STANDARDS

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

THE GAMING EQUIPMENT STANDARDS – CENTRAL ELECTRONIC MONITORING SYSTEM FOR ROUTE OPERATIONS, 2018

ARRANGEMENT OF STANDARDS

PART I

PRELIMINARY PROVISIONS

1. Citation
2. Scope
3. Interpretation
4. Abbreviations

PART II

GENERAL REQUIREMENTS

5. Documentation
6. Enclosure identification
7. Enclosure construction
8. Enclosure security
9. Access detection systems

PART III

ELECTRICAL REQUIREMENTS

10. Enclosure wiring
11. Electromagnetic compatibility
12. Power supply

PART IV

COMPUTER AND PERIPHERAL HARDWARE REQUIREMENTS

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

PART V

SOFTWARE REQUIREMENTS

23. General
24. Verification of source code compilation
25. Validity checks
26. Critical memory
27. Program memory
28. ROM program storage

PART VI

SYSTEM FUNCTIONAL REQUIREMENTS

29. Auditing information
30. Cashout by printed ticket
31. Clocks
32. Electronic funds transactions
33. Central logging of information
34. Control of gaming equipment
35. Back-ups and recovery

36. Encryption of stored data
37. Handling of master resets
38. Recording of game play statistics
39. Recording of significant events
40. Security of the significant event log
41. Storage of the significant event log
42. System security requirements
43. Permitted devices
44. Metering
45. Permitted software
46. Communication with GMs
47. Reactivation of game play
48. Signatures
49. Transaction logging
50. Site data logger device
51. Cashout while disabled – Non-permitted occasions

PART VII

COMMUNICATION REQUIREMENTS

52. General
53. Cellular network communication

PART VIII

DATA COMMUNICATION REQUIREMENTS

54. Remote control of GMs
55. Communication failure and recovery
56. Accuracy of communication speed
57. Error detection
58. Error detection and recovery
59. Message recovery

60. Flow control
61. Protocol
62. Higher level protocol
63. Layered protocol
64. Message authentication in low level communication
65. Message framing in low level communication
66. Multi-dropping
67. Period meters
68. Software meters
69. Restart/recovery
70. Simulator

PART IX

SIGNIFICANT EVENTS REQUIREMENTS

71. General
72. Gaming Device and terminal events
73. Player/staff cards (if applicable)
74. Banknote acceptance (if applicable)

PART I

PRELIMINARY PROVISIONS

1. Citation

These Standards may be cited as **The Gaming Equipment Standards – Central Electronic Monitoring System for Route Operations, 2018**.

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 central electronic monitoring system (CEMS) in slot machines and route operations as stipulated under section 26(1)(b) of the Act.

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, Cap. 41 ("the Act") and the Gaming Regulations ("the Regulations") made under the Act, and:

"approved" means approved by GBT;

"banknote acceptor" or "bill acceptor" or "bill validator" or "note acceptor" means a device that is fitted with photo-optic and other sensors (internal or external to the device) and that is used to accept and validate paper or plastic legal tender or approved coupons. Where reference is made to a "bill acceptor system", this is intended to include all bill handling components, whereas "bill validator system" refers to the validator unit and its sub-components, excluding other parts of the handling system;

"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 GD, whether the GD pays credits from the hopper, by electronic transaction or by issuing a ticket;

"central electronic monitoring system" or "central monitoring system" or "monitoring and control system" means a host, data controller unit, bank controller and communications interface to each gaming device and the connections between them intended to receive data from or send data to a relevant gaming device or central system where such data relates to the security, accounting or operation of the relevant gaming device, the central system or any games or features played on, or associated with, the relevant gaming device; and to perform such other functions as may be determined by GBT from time to time. It is an electronic system or a computer system to which relevant gaming devices may be connected directly or indirectly, and which is designed or adapted for use to:

(1) register all or part of the gaming taking place through such relevant gaming device; and, or

(2) supervise all or part of the operations carried out in or through such relevant gaming device; and, or

(3) to store and provide reports and information on the aforesaid matters;

"certification authority" means authority appointed to certify all gaming devices (GDs), both hardware and software;

"coin acceptance device" means a coin input devices, together with the coin validator, photo-optic sensors (internal or external to the validator) and any additional devices used to accept and validate a coin;

"coin dispensing device" means a device, together with coin storage mechanism (for example, hopper or tubes), photo-optic and other sensors (internal or external to the device) and any other devices and pathways used to pay out coins to the player;

"critical data" means data contained in critical memory as follows:

(1) all metering required by these Standards;

(2) GD or game configuration data (or both);

(3) information that pertains to the last five games (including the current game, if incomplete);

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

(5) current credits; and

(6) information regarding any significant events;

“critical memory” means memory locations for storing critical data;

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

“game” means combination of events, including player interaction with the GD, 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.

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

"gaming machine" or "slot machine" means a machine with which the player interacts for the purpose of gaming;

"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 GD is powered up, but is not active in the execution of a game, a test routine, an audit, a calibration, or a data interchange with an external device;

"jackpot" means award, in excess of the maximum prize as specified on a game's paytable that is available to be won by a player as a result of activity on a GD

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

"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 or the GD;

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

"maximum stake" means maximum bet or wager that is permissible in terms of legislation;

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

"multigame" means more than one game type offered by the gaming software on a single GD;

"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);

"read-only access" means type of access for data or files that permits opening, viewing, printing, copying, downloading and any other such function, however, it does not permit any change to such data or file;

"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;

"site data logger" means on-site or intermediate data collector for a monitoring and control system includes data collection units contained within, or as part of, GDs;

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

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

"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 GD might display this value in credits or monetary value.

4. Abbreviations

a.c. alternating current

AM	Amplitude Modulation
ARQ	automatic retry query
BCD	binary coded decimal
CA	certification authority
CAD	coin acceptance device
CDD	coin dispensing device
CEMS	central electronic monitoring system
CLI	calling line identification
CPU	central processing unit
CRC	cyclic redundancy check
EMI	electromagnetic interference
EPROM	erasable programmable read-only memory
GBT	Gaming Board of Tanzania
GD	gaming device
GM	gaming machine
GPS	Global Positioning System
I/O	input/output
ITE	information technology equipment
ISDN	integrated services digital network
km	kilometers
LAN	local area network
MAC	message authentication code
NAK	negative acknowledgement

PCB	printed circuit board
PLD	programmable logic device
PSTN	public switched telephone network
RAM	random access memory
RNG	random number generator
ROM	read-only memory
TL	test laboratory
WORM	write-once read-many

PART II

GENERAL REQUIREMENTS

5. Documentation

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

(2) The operating manual shall accurately depict the use of the GD 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 GD 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 GD.

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

(5) Documentation of the protocol shall clearly explain all messages, conventions, definitions, data formats, etc., used in that protocol.

(6) The protocol documentation shall clearly state the data formats that shall be used for all data components used. Examples of areas that shall be specified are:

(a) Byte order for data that contain more than one byte. This shall be specified as either Big Endian / Motorola / Left to Right or Little Endian / Intel / Right to Left.

(b) Bit order where bits are referenced. There shall be an indication whether bit numbering starts from 0 or 1 and whether it runs from left to right or right to left.

(c) Negative number format, where used, shall be specified (e.g. ones complement, twos complement).

(d) String definition shall be specified including:

(i) string termination indication (e.g. ending null or preceding length byte);

(ii) string maximum lengths; and

(iii) padding techniques, if any, for strings less than the maximum length.

(e) Special characters, including escape sequences. If used, each character or sequence shall be clearly identified as to its function (e.g. formatting or font sequences).

6. Enclosure identification

(1) The GD 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) a unique serial number; and

(c) the date of manufacture.

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

(3) Each external key switch of the gaming equipment enclosure, switches and player buttons shall be labelled, either according to its function or to the series of events initiated by its activation. If a key lock initiates some kind of user activity other than simply unlocking a door, then its function shall be labelled (e.g. if a key lock turns one way to enter audit mode, and turns the opposite way to enter cancel credit mode, then both directions shall be labelled accordingly).

7. Enclosure construction

(1) The enclosure shall be of a sturdy construction with a locking system that resists the kind of unauthorized entry that the GD 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 GD is likely to be subjected in a gaming venue.

(2) Areas 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 (e.g. buttons and handles) on the enclosure that are accessible to patrons or staff, and all attachments to the enclosure (e.g. labels and identification plates) shall be sufficiently robust to prevent their unauthorized removal.

(4) Door support devices shall be of construction solid enough to prevent sagging of the door and any problems with door sensor alignment.

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

(6) Hinge centre pins, if used, shall not be able to be removed without leaving evidence of tampering.

8. Enclosure security

(1) Where holes, gaps or slots exist in the exterior of a secure area, there shall be sufficient protection to ensure that the insertion of foreign objects shall not compromise the security or safety of that secure area.

(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) When the door of the GD is shut, it shall not be possible to insert any object into the GD in such a way that the access detection sensor is disabled.

(3) The access 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 alarm door open condition (e.g. by bumping the door).

(5) If the access detection system is disconnected, the gaming equipment shall interpret this action as the door having been opened.

(6) The GM shall deactivate game play upon the opening of a door but may immediately reactivate when the door is closed, unless it has noticed the changing of counters or insertion of coins while this door is open, which is deemed to be interference and precludes automatic reactivation unless the GM was placed in test mode. In such case a significant event message shall be sent and the CEMS shall add the staff card number to the event message. If no card number is available, the message shall be tagged by the CEMS as an unauthorized access.

PART III

ELECTRICAL REQUIREMENTS

10. Enclosure wiring

(1) The GD (and any associated equipment as determined by legislation) shall comply with the compulsory Standards for safety of electrical and electronic equipment.

(2) All connectors and wires shall be easily identifiable, both in the GD itself and on the circuit diagrams in the manuals.

11. Electromagnetic compatibility

(1) Electromagnetic interference

The GD 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 GD 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 GD shall not have its security properties changed by the application of a magnetic interference level to the GD. When tested the GD shall withstand a magnetic field that alternates at 50 Hz or 60 Hz and that have amplitude of 1 A/m. The GD 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 GD.

(b) Immunity to impulse magnetic field: A GD shall not have its security properties changed by the application of a magnetic interference level to the GD. The GD 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 GD.

(4) Temporary electrostatic disruption

When the GD is tested at a level of 8 kV for air discharge and 4 kV for contact discharge:

(a) 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 GD; and

(b) there shall be no abnormal payout from a CDD.

(5) Fast transient voltage

(a) The GD shall employ sufficient power supply filtering to prevent disruption to the device when the GD 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 GD 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 GD.

(6) Surge voltage

The GD 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 GD 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 GD.

(7) Long-term voltage level change

GDs shall operate normally during voltage changes within the legislated supply variations with which utility companies are required to comply (typically 10% above and 10% below the nominal 230 V). When tested in accordance with the following procedures, the GD 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 GD:

(a) Connect the gaming equipment to a variable voltage power supply. Set the supply voltage to 1.10 times the rated value and operate the gaming equipment for 15 min. Check for compliance.

(b) Repeat the test with the supply voltage set to 0.90 times the rated value. Check for compliance.

(8) Surges and sags of voltage

The GD shall employ 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. When tested in accordance with the following procedures, the GD shall exhibit a capacity to recover or reset and complete any interrupted play or data collection without loss or corruption of any control or data information associated with the GD:

(a) connect the GD 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 s and return rapidly to the rated voltage; and

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

It is acceptable for the GD to reset, provided that no damage to the equipment or loss or corruption of the data is experienced.

12. 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 GD shall be able to operate from a 230 V, 50 Hz main power source, which might deviate 10% above and below nominal voltage and 1% above and below nominal frequency.

(3) Where a GD 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

13. Random access memory (RAM)

(1) GD RAM data storage shall be capable of reliably preserving its memory contents for at least 72 hours with the mains power switched off.

(2) When the battery is at or below its 72 hours capacity limit, the GD shall automatically generate a type 4 significant event message to the monitoring and control system and disable itself. It shall not be possible to reset the GD until the battery capacity has increased above the 72 hours 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 hours.

(3) RAM clears of the GD shall not be possible except by accessing the logic area in which the RAM is housed.

(4) In a GD, batteries shall be secured and connected to the board(s) that contain RAM such that the batteries cannot be easily disconnected.

14. 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 GD 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 the monitoring and control system:

(a) all auditing meters;

(b) current credits;

(c) GD or game configuration data (for example, GD address, denomination); and

(d) significant event information.

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

15. 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 GD to fail to comply with these Standards or with legislation shall not be contained within the GD. This includes EPROMs that have a range of parameters that are used for setting up the device.

16. Programmable logical elements

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

17. Circuit boards

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

18. Switches and jumpers

(1) If switches or jumpers that have the potential to cause the GD 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 GD to enter "Tilt" mode, which in turn shall be signalled to the monitoring and control system. As long as the switch or jumper is set in this manner, it shall not be possible to reset the GD.

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

19. Communication

(1) Where multiple GDs communicate over a single multi-drop transmission medium, each GD 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) Gaming equipment 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.

20. Video monitors and touch screens

Where fitted, video monitors shall not present a hazard.

21. Global Positioning System (GPS)

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

(2) The GPS device will send location coordinates to CEMS not less than every 1 hour.

(3) The GPS coordinates shall be of accuracy of not more than 100 meters.

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

(5) During registration or installation of GD, the GPS coordinated recorded will be considered as the original GPS coordinates of the GD.

(6) GD should send type 3 significant event to the CEMS whenever the GD is outside the radius of 2km from the original GPS coordinates that was captured during device registration and/or installation.

22. Printers (if applicable)

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

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

PART V

SOFTWARE REQUIREMENTS

23. General

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

(a) module name;

(b) version number;

(c) revision number; and

(d) description of functions performed.

(2) 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.

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

(4) All program source codes for site data loggers shall be made available for examination by the TL.

24. Verification of source code compilation

(1) The party that submits software shall provide the wherewithal 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 GD submitted for certification.

(2) When compiled, all source code supplied to the TL shall generate object code that is exactly the same as that installed in the GD.

(3) 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 (e.g. if a particular compiler option is set or not set).

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

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

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

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

(a) All logical copies of critical memory shall be recreated using the good logical critical memory as a source.

(b) 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.

25. Validity checks

(1) 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. Critical memory storage shall be maintained by a methodology that enables errors to be identified and acted upon. This methodology may involve signatures, or checksums, or partial checksums, or multiple copies, or timestamps or the effective use of validity codes (or any combination of these). RAM and program storage device space that is not critical to GD security need not be validated.

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

(3) If a validity check fails, the software shall act in accordance with the requirements for error event handling.

(4) So as not to complicate the validation of software, all individual device-specific information (e.g. GD identification number or address, venue name and touch screen calibration) and all device group specific information (e.g. jackpot configuration/parameters) shall be stored separately from any common information (i.e. common to all GDs 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 may be included on the game software storage device (e.g. EPROM or CD) make it impossible to obtain a signature that is common to all devices.

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

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

(b) unrecoverable memory corruption.

(6) A validity check of GD critical memory shall be undertaken at least after every restart of the device or transaction of significance (e.g. logic door closed, door closed, parameter change or reconfiguration). After a device restart (e.g. power off and on), the device shall complete its validity check of the critical memory area and then perform a comparison check of all good logical copies of critical memory.??

26. Critical memory

(1) To cater for disruptions that occur during the update process of critical memory, at any point in time during an update there shall exist sufficient information that allows the software to fully cater for such disruptions (e.g. the software shall be able to identify the state of each copy of critical memory and recover from the most appropriate good copy to complete the update in each case of a disruption).

(2) 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).

(3) When updating meters in critical memory, the software shall ensure that errors in one logical copy of the meters are not propagated through to other good copies.

27. Program memory

(1) Labelling

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

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

(b) name of manufacturer;

(c) development number or variation;

(d) version number;

(e) type and size of media; and (if applicable)

(f) location in GD (if critical, e.g. socket position 3 on PCB).

(2) Read/write storage

(a) 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.

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

(3) Read/write storage media

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

(b) A read/write storage device (e.g. 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.

(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/files on the storage device.

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

(e) The method of loading programs to the storage media (e.g. disk file transfer or down-line load) shall be certified by the CA.

(4) Flash memory devices

If permitted by GBT, the downloading of program data to reprogrammable memory program storage devices by means of the monitoring and control system shall be protected from unauthorized reading, erasure or copying.

(5) Loading programs to flash memory devices

(a) If the downloading of programs into a reprogrammable memory device by means of the monitoring and control system is permitted by GBT, the method of doing so and of verifying such programs shall be evaluated by the TL and certified by the CA.

(b) A reprogrammable memory device shall be protected from unauthorized modification which shall be permitted only once appropriate security measures are satisfied (e.g. if a high voltage chip that allows modification of the reprogrammable memory devices is installed on the PCB).

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

(f) The use of jumpers or similar devices can be used to enable/disable erasure/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 GD shall not be able to enter "Play" mode. These jumpers shall be located within the logic area of the GD.

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

(h) Any unauthorized access to the contents of a reprogrammable memory device through erasure, writing to the contents, and so on, shall result in an event that shall be stored in non-volatile memory in the same way that a "door open" event is stored. Clearance of the event shall not be possible other than under the control of the GD hardware and software.

(6) WORM storage devices

(a) A WORM (e.g. 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/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/files on the WORM (e.g. inserting a CD-ROM in another PC which then conducts a full signature check and directory search check over the CD-ROM space).

(d) Old approved versions of programs may be held on a WORM. However, it shall be possible to clearly identify which files belong to which version of the program.

28. 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).

PART VI

SYSTEM FUNCTIONAL REQUIREMENTS

29. Auditing information

A program shall be available that lists all the registered users on the system and the privilege level of each one.

30. Cashout by printed ticket

A ticket request shall be rejected by the system if the device that generates the ticket security feature is not able to issue such a feature and the system shall initiate the appropriate error handling procedure.

A security feature includes any mark, attribute or element (e.g. a ticket number) that is added or attached to the ticket in order to allow the ticket to be validated.

31. Clocks

(1) There shall be an internal clock in the host that reflects the current time and date. The time of the clock shall be maintained to an accuracy better than 0.5 seconds over a 24 hour period.

(2) The clock shall be used at least for the following purposes:

(a) time stamping of significant events;

(b) time stamping of player transactions such as credit transfer to/from a GD;

(c) time stamping of configuration changes; and

(d) ticket issuing transactions.

(3) The site data logger shall have a means of synchronizing its time and date with the system's clock.

(4) The host shall be able to update all clocks in intermediary devices attached to the system. Individual GMs are not required to have clocks.

(5) The host shall be able to update its own internal clock(s).

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

(7) The only acceptable all-numeric date format is dd-mm-yyyy.

(8) Only 24-hour time formats are acceptable.

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

(10) A site data logger's clock shall not be inaccurate by any more than 0.5 seconds over a 24 hour period.

(11) GDs shall operate and communicate correctly, and handle date and time rollovers including leap years.

32. Electronic funds transactions

In a system that supports electronic funds transactions the following shall apply:

(1) storage of electronic funds on the system shall be secured against invalid access or update by means of, at least, a password;

(2) all electronic funds transactions shall be maintained in a system log;

(3) inactive accounts reflecting moneys held in the system shall be protected against all forms of illicit access or removal by means of, at least, a password;

(4) all electronic funds transaction shall be treated as vital information to be recovered by the system after failure; and

(5) all electronic funds transactions shall be correctly updated to the storage media and the system.

33. Central logging of information

(1) Game play statistics, game play meter information, machine event data and machine configuration data (including configured games where applicable), as defined in the standards for the applicable GD, shall be held for each individual GD in the host for at least the current and previous year. This data may also be held in intermediate points in the monitoring system.

(2) The units in which each statistic is measured shall be certified by the CA.

(3) Provision shall be made on the host to log all significant events that are described in clause 11.

(4) Calculated return to player statistics for each game shall be able to be maintained for at least the current and previous year.

(5) Where a GD is unable to operate without the loss of any information (e.g. metering, transactions or significant events) it shall immediately disable any further game play.

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

(7) All accounting and security event data shall be held and be able to be accessed or retrieved from back-up storage; it shall be possible to store backed-up data for at least five years.

(8) Accounting and security event data shall be held for each individual GD as well as accumulated for each venue.

34. Control of gaming equipment

(1) The host shall provide an interrogation program that enables comprehensive on-line searching of the significant event log for at least the current year and the previous year. The interrogation program shall be able to do a search based at least on the following:

(a) date and time range;

(b) GD unique ID number;

(c) venue number; and

(d) significant event number(s).

(2) There may be a need to log onto the computer to execute external audit and interrogation programs. The password that GBT's staff uses shall give them read-only access to all data; (i.e. they shall have no ability to change anything on the production system whatsoever). However, there should be sufficient

space available to enable GBT's inspector to write a data file or report on the read-only information.

(3) The host shall provide read-only access for GBT's staff to perform the following tasks, where appropriate:

(a) determine operational software revision;

(b) view downloadable software percentage variations and games, where applicable;

(c) perform signature checks;

(d) verify that GDs and other equipment are operational; and

(e) ??? any other information that will be required by GBT from time to time.

(4) If a GM loses communication with its site data logger, the GM shall disable itself.

(5) A site data controller that has not transferred its summary meter and significant event data to the host for a period of longer than 72 hours shall automatically disable connected GMs, but shall be able to continue data collection thereafter.

(6) The CEMS shall have provision for unique GD addresses (ID numbers) to allow each GD to be individually and uniquely identified to the CEMS.

(7) If the site data logger goes off-line 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 not pay them out (i.e. it shall not permit a cashout), but shall retain them until re-enabled when the site data logger comes back on line.

The recommended practice in this situation is for the site owner to pay the player and collect the credits when the machine comes on-line again.

(8) If the site data logger instructs the GM to disable (e.g. 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).

(9) The host shall be able to enable and disable game play at any of the connected GMs at any time.

(10) The host shall be able to implement the automatic shutdown of connected GMs on a time schedule basis. The schedule shall cater for different operating hours on a daily basis and also for special occasions such as public holidays.

(11) If multigames are permitted by GBT, there shall be a method available so that it is possible to disable and enable individual games on multigame GMs. If it is not possible to accomplish individual game enable and disable, the entire machine shall be capable of being enabled or disabled.

35. Back-ups and recovery

(1) In the event of a failure whereby the host cannot be restarted in any other way, it shall be possible to reload the database from the last back-up point (e.g. the previous night) and fully recover at least all of the following vital transactions:

(a) significant events;

(b) tickets generated or redeemed (or both), including current account balances;

(c) account information including winnings, bets, cash deposits and cash withdrawals, PIN changes, expiry date and site where issued;

(d) manual database updates;

(e) operator network reconfiguration, including addition of gaming equipment, deletion of gaming equipment, modification of gaming equipment (e.g. card to coin, different denominations, new games), addition of sites, deletion of sites and line swapping;

(f) meter statistics; and

(g) current system encryption keys.

(2) There shall be at least two physical copies of each data file and system database on the host.

(3) Backups of the system shall be able to be made on at least a daily basis. Mirrored disk copies are not adequate for these backups where the "mirrors" are controlled by the same CPU.

36. Encryption of stored data

(1) Storage of PINs or passwords (or both) on the system and site data logger shall be in an encrypted, non-reversible form. A person who reads the file that stores the PIN or password data (or both), should not be able to reconstruct the PIN or password (or both) from that data, even if he/she knows the creation algorithm.

(2) The following information classes shall be encrypted (reversible) for storage for recovery purposes:

(a) encryption/decryption keys; and

(b) seed information (for signature or RNG) that is not logically stored in a password protected area of the highest access level.

(3) All communication between the host and the site data logger shall be encrypted. However, in order to cater for situations when difficulties with communication are encountered that make encryption undesirable, a password-protected and secure function to disable encryption is permissible. The method of disabling and the procedure to be followed shall be certified by the CA.

Examples of information that require encryption include:

(a) RNG seeds;

(b) signature seeds (algorithm coefficients);

(c) signature results;

(d) encryption keys, where the implementation chosen requires transmission of keys;

(e) PINs;

(f) passwords;

(g) software uploads and downloads of any security related software (e.g. signature and RNG);

(h) transfers of money to/from player accounts;

(i) transfer of money between GDs; and

(j) parameters, configuration and win messages.

(4) The encryption algorithm, its implementation and operational procedures that pertain shall be certified by the CA. The following are encryption characteristics that shall be considered:

(a) Encryption algorithms shall be demonstrably secure against cryptanalytic attacks.

(b) The minimum width (size) for encryption keys is 64 bits.

(c) A secure method shall be used for changing the current encryption key set, for example public key encryption techniques to transfer new key sets. The current key set shall not be used to "encrypt" the next set.

(d) There shall be a secure method of verification that only approved devices are communicating with the system and vice versa. This requirement especially applies to communication methods that use public networks, including but not limited to:

(i) dial-up modems;

(ii) cellular networks; and

(iii) ISDNs.

(5) When requested, documentation and development tools shall be supplied to:

(a) the TL and the CA; and

(b) all manufacturers and suppliers of GDs and other gaming equipment that need to interface with the protocol.

37. Handling of master resets

(1) The host shall be able to identify and properly handle the situation where master resets havebeen performed.

(2) The monitoring and control system shall be able to determine the last valid meter readings that were stored within the specific GDs before the master reset occurred.

(3) The system shall perform reasonableness checks against the meter values that were last recorded automatically in order to highlight discrepancies.

38. Recording of game play statistics

The system shall be capable of recording and storing statistics of significant events and game play activity as required by legislation.

39. Recording of significant events

Significant events (as detailed in clause 11) shall be automatically logged by the system as they occur. The format used for the storage of the significant event data shall include the following:

(1) The date and time of the event.

(2) The identity of the GD that generated the event.

(3) The venue number or name, in cases where the system controls multiple gaming venues.

(4) A unique code that defines the event. GBT shall be provided with a valid and current list and a description of all event codes. The codes may be text or numerals, and shall include a brief text that describes the event in English.

40. Security of the significant event log

The system shall resist unauthorized access to or tampering with the significant events data file(s) by at least the following strategies:

(1) access to the significant events data file(s) shall be read-only and restricted by password security;

(2) the only valid method of writing to the significant events data file in the system software shall be output sequential, i.e. no random update methods are permitted; and

(3) it is mandatory that the event data file and software shall be so structured that it is not possible for unauthorized modifications to remain undetected.

41. Storage of the significant event log

(1) The specific significant events prescribed by GBT, regardless of the source of these events, shall be stored at the central point or intermediate points of the system. All the significant events shall be stored on disk in a file (or files).

(2) It shall be possible to retrieve events in a chronological order.

(3) These events may also be stored in subsidiary points of the monitoring system (e.g. GDs, local controllers, remote controller and regional computers).

(4) When communications are established to the host, for example by means of a site dial-up, all events queued in GDs shall be forwarded to the host.

42. System security requirements

(1) The host and site data logger of the monitoring system shall provide for security against illegal or unauthorized access.

(2) Where PINs and passwords are used they shall be able to be changed periodically.

43. Permitted devices

The host shall not transfer data to or gather data from any GD attached to the network unless the legitimacy of that device has been established.

44. Metering

The host shall be capable of gathering metering data once every 24 hours from the site data logger(s).

45. Permitted software

Only programs and data files certified by the CA and approved by GBT may be stored or used (or both) on the host. The operating system on which the CEMS

operates shall be approved and shall form part of the certification documentation. The TL shall be supplied with a copy (on a removable digital storage medium) of all fixed files (i.e. not temporary scratchpad files) and programs on the host. The following items shall be included:

(1) operating system programs;

(2) applications programs;

(3) fixed data files; and

(4) software signature seeds, where applicable.

46. Communication with GMs

The host shall be able to communicate with the site data logger at any specific venue, or with the individual GMs (or both)

(1) on a time schedule basis, and

(2) on command, via the CEMS.

47. Reactivation of game play

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

(1) If a door open event occurs other than a logic door open, the GM may reactivate automatically when the door is eventually closed.

(2) If the PIN retry limit is exceeded for a player's account card, the GM shall remain deactivated until the card is removed.

(3) If the power supply to a GM fails, the GM is deactivated as a matter of course. It is permitted for the GM to automatically reactivate itself unless it determines that the logic door(s) has(have) been opened while the power was down, in which case the GM shall remain deactivated until manually reactivated.

Such reactivation should only occur after GBT audit procedures have been satisfactorily completed.

The venue operator may choose to require manual reactivation in both cases.

(4) If a GM is automatically deactivated at the end of the venue's current session it is permissible for the monitoring and control system to automatically reactivate the GM when the next permitted session starts.

(5) If the GM is deactivated after losing communication with its site data logger, it may reactivate as soon as communication is restored, unless its logic door(s) has(have) been opened while communication was lost.

48. Signatures

(1) The host and site data logger shall have the ability to request a GM to calculate a signature value, which is a function of the GD program memory. This calculation shall use variable parameters passed to the GM by the host or site data logger so that the GM cannot be programmed to return the same correct answer every time.

(2) Signature checking for GMs shall take place in response to type 4 significant events.

(3) The signature algorithm used by the monitoring system is subject to certification by the CA and shall comply with the following requirements:

(a) the algorithm shall be a function of the entire range of the GD program memory and fixed data;

(b) the signature algorithm shall detect at least 99,995 % of all possible data errors;

(c) the algorithm shall combine the bits in a complicated and cross-interactive way, for example, the CRC method; the use of primitive techniques such as parity or simple checksum is inadequate;

(d) the algorithm shall produce a result of at least 16 bits in width;

(e) the seed information shall be at least 16 bits in length; and

(f) the seed information shall influence the behaviour of the algorithm in a non-trivial way, to the satisfaction of the CA.

49. Transaction logging

The site data logger shall record with time and date stamp all vital transactions received from GDs, cashier stations, control stations, coin counters and other elements of the CEMS in a log file(s) or database.

50. Site data logger device

Where the system utilizes a site data logger as part of the communications environment, the interface for the venue employee shall comply with these Standards.

51. Cashout while disabled – Non-permitted occasions

A GD shall not permit a cashout to be performed during any of the following conditions:

(1) during game play;

(2) while the GD is in demonstration, test or audit mode; and

(3) while the GD is in a fault condition that requires manual activation.

Manual reactivation implies that the GD is reactivated for game play before the cashout is permitted.

PART VII

COMMUNICATION REQUIREMENTS

52. General

(1) This clause refers to requirements and principles that apply to communication within a system's network. It primarily refers to communication by the system or its components with a GD, but also applies to communication between other components or devices (or both) that form part of the system.

(2) The generic term "protocol" shall be deemed to include the hardware interface, the line discipline and the message formats of the communication.

(3) Where electronic data communication is used by the system, complete documentation of the network structure, message formats and protocols proposed shall be submitted to the TL for evaluation. The following shall apply:

(a) All electronic data communication shall be protocol based and incorporate an error detection and correction scheme.

(b) All electronic data communication shall ensure that the data passed between nodes are verified for accuracy and completeness. The methodology used shall be fully documented for review by the TL and certification by the CA.

(c) All electronic data communication interfaces shall be constructed and so finished as not to create a safety hazard or create a risk of injury.

(d) All electronic data communication over the PSTN, dedicated leased lines supplied by the telecommunications company, or private lines deemed by the TL to warrant data security, shall employ encryption. The encryption algorithm shall employ variable keys.

(e) Signature verification of all venue equipment software shall be initiated by a separate component of the central monitoring and control system.

(f) Game play statistics information and event data shall be passed to the system by an approved electronic data communications means in a timely manner by schedule or on demand (or both).

53. Cellular network communication

The following requirements apply if an user/operator intends to use a cellular network, or the equivalent, for dial-up communication between the system and some or all of the remote venues.

(1) Each site that will use cellular communication shall have one or more defined clear paths to a cellular relay within range.

(2) Messages shall be encrypted.

(3) A method shall be provided to verify that the system is communicating with the correct venue, and vice versa, if required. CLI is not considered adequate for this purpose.

(4) The time to complete daily polling of GDs/venues over a cellular network shall be such that it shall be possible to conduct a poll for the entire network daily. Thus the time to complete polling of a venue using cellular communication should not be substantially longer than through standard modem dial-up.

PART VIII

DATA COMMUNICATION REQUIREMENTS

54. Remote control of GMs

Only control functions of GDs that have been approved may be implemented. These control functions shall be clearly specified in the protocol documentation. It shall not be possible to change the outcome of a game by means of the communication system.

55. Communication failure and recovery

All GDs shall be able to handle the following range of failures without loss of data:

(1) failure of central computer LAN interfaces;

(2) failure of the central LAN;

(3) failure of central data communication interface devices;

(4) failure of single data communication interface;

(5) high data communication error rates on line;

(6) a foreign or additional device placed on a LAN;

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

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

(9) LAN failure on regional or local controller (if any);

(10) LAN failure on cashier terminal (if any); and

(11) data communication interface failure on a GD.

56. Accuracy of communication speed

Where a user/operator requires communication to be implemented, such that more than one GD may communicate using the same transmission medium, each GD 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).

57. Error detection

(1) The low level communication protocol shall cater for sophisticated error detection (e.g. by using CRCs). Vertical parity or simple checksum byte (logical or arithmetic sum) (or both) are not acceptable error detection schemes.

(2) The data communication shall be able to withstand varying error rates from low to high. Data communication error generators might be used by the TL to verify this requirement.

(3) All levels of the protocol shall be able to detect and discard duplicate messages unless full functionality of the system can be guaranteed otherwise.

(4) Where critical data and information (e.g. credits, metering information and information that pertain to a game outcome) are transferred between microcontrollers, an error check shall be done on the transferral. This check shall be at least a CRC. Parity checking or simple check sums are not adequate.

(5) Where any data (e.g. credits, metering information, activation/de-activation commands, information that pertains to a game outcome and error events) are transferred between a GD and an external device, such as components of a monitoring and control system, an error detection and correction system shall be employed. Data errors shall be detectable to a minimum accuracy of 99.995 %.

58. Error detection and recovery

All protocols shall use communication techniques that have proper error detection and recovery functions. Output-only pulse based or "wiring harness" interfaces are not acceptable.

59. Message recovery

The low level protocol shall cater for recovery of messages when they are received in error or not received at all. The following requirements apply:

(1) There shall be positive acknowledgement of all good data messages of a critical nature received.

(2) If multiple messages have been sent it shall be clear which messages are being positively acknowledged.

(3) Messages received in error shall initiate ARQ functions. Implementations may include NAK of messages received in error, window rotation schemes, timeout recovery, etc.

(4) Secure messages (e.g. credit transfer, significant events and signature results) shall not use the "broadcast" interfaces. The above requirements are not applicable to broadcast or unconfirmed message types.

60. Flow control

(1) The low level protocol shall implement a method of flow control to enable the GM and its host/site data logger interface to slow down or temporarily halt the message flow from its partner at certain instances, unless full functionality of the system can be guaranteed.

(2) Events may be queued at intermediate points of the system (e.g. in a site data logger) or in the originating device (e.g. the GM).

(3) The host shall be capable of gathering significant event data from the site data logger once every 24 hours.

(4) If the GM is unable to send messages to the monitoring and control system 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 monitoring and control system.

61. Protocol

(1) The CA shall certify the message formats used for data communication.

(2) The adequacy of documentation, which is intended for distribution to suppliers for developing interfaces to the monitoring and control system by means of the chosen protocol, shall be assessed by the TL.

(3) The CA shall certify a protocol only if the devices that implement the protocol are able to comply with the requirements of these Standards.

62. Higher level protocol

The following are characteristics that shall apply to the higher level communication protocol:

(1) there shall be no restrictions placed on characters that might be included in messages passed to or from the higher to lower level;

(2) the interface shall cater for messages of variable length, including those longer than the standard buffer size of the lower level; and

(3) a method of flow control shall be implemented to prevent loss of vital messages.

63. Layered protocol

(1) The protocol shall be layered such that there are a minimum of two layers specified (i.e. low level and application level layers are a minimum requirement).

(2) Each layer shall not be dependent upon each other for recovery of errors (e.g. the lowest level protocol shall not count on higher levels to resolve all communication errors).

(3) Each layer shall cater for the possible loss of messages when restarts or other such events occur from one end or the other.

64. Message authentication in low level communication

Unless full encryption is used on all messages, MACs shall be used with key message types, such as metering, to enable the system to determine when invalid

modification to such messages has taken place. Use of MACs may be considered as an alternative to encryption for all but the most secure message types (e.g. password transmission).

65. Message framing in low level communication

(1) The low level communication protocol shall provide a clear and precise method of framing messages so that there is no chance of a partial message being acted upon by the receiver.

(2) If the framing method involves the use of unique starting or ending characters (or both), a method of "transparency" shall be implemented so that these characters can be sent as part of the data component of the message, and not interpreted as control characters. This requirement applies both to data and error detection sequences such as CRCs.

66. Multi-dropping

(1) Multi-dropping capability is required for all protocols that communicate with GMs except those systems that use a single or dedicated communication interface for each GM.

(2) Multi-dropping of multiple GDs on a single communication line is acceptable provided that:

(a) a unique method of identifying/addressing each legitimate component on the line is provided, either static or dynamic;

(b) adequate timeout facilities are provided;

(c) a method of identification and rejection of illegitimate components exists;

(d) a method is present to prevent or reduce the risk of simultaneous transmissions by the multidropped equipment (appropriate methods are polling, collision detection with random back-off restart times, token ring, etc.);

(e) the hardware interface requirements are met;

(f) adequate controls exist to prevent communication stoppage due to deadlock; and

(g) if the transmission speed is determined by a communication port of the device (e.g. for asynchronous transmission), the protocol shall specify a maximum transmission speed (baud rate) tolerance within which devices shall operate in order to prevent deterioration of the performance of the line.

67. Period meters

If the system uses period meters (e.g. for performing cash or banknote clearances), these may only be cleared after a master reset or upon activation of some planned, external intervention (e.g. a drop box door open signal or a cash clearance signal).

68. Software meters

(1) The following requirements for the protocol exist for meters implemented in the software:

(a) the protocol shall clearly state the method of storage for each kind of meter (e.g. binary and BCD);

(b) the protocol shall clearly state the unit measure for each meter (e.g. cents or counter); and

(c) the protocol shall provide for sufficient width to ensure that no overflow can occur without its being noticed by the monitoring system.

(2) Meters forwarded by a GD shall always be reconcilable relative to the other meters. For example, this might require an appropriate locking mechanism to prevent imbalances during such events as game play, money in and money out.

69. Restart/recovery

The following are requirements for the restarting or recovery of communication messages:

(1) the higher level protocol shall employ technique(s) (e.g. end to end acknowledgement) such that it shall not lose messages, regardless of whether the higher or lower level restarts communication; and

(2) the higher level protocol shall employ technique(s) (e.g. transmission numbers), such that repeated messages are identified and discarded, even when one end or the other restarts.

These requirements do not apply to unsecured messages (e.g. broadcast messages).

70. Simulator

If a simulator is provided to enable development of the protocol in GDs and other gaming equipment that interface with the protocol and assist in the testing of the GDs by other suppliers, the TL and the CA, then the simulator shall:

(1) adequately support and execute all transactions and message types that are used by the protocol;

(2) have a function to thoroughly check every requirement, behaviour, function or feature the protocol dictates;

(3) run on standard, freely available equipment such as a personal computer or the equivalent; alternatively, the supplier shall loan, on request, suitable hardware on which the simulator can operate to suppliers of GDs, provided that such suppliers are licensed by GBT;

(4) be provided, together with all relevant documentation, on request to all suppliers of GDs; and

(5) be provided, together with all relevant documentation, to the TL and CA free of charge.

PART IX

SIGNIFICANT EVENTS REQUIREMENTS

71. 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 GD shall detect and record an event, the GD 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) This clause provides a summary of the significant events that are specified by the CA or GBT. 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 GD shall cause a clearly displayed message that an event has occurred and, unless otherwise indicated, shall also result in the following:

(a) all player inputs shall be disabled, including coin and banknote input;

(b) an identifiable alarm shall be activated, which may be either a tower light, or a sound of at least 1,5 s duration (or both);

(c) any game result shall be saved; the reels or video display shall not display a false game outcome; and

(d) if the GD was in CDD payout, the CDD shall be turned off and the brake applied.

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

(a) any messages shall be removed;

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

(c) the alarm shall be turned off; and

(d) any game play when the fault event occurred shall restart from the beginning of the play or from the point at which the interruption occurred and conclude normally, using the data that were saved previously.

(8) Generic significant events are applicable to all GDs 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 GD fault conditions shall activate an alarm, which shall include either a tower light or sound (or both).

(10) An alarm shall be raised for any of the following banknote acceptor specific conditions, unless done by staff authorized to do so and in accordance with an approved procedure:

(a) opening of the banknote acceptor area outer door (if separate from the GD main door); or

(b) opening of the banknote storage area door.

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

72. Gaming Device and terminal events

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

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

It is acceptable if the GD only detects the changes when restarting.

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

(3) Error detected in hardware or software (type 4): Failure of internal test.

It is understood that failure of some test(s) means that the GD cannot function, in which case it shall disable itself immediately.

Excludes hardware input devices that do not influence the game results.

(4) Logic area access (type 4): Opening of the logic area door.

The GD shall detect the opening of the logic area door (or access to the logic area).

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

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

(7) Enter test/audit mode (type 2)

If the GD has a test mode or special staff/audit mode, a significant event shall be signalled when such mode is entered.

(8) Exit test/audit mode (type 2)

If the GD has a test mode or special staff/audit mode, a significant event shall be signalled when such mode is exited.

(9) Coin jam (type 2)

Sensors in the coin path shall indicate when a coin is jamming the path.

(10) "CDD runaway", "coin out tilt" or "extra coin(s) paid" (type 2): One or more coins are improperly paid by the CDD.

(11) General enclosure access (type 2): Opening of outer enclosure door, excluding the drop box door.

This message shall be sent by the GM 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 CEMS 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 CEMS.

(12) 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 CEMS as an unauthorized access.

(13) CDD empty/malfunction (type 2)

(14) Enclosure door closed (type 2)

A sensor registers that a door has been closed.

(15) Cancel credit (type 2)

Any incident of a manual cancel credit (e.g. due to book/handpay) shall indicate a significant event. The value of the credits shall be included in the significant event report.

(16) Coin interference (type 2/R): External interference with a coin/token acceptor or validator.

This refers to coin yo-yo, stringing, etc.

(17) Reel error (type 2): A reel position does not agree with software control.

(18) Collect credit (type 1): Cashout that exceeds the limit specified by legislation.

(19) Banknote receptacle is removed (if the banknote storage area uses a receptacle) (type 2)

The GD shall automatically disable itself, after reporting the event to the monitoring and control system.

(20) Communication failure (type 2/R): Failure of communication link between GD and the next point in the monitoring system.

Failure is defined as the inability to send messages to or, where applicable, to receive messages from the monitoring and control system.

(21) Printer failure (type 2)

The software shall register and react to any printer fault conditions, and shall allow the machine to complete the printing of the current ticket and then pause printing and display an appropriate onscreen message until the problem has been solved and rectified.

(22) Software validation or signature failure (type 4): It is assumed that modification or unauthorized reading (or both) of the contents of the restricted components of the GD or loading of unapproved software (or both) could have occurred.

The GD shall be manually reactivated, after GBT audit procedures (if any) are satisfied.

(23) 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.

(24) Game play deactivated (type 3): Deactivation of game play.

If a significant event has not already been logged (by the system or the GD) when deactivation occurs, the GD shall ensure that such an event is reported to the system as soon as possible. If the GD receives instruction to deactivate from any other part of the monitoring system, it shall deactivate immediately after reporting this deactivation, and shall not reactivate until it is instructed to do so by the system.

(25) Game play activated (type 1): Activation includes reactivation of game play.

Activation and deactivation at normal commencement and conclusion of business require the generation of significant events so that the monitoring system can identify that the GD status has changed. This does not mean that the system shall send a separate message to the central controller of the system for each one of these events. The system may send a message that indicates change of status of several items of the GD as long as the status change events all occur within a period set by legislation.

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

(27) Enter Demonstration Mode (type 2/R)

Where demonstration mode is permitted by legislation, and the GD enters this mode, it shall create and transmit a type 2/R event.

(28) Exit Demonstration Mode (type 2/R)

Where demonstration mode is permitted by legislation, and the GD exits this mode, it shall create and transmit a type 2/R event

(29) Banknote storage area access (type 2): This message is sent by the GM when the banknote storage area is accessed.

When the message is sent, the CEMS 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 CEMS.

This message is intended for use only with GMs where the banknote storage area is external to the main enclosure.

(30) Banknote acceptor mechanism is disconnected (type 1)

(31) User logon/logoff (type 1): A user logs on with a correct password or logs off, from a GD other than a GM.

This event shall be detected and reported to the host or the site data logger as soon as possible but within a maximum of 10 s after restoration of communication.

(32) Logon failure (type 1/R): A user incorrectly enters his/her PIN three consecutive times on a GD other than a GM.

The event shall be detected and reported to the host or the site data logger as soon as possible, but within a maximum of 10 s after restoration of communication.

73. Player/staff cards (if applicable)

(1) Unauthorized staff PIN (type 1/R): Incorrect PIN entered three times consecutively with a staff machine card.

The system shall ensure that the card is blocked from any further use. It is not necessary to disable the GD or the player interface.

(2) Unauthorized player PIN (type 1): Incorrect PIN entered three times consecutively with a player card.

The system shall ensure that the card is blocked from any further use. It is not necessary to disable the GD or the player interface.

(3) Unauthorized card (type 1/R): Use of a stolen or unauthorized staff machine card or player card.

The GD card reader shall not accept an illicit card or a card that is not authorized for use at that specific time.

74. Banknote acceptance (if applicable)

Banknote reject state (type 1): The GD shall report banknote reject events to the monitoring and control system.