
	Collaboration					Collaboration report May 2022 between two projects under the DCMS 5G Testbed and Trials programme, 5G Logistics and 5G Ports. The aim of this report to identify requirements for ports and their stakeholders to enable the wider deployment of 5G within the UK port sector.			
	5G lessons					Digital Catapult Industrial 5G Uncovered webinar - Industrial 5G: Technical lessons learned, ThreeUK Presenting [18th January 2022]			
	Showcase (Webinar/Conferences)								

Lessons Learnt

Tab Purpose: It is a key aim of the 5G Programme to capture and share lessons learnt. Both process and findings lessons should be included e.g. barriers to deployment and solutions identified, best practices, new business models identified, issues with managing the project. Lessons should include mitigation strategies for risks and issues that worked. Please also include **Update Frequency:** To be updated quarterly.

	Lesson Summary	Challenge (where appropriate)	Resolution (where appropriate)	Further Detail	Permission to share with wider public audience (Full)/Just DCMS (Internal Only)	Date Lesson Recorded
1	Understand and resource for GFA requirement responsibilities	Requirements for resource as the lead consortium member were not understood and as such this was not factored into the original application or costs	Change request agreed to put different resources on the claims but within the original budget.	Although the detail is clear within the context of the GFA it would be helpful to have a practitioners guide for what is actually required and likely skill set/ time overhead for lead partners so it is clearly understood outside of the legal documents	Full	12/3/2021
2	Earlier engagement of key suppliers	Concluding supply agreements with Tier 1 vendors for products that are not yet commercially available.	Required very considerable number of Group and internal senior level resources to create Trial Agreement contracts in a compressed timescale to meet DCMS requirements for evidencing POs	Negotiations of this nature take considerable effort for all Parties and flow down of DCMS collaboration conditions and sharing of documents and information cannot fully be realised in the way envisaged. Working with supply chain and subcontractors on agreements at time of bid submission would be advantageous	Just DCMS	25/3/2021
3	5G Spectrum access	Getting access to the right 5G spectrum for a large outdoor deployment such as a port where high level of performance is required	Work with equipment vendor to ensure right selection of 5G radio to maximise performance	Getting access to the right spectrum and matching 5G equipment needs careful considerations and planning specially if a long term commercial deployment is being planned	Just DCMS	26/3/2021
4	Stakeholder engagement	It's important to engage the right internal stakeholders, especially engineering teams in this context, to ensure that the business benefits of 5G are appreciated and this isn't seen as an IT project	Fortnightly meeting set up between the project consortium and Port of Felixstowe engineering to make sure all parties stay aligned		Full	24/5/2021
5	5G Spectrum access	There is no way currently to secure 5G spectrum beyond test and development license use, from Ofcom	No resolution at present beyond the lifetime of the project	If there is no solution to getting a license granted for 5G across the whole Port and potentially a wider FreePort area then the sustainability of 5G in the Port is gone and the business case for the trial participation is removed. This is a serious issue.	Full	24/5/2021
6	R&D in an operational environment	It is very hard to get access to operational equipment (cranes) in 24x7 environments for R&D Projects where the outcomes are not guaranteed and there's a lot of trial and error	Potential extension of the project timeline or reduction in scope to achieve the maximum possible with the access available		Full	25/8/2021
7	R&D 'fit outs'	What is considered acceptable for innovation projects such as approach to fixings etc. may not be (isn't) appropriate for long term use in operational areas	Pause project to remediate existing fit outs to make sure they meet Port, regulatory and Health and Safety requirements		Full	25/8/2021
8	Cashflow Forecast Spreadsheet needs a rework	It is very difficult and time consuming to provide the consolidated CFP For the project when milestones move etc.	The spreadsheet needs to be updated so that the base level of information from all partners is provided by milestone and then this flows up to create a 'by grant claim' view. The current process doesn't work for the lead partner (happy to explain more as needed)	The CFP requires information by both grant claim and milestone. The template should start with the milestone info and then build up from there. Happy to explain more as needed	Just DCMS	4/11/2021
9	Collaboration Report - Recognition of private or public 5G service dependent on size of port and breadth of use cases	Recognition that different ports having different needs	Clearly articulated use cases and value that links to overall business strategy	Ports need to identify a portfolio of different use cases with clearly articulated value which link to their overall business strategy. For larger ports, these are likely to be within the port estate and can rely solely on private 5G networks. However, for smaller ports, there may be opportunities from using or providing a public 5G service as well, particularly in more remote areas.	Full	28/6/2022
10	Collaboration Report - Flexibility in the deployment of 5G networks with ports, so that they can adapt and expand over time	'bi ban ' approach is challenging to adopt for ports	Using technology that has both 4G and 5G capabilities offers a progressive evolution	It is clear that a 'bi ban ' approach is challenging to adopt for ports and therefore using technology that has both 4G and 5G capabilities offers a progressive evolution. This applies to both the radio network and the hardware, the latter in particular being a constraint on adoption. This also enables ports to explore different use case possibilities and acquire a deeper understanding of how 5G should be best deployed to maximise its value. This then informs later, large-scale deployments.	Full	28/6/2022
11	Collaboration Report	Wider rollout of 5G network where 4G coverage does not exist	Faster rollout of 5G network	In considering the roll out of public 5G networks, there would be benefits from a faster deployment to more rural areas where ports (and other industries including tourism) may be able to exploit the capabilities offered more quickly, avoiding the lack of 4G coverage and providing access to directly using 5G. This would require a shift from providing coverage based on population centres.	Full	28/6/2022
12	Collaboration Report - upskilling	Trade Unions - negotiations	Retraining and redefinition of job descriptions	Adoption of 5G requires a collaborative approach that focuses on processes, technology and people. There is evidence that the first two are already happening successfully in the UK port sector, but people issues remain. In changing workforce attitudes and for the effective upskilling of digital literacy, there is a need to engage with trade unions effectively.	DCMS only	28/6/2022


13	Collaboration Report - Port Sector, sharing experiences, best practice and learning.	Current uncertainties when learning from 5G deployments	Port trade union associations facilitation of experiences	More generally, the port sector needs to work together in sharing experiences, best practices and learning from 5G deployment, as this will reduce many of the current uncertainties and therefore make the business benefits clearer. This will also help to develop a larger market for use cases and hardware, creating wider benefits 19 within the market. Port industry trade associations can help to facilitate this.	Full	28/6/2022
14	Collaboration Report - attracting new IT recruits to match new technologies	Competitive IT skills within wider market	Wider advertising / visibility of career opportunities across the port sector.	Working together across the sector will also be effective in addressing the issues raised around skills and the attractiveness of the industry to new recruits, particularly in new areas of expertise such as IT solution developers. Ports are competing with other industries for this talent and presenting a wider view of the opportunities across the sector will help career pathways to emerge, even if these are across different ports.	Full	28/6/2022
15	Collaboration Report - Funding of Trials including skills development	Bringing together of multiple government departments and UK port strategy	Combining digitalisation within existing port policy developments such as freeports.	Continued government support is required across the above recommendations. Financial support through initiatives such as the 5G Testbeds and Trials Programme help to offset the risks and can encourage collaborative working. Funding for skills development, such as through Apprenticeships, can help bring in new talent. Beyond financial support, government can also facilitate adoption through planning regulations as well as spectrum standardisation and access. A challenge, however, is bringing together multiple government departments and a UK port strategy could be a means to achieve this, combining digitalization with existing port policy developments such as freeports.	Full	28/6/2022
16	Paper titled 'Lessons learned from an IoT Deployment in Quay Side Cranes in the Port of Felixstowe' co-authored by the team from University of Cambridge, BMS, Three UK and Port of Felixstowe captures all the steps taken, challenges faced and the lessons learned with sourcing, installation, calibration and communication of sensors in this deployment. This paper is now published and presented at the AMEST 2022 international conference, also supplied to DOMS. Summary of each lesson follows:-	See below	See below	See below	Full	21/3/2022
17	IoT deployment - sourcing, installation, calibration and communication of sensors in this deployment.	Know your sensing targets and measurable parameters	These targets are identified by an analysis of failure modes which inform the engineering parameters (e.g. vibration, temperature) that needs to be monitored	Lesson 1. Know your sensing targets and measurable parameters. It is key for any IoT deployment to start by identifying and prioritising the components for monitoring. These targets are identified by an analysis of failure modes which inform the engineering parameters (e.g. vibration, temperature) that needs to be monitored. In other words, identifying which assets fail more often and what are the failure types; what are the symptoms and effects of each failure. Symptoms define the parameters to be measured.	Full	21/3/2022
18	IoT deployment - sourcing, installation, calibration and communication of sensors in this deployment.	Operational challenges associated with sensor targets should be considered. These locations may change during sensor calibration, but they are always good indicators to begin the deployment.	involve experts' opinion becomes a valuable source of information to identify them. Deeper engagement with engineers / main stakeholders / during the bid stage	Lesson 2. Involve targets' experts. The operational challenges associated with sensor targets should be considered. These locations may change during sensor calibration, but they are always good indicators to begin the deployment. Experts' opinion becomes a valuable source of information to identify them. For instance, vibration monitoring on the QC hoist ropes was not practical due to the variable speed at which the hoists operate. Experts' opinion is valuable not only to identify the targets but also to advise the ideal location to place a sensor for monitoring each component. Experienced engineers and technicians are even capable of identifying any potential faults to the engines and gearboxes by sound or touch, which translates into the exact location of the housing in a component to monitor.	Full	21/3/2022
19	IoT deployment - sourcing, installation, calibration and communication of sensors in this deployment.	Communication issues between the sensors and the network gateways.	Understand targets' environment.	Lesson 3. Understand targets' environment. The targets and exact locations may be constrained by communication issues between the sensors and the network gateways. The need for power in wired sensors can also become a challenge, especially in industrial settings like a crane where cable management is not trivial. The length of cables may cause fluctuations and drop of power resulting in faults (e.g. sensors not sending data, not measuring the features correctly).	Full	21/3/2022
20	IoT deployment - sourcing, installation, calibration and communication of sensors in this deployment.	Selecting appropriate Sensors: Custom sensors may be considered when within a budget or when available industry-ready sensors cannot measure identified parameters	Particular sensor communication technologies may be a requirement depending on the sensors' environment and amount and speed of data to be transmitted.	Lesson 3.2 Sensor selection. Industry-ready and custom sensors are the two options for sensor selection. Custom sensors may be considered when within a budget or when available industry-ready sensors cannot measure identified parameters. In that case, the individual parts to monitor desired parameters must be acquired separately and assembled on a common board. It is common to start off with an industry-graded sensor and try to mirror or extend its capabilities into a custom sensor prototype. Particular sensor communication technologies may be a requirement depending on the sensors' environment and amount and speed of data to be transmitted.	Full	21/3/2022
21	IoT deployment - sourcing, installation, calibration and communication of sensors in this deployment.	Manage Custom sensors expectations	Prototypes must be developed into final product	Lesson 4. Manage custom sensors expectations Custom sensors' parts are normally cheaper, sometimes even as precise as industry-grade sensors, but require expert knowledge for assembly, configuration, and data collection. While custom sensors are flexible and can accommodate all desired parts in one board, but that makes them bulkier and less power efficient. Custom sensors must be first considered as prototypes and expectations from their performance must be managed. After testing, prototypes must be developed into final products with reliable power and communication efficiency to support sensor performance	Full	21/3/2022
22	IoT deployment - sourcing, installation, calibration and communication of sensors in this deployment.	Testing of sensors. Sensor candidates must be capable of measuring between and beyond the working thresholds of each parameter the targets operate in a normal situation.	Testing must be executed in a controlled environment to check against manufacturer specifications, but also in terms of communication performance. Sensor communication technologies and protocols must be tested in the final environment. Temperature, corrosion, and water protection may be considered at this point.	Lesson 5. Test your sensors. Sensor candidates must be capable of measuring between and beyond the working thresholds of each parameter the targets operate in a normal situation. The failure modes inform the required precision using the sensors which will play a role while analysing changes in the operation of the monitored targets. Both, industry-ready or custom sensors must be first tested in a controlled environment to check against manufacturer specifications, not only in terms of parameters and thresholds but also in terms of communication performance. Sensor communication technologies (e.g. Bluetooth, WiFi, 5G), and protocols (e.g., MQTT, Kafka, Websockets, CoAP) must be tested in the final environment. Temperature, corrosion, and water protection may be considered at this point.	Full	21/3/2022
23	IoT deployment - sourcing, installation, calibration and communication of sensors in this deployment.	Be aware of supply chains - availability of parts and lead times	Alternative suppliers should be sought beforehand to mitigate against any delays.	Lesson 6. Be aware of supply chains Some sensor candidates and parts might be unavailable or delayed due to supply chain issues. Additionally, some sensors could malfunction during the deployment and may need replacements. Alternative suppliers should be sought beforehand to mitigate any delays. Calibration is necessary to ensure precision, consistency of measured parameters and minimise uncertainty. Sensor location plays a major role in the precision of the sensor which must be attached as close as possible to the real source of the parameter generation in the monitored target. For example, a gearbox dissipates energy in the form of temperature which will be higher than normal if the couplings are not well lubricated and need maintenance; the temperature sensor should be attached as close as safely possible to the couplings, and if it must be in the gearbox housing, gearbox ventilation intake must be avoided. Knowledge from inspectors and maintenance engineers can also be valuable while calibrating the sensors since they can identify the best location in each monitored target for most sensors. Sensor locations must be identical across all similar monitored targets	Full	21/3/2022
24	IoT deployment - sourcing, installation, calibration and communication of sensors in this deployment.	Consistent sensors' position. Some sensors measure vibration across 3-axes and the readings depend on the orientation in which the sensors are positioned	Consistent positioning should be addressed even more carefully when assembling custom sensors, where each part should be assembled identically.	Lesson 7. Consistent sensors' position Sensor consistency is affected by how the sensor is positioned on the monitoring target. This can be easily overlooked while attaching the sensors to the selected location. Sensor position impacts how sensed parameters are interpreted. For instance, some sensors measure vibration across 3-axes and the readings depend on the orientation in which the sensors are positioned. The readings must be pre-processed for analysis if the sensors are positioned inconsistently. This increases the complexity of the data pipelines. Consistent positioning shall be addressed even more carefully when assembling custom sensors, where each part should be assembled identically. Most sensors have some reference to this in their specification/documentation, but visible marks on the sensor itself support consistent deployment.	Full	21/3/2022

25	IOT deployment - sourcing, installation, calibration and communication of sensors in this deployment.	Mirror sensor configuration.	Keep the exact same configuration for similar monitored targets to ensure consistency.	Lesson 8. Mirror sensor configuration. Some sensor parameters can be fine-tuned through configuration, sometimes in terms of sampling frequency (i.e., how often a measurement is taken), or granularity (i.e., how precise each measurement is). It is vital to keep the exact same configuration for similar monitored targets to ensure consistency.	Full	21/3/2022				
26	IOT deployment - sourcing, installation, calibration and communication of sensors in this deployment.	Document deployment Sensors' location, position, and configuration must be documented thoroughly to minimise uncertainty while using generated data during analysis.	Important to create and document sensible and understandable sensors identifiers	Lesson 9. Document deployment Sensors' location, position, and configuration must be documented thoroughly to minimise uncertainty while using generated data during analysis. It is vital to understand where do the readings generated from the sensors actually belong within the monitored targets and locations. Therefore, it is important to create and document sensible and understandable sensors identifiers that enable the association with monitored targets and locations while collecting and analysing the data (see 3.6).	Full	21/3/2022				
27	IOT deployment - sourcing, installation, calibration and communication of sensors in this deployment.	Volume and Velocity It is easy to underestimate the amount of data and the rate that an IoT deployment can generate	The low latency technologies (e.g., WiFi/5G) offer real-time interactivity for services which is key to the success of near-real time condition monitoring and predictive maintenance of critical assets like QCs	Lesson 10. Do not underestimate. Volume and Velocity It is easy to underestimate the amount of data and the rate that an IoT deployment can generate. Vibration sensors are a good example of this problem, as they can generate data in the range of kHz (i.e., 1000s of data points/second). Reliable communication technology selection supports the scalability of IoT projects. The low latency technologies (e.g., WiFi/5G) offer real-time interactivity for services which is key to the success of near-real time condition monitoring and predictive maintenance of critical assets like QCs. Large-bandwidth technologies supports more sensors to be connected. Edge computing can be employed to reduce the communication burden.	Full	21/3/2022				
28	IOT deployment - sourcing, installation, calibration and communication of sensors in this deployment.	Maintenance of the sensors themselves must not be overlooked, as it is almost impossible to avoid communication losses during their lifetime.	Battery and power connectors corrosion in tough environments (like in a port environment) must be taken into account as well. Asset management procedures apply to the sensors similarly to any other monitored target, with the advantage of sensors reporting self-monitoring data themselves	Lesson 11. Do not forget sensor maintenance. It is also important to consider the maintenance of the sensors themselves, as it is almost impossible to avoid communication losses during their lifetime. Even with good coverage, sensors and gateways misbehaviour will create communication issues. Power losses are the usual reason for loss of communication. Most sensors work on batteries, but even if the sensors are wired, power fluctuations or source power losses must be considered. This power and communication losses reflect in timestamps drifts (see 3.6) and data loss. Battery and power connectors corrosion in tough environments (like in a port environment) must be taken into account as well. Asset management procedures apply to the sensors similarly to any other monitored target, with the advantage of sensors reporting self-monitoring data themselves	Full	21/3/2022				
29	IOT deployment - sourcing, installation, calibration and communication of sensors in this deployment.	Without a time stamp reference, data loses its meaning because it cannot be matched with the real operation of the monitored asset.	Sensors and gateways must be synchronised with a common time server used by the network and maintained when a clock drift is identified.	Lesson 12. No timestamp, no value. Without a time stamp reference, data loses its meaning because it cannot be matched with the real operation of the monitored asset. Not only is important to get a timestamp at the source but also at every other node in the network that the data is passing through. Many times, the clocks at the sensors drift causing data quality defects. Having a timestamp at other nodes supports the identification of these data quality defects and serve as the solution since the next node timestamp can be used. Sensors and gateways must be synchronised with a common time server used by the network and maintained when a clock drift is identified.	Full	21/3/2022				
30	IOT deployment - sourcing, installation, calibration and communication of sensors in this deployment.	Ensure concurrent storage.	Assure partition of the ingestion job adequately	Lesson 13. Ensure concurrent storage. When it comes to storage, data from IoT sensors can be produced rapidly which can cause concurrency problems. It is also important to partition the ingestion job adequately to prevent data losses if individual ingestion modules fail.	Full	21/3/2022				
31	IOT deployment - sourcing, installation, calibration and communication of sensors in this deployment.	Individual readings are sometimes stored at file level, causing indexing problems in the file system.	Appropriate aggregation of readings must be plan to avoid slow data reading	Lesson 14. Plan data life-cycle. Data storage granularity is commonly ignored. Individual readings are sometimes stored at file level, causing indexing problems in the file system. Appropriate aggregation of readings must be plan to avoid slow data reading. Data storage capacity can become a constraint in the medium-long term. Not only because of the vast amount of data collected every minute but also in cases when data shall be pre-processed and stored again. Historical data storage and disposal criteria should be adopted from the very start to avoid overloading the data service	Full	21/3/2022				
32	Little physical team building during the project, relationships are quite distant and limited	Largely due to COVID-related restrictions	More on site collaboration workshops		Full	9/8/2022				
33	Collaboration between University of Cambridge and BMS is strong and well developed.				Full	9/8/2022				
34	Choosing Partners - Could talk about Partners – one that can scale down and invested interested pin showcasing /sharing successful outcome.	Shared accountability to a successful outcome	Partner that can scale down and share of costs at Trial level - use as a showcase to promote mutual growth in business.	Felixstowe port is a small network in comparison to wider large scale businesses. Their maybe less monetary gain for the but as a show case, if proven successful, would promote uptake across other ports and/or other industries.	Full	9/8/2022				
<p>When completing the BR templates, project partners should note the following:</p> <table border="1"> <thead> <tr> <th>DO</th> <th>DON'T</th> </tr> </thead> <tbody> <tr> <td> <ol style="list-style-type: none"> 1) Explain the context of the lesson learned/issue [What/Why/How] 2) Emphasise what the impact on the project's life cycle or project outcome/end result? 3) Use clear, succinct, plain language, avoid technical jargon. 4) Provide a substantial level of detail when recording lessons, if possible. 5) Always keep in mind how the lessons and benefits will affect the end user. This is key (eg. increase efficiency in delivering X, less time to complete Y) 6) Liaise with DCMS project leads on a regular basis and keep track of lessons that are 'active' and 'closed'. 7) Ensure there is a consistent approach when recording all your lessons. </td> <td> <ol style="list-style-type: none"> 1) Include vague descriptions of lessons. A concise summary will suit. 2) Use technical jargon. Think of your audience - DCMS officials may not be familiar with technical terms. 3) Include lessons as the last item on the agenda during review meetings. 4) Leave any blanks when recording information in the BR templates. 5) Treat completing the lessons learned as an admin task. </td> </tr> </tbody> </table>							DO	DON'T	<ol style="list-style-type: none"> 1) Explain the context of the lesson learned/issue [What/Why/How] 2) Emphasise what the impact on the project's life cycle or project outcome/end result? 3) Use clear, succinct, plain language, avoid technical jargon. 4) Provide a substantial level of detail when recording lessons, if possible. 5) Always keep in mind how the lessons and benefits will affect the end user. This is key (eg. increase efficiency in delivering X, less time to complete Y) 6) Liaise with DCMS project leads on a regular basis and keep track of lessons that are 'active' and 'closed'. 7) Ensure there is a consistent approach when recording all your lessons. 	<ol style="list-style-type: none"> 1) Include vague descriptions of lessons. A concise summary will suit. 2) Use technical jargon. Think of your audience - DCMS officials may not be familiar with technical terms. 3) Include lessons as the last item on the agenda during review meetings. 4) Leave any blanks when recording information in the BR templates. 5) Treat completing the lessons learned as an admin task.
DO	DON'T									
<ol style="list-style-type: none"> 1) Explain the context of the lesson learned/issue [What/Why/How] 2) Emphasise what the impact on the project's life cycle or project outcome/end result? 3) Use clear, succinct, plain language, avoid technical jargon. 4) Provide a substantial level of detail when recording lessons, if possible. 5) Always keep in mind how the lessons and benefits will affect the end user. This is key (eg. increase efficiency in delivering X, less time to complete Y) 6) Liaise with DCMS project leads on a regular basis and keep track of lessons that are 'active' and 'closed'. 7) Ensure there is a consistent approach when recording all your lessons. 	<ol style="list-style-type: none"> 1) Include vague descriptions of lessons. A concise summary will suit. 2) Use technical jargon. Think of your audience - DCMS officials may not be familiar with technical terms. 3) Include lessons as the last item on the agenda during review meetings. 4) Leave any blanks when recording information in the BR templates. 5) Treat completing the lessons learned as an admin task. 									






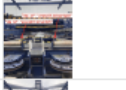
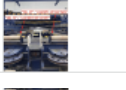
Substainability Statement

<p>Provide a statement addressing how the grant recipient (lead partner) and project consortium plans to handle assets from the project; state any further delivery outputs after the grant funding period ends;</p>
<p>Hutchison's current 4G network becomes end of life by 2023 and plans to go to tender with the intent of replacing with 5G network across the whole of the port.</p>
<p>Learnings from the trial will enable:-</p> <ul style="list-style-type: none"> · more accurate definition for the 5G tender specification · the ambition to make further use of CCTV cameras and provide remote vision of surrounding cranes.
<p>Hutchison also remains committed to the concept of predictive maintenance to drive a commercially viable product and plan to continue maturing insight with the University of Cambridge and Bluemesh Solutions over the next 6 months, using the ports 4G existing network.</p>
<p>Plans to handle Assets beyond project closure, both Core and RAN assets are end of life with no operational use and will be disposed of responsibly as appropriate. IOT devices will remain for 6 months to support maturing insight on predictive maintenance, may remain on site but have no future commercial value?. Richard to affirm.</p>
<p><i>The market for IOT devices is growing and is estimated by some market commentators to reach US\$1 Trillion by 2028. Protecting IOT devices used on strategic assets is very important because interference with data can have technical and economic impacts. IOT devices increase the performance of engineering assets but can also increase the risk of hacking and organised attacks. By combining QuantumCloud with MQTT, Arqit and BMS have a potential product with global potential. In February 2022 Arqit and BMS signed a technical collaboration agreement. In May 2022 Arqit and BMS signed a commercial head of agreement to exploit the Quantum Secure MQTT idea in collaboration. Both parties have had High Level discussion on how to create a product that customers may purchase, probably on a platform as a service model.</i></p>

Configuration

		5G Testbeds and Trials Programme Benefits Realisation Record Sheet Cover Page	
This sheet contains information about: the document purpose, important notes, contacts, and an index of the contents			
VERSION	Master Re-draft Benefits Realisation 5G Ports Tracker V3 01.09.2022	Master Re-draft Benefits Realisation 5G Ports Tracker V6 07.09.2022	Master Re-draft Benefits Realisation 5G Ports Tracker V7 14.09.2022
DATE	31/8/2022	7/9/2022	14/9/2022
Project information & Employment			
TRLs	No. 1 and 3 Actual and Targets updated		
Testbed monitoring			
Use Case Monitoring	Use Case 1. Metrics updated - Technical Knowledge suggested via Graham to be agreed with ALL. Use Case 3. Added "Access to information on discords (ie unusual patterns that we detect on monitored parameters in comparison to normal operational behaviour of the component)". Loretto and Manu to affirm wording but needs to be agreed with ALL.	Updated with quantifiable metric and issued to DCMS	
Knowledge Creation & Dissemination	3 items (No. 9-11) added via Phillipa and agreed Many items added noted from Monthly Project Delivery Group slides Jan 2022-Jul 2022 and Communication Tracker		
Lessons Learnt	4 items (No. 9-12) added via Phillipa and agreed Lessons from Collaboration report included. Made reference AMEST paper Lessons Learned from IOT deployment in quayside cranes in the port of Felixstowe		
IOT Strategic Paper	Trustive - Three POF 5G Trial Documentation Set v1.0.pft	Security Trial 5G	

Asset Register - Blue Mesh (Processing Resources)

Asset Name/ID	Type	Description	Classification	Make	Model	Serial number	MAC	IP	Physical Location	Ping Test 5G CPE (10.232.3.33 to 10.232.3.38)	Ping Test Relay Server (10.100.8.12)
C51-001	Crane - Sensor	Sensor - Gearbox		ST Micro	STWINKT1B		n/a	n/a	5gport/qc51/backvideogear		
C51-002	Crane - Sensor	Sensor - Gearbox		ST Micro	STWINKT1B		n/a	n/a	5gport/qc51/frontleftgear		
C51-003	Crane - Sensor	Sensor - Gearbox		ST Micro	STWINKT1B		n/a	n/a	5gport/qc51/backrightgear		
C51-004	Crane - Sensor	Sensor - Gearbox		ST Micro	STWINKT1B		n/a	n/a	5gport/qc51/frontrightgear		
C51-005	Crane - Sensor	Sensor - Trolley Drive		ST Micro	STWINKT1B		n/a	n/a	5gport/qc51/middle		
C51-006	Crane - Sensor	Sensor - Drive Cabin Right		ST Micro	STWINKT1B		n/a	n/a	5gport/qc51/driverright		
C51-007	Crane - Sensor	Sensor - Drive Cabin Left		ST Micro	STWINKT1B		n/a	n/a	5gport/qc51/driverleft		
C52-001	Crane - Sensor	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc52/backvideogear		
C52-002	Crane - Sensor	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc52/frontleftgear		
C52-003	Crane - Sensor	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc52/backrightgear		
C52-004	Crane - Sensor	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc52/frontrightgear		
C52-005	Crane - Sensor	Sensor - Trolley Drive	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc52/middle		
C52-006	Crane - Sensor	Sensor - Drive Cabin Right	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc52/driverright		
C52-007	Crane - Sensor	Sensor - Drive Cabin Left	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc52/driverleft		
C53-001	Crane - Sensor	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc53/backvideogear		
C53-002	Crane - Sensor	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc53/frontleftgear		
C53-003	Crane - Sensor	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc53/backrightgear		
C53-004	Crane - Sensor	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc53/frontrightgear		
C53-005	Crane - Sensor	Sensor - Trolley Drive	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc53/middle		
C53-006	Crane - Sensor	Sensor - Drive Cabin Right	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc53/driverright		
C53-007	Crane - Sensor	Sensor - Drive Cabin Left	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc53/driverleft		
C54-001	Crane - Sensor	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc54/backvideogear		
C54-002	Crane - Sensor	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc54/frontleftgear		
C54-003	Crane - Sensor	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc54/backrightgear		
C54-004	Crane - Sensor	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B		n/a	n/a	5gport/qc54/frontrightgear		

C54-005	Crane - Sensor	▼	Sensor - Trolley Drive	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc54/middle		
C54-006	Crane - Sensor	▼	Sensor - Drive Cabin Right	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc54/driverright		
C54-007	Crane - Sensor	▼	Sensor - Drive Cabin Left	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc54/driverleft		
C55-001	Crane - Sensor	▼	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc55/backvideogear		
C55-002	Crane - Sensor	▼	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc55/frontleftgear		
C55-003	Crane - Sensor	▼	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc55/backrightgear		
C55-004	Crane - Sensor	▼	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc55/frontrightgear		
C55-005	Crane - Sensor	▼	Sensor - Trolley Drive	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc55/middle		
C55-006	Crane - Sensor	▼	Sensor - Drive Cabin Right	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc55/driverright		
C55-007	Crane - Sensor	▼	Sensor - Drive Cabin Left	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc55/driverleft		
C56-001	Crane - Sensor	▼	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc56/backvideogear		
C56-002	Crane - Sensor	▼	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc56/frontleftgear		
C56-003	Crane - Sensor	▼	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc56/backrightgear		
C56-004	Crane - Sensor	▼	Sensor - Gearbox	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc56/frontrightgear		
C56-005	Crane - Sensor	▼	Sensor - Trolley Drive	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc56/middle		
C56-006	Crane - Sensor	▼	Sensor - Drive Cabin Right	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc56/driverright		
C56-007	Crane - Sensor	▼	Sensor - Drive Cabin Left	see images for Crane 51	ST Micro	STWINKT1B	n/a	n/a	5gport/qc56/driverleft		
C51-001	Crane - Sensor Ga	▼	Sensor - Gearbox		Raspberry Pi	Raspberry Pi 4 Model B (2GB)			5gport/qc51/backvideogear	2.7ms	14.4ms
C51-002	Crane - Sensor Ga	▼	Sensor - Gearbox		Raspberry Pi	Raspberry Pi 4 Model B (2GB)			5gport/qc51/frontleftgear	3.6ms	19.6ms
C51-003	Crane - Sensor Ga	▼	Sensor - Gearbox		Raspberry Pi	Raspberry Pi 4 Model B (2GB)			5gport/qc51/backrightgear	3.4ms	16.1ms
C51-004	Crane - Sensor Ga	▼	Sensor - Gearbox		Raspberry Pi	Raspberry Pi 4 Model B (2GB)			5gport/qc51/frontrightgear	4.2ms	17.8ms
C51-005	Crane - Sensor Ga	▼	Sensor - Trolley Drive		Raspberry Pi	Raspberry Pi 4 Model B (2GB)			5gport/qc51/middle	2.7ms	14.3ms
C51-006	Crane - Sensor Ga	▼	Sensor - Drive Cabin Right		Raspberry Pi	Raspberry Pi 4 Model B (2GB)			5gport/qc51/driverright	19.1ms	19.3ms
C51-007	Crane - Sensor Ga	▼	Sensor - Drive Cabin Left		Raspberry Pi	Raspberry Pi 4 Model B (2GB)			5gport/qc51/driverleft	11.1ms	18.1ms
C52-001	Crane - Sensor Ga	▼	Sensor - Gearbox		Raspberry Pi	Raspberry Pi 4 Model B (2GB)			5gport/qc52/backvideogear	3ms	19.5ms
C52-002	Crane - Sensor Ga	▼	Sensor - Gearbox		Raspberry Pi	Raspberry Pi 4 Model B (2GB)			5gport/qc52/frontleftgear	3.9ms	16.6ms
C52-003	Crane - Sensor Ga	▼	Sensor - Gearbox		Raspberry Pi	Raspberry Pi 4 Model B (2GB)			5gport/qc52/backrightgear	4.8ms	16.7ms
C52-004	Crane - Sensor Ga	▼	Sensor - Gearbox		Raspberry Pi	Raspberry Pi 4 Model B (2GB)			5gport/qc52/frontrightgear	4.2ms	15ms
C52-005	Crane - Sensor Ga	▼	Sensor - Trolley Drive		Raspberry Pi	Raspberry Pi 4 Model B (2GB)			5gport/qc52/middle	4.5ms	14.1ms
C52-006	Crane - Sensor Ga	▼	Sensor - Drive Cabin Right		Raspberry Pi	Raspberry Pi 4 Model B (2GB)			5gport/qc52/driverright	6.1ms	18ms








C52-007	Crane - Sensor Ga	Sensor - Drive Cabin Left	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc52/driverleft	5.6ms	18.2ms
C53-001	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc53/backvideogear		
C53-002	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc53/frontleftgear	4.8ms	17.6ms
C53-003	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc53/backrightgear	3.4ms	17.2ms
C53-004	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc53/frontrightgear	4.1ms	16.6ms
C53-005	Crane - Sensor Ga	Sensor - Trolley Drive	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc53/middle	4ms	15.4ms
C53-006	Crane - Sensor Ga	Sensor - Drive Cabin Right	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc53/driverright	10.3ms	20.8ms
C53-007	Crane - Sensor Ga	Sensor - Drive Cabin Left	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc53/driverleft	8.8ms	21.9ms
C54-001	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc54/backvideogear	3.8ms	22ms
C54-002	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc54/frontleftgear		
C54-003	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc54/backrightgear	5.4ms	17.1ms
C54-004	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc54/frontrightgear	3.2ms	20.1ms
C54-005	Crane - Sensor Ga	Sensor - Trolley Drive	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc54/middle	4.4ms	14.7ms
C54-006	Crane - Sensor Ga	Sensor - Drive Cabin Right	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc54/driverright		
C54-007	Crane - Sensor Ga	Sensor - Drive Cabin Left	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc54/driverleft		
C55-001	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc55/backvideogear	23.7ms	14.8ms
C55-002	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc55/frontleftgear	3.6ms	17.8ms
C55-003	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc55/backrightgear	2.6ms	14.4ms
C55-004	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc55/frontrightgear	2.6ms	12.1ms
C55-005	Crane - Sensor Ga	Sensor - Trolley Drive	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc55/middle	3.4ms	15.8ms
C55-006	Crane - Sensor Ga	Sensor - Drive Cabin Right	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc55/driverright		
C55-007	Crane - Sensor Ga	Sensor - Drive Cabin Left	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc55/driverleft	5.9ms	16.5ms
C56-001	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc56/backvideogear	3.8ms	18.2ms
C56-002	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc56/frontleftgear	4.4ms	13.7ms
C56-003	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc56/backrightgear	4.9ms	16.3ms
C56-004	Crane - Sensor Ga	Sensor - Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc56/frontrightgear	3.2ms	19.1ms
C56-005	Crane - Sensor Ga	Sensor - Trolley Drive	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc56/middle	4.3ms	15.7ms
C56-006	Crane - Sensor Ga	Sensor - Drive Cabin Right	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc56/driverright		
C56-007	Crane - Sensor Ga	Sensor - Drive Cabin Left	Raspberry Pi	Raspberry Pi 4 Model B (2GB)	5gport/qc56/driverleft	8.3ms	16.6ms
C-51 WIFI 1	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 918 - External Version	Crane 51 - Drivers Cabin		
C-51 WIFI 2	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 918 - External Version	Crane 51 Connected to 5G Access Point via Ethernet Cable.		
C-52 WIFI 1	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 918 - External Version	Crane 52 - Drivers Cabin		
C-52 WIFI 2	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 918 - External Version	Crane 52 Connected to 5G Access Point via Ethernet Cable.		
C-53 WIFI 1	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 918 - External Version	Crane 53 - Drivers Cabin		
C-53 WIFI 2	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 918 - External Version	Crane 53 Connected to 5G Access Point via Ethernet Cable.		
C-54 WIFI 1	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 918 - External Version	Crane 54 - Drivers Cabin		
C-54 WIFI 2	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 918 - External Version	Crane 54 Connected to 5G Access Point via Ethernet Cable.		
C-55 WIFI 1	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 918 - External Version	Crane 55 - Drivers Cabin		
C-55 WIFI 2	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 918 - External Version	Crane 55 Connected to 5G Access Point via Ethernet Cable.		
C-56 WIFI 1	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 918 - External Version	Crane 56 - Drivers Cabin		
C-56 WIFI 2	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 918 - External Version	Crane 56 Connected to 5G Access Point via Ethernet Cable.		
Virtual Server 1	Application Server	Relay Server (MQTT)	Windows	see PoF Data Centre	Virtual inside PoF		
Virtual Server 2	Application Server	Data Processing Server (PLC and Data Compression)	Linux (Ubuntu)	see PoF Data Centre	Virtual inside PoF		
Google Instance 1	Application Server	MQTT Bridge (PoF to Cambridge)	Linux (Ubuntu)	Linux 10 Debian / Buster	Virtual inside Google West		

C56-005	Crane - Sensor Gatew.	Software for Pi Gateways	On cranes as Sensor Gateway Device	Raspian / Debian 10	Open-Source			Blue Mesh Solutions	Update schedule to be decided
C56-006	Crane - Sensor Gatew.	Software for Pi Gateways	On cranes as Sensor Gateway Device	Raspian / Debian 10	Open-Source			Blue Mesh Solutions	Update schedule to be decided
C56-007	Crane - Sensor Gatew.	Software for Pi Gateways	On cranes as Sensor Gateway Device	Raspian / Debian 10	Open-Source			Blue Mesh Solutions	Update schedule to be decided
C-51 WIFI 1	WiFi Access Point	Software for WiFi access points.	On cranes to control WiFi hardware and sec	1.4.2.25/08/2021	Proprietary	September > December 2021		Blue Mesh Solutions	Update schedule to be decided
C-51 WIFI 2	WiFi Access Point	Software for WiFi access points.	On cranes to control WiFi hardware and sec	1.4.2.25/08/2022	Proprietary	September > December 2021		Blue Mesh Solutions	Update schedule to be decided
C-52 WIFI 1	WiFi Access Point	Software for WiFi access points.	On cranes to control WiFi hardware and sec	1.4.2.25/08/2023	Proprietary	September > December 2021		Blue Mesh Solutions	Update schedule to be decided
C-52 WIFI 2	WiFi Access Point	Software for WiFi access points.	On cranes to control WiFi hardware and sec	1.4.2.25/08/2024	Proprietary	September > December 2021		Blue Mesh Solutions	Update schedule to be decided
C-53 WIFI 1	WiFi Access Point	Software for WiFi access points.	On cranes to control WiFi hardware and sec	1.4.2.25/08/2025	Proprietary	September > December 2021		Blue Mesh Solutions	Update schedule to be decided
C-53 WIFI 2	WiFi Access Point	Software for WiFi access points.	On cranes to control WiFi hardware and sec	1.4.2.25/08/2026	Proprietary	September > December 2021		Blue Mesh Solutions	Update schedule to be decided
C-54 WIFI 1	WiFi Access Point	Software for WiFi access points.	On cranes to control WiFi hardware and sec	1.4.2.25/08/2027	Proprietary	September > December 2021		Blue Mesh Solutions	Update schedule to be decided
C-54 WIFI 2	WiFi Access Point	Software for WiFi access points.	On cranes to control WiFi hardware and sec	1.4.2.25/08/2028	Proprietary	September > December 2021		Blue Mesh Solutions	Update schedule to be decided
C-55 WIFI 1	WiFi Access Point	Software for WiFi access points.	On cranes to control WiFi hardware and sec	1.4.2.25/08/2029	Proprietary	September > December 2021		Blue Mesh Solutions	Update schedule to be decided
C-55 WIFI 2	WiFi Access Point	Software for WiFi access points.	On cranes to control WiFi hardware and sec	1.4.2.25/08/2030	Proprietary	September > December 2021		Blue Mesh Solutions	Update schedule to be decided
C-56 WIFI 1	WiFi Access Point	Software for WiFi access points.	On cranes to control WiFi hardware and sec	1.4.2.25/08/2031	Proprietary	September > December 2021		Blue Mesh Solutions	Update schedule to be decided
C-56 WIFI 2	WiFi Access Point	Software for WiFi access points.	On cranes to control WiFi hardware and sec	1.4.2.25/08/2032	Proprietary	September > December 2021		Blue Mesh Solutions	Update schedule to be decided
Virtual Server 1	Application Server	O/S - Windows	Data Centre						
Virtual Server 1	Application Server	MQTT - Mosquito	Data Centre	Version 2.0.13	27.10	Open-Source			
Virtual Server 2	Application Server	O/S Linux 10	Data Centre						
Virtual Server 2	Application Server	Makitron PLC Data Logger	Data Centre						
Google Cloud Instance	Application Server	O/S Linux 10	Google Cloud	Linux 10		Open-Source	Rental - PaaS	Blue Mesh Solutions	
Google Cloud Instance	Application Server	MQTT - Mosquito	Google Cloud	Version 2.0.13	27.10	Open-Source			

(Information)

Data name	Description and Purpose	Classification	Generating location	Storage location	Purpose	Groups with Access	Owner	Other Notes
HR	HR data for staff and contractors	Confidential	HR users	HR server and backups	Staff management	HR_Users	HR Director	

Asset Register - Master copy 14 Sept (Processing Resources)

Asset Name/ID	Type	Description	Classification	Make	Model	Serial number	MAC	IP	Physical Location	Date Purchased	Owner	Other Notes	Patch & Update	Ping Test 5G LTE (18.232.3.35) (18.232.3.36)	Ping Test Hedy Server (10.100.8.12)
ASSET 0001	Server	File storage	Confidential	Dell	PowerEdge T330	X1234567890	00:00:5e:00:53:af	10.10.1.55	First floor server room	10/22/2019	IT Director	Will be replaced as part of cloud migration			
C51 001	Crane Sensor	Sensor Gearbox		ST Micro	STWINK1B		n/a	n/a	5gport/qc51/backvideogear	2021	Blue Mesh Solutions				
C51 002	Crane Sensor	Sensor Gearbox		ST Micro	STWINK1B		n/a	n/a	5gport/qc51/frontleftgear		Blue Mesh Solutions				
C51 003	Crane Sensor	Sensor Gearbox		ST Micro	STWINK1B		n/a	n/a	5gport/qc51/backrightgear		Blue Mesh Solutions				
C51 004	Crane Sensor	Sensor Gearbox		ST Micro	STWINK1B		n/a	n/a	5gport/qc51/frontrightgear		Blue Mesh Solutions				
C51 005	Crane Sensor	Sensor Trolley Drive		ST Micro	STWINK1B		n/a	n/a	5gport/qc51/middle		Blue Mesh Solutions				
C51 006	Crane Sensor	Sensor Drive Cabin Right		ST Micro	STWINK1B		n/a	n/a	5gport/qc51/driverright		Blue Mesh Solutions				
C51 007	Crane Sensor	Sensor Drive Cabin Left		ST Micro	STWINK1B		n/a	n/a	5gport/qc51/driverleft		Blue Mesh Solutions				
C52 001	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc52/backvideogear		Blue Mesh Solutions				
C52 002	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc52/frontleftgear		Blue Mesh Solutions				
C52 003	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc52/backrightgear		Blue Mesh Solutions				
C52 004	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc52/frontrightgear		Blue Mesh Solutions				
C52 005	Crane Sensor	Sensor Trolley Drive	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc52/middle		Blue Mesh Solutions				
C52 006	Crane Sensor	Sensor Drive Cabin Right	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc52/driverright		Blue Mesh Solutions				
C52 007	Crane Sensor	Sensor Drive Cabin Left	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc52/driverleft		Blue Mesh Solutions				
C53 001	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc53/backvideogear		Blue Mesh Solutions				
C53 002	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc53/frontleftgear		Blue Mesh Solutions				
C53 003	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc53/backrightgear		Blue Mesh Solutions				
C53 004	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc53/frontrightgear		Blue Mesh Solutions				
C53 005	Crane Sensor	Sensor Trolley Drive	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc53/middle		Blue Mesh Solutions				
C53 006	Crane Sensor	Sensor Drive Cabin Right	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc53/driverright		Blue Mesh Solutions				
C53 007	Crane Sensor	Sensor Drive Cabin Left	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc53/driverleft		Blue Mesh Solutions				
C54 001	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc54/backvideogear		Blue Mesh Solutions				
C54 002	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc54/frontleftgear		Blue Mesh Solutions				
C54 003	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc54/backrightgear		Blue Mesh Solutions				
C54 004	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc54/frontrightgear		Blue Mesh Solutions				
C54 005	Crane Sensor	Sensor Trolley Drive	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc54/middle		Blue Mesh Solutions				
C54 006	Crane Sensor	Sensor Drive Cabin Right	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc54/driverright		Blue Mesh Solutions				
C54 007	Crane Sensor	Sensor Drive Cabin Left	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc54/driverleft		Blue Mesh Solutions				
C55 001	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc55/backvideogear		Blue Mesh Solutions				
C55 002	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc55/frontleftgear		Blue Mesh Solutions				
C55 003	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc55/backrightgear		Blue Mesh Solutions				
C55 004	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc55/frontrightgear		Blue Mesh Solutions				
C55 005	Crane Sensor	Sensor Trolley Drive	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc55/middle		Blue Mesh Solutions				
C55 006	Crane Sensor	Sensor Drive Cabin Right	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc55/driverright		Blue Mesh Solutions				
C55 007	Crane Sensor	Sensor Drive Cabin Left	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc55/driverleft		Blue Mesh Solutions				
C56 001	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc56/backvideogear		Blue Mesh Solutions				
C56 002	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc56/frontleftgear		Blue Mesh Solutions				
C56 003	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc56/backrightgear		Blue Mesh Solutions				
C56 004	Crane Sensor	Sensor Gearbox	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc56/frontrightgear		Blue Mesh Solutions				
C56 005	Crane Sensor	Sensor Trolley Drive	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc56/middle		Blue Mesh Solutions				
C56 006	Crane Sensor	Sensor Drive Cabin Right	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc56/driverright		Blue Mesh Solutions				
C56 007	Crane Sensor	Sensor Drive Cabin Left	see images for Crane 51	ST Micro	STWINK1B		n/a	n/a	5gport/qc56/driverleft		Blue Mesh Solutions			2.7ms	14.4ms
C51 001	Crane Sensor Ga	Sensor Gearbox		Raspberry Pi	Raspberry Pi 4 Model B (2GB)				5gport/qc51/backvideogear	May 2021 > September 2021				3.6ms	19.6ms
C51 002	Crane Sensor Ga	Sensor Gearbox		Raspberry Pi	Raspberry Pi 4 Model B (2GB)				5gport/qc51/frontleftgear	May 2021 > September 2021				3.4ms	16.1ms
C51 003	Crane Sensor Ga	Sensor Gearbox		Raspberry Pi	Raspberry Pi 4 Model B (2GB)				5gport/qc51/backrightgear	May 2021 > September 2021				4.2ms	17.8ms
C51 004	Crane Sensor Ga	Sensor Gearbox		Raspberry Pi	Raspberry Pi 4 Model B (2GB)				5gport/qc51/frontrightgear	May 2021 > September 2021				2.7ms	14.3ms
C51 005	Crane Sensor Ga	Sensor Trolley Drive		Raspberry Pi	Raspberry Pi 4 Model B (2GB)				5gport/qc51/middle	May 2021 > September 2021				19.1ms	19.3ms

C31 006	Crane	Sensor Ga	Sensor	Drive Cabin Right	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:51/driverlight	May 2021 > September 2021					11.1ms	18.1ms
C31 007	Crane	Sensor Ga	Sensor	Drive Cabin Left	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:51/driverleft	May 2021 > September 2021					3ms	19.5ms
C32 001	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:52/backvideogear	May 2021 > September 2021					3.9ms	16.6ms
C32 002	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:52/frontleftgear	May 2021 > September 2021					4.8ms	16.7ms
C32 003	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:52/backrightgear	May 2021 > September 2021					4.2ms	15ms
C32 004	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:52/frontrightgear	May 2021 > September 2021					4.5ms	14.1ms
C32 005	Crane	Sensor Ga	Sensor	Trolley Drive	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:52/middle	May 2021 > September 2021					6.1ms	18ms
C32 006	Crane	Sensor Ga	Sensor	Drive Cabin Right	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:52/driverlight	May 2021 > September 2021					5.6ms	18.2ms
C32 007	Crane	Sensor Ga	Sensor	Drive Cabin Left	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:52/driverleft	May 2021 > September 2021		Spport/lq:53/backvideogear				
C33 001	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:53/backvideogear	May 2021 > September 2021					4.8ms	17.6ms
C33 002	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:53/frontleftgear	May 2021 > September 2021					3.4ms	17.2ms
C33 003	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:53/backrightgear	May 2021 > September 2021					4.1ms	16.6ms
C33 004	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:53/frontrightgear	May 2021 > September 2021					4ms	15.4ms
C33 005	Crane	Sensor Ga	Sensor	Trolley Drive	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:53/middle	May 2021 > September 2021					10.3ms	20.8ms
C33 006	Crane	Sensor Ga	Sensor	Drive Cabin Right	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:53/driverlight	May 2021 > September 2021					8.8ms	21.9ms
C33 007	Crane	Sensor Ga	Sensor	Drive Cabin Left	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:53/driverleft	May 2021 > September 2021					3.8ms	22ms
C34 001	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:54/backvideogear	May 2021 > September 2021		Spport/lq:54/frontleftgear				
C34 002	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:54/frontleftgear	May 2021 > September 2021					5.4ms	17.1ms
C34 003	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:54/backvideogear	May 2021 > September 2021					3.2ms	20.1ms
C34 004	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:54/frontrightgear	May 2021 > September 2021					4.4ms	14.7ms
C34 005	Crane	Sensor Ga	Sensor	Trolley Drive	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:54/middle	May 2021 > September 2021						
C34 006	Crane	Sensor Ga	Sensor	Drive Cabin Right	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:54/driverlight	May 2021 > September 2021						
C34 007	Crane	Sensor Ga	Sensor	Drive Cabin Left	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:54/driverleft	May 2021 > September 2021						
C35 001	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:55/backvideogear	May 2021 > September 2021					23.7ms	14.8ms
C35 002	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:55/frontleftgear	May 2021 > September 2021					3.6ms	17.8ms
C35 003	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:55/backrightgear	May 2021 > September 2021					2.6ms	14.4ms
C35 004	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:55/frontrightgear	May 2021 > September 2021					2.6ms	12.1ms
C35 005	Crane	Sensor Ga	Sensor	Trolley Drive	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:55/middle	May 2021 > September 2021			Spport/lq:55/driverlight		3.4ms	15.8ms
C35 006	Crane	Sensor Ga	Sensor	Drive Cabin Right	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:55/driverlight	May 2021 > September 2021					5.9ms	16.5ms
C35 007	Crane	Sensor Ga	Sensor	Drive Cabin Left	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:55/driverleft	May 2021 > September 2021					3.8ms	18.2ms
C36 001	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:56/backvideogear	May 2021 > September 2021					4.4ms	13.7ms
C36 002	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:56/frontleftgear	May 2021 > September 2021					4.9ms	16.3ms
C36 003	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:56/backrightgear	May 2021 > September 2021					3.2ms	19.1ms
C36 004	Crane	Sensor Ga	Sensor	Gearbox	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:56/frontrightgear	May 2021 > September 2021					4.3ms	15.7ms
C36 005	Crane	Sensor Ga	Sensor	Trolley Drive	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:56/middle	May 2021 > September 2021			Spport/lq:56/driverlight			
C36 006	Crane	Sensor Ga	Sensor	Drive Cabin Right	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:56/driverlight	May 2021 > September 2021					8.3ms	16.6ms
C36 007	Crane	Sensor Ga	Sensor	Drive Cabin Left	Raspberry Pi	Raspberry Pi 4 Model B (2GB)				Spport/lq:56/driverleft	May 2021 > September 2021						
C 51 WiFi 1	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 938 - External Version						Crane 51 - Drivers Cabin							
C 51 WiFi 2	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 938 - External Version						Crane 51 Connected to 5G Access Point via Ethernet Cable.							
C 52 WiFi 1	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 938 - External Version						Crane 52 - Drivers Cabin							
C 52 WiFi 2	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 938 - External Version						Crane 52 Connected to 5G Access Point via Ethernet Cable.							
C 53 WiFi 1	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 938 - External Version						Crane 53 - Drivers Cabin							
C 53 WiFi 2	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 938 - External Version						Crane 53 Connected to 5G Access Point via Ethernet Cable.							
C 54 WiFi 1	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 938 - External Version						Crane 54 - Drivers Cabin							
C 54 WiFi 2	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 938 - External Version						Crane 54 Connected to 5G Access Point via Ethernet Cable.							
C 55 WiFi 1	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 938 - External Version						Crane 55 - Drivers Cabin							
C 55 WiFi 2	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 938 - External Version						Crane 55 Connected to 5G Access Point via Ethernet Cable.							
C 56 WiFi 1	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 938 - External Version						Crane 56 - Drivers Cabin							
C 56 WiFi 2	WiFi Access Point	WiFi Access Point for Crane Sensors	Drey Tek	Vigor 938 - External Version						Crane 56 Connected to 5G Access Point via Ethernet Cable.							
Virtual Server 1	Application Server	Relay Server (MQTT)	Windows	see PoF Data Centre						Virtual inside PoF	n/a						Blue Mesh & PoF
Virtual Server 2	Application Server	Data Processing Server (PLC and Data Compression)	Linux (Ubuntu)	see PoF Data Centre						Virtual inside PoF	n/a						Blue Mesh & PoF
Google Instance 1	Application Server	MQTT Bridge (PoF to Cambridge)	Linux (Ubuntu)	Linux 10 Debian / Buster						Virtual inside Google West	n/a						Blue Mesh & Google
CPE (IoT) QCS2	CPE	5G ODU	WNC	FWO 50E	IMEI: 35507011000 00:DA-E4-04-8B-D7	10.232.3.33				QCS2							234513133790031
CPE (IoT) QCS6	CPE	5G ODU	WNC	FWO 50E	IMEI: 35507011000 00:DA-E4-55-AE-16	10.232.3.34				QCS6							234513133790032
CPE (IoT) QCS3	CPE	5G ODU	WNC	FWO 50E	IMEI: 35507011000 00:DA-E4-C3-8A-24	10.232.3.35				QCS3							234513133790089
CPE (IoT) QCS1	CPE	5G ODU	WNC	FWO 50E	IMEI: 35507011000 00:DA-E4-05-26-0A	10.232.3.36				QCS1							234513133790094
CPE (IoT) QCS4	CPE	5G ODU	WNC	FWO 50E	IMEI: 35507011000 00:DA-E4-07-45-97	10.232.3.37				QCS4							234513133790095
CPE (IoT) QCS5	CPE	5G ODU	WNC	FWO 50E	IMEI: 35507011000 00:DA-E4-F8-DC-61	10.232.3.38				QCS5							234513133790012
CPE CCTV	CPE	5G ODU	WNC	FWO 50E	IMEI: 35507011000 00:DA-E4-8D-F2-D8	10.232.3.3				eRTG Block E							234513133790172 (CCTV CPE)
CPE PLC	CPE	5G ODU	WNC	FWO 50E	IMEI: 35507011000 00:DA-E4-92-20-84	10.232.3.17				eRTG Block E							234513133790025 (PLC CPE)
Ericsson 5G	5G Core	5G Core	Dell R640	Dell R640						Tomline HouseDC							5GCore, LIDM, E VNFs, Standalone CNOM & Tools
Ericsson 5G	5G IP Router	5G IP Router	Router 6675	Router 6675						Tomline HouseDC							Ericsson IP Router
Ericsson 5G	5G NR Baseband	5G NR Baseband	Baseband 6630	Baseband 6630						Tomline HouseDC							Ericsson BBU
Ericsson 5G R8125 1	5G Micro Radio Sy	5G Micro Radio System	Radio 4408	Radio 4408						Light Pole R8125							Ericsson RRU
Ericsson 5G R8123 2	5G Micro Radio Sy	5G Micro Radio System	Radio 4408	Radio 4408						Light Pole R8125							Ericsson RRU
Ericsson 5G R8123 1	5G Micro Radio Sy	5G Micro Radio System	Radio 4408	Radio 4408						Light Pole R8123							Ericsson RRU
Ericsson 5G	5G Synchronizatio	GNSS	Robust GNSS	GNSS						Tomline HouseDC							Ericsson GNSS
Ericsson 5G	5G DC Power Supp	DC Power Supply	Vertiv NetSure	Vertiv NetSure 2100 A31 53						Tomline HouseDC							Ericsson Power supply

C-51 WIFI 1	WiFi Access Point	Software for WiFi access points.		On cranes to control WiFi hardware and sec 1.4.2 25/08/2021	Proprietary		September > December 2021	Blue Mesh Solutions	Update schedule to be decided
C-51 WIFI 2	WiFi Access Point	Software for WiFi access points.		On cranes to control WiFi hardware and sec 1.4.2 25/08/2022	Proprietary		September > December 2021	Blue Mesh Solutions	Update schedule to be decided
C-52 WIFI 1	WiFi Access Point	Software for WiFi access points.		On cranes to control WiFi hardware and sec 1.4.2 25/08/2023	Proprietary		September > December 2021	Blue Mesh Solutions	Update schedule to be decided
C-52 WIFI 2	WiFi Access Point	Software for WiFi access points.		On cranes to control WiFi hardware and sec 1.4.2 25/08/2024	Proprietary		September > December 2021	Blue Mesh Solutions	Update schedule to be decided
C-53 WIFI 1	WiFi Access Point	Software for WiFi access points.		On cranes to control WiFi hardware and sec 1.4.2 25/08/2025	Proprietary		September > December 2021	Blue Mesh Solutions	Update schedule to be decided
C-53 WIFI 2	WiFi Access Point	Software for WiFi access points.		On cranes to control WiFi hardware and sec 1.4.2 25/08/2026	Proprietary		September > December 2021	Blue Mesh Solutions	Update schedule to be decided
C-54 WIFI 1	WiFi Access Point	Software for WiFi access points.		On cranes to control WiFi hardware and sec 1.4.2 25/08/2027	Proprietary		September > December 2021	Blue Mesh Solutions	Update schedule to be decided
C-54 WIFI 2	WiFi Access Point	Software for WiFi access points.		On cranes to control WiFi hardware and sec 1.4.2 25/08/2028	Proprietary		September > December 2021	Blue Mesh Solutions	Update schedule to be decided
C-55 WIFI 1	WiFi Access Point	Software for WiFi access points.		On cranes to control WiFi hardware and sec 1.4.2 25/08/2029	Proprietary		September > December 2021	Blue Mesh Solutions	Update schedule to be decided
C-55 WIFI 2	WiFi Access Point	Software for WiFi access points.		On cranes to control WiFi hardware and sec 1.4.2 25/08/2030	Proprietary		September > December 2021	Blue Mesh Solutions	Update schedule to be decided
C-56 WIFI 1	WiFi Access Point	Software for WiFi access points.		On cranes to control WiFi hardware and sec 1.4.2 25/08/2031	Proprietary		September > December 2021	Blue Mesh Solutions	Update schedule to be decided
C-56 WIFI 2	WiFi Access Point	Software for WiFi access points.		On cranes to control WiFi hardware and sec 1.4.2 25/08/2032	Proprietary		September > December 2021	Blue Mesh Solutions	Update schedule to be decided
Virtual Server 1	Application Server	O/S - Windows		Data Centre					
Virtual Server 1	Application Server	MQTT - Mosquito		Data Centre	Version 2.0.13 27.10.21	Open-Source			
Virtual Server 2	Application Server	O/S Linux 10		Data Centre					
Virtual Server 2	Application Server	Maktron PLC Data Logger		Data Centre					
Google Cloud Instance	Application Server	O/S Linux 10		Google Cloud	Linux 10	Open-Source	Rental - PaaS	Blue Mesh Solutions	
Google Cloud Instance	Application Server	MQTT - Mosquito		Google Cloud	Version 2.0.13 27.10.21	Open-Source			
CPE (IoT)-QC52	CPE Firmware	CPE Firmware		CPE	3PN_v01.03.214640_a346254e97_fota	Proprietary			
CPE (IoT)-QC56	CPE Firmware	CPE Firmware		CPE	3PN_v01.03.214640_a346254e97_fota	Proprietary			
CPE (IoT)-QC53	CPE Firmware	CPE Firmware		CPE	3PN_v01.03.214640_a346254e97	Proprietary			
CPE (IoT)-QC51	CPE Firmware	CPE Firmware		CPE	3PN_v01.03.214640_a346254e97	Proprietary			
CPE (IoT)-QC54	CPE Firmware	CPE Firmware		CPE	3PN_v01.03.214640_a346254e97	Proprietary			
CPE (IoT)-QC55	CPE Firmware	CPE Firmware		CPE	3PN_v01.03.214640_a346254e97	Proprietary			
CPE -CCTV	CPE Firmware	CPE Firmware		CPE	3PN_v01.06.220460_d27c35bcd2_fota	Proprietary			
CPE -PLC	CPE Firmware	CPE Firmware		CPE	3PN_v01.06.220460_d27c35bcd2_fota	Proprietary			
Ericsson 5G	5G Core	5G Core		5G Core	Trial Release	Proprietary			
Ericsson 5G	5G IP Router	5G IP Router		5G IP Router	NA	NA			
Ericsson 5G	5G NR Baseband	5G NR Baseband		5G BBU	21.Q2 Release	Proprietary			
Ericsson 5G_RB125_1	5G Micro Radio System	5G Micro Radio System		5G RRU	21.Q2 Release	Proprietary			
Ericsson 5G_RB125_2	5G Micro Radio System	5G Micro Radio System		5G RRU	21.Q2 Release	Proprietary			
Ericsson 5G_RB123_1	5G Micro Radio System	5G Micro Radio System		5G RRU	21.Q2 Release	Proprietary			
Ericsson 5G	5G Synchronization	5G Synchronization		5G GNSS	NA	NA			
Ericsson 5G	5G DC Power Supply	5G DC Power Supply		5G Power supply	NA	NA			

(Information)

Data name	Description and Purpose	Classification	Generating location	Storage location	Purpose	Groups with Access	Owner	Other Notes
HR	HR data for staff and contractors	Confidential	HR users	HR server and backups	Staff management	HR_Users	HR Director	

Image Credit: The Bristol Port Company

Anchoring 5G in UK Ports

Understanding how to accelerate the roll out of 5G within the UK port sector

Findings from the 5G Smart Ports Collaboration as part of the Department for Culture, Media and Sport's 5G Testbeds and Trials programme

May 2022



Contents

Contents	2
Acknowledgements.....	2
Executive Summary.....	3
Introduction	4
Why is 5G important for ports?	6
5G Logistics.....	8
5G Ports.....	9
Approach Taken	10
Operational Challenges.....	11
Enablers and Barriers	14
Conclusions and Recommendations	18

Report by:

Andrew Potter, Cardiff University, PotterAT@cardiff.ac.uk

Yingli Wang, Cardiff University, WangY14@cardiff.ac.uk

Mohamed Naim, Cardiff University, NaimMM@cardiff.ac.uk

Content correct as at May 2022



Acknowledgements

This work would not have been possible without support and contributions from many people and organisations.

Funding for the research has come from the Department of Culture, Media and Sport through the 5G Testbeds and Trials programme, and is a collaborative project between the 5G Logistics and 5G Ports projects. We would like to thank all the partners on these projects for their help and support throughout the collaborative project.

We would also like to thank all the participants who gave up their time for either the workshop or interview. The variety and quality of the discussions has provided detailed insights into 5G within the UK port sector. We are also grateful for the support of the UK Major Ports Group when organising the workshop.

Executive Summary

The port sector plays a critical role in supporting the UK economy, and the efficient and effective movement of trade through these locations is essential. As with other industrial sectors, digitalization is becoming increasingly important and 5G enabled technologies offer new opportunities to further enhance this efficiency and effectiveness.

However, the UK port sector can often be conservative in its adoption of new technologies. While 5G adoption is generally at an early stage, there is the opportunity for the sector to become more proactive in adopting this technology. This report explores in more detail what the opportunities are for 5G technology in the UK port sector, and the enablers and barriers to widespread adoption.

5G will overcome many of the current shortcomings with 4G and Wifi based applications, and we have identified a range of potential use cases for the port environment including:

- Health and safety
- Automation
- Tracking
- Drones
- Asset monitoring
- Data sharing
- Value adding applications

What is clear, however, is that any 5G deployment will need to bring together multiple use cases in order to justify the investment in the technology.

However, there are a wider range of barriers and enablers to wider adoption of 5G, which we categorise as:

- Investment decision making, which includes alignment with digital strategy, building the business case in light of existing investments and asset renewals and the availability of funds.
- Use case benefits, which are often seen as uncertain now but are likely to be significant as new use cases develop in the future.
- Implementation related, with technology readiness being a barrier but collaborative working acting as an enabler.
- Workforce concerns, including the skills and attitudes of the existing port workforce and recruitment challenges where the port industry needs to access new pools of talent.
- Government support, through financial measures as well as standards, spectrum availability and supporting skills development.

From this understanding of barriers and enablers, the UK port sector can work to adopt 5G more effectively. In doing so, sharing experiences, best practices and learning will further enhance understanding within the sector.

Introduction

Ports play a critical role in UK supply chains, supporting the international trade of both imports and exports. It is critical that goods move as smoothly and efficiently through ports as possible to ensure that supply chains do not become disrupted.

The past 30 years has seen a significant change in port operations, with technology playing an increasingly important role. Digitalization is becoming commonplace, with the latest generation of ports now being labelled Smart Ports. Figure 1 shows the evolution towards Smart Ports and their characteristics.

A key facilitator of this evolution has been the growth in web-enabled technologies, and increased capability of telecommunication networks to support this. The emergence of 5G offers new opportunities for ports to embrace digitalization, with increased capabilities for handling data allowing improvements to both physical and information flows. It is clear that the next 5 years will see investment in 5G increase significantly by both ports and the wider logistics sector.

As of 2022, the adoption of 5G within the UK ports sector is still at an early stage, with some initial use case trials funded both by the Department for Culture, Media and Sport (DCMS) as well as by the ports themselves. However, there is interest more generally within the sector, recognizing the opportunities the technology can bring.

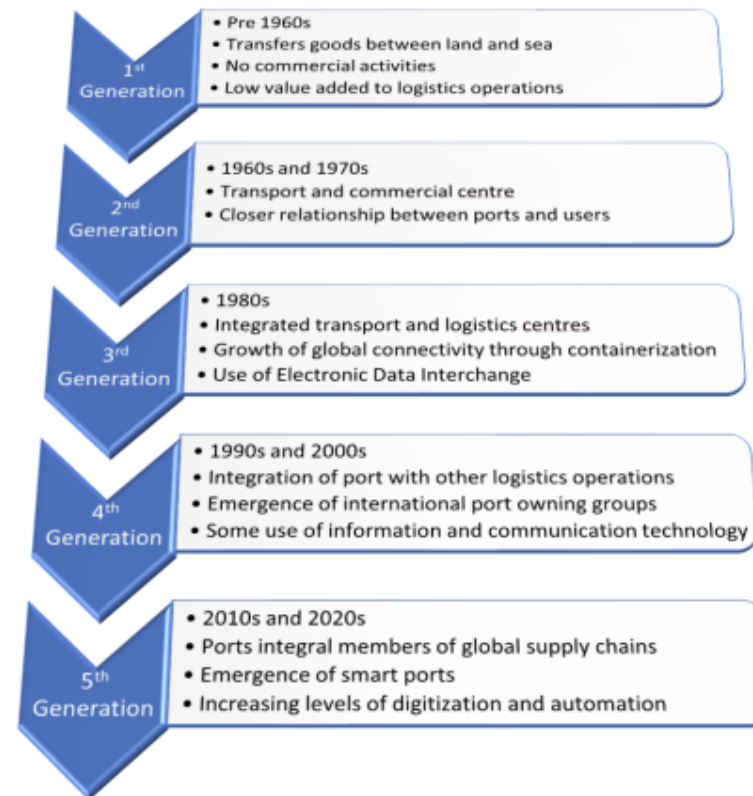


Figure 1: The evolution of Smart Ports
(adapted from [Molavi, Lim and Race, 2020](#))

This report results from a collaboration between two projects under the DCMS 5G Testbed and Trials programme, 5G Logistics and 5G Ports (more details on these projects can be found on pages 8 and 9). Building on experience within each project, the collaboration work has engaged with the sector more widely to examine what the opportunities are for 5G in the UK ports sector, as well as the barriers and enablers for wider adoption.

The aim of this report is to identify requirements for ports and their stakeholders to enable the wider deployment of 5G within the UK port sector. While recognizing that ports will compete to attract traffic, when deploying a new technology such as 5G there is also much to learn from each other's experiences. By identifying how ports can build the case for 5G deployment, the intention is to support this wider roll out, bringing benefits for the UK economy through more efficient and effective trade.

To inform our work, we have been speaking to UK port sector representatives, from small harbours to global gateway ports. These ports are at different points in the journey to 5G, from having initial thoughts through to investing in 5G technologies. Data collection has taken place during late 2021 and early 2022, and the report's content reflects our analysis of these discussions, rather than an industry-wide perspective on 5G deployment.

Why is 5G important for ports?

It is likely that 5G will see major deployment in the next 5 years within the logistics industry, particularly in support of wider moves towards digitalization and automation in the sector. This will enable companies to meet continually increasing demand for greater transparency and reliability in speed in the movement of their freight. Underpinning all of this is the need for communication networks to handle and process increasing amounts of data.

5G will provide the capability to do this, exceeding the capabilities of existing 4G and Wifi networks where wireless communication is required. The benefits can be considered in relation to:

- Volume – 5G networks will enable a greater amount of data to be handled when compared to existing wireless technologies. This will provide, for example, the capability for an increased number of sensors to be deployed around the port estate to allow the tracking of mobile assets and cargo.
- Velocity – Using 5G will provide a greater bandwidth for handling data, allowing it to be transmitted at a higher speed. In doing so, activities such as automation and remote working within ports becomes more feasible, especially for mobile assets which cannot have a fixed connection.
- Veracity – 5G can provide more reliable connections for data transfer, giving assurance that the flow of data will not be disrupted. This can support mission critical control activities and better quality video transmissions for the purposes of security or remote maintenance.

- Variety – 5G networks have the ability for network virtualization to allow different systems to use the same communication infrastructure. This reduces the need for multiple communication networks to be installed, while ensuring security is maintained between different users.

Ports around the world are now developing and testing 5G use cases that cover all stages in the movement of freight as well as in other functions supporting port operations. Figure 2 summarises these 5G use cases, as well as providing examples of ports which have trialled or deployed them. Use cases are very important as they create the value proposition from 5G.

The use cases demonstrate the capability of 5G to enhance various processes, including

- increased monitoring of freight, assets and environmental measures
- automation of processes to speed up flow and reduce the risk of accidents to port workers
- use of video, including coverage from tugboats and the use of drone based camera to enhance safety and security.

Beyond these use cases, there are other examples of port digitalization which would benefit from 5G adoption. This includes energy management within the port, autonomous vessels and using artificial intelligence for resource allocation.



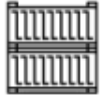

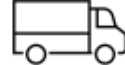

	Port Waters	Unloading	Storage	Transfer	Port Gate and external sites	Other Applications
						
Current 5G Use cases	<ul style="list-style-type: none"> • Tracking on barges and tugs • Streaming video from tugboats • Augmented reality to aid berthing 	<ul style="list-style-type: none"> • Monitoring and managing equipment • Remote control of cranes • Detecting container damage 	<ul style="list-style-type: none"> • Sensors to monitor cargo • Tracking containers and cargo • Added value cargo services 	<ul style="list-style-type: none"> • Sensors to monitor cargo • Navigation of automated guided vehicles • Traffic control • Work allocation 	<ul style="list-style-type: none"> • Sensors to monitor cargo • Tracking containers and cargo 	<ul style="list-style-type: none"> • Remote site support using virtual and augmented reality • Monitoring environmental impacts • Security monitoring using drones • Health and Safety
Locations using 5G	<ul style="list-style-type: none"> • Antwerp • Livorno • Zeebrugge 	<ul style="list-style-type: none"> • Felixstowe • Koper • Qingdao 	<ul style="list-style-type: none"> • Bristol • Livorno • Southampton 	<ul style="list-style-type: none"> • Felixstowe • Hamburg • Livorno • Piraeus 	<ul style="list-style-type: none"> • Bristol • Southampton 	<ul style="list-style-type: none"> • Belfast • Bristol • Riga • Hamburg • Piraeus • Rotterdam • Zeebrugge

Figure 2: Existing 5G use cases within ports

5G Logistics

The [5G Logistics](#) project is trialling the power of private 5G networks for supply chain efficiency, visibility and traffic management.

Led by the West of England Combined Authority, the 12-partner-strong consortium includes: the region's major port, The Bristol Port Company; academic facilities at the University of Bristol Smart Internet Lab and Cardiff Business School; Gravity, the new 616-acre commercial smart campus; automated drones solution provider, Unmanned Life; Bristol City Council and 5G private network businesses, Cellnex, ADVA, AttoCore and Airspan.

Set to complete in June 2022, the project trials three use cases:

1. **Geo-fenced asset tracking and condition monitoring:** Using 5G internet of things (IoT), goods containers and pallets are being tracked within the 5G testbeds – and between them, using a public network. This level of visibility is expected to become critical in a modern freeport scenario, where products can move customs-free between a central port zone and remote 'freezones' up to 45km away. The goods containers are also kitted out with sensors measuring temperature, light, humidity and more – and transmitting this data in real-time to a user dashboard.
2. **Automated drone surveillance and emergency response:** The project is using the reliability and bandwidth offered by 5G to test automated drone perimeter inspections and incident response at the port. Security for goods and workers is paramount in a port

environment, which can span large areas and has an ever-changing landscape.

3. **Smart junctions:** The smart junction use case is exploring how 5G features such as deterministic low latency to mobile edge compute (MEC) and enhanced location services might shape future intelligent traffic system (ITS) architectures. Trials involve moving non-safety critical traffic optimisation features (normally running on-street), into the MEC. The trials also explore how vehicle location data could be used to improve algorithms to optimise junction efficiency for HGVs – common around ports.



Image credit: The Bristol Port Company

5G Ports

This [project](#) at the Port of Felixstowe will use 5G Internet of Things (IoT) devices and predictive data analytics to reduce unscheduled downtime of cranes, to boost the productivity and efficiency of the operation of the port's ship-to-shore quay cranes. It will also show how the use of 5G technology, replacing fibre optical cable, will improve the performance of remote control yard cranes enabling the port to increase both efficiency and safety and develop new skills amongst its workforce. The project involves the University of Cambridge, Three UK and Bluemesh Solutions Ltd.

AI enabled predictive maintenance: Quay cranes are one of the most critical assets in a port, and their availability and efficiency of these cranes is often the determining factor in port productivity. However, cranes are prone to disruptions due to the extensive stresses and cyclic loading they experience during operations. Unexpected disruptions can lead to stoppages in loading/unloading operations, affecting turnaround times for vessels. This project is monitoring the condition of the critical components of the cranes using low-cost IoT sensors communicating via 5G technology. Artificial intelligence is employed to identify pre-disruption trigger events to guide the predictive maintenance strategy.

The project will demonstrate the effectiveness of AI using 5G IoT to improve the efficiency of quay cranes by reducing their downtime attributable to component failures and thereby increasing their availability and moves per hour.

Remote control of yard cranes: Remote control of assets is important to the Port for health and safety by removing operators from the quay and also to attract a wider pool of employees, including those with some disabilities, who are otherwise unable to work in certain roles on the Port.

5G provides critical latency and throughput capabilities needed to enable the crane critical operating systems to operate and to transfer the multiple CCTV feeds that the operator requires. This use case is testing high upload rather than download volumes and operating at less than 16ms latency.



Image credit: Port of Felixstowe

Approach Taken

The focus of this work has been to understand what needs to happen to accelerate the use of 5G within the UK ports sector. In doing so, two main questions were posed:

1. What are the key operational challenges the UK port sector faces that 5G could help with? And how?
2. What are the enablers and barriers to investment in 5G?

The first of these questions recognises that, for 5G to be more widely adopted, it needs to help ports improve their current operations. It may be that use cases have yet to be fully developed, and so the question allows a breadth of opportunities to be identified.

The second question more closely examines how organisations may transition from being interested in 5G deployment to committing to investment.

To get industry opinions, a workshop was held with six representatives from organisations with active involvement in the UK port sector. This was complemented by six further interviews where participants were unable to attend the workshop.

In the workshop, a short presentation was given summarising the current use of 5G in the port sector globally and highlighting some of the potential opportunities offered. Information about the two collaborating DCMS-funded projects was also covered. An open discussion session was then held focusing on the two questions above.

For interviews, a similar approach was taken although the presentation element was adjusted to reflect the current experiences of the interviewee with 5G deployment in their organisation.

These covered a wide range of port operations including small, local government owned harbours, Trust Ports and large, multi-port owning groups. Geographically, participants had operations throughout the UK, with the port-owning groups having overseas operations too. Most participants were responsible for IT within the port although those from smaller ports had a wider range of responsibilities. In addition to port operators, participants included representatives from trade bodies as well as 5G technology and logistics providers.

In terms of experience with 5G, some participants were well along the path towards investing, either undertaking trials or going out to tender. However, many were still exploring potential opportunities and some were more cautious, knowing a little about 5G without fully considering whether it offered opportunities for their organisation.

The qualitative data from the workshop and interviews has been analysed by the team at Cardiff University, complemented by academic literature and trade press articles as appropriate.

Operational Challenges

In discussing the operational challenges for 5G adoption, much of the focus was on the potential **use cases** that could improve existing port operations. However, some challenges were also raised related to **management** and **technology** issues. These need to be considered before building a business case and considering the enablers and barriers. Each of these is now discussed in more detail.

Use cases

Through the discussions, a range of different use cases were identified which would take advantage of the capabilities of 5G (see Figure 3). While all of the use cases can be standalone examples, they can also support other use cases. The most frequently mentioned examples related to health and safety, automation and tracking of resources and cargo. There are often links between these use cases.

- **Health and safety (H&S):** The focus here is on keeping workers out of dangerous areas within the port, either by tracking their location or using automation. For dangerous, repetitive tasks, 5G and AI enabled robotics can help companies to prevent incidents while saving time and cost, as robots are capable of working in hazardous environments and alleviating strenuous tasks. While H&S was the most frequently mentioned opportunity, it was also recognised that tackling this issue alone may not justify investment in 5G.
- **Automation:** Enabling activities to be controlled remotely offers good potential, both for fixed and mobile assets. However, these use cases are likely to emerge in the medium term, given the



Figure 3: Potential 5G Use Cases in Ports

significant investment requirement and dependency on the existing technology maturity of a port.

-
- **Tracking:** To quote one participant, this would involve tracking “anything that moves”, including workers, vehicles and cargo. Given that tracking capabilities already exist, use cases will need to exploit the enhanced value of 5G in terms of intensive real time and low latency connectivity at scale.
 - **Drones:** These offer a range of different opportunities, including goods/items delivery, video monitoring from hard-to-reach locations (e.g. aerial views), servicing hard-to-access locations or enhancing security monitoring across the port estate.
 - **Asset monitoring:** 5G provides the opportunity for monitoring the condition of port assets, such as cranes, to allow predictive maintenance and avoid unplanned unavailability of equipment – which can come at a high cost.
 - **Data sharing:** Using and sharing data in (near) real time manner is increasingly important for port operators, providing the much needed end to end supply chain visibility to relevant stakeholders including shippers, logistics service providers, and government agencies such as customs clearance. 5G, as a critical supporting infrastructure, plays a significant role in this.
 - **Value adding applications:** These use cases relate to opportunities for providing value adding services to the freight and/or passengers making use of the port. Currently, very few customer focused use cases have been adopted and more discussion on these came from the smaller ports. These ports may be tourist destinations or host cruise ships, and therefore opportunities exist for 5G use cases that can improve the visitor experience.

Elsewhere, use cases related to environmental monitoring within ports have been developed. However, discussions with participants indicated that current thinking related to use cases in other areas, while recognising there may be environmental benefits as a consequence.

Management

There was a general belief among ports regarding the importance of digital transformation, particularly in providing competitiveness while coping with uncertainties and disruptions such as Covid-19 and geopolitical turmoil. However, efforts and investments on digital technologies tend to be conservative. In particular, ports can be risk averse when it comes to experiments with and the trial use of emerging technologies, preferring to see investment elsewhere before investing in deployment.

For smaller ports, there are added challenges in having the resources and in-house expertise available for undertaking innovation, as management teams may be small with individuals having multiple roles within the port. Consequently, leading in innovation has a lower priority than other, and port management tends to focus more on operational activities.

This tendency to be risk averse then filters through into justifying the need for investing in 5G. For many use cases, investments in 4G and Wifi are generally seen as sufficient for current business needs and there are often substantial switching costs when transiting from legacy systems to new digital solutions. Interoperability as well as the redesign of IT infrastructure and restructuring of internal processes

and practices can be expensive, leading to less desirable efficiency gains. Therefore, the case for 5G investment is reduced unless there are wider strategic objectives to be seen as leaders in this technology. However, where 5G investments are more easily justified is in the development of new infrastructure within the port estate, where legacy systems are not present.

Technology

Participants identified that 5G may offer the opportunity to overcome some of the challenges they face with their current use of Wifi and 4G. In the case of the former, issues identified include the available bandwidth for handling increasing amounts of data, reliability of connections and security concerns. Another issue with Wifi was the presence of Faraday cages creating deadspots, as a result of the equipment and containers passing through ports.

For 4G, the main concern was network coverage. Ports are often in more peripheral areas and, while many of these now have reasonable coverage, there remain parts of the UK where 4G signals can be patchy, and for port operators in these more remote areas, this can lead to blackspots.

Despite these concerns, for many operators existing Wifi and 4G networks are sufficient for current operations, and may have redundancy to accommodate further growth. As noted earlier, this creates a challenge for justifying further investigations into 5G deployment.

There are also concerns about 5G coverage. Where ports deploy their own private network, there may be a large area of land to be covered with 5G and this leads to the need for significant investment. For some ports, a public or hybrid (public/private) network may be an alternative, but these then depend upon the coverage available. Solutions to overcome security concerns around public networks are now becoming available. 5G networks are currently more focused on urban areas, whereas ports are often away from these.

Enablers and Barriers

In considering the enablers and barriers to 5G adoption by UK ports, five general themes emerged: Investment decision making, use case benefits, implementation activities, workforce and government support. Within each of these, a range of enablers and barriers existed, as summarised in Figure 4. It should be noted that some barriers are becoming enablers as ports digitalise their operations, and these are shown with dotted arrows.

Investment decision making

These issues extend some of the earlier points made about management issues when discussing opportunities and challenges. The **digital strategy** of a port operator is significant, and is moving from being a barrier to being an enabler.

The ports and logistics sector in the UK is quite traditional in its outlook and, until relatively recently, had not significantly embraced the opportunities offered by digitalization. Where digitalization has now occurred, 4G and Wifi networks are normally sufficient to support this.

However, changes are coming as a result of various pressures and there is a greater recognition that ports need to embrace digitalization to improve operational efficiency and productivity, increase safety, reduce emissions, and improve sustainability. Ultimately, ports will need to adapt in much the same way as they have done over time in response to external pressures.

The **business case** for investing in 5G can also be a barrier to investment. Any decision needs the investment cost to be compared with quantifiable benefits and, currently, there are challenges with both of these. With the port sector often not leading on innovation, these uncertainties can then represent a barrier.

An initial barrier is the **availability of funding** for the 5G investment. Ports have finite resources, and it may be that other areas of the business are deemed more important for investment, particularly if they directly benefit the movement of cargo. Related to this, some participants directly identified the cost of 5G provision as a barrier.

Existing investments in 4G and Wifi can also represent a barrier, with participants already having these networks in place. Therefore, moving the whole port environment to 5G is difficult to justify, leading to a more incremental approach. However, the incremental approach can also then reduce some of the benefits that can be achieved.

What is seen as a way forward is to adopt a hybrid approach, whereby radio masts can support both 4G and 5G, with a switch towards the latter over time as required.

Another enabler for port operators is for 5G investments to **align with wider asset renewal cycles**. Much port infrastructure predates the internet era and therefore telecommunications equipment needs to be retrofitted. By contrast, new build facilities can include the physical infrastructure for 5G connectivity and may need wireless communication methods to be installed. In these situations, the justification for 5G can be stronger.

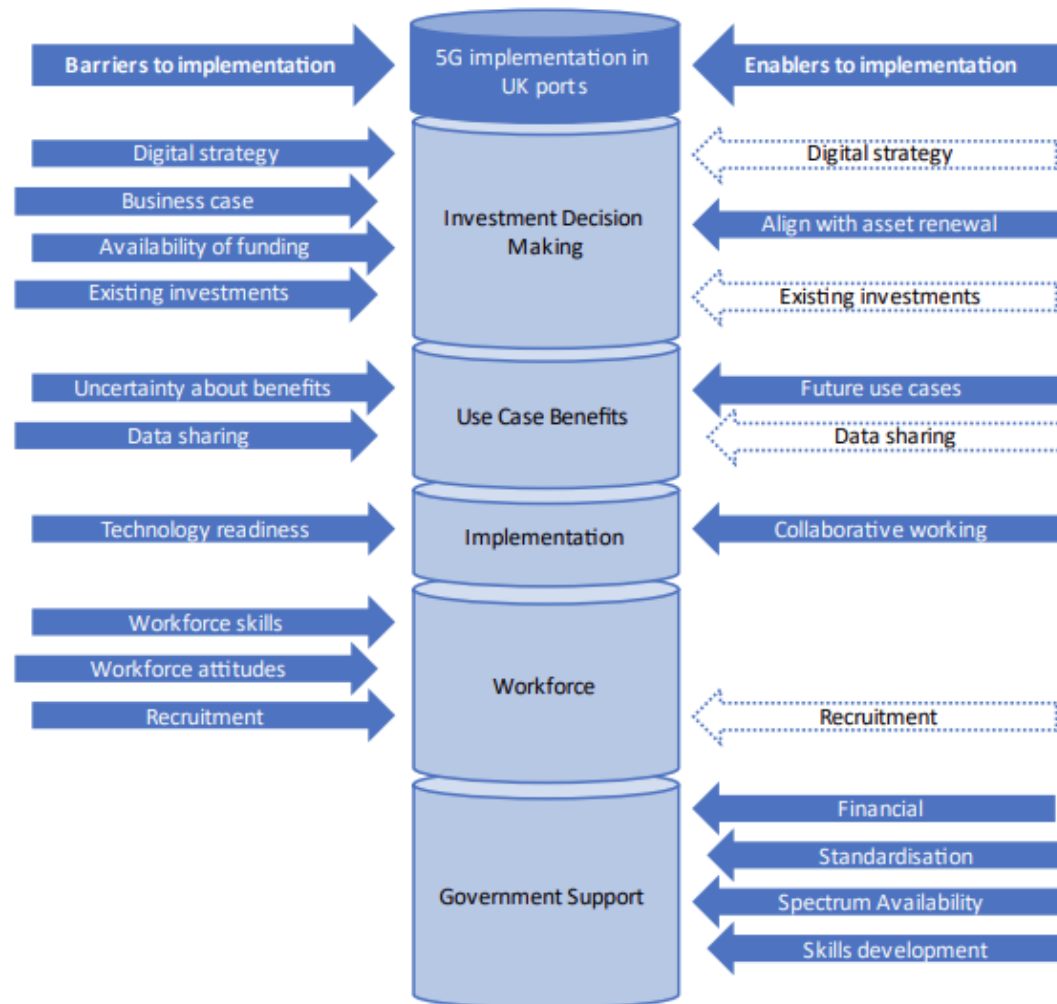


Figure 4: Barriers and enablers to 5G adoption in UK ports

Use case benefits

The other side of any 5G investment decision are the benefits that come from use case introduction. Although many believe ports would benefit from 5G deployment in general, there remains **uncertainty on the benefits** because of the early stage of deployment. Many of the use cases currently being developed are similar to existing systems and therefore the question is what 5G can do differently. It is likely that the biggest monetizable benefits will occur in use cases that improve processes within the ports, and will provide a foundation for H&S and environmental use cases. Multiple use cases are likely to be needed for 5G to be a viable commercial proposition for an individual port. The findings from the 5G Trials and Testbeds programme will be important in reducing the uncertainty for ports.

Seeing the opportunities and benefits that may emerge from **future use cases** is likely to be an enabler in the UK port sector. As one participant observed, investing in 5G is about “building for the future rather than today”. Current trials will need to scale up and as use cases get implemented, new opportunities will emerge. The potential for greater coordination in port processes represents a significant opportunity that could be revolutionary if realized.

However, greater coordination is likely to require increased **data sharing** and collaboration. Current mindsets may limit the extent to which this can happen. There remains resistance in the port and logistics sector with data sharing – a common barrier found in other industries too. Thinking is shifting towards a more collaborative culture in the ports’ ecosystem, for instance as evidenced by the developments of port community systems around the world.

Implementation

Turning to the implementation of 5G networks, a common observation was that current **technology readiness** was a barrier to wider adoption. Off the shelf solutions are not widely available and, given the complexities of 5G deployment, operators lack confidence that a network can be set up to deliver what is expected. There are also issues with the availability of devices able to connect to 5G networks. Over time, this barrier should reduce as availability improves.

Conversely, **collaborative working** and knowledge sharing between a wide range of stakeholders was seen as an enabler for 5G deployment. This includes network providers, use case developers, government (both national and local) and, particularly for smaller ports, the wider community. In doing so, a better understanding of 5G capabilities and opportunities can be developed, increasing the likelihood of successful deployment. Equally, sharing experiences within the port sector more widely further enhances this.

Workforce

There was much discussion with participants around various workforce issues relating to the deployment of 5G, with three particular barriers emerging: workforce skills, workforce attitudes, and recruitment.

Digitalization within ports has changed the **workforce skills** requirements throughout the port, from offices to the quayside. A substantial proportion of that workforce would not be considered early adopters of new technology, and therefore barriers exist in introducing digital working practices. From the discussions, some ports

have been more successful in this transition than others, providing opportunities for shared learning.

However, deployment requires not just new skills but also changes in **workforce attitudes** towards technology. Existing working practices can be embedded and organisational inertia can be a barrier to digital innovations. Terminology used by technology providers may be poorly understood. There may also be nervousness amongst the workforce that digitalization may lead to job losses. Participants also noted that ports can be highly unionised, and therefore trade unions can play an important role in supporting deployment.

Several issues relating to **recruitment** were also identified. As with other areas of logistics, ports have an aging workforce and one with a high turnover of people. However, attracting new and younger workers to the industry can be challenging as it is perceived as a traditional and manual sector. It may be that opportunities created by 5G, such as automation and virtual reality, may change this perception.

Recruitment to support digitalization is creating new challenges, with roles such as developers now being sought by ports. This is a new employment market for ports, and one where they are competing against employers who may be seen as more attractive due to the nature of work or geographical location. Ports are having to adapt to these new labour markets and changes accelerated by the pandemic, such as hybrid working, can facilitate this.

Government support

Finally, government support was seen as an important enabler in delivering 5G more widely in the UK port sector. The most commonly discussed issue was **financial support** through grants and project funding to reduce the financial risks associated with innovation. Government support enables use cases to be implemented in a test environment, enabling them to reach a technology maturity level from where commercial adoption can take place. It was recognised that financial support can only go so far and there will be a need for the UK port sector to take on more of the financial risk over time, once an appropriate maturity level is reached.

Beyond this, several other areas were identified where government support would benefit the deployment of 5G:

- **Standardisation:** this will be required to enable use cases to work with each other and with existing systems. While government can play a supporting role here, there are also opportunities for port industry bodies to facilitate this.
- **Spectrum availability:** ensuring that ports are able to get licences for private 5G networks in a timely manner.
- **Skills development:** as noted above, workforce issues are a challenge for and government support to people into the ports industry would be welcomed.

One challenge identified with this is where responsibility lies within government departments as the issues cut across a range of responsibilities, and with national, devolved and local administrations.

Conclusions and Recommendations

Digitalisation has influenced the port sector significantly during the past decade. It is clear that the adoption of 5G within the port sector represents the next step in wider digitalization of the industry. The opportunities that it can unlock represent a step change over existing technologies. Therefore, it is essential that the UK port sector expands its use of this technology.

There is a clear appetite for 5G adoption by ports both large and small, with a wide variety of potential use cases being identified. This is despite the industry often being seen as risk averse when it comes to innovation and not wishing to be the first adopters. 5G will bring the capability to handle large volumes of data, connect large numbers of devices and bring a high degree of latency, all critical in enabling port based use cases.

As more ports look to adopt 5G, so a variety of barriers have emerged and these will need to be overcome into the future. However, there is already evidence that some barriers are becoming enablers as the UK port sector increasingly focuses on digitalisation. This will help to accelerate the pace of the transition to 5G.

Based on the findings outlined earlier, the following recommendations are suggested:

- Ports need to identify a portfolio of different use cases with clearly articulated value which link to their overall business strategy. For larger ports, these are likely to be within the port estate and can rely solely on private 5G networks. However, for

smaller ports, there may be opportunities from using or providing a public 5G service as well, particularly in more remote areas.

- There needs to be flexibility in the deployment of 5G networks with ports, so that they can adapt and expand over time. It is clear that a 'big bang' approach is challenging to adopt for ports and therefore using technology that has both 4G and 5G capabilities offers a progressive evolution. This applies to both the radio network and the hardware, the latter in particular being a constraint on adoption. This also enables ports to explore different use case possibilities and acquire a deeper understanding of how 5G should be best deployed to maximise its value. This then informs later, large-scale deployments.
- In considering the roll out of public 5G networks, there would be benefits from a faster deployment to more rural areas where ports (and other industries including tourism) may be able to exploit the capabilities offered more quickly, avoiding the lack of 4G coverage and providing access to directly using 5G. This would require a shift from providing coverage based on population centres.
- Adoption of 5G requires a collaborative approach that focuses on processes, technology and people. There is evidence that the first two are already happening successfully in the UK port sector, but people issues remain. In changing workforce attitudes and for the effective upskilling of digital literacy, there is a need to engage with trade unions effectively.
- More generally, the port sector needs to work together in sharing experiences, best practices and learning from 5G deployment, as this will reduce many of the current uncertainties and therefore make the business benefits clearer. This will also help to develop a larger market for use cases and hardware, creating wider benefits

within the market. Port industry trade associations can help to facilitate this.

- Working together across the sector will also be effective in addressing the issues raised around skills and the attractiveness of the industry to new recruits, particularly in new areas of expertise such as IT solution developers. Ports are competing with other industries for this talent and presenting a wider view of the opportunities across the sector will help career pathways to emerge, even if these are across different ports.
- Continued government support is required across the above recommendations. Financial support through initiatives such as the 5G Testbeds and Trials Programme help to offset the risks and can encourage collaborative working. Funding for skills development, such as through Apprenticeships, can help bring in new talent. Beyond financial support, government can also facilitate adoption through planning regulations as well as spectrum standardisation and access. A challenge, however, is bringing together multiple government departments and a UK port strategy could be a means to achieve this, combining digitalization with existing port policy developments such as freeports.



Image credit: The Bristol Port Company