**STANDARDS**

---

*Made under Section 7(2)(h) and Section 86B(2) of The Gaming Act, Cap. 41*

---

# THE GAMING EQUIPMENT STANDARDS – SMART INTERFACE FOR GAMING MACHINES, 2019

---

## ARRANGEMENT OF STANDARDS

14. Random access memory (RAM)
15. Critical memory requirements
16. Program memory storage requirements
17. Programmable logical elements
18. Circuit boards
19. Switches and jumpers
20. Communication
21. Video monitors and touch screens
22. Global Positioning System (GPS)
23. Printers (if applicable)

PART V

SOFTWARE REQUIREMENTS

24. Source code
25. Critical memory requirements
26. Program memory storage
27. Random number selection process
28. Information display
29. Prescribed display formats
30. Data communication
31. Metering – Audit meters and displays
32. Metering – Player displays
33. Metering – Labelling

PART VI

OPERATIONAL REQUIREMENTS

34. Access to restricted features
35. Set-up – Device configuration
36. System security
37. Master reset
38. Door open procedures
39. Door close procedures

# PART I

# PRELIMINARY PROVISIONS

## 1. Citation

These Standards may be cited as **The Gaming Equipment Standards – Smart Interface for Gaming Machine, 2019**.

## 2. Scope

These standards specify the general hardware and software requirements and the list of significant events required by the Gaming Board of Tanzania (GBT) for gaming machines.

GBT requires that this equipment be attached to a Gaming Regulatory Electronic Monitoring system (GREMS), and therefore the *The Gaming Equipment Standards – Central Electronic Monitoring System, 2018* and *The Gaming Equipment Standards – Gaming Devices for Route Operations, 2018* are also applicable.

## 3. Interpretation

In these Standards, unless inconsistent with the context, the words and expressions used have the meanings assigned to them in the Gaming Act, 2003 ("the Act") and the Gaming Regulations ("the Regulations") made under the Act, and:

"approved" means approved by GBT;

"bet" or "wager" means amount of coins or credits put at risk at the beginning of a game or during a game;

"cash" means coins, banknotes, tokens, magnetic or smart cards or any other legal representation of money in the gaming environment;

"cashout" means action initiated by a player when redeeming available credits from a gaming machine (GMs), whether the GM pays credits from the hopper, by electronic transaction or by issuing a ticket;

"certification authority" means authority appointed by GBT to certify all gaming devices, both hardware and software;

"critical data" means data contained in critical memory and refers to:

(1) all metering required by these Standards;

(2) SIGMa configuration data (or both);

(3) data held on SIGMa collected from the gaming device but have not sent to the GREMS server;

(4) software state (the last normal state the SIGMa software was in before interruption); and

(5) information regarding any significant events;

"critical memory" means memory locations for storing critical data;

"electronic funds transfer" means advanced funds transfer system whereby credits are transferred to or from a GM by any means other than coins, tokens or banknotes;

"equipment" means any hardware, software, firmware, flashware or any combination in whole or in part of these intended for use in gaming;

"error event" means set of operational conditions for a SIGMa that constitutes a deviation from the normal conditions or the conditions specified during a game, during idle mode or during data interchange with another SIGMa;

"feature" means activity within a game triggered by an outcome within that game. Any additional free game, free spin of certain reels, or secondary choice necessary to complete a game is considered a feature;

"game" means combination of events, including player interaction with the GM, that determine what prize may eventually be won from an amount staked or bet by the player. The game begins when the player:

(1) makes a bet from the player's credit meter that is not part of any previous game; or

(2) inserts one or more coins or any form of wager and game play is initiated.

The game is considered completed when the player:

(1) cannot continue play activity without committing additional credits from the credit meter or CAD; and

(2) has no credits at risk.

The following elements are all considered to form part of a single game, in other words, the game is not considered to have been completed until all the "elements" have been completed:

(1) games that trigger a free game feature and any subsequent free games;

(2) features occurring or triggered in a single game;

(3) "second screen" bonus feature(s);

(4) games with player choice (for example, draw poker or blackjack);

(5) games where the rules permit wagering of additional credits, for example, blackjack insurance or the second part of a two-part keno game; and

(6) game feature (for example, double-up).

The game is not considered to be completed until all the appropriate meters for the game have been updated.

"game feature" means a feature within a game that is only entered following a win, and which involves the risking of all or part of the result of that win. Game feature bets may incorporate a variety of symbols, player choices, or win chances;

"gaming device" or "GD" means any device manufactured with the intention of being used for gaming purposes, including the monitoring and control system, GDs, GMs, SIGMa, host, data controller unit, bank controller or any combination of these, including software;

"gaming machine" or "slot machine" or "GM" means a machine with which the player interacts for the purpose of gaming in processing gaming transactions, including the monitoring and control system, host, data controller unit, bank controller or any combination of these, including software such as casino tables, slot machines, lottery terminals, point of sale devices and any other such system that GBT will deem to be a gaming machine;

"gaming public" means persons or players who engage in gaming activities;

"host" means central computer(s) of a monitoring and control system on which the software is loaded, and that is (are) certified by the CA;

"idle mode" means state in which a SIGMa is powered up, but is not active in the execution of a test routine, an audit, a calibration, or a data interchange with GM or an external device;

"legislation" means the Act and any Regulations or Rules made in terms of such Act;

"licensed premises" means any premises licensed in terms of the regulation 19 and 20 of the Gaming Regulations, 2003;

"logic area" means secure enclosure area that houses electronic components that have the potential to influence the operation of the host, the data controller unit, the bank controller. GD, GM or the SIGMa;

"master reset" means intentional memory clear of the random access memory (RAM) and other volatile memory of a SIGMa;

"memory" means locations within the GD, GM or SIGMa for storing electronic data, and the data stored therein;

"period meter" or "soft meter" means a meter implemented in software. These meters are used to record meter values since a given event (e.g. coins and bills in since the last clearance);

"Regulations" means Gaming Regulations made under the Act, as amended from time to time;

"reprogrammable memory device" means type of on-chip memory storage device;

"significant event" means set of operational conditions to be recorded by the monitoring and control system for GDs during a game, during idle mode or during data interchange with another GD;

"smart interface for gaming machines" or "SIGMa" or "site data logger" means on-site or intermediate data collector for a monitoring and control system includes data collection units contained within, attached to or as part of GD, with a purpose of collecting transactional and regulatory information from gaming machines (GM) and send them to GREMS server as by specification set by the *GREMS Tractions Posting API Document*. The information sent includes, but not limited to:

(1) all transactions performed by the gaming machine, ie. every stake or spin and payout or winnings;

(2) all significant events specified in the applicable standards;

(3) signatures from the GM's software; and

(4) GPS coordinates of the GM and/or the SIGMa;

"stake" means total monetary value of all bets or wagers put at risk to play a single game;

"test laboratory" or "TL" means an approved laboratory whose test results are accepted by GBT;

"token" means circular elements with an indicated monetary value that might be put into GM;

"turnover" or "handle" means monetary value of the total of all cash or credits (or both) staked on game play;

"win" or "award" or "prize" means number of credits or monetary value awarded to the player as a result of a winning combination or combinations at the end of a single play within a game;

"winning combination" means one or more winning patterns that result in credits being added to:

(1) the total win meter; and

(2) the win display;

"winning pattern" means set of symbols that participates in a winning combination (including substitution);

"winnings" means monetary value of the total of all coin or credits added to the total win meter and the win display during a game, as a result of any game outcome according to the game rules, resulting in credits being added to the total win meter and to the win display. A GM might display this value in credits or monetary value.

## 4. Abbreviations

| | |
|---|---|
| a.c. | alternating current |
| API | Application Programming Interface |
| AM | Amplitude Modulation |
| CA | certification authority |
| CAD | coin acceptance device |
| CAS | coin acceptance system |
| CDD | coin dispensing device |
| GREMS | gaming regulatory electronic monitoring system |
| CPU | central processing unit |
| CRC | cyclic redundancy check |
| EDC | error detection and correction |
| EFT | electronic funds transfer |
| EMC | electromagnetic compatibility |

| | |
|---|---|
| EMI | electromagnetic interference |
| EPROM | erasable programmable read-only memory |
| SIGMa | Smart Interface for Gaming Machines |
| GBT | Gaming Board of Tanzania |
| GD | gaming device |
| GM | gaming machine |
| GPS | Global Positioning System |
| I/O | input/output |
| ITE | information technology equipment |
| km | kilometers |
| LAN | Local Area Network |
| OE | Original equipment |
| MAC | media access control |
| PCB | printed circuit board |
| PLD | programmable logic device |
| RAM | random access memory |
| RNG | random number generator |
| RTP | return to player |
| TL | test laboratory |
| WORM | write-once read-many |

PART II

GENERAL REQUIREMENTS

## 5. Documentation

(1) Each SIGMa model shall have readily available and pertinent operating and service manuals.

(2) The operating manual shall accurately depict the use of the SIGMa in its operating environment, and shall provide sufficient detail and be sufficiently clear in its wording and diagrams to enable the relevant personnel to understand the manual with minimal guidance.

(3) The service manual shall accurately depict the SIGMa that it is intended to cover, and shall provide sufficient detail and be sufficiently clear in its wording and diagrams to enable a competent person to perform repair and maintenance in a way that is conducive to the long-term reliability of the SIGMa.

(4) Software documentation shall include an edit history providing details of all changes to code (what, why, who and when).

## 6. Enclosure construction

(1) The enclosure shall be of a sturdy construction with a locking system that resists the kind of unauthorized entry that the SIGMa is likely to be subjected to in a gaming venue. The enclosure shall be so designed to protect internal components from any external abuse to which the SIGMa is likely to be subjected in a gaming venue.

(2) Exterior of the enclosure that are accessible to patrons and staff shall be so constructed and so finished as not to create a safety hazard or create a risk of injury.

(3) All protuberances (for example, buttons and handles) on the enclosure that are accessible to patrons or staff, and all attachments to the enclosure (for example, labels and identification plates) shall be sufficiently robust to prevent their unauthorized removal.

(4) Spilled liquid shall not be able to enter the logic area, the power supplies, or areas that contain wiring of voltage exceeding 32 V DC.

(5) Enclosure pins or screws, if used, shall not be able to be removed without leaving evidence of tampering, by sealing it with lead, wax or any other such material.

(6) The material of the enclosure shall be made of impact-resistant material;

**7. Enclosure identification**

(1) The SIGMa shall have an identification badge that bears the following information permanently affixed to the exterior of the enclosure by the manufacturer in a position that allows it to be read easily after the equipment has been installed:

(a) the name of the manufacturer;

(b) the date of manufacture.

(c) a unique serial number;

(d) IMIE number; and

(e) MAC address(es).

(2) The serial number shall be marked or affixed in a permanent manner onto the exterior of the SIGMa enclosure in a position that allows it to be read easily after the equipment has been installed.

(3) All LED indicators or input device attached to the enclosure shall be cleared labelled or otherwise identified in the SIGMa manual, either according to its function. Any colour indicators shall be clearly described in the SIGMa manual. The SIGMa manual will contain a clear description of all indicators or key functions.

**8. Enclosure security**

(1) A SIGMa shall be stored within one or more secure areas of the GM. Unauthorized access to a secure area by physical means shall be detectable.

(2) A secure area shall resist forced entry and shall retain evidence of attempts at such entry.

(3) Access to a locked area "A" shall not be possible from another locked area "B" without the use of a key or other secure access device for locked area "A".

**9. Access detection systems**

(1) All access points shall have access detection sensors.

(2) The enclosure shall be fitted with anti-tampering sensor, which detects tampering and triggers a type 4 significant event and disable the GM operation. This

tampering detection should occur whether SIGMs is switched on or off, or whether the SIGMa is on-line or off-line. It shall remain able to detect this event with the mains power off for at least 24 hours. This event shall be reported once the mains power is restored, or the SIGMa is back on line (or both).

(3) The tampering detection system shall be secure against attempts to disable it or to interfere with its normal mode of operation. Cable runs and mountings for the logic area access sensors shall be securely protected.

(4) It shall not be possible to create a false tempering alarm.

(5) The SIGMa shall deactivate game play of GM upon the opening of a SIGMa enclosure but may immediately reactivate when the SIGMa enclosure is closed.

**10. Logic areas**

(1) The following are the items of electronic componentry that shall be housed in one or more logic areas:

(a) central processing units (CPUs) and other electronic components involved in the operation and components housing the system firmware program storage media);

(b) communication controller electronics and components housing the communication program storage media; and

(c) all reprogrammable memory devices that affect the function of the SIGMa.

(2) Communication, input/output (I/O) and display interfaces that do not significantly influence the operation of the SIGMa may be excluded from the logic area.

(3) Logic areas shall be fitted with access detection systems that shall enable the software and the system to detect whether the logic area is open or closed, regardless of whether the mains power is switched on or off, or whether the SIGMa is on-line or off-line. It shall remain able to detect this event with the mains power off for at least 24 hours.

(4) If the logic area is opened more than once while the SIGMa is off-line or powered off, the SIGMa shall, for the purposes of event reporting, treat this as a single entry.

(5) There shall be a facility for storing a logic area open event for at least 14 days.

(6) Provision shall be made on the logic area such that a physical seal can be fitted which would be broken if the logic area was accessed.

(7) It shall not be possible (without a detailed technical knowledge of the SIGMa) to reset the logic area open state (without detection) when the logic area is open (for example, the access detection system shall not be able to be tampered with or replaced without leaving evidence that this has occurred).

(8) It shall not be possible to insert a device into the logic area that can disable the door open sensor of the logic area when the door is shut without such act being detected or leaving evidence of tampering.

(9) If the logic area consists of a circuit board with no door as such, as the entire board can be removed and accessed, the security requirements for the logic doors extend to logic units (i.e. removal of the circuit board is equivalent to opening the door).

(10) It shall not be possible to reset the logic area door open state, by either hardware or software means, if the logic door is still open.

(11) It shall not be possible to access the data bus, address bus, or control lines of any of the circuit boards without gaining access to a logic area.

## PART III

## ELECTRICAL REQUIREMENTS

### 11. Enclosure wiring

All connectors and wires shall be easily identifiable, both in the SIGMa itself and on the circuit diagrams in the manuals.

### 12. Electromagnetic interference

(1) Electromagnetic interference

The SIGMa shall comply with the requirements for ITE equipment on radio disturbance characteristics. This requirement is subject to the requirements of the TCRA relating to emissions causing interference with other electronic communications equipment.

(2) Electromagnetic immunity:

When the SIGMa is tested in electromagnetic immunity at severity level 2, at an electric field strength of 3 V/m, and over the frequency range 80 MHz to 1,0 GHz with 80% AM modulation at 1 kHz, it shall not divert from normal operation by the application of electromagnetic interference (EMI).

(3) Magnetic immunity

(a) Immunity to alternating magnetic field at mains frequency: A SIGMa shall not have its security properties changed by the application of a magnetic interference level to the SIGMa. When tested the SIGMa shall withstand a magnetic field that alternates at 50 Hz or 60 Hz and that have amplitude of 1 A/m. The SIGMa shall exhibit a capacity to recover or reset and complete any interrupted play without loss or corruption of any control or data information associated with the SIGMa.

(b) Immunity to impulse magnetic field: A SIGMa shall not have its security properties changed by the application of a magnetic interference level to the SIGMa. The SIGMa shall withstand an impulse magnetic field strength of 100 A/m (peak) and shall exhibit a capacity to recover or reset and complete any interrupted play without loss or corruption of any control or data information associated with the SIGMa.

(4) Temporary electrostatic disruption

When the SIGMa is tested at a level of 8 kV for air discharge and 4 kV for contact discharge, it shall exhibit a capacity to recover or reset and complete any interrupted play without loss or corruption of any control or data information associated with the SIGMa.

(5) Fast transient voltage

(a) The SIGMa shall employ sufficient power supply filtering to prevent disruption to the device when the SIGMa is tested with the application of the following fast transient voltages (rise time: 5 ns, duration: 50 ns):

(i) to the a.c. power lines of the power supply: 0,5 kV; and

(ii) to the I/O lines: 0,5 kV.

(b) The SIGMa shall exhibit a capacity to recover or reset and complete any interrupted play without loss or corruption of any control or data information associated with the SIGMa.

(6) Surge voltage

The SIGMa shall employ sufficient power supply filtering to prevent disruption. When a surge voltage (rise time: 1,2 µs, duration: 50 µs) of 1 kV is applied to the a.c. power lines of the power supply and 2 kV is applied to earth, the SIGMa shall exhibit a capacity to recover or reset and complete any interrupted play without loss or corruption of any control or data information associated with the SIGMa.

(7) Long-term voltage level change

When a SIGMa is operating at its rated voltage, and the voltage is changed to 253 V for 15 min, and 207 V for 15 min before being returned to the rated voltage, the SIGMa shall show the capacity to recover or reset and to complete any interrupted play without loss or corruption of any control or data information associated with the SIGMa. There may be a break between the two periods of abnormal operation.

This requirement is to demonstrate the ability of the SIGMa to operate normally during voltage changes within the tolerances with which utility companies are required to comply (typically 10% above and 10% below the nominal 230V).

(8) Surges and sags of voltage

When the voltage supply to the SIGMa is varied in accordance with the following procedures, the SIGMa shall exhibit a capacity to recover, or to reset, and to complete any data collection or transmission without loss or corruption of any control or data information associated with the SIGMa, or any damage to the equipment:

(a) connect the SIGMa to a variable voltage power supply. Set the supply voltage to the rated value. Operate the gaming equipment for 15 min;

(b) increase the supply voltage rapidly (i.e. within 0.5 s) to 1.20 times the rated voltage, maintain for 5 seconds and return rapidly to the rated voltage; and

(c) reduce the supply voltage rapidly to 0.80 times the rated value, maintain for 5 seconds and return rapidly to the rated voltage.

This requirement is to demonstrate that the SIGMa has sufficient power supply filtering to prevent disruption to the device in the event of surges or sags in the mains supply of 20% above and 20% below the nominal supply voltage.

**13. Power supply**

(1) All ratings of fuses shall be clearly stated on or near the fuse holder, and switches on the power supply shall clearly indicate in a permanent manner the "on" and "off" positions.

(2) The SIGMa shall be able to operate from a 220VAC, 50Hz main power source, which might deviate 10% above and below nominal voltage and 1% above and below nominal frequency.

(3) Where a SIGMa enclosure contains more than one power switch, each switch shall be so marked in a permanent manner to indicate clearly to which board or component it applies.

## PART IV

## COMPUTER AND PERIPHERAL HARDWARE REQUIREMENTS

### 14. Hardware features

(1) The SIGMa should have a 32-bit microcontroller that is capable to generate a 1024-bit digital signature for each XML sent to the GREMS in real-time basis, of which all fuses are locked with no possibility of internal memory read-back.

(2) The SIGMa should be a stand-alone embedded device that does not require any additional peripheral device/hardware to operate, such as computer, server, monitor, keyboard, etc.

(3) It should be of a size that can fit inside a GM (preferably in the logical area) without causing any environmental, mechanical and electrical harm to the GM.

(4) The SIGMa should bind/pair with the specific GM at hardware level in such a manner that, the SIGMa can only be connected to that GM unless approved by the GBT.

(5) It should use solid-state memory technology to ensure reliability, durability and to facilitate fast boot-up and access of software and data.

(6) SIGMa should be able to start without manual intervention or switching of a person after return of power in the event of an outage.

### 15. Random access memory (RAM)

(1) SIGMa RAM data storage shall be capable of reliably preserving its memory contents for at least 14 days with the mains power switched off.

(2) When the battery is at or below its 14 days capacity limit, the SIGMa shall automatically generate a type 4 significant event message to the monitoring and control system and disable the GM. It shall not be possible to reset the SIGMa until the battery capacity has increased above the 14 days capacity limit, either by recharging or replacement of the battery. If a rechargeable battery is used, the power source shall be capable of recharging the battery to its full capacity within 24 hour.

(3) RAM clears of the SIGMa shall not be possible except by accessing the logic area.

(4) In a SIGMa, batteries shall be secured and connected to the circuit boards that contain RAM such that the batteries cannot be easily disconnected.

**16. Critical memory requirements**

(1) Manufacturers shall ensure that critical data are recorded in at least two physically separate and distinct hardware devices (which may be of the same type), either within the SIGMa or the local data logger (or both). This critical data record shall be retained on these devices until such time that at least the following data have been successfully transmitted to GREMS server:

(a) all auditing meters;

(b) current credits;

(c) GPS coordinates of the location of SIGMa;

(d) SIGMa or GM configuration data (for example, GM address, denomination); and

(e) significant event information.

(2) These devices shall be capable of being reliably updated at every critical memory change.

(3) The SIGMa should have a nonvolatile memory to store data received from the gaming machine for at least 72 hours, when there is a failure of a communication link between the SIGMa and the next point in the monitoring system.

**17. Program memory storage requirements**

(1) All ROMs (for example, EPROMs, CD-ROMs and PLDs) shall be clearly marked to identify the software and the revision level of the information stored in the devices.

(2) All EPROMs (and PLDs that have erasure windows) shall be fitted with covers over their erasure windows.

(3) EPROMs that contain any settings or programs that have the potential to cause the SIGMa to fail to comply with these Standards or with legislation shall not be contained within the SIGMa. This includes EPROMs that have a range of parameters that are used for setting up the device.

## 18. Programmable logical elements

All programmable logic elements that incorporate read-inhibit fuses shall be programmed to prevent unauthorized reading or copying of these elements.

## 19. Circuit boards

Patch wires and track cuts may be present, but shall be documented in the service manual in an appropriate manner.

## 20. Switches and jumpers

(1) If switches or jumpers that have the potential to cause the SIGMa not to comply with these Standards, or with legislation, are present, then setting them in a manner that would result in non-compliance shall cause the SIGMa to enter "Tilt" mode, which in turn shall be signalled to the GREMS. As long as the switch or jumper is set in this manner, it shall not be possible to reset the SIGMa.

(2) All switches and jumpers that have the potential to affect the communications or operational characteristics of the SIGMa shall be documented for evaluation by the test laboratory (TL).

## 21. Communication

(1) Where multiple SIGMas communicate over a single multi-drop transmission medium, each SIGMa shall operate at an accurate and consistent baud rate, which shall ensure consistently accurate and error free communication (over and above the error checking and correction requirement).

(2) SIGMa communication interfaces shall not present a hazard.

(3) Ports for communication cabling shall be clearly and permanently labelled according to their function.

(4) Ports for communication cabling (other than external ports used exclusively for auditing) shall be located within a secure area to prevent unauthorized access to the ports and to the attached cables.

(5) The connection or interaction of a SIGMa with a GREMS shall not affect the function of the SIGMa or affect the game in any way, other than to:

(a) disable the SIGMa or game under the appropriate, approved circumstances, for example, when off-line to the next point in the monitoring and control system; and

(b) introduce small delays (unperceivable to the player) in the duration of the game to facilitate communication with the monitoring and control system.

**22. Video monitors and touch screens**

Where fitted, video or LCD monitors shall not present a hazard.

**23. Global Positioning System (GPS)**

(1) There shall be a GPS device attached or in-built into the SIGMa that will monitor it's location.

(2) The GPS coordinates shall be of accuracy of not more than 10 meters.

(3) External antennas may be placed to increase the accuracy of the GPS coordinates.

(4) During registration or installation of SIGMa, the GPS coordinated of the licensed premise hosting the GM will be recorded.

(5) Any change of GM's licensed premise will require GBT to reconfigure the SIGMa accordingly, after obtaining necessary approvals from GBT.

(6) The GPS device will send location coordinates to GREMS on following conditions:

(a) When the SIGMa has been powered on;

(b) Whenever the SIGMa is outside the radius of 1km from the GPS coordinates of the GM's designated licensed premise that was configured in the SIGMa. SIGMa should send type 3 significant event to the GREMS;

(c) When there is a time lapse of not more than 30 days since it's last sent GPS location to GREMS;

**24. Printers (if applicable)**

(1) If a SIGMa is equipped with a printer, the printer shall be located in a secure area other than the logic area.

(2) The printer paper shall be easily replaced without any need to access the logic area of the SIGMa. Instructions for the loading of printer paper shall be given in the operating manual.

(3) The software shall register and react to any printer fault conditions and shall allow the machine to complete the printing of the current job and then pause printing and display appropriate on-screen messages.

PART V

SOFTWARE REQUIREMENTS

## 25. Source code

(1) General

(a) SIGMa should be installed with own embedded system software with no commercial licenses required.

(b) The following shall appear in all source code modules:

(i) module name;

(ii) version number;

(iii) revision number; and

(iv) description of functions performed.

All source code shall be appropriately documented to ensure that TL is able to identify modules and revisions.

This does not apply to commercially available software that does not influence the core operations of the SIGMa. The intention here is to allow for easier analysis on changes made on various version modules.

(c) So as not to complicate the validation of software, all individual device-specific information (for example, SIGMa identification number or address, venue name and touch screen calibration) and all device group specific information shall be stored separately from any common information (i.e. common to all SIGMas of a particular type).

The intention here is that it should be possible to easily verify game software. Venue and other location-specific information, date of compilation, etc., that might be included on the game software storage device (for example, EPROM or CD) make it impossible to obtain a signature that is common to all devices.

(d) Each SIGMa shall have a function or program that displays the current software version(s) installed on the device.

(2) Control and upgrade

(a) Software media shall be clearly labelled, and shall contain sufficient information to identify the version and modification level. The identification used is at the discretion of the supplier but shall strictly follow the supplier's identification system as detailed in the supplier's software configuration control procedures.

(b) Superseded approved versions of programs may be held on the storage media. However, it shall be possible to clearly identify which files belong to which version of the program.

(c) The method of loading programs to the storage media (for example, disk file transfer or download) shall be certified by the CA.

(3) Verification

(a) All program source codes for SIGMas shall be made available for examination by the TL.

(b) The party that submits software shall provide the means to demonstrate, or otherwise prove to the satisfaction of the TL, that the source code supplied compiles to the same executable code as contained in the firmware program store of the SIGMa submitted for certification.

(c) When compiled, all source code supplied to the TL shall generate object code that is exactly the same as that installed in the SIGMa. The TL shall verify that the program or source code modules comply with the requirements of this document.

This does not apply to commercially available software that does not influence the core operations of the SIGMa.

(d) If redundant sections of code exist in the program, the supplier shall provide an indication of the areas of code which are redundant.

One way of achieving this goal is to use compiler directives that omit sections of code (for example, if a particular compiler option is set or not set).

## 26. Critical memory requirements

(1) Critical memory

Critical memory shall store all critical data.

(2) Maintenance

(a) To cater for disruptions that occur during the update process of critical memory, at any point in time during an update there shall be sufficient

information to allow the software to fully recover from such disruptions without loss of critical data.

(b) The result of the critical memory validation shall be stored and kept always up to date (i.e. shall be updated after every instance of critical memory change).

(c) A validity check of critical data memory shall be undertaken at least before a game play.

(d) When meters in critical memory are being updated, the software shall ensure that errors in one copy of the meter readings are not propagated to other good copies.

(3) Detection of corruption

(a) Any failure of a validity check shall be classed as either:

(i) recoverable memory corruption, if at least one copy of critical memory is established to be good; or

(ii) unrecoverable memory corruption.

(b) A validity check of SIGMa critical memory shall be undertaken at least after every restart of the device or transaction of significance (for example, parameter change or reconfiguration). After a device restart (for example, power off and on), the device shall complete its validity check of the critical memory by performing a comparison check of all logical copies of critical memory.

(4) Recovery

(a) If the SIGMa is so designed that after an uncorrectable memory corruption it is possible to view all logical copies of data, the SIGMa shall highlight which of these figures are expected to be good as opposed to those that might be corrupted.

(b) An unrecoverable memory corruption shall result in a RAM error.

(c) If an unrecoverable memory corruption occurs, it shall require a master reset.

(d) If validity checking of critical memory information fails, and data memory remains operational, the software could recover critical memory information in order to continue to operate. This option has the following implications:

(i) all logical copies of critical memory shall be recreated using the good logical critical memory as a source; and

(ii) the device shall verify that the recreation of the critical memory was successful before attempting to identify any permanent physical memory failure. If such permanent memory failure is determined, the device shall enter the unrecoverable memory corruption sequence.

## 27. Program memory storage

(1) Labelling

All program storage media shall be uniquely labeled, identifying the following:

(a) the program name (and the software shell name, if applicable);

(b) the name of the manufacturer;

(c) the development number or the variation;

(d) the version number;

(e) the type and size of media; and

(f) if applicable, the location in the SIGMa (if critical).

(2) Write-once read-many (WORM) memory

(a) A WORM (for example, CD-ROM) used as a program or fixed data storage device shall be written such that only the actual program and data required are written to the WORM.

(b) The operational software shall provide an integrity check method to verify that there are no additional or missing program or data records or files on the WORM.

(c) There shall be an ability to conduct an integrity check independent of the device's operational software to verify that there are no additional or missing program or data records or files on the WORM (for example, inserting a CD-ROM in another PC which then conducts a full signature check and directory search check over the CD-ROM space).

(d) The method of changing to different versions of the program, including reversion to old versions, shall be certified by the CA.

(3) Reprogrammable memory

(a) If a reprogrammable memory device is irreversibly configured at the hardware level as a read-only device (for example, the write line is cut off), it shall be treated for all purposes as an EPROM.

(b) A reprogrammable memory program storage device shall be protected from unauthorized modification. Modification shall only be permitted once the TL and the CA or GBT (or both) are satisfied with the appropriate security measures (for example, if a high voltage chip that allows modification of the reprogrammable memory devices is installed on the printed circuit board (PCB)). The method of securing the reprogrammable storage device shall be verified by the TL and certified by the CA on a case-by-case basis.

(c) Before the termination of any programming operation on reprogrammable memory, each byte programmed shall be verified by a program comparison controlled by the programming device.

(d) Only the actual program and fixed data required shall be written to the reprogrammable memory device.

(e) The use of jumpers or similar devices can be used to enable or disable a reprogrammable memory, erasure or writing to reprogrammable memory provided there is a feedback signal to the software so that the setting of the jumper position can be recorded or appropriately acted upon. If a jumper or switch is set to "Write", then the SIGMa shall not be able to enter "Play" mode. These jumpers shall be located within the logic area of the SIGMa.

(f) All reprogrammable memory devices shall be housed in a secure area.

(4) Read or write storage

(a) A read or write storage device (for example, disk or tape) used for storage of program or fixed data shall be written in such a way that only the actual program and fixed data required by the program are written to the storage device.

(b) The operational software shall provide an integrity check method to verify that there are no additional or missing program or fixed data records or files on the storage device.

(c) There shall be an ability to conduct an integrity check independent of the device's operational software to verify that there are no additional or missing program or data records or files on the storage device.

(d) All methods of integrity checking shall have the ability to identify files or records that contain variable data and exclude them from the signature calculation.

(5) ROM program storage

All unused areas of ROM shall be written with the inverse of the erased state, which for most EPROMs are zero bits (00 hex), rather than one bits (FF hex).

(6) Verification

(a) All non-critical memory RAM shall be checked for corruption at each power up.

(b) All devices that contain program memory or critical memory shall be validated by software. This validation may include self-checking by specific devices with internal programs. RAM and program storage device space that is not critical to SIGMa security need not be validated.

(c) The TL shall certify the method of signature checking used, which shall include:

(i) a secure means of signature verification of all software resident on certain processor boards associated with a SIGMa;

(ii) self-checking methods used by programmable coin mechanisms, banknote acceptors, smart card readers and intelligent displays; and

(iii) if the signature requirement is to be met by the self-checking method, evidence provided by the supplier of the device that a self-check has been performed. The details of the checks performed shall also be provided to the CA for approval.

(d) Memory that does not change dynamically (for example, EPROM) shall be validated by the SIGMa at least every time the hardware is reset (for example, at power on), the software is reset (where this is possible) or after a type 4 significant event. Failure of the validation shall be reported to the monitoring and control system, if possible. The fact that the SIGMa activates normally is deemed to be proof that validation was successful.

(e) If a validity check of the software fails, it is understood that this means that the SIGMa cannot function as intended, in which case it shall disable itself immediately. This excludes transaction devices that do not influence the game results.

(f) An error detection scheme shall detect at least 99.995 % of all possible data errors.

(g) The integrity of the operation of the device shall be protected from nefarious or accidental use of the unused portions of the program memory storage media.

(h) The initial value of the cyclic redundancy check (CRC) register is not an acceptable seed.

(i) The following principles apply to signature seeding:

(i) the seed information shall be at least 15 bits in length; and

(ii) the seed information shall influence the behaviour of the algorithm in a non-trivial way.

(j) Signature algorithm seeds (or more generally "algorithm coefficients") shall be supplied by the initiator of the signature request at the time of activation.

**28. Prescribed display formats**

(1) If dates and times are displayed, they shall be displayed in a consistent format.

(2) The acceptable all-numeric date formats are dd-mm-yyyy or dd-mm-yyyy.

The preferred date format is dd-mm-yyyy. This requirement does not apply to the date format on displays that are not accessible to the player, such as set-up screens.

(3) The 24-hour time formats are acceptable.

(4) Field separators within times shall be colons ( : ) or full stops ( . ). The time of day shall be given as East African standard time.

**29. Data communication**

(1) Data format

(a) SIGMa should send the information collected from GM in on real-time basis as specified by GBT.

(b) The information sent should be in XML format as specified by GBT.

(c) It should be capable to digitally sign each XML that is sent to GREMS using 1024-bit private key encryption.

(2) Communication method

(a) SIGMa should be capable to provide data connection to GREMS server in a secure way via IPSec/VPN through the following methods:

(i) Ethernet 10BASE-T (IEEE 802.3i) or higher;

(ii) WiFi 802.11b or higher; and

(iii) Mobile Data Network 3G or higher via SIM card locally installed in the SIGMa.

(b) SIGMa should support connectivity to GM that supports internationally acceptable protocols such as SAS, G2S or any other protocol that is used in the GM.

(c) SIGMa should have a USB 2.0 or higher interface to allow for authorized technicians to perform various functions, such as diagnosis, upgrade software/firmware or copying log files.

(3) Communication failure

(a) If there is a failure of a communication link between the SIGMa and the next point in the monitoring system (i.e. the inability to send or, where applicable, to receive messages to and from the monitoring and control system) then, when communication is restored, the SIGMa shall check whether there was a configuration or software change. If there was, then the SIGMa shall send a type 4 significant event message as soon as possible after reactivation, before start sending all such data buffering on nonvolatile memory during the communication failure.

(b) If the GM is unable to send messages to the SIGMa, then the GM may complete the current game and permit cashout but shall then disable further game play until able to forward these messages to the SIGMa. Then the SIGMa shall send a type 4 significant event message as soon as possible after starting to send messages.

(c) All SIGMas shall be able to handle the following range of failures without loss of data:

(i) failure of central computer network interfaces;

(ii) failure of the central network;

(iii) failure of central data communication interface devices;

(iv) failure of single data communication interface;

(v) high data communication error rates on line;

(vi) a foreign or additional device placed on a network;

(vii) a foreign or additional device placed between network bridges, communication controllers, or on data communication lines between sites;

(viii) single data communication port failure on remote controller (if any);

(ix) network failure on regional or local controller (if any);

(x) network failure on cashier terminal (if any); and

(xi) data communication interface failure on a SIGMa.

(4) Active daily period

If the SIGMa instructs the GM to disable (for example, at the end of an active daily period) during game play, the GM shall complete the current game (including any feature games) before immediately disabling itself. If there are any credits remaining on the player's credit display, the machine shall allow the player to collect those credits (i.e. it shall permit a cashout).

**30. Metering – Audit meters and displays**

(1) Unless otherwise specified in legislation, the value displayed by the meter may be in either credits or in monetary values as long as the units used are clearly shown near to the meter or display. Alternative wording for the meter name might be approved by GBT on a case-by-case basis.

(2) The "total bet" meter is defined as the total value of all credits bet. It is a required soft meter and shall be designated on all reports or displays as "Total Bet". It shall, in addition, be recorded by the monitoring and control system. In the case of multigame SIGMas, this meter is also required and a separate value shall be maintained for each configured game on the SIGMa.

(3) The "total win" meter is defined as the total value of all credits won. It is a required soft meter and shall be designated on all reports or displays as "Total Win". It shall, in addition, be recorded by the monitoring and control system. In the case of multigame SIGMas this meter is also required and shall be maintained for each configured game on the SIGMa.

(4) The "total coin box drop" meter is defined as the total value of coins or tokens to the coin box drop of the SIGMa. It is a required soft meter and shall be designated on all reports or displays as "Total Coin Box Drop". It shall, in addition, be recorded by the monitoring and control system. An additional period meter is required in audit mode, to be reset following each clearance of the coin drop storage area.

(5) The "total bill drop" meter is defined as the total value of all bills entered into the bill acceptor connected to the SIGMa. It is a required soft meter and shall be

designated on all reports or displays as "Total Bill Drop". It shall, in addition, be recorded by the monitoring and control system. An additional period meter is required in audit mode, to be reset following each clearance of the bill storage area.

(6) The "total games played" meter is defined as the total number of games started and completed on the SIGMa. The units shall be in games. It is a required soft meter and shall be designated on all reports or displays as "Total Games Played". It shall, in addition, be recorded by the monitoring and control system. In the case of multigame SIGMas this meter is also required and shall be maintained for each configured game on the SIGMa.

(7) The "total hand pay" meter is defined as the total value of all hand pays, including hand pays less than one coin or token, hand pays greater than the CDD limit. It is a required soft meter and shall be designated on all reports or displays as "Total Hand Pays". It shall, in addition, be recorded by the monitoring and control system.

(8) The "total cash in" meter is defined as the total value of all cash entered into the SIGMa (including amounts transferred from a card in an EFT environment). It shall be designated on all reports or displays as "Total Cash In". Separate meters for "cash", "EFT transactions" and "tickets/vouchers" that are added to derive the "total cash in" amount are acceptable.

(9) The "total cash out" meter is defined as the total value of all cash paid out of the SIGMa (including hand pays, printed tickets and vouchers and amounts transferred to a card in an EFT environment). It shall be designated on all reports or displays as "Total Cash Out". Separate meters for "cash" "EFT transactions" and "tickets/vouchers" that are added to derive the "total cash out" amount are acceptable.

(10) The "total EFT in" meter is defined as the total value of all credits transferred from a card to a SIGMa in an EFT environment. If the SIGMa has EFT functionality, this shall be designated on all reports or displays as "Total EFT In". If the SIGMa does not support EFT, this meter is not required.

(11) The "total EFT out" meter is defined as the total value of all credits transferred to a card from a SIGMa in an EFT environment. If the SIGMa has EFT functionality, this shall be designated on all reports or displays as "Total EFT Out". If the SIGMa does not support EFT, this meter is not required.

(12) The "last five bills in" display shall enable the SIGMa to display, in audit mode, the monetary value of each of the last five bills entered into the bill acceptor. The bills shall be listed in the order they were entered, with the most recently entered bill listed first.

(13) A meter or display shall be updated and recorded by the monitoring and control system as the event occurs. All meters shall be added to, not incremented with the exception of coin-handling meters (i.e. coin-in and coin-out meters) which may be either added or incremented. The term "added" indicates the fetching of the current value from memory, conducting an arithmetic add operation and storage of the result in memory.

(14) When a meter, of any type, reaches its maximum value, it shall automatically revert (i.e. "wrap round") to zero and subsequently continue counting (from zero) in the normal way.

(15) SIGMa shall have access to a function that enables the display of all metered information retained by the SIGMa. It is not mandatory that metering information be displayed on the device from which the information originates. The information may be displayed on an external device or on a computer (or on both) to which the SIGMa has communicated such information.

## PART VI

## OPERATIONAL REQUIREMENTS

### 31. Access to restricted features

Access to the following restricted features of SIGMa shall be regulated by at least a key switch, or by key-based access to the inside of the machine cabinet:

(1) auditing information;

(2) statistical information;

(3) test functions; and

(4) any other features deemed by GBT to be restricted.

### 32. Set-up – Device configuration

(1) Configuration of variables

(a) A variable required to be set during device configuration or set-up shall not be able to be changed except following a valid memory clearance, unless able to be changed by some other secure method certified by the CA.

(b) A SIGMa shall not be able to be operated unless all configuration variables are set. A device may be configured remotely or by direct access by means of an approved mechanism.

(c) If memory becomes corrupted, a SIGMa shall not assume default values and recommence gaming operation unless the assumed values have been configured by an approved mechanism.

(2) Device enrolment

The unique SIGMa monitoring and control system address shall only be able to be configured in a SIGMa during the set-up mode. There shall be no configurable parameters on a SIGMa, whether set manually or set by the monitoring and control system that are not certified by the CA and approved by GBT.

(3) Reconfiguration

All configuration settings required for the proper operation of the SIGMa shall be entered before the SIGMa can enter "Play" mode. If all configuration settings required have not been entered, the SIGMa shall detect this condition and remain disabled.

**33. System security**

(1) SIGMa shall have the following secured access, local or remote, to configuration parameters separated from one another by means of PIN or password:

(a) GBT access: access related to configuration related to data sent to GREMS server such as GREMS IP address, GPS coordinates, application based encryption, and any other configuration parameters deemed by GBT to be included;

(b) SIGMa manufacturer access: this access is related to basic configuration and software that will make SIGMa functional such as software or firmware updates, device diagnosis, network level encryption, etc.

(c) Operator access: this access is related to operational matters, such as, connectivity of SIGMa to local connectivity configuration, such as LAN IP address, WiFi password, etc.

(2) SIGMa shall disable all player inputs and suspend all gaming functions while any of its secure areas are opened or remain open.

(3) SIGMas shall not have any functions or parameters adjustable by or through any separate computer, input device or input codes, except for the following:

(d) the adjustment of features that do not affect functionality in any way;

(e) the downloading in an authorized manner of any software, data or operational parameter; and

(f) an approved configuration (set-up) mode.

(4) In general, the reactivation of a SIGMa that has been deactivated shall require manual intervention by the gaming venue operator or the system operator. The following exceptions apply:

(a) if a door open event occurs other than a logic door open, the SIGMa may reactivate automatically when the door is eventually closed;

(b) if the power supply to a SIGMa fails, the SIGMa is deactivated as a matter of course. It is permitted for the SIGMa to automatically reactivate itself unless it determines that there was a configuration or software change while the power was down, in which case the SIGMa shall remain deactivated until manually reactivated.

(5) If a SIGMa loses communication with GREMS server for over a period of 48 hours, the SIGMa shall disable itself.

(6) Where a SIGMa is unable to operate without the loss of any information (for example, metering, transactions or significant events) it shall immediately disable any further game play on GM.

(7) If a significant event has not already been logged (by the system or the SIGMa) when deactivation occurs, the SIGMa shall ensure that such an event is reported to the system as soon as possible.

**34. Master reset**

(1) Following the initiation of a master reset procedure (using an approved RAM clear method), the game program shall execute a routine which initializes each and every bit in RAM to the default state.

(2) It shall not be possible to reset any critical RAM without first accessing the logic area.

(3) A configuration setting that is required to be entered during set-up mode immediately following a master reset shall not be able to be changed after the machine leaves set-up mode.

## 35. Test or service mode

(1) While the SIGMa is operating in the test mode, there shall be clear notification that the SIGMa is in that mode (for example, by LED light signal or on-screen message).

(2) Opening the main enclosure of the SIGMa may automatically place the SIGMa in a service or test mode. A diagnostics test mode may also be entered by means of an appropriate instruction from an attendant during an "Audit" mode access.

(3) If there are any test-mode states which cannot be automatically cancelled by closing the door, (for example, if it is first necessary to manually set a switch) or exit from the "Audit" mode (if that was the method of entry to the "Test" mode), the action necessary shall be indicated on the machine and in the relevant manuals.

## 36. Visual displays

(1) Diagnostic mode display should enable authorized technician to perform simple setup or diagnosis such as, setting of:

(a) GREMS server IP address;

(b) GREMS TCP/IP port;

(c) Device WAN and LAN IP address;

(d) GM ID and/or serial number; and

(e) Device GPS coordinates;

Access to this mode should be protected by password or PIN.

(2) Touch screens, if used, shall comply with the following:

(a) touch screens, shall be resistant to scratching from conditions likely to occur during normal use;

(b) touch screens shall be accurate, and once calibrated shall maintain that accuracy for at least the manufacturer's recommended maintenance period;

(c) touch screens shall be designed and installed such that static build-up is minimized to a level that ensures no humanly perceptible static is discharged through a grounded patron that touches the screen;

(d) SIGMas that employ touch screens shall have a recalibrating facility that may be either manual or automatic, but in any case shall not require access to a logic area;

(e) touch screen selected input shall always be interpreted accurately and acted upon in accordance with the description of the choice (indicated on the screen) made by the player;

(f) if the opening of the SIGMa door is found to affect touch screen calibration and recalibration is carried out with the door open, there shall be in place means to ensure that the recalibration is correct when the door is closed (for example, two sets of calibrations one for door open and one for door closed);

(g) touch screen button icons shall be sufficiently separated to reduce chances of the wrong icon being selected due to incorrect calibration or parallax errors; and

(h) all buttons and touch points shall be documented for evaluation by the TL and certification by the CA.

## PART VII

## SIGNIFICANT EVENTS REQUIREMENTS

### 37. General

(1) Where these Standards states that the system shall detect and record significant events, a particular implementation is not implied. As long as the CA can be assured that these events are detected and reported, the method that is used to do so is of little concern. However, if it is stated in this document that the SIGMa shall detect and record an event, the SIGMa shall be programmed to create the event response internally, pass it to the host of the system as soon as possible and, where required, deactivate game play.

(2) Subclause (3) provides a summary of the significant events that are specified by the CA. In the case of each significant event, the type of event (relative to requirements for deactivation and reactivation) is indicated. Each of the significant events shall be tested during the formal acceptance tests.

(3) In the following list, four types of significant event are defined:

(a) type 1: information only (no deactivation);

(b) type 2: events that lead to automatic deactivation but also allow for immediate automatic reactivation when the problem is solved (for example, authorized door open);

(c) type 3: events that lead to automatic deactivation and require manual reactivation; and

(d) type 4: events that lead to automatic deactivation and require manual reactivation, but only after the GBT audit procedures have been followed. These procedures might involve immediate approval for reactivation, or the approval could be withheld until physical inspection by an GBT inspector is completed.

(4) To some significant events a suffix "/R" is appended, which means that the event has to be reported by the system in the daily type 4 events report. Note that not all events with this description are type 4 events.

(5) By definition, all type 4 events shall be reported. The phrase "manual reactivation" is understood to include closing of the logic door (if necessary) or turning of a reset key.

(6) Significant events other than type 1 that occur on a SIGMa shall cause a clearly displayed message that an event has occurred.

(7) The following actions shall be performed, if possible, on clearing of the fault on a SIGMa:

(a) any messages shall be removed;

(b) any relevant player inputs shall be re-enabled; and

(c) the alarm shall be turned off.

(8) Generic significant events are applicable to all SIGMas controlled by the system. All generic significant events shall be detected and notified as soon as possible, but before any game can be played.

(9) All SIGMa fault conditions shall activate an alarm, which shall include either a light or sound, or both.

(10) To assist with service and fault diagnosis, the nature of the event shall be displayed.

**38. SIGMa and terminal events**

(1) Configuration change (type 4): Change of denomination, switches or jumpers, etc.

(a) The SIGMa shall detect and report any configuration changes made to the device (even if the power is off when this occurs or the SIGMa is not able to communicate with the system) and pass it to the system before game play is reactivated.

(b) It is acceptable if the SIGMa only detects the changes when restarting.

(c) Reportable changes include any change to any configuration that alters the metering or the game outcome or the RTP of the game. Changes that need not be reported include, for example, the sound, the tower light, settings that might enable or disable a peripheral, or changes to the visual aesthetics of the SIGMa.

(2) Master reset (type 4): Intentional memory clear of the RAM and other volatile memory of a SIGMa has occurred.

(3) Error detected in volatile memory (type 4): Failure of internal test. The failure of some test(s) means that the SIGMa cannot function correctly, in which case it shall disable itself immediately after reporting the event to the monitoring and control system (if possible).

(4) Logic area access (type 4): Opening of the logic area door. The SIGMa shall detect the opening of the logic area door (or access to the logic area).

(5) Power on (type 1): Power is successfully restored and the device can operate.

(6) Logic area closed (type 1): A sensor registers that a logic door has been closed.

(7) Enter test or audit mode (type 2): If the SIGMa has a test mode or special staff or audit mode, a significant event shall be signalled when such mode is entered.

(8) Exit test or audit mode (type 2): If the SIGMa has a test mode or special staff or audit mode, a significant event shall be signalled when such mode is exited.

(9) General enclosure access (type 2): Opening of outer enclosure door, excluding the drop box door. This message shall be sent by the SIGMa if it has noticed any interference, such as the changing of counters or insertion of coins, while this door is open. When the message is sent, the monitoring and control system shall add the staff card number to the event message. If no card number is available, the message shall be tagged as an unauthorized access by the monitoring and control system.

(10) Drop box door open (type 1): Opening of drop box door. When the message is sent, the monitoring and control system shall add the staff card number to the event message. If no card number is available, the message shall be tagged by the monitoring and control system as an unauthorized access.

(11) Enclosure door closed (type 2): A sensor registers that a door has been closed.

(12) Cancel credit (type 2): Any incident of a manual cancel credit (for example, due to book or hand pay) shall indicate a significant event. The value of the credits shall be included in the significant event report.

(13) Low memory back-up battery (type 4): The voltage that is produced by the battery or another device for maintaining the contents of RAM is approaching a level below which the memory cannot be maintained for a minimum of 14 d without mains power and data might be lost or corrupted.

(14) Collect credit (type 1): Cashout that exceeds the limit specified by legislation. This significant event is not specified in the legislation at present, but may be required later.

(15) Software validation or signature failure (type 3): It is assumed that modification or unauthorized reading (or both) of the contents of the restricted components of the SIGMa or loading of unapproved software (or both) could have occurred. The SIGMa shall be manually reactivated after the problem is rectified. Equipment in a casino environment is not required to be capable of doing signature checking in response to a request from the GREMS.

(16) Credit limit exceeded (type 1/R): Machine credit that exceeds the limit specified in legislation. Only the first occurrence during a particular customer's session shall be sent.

(17) Maximum prize win (type 1/R): Winning of a prize that equals the limit specified by legislation.

## ANNEX

## GUIDELINES FOR SUBMISSION AND SCOPE OF TESTING

Testing for statutory compliance should in no way be considered or relied upon as quality assurance testing. The onus lies with the manufacturer or supplier that proper quality assurance and functionality testing is undertaken on a product before it is submitted for compliance testing.

### A1. General

(1) These Standards serve the following purposes:

(a) Fundamental 1: The protection and safety of the public, which includes but may not be limited to:

(i) fairness of the game;

(ii) integrity of the data associated with the above inclusive of any RNG and the results it may generate;

(iii) mechanical safety of any equipment;

(iv) electrical safety of any equipment;

(v) the generation, communication and transmission, recording and recall of the required significant events event and status reporting in this regard; and

(vi) integrity of communicated data;

(b) Fundamental 2: The collection of fees, taxes and levies paid by licensees, which includes but may not be limited to

(i) auditability of fees, taxes and levies paid;

(ii) integrity of the data associated with (i) above;

(iii) the generation, communication and transmission, recording and recall of the required significant events event and status reporting in this regard;

(c) Fundamental 3: Dispute resolution, which includes but may not be limited to

(i) integrity of the associated data,

(ii) the integrity and accuracy of gaming or game related data communicated to the public, including the accuracy of awards or payments made to a player including the physical or actual amounts dispensed or handed to a player,

(iii) the accurate counting and recording of bets wagered, regardless of the origin or media of the wager,

(iv) the retention of current and past game status and results;

(d) Fundamental 4: Compliance of the equipment, or a particular gaming game with the regulations and the rules of GBT.

(e) Fundamental 5: Inherently, the highest possible level of compliance with the greatest number of requirements in these Standards, and the regulations and rules .

(2) These compulsory requirements should be met by the appropriate equipment before submission for gaming testing or verification. Compliance with these

requirements should be included with the submission and the submission will be held in abeyance until such time as this requirement is met.

(3) Persons making submissions to a test laboratory (TL) should be aware that such submissions are subject to the audit and verification of submissions and arising test or evaluation reports, by both the laboratory accreditation authority and GBT.

## A2. Interpretation

(1) These Standards are, as a norm, produced in standardized English and are aimed at experienced technical or compliance persons. The basic rules of the interpretation of statutes apply to these Standards, namely:

(a) the literal interpretation of an English speaking person qualified in the fundamentals given in clauseA1; and

(b) the intent of these Standards as interpreted by an English speaking person qualified in the fundamentals in clause A1 and confirmed by a test laboratory that is accredited against these Standards.

(2) In the event that these Standards cannot be interpreted to a high degree of certainty by the above means or is grey or silent on a particular requirement, a query may be addressed by GBT.

(3) The query will be considered by a panel of knowledgeable persons and a written clarification or interpretation provided.

(4) For a query to be considered, the following information should be included:

(a) the applicable part of these Standards;

(b) the publication date of these Standards being referred to;

(c) the section heading in which the requirement being queried is carried;

(d) the section number of the requirement being queried;

(e) a description in standardized English as to the circumstances causing the query;

(f) a description in standardized English of the type and nature of equipment or software (or both) the query applies to; and

(g) the submitter's unique reference number or code for the query.

(5) In the event of a dispute as to the interpretation of these Standards or their scope of application (or both), the interpretation of the GBT should be regarded as final.

## A3. Preparation for testing or verification

(1) When gauging which hardware or software should be submitted for testing or verification by a test laboratory, the following ambit of the respective standards are applicable:

(a) from the first point at which a player may insert a coin, token, bank note into a machine or game terminal for the direct purposes of converting these value instruments into credits with which to make a wager; or

(b) from the first point at which a player may insert, or hand in for conversion, a coin, token, bank note, ticket or electronic value instrument, for conversion into credits with which to make a wager;

(c) to the point in a game where these credits are "cashed out" and no further games can be played; and,

(d) to the point where credits, coins, tokens, bank notes, tickets or any other value instrument are credited or dispensed as redemption of a player balance; and

(e) where a players credits are utilized in any manner in the participation or operation of a jackpot or progressive; and

(f) where the transactions detailed in (a) and (e) are recorded for purposes of maintaining a player account or balance, and recorded for storage for later recall for purposes of reporting on an GREMS, recall of all data for dispute purposes, conducting and reconciling a drop or count and for audit purposes.

(2) Inclusive of any processes in-between the processes in subclause (1)with the appropriate event, metering and accounting and error reporting, the accuracy and integrity of any calculation required in any of the processes in subclause (1), the accuracy and integrity of data communication or storage in any device or process through which data associated with all the points above may be:

(a) initiated,

(b) transmitted, received, or

(c) temporarily or permanently stored.

## A4. Minimum submission guidelines

(1) The testing of equipment for compliance with these Standards is conducted as type testing, where the equipment under test is in the same configuration as it is expected to be operated in the field.

(2) This matching of configurations is inclusive of every hardware configuration intended to be utilized and which should be uniquely identified for practical testing purposes.

(3) The testing of the GREMS takes places where the GREMS and any associated SIGMas connected to the GREMS are functioning as a whole to emulate the expected operating environment in which the combinations of equipment are expected to operate.

(4) Where a SIGMa is to be added to a GREMS environment, or any form of upgrade or change of the GREMS environment is to be undertaken, this likewise should be tested in a replica environment.

(5) No GREMS environment change will be considered as only verifying a single element of the environment. Testing is expected to include the anticipated effects on the compliance and environment as a whole, as a result of the changing of a single element.

(6) Regardless of the country or laboratory at which a submission is made for testing, the following documentation should be provided at the time of the submission and may be included with the test results or evaluation report (or both) provided to the certification authority or to GBT:

(a) An original formal request for the equipment or software being submitted, in standardized English, formally declaring which Standards the equipment or software has been designed to meet, signed by the applicant.

This declaration is specifically to include the requirements in the applicable Standards as to which the equipment or software meets and a detailed explanation of the requirements that the equipment or software does not meet and why this is the case.

(b) Documents stating that no known default setting or configuration whether soft or hard, a RAM clear, a master reset, will result in a non-compliant configuration or operation of a SIGMa in such a manner as to be detrimental to the public or GBT.

(c) Documents stating that in the design, implementation and in-house testing or quality control due regard has been taken to prevent non-compliant or detrimental configurations which may be caused by human error on behalf of a maintenance function of the manufacturer's or supplier's maintenance personnel, or those of the licensed operator.

These documents may be evaluated by the test laboratory and where the test laboratory is not satisfied that fundamental 5 (see clause A.1) is not being met in the laboratories opinion, the submission may not proceed.

The test laboratory may indicate on its test or evaluation report that requirements declared as not being met are appropriate and that in their opinion, these requirements are not applicable to the equipment or software being submitted in the environment as it is intended to be used.

A copy of the declaration may be attached to the test or evaluation report and kept with the report.

(d) A full set of users' and operators' manuals, and release notes detailing

(i) the assembly, set-up and configuration of the equipment,

(ii) the first level maintenance of the equipment inclusive of fault codes and fault identification logic,

(iii) the correct and proper operation of the equipment by both the operator or licensee and the player,

(iv) for changes to equipment previously submitted, a listing of changes to the design concept implementation or methodology in the creation or operation of equipment which has not been previously reviewed by a test laboratory,

(v) for the verification of data communication and in particular, the verification of data error detection and correction, the following additional information should be provided:

(1) a full set of technical documentation and descriptive relating to the construction and functioning of the protocols under review, both during normal data communication and in the event of an unexpected break in communications;

(2) a full set of technical and descriptive documentation, including any calculations and associated formulae, which in detail describes the methodology employed in meeting the error detection and correction (EDC) requirements of these Standards and which should confirm the source code implemented for this purpose;

(3) documents that indicate whether any wire to a logic area access device or sensor should be:

- broken (open circuited);
- short circuited with another wire or conductive frame of the SIGMa;
- partially open circuited;
- partially short circuited; or

- partially short circuited to another wire or conductive frame of the SIGMa.

(7) The appropriate logic area access significant event should be reported to the GREMS, and the SIGMa should accordingly be disabled for further play.

## A5. Maintenance of a defect schedule

(1) Where during testing a defect is found in a particular manufacturer's or supplier's equipment under test and is contrary either to the applicable Standards or a compliance letter (see sub-clause (2)), a schedule of all these defects for the particular manufacturer or supplier should be maintained by the test laboratory detailed with the required the Standards not met or undertaking in the compliance letter not correctly met.

(2) In any retesting of the equipment which may have failed and for all subsequent applicable equipment provided for testing thereafter, all applicable defects should specifically be checked by the test laboratory and the result included in the test or evaluation report as required by the applicable Standards. The test laboratory is requested to report to the manufacturer or supplier any defect which reoccurs in equipment under test for the manufacturer or supplier to action.

## A6. Deviations from these Standards

(1) In line with international practice, provision is made for a manufacturer or supplier to apply to GBT, to deviate from, or be exempted from, certain requirements in these Standards, where compelling reasons to do so may exist.

(2) All requests received will be reviewed by a panel of knowledgeable persons, representative of the gaming industry, nominated by the technical committee.

(3) A request to deviate from a requirement in these Standards should be made in writing at any time to the address provided for standards queries, which shall be clearly motivated and justified as to the need for this deviation.

(4) Alternately, the manufacturer or supplier may request in writing to make oral presentations to GBT, where again the need to deviate should be motivated and justified.

(5) GBT will respond to each request during which the applicant might be expected to answer queries from the panel, which might be technical in nature.

## A7. Deviations from the GBT rules and requirements

(1) These deviations are ordinarily dealt with by GBT, as it sees fit.

(2) Any deviations in this regard are at the sole discretion of GBT concerned.

## A8. Ancillaries to equipment (add-ons)

(1) Ancillaries refer to any equipment which is not originally designed or made by the original equipment (OE) manufacturer or supplier, or is provided by an alternate manufacturer or supplier, to be connected or associated with previously tested equipment to provide an additional functionality or features to the equipment that fall within or affect the scope of these Standards.

(2) This may include but is not limited to for example jackpot and value represented fills, such as hopper fills, functionality, queuing systems, enhanced reporting systems, and automatic or automated cashier positions.

(3) Where ancillaries to equipment connects to, reads, monitors, utilizes and acts upon, or displays data or events (or both) by physically or logically connecting or interacting with the equipment whether via a cached or 'copy' database or not, GBT may require that sufficient review, verification and testing in terms of these Standards take place to ensure that add-on in no reasonable way, affects, disrupts or alters the operation of the equipment, within the scope of these Standards, and as approved.

(4) A submission in this regard should contain two letters of compliance from the OE designer, implementer, manufacturer or supplier and the add-on designer, implementer, manufacturer or supplier providing the necessary undertakings required in an ordinary submission and that the inclusion of add-on in no way affects or disrupts the original approved operation of the equipment.

(5) The test laboratory should, in conjunction with the OE and add-on manufacturer or supplier, determine which requirements in these Standards can be applied to the equipment under test and add-on to be able to make the necessary verification of the possible effect of an add-on.

(6) The requirements in these Standards utilized for this purpose should be listed in the resulting test report issued by the laboratory and provided to the certification authority for its records.