Site Controller Minimum Technical Requirements

Version 3.0

Queensland Government

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

1 Contents

2 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.

"EMS" means Electronic Monitoring System.

"LMO" means Licensed Monitoring Operator

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 with the device.)

The Site Controller is considered to perform the following primary functions:

- Monitor and control the EGMs at a gaming venue in accordance with OLGR's monitoring requirements and procedures.
- Reliably collect and store EGM event and metering information until successful transmission to the monitoring system central computer.
- Help manage or control gaming related value added services at the gaming venue e.g. player tracking, performance analysis.

3 General

3.1 SC's must not be used for any purpose other than the monitoring and control of gaming equipment and providing gaming related value added services.

3.2 Any value added service must not be able to degrade or interfere with basic monitoring under any conditions.

3.3 All SC's must be prominently identified with the following information:

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

3.4 A SC must automatically restart operations after a loss of power without the need for manual intervention.

3.5 SC's must be located in a suitable position in a venue. The general public must not have easy access to any SC. However SCs must be located in a convenient position to allow easy access for tamper seal inspections or maintenance by authorised persons.

3.6 A SC must support all OLGR mandated EGM protocols and interface specifications.

3.7 SC's must utilise the required EGM LAN as specified in other OLGR requirements documents.

3.8 The SC must have at least the following labelled status indicators visible from the exterior of the sealed SC cabinet:

- A power good indicator.

3.9 If it is intended that the SC also triggers prizes that are a gaming tax deduction; then be advised the SC is considered a gaming machine and all applicable technical requirements will apply. Contact the OLGR for more information in this case and for a list of additional applicable requirements documents.

4 Electrical

4.1 SCs must be able to operate on a **240VAC, 50 Hz** mains power supply. *It is recommended that SCs are able to continue operating where the power may fluctuate in the range +10VAC / -30VAC (uncalibrated).*

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

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

4.4 The SC's associated power and data cables must be located within a gaming venue so they are not easily accessible by the general public.

5 SC Non-Volatile Storage

5.1 The SC must store all received EGM events, meters, configuration and control variables in Non-Volatile storage medium or memory (NV-RAM).

5.2 It must be demonstrated that the SC has enough NV-RAM capacity to provide basic EGM monitoring[i] for at least **72 hours** of being offline from the EMS central host without running low on NV-RAM.

5.3 Acceptable types of SC NV storage are: Zero-Power RAM, battery-backed RAM, and SSD (Solid State Drive) and hard drive based devices under certain conditions*.

* Conditions of use regarding SSDs and hard drives:

1. The drive must be capable of operating in a SC without replacement for a minimum of **10 years** under expected operating conditions.

2. The drive controller must incorporate wear levelling and automatic management of bad blocks and sectors.

3. The SC must be able to detect and report on any drive that is nearing end-of-life and gracefully disable SC operation before new data can no longer be written to the device.

4. The file system on drive devices must be suitable for use and partitioned appropriately. (For example SSD based SCs refer: https://en.wikipedia.org/wiki/Solid-state_drive#Suitable_file_systems)

5. The SC must able to automatically recover from unexpected power losses without loss or corruption of data. Related s5.9.

6. Copies of data must be maintained on at least **two** separate drives. Updates to each drive must be performed independently such that no single operation, even if influenced by a single component failure, will result in data loss or corruption of both sources or prevent the updates to the other devices from completing.[ii]

7. The drives must have a higher than average mean time between failure (MTBF) rate in comparison with a wide range of drives of the same

[i] Assume normal operation of the gaming venue, the maximum number EGMs the SC can support, no value added services that require an on-line WAN (e.g. WAN linked progressive jackpots), and daily machine clearances and overnight power downs.

[ii] Be wary of RAID solutions, as many third party RAID implementations also require a UPS and orderly shutdowns to avoid major issues and loss of data.

technology.

5.4 NV data retention supported by battery backup or similar means must be sufficient to maintain the current SC information for at least **30 days** without mains power.

5.5 If battery-backed NV-RAM is used, the SC must have low-battery detection. NV-RAM that has a power-off lifetime of at least **10 years** is exempt, e.g. typically zero-power RAM does not require low-battery detection.

5.6 If battery-backed or zero-power NV-RAM is used then batteries must be labelled with a year of manufacture.

5.7 For SCs supporting QCOM v1.x; any new or changed data as a result of EGM monitoring and control needing to be stored in VR-RAM, must be able to be saved to NV-RAM within a period of **half** the QCOM v1.x poll cycle rate used by the SC.

With respect to other EGM interfacing protocols the SC may implement; the general requirement is that the SC must successfully write received data to NV-RAM before sending back an acknowledgement for that data. (Related: section 5.9 below.)

5.8 Write caches must not be used on NV-RAM unless the write cache is also suitable NV-RAM under these requirements.

5.9 Any updates to NV-RAM must be transactional and/or consist of multiple states such that a sudden reset or power loss will not cause the loss or corruption of any data, including data currently being written.

5.10 SCs must incorporate a NV Real Time Clock which it must use to maintain the correct time across power outages.

6 SC Physical Security

6.1 The SC must be able to be secured via physical tamper seals and be secured as such during operation at all times.

6.2 Access to the interior of the SC must only be possible by breaking at least one tamper seal or by causing obvious permanent external damage.

(Particular consideration must be given to PC based SC's in relation to this requirement as often access without seal break can be obtained via pop-off covers in relation to spare drive bay covers, or by unscrewing the power supply, or the removal of other panels).

6.3 SCs housing must have electronic cabinet/door access detection.

6.4 Accessing the SC housing door shall disable the EGMs under it and cause an automatic erasure of the SC security keys (as applicable).

The SC may not reset from the condition above until the event is acknowledged and authorised by the central monitoring system computer or authorised person.

7 SC Logical Security and Integrity

7.1 SC must verify its application software once per restart (before commencing EGM monitoring operations) for possible corruption due to failure of the program storage media. A SHA1 or better algorithm must be used.

7.2 Whenever the SC establishes a connection with a higher level computer (or SC) in the monitoring system, two-way authentication must take place (E.g. TLS protocol or similar must be used).

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

ii) No EGM related data must be accepted by the higher level computer (or SC) from the SC below it, if the authentication failed.

iii) All data sent by the SC to a higher level computer in the EMS must be sanity checked by the higher level computer in a similar fashion in which a SC sanity checks all data received from the EGMs it monitors. (Particularly with respect to date and time stamps and meters.) Suspect data must be logged as an event and dealt with in an appropriate manner to help ensure that invalid data is never propagated or treated as valid.

7.3 It must not be possible to obtain unauthorised access to the SC's operating system, internal drives, data or databases without breaking a tamper seal.

7.4 It must not be possible to force a SC to boot from any externally accessible drives or ports without first breaking a tamper seal.

7.5 If the SC has a BIOS or similar program, then:

7.5.1 Access to BIOS setup must be password protected or better. The password must only be available to authorised personnel.

7.5.2 BIOS settings and data must be stored in flash memory or similar. Battery backed NV memory types for BIOS data are not acceptable.

8 SC Source Code and Compilation

8.1 SC source code must be submitted to OLGR for evaluation and approval. Exemptions may be granted for SC software (such as operating systems, BIOS software and database drivers) which is commercially available third party software (i.e. third party with respect to the SC software developer). For more information refer to the OLGR submission requirements document.

9 SC Diagnostic Functions

A wide range of remotely accessible SC diagnostic functions is recommended. This section lists mandatory SC diagnostic functions.

9.1 EGM to SC communications logger – QCOM v1.x only.

This is the ability for the SC to log EGM to SC raw 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.

10 Downloadable SC Software

10.1 SC support for remote software upgrades via the EMS central host is mandatory.

10.2 The methodology utilised must be secure and authenticated.

10.3 Downloads must be able to be performed in the background so that the SC may continue normal operation.

10.4 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.

10.5 Whenever the SC connects to the host, or at least once a day, the EMS host must verify that the SC software version is correct.

11 Revision History

Version	Changes	QIR	Who	Release Date	Incept Date
3.0 *edocs # 1645216*	Minor type fix and clarification s5.7 & 5.9.	NA	RL	6 Jan 2017	RD+1 year
3.0-draft *(for industry review)*	- Updated to DJAG template. - Added new SSD storage requirements. - Major review and cull of outdated requirements. (The last review was 2003)	NA	JA / RL	23 Nov 2016	
2.1	Updated to DEEDI report template	NA	RLL	20/8/2010	
2.0	Converted 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 NV-RAM 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	