Site controller minimum requirements

Version 2.1.1

Queensland Government

© The State of Queensland (Department of Justice and Attorney-General) 2016. Copyright protects this publication. The State of Queensland has no objection to this material being reproduced but asserts its right to be recognised as author of its original material and the right to have its material remain unaltered. Enquiries should be addressed to crown.copyright@qld.gov.au

The information contained herein is subject to change without notice. The copyright owner shall not be liable for technical or other errors or omissions contained herein. The reader/user accepts all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from using this information.

The QCOM specification is the intellectual property of The State of Queensland. In order to implement the QCOM specification or subsequent versions, the necessary licensing arrangements will be required to be entered into.

For further information, please contact the Office of Liquor and Gaming Regulation on 13 QGOV (13 74 68) or visit www.business.qld.gov.au/industry/liquor-gaming

1 Contents

1 Introduction

Purpose

This document defines the minimum technical requirements for Site Controllers in EGM monitoring systems.

Applicability

This document is applicable to LMOs and developers of EGM monitoring systems.

Definitions

“EGM” means Electronic Gaming Machine.

In this document, the term “site” or “venue” means a licensed gaming premise containing EGMs.

The term “Site Controller” (SC) refers to all of the Licensed Monitoring Operators’ (LMO) monitoring system’s on-site hardware (excluding dedicated networking hardware) which monitors and controls the Electronic Gaming Machines (EGMs) and forms a part of basic monitoring service.

Some SCs may consist of more than one discrete device. In this case, each device is considered a part of the overall SC and each device must adhere to these minimum requirements individually.

(If a device that is potentially a SC, is acting only as a communications router with respect to basic monitoring services, then it not required to conform to these requirements. A SC router will generally be deemed acceptable as long as no data can be lost as a result of a failure the device.)

The Site Controller serves the following main functions:

- to monitor and control the EGMs at a site (via the EGM communication protocol) in accordance with QOGR basic monitoring service requirements and procedures.
- to reliably collect and redundantly store (by storing the information in both the EGM and SC) EGM event and metering information en-route to the monitoring system central computer and QOGR.
- to assist controlling value added services to the site. eg. player tracking, performance analysis.

Due to the diversity of Site Controller designs, these requirements are always open for discussion. Exemption of any requirement is at the discretion of the Chief Executive, QOGR.

2 General

2.1 Providing value added services (ie. anything not a part of basic monitoring) in a SC is discouraged except where necessary. A value added service must not be able to degrade or interfere with basic monitoring under any conditions. (eg. slowing or suspending EGM communications while generating a value added service report)

2.2 All SCs must be prominently identified with the following information:-

- LMO name.
- "SITE CONTROLLER".
- A manufacturer assigned serial number.
- Model Number.
- Service contact and details.
- Sealing point/s (eg. an arrow with "SEAL" label) and required seal type (if any).

2.3 A SC must automatically restart after a loss of power without manual intervention.

2.4 SCs must be located in a suitable position in a venue. The general public must not have access to the SC. However, the SC must be located in a convenient position to allow easy access for a seal inspection or maintenance.

2.5 A SC must support all EGM protocols currently in use by the QOGR and on the same port unless directed otherwise by the QOGR.

2.6 A single SC must be able to support a minimum of 32 EGMs and must use the LAN defined and specified in the document "EGM Communications Interface and LAN requirements".

3 Manuals

3.1 SC operating manuals must be supplied to QOGR, the venue and the licensed repairer.

3.2 Operating manuals must clearly describe all operations and procedures relating to the SC.

3.3 SC service/maintenance manuals must be supplied to QOGR and the licensed repairer.

3.4 Service manuals must contain all technical information, and on/off site service/installation procedures and information to the point of return to manufacturer.

3.5 Service manuals must contain procedures which must be undertaken to clear the SC RAM.

3.6 The above manuals must be approved by QOGR. SCs will not be approved unless all SC manuals are considered acceptable by QOGR.

3.7 Current manuals must be lodged with QOGR at all times. Manuals must be thorough and easily interpreted.

4 Electrical

4.1 It is recommended that SCs are able to operate on a 240VAC, +10VAC/-30VAC 50hz mains power supply. (A few sites have been observed to have significant extended power sags down to 215VAC)

4.2 SCs may have to operate in a temperature range of 10-50 degrees Celsius depending where it is located.

4.3 ESD 240VAC power line filters and surge protection are mandatory on all SC equipment.

4.4 The SC should not be adversely affected (ie. damaged or loss of data) by:-

4.4.1 electromagnetic radiation (E.M.R.),

4.4.2 radio frequency interference (R.F.I.), refer IEC 801-3: 1984 "Immunity to Radiated Fields".

4.4.3 mains power fluctuations, including black outs, brown outs, power surges, sags, spikes and notches, refer IEC 801-2: 1991 "Immunity to Electrostatic Discharges", IEC 801-5 "Draft Immunity to Conducted High Energy Pulses" and RS01: Immunity to Magnetic Fields (MIL-STD-461C)

4.4.4 mains transients, refer IEC 801-4: 1988 "Immunity to Electrical Fast Transients"

4.4.5 signals superimposed on mains supply,

4.4.6 extreme temperature variation (refer AS1099),

4.4.7 extreme humidity variation (refer AS1099),

4.4.8 effect from deposits of suspended particles, e.g., dust, cigarette smoke (refer AS1099.3.7),

Also be aware of CISPR 22: 1993/AS3548: 1995 EMC Standard (now mandatory in Australia) and AS3260.

4.5 SCs must have power fail detection, which allows the SC to detect an imminent failure of mains power, execute power down procedures and power down safely. This requirement is to avoid SC NV-RAM corruptions.

4.6 All power and data cables must be routed within a site so they are not easily accessible by the general public.

4.7 SCs must be protected against ESD when applied to its outer case or on any protruding wires. The minimum level of protection is the 15kV "Human Body Model" except where stated otherwise.

4.8 Any device electrically connected to an EGM which is not completely internal to the EGM (ie. it has external to the EGM, ports, wires, displays or components), must provide ESD protection on all external items and on the electrical connection between itself and the EGM.

Any ESD onto a SC or other third party device in this category must not be possible to enter the EGM via power or data communications cables.

5 SC Non-Volatile Storage

5.1 The SC must store all received EGM events, meters, configuration and control variables in a Non-Volatile storage media.

5.2 The SC must have enough non-volatile storage capacity to provide uninterrupted EGM monitoring during normal operation.

5.3 Uninterruptable Power Supplies (UPS) combined with a volatile storage device or magnetic media (eg. hard disks) are not acceptable for NV storage.

Hard disks (and other magnetic media) must not be used to store any NV data directly related to providing basic monitoring or the regulatory return to player. However, software and value-added services may use magnetic media.

5.4 Two examples of acceptable NV storage media is Zero-Power RAM and Battery Backed SRAM. Flash devices are not acceptable because of their limited write cycles.

5.5 Data retention as supported by battery backup or other means as approved by the Executive Director should be sufficient to maintain the current SC information for a period of time not less than 30 days without mains power.

5.6 NV-RAM must have low-battery detection. NV-RAM that has a power-off life of at least ten years is exempt. Eg zero-power RAM does not require low-battery detection.

5.7 If zero-power NV-RAM is used then it must be labelled with a date of manufacture.

5.8 Any new or changed data as a result of a poll to an EGM must be able to be written to NV-RAM within 0.5 seconds. Ie, the write time of the NV-RAM must be significantly less then 0.5 seconds at all times. (Limit is imposed by QCOM poll cycle).

5.9 Write caches must not be used on NV-RAM.

(Good test for NV-RAM: Monitor communications between the EGM & SC. Play a game, as soon as the plays meters are acknowledged by the SC (next poll after meters response), immediately

cut power to SC, power down the EGM, power up the SC and ensure last sent meters were saved on the SC)

5.10 SCs must have a NV Real Time Clock.

5.11 Any single or multiple failure of a component in the SC (such as a CPU, circuit board or hard-drive etc) other than the NV-RAM must not result in a loss or corruption of NV-RAM data.

6 SC Physical Security

6.1 The SC must be a securely housed device able to be secured via regulatory seals. Access to the interior must only be possible by breaking a regulatory seal. Seals currently utilised require a 6mm hole.

(Particular attention must be given to PC based site controllers for this requirement, often easy access can be obtained be removing spare drive bay covers, or by unscrewing the power supply, or removing other panels).

6.2 SCs must have electronic cabinet/door access detection.

6.3 Access of the SC cabinet door shall disable the EGMs under it and cause an automatic erasure of the SC security keys (as applicable).

6.3.1 The SC may not reset from this condition until the event is authorised by the central monitoring system computer.

6.4 Consideration should be given to preventing damage from tampering of exposed ports on a SC (power and communications), by leaving them electrically disconnected if not in use, or capped.

6.5 Bootable removable media drives (eg. Floppy disk drives) are to be electrically disconnected whilst the SC is operational. Bootable drives are only to be connected for maintenance or upgrade purposes. Exception: if the bootable feature can be securely disabled then the drive may remain connected.

7 SC Logical Security and Integrity

7.1 Where information is transferred between microprocessors or sub-systems, there must be error checking on the transferral. This check should be at least a Cyclic Redundancy Check (CRC). Parity checking or check-sums are not adequate.

7.2 SC programs must test themselves during power-up and reset for possible corruption due to failure of the program storage media. Use of Cyclic Redundancy Check (CRC) calculations (32 bit) is a minimum.

Other test methodologies must be of a type acceptable to QOGR.

7.3 During power up, the SC software must be able to detect any change in program from when the device was last powered down. If a change has been detected, the

device must lock-up, displaying an appropriate message until the SC program is authenticated by the host system.

7.4 The SC program must check for corruption of NV-RAM locations used for crucial gaming device functions including, but not limited to:

7.4.1 configuration data,
7.4.2 random number generator outcome (if applicable),
7.4.3 all metering information and any error/EGM states,
7.4.4 critical memory pointers,
7.4.5 the event buffer.

At least every power up these memory areas must be checked for corruption. Detection of any uncorrectable corruption shall be deemed to be a malfunction and must result in a RAM ERROR fault condition.

7.5 All volatile memory must be tested by the SC on power up. Any detected failure must be treated as a critical error.

7.6 There must be **NO** provision for an easily accessible 'RAM reset' button/switch to reset the meters and other areas of electronically stored data. RAM clears of valid data MUST be undertaken by accessing the sealed computer compartment of the device, or via highly secure password or encrypted access.

7.7 Cases of "RAM corruption", which should be infrequent, must only be attended to by licensed technical personnel.

7.8 Provide details of ALL program checks and when they are performed.

7.9 Whenever the SC establishes a connection with a higher level computer (or SC) in the monitoring system, the higher level computer must validate the SC's program via a digital signature or encryption authentication scheme.

7.9.1 This connection/authentication must take place at least once per day.

7.9.2 No data must be permanently accepted by the higher level computer (or SC) from the SC below it, if the SC's program does not authenticate.
7.9.3 All data sent by the SC to a higher level computer must be verified by the higher level computer for integrity and reasonableness. Eg, date and time stamps and meter increments.

7.10 Any failure of the above listed security/integrity requirements will cause the SC to immediately disable the EGMs under it until the problem is addressed.

7.11 All communications ports on a SC, must perform only their intended functions, there must be no undocumented functions or adverse affects on the SC as a result of invalid, corrupt data or tampering.

7.12 It must not be possible to obtain unauthorised access to the SC’s operating system.

7.13 It must not be possible to be able to load unauthorised software to a SC.

7.14 It must not be possible to exit or break out of the SC software into the operating system, or bypass the software altogether without breaking a regulatory seal first. This event must not be able to go undetected by the monitoring system.

8 SC Source Code and Compilation

8.1 SC source code must be submitted to QOGR for evaluation and approval before placing in the field. Exemptions may be granted for SC software (such as; operating systems, BIOS software and database drivers) which is commercially available third party software (ie. third party with respect to the SC software developer).

8.2 The following items must appear in all source code modules:

8.2.1 Module Name
8.2.2 Version Number
8.2.3 Brief description of module function.
8.2.4 Edit History: Who, When, Why.

8.3 All submitted source code must be commented in an informative and useful manner.

8.4 Poorly commented code may seriously impair the software validation process and greatly reduce the degree of confidence in the reliability and integrity of the code.

8.5 It is further expected that all source code submitted is correct, complete and compilable.

8.6 Failure to comply with the above will result in the total rejection of a given submission.

8.7 Submitted source code must be able to be compiled and verified with the SC by QOGR upon request at any time. Failure of the source code to reconcile with a SC will result in either immediate rejection of a submission, or withdrawal of approval for the SC.

9 SC Diagnostic Functions

9.1 All SCs must have built-in diagnostic functions including but not limited to

9.1.1 All input and output ports,

9.1.2 RTC, RAM & ROM

9.1.3 WAN and LAN,

9.1.4 displays and all peripherals.

Display of the diagnostic function results may be via built in displays (even simple LED displays). Exemptions may be given for easily replaceable black box type site controllers.

10 Down-loadable SC Software

Down-loading of program software to SCs is acceptable and encouraged to reduce the cost of software upgrades. However the following requirements must be met:-

10.1 There must be encryption or password protection on the download.

10.2 Downloads must be able to be performed in background so the SC may continue normal operations at all times.

10.3 There must be no loss of data in the monitoring system when switching over SC programs. It is acceptable to temporarily disable EGMs and cease monitoring for the switch over.

10.4 EGM to SC communications logger

(This requirement is optional, but is recommended as it could help LMOs remotely diagnose communications problems)

This is the ability for the SC to log EGM to SC protocol traffic for a specific EGM when requested to a file on demand and be able to later send the log file to the host system computer for diagnostic purposes. Ideally, once logging is enabled it should log the last 10 minutes (~40K bytes) worth of traffic until told to stop. The ability to also stop logging upon the occurrence of a specific EGM/SC event is also useful.

11 Status Displays

11.1 The SC will have at least the following labelled status indicators visible from the exterior of the sealed SC cabinet.

11.1.1 Power good indication. Labelled “POWER”

11.1.2 Software heart-beat indication.

11.1.3 A SC general fault/error indicator. Labelled “FAULT”

12 PC-Based Site Controllers

PC-based SCs are acceptable provided they meet the following requirements:-

12.1 PC-based SCs must not be able to be used for any purpose other than the control of gaming equipment and providing gaming value added services.

12.2 Access to BIOS setup must be password protected. The password must only be available to authorised personnel.

12.3 A failure of a CMOS backup battery must not allow access to the system or software or allow a removable media device to become bootable. If this is a

possibility, then the SC must be able to detect and report a CMOS backup battery failure to the host and disable until the problem is fixed.

13 SC Software Testing Environment Requirements

13.1 SC testing may be carried out at QOGR or other approved premises.

13.2 SCs and manuals must be submitted for evaluation and approval to QOGR only once they have completed and passed the monitoring system providers own test procedures.

13.3 Provide a complete list of all SC generated events and descriptions.

13.4 A test bed must be provided by the LMO which consists of the following:-

13.4.1 Two PCs, each connected to the SC which will run QOGR EGM protocol emulation software.

13.4.2 Two or more QOGR approved EGMs running the QOGR EGM protocol. The EGMs & SC must be connected as per an actual site installation (this is a part of the evaluation).

13.4.3 An on-line WAN connection to the site controller running the actual monitoring system WAN protocol. This must be the actual monitoring system itself. It is noted that some monitoring systems are dial-up connection systems, however they must be able to operate in an on-line mode for test purposes.

A host terminal must be provided and located in the same room as the SC under test.

13.4.4 The ability to quickly and easily generate/receive all reports from the central system. *

13.4.5 The ability to quickly and easily configure the site and system. *

* The LMO must make readily available the necessary monitoring system operator personnel for the duration of the evaluation.

13.4.6 An on-line display of a selected EGM's or SC's current meters, events and status.

13.5 It is acknowledged that the SC may provide the host system with many different types of EGM auditing information (eg. mtd meters, ytd meters, etc.). QOGR will only be testing the fundamental meters from the EGM (as all required regulatory reports and auditing information can be derived from these meters). A definition of the fundamental EGM meters is contained in the QOGR SC operating procedures document.

14 Revision History

Version	Changes	QIR	Who	Release Date	Incept Date
2.1.1	Updated to JAG report template	NA	JG	31/5/16	
2.1	Updated to DEEDI report template	NA	RLL	20/8/2010	
2.0	• Coverted to Word • General Review • Added requirements for the labelling of SCs. • Added requirements regarding acceptable locations for SCs in venues. • Clarified requirements regarding use of NVRAM in SCs. • Other changes as indicated.		RLL	23/6/2003	
1.2			RLL	15/10/1997	
1.1			RLL	3/10/1997	
1.0	First draft		RLL	10/9/1997	