Guidance

G0213 A3 Asset Remote Condition Monitoring, Alarm and Alert Management

Contents

1 Purpose

The purpose of this document is to assist in the provision of a consistent and integrated Asset Remote Condition Monitoring (ARCM) approach within Transport for London (TfL).

2 Scope

2.1 This guidance applies to those who specify, design, install, maintain and operate TfL ARCM systems.

2.2 This guidance document amplifies some specific requirements mandated by the LU standard **S1213** 'Asset Remote Condition Monitoring'.

Note: Sections of S1213 are quoted in appropriate sections within this document. Clauses and notes from the standard are shown as text in italics within a box as shown in the, for example below:

> *3.14 All* Remote Condition Monitoring (*RCM) equipment shall be registered as an asset on the company asset register.*

3 Introduction

3.1 The company's asset management strategy defines the company's aspiration to transition towards more predictive, condition and risk based maintenance regimes with the aim of maximising the efficient delivery of our customer services.

3.2 LU standard S1213 'Asset Remote Condition Monitoring' defines TfL's requirements in relation to these assets and this document provides accompanying guidance aimed at optimising the benefits resulting from the introduction or expansion of these systems.

3.3 A core principle of this guidance and S1213 is that Condition Monitoring (CM) assets should not be treated differently to other assets; projects should apply the current TfL best practice project delivery process (Pathway) and follow all governance steps for delivery of ARCM projects including: asset documentation; maturity and capability assessments; training; handover and entry into the relevant maintenance management system, as a maintainable asset

3.4 To ensure that the development and introduction of ARCM systems comply with the company's requirements it is essential that ARCM projects and initiatives adhere to the TfL Pathway process mandated for all project and programme work.

4 Guidance

4.1 The Pathway Project Management Plan (PPMP)

As mandated in the Pathway manual, ARCM projects are required to comply with the TfL Pathway process.

To assist those involved in the design, development, delivery and operation of ARCM systems a generic ARCM Pathway Project Management Plan (PPMP) has been developed.

This PPMP is located at

http://onelink.tfl.gov.uk/sites/tflpathway/a11/b6/pid20/SitePages/Default.aspx.

Contacts for additional Pathway guidance have been included within the above.

The following guidance provides additional support for those required to comply with the requirements S1213 'Asset Remote Condition Monitoring'.

3.11 A defined Process for the analysis of the data captured and the establishment of the condition of the Asset shall be used. The requirements of the Process are to:
- *a) Specify the data requirements of RCM systems*
- *b) Comply with standard S1217 'Integration of Human Factors into Systems Development'*
- *c) Comply with Standard S1218 'Human Systems Interaction - Dialogues and Notifications'.*

5.3 The RCM system shall be designed and optimised using the methodology in section 4 of BS ISO 13379 to:
- *a) Decide the problem*
- *b) Define the user needs*
- *c) Decide if RCM is the right solution*
- *d) Identify and measure only the correct parameters*
- *e) Define the timeliness of access to data for both 'immediate' and 'historic' analysis*
- *f) Design and optimise the RCM system*
- *g) Optimise customer transport service.*

10.1 The design requirements shall include the provision of appropriate Operations, Maintenance, and Technical manuals accepted by the Operators and Maintainers. These shall include RCM system fault and response actions

10.2 Training and competence for the operation, management and maintenance of the RCM system shall form part of the requirements capture

4.2 Developing the Alarm and Alert Philosophy

3.3 The design and presentation of alarms and alerts to users shall comply with the Human systems Interaction – Dialogues and Notifications standard S1218 'Human Systems Interaction - Dialogues and Notifications'.

The Alarm and Alert Philosophy document establishes the principles and processes to design implement and maintain Alarm and Alert *systems*. It is deemed as the cornerstone of an effective Alarm and Alert *system* management programme.

The philosophy should define the performance goals for the Alarm and Alert *system* and describe the key work practices, roles and responsibilities. This document provides guidance for a consistent approach to Alarm and Alert *system* management and so should promote:

a) Clearly defined roles and responsibilities for Alarm and Alert *system* management within the company or business area covered by the philosophy

b) Consistency of Alarm and Alert design and presentation

c) Alignment with corporate risk management goals and objectives

d) Alignment with good engineering practice

e) Efficient Alarm and Alert rationalisation and design activities.

The following criteria will need to be considered in developing and implementing the principles in the Alarm and Alert Philosophy:

a) The design of the Alarm and Alert *system* must not adversely affect the safety or performance of the system it is monitoring

b) The requirement for Alarm and Alert Notifications needs to be questioned in order to verify that there is a requirement for, or benefit from, reporting the condition

c) Operators will respond to all Alarm and Alert Notifications, taking into account the priority of the Notification. In some circumstances taking no direct action may be a valid operator response

d) The Alarm and Alert *system* should be designed so the operator is capable of effectively responding to all alarms and alerts in all anticipated scenarios. Operators will be trained on the relevant parts of the Alarm and Alert *system* to ensure that they have the capability to monitor it

e) The Alarm and Alert *system* will be subject to periodic review and revision as part of an audit process

f) The philosophy will be reviewed regularly to reflect best corporate and industry practice, as well as all appropriate national and international standards and guidance.

4.2.1 Recognising the importance of an Alarm and Alert Philosophy

An Alarm and Alert Philosophy should be produced to inform the business of how Notifications and Supplemental Messages are to be managed within the environment that the system is required to operate, for example within a control room where multiple separate Alarm and Alert systems may be deployed.

Justifying the installation, operation, maintenance and management cost of an Alarm and Alert system can be a challenging task. From a business case standpoint Alarm and Alert system management should not be looked at as a technology, but as a business enabler and risk management investment.

The importance of the Alarm and Alert system needs to be recognised at senior management level and an Alarm and Alert Philosophy document produced as referenced in Table 1.

When the Alarm and Alert Philosophy has been developed; sufficient resources and finances need to be in place to manage its requirement.

The senior management buy-in to the importance of the Alarm and Alert Philosophy should ensure that both human and financial resources are focused to maintain and improve Alarm and Alert system performance throughout its lifecycle.

4.2.2 ARCM philosophy contents

Alarms and alerts, and event data are pieces of information, which are provided to people, in order to allow them to make decisions, and, if necessary take or initiate actions. The defining characteristic of an Alarm and Alert is that it provides information which needs to be acted upon within a time limit, in order to deal with an undesirable situation, or to prevent an undesirable situation occurring.

In order to decide which pieces of information need to be given the status of alarms or alerts. It is vitally important to understand the purpose of the Alarm and Alert system, the users and decisions they can make, or actions they can initiate, within the overall controlling interactive system – composed of people, processes, hardware and software.

If this information and decision mapping is not properly undertaken, there is a high probability that information of all kinds, Alarm and Alert s and alerts in particular, will be presented to a person who is not remitted to make a relevant decision or take a relevant action. Unnecessary or irrelevant information can cause excessive demands of those individuals remitted to make key decisions or undertake take key actions. As a consequence such unnecessary information should be avoided to minimise the likelihood of human error.

Table 1, below identifies the mandatory and recommended requirements for inclusion in the content an Alarm and Alert Philosophy document.

Table 1 – Alarm and Alert **Philosophy Contents**

Alarm and Alert **Philosophy Contents**	**Mandatory Requirement**	**Recommended Requirement**
Define the purpose of the Alarm and Alert **systems** Define the purpose and objectives of the Alarm and Alert systems in order to direct participants during design and improvement activities.	Yes	
References A list of appropriate references in the form of national guidance documents, company standards and any other subject related documentation.		Yes
Roles and responsibilities The responsibilities for the activities of the *Alarm and Alert system* lifecycle are established in the Alarm and Alert Philosophy. Specific aspects to cover include the following: a. Ownership of the *Alarm and Alert systems*, the philosophy and related documents. b. The role responsible for the management and regular maintenance of the A*larm and Alert systems*. c. The role responsible for the technical support to	Yes	

resolve problems with the A*larm and Alert systems.* d. The role responsible to ensure that the requirements outlined in the Alarm and Alert Philosophy are followed.		
High level A*larm and Alert system* design principles The criteria for selection and principles for design of Notifications should be consistent with the definitions of an Alarm and Alert.	Yes	
Guidance on rationalisation criteria To maximise the functionality of an A*larm and Alert system* it is critical that the operator only receives Alarm and Alert Notifications that are meaningful and actionable. Supplementary messages should only be presented where there is a benefit to the operator of knowing that information.	Yes	
Guidance on prioritisation criteria Consistent priorities aid the operator in deciding the order of response during a period of high frequency Notification events	Yes	
HFI design guidance The HMI design for alarms and alerts should be consistent with the Alarm and Alert Philosophy and the overall HMI design philosophy. The capabilities of the control system should be considered in the HMI design.	Yes	
Define company or business unit requirements for A*larm and Alert system* performance monitoring Metrics used to monitor A*larm and Alert system* performance against the target performance levels.	Yes	
Define company or business unit requirements for A*larm and Alert system* maintenance To include but not limited to the following elements: a. Alarm and Alert system record keeping. b. Requirements around out of service assets c. The policy for use of interim monitoring When, for example, an Alarm and Alert is taken out of service for extended periods (e.g., days, weeks, or months). Such cases should be examined to determine if an interim Alarm and Alert or procedure is necessary.	Yes	
Define the company or business unit requirements for testing of A*larm and Alert systems.* To ensure adequate testing of the A*larm and Alert system* throughout its lifecycle.	Yes	

Define the *Alarm and Alert system* documentation requirements. A master Alarm and Alert and Supplemental Message database or rationalisation of information should be retained, along with periodic *Alarm and Alert system* performance reports.		Yes
Guidance on the implementation of *Alarm and Alert systems* A basic approach for *Alarm and Alert system* commissioning and handover to ensure consistency for all Alarm and Alert systems.	Yes	
Define the process for change management of *Alarm and Alert systems* a. Temporary changes to functionality (e.g. assets out of service). b. Temporary changes to Notification or Supplemental Message attributes. c. Permanent changes to Notification and Supplemental Message database or attributes.	Yes	
Define policy on *Alarm and Alert system* history preservation *Alarm and Alert systems* can generate and log large amounts of information during operation. It is necessary to define what aspects and duration of the *Alarm and Alert system* history should be preserved.	Yes	
Any special *Alarm and Alert system* design considerations To specify the rules and methods for the design of *Alarm and Alert systems* covering special circumstances, such as, the process to transfer the responsibilities for Alarm and Alert response to another operator.		Yes
***Alarm and Alert system* training and operating procedures** To include, but not limited to, the following elements: a. The job role or personnel requiring training. b. An outline of training requirements. c. When training is required.		Yes

4.2.3 Developing the Alarm and Alert management strategy

(11.1)	*Alarm and Alerts shall be managed using the Alarm and Alert Management Strategy.*

An Alarm and Alert management strategy is required to ensure each Alarm and Alert system provides the functions required of it. Hence one of the primary tasks before commencing an Alarm and Alert Strategy is to clearly identify the purpose of the

Alarm and Alert system. An Alarm and Alert Strategy can cover a single system, multiple systems or operating environments where multiple separate Alarm and Alert systems are deployed, for example in a control room.

The Alarm and Alert Strategy should define who will have ongoing ownership of this strategy and be responsible for any changes to it.

Careful consideration should be given to the functionality where an alarm or alert Notification or Supplemental Message is presented to multiple users, at the same time, or to different uses at certain times of the day where for example the control is transferred to another control room during certain times of the day. The ownership and control of the Alarm and Alert system should be clearly identified in the Alarm and Alert Philosophy.

4.2.4 Alarm and Alert management strategy principles

The following generic principles are applicable to the development of a strategy for any Alarm and Alert system:

A. Identify notifiable conditions

- For any asset or system being monitored a list should be compiled of the possible conditions the asset or system can report.
- This list should be analysed to see if there is a requirement for, or benefit from, reporting the condition. This process should consider the benefit to the operator and to the maintainer of the asset or system. If there is no benefit to knowing the condition, then it should not be reported. The asset or system may still keep its own log of the event.
- It is possible for an Alarm and Alert *system* to use a logic function to generate Notifications from individual events that do not in themselves constitute a condition that would be reported to a user. For example, multiple occurrences of the same event in a set time period or a particular sequence of events.

B. Identify recipient

- Identify the recipient for each notifiable condition for example, Local Operator, Service Control Centre, Faults Reporting Centre, Maintenance Control Centre, Maintainer etc.
- It is quite possible and indeed likely that a condition may need to be reported to more than one recipient. However, it is important to note that not all recipients will necessarily view the condition with the same priority, level of detail or have the same action responsibility.

C. Categorise and prioritise

- For each recipient the condition should be categorised as either sub-categorisation of Notification; an alarm or alert, or categorised as a Supplemental Message. LU standard S1218 'Human systems interaction – dialogues and Notifications' describes the Notification classifications in more detail. Supplemental Messages do not breach Alarm and Alert / alert thresholds but may include event or environmental data which assists the

user to interpret system data or assist in decision making e.g. multiple occurrences of the same event in a set time period or a particular sequence of events.

- Alarms and alerts should be prioritised. The priority will depend on consideration of severity of the condition, the impact of the condition, and time elements associated with the presentation of the Alarm and Alert Notification, the last time to take action, and the estimated time of impact. Alarms are always a higher priority than reliability related alarms. S1218 describes Notification prioritisation in more detail. The prioritisation method used should be detailed in the Alarm and Alert Strategy.

D Presentation

- Alarms, alerts and Supplemental Messages ideally need to be presented to the recipient in a manner that clearly informs what has happened, what the impact is and what needs to be done about it.
- For multiple presentations of Notifications on different interfaces from the same Alarm and Alert system, the operators' roles and responsibilities should be clearly defined in the Alarm and Alert Strategy to ensure there are no conflicts when responding to these Notifications.
- Alert Notifications should be comprised of the following information as a minimum. Identifier, description, source, priority, correct operator response guidance, time presented. Alarm Notifications should be comprised of the same information plus an estimated time of impact and impact severity.
- Alarm and Alert systems should be designed to meet End User needs and operate within the operator's capabilities and system capacity. This means that the information Alarm and Alert systems present should:

    - Be relevant to the operator's role at the time;
    - Indicate clearly what response is required;
    - Be presented at the rate at which they are generated (where this exceeds the operator's capabilities, consideration must be given to the interactive system design and include consideration of additional resource to manage Notifications).

4.3 Developing an Alarm and Alert response

TfL aspires to treat all Alarm and Alert s in the same way across all asset areas.

In order to achieve this Alarm and Alert response process should meet the following requirements:

- The human factor requirements defined in LU standards S1217 and S1218
- Appropriate thresholds should be defined for alerts and Alarm and Alert s
- Alarm and Alerts should be notified to a user
- Alarm and Alert s should generate a user action

- Alarm and Alert and alert data should be analysed along with other relevant data on a periodic basis in order to review the system thresholds and to identify potential improvement opportunities. This frequency should be defined based on the severity, criticality and potential impact on safety and the service
- All Alarm and Alert s generated should be captured as items within Ellipse or Maximo
- The presentation of Alarm and Alert s should be at a rate that does not overload the End User.

4.3.1 Characteristics of alarms and alerts

Alarms and alerts should be notified to an End User who should instigate a response in accordance with the Directors Risk Assurance Change Control Team (DRACCT) approved alert and Alarm and Alert management process.

A. Characteristics of an alarm:
   - Presents risk to the business in terms of safety, performance and/or cost
   - Requires acknowledgement
   - Requires a response within an agreed/specified timeframe
   - Requires a Work Order to be raised
   - Requires positive confirmation that the work is complete
   - Alarm output is repeatable and known.

B. Characteristics of an alert:
   - Requires analysis to identify potential risk to the business
   - Issue has potential to raise a future risk to the business
   - Discrete analysis identifying trends, patterns, anomalous behaviour over time is required.

4.3.2 Alarm and Alert - management process

The following DRACCT approved process has been developed to meet the requirements of S1213 and the aspiration of the business to manage all Alarm and Alert s in the same way.

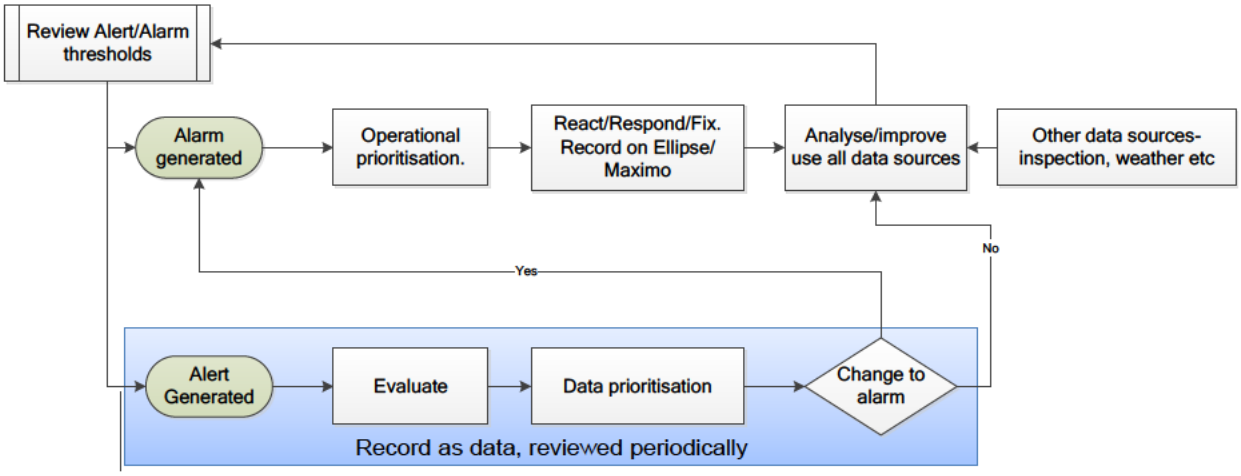


Figure 1 – DRACCT approved process for the management of alarms and alerts

It should be noted that this is a generic process; therefore, when looking to implement this for a specific asset, consideration should be given to the guidance provided in the following sections.

4.3.3 Alarm and Alert prioritisation

A suggested criticality prioritisation for Alarm and Alert thresholds is shown in Table 2 (below).

Table 2 – Suggested Alarm and alert threshold criticalities

Table

Risk	Alarm and Alert/Alert Priority		Priority Band BS EN 62682: (2015)
High	**Alarm**	**Safety Criticality**	Critical
High	**Alarm**	Safety requiring immediate operational response to prevent a safety issue arising	High
Medium	**Alarm or alert**	Not Safety-Related, time critical	Medium
Low	**Alert**	Not Safety-Related, non-time critical – operator response required but low urgency	Low
Low	**Alert**	Informative or operational awareness – no operational response required	Low

A practical example of how Alarm and Alert thresholds can be linked to maintenance interventions is shown below in Table 3.

Time Required to capture operator attention so that appropriate action can be taken	Most Likely consequence of not taking action			
	Safety or Performance Impact	Medium performance impact	Small performance Impact	Normal system event/ very low or no performance impact
High Immediate or (within x mins)	High priority	Medium Priority	Low priority	Alert
Medium: Next Engineering hours	Medium Priority	Low Priority	Low priority	Alert
Low: Next Scheduled Maintenance	Low Priority	Low priority	Low priority	Alert
None (attention not essential from operator)	N/A	Alert	Alert	Alert

Table 3 – A practical example linking alarms and alerts to maintenance responses

4.3.4 Roles and responsibilities

In defining the various process roles and responsibilities adequate consideration should be given to:

- Who carries out each stage of the process?
- How often should each stage of the process be carried out?
- With whom, and how, should each person carrying out the process communicate?
- What data sources are available and how should they be used and visualised?

The following key principles should be applied when considering the provision of specific work instructions for each of the process roles, identified above.

- Alarm, alert and event data should be recorded in a manner that it is easily accessible for analysis

- Individuals analysing alarm, alert and event data should be technically competent in the condition monitoring system and the asset being monitored such that they may verify or challenge the appropriateness of specific maintenance practices and / or identify potential ARCM system improvements
- Those required to analyse the data, in accordance with the defined review periodicity, may include the asset owner, a data analyst, or another competent engineer. All should be able to present trends and analysis in a way that is meaningful such that the asset owner may consider modifications to the Alert/ Alarm and Alert thresholds in response to the analysis results
- Evaluation and data prioritisation may be carried out by a software algorithm where standard outputs from the system exist.

4.3.5 Frequency of Alarm and Alert reviews

Review period frequencies should be established in order to verify that alarms and alerts are both timely and meaningful. Reviews should vary dependent on such factors as, but not limited to:

- The impact of time required to respond to alarms or alerts
- The criticality of the asset to service
- The frequency of asset reporting, to allow effective plans to be implemented
- The performance of the asset in providing a service; where an asset is performing badly and has poor availability, the asset owner should consider analysing data on a more frequent basis.

When looking to vary Alarm and Alert thresholds, the user should consider the context of the service provided by the asset to include, but not limited to:

- Geographical Location – the response required at a key Central London location may be different to the response required in a less heavily used area
- The environment within which the asset is required to operate – tunnel, open section etc
- The potential impact of service failures on our customers – for example, should an escalator fail at Bank this could quickly lead to station control, closure and suspension of the Waterloo and City line. An escalator failure within a bank of three at Wood Green would have a lower impact on service
- The trend of alerts over time and whether these signify a pre cursor to an Alarm and Alert or a failure.

4.4 Clarification on Safety Integrity Level (SIL) requirements

3.4	*RCM software used in railway applications shall be designed and maintained to attain SIL 0 (or equivalent) rating as per BS EN 50128.*

This is demonstrated in figure 2 (taken from S1213):

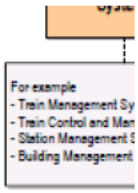


Figure 2 – Context diagram for Asset Remote Condition Monitoring

Further clarification is provided in S1210 'Safety related software'

"The scope of this standard is limited to software that supports safety functions in the context of an operational railway. This excludes non-safety related information management and support functions that are regarded as business systems, back-office, and non-operational IT information systems."

ARCM systems are defined as being safety-related but do not as a rule impact on the operation or control of the railway.

As such they are required to attain a Safety Integrity Level (SIL) of 0 as defined in BS EN 50128.

In order to meet the requirements of SIL-0, the software provider needs to demonstrate ISO 9000 compliance or equivalent.

Further guidance on meeting the requirements of SIL-0 is available in BS EN 50128.

If further clarification is required, the person accountable of standard S1210 may be consulted.

4.5 Maturity level classifications

3.10	*New or updated RCM systems shall achieve Process maturity level 3 ("standardised") through their life cycles as described in G0213 'Asset Condition Monitoring, Alarm and alert and Alert Management'.*

4.5.1 Responsibilities

Each manager who has responsibility for the ownership and operation of an RCM system needs to verify, before the systems acceptance into Business as Usual (BAU) use, that the system has achieved, as a minimum, a Process Maturity of Level 3 (standardised)

This may include operational business managers, e.g. depot managers, track managers, signal managers, stations engineering maintenance managers etc.

Project delivery managers are responsible for ensuring that the PPMP requirements have been met and that the required technical and process levels have been achieved prior to the projects submission to the User Acceptance Manager for their formal business as usual adoption approval.

The following guidance has been provided to assist those required to assess or accept remote condition monitoring systems into business as usual. It should however, be recognised that the Pathway process will always take precedence should any conflicts arise.

4.5.2 Technical capability classifications

This section details the different technical capability classification levels for remote condition monitoring. It may be uneconomical to install the same level of capability across the entire network due to varied usage trends, complexity and significance of the assets being monitored. Understanding the current technical use and potential condition monitoring asset capability helps in assessing the cost and benefits of installing remote condition monitoring equipment.

Four levels of technical capability are defined below. The levels are based on the BS ISO 13379 Condition monitoring and diagnostics of machines — data processing, communication and presentation. Each progressive level is assumed to increase the complexity of the remote condition monitoring systems.

Level 1 Capability: State detection

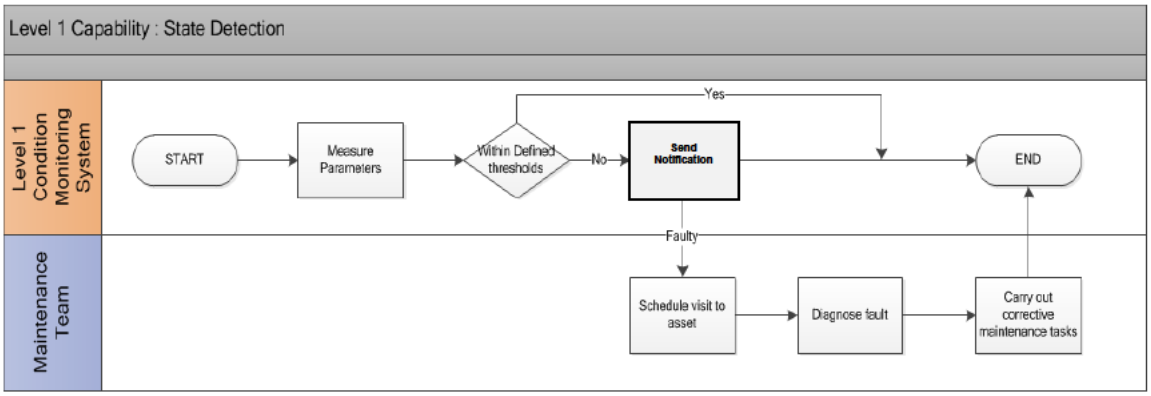


Figure 3: Level 1 Capability - state detection

This level compares features against expected values or operational limits i.e. Anomaly detection.

The condition monitoring system measures key parameters on the asset and determines if the measurements are indicative of a healthy asset or a faulty one. If a fault is suspected, a Notification is sent and responded to in accordance with the Alarm and Alert management process.

Level 2 Capability: Health assessment

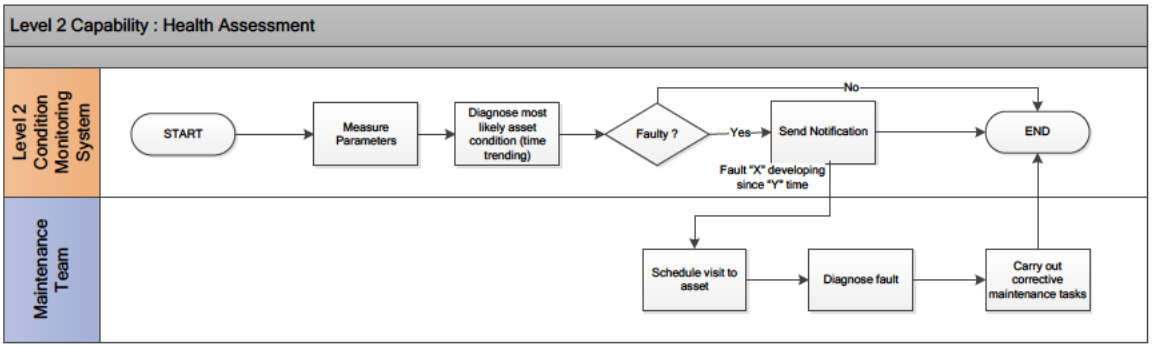


Figure 4: Level 2 Capability - Health Assessment

This level determines the current health of the asset or its subcomponents through diagnostics. The ARCM system monitors degradation of the assets performance, over time, by comparing its current measurement parameters with previous records. Automatic Notifications are sent when degradation of the assets performance falls below the pre-determined performance levels encompassed in the ARCM systems design.

Level 3 Capability: Prognostic assessment

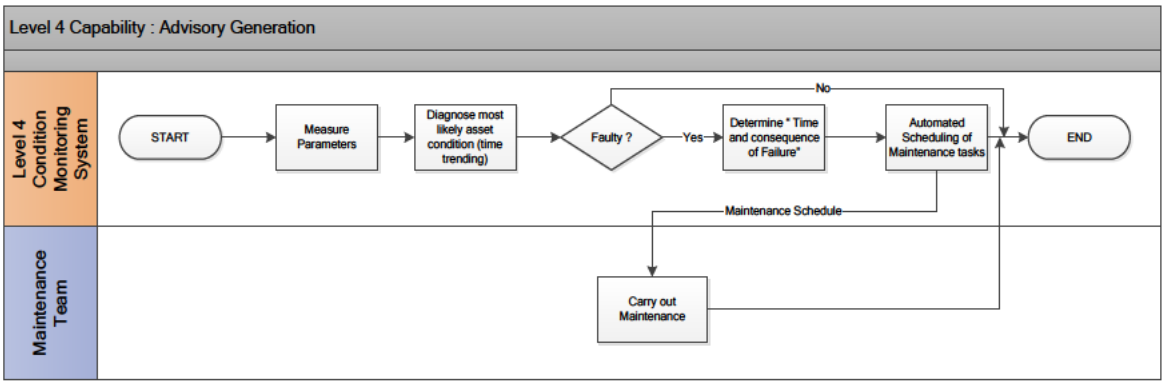


Figure 5: Level 3 Capability - Prognostic Assessment

A condition monitoring asset at this level sends an advance indication of a future event/ prediction around time to failure.

The automatic system determines the condition of the asset; when a fault develops the Alarm and Alert and the maintainer is also given an indication of how much time remains before a failure occurs as well as a prediction of the failure consequence. It enables the operator detect and isolate a fault ascribed to a specific platform component or system while the system is still functional and provides the ability to determine the remaining useful life (RUL) until failure.

Level 4 Capability: Advisory generation

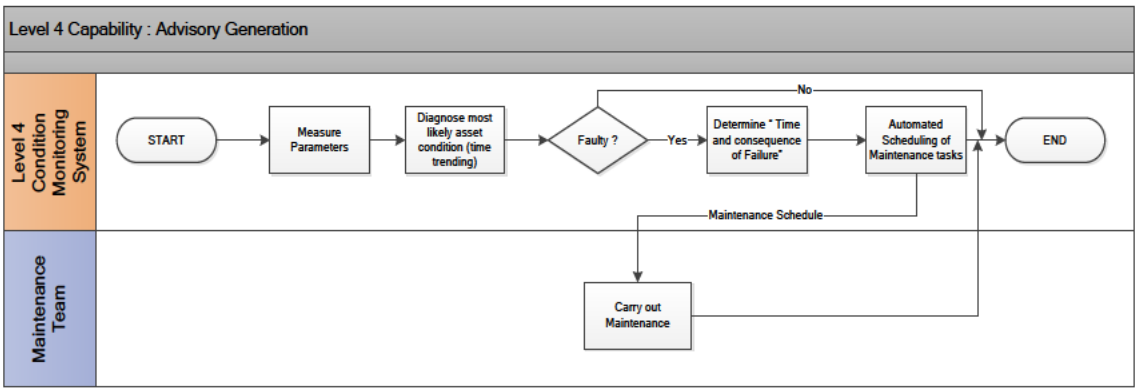


Figure 6: Level 4 Capability - Advisory Generation

This level allows for condition based maintenance in truest sense by enabling automated work order planning and scheduling based on the diagnosis of the fault and the ability to determine the remaining useful life (RUL) until failure.

4.5.3 Process maturity classifications

This section describes the different process maturity levels and follows the same principle as defined in the industry recognised standards, Business Process Maturity Model (BPMM) and Capability Maturity Model and Integration (CMMI).

The five maturity process levels below describe evolutionary stages in which an organization manages the maturity growth of its processes.

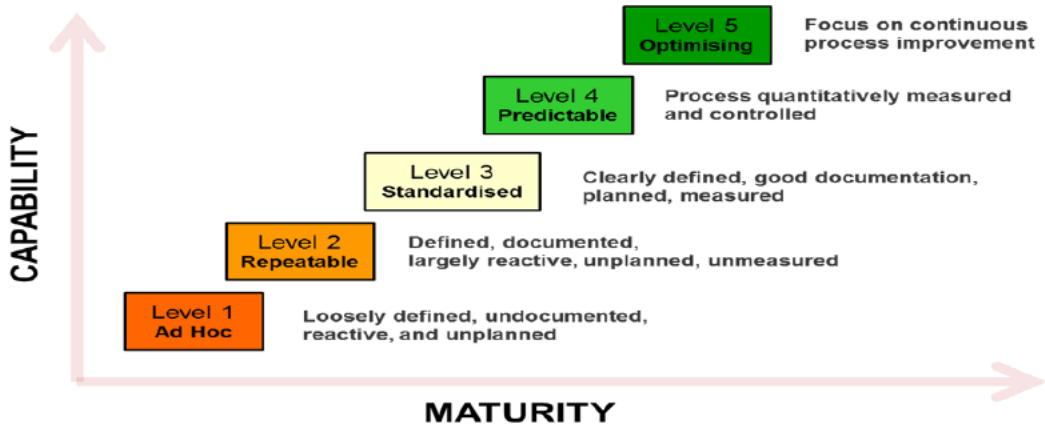


Figure 7: Process Maturity Classifications

Maturity Level 1: Ad Hoc (Chaotic)

It is characteristic of processes at this level to be undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled, and reactive manner by users or events. Success is likely to depend on individual efforts, and is not considered to be repeatable, because processes would not be sufficiently defined and documented to allow them to be replicated.

Maturity Level 2: Repeatable

It is characteristic of processes at this level that some of the processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

Maturity Level 3: Standardised

It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place and used to establish qualitative consistency of process performance across the business unit/ department.

Note:	It is from process maturity level 3 (Standardised) that acceptance of the system into BAU becomes possible and from where further process maturity growth should be strived for.

Maturity Level 4: Predictable

It is characteristic of processes at this level that, using process metrics, management can effectively control the current process. The performance of process at this level is controlled using statistical and other quantitative techniques, and is quantitatively predictable.

Maturity Level 5: Optimising

It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements. The goals set for the process at this level are being analysed for achievements and improved regularly. The timelines, cost targets, satisfaction levels are being achieved regularly and the targets also are being tightened by using continuous quality improvement techniques such as Six Sigma, Kaizan, etc.

4.6 Assessing the Systems Readiness for BAU Migration

The assessment of an ARCM's readiness for acceptance into Business as Usual may be conducted in three parts as follows:

4.6.1 Part 1 – Technical capability assessment

Appendix A: provides a questionnaire that can be used to assess the Technical Capability of an ARCM system as the first of three parts of the overall assessment process.

4.6.2 Part 2 – Process maturity assessment

Appendix B: provides a questionnaire that can be used to evaluate the maturity of the ARCM systems management process as the second part of the ARCM assessment process.

4.6.3 Part 3 - ARCM System Readiness Report

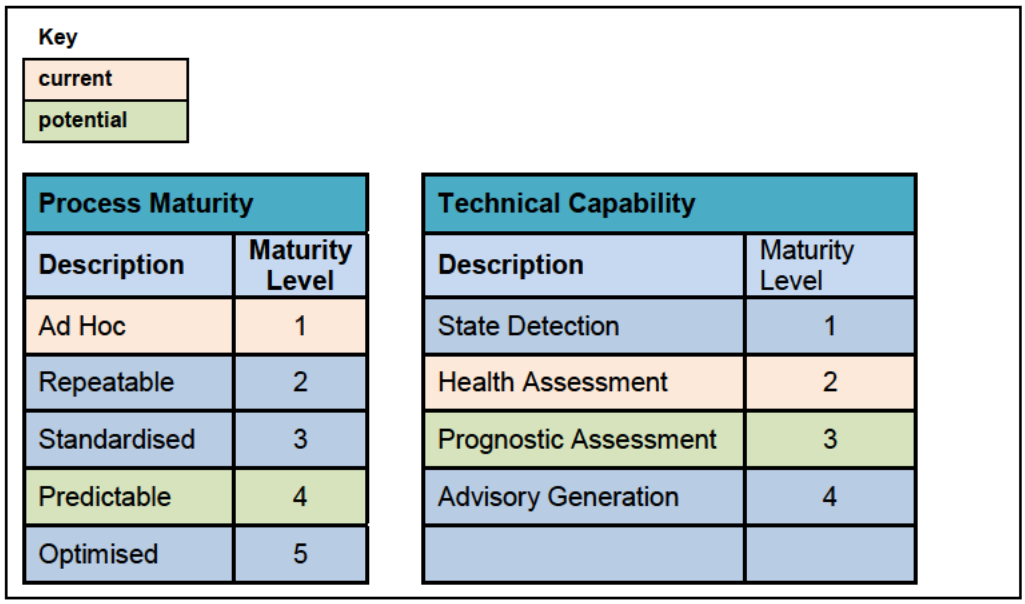
Appendix C: provides the User Acceptance Manager's with objective evidence of the overall ARCM systems readiness for transition into business as usual use.

The report provides an evaluation of the systems collective maturity and will support the delivery of the PPMP requirements.

This evaluation is represented (see below) as a ratio of the current technical usage level and process maturity level.

Current System Maturity = Current Process Maturity / Technical Use	P/T
Potential Process Maturity = Potential Process Maturity / Technical Potential	Pp/Tp

The following illustration shows an asset with a current process maturity level "Ad Hoc" and current technical usage at "Health Assessment" giving it an overall current system maturity at 1/2 with the potential to reach 4/3.



Process Maturity	
Description	**Maturity Level**
Ad Hoc	1
Repeatable	2
Standardised	3
Predictable	4
Optimised	5

Technical Capability	
Description	Maturity Level
State Detection	1
Health Assessment	2
Prognostic Assessment	3
Advisory Generation	4

5 Responsibilities

5.1 The Technical Contents Manager

5.1.1 The technical contents manager is the nominated person to hold knowledge of all ARCM and Notification Management systems and is therefore able to advise if an existing system should be expanded rather than purchasing a new system.

5.1.2 The technical contents manager is responsible for seeking and obtaining other expert advice for any part of ARCM systems for which they he is not the recognised TfL LU expert. (for example, advice from Technology & Data (T&D)) experts for data interface requirements).

5.2 The User Acceptance Manager

5.2.1 The User Acceptance Manager is responsible for verifying that all of the End User requirements have been met and that the system is approved for Business as Usual use.

6 Supporting information

This guidance should be read in conjunction with:

- TfL Cat 1 Standard S1213 'Asset Remote Condition Monitoring'
- The ARCM Pathway Project Management Plan (PPMP)

7 Person accountable for the document

Name	Job title
Stephen Foot	Head of Asset Condition

8 Definitions

Term	Definition	Source
Alarm and Alert	A system response that is prioritised according to the severity of impact on safety, or reliability, and time available to the user in which to fully, or partially, mitigate the impact.	Glossary
Alarm and Alert Strategy	Documents that define the functional and technical requirements and performance of Notification Systems.	Glossary
Alarm and Alert Philosophy	Is a document that establishes the basic definitions, principles, and processes to design, implement, and maintain a Notification System.	Glossary
Alert	A system response with lower priority user action than an Alarm and Alert that is prioritised according to time available to the user in which to complete the action.	Glossary
Asset Remote Condition Monitoring	Asset Remote Condition Monitoring (ARCM) is the monitoring of relevant operating parameters of assets from a different location to the asset being monitored with the aim of: • Predicting & preventing failures, and • Improving maintenance efficiency.	Glossary
End User(s)	Includes the maintainer and the asset user responsible for monitoring & processing Alarm and Alerts & Alerts and other users using the system.	Glossary
Notification	A type of system response. There are two types of Notification: Alarm and Alert and Alert.	Glossary
Notification Management	Refers to Alarm and Alert and Alert Management.	Glossary
Predictive Maintenance	Typically a non-invasive task intended to identify a specific condition of an asset. This knowledge of the asset enables preventive maintenance to be performed at the optimum time based on the forecast of condition degradation and in advance of asset failure.	Glossary

Supplemental Message	Supplemental Messages may include event or environmental data which are not classified as warranting an Alarm and Alert or alert but provide information of value to the receiver. E.g. multiple occurrences of the same event in a set time period or a particular sequence of events etc.	Glossary
TfL Pathway	TfL's management and assurance methodology that is mandated for all project and programme work.	Glossary
User Acceptance Manager	A suitably competent London Underground individual, shall be responsible for all human factors related activities performed by London Underground and for the acceptance process for operability issues	Glossary

9 Abbreviations

Abbreviation	Meaning
ARCM	Asset Remote Condition Monitoring
BAU	Business as Usual
CM	Condition Monitoring
DRACCT	Directors Risk, Assurance and Change Control Team.
HFIP	Human Factors Integration Plan
LU	London Underground
LUL	London Underground Limited
PPMP	Pathway Project Management Plan
RUL	Remaining Useful Life
SIL	Safety Integrity Level
TfL	Transport For London

10 References

Document no.	Title or URL
S1210	Safety related software
S1217	Integration of human factors into system development
S1218	Human systems Interaction – dialogues and notifications
BS ISO 13379	Condition Monitoring and diagnostics of machines – Date interpretation and diagnostic techniques – General guide lines

BS EN 50128.	Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems
BS EN 62682: 2015	Management of Alarm and Alert s systems for the process industries

11 Document history

Issue no.	Date	Changes	Author
A1	April 2013	A new guidance document produced as per DRACCT Action No. 01617. This guidance is related to Category 1 Standard (S1213).	Chris Welford
A2	February 2016	Standard change, incorporating Alarm and Alert Management in accordance with DRACCT Ref No. 04283 Santos Bunga	Santos Bunga
A3	November 2017	A new guidance document produced as per DRACCT Action No 05553 . This guidance is related to revisions to Category 1 Standard (S1213).	Steve Duncan

12 Attachments

This page intentionally left blank

12.1 Appendix A: Technical Capability Assessment

Technical Capability Assessment

System under Assessment

< >

Subject	Name & Signature	Business Unit
Document Owner		
Assessment Date		
Process Owner		
Technical Assessor		

Serial	Check	Findings & Recommendations
1	**Asset Overview**	
1.1	What is the function and applicable performance standards of the asset being monitored?	
1.2	How can it fail to fulfil its functions?	
1.3	What causes each functional failure?	
1.4	What happens when each failure occurs?	
1.5	In what way does each failure matter/ What is the impact of each failure?	
1.6	What is the current inspection and maintenance regime?	.
1.7	What is the current performance of the asset (in terms of SAF counts and LCH impacts , MTBF /MDBF etc.?	
1.8	Has the failure analysis identified and recommended actions to address failure modes where suitable preventative tasks could not be found? e.g. condition monitoring, routine change, re-design, supplementary inspections.	
2.	**Asset Remote Condition Monitoring (ARCM) System**	
2.1	What is the ARCM system? What documentation exists to describe the system?	

2.2	Does the system comply with the requirements contained within LU Cat 1 Standard S1213 ?	

Serial	Check	Findings & Recommendations
2.3	Who supplied the system?	
2.4	Has the system been configured using a commercial 'off the shelf' product?	
2.5	Have the (end to end) system ownership and maintenance responsibilities been clearly defined?	
2.6	Who repairs the system when it breaks down?	
2.7	Who is responsible for the management of Obsolescence in accordance with the requirements of LU Cat 1 Standard S1043 'Obsolescence Management'?	
2.8	If owned by a third party what is the contractual arrangement & scope of supply? Detail any Service Level Agreements with Suppliers including corporate Technology & Data (T&D) if appropriate.	
2.9	Who are the systems 'primary' users? Alarm and Alerts? Alerts? Where are their requirements captured?	
2.10	Who are its 'secondary' users? Engineers? Data Analysts? Where are their requirements captured?	
2.11	Who are its tertiary users? E.g. S&ND and any others who may wish to use the systems data to make business decisions. Where are their requirements captured?	

Serial	Check	Findings & Recommendations
2.12	What shortfalls, if any, have been identified by the systems users? How are these being addressed?	
2.13	Can the system demonstrate its operational availability at all of its required times?	
3.	**Data Acquisition**	
3.1	What & how is data gathered by the system?	
3.2	On what basis was the data requirement defined?	
3.3	Who owns this data?	
3.4	Where and how is it stored?	
3.5	Has the collection, and configuration of the systems data and the arrangements for its usage been optimised?	
4.	**Data Manipulation**	
4.1	Does the system have correctly defined attributes and understanding of what should be the right operating condition depending on configuration / environment, usage levels etc.?	

Serial	Check	Findings & Recommendations
4.2	How were the Alarm and Alert measurement parameters derived?	
4.3	How were the Alarm and Alert trigger levels derived?	
4.4	Does LU have access to the raw data?	
5.	**Alarm and Alert Management**	
5.1	Does the system compare features against expected values or operational limits?	
5.2	At the time of the assessment: What is the average Alarm and Alert rate: • Per Hour? • Per Day ? What percentages of Alarm and Alerts have been recorded as: • False Positives? • False Negatives? • Exceeding the Response time? • Exceeding the Clearance time? What is the percentage distribution of Alarm and Alerts: • High? • Medium? • Low?	
5.3	How successful is the system in preventing service affecting failures?	

Serial	Check	Findings & Recommendations
5.4	What KPI's and reporting arrangements have been put in place to measure the systems level of performance? E.g. • Alarm and Alert rates. • Response times. • Clearance times etc.	
5.5	Has the system already delivered efficiency benefits? If so quantify:	
6.	**Health Assessment**	
6.1	Does the system determine the current health of the asset being monitored or its sub-components through diagnostics?	
7	**Prognostic Assessment**	
7.1	Does the system provide advance indication of a future event / prediction around the consequence and time to failure?	
7.2	With further development, is it likely that the system could provide prognostic assessment?	
8.	**Advisory Generation**	
8.1	Following the prognostic assessment, does the system provide Condition based maintenance and /or automated work order planning and scheduling?	

Serial	Check	Findings & Recommendations
9	**Asset Management**	
9.1	Has the ARCM system been registered in Ellipse / Maximo in accordance with the requirements defined in Cat 1 Standard (S1011) 'Product Acceptance and Registration'?	
9.2	Has an O&M Manual been produced?	
9.3	Is evidence available to verify that suitable installer and maintenance training been rolled out against the Operating and Maintenance (O&M) requirements?	
9.4	Have the requirements defined in the Pathway Product Management Plan been met?	
10	**User Observations & Recommendations**	
10.1	Does the system currently meet the needs of its users?	
10.2	Do the users or consider that, with further development, the system has the potential to deliver additional LCH or efficiency benefits?	
10.3	What actions are recommended by the users / assessor to secure the potential benefits identified in 10.2 above	
11.	**Technical Capability**	
11.1	The Technical capability of the system is established from the completion of the questions provided above.	

Technical Capability (TC)	
Description	TC Level
State Detection	1
Health Assessment	2
Prognostic Assessment	3
Advisory Generation	4

End

This page intentionally left blank

12.2 Appendix B: Process Maturity Assessment

Asset Remote Condition Monitoring
Process Maturity Assessment

Document Owner		
Process Owner		
Assessor		

No	Criteria			Level 1	Level 2	Level 3	Level 4	Level 5	Prompt Question	Recommendations
	Primary	Sub Component	Supporting script	Ad Hoc	Repeatable	Standardised	Predictable	Optimising		To achieve level 3 or to move to the next maturity level
1	PROCESS	**Standardisation**	A standardized process is a repeatable, consistent way of performing tasks that can span organizational boundaries. Benefits - • Implementing standardized processes usually results in lower process overheads and can reduce the complexity of information systems. • Repeat performance of a task gives the same expected results every time.	No processes/ procedures are documented.	Part of the process /procedures are documented but may be out of date and no regular review dates have been established.	Parts of the process/procedures are documented and what is documented is regularly refreshed.	Most of the process/procedures are documented and what is documented is regularly refreshed and kept current	The full process is documented end to end. Cross process interfaces are identified and documented, across all business units. The full process is always up-to-date.	Please select the statement which best describes the current standardisation of the process	
2		**Operational Levels**	Service/ Operational levels are agreements that define how the various internal groups within a company plan to deliver a service or set of services	Service / Operational levels are not defined.	Service/ Operational levels are defined.	Service/ Operational levels are defined and measured.	Service/ Operational levels are defined, measured and reported.	Service/ Operational levels are reported at required frequency and revisited every year.	Please select the statement which best describes the operational levels of the process.	
3		**Fragmentation**	Business fragmentation occurs when critical processes aren't managed as an integrated system. Processes become a complex series of handoffs between functions, jobs and information systems. Each handoff represents an opportunity to introduce error,	5 or more handoffs	3 or 4 handoffs	Two hand - offs	1 hand- off	No hand -off	Please select the statement which best describes the number of hand-offs that occur within the process (internal and/or external to your department whereby a work item in the	

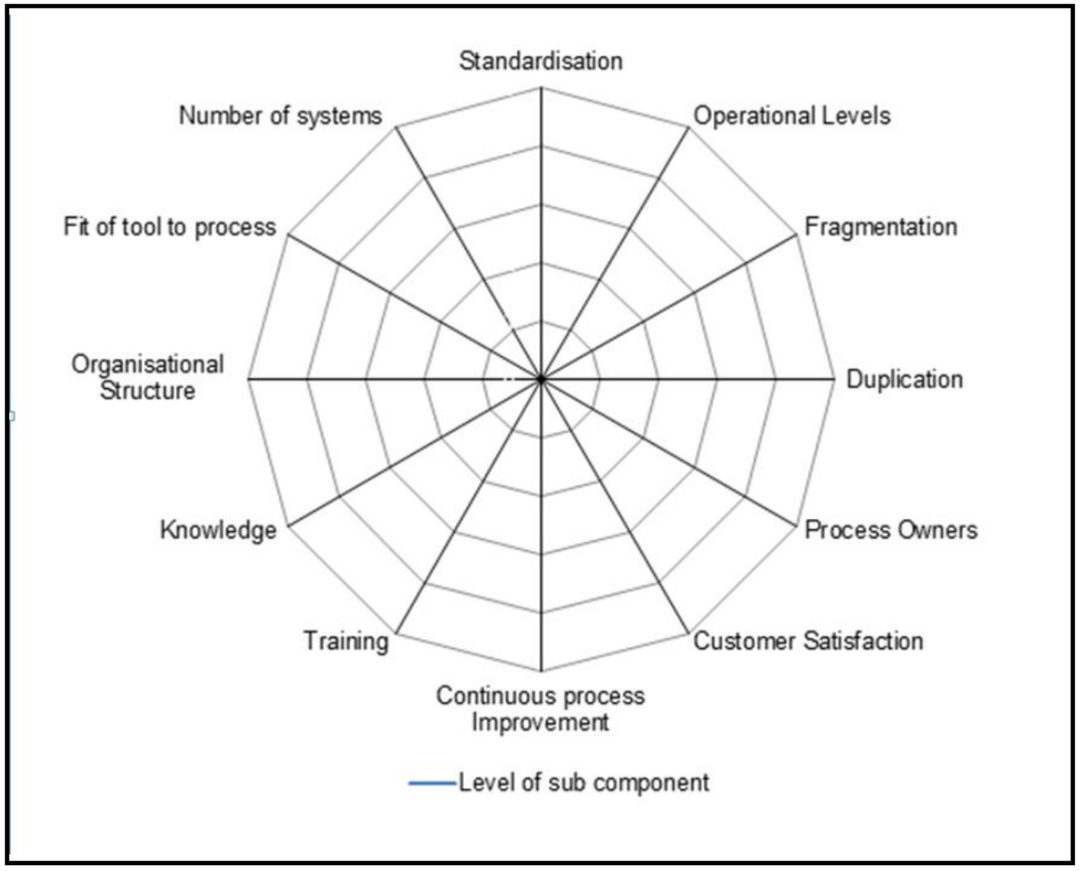
			delay and added cost. Devoid of an integrated process management framework, process value deteriorates. The potential for resistance increases and the speed of implementing improvements declines.						process is passed between individuals	
4		**Duplication**	Examples - Duplication of efforts.	Similar or same activities repeated by multiple teams		Some duplication of activities across teams		No duplication of activities	Please select the statement which best describes the amount of duplication (to the best of your knowledge) that occurs within the process either within your department or is performed elsewhere (in addition to your department)	
5		**Process Owners**	The individual(s) responsible for process design and performance. The process owner is accountable for sustaining the gain and identifying future improvement opportunities on the process.	No process owner exists		An informal process owner exist		The process owner is formally identified and communicated	Please select the statement which best describes the level of process ownership that currently exists for your process	
6		**Customer Satisfaction**	How well does the system meet the needs of its customers/stakeholders?	Doesn't meet customer expectations		Meet customer expectations		Exceeds customer expectation	Please select the statement which best describes how satisfied your customers are: Primary? Secondary? Tertiary?	
7		**Continuous process Improvement**	Continuous process improvement refers to ongoing efforts to improve business processes. Continuous process improvement is a formal, ongoing approach to improving processes and, ultimately productivity, services and products. Processes are constantly evaluated, often based on employee and customer feedback and adapted as needed to meet organization goals.	No process improvement in the last 12 months	Continuous process improvement identified	Continuous process improvement identified and in progress	Continuous process improvement identified and implemented	Formalised continuous process improvement rigor in place	Please select the statement which best describes the level of continuous process improvement rigor embedded in the process	

8	**PEOPLE**	**Training**	Training is based on initial skills assessment and training provided where additional/new skills are required.	No process training exists.	Training is predominantly hands-on (on the job) with various individuals providing the training.	Some training is conducted based on documented materials with some training being hands –on.	Formal training is documented and records are always up to date. Assessments are regularly conducted with refresher courses provided when needed.	Training material is up to date and regular assessments are conducted with relevant refresher training provided.	Please select the statement which best describes the type of training available on the existing processes.	
9		**Knowledge**	How well do individuals understand the end to end process?	People are not aware of the end to end process. Only aware of the tasks they or their team needs to perform.		People can name the process they perform and how it fits into the overall process flow and adds value.		People can describe the overall End to End process along with its customers, suppliers, inputs, outputs and the value of the process.	Please select the statement which best describes the level of knowledge that people have of the end to end process (of which they execute a part thereof)	
		Organisational Structure	How well are the organisational roles and responsibilities defined for those required to execute the process.	Roles and responsibilities are not defined.		Roles and responsibilities are not formally defined and documented.		Roles and responsibilities are formally defined and documented for each role in the end to end process.	Please select the statement which best describes the level of role and responsibility definition for the people executing the process	
11	**Tools Used**	**Fit of tool to process**	Define how well he tools used fit the requirements of the process users.	Tools used are in majority manual and not designed specifically for the process.	Tools used are a mix of automated (systems) and manual tools and are partly designed based on the process.	Tools used are in the majority automated (systems) and, are partly based upon the needs of the process being executed.	Tools used are in the majority automated (systems) and are largely based on the needs of the process.	Tools used predominantly automated (systems) and have been fully designed to meet the needs of the process and its users.	Please select the statement which best describes whether tools used are systems or manual processes and their fit to the process	
12		**Number of systems**	Define how many systems are involved in the delivery of the process.	Number of systems used > 5	Number of systems used 4	Number of systems used 3	Number of systems used 2	Only 1 system used	Please select the statement which best describes the number of automated applications (systems) used in the process	

Process Evaluation		
PROCESS	No	Level Score
	1	
	2	
	3	
	4	
	5	
	6	
	7	
PEOPLE	8	
	9	
	10	
TOOLS USED	11	
	12	
Process Maturity Level = Average Level Score		

Process Maturity of < > System

Plot level scores and join them (clockwise) to complete the maturity level spider diagram.



Technical Capability

< **>**

Insert Capability Assessment level from Appendix 'A'

Note: It is from maturity level 3 (Standardised) that acceptance of the system into BAU becomes possible and from where further maturity growth should be strived for.

12.3 Appendix C: System Evaluation Report

Asset Remote Condition Monitoring

System Evaluation Report

< Insert Name of ARCM System>

Document Owner	
Date	
Version	
Status	
Process Owner	
Asset Condition & Operational Engineering	
User Acceptance Manager	

1. Introduction

1.1 Process Overview/Objective/Description

The aim of this document is to provide a final systems summary report after concluding **the** current state assessments of the < > Asset Remote Condition Monitoring (ARCM) system. It provides a holistic view of the technical capability and the business critical processes and addresses all of the factors that can affect performance of the overall system.

The technical capability of the system has been examined to assess its current capability and its potential for further development.

Processes take input from one or more sources (including other processes), manipulate the input, utilise resources according to the policies and produce output (including output to other processes). Processes should have clear business objectives for existing, accountable owners, clear roles and responsibilities around the execution of each activity, and the means to undertake and measure effective performance. To this end the systems processes have been assessed to affirm their effectiveness in the application of reliable and repetitive collection of activities, procedures and controls to perform their given tasks.

Whilst the description of the process in this document is at a summary level it is broad enough to provide information on the factors that may cause a failure to achieve objectives, or that could compromise other parts of the business i.e. the detail on the impact and cause of risks

1.2 Background

One of the key focus areas for the future maintenance of the companies engineering assets is to maximise the reliability benefits being gained from its ARCM systems. The ARCM of < Assets > is the focus of this report.

1.2.1 Problem statement

The reliability of the companies engineering assets are less than desirable due to an inability to detect asset degradation in a manner that permits failures to be predicted and prevented through appropriate and timely remedial interventions.

Consequentially, the business is keen to understand the processes through which < Asset >condition data is collated and managed, in order to determine the value they bring to our customers and in addition permitting areas of opportunity to be identified.

1.2.2 Goal statement

Conduct a system maturity assessment to ascertain the Technical and Process capability of the < Insert System> condition monitoring. This will include:

- Documenting how condition data is currently gathered and utilised.
- Identifying key roles and responsibilities for the collection and management of periodic performance data – Owners and principal users.

- Establishing what formal documentation currently exists.
- Documenting the Current & Potential Technical Capability of the system.
- Identify the potential technical capability of the system.
- Identify the potential process maturity for the system.
- Recommend actions to realise this capability.

2. Process Scope

Defines precisely where the processes start and end, and what is specifically included and explicitly excluded.

2.1 In scope:

End to End process management followed across < system > Asset Remote Condition Monitoring. These include: Alarm and Alert & Alert management, the management of responses and performance reporting.

2.2 Out of scope:

Any other condition monitoring asset in use across London Underground.

2.3 Process boundaries:

A. Process starts:

For example, the process starts when registered users receive alerts or Alarm and Alerts from the < Insert System> system.

B. Process Ends:

For example, the process ends when the Condition Base Monitoring (CBM) team review the completed report.

3. Key Performance Indicators (KPIs)

The system owner must develop specific KPI's to determine the effectiveness and value being derived from the introduction and continued operation of the system.

Measures may include; MTBF and LCH and measures of Alarm and Alert system performance.

4. Benefits realisation

Highlight the benefits described in the business case as a result of implementing the condition monitoring capability.

Define what arrangements have been put in place to measure the achievement of these benefits.

5. Process diagram(s)

<Insert a Process Diagram for each of the processes identified >

Entry Point	Threshold breach recorded by the ACM system
Inputs	Graphical User Interface (GUI) and text message alerts to registered users
Outputs	Relevant action taken to address alert /fault
Exit Criteria	Alert investigated and report closed

6 Process Description(s)

This section provides a general description of how the activities in the process happen and the responsible role for each activity. This section supplements the above process flow section

< Process>

Activity Number	Activity Description	Responsible Role
1.0		
2.0		
3.0		
4.0		
5.0		
6.0		
7.0		

< Process>

Activity Number	*Activity Description*	*Responsible Role*
1.0		
2.0		
3.0		
4.0		
5.0		
6.0		

7. Roles and Responsibilities

Summarise the key responsibilities for each role

Name	Title and Business Area	Business Process Role

8. Process risks and mitigation/control

The section covers the process risks and controls and should be completed along with the process owner. In order to address the risks identified, do we plan to accept, transfer, avoid or actively mitigate? To influence the business decision, three types of control need to be considered:

A. Preventative controls:

These controls are designed to prevent the possibility of a process or associated system failure occurring. Examples – Segregation of duties, passwords and physical control over assets

B. Detective controls:

These controls are designed to detect errors or failure which may have already occurred. Examples – Exception reporting, reconciliation and audits

C. Corrective controls:

These controls are designed to correct an error or failure that has occurred. Examples – Reconfiguration of a compromised system

Risk	Impact	Likelihood (H/M/L)	Control Description	P/D/C Control Type

P/D/C control type – predictive / detective/corrective

9. Operational/ service level agreements

This section includes the performance thresholds and the measurements (SLAs, process targets etc.). These should be determined and agreed to support ongoing operational and efficiency improvement. How will it be monitored, reported and escalated?

Performance Measures	Targets
E.g. Standard fault clearance time (period from receipt of fault rectification notice) for <system>faults	

10. Management information requirements

Provide description of reporting and information requirements (be specific about the information required).

Information Required: < >
Who will use it: < >
Why will it be used: <e.g. Performance monitoring , Predict and prevent faults>
Distribution < >
Frequency : < >
Format/Method: < >

11. System maturity assessment

In assessing the systems maturity, the examiner is required to establish the technical capability of the system and the maturity of the processes used in its operation

11.1 Technical maturity

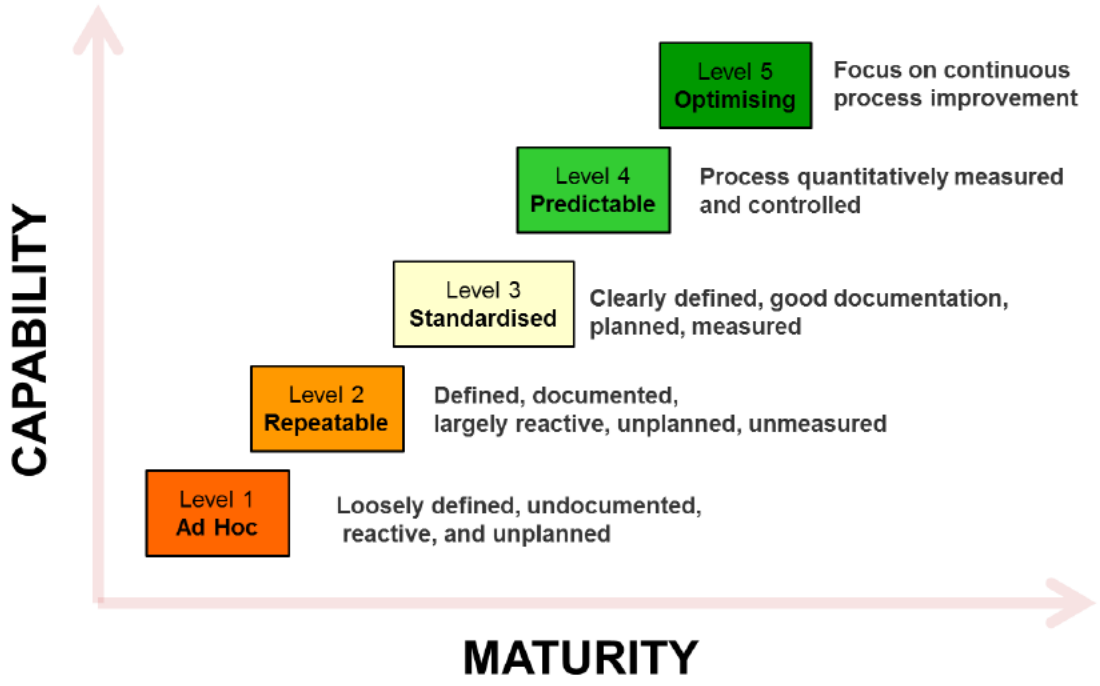
The technical maturity capability is based on the responses of the system owners technical experts to the question posed in Appendix A -ARCM technical assessment coupled with the observations of the assessor.

Please refer to Appendix A for the link to the RCM System - Technical Evaluation

11.2 Process maturity

The process maturity assessment is a framework based on “best practices”. It describes the essential elements of effective processes. These process elements provide a foundation for quantitative control of the process, which is the foundation of continuous process improvement.

The assessment describes an evolutionary improvement path that guides the business units in moving from immature, inconsistent processes to mature, disciplined processes. Below are the different levels of process maturity.



The process maturity level is determined based on the responses to the questions posed in Appendix B: Process Evaluation by the Process Experts or Process Owners together with the observations of the Assessor during the process assessment. Process assessment covers many areas such as continuous improvement, training, tools, systems and documentation.

12. System findings and recommendations

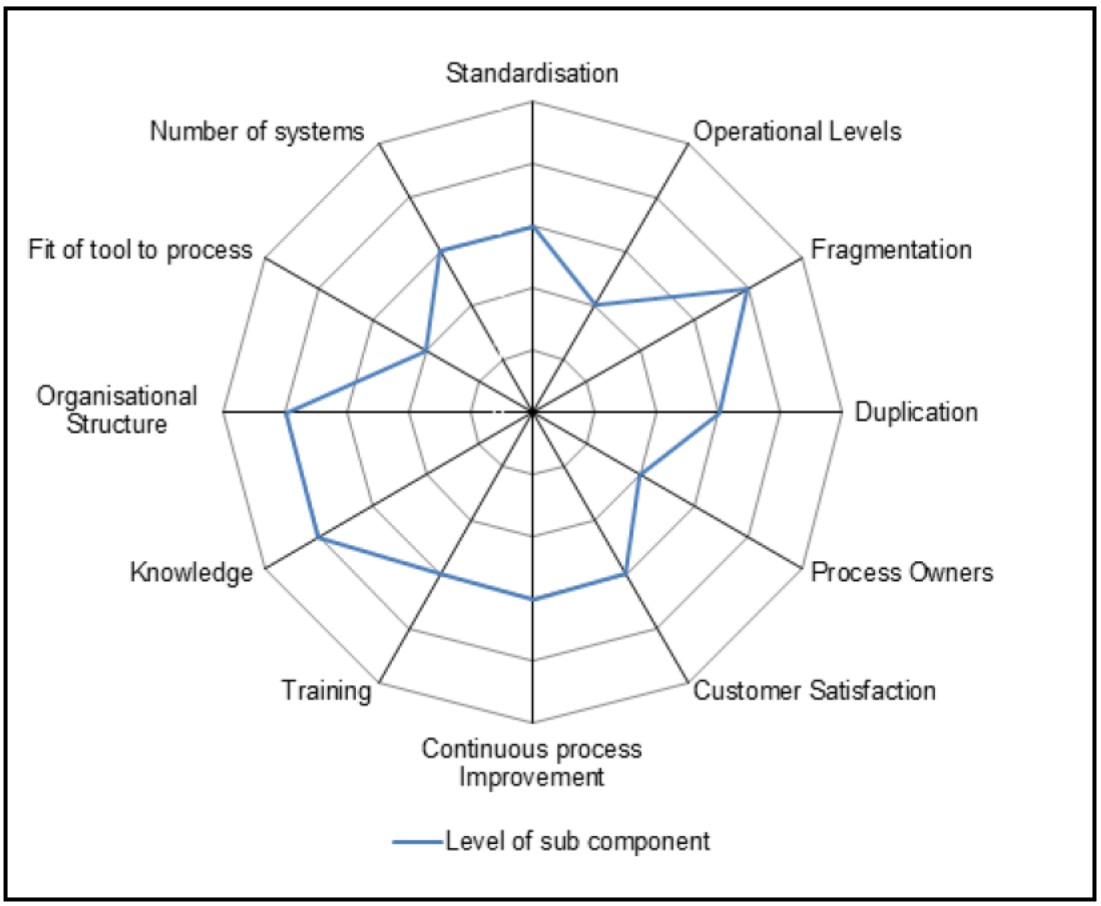
As part of the process consultation done along with the process and technical experts, the Business Improvement team has assessed the process *< System >* and determined the following findings.

Process Maturity: < Level >

Tech Capability: < Level >

Copy & Attach Web Diagram from Appendix B as exampled below

Process Maturity



12.1 Current state recommendations

This section summarises the recommendations contained within F5790 RCM Technical Evaluation Questionnaire and F5791 RCM Process Evaluation Questionnaire attached as Appendices 1& 2 respectively. These recommendations are aimed at demonstrating how the system can be further developed to progress to the next higher level of maturity.

A. Recommendation list for Technical Improvement

T1. E.g.
T2. Etc.

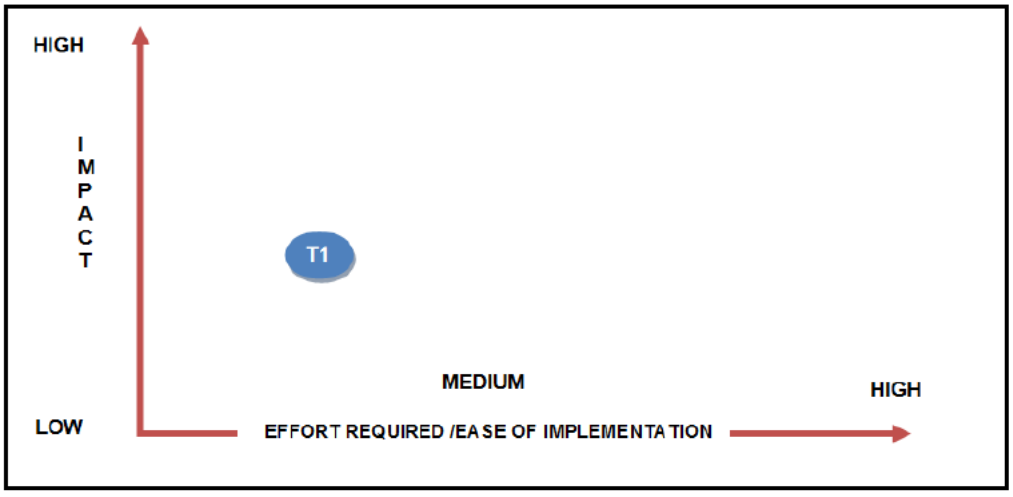
B. Recommendations for Process Improvement

P1. E.g.
P2. Etc.

13. Improvements prioritisation: impact-effort matrix

The Impact-Effort Matrix is an effective tool designed specifically for the purpose of assisting decision making regarding which of the suggested potential improvement solutions appear to be easiest to implement. It provides a matrix indicating the improvement impact offered from each potential solution together with an assessment regarding their ease of implementation.

The following recommendations have been prioritised after consultation with the process experts.



14. Appendices

Appendix A< Attach completed copy of Appendix A Technical Evaluation >

Appendix B < Attach completed copy of Appendix B Process Evaluation >

14.1 Related policies/procedures documents

This process is supports delivery of the following related document

Document Name	Document Description	Document Owner
S1213	Asset Remote Condition Monitoring	Stephen Foot - Head of Asset Condition

15. Document history

Version	Status	Date	Comments