Monitoring system minimum technical requirements

Version 3.1.1

Queensland Government

Contents

1   General

1.1   Introduction

Policy

Monitoring systems must provide at a minimum the equivalent level of monitoring and functionality as the old QOGR central monitoring system (DUCMS). The ANZ National standards document entitled "PRINCIPLES FOR THE FUNCTIONALITY OF GAMING MACHINE MONITORING AND CONTROL SYSTEMS" may also be of assistance in the design of the monitoring system.

Purpose

The purpose of this document is to:

- Advise the industry of QOGR's minimum technical requirements for Monitoring Systems.
- Ensure requirements are consistently applied.
- Achieve a high standard of integrity of monitoring of gaming machines in Queensland.

Scope

This document is applicable to all monitoring operators of regulated gaming machines in Queensland. It contains a number of minimum technical and functional requirements for the development, implementation and operation of a CMS and the monitoring system *in general*. This is not a comprehensive requirements document, as many more monitoring system technical requirements have been previously released in other OLGR technical requirements documents.

Please refer to the following documents for further requirements :

- Local Area Electronic Gaming Machine Communications Protocol "QCOM"
- Local Area Electronic Gaming Machine Communications Protocol Site Controller Protocol Operating Procedures.
- EGM Communications Interface and LAN Requirements.
- Gaming venue Electronic Meter Access.
- Site Controller Minimum Technical Requirements.
- EGM Card and Card Reader Requirements.
- Program Storage Device Verification Minimum Technical Requirements.
- Data Requirements for Monitored EGMs

1.2   Terms and Abbreviations

Central Monitoring System(CMS)
Refers to all of the Operator's non-gaming venue hardware and software which monitors and controls Electronic Gaming Machines (EGMs) and other gaming equipment**.**

Monitoring System (MS)
Refers to the entire monitoring system from the EGMs to the host system computer and database inclusive.

Database
Refers to all received EGM meters and events, plus the monitoring systems configuration data (ie. a complete history of where EGMs are located and what software they are running).

Operator
Refers to any licensed organisation that is responsible for the monitoring of gaming equipment in Queensland. This includes Licensed Monitoring Operators (LMOs) and casino operators.

2 General Requirements and Functionality

2.1 The overall requirement is that the monitoring system must provide at a minimum the equivalent level of monitoring and functionality as the old OLGR central monitoring system (DUCMS).

The ANZ National standards document entitled "PRINCIPLES FOR THE FUNCTIONALITY OF GAMING MACHINE MONITORING AND CONTROL SYSTEMS" may also be of assistance in the design of the monitoring system.

2.2 The monitoring system must support all versions of the OLGR EGM Protocol and I.G.T. EGM Protocol (Version 0.42).

2.3 The monitoring system must implement the latest version of the *Data Requirements for Monitored EGMs* document.

2.4 The CMS must have the ability to disable/enable individual EGMs.

2.5 The CMS must have the ability to disable/enable individual games in EGMs.

eg. The OLGR could issue notice for all EGMs of a specific manufacturer with a specific software version, a specific game version and installed after a certain date to be immediately disabled (instigated immediately and completed within 8 hours). To avoid this being a major exercise it is recommended the monitoring system have some automation in this area.

2.6 The CMS must only allow EGMs running OLGR approved software to be enabled.

2.7 The CMS must automatically determine which game variations are approved for the applicable jurisdiction and only allow those game variations to be enabled.

2.8   The monitoring system must be able to support (monitor and control) 16 games per EGM as a minimum. Support of greater than this amount is at the discretion of the LMO.

2.9   The CMS must support upon EGM configuration the selection of only approved betting units for resident games in the EGM.

2.10   Operators must be able to immediately disable (instigated immediately and completed within 8 hours) all EGMs. This is to cater for the situation where a problem occurs in the monitoring system which could result in the loss or corruption of data, or could result in a financial loss to any party, or causes any regulatory requirement (eg. minimum percentage return to player) not to be met.

        The CMS must connect to every site at least once per day, authenticate SC's and EGM's programs and retrieve all current meters and events. A failure for a device in the monitoring system to authenticate must cause all devices under it to automatically disable.

2.11   The CMS must automatically enable/disable each venue in accordance with its licensed gaming operating hours and special events eg. Christmas closing.

2.12   The OLGR must be able to access any part of the monitoring system programs, memory and databases at any time with the assistance of the appropriate operator personnel.

2.13   The monitoring system must be able to be installed in any existing or future site, without requiring the EGMs to be RAM cleared.

2.14   The CMS must not require the EGM's power to be left on overnight. (The Operator may recommend that power may be left on the EGMs for security monitoring of machine doors when money is being left in the EGMs overnight.)

2.15   It is recommended all hardware/equipment in the monitoring system be certified with respect to AS/NZS 60950:2000 : Safety of information technology equipment.

2.16   The current date and time must be centrally maintained by the CMS and broadcast to the SCs at least once a day over the wide area network (WAN) or more frequently if required. The current date and time maintained by the CMS must be automatically updated from a trusted time server, or be manually checked once per day, or be verified by some other approved method.

2.17   There must be an exception display or equivalent where a specific range of important events can be viewed and acted upon.

3 Security

3.1 It is recommended the monitoring system should be designed and operated with consideration to the Australian Government Information Technology Security Manual (ACSI 33) - Security Guidelines for Australian Government IT Systems and ITSEC Class F-C2 as a guide for a minimum level of software security.

> For more information, refer to the "Security information" pages of the Defence Signals Directorate web site at www.dsd.gov.au.

4 CMS Diagnostic Requirements

4.1 The Operator must ensure that a test monitoring system (including a non-live test venue as per Site Controller requirements) is available at all times, for the diagnosis of problems and the testing of upgrades. The test monitoring system must be able to operate without interfering with the live system or data in any way.

4.2 As an EGM monitoring system involves the inter-connectivity of a number of different manufacturer's equipment (specifically the EGMs and the monitoring system), it is the monitoring system operator's responsibility to diagnose the location of any bugs or problems between different manufacturer's equipment in the monitoring system.

This responsibility remains with the operator until it can be proved (either by demonstration, duplication or low level communications log) who the responsible party is, at which time the problem may then officially be transferred to the responsible party for diagnosis and rectification.

5 CMS Accommodation

5.1 The CMS must be housed in a secure area, whereby only authorised personnel may enter and gain access.

5.2 Refer to Australian Standard AS 2834-1995 "Computer accommodation" with respect to the CMS location and housing requirements.

6 Continuity of Service

6.1 In the event of a disaster at the operators premises, where it is not possible to provide monitoring services, it must be possible to restore monitoring from an alternative premises within 6 hours.

7 Power

7.1 The CMS must have an uninterruptible power supply (UPS) which, in the event of a mains power outage, allows sufficient time for the system to automatically be shut down in an orderly manner with no loss or corruption of data.

7.2 The UPS must be installed, serviced and tested strictly according to the manufacturers requirements and specifications. Service logs must be maintained by the operator.

8 Communications

8.1 Any electronic communications in the monitoring system must have error detection of at least a 16 bit Cyclic Redundancy Check Standard.

8.2 All data received by the CMS must be verified for integrity, and reasonableness. There must never be any loss of data in the monitoring system as a result of a communication fault or corruption, except if the communicated data is specifically defined as unconfirmed data.

8.3 Encryption of data is only mandatory when communicating the following types of information:-

Personal Identification Numbers (PIN) relating to cash accounts (Refer Australian Standards for EFTPOS)

Any information which, if made public, could compromise the security or integrity of the monitoring system or jackpot system.

8.4 Message Authentication

More applicable to gaming applications than encryption, where the protection required is not from disclosure but a guarantee that the information is received unaltered and from the actual indicated source. eg. Jackpot events.

Full message authentication requirements are planned to be introduced into EGMs and jackpot systems as required (with respect to the size of participating jackpots).

9 Database and Data Storage

9.1 The CMS must maintain two physical copies of the database.

9.2 All received data must be stored fault tolerantly in the databases before the monitoring system may purge data from the SCs or EGMs.

9.3   Backups of the database must be made daily.

9.4   Backups of the database must be stored off site.

9.5   In the event of a complete system failure, it must be demonstrated that the system can be completely reloaded and started from the point of the last database backup.

9.6   Write access to the database must be monitored and strictly controlled and must be possible by authorised personnel only.

10   Meters and Accountancy Information

10.1   It must not be possible to delete or alter any meters or accountancy information in the monitoring system without the action being detected and logged.

10.2   The monitoring system must automatically detect the event of a meter roll-over (wrap) and be able to automatically calculate the actual meter increment.

10.3   The monitoring system must automatically detect and handle the condition of an EGM RAM clear and be able to calculate the actual meter increment over the event.

10.4   All meters and accountancy information in the monitoring system must be date and time stamped.

10.5   Meters up to 3 months old must be readily available from the CMS for all EGMs, before being archived in long term storage.

11   CMS Event Requirements

Refer to the document titled "OLGR Licensed Operator Event Reporting Requirements" for additional event reporting requirements.

11.1   All events must be logged upon the occurrence of the event with the current date and time.

11.2   All events in a monitoring system (CMS, SC and EGM events) must be stored by the LMO for a period of at least 5 years.

11.3   All events must be stored in the monitoring system with a time and date, device ID/serial number, event sequence number, event code and any extended event data.

11.4   Each source of events in the monitoring system (ie. the CMS, SCs & EGMs) must run its own event sequence number. Ideally, as events are passed up to the CMS, each stage should append a sequence number onto the event.

11.5   The OLGR must be kept up to date at all times with documentation defining all events generated by the monitoring system (excluding EGM generated events). The documentation must define the events and describe precisely when and where they are logged.

11.6   It must not be possible to delete or change any events in the monitoring system without the action being detected and logged.. Note, any loss or corruption of events in a monitoring system may be grounds for immediate withdrawal of approval of the monitoring system.

11.7   Event Types

The system shall support at least the following event types:-

EGM Events.

Refer to the "Local Area Electronic Gaming Machine Communications Protocol (QCOM)" and the "Local Area Electronic Gaming Machine Communications Protocol Site Controller Protocol Operating Procedures" documents for full event details and text requirements for both protocols. Note, EGM events defined as unnumbered events (Refer EGM Protocol) should not appear in the event reports by default (they are not required to be stored by the MS).

SC Events

Refer to the "Local Area Electronic Gaming Machine Communications Protocol Site Controller Protocol Operating Procedures" document for full event details and text requirements. Event codes may be assigned at the discretion of the monitoring system.

CMS Events

The following events are the minimum range of events the CMS must support. This list will not cover all possible CMS events due to the different types and functions the CMSs may have.

"CMS-SC Not Responding"	A connection to a site is lost or terminated.
"CMS-SC Resumed Responding"	A new connection is made to a site.
"CMS-SC Invalid Address" + *Details*	An invalid address was received from a SC the CMS was connecting to.

"CMS-EGM Meter Adjustment" + *Full Details: Meter ID, who, amount*	Logged whenever an EGM meter is adjusted.
"CMS-SC Invalid Program Signature" + *Details*	Logged upon receipt of a SC program signature which the CMS considers to be incorrect.
"CMS-SC Unreasonable Meter increment" + *Details*	The CMS must place reasonable meter increment on all meters it receives from SCs, including progressive meters.
"CMS-EGM Commissioned" + *Details*	Logged whenever an EGM is installed in a site. Alternatively this event may be logged by the SC.
"CMS-EGM Decommissioned" + *Details*	Logged whenever an EGM is removed from a site. Alternatively this event may be logged by the SC.
"CMS-SC Commissioned" + *Details*	Logged whenever a SC is installed in a site.
"CMS-SC Decommissioned" + *Details*	Logged whenever a SC is removed from a site.
"CMS-SC Connect Failed" + *Reason*	Logged for every unsuccessful connection attempt to a SC by the CMS. Eg. busy signal, no answer.

11.8   For auditing purposes, any changes to a site's configuration (eg. game conversions, adding removing EGMs, site open/close times, a change in jackpot parameters, etc.) should result in one or more CMS events with full details.

11.9   Event Reporting

Event reports must be readily available from the MS for all events up to 3 months old.

It is expected that selected event reports over the most recent seven days for a specific average sized venues will not take longer than 30 seconds to generate.

Event reports must be able to be generated over the following selection criteria:-

A date and time period.
A range of event types.
A specific EGM at a venue, or a range of EGMs at a venue, or all EGMs at a venue.
A specific venue or SC, or a range of venues or SCs, or all venues or SCs.

SC Events and host events for the venue must be always included in an event report by default unless they are specifically not requested. This refers to SC generated events and system generated SC Events (Refer "Local Area Electronic Gaming Machine Communications Protocol Site Controller Protocol Operating Procedures"

An event report must be able to be sorted by the following keys in either order:- Date and Time or serial number. When primarily sorting on serial number the report must automatically sort on time as the secondary key.

Event reports must be able to be produced on a display (VDU) or printed or to a file in the following formats :

- ASCII Text
- Microsoft Excel
- PDF (Portable Document Format)

11.10 Event Archiving

Events older than at least three months must be archived onto long term storage media.

Event reports must be able to be easily generated from archives if required. This must take no longer than 2 working days.

11.11 Event Report Format. **Appendix A** Indicates the general format event reports must have.

12 Revision History

Version	Changes	QIR	Who	Release Date	Incept Date
3.1.1	• Updated to new DJAG report document template		JG	11/04/2016	
3.1	• Updated to new DEEDI report document template • QOGR->OLGR		YL	20/08/2010	
3.0	• Added "Continuity of Services" section • Updated document and standards references • Changed formatting		MB	15/03/2005	
2.0	• Removed the section on Jackpot Systems. This is not a separate document • Combined this document with the LMO Event Reporting Requirements document v1.1 • Refer Red-line and strike out text throughout this document for other changes		RLL	13/11/2000	
1.1	• Updated copyright notice in accordance with OLGR policy • Changed Section 10 numbering • Refer Redline and strikeout for other changes		RLL	31/03/1998	
1.0	• Initial Release		RLL	07/10/1997	

Appendix A – General Report Format

<table>
<tr><td>Report Date: dd/mm/yy hh:mm:ss</td><td><u>EGM Event Report for OLGR</u></td><td>Page x of x</td></tr>
</table>

LMO: [Licensed Monitoring Operator Name]   **Events from:** dd/mm/yy hh:mm:ss, **until:** dd/mm/yy hh:mm:ss

Events last received at: dd/mm/yy hh:mm:ss   **EGMs:** [ALL] or [specific EGM serial no. list]   **Event Types:** [ALL] or [specific event code list]

Venue: [ALL] or [Venue ID / Name / City,Town or Shire]   **Sort Priority:** Serial, DateTime

SCID	Serial No.	Date & Time	Sequence	Code	Event	Additional Data
xxxx	xxxxxxxx	dd/mm/yy hh:mm:ss	xxxxx/xxx	xxxx	Event Description	Additional Event Information
xxxx	xxxxxxxx	dd/mm/yy hh:mm:ss	xxxxx/xxx	xxxx	Event Description	Additional Event Information
xxxx	xxxxxxxx	dd/mm/yy hh:mm:ss	xxxxx/xxx	xxxx	Event Description	Additional Event Information
		.			.	.
		.			.	.
		.			.	.

Definitions

Report Date:	The date and time the report was generated.
Sort Priority:	Lists the primary and secondary report sort order.
Events from: until:	The start and end date and time of selected event report.
Events last received at:	The date and time an event report is valid to for this site (ie. the time the venue was last contacted to receive the latest events).
SCID column	The ID number of the Site Controller the EGM is connected to
Serial No.	The EGM manufacturer ID and Serial Number (8 digits)
Date & Time	This column is the date and time of the event
Seq column	This is the event sequence number of the event. Refer OLGR protocol document.
Code column	The event code of the event (4 digit hexadecimal)

NOTES

The report must be for A4 Landscape size pages.

In the SCID and Serial No. columns, if the previous line has the same value, then the entry does not need to be reprinted unless it is the first line of a new page.

Events generated by the EGM must appear in normal text, all other events and system events must appear in bold print.

The first header line must appear on every page of the event report.