ISBN 978-0-626-39022-8

SANS 1718-9:2021

Edition 3

SOUTH AFRICAN NATIONAL STANDARD

Gambling equipment

Part 9: Central monitoring system for limited payout machines

WARNING
This document references other documents normatively.

Published by the South African Bureau of Standards
1 Dr Lategan Road Groenkloof ✉ Private Bag X191 Pretoria 0001
Tel: +27 12 428 7911 Fax: +27 12 344 1568
www.sabs.co.za

This page has been left blank intentionally

COPYRIGHT PROTECTED DOCUMENT

SABS – Standards Division

The objective of the SABS Standards Division is to develop, promote and maintain South African National Standards. This objective is incorporated in the Standards Act, 2008 (Act No. 8 of 2008).

The SABS continuously strives to improve the quality of its products and services and would therefore be grateful if anyone finding an inaccuracy or ambiguity while using this standard would inform the secretary of the technical committee responsible, the identity of which can be found in the foreword.

Buying Standards

Contact the Sales Office for South African and international standards, which are available in both electronic and hard copy format. Tel: +27 (0) 12 428 6883 email: sales@sabs.co.za

South African National Standards are also available online from the SABS Webstore www.store.sabs.co.za

Information on Standards

SABS Customer Services provide comprehensive standards-related information on national, regional and international standards. Tel: +27 (0) 12 428 7911 / 0861 27 7227 email: info@sabs.co.za

SANS 1718-9:2021
Edition 3

Table of changes

Change No.	Date	Scope

Foreword

This South African standard was prepared by National Committee SABS/TC 1095, *Standardization in the field of gambling equipment*, in accordance with procedures of the South African Bureau of Standards, in compliance with annex 3 of the WTO/TBT agreement.

This document was approved for publication in March 2021.

This document supersedes SANS 1718-9:2005 (edition 2).

This document is referenced in the National Gambling Act, 2004 (Act No. 7 of 2004) and the National Regulator of Compulsory Specification Act, 2008 (Act No. 5 of 2008).

Reference is made in 5.1.1 to the relevant national legislation (see foreword). In South Africa this mean the National Gambling Act, 2004 (Act No. 7 of 2004) and the National Regulator of Compulsory Specification Act, 2008 (Act No. 5 of 2008).

SANS 1718 consists of the following parts, under the general title *Gambling equipment*:

Part 1: Casino equipment.

Part 2: Limited payout gambling equipment.

Part 3: Monitoring and control systems for gambling equipment.

Part 4: Wagering record-keeping software.

Part 5: Local area and wide area jackpot and progressive jackpot equipment.

Part 7: Tokens.

Part 8: Roulette wheels.

Part 9: Central monitoring system for limited payout machines.

Part 10: Server Based Gambling

Annex A is for information only.

Compliance with this document cannot confer immunity from legal obligations.

Introduction

The requirements in this part of SANS 1718 are supplementary to and do not replace any of the requirements of relevant legislation or supporting regulations of the provincial licensing authorities (PLAs) in South Africa.

The intention of this part of SANS 1718 is to place sufficient controls on software and operations to ensure that wagering is fair, safe, secure, reliable, and auditable.

It is not the intention of this part of SANS 1718 to unreasonably

a) mandate a single solution or method of realizing an objective,

b) limit technology application of software,

c) limit creativity and variety of choice,

d) limit marketability, or

e) advantage any supplier or manufacturer of software.

Alternative implementations to the requirements contained in this part of SANS 1718 will be considered on a case-by-case basis by the provincial licensing authority (PLA).

Situations or considerations that arise from evaluation of systems, which have not been addressed in this part of SANS 1718 (for example, owing to omissions or the use of new technology), will be resolved at the sole discretion of the PLA as part of the approval process.

Contents

Contents *(concluded)*

This page is intentionally left blank

Gambling equipment

Part 9:
Central monitoring system for limited payout machines

1 Scope

This part of SANS 1718 specifies the general hardware and software requirements and the list of significant events for a central electronic monitoring system for limited pay-out machines (LPMs).

NOTE Guidelines on the submission and scope of testing are given in annex A.

2 Normative references

The following referenced documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies. Information on currently valid national and international standards can be obtained from the South African Bureau of Standards.

SANS 222/CISPR 22, *Information technology equipment – Radio disturbance characteristics – Limits and methods of measurement*.

SANS 60335-2-82/IEC 60335-2-82, *Household and similar electrical appliances – Safety – Part 2-82: Particular requirements for amusement machines and personal service machines*.

SANS 60950-1/IEC 60950-1, *Information technology equipment – Safety – Part 1: General requirements*.

SANS 61000-4-2/IEC 61000-4-2, *Electromagnetic compatibility (EMC) – Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test*.

SANS 61000-4-3/IEC 61000-4-3, *–Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test*.

SANS 61000-4-4/IEC 61000-4-4, *Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test*.

SANS 61000-4-5/IEC 61000-4-5, *Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity test*.

SANS 61000-4-8/IEC 61000-4-8, *Electromagnetic compatibility (EMC) – Part 4-8: Testing and measurement techniques – Power frequency magnetic field immunity test*.

SANS 61000-4-9/IEC 61000-4-9, *Electromagnetic compatibility (EMC) – Part 4-9: Testing and measurement techniques – Pulse magnetic field immunity test*.

3 Definitions and abbreviations

3.1 Definitions

3.1.1
approved
approved by the PLA

3.1.2
banknote acceptor
bill acceptor
bill validator
note acceptor
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 coupons approved in that jurisdiction

NOTE Where reference is made to a "banknote acceptor system", this is intended to include all bill handling components, whereas "Banknote validator system" refers to the validator unit and its sub-components, excluding other parts of the handling system.

3.1.3
bet
wager
amount of coins or credits put at risk at the commencement of a game or during a game

3.1.4
cash
coins, banknotes, tokens, magnetic or integrated circuit (for example, ″smart″) cards or any other legal representation of money in the gambling environment

3.1.5
cashout
action initiated by a player when redeeming available credits from a GD

NOTE This term is used whether the GD pays credits from the hopper, by electronic transaction or by a ticket.

3.1.6
certification authority
CA
authority appointed to certify all gambling devices (GDs), both hardware and software

3.1.7
coin acceptance device
CAD
coin input devices, together with the coin validator or comparator, photo-optic sensors (internal or external to the comparator), and any additional devices used to accept and validate a coin

3.1.8
coin dispensing device
CDD
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

3.1.9
critical data
data contained in critical memory as follows:

a) all metering required by this part of SANS 1718;

b) gambling devices (GDs) or game configuration data (or both);

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

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

e) current credits; and

f) information regarding any significant events

NOTE Information pertaining to the last five games is only required if applicable to that type of GD.

3.1.10
critical memory
memory locations for storing critical data

3.1.11
error event
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

3.1.12
external device
any device which attaches either physically or logically (or both) to the central electronic monitoring system (CEMS)

3.1.14
game
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

NOTE 1 Definitions of "game" in legislation take precedence over this definition.

NOTE 2 The game commences when the player

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

b) inserts one or more coins or any form of bet and game play is initiated

NOTE 3 The game is considered completed when the player

a) cannot continue play activity without committing additional credits from the credit meter or coin acceptance device (CAD), and

b) has no credits at risk.

NOTE 4 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:

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

b) features occurring or triggered in a single game;

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

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

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

f) gamble feature (for example, double-up).

NOTE 5 The game is not considered to be completed until all the appropriate meters for the game have been updated.

3.1.13
gambling device
GD
any device intended for the use of gambling purposes, including the monitoring and control system, GDs, host, data controller unit, bank controller or any combination of these, including software

3.1.14
gambling machine
slot machine
machine with which the player interacts for the purpose of gambling

NOTE The definitions in the appropriate legislation take precedence over this definition.

3.1.15
host
central computer(s) of a monitoring and control system on which the software is loaded, and that is (are) certified by the certification authority (CA)

3.1.16
idle mode
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

3.1.17
legislation
national or provincial legislation that deals with gambling, wagering, betting or horse-racing and any regulation or rule made in terms of such legislation

3.1.18
logic area
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

3.1.19
master reset
intentional memory clear of the random access memory (RAM) and other volatile memory of a GD RAM

3.1.20
memory
locations within the GD for storing electronic data, and the data stored therein

3.1.21
monitoring and control system
central electronic monitoring system
central monitoring system
host, data controller unit, bank controller and communications interface to each gambling machine and the connections between them

3.1.22
multigame
more than one game type offered by the gambling software on a single GD, if permitted by the PLA

3.1.23
period meter
soft meter
meters implemented in software that is used in a similar way to the odometer (for example, "trip meter") on a car

NOTE These meters are used to record meter values since a given event (for example, coins and bills in since the last clearance).

3.1.24
provincial licensing authority
PLA
body responsible in terms of the relevant legislation for issuing and controlling GD approvals

3.1.25
reprogrammable memory device
type of on-chip memory storage device

3.1.26
significant event
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

3.1.27
stake
total monetary value of all bets or wagers put at risk to play a single game

3.1.28
standard time
time according to the time information available from NTP servers maintained by the South African National Metrological Laboratory

NOTE Time signals should preferably be derived from the secondary (Stratum 2) server available at tock.nml.csir.co.za.

More information on synchronizing a personal computer's (PC) internal clock with the NTP server is available at http://www.time.za.net/.

3.1.29
test laboratory
TL
laboratory whose test results are accepted by the CA

3.1.30
win
award
prize
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

3.1.31
winnings
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

3.1.32
winning combination
one or more winning patterns that result in credits being added to

a) the total win meter, and

b) the win display

3.1.33
winning pattern
set of symbols that participates in a winning combination (including substitution)

NOTE A GD might display this value in credits or monetary value.

3.2 Abbreviations

ARQ	automatic retry query
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
EMC	electromagnetic compatibility
EMI	electromagnetic interference
EPROM	erasable programmable read-only memory
GD	gambling device
I/O	input/output
ISDN	integrated services digital network
PLA	provincial licensing authority
LAN	local area network
LPM	limited payout machine
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

4 General requirements

4.1 Documentation

4.1.1 Each GD model shall have readily available and pertinent operating and service manuals.

4.1.2 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.

4.1.3 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.

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

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

4.2 Enclosure identification

4.2.1 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.

4.2.2 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.

4.2.3 Each external key switch of the gambling 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 (for example, 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).

4.3 Enclosure construction

4.3.1 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 gambling 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 gambling venue.

4.3.2 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.

4.3.3 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.

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

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

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

4.4 Enclosure security

4.4.1 A secure area shall resist forced entry and shall retain evidence of attempts at such entry.

4.4.2 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".

4.5 Access detection systems

4.5.1 All access points shall have access detection schema.

4.5.2 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.

4.5.3 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.

4.5.4 It shall not be possible to create a false alarm door open condition (for example, by bumping the door).

4.5.5 If the access detection system is disconnected, the gambling equipment shall interpret this action as the door having been opened.

4.5.6 The GD 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 GD was placed in test mode. In such case a significant event message shall be sent and 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.

5 Electrical requirements

5.1 Enclosure wiring

5.1.1 The GD (and any associated equipment as determined by relevant national legislation (see foreword)) shall comply with the compulsory South African national standards for the safety of electrical and electronic equipment.

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

5.2 Electromagnetic compatibility (EMC)

5.2.1 Electromagnetic interference

The GD shall comply with the requirements for class A ITE equipment, as contained in SANS 222.

5.2.2 Electromagnetic immunity

When the GD is tested in accordance with the procedure given in SANS 61000-4-3, 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).

5.3 Magnetic immunity

5.3.1 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 in accordance with SANS 61000-4-8, the GD shall withstand a magnetic field that alternates at 50 Hz or 60 Hz and that has an 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.

5.3.2 Immunity to impulse magnetic field

The GD shall not have its security properties changed by the application of a magnetic interference level to the GD. When tested in accordance with SANS 61000-4-9, 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.

5.4 Temporary electrostatic disruption

When the GD is tested in accordance with SANS 61000-4-2, 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 the coin dispensing device (CDD).

5.5 Fast transient voltage

5.5.1 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) in accordance with SANS 61000-4-4:

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

b) to the input/output (I/O) lines: 0,5 kV.

5.5.2 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.

5.6 Surge voltage

The GD shall employ sufficient power supply filtering to prevent disruption when tested in accordance with SANS 61000-4-5. 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.

5.7 Long-term voltage level change test

When the GD 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 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. There may be a break between the two periods of abnormal operation.

NOTE This requirement is to demonstrate the ability of the GD 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 230 V).

5.8 Voltage supply

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

a) connect the GD to a variable voltage power supply. Set the supply voltage to the rated value. Operate the gambling 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.

c) reduce the supply voltage rapidly to 0,80 times the rated value, maintain for 5 s and return rapidly to the rated voltage.

NOTE This requirement is to demonstrate that the GD 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.

5.9 Power supply

5.9.1 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.

5.9.2 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.

5.9.3 Where the 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.

6 Computer and peripheral hardware requirement

6.1 Random access memory (RAM)

6.1.1 GD RAM data storage shall be capable of reliably preserving its memory contents for at least 72 h with the mains power switched off. When the battery is at or below its 72 h 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 h 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 h.

NOTE 1 Only where RAM maintained by battery is implemented.

NOTE 2 General significant event messages such as "tilt" are not acceptable.

6.1.2 RAM clears of the GD shall not be possible except by accessing the logic area.

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

6.2 Critical memory requirements

6.2.1 Manufacturers shall ensure that critical data are recorded in at least two separate devices or locations (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/game configuration data (for example, GD address, denomination); and

d) significant event information.

6.2.2 These devices shall be capable of being reliably updated at every critical memory change.

6.3 Programmable logical elements

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

6.4 Memory requirements

6.4.1 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.

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

6.4.3 A reprogrammable memory program storage device shall be protected from unauthorized modification. Modification shall only be permitted once the TL and the CA or the PLA (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.

6.5 Circuit boards

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

6.6 Switches and jumpers

6.6.1 If switches or jumpers that have the potential to cause the GD not to comply with this part of SANS 1718 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.

6.6.2 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).

6.6.3 The requirement in 6.6.1 and 6.6.2 shall apply to software configurations (if applicable).

6.7 Communication

6.7.1 The GD – CEMS (MCS) communications environment should be considered industrial in nature and subject accommodate for frequent interruption and interference. The means shall consider and address this in its design and implementation.

6.7.2 The means of communication shall be reviewed and verified by the TL to conform to the requirements of this part of SANS 1718. The verification of results shall be possible to be performed after installation. 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).

6.7.3 Gambling equipment communication interfaces shall not present a hazard. Compliance with the compulsory requirements for the safety of electrical and electronic equipment, as contained within legislation.

6.7.4 Ports for communication cabling shall be clearly and permanently labelled according to their function.

6.7.5 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.

6.8 Video monitors and touch screens

Where fitted, video monitors shall not present a hazard. Compliance with the compulsory requirements for the safety of electrical and electronic apparatus

6.9 Printers (if applicable)

6.9.1 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.

6.9.2 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.

6.10 External devices

External devices that affect game outcome and determination of revenues should be tested to the relevant part of SANS 1718 series.

7 Software requirements

7.1 General

7.1.1 The following shall appear in all source code modules:

a) module name;

b) version number;

c) revision number; and

d) description of functions performed.

7.1.2 The TL shall ensure that the program or source code modules have not been modified.

NOTE This does not apply to commercially available software that has no effect on the game play or game result determination.

7.1.3 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.

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

7.1.5 All program source codes for the GD shall be made available for examination by the TL.

7.2 Verification of source code compilation

7.2.1 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.

7.2.2 When compiled, all source code supplied to the TL shall generate object code that is exactly the same as that installed in the GD. The TL shall verify that the program or source code modules comply with the requirements of this part of SANS 1718.

NOTE This does not apply to commercially available software that does not influence game play or result determination.

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

NOTE 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).

7.2.4 An unrecoverable memory corruption shall result in a critical memory error.

7.2.5 If an unrecoverable memory corruption occurs, it shall require a master reset.

7.2.6 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.

7.3 Validity checks

7.3.1 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. RAM and program storage device space that is not critical to GD security need not be validated.

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

7.3.3 If a validity check of the software fails, it is understood that this means that the GD cannot function as intended, in which case it shall disable itself immediately.
NOTE Excludes transaction devices (for example, CDD, CAD and ticket printers) that do not influence the game results.

7.3.4 So as not to complicate the validation of software, all individual device-specific information (for example, GD 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 GDs of a particular type).

NOTE 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.

7.3.5 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.

7.3.6 A validity check of GD critical memory shall be undertaken at least after every restart of the device or transaction of significance (for example, logic door closed, door closed, 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.

7.4 Critical memory

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

7.4.2 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).

7.4.3 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.

7.5 Program memory

7.5.1 Labelling

All removable program storage media shall be uniquely labelled, 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 (if applicable)

f) the location in the GD (if critical).

7.5.2 Read/write storage

7.5.2.1 Superseded approved versions of programs shall be deleted and only current versions shall be available. However, it shall be possible to clearly identify which files belong to which version of the program.

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

7.5.3 Read/write storage media

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

7.5.3.2 A read/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.

7.5.3.3 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.

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

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

7.5.4 Loading programs to flash memory devices

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

7.5.4.2 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.

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

7.5.4.4 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.

7.5.4.5 The use of jumpers or similar devices can be used to enable/disable erasure/writing to reprogrammable memory provided here 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.

7.5.4.6 All reprogrammable memory devices shall be housed in a secure area.

7.5.4.7 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.

7.5.5 Write-once read-many (WORM) storage devices

7.5.5.1 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.

7.5.5.2 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.

7.5.5.3 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 (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).

7.5.5.4 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.

8 System functional requirements

8.1 Auditing information

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

8.1.2 There shall be log and report of all user activities, and configuration changes, made by a user in the CEMS. This shall be recorded by date and time of the activities or change actually occurring.

8.2 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.

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

8.3 Clocks and time stamping

8.3.1 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 1,0 s over a 24 h period.

8.3.2 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.

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

8.3.4 The host shall be able to update all clocks in intermediary devices attached to the system.

NOTE Individual GDs are not required to have clocks.

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

8.3.6 If dates and times are displayed, they shall be displayed in a consistent format.

8.3.7 The only acceptable all-numeric date formats are yyyy-mm-dd or dd-mm-yyyy.

NOTE 1 The preferred date format is yyyy-mm-dd.

NOTE 2 This requirement does not apply to the date format on displays that are not accessible to the player, such as set-up screens.

8.3.8 Only 24-hour time formats are acceptable.

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

8.3.10 A site data logger's clock shall not be inaccurate by any more than 0,5 s over a 24 h period.

8.3.11 The GDs shall operate and communicate correctly, and handle date and time rollovers including leap years.

8.4 Electronic funds transactions

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

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

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

c) 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;

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

e) all electronic funds transactions shall be correctly updated to the storage media and the system; and

f) the MCS shall maintain a record of the EFT meter values for each EFT transaction, including any unsuccessful attempts to conduct such a transaction, for a minimum of seven days.

8.5 Central logging of information

8.5.1 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.

8.5.2 The units in which each statistic is measured shall be certified by the CA.

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

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

8.5.5 Where the GD 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.

8.5.6 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.

8.5.7 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.

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

8.6 Control of gambling equipment

8.6.1 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).

8.6.2 There may be a need to log onto the computer to execute external audit and interrogation programs. The password that the PLA's inspector 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).

8.6.3 If the GD loses communication with its site data logger, the GD shall disable itself.

8.6.4 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 h shall automatically disable connected GDs, but shall be able to continue data collection thereafter.

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

8.6.6 If the site data logger goes off-line during game play, the GD 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 either allow the player to collect those credits before disabling (i.e. it shall permit a cashout) or permit a manual hand pay.

NOTE 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.

8.6.7 If the site data logger instructs the GD to disable (for example, at the end of an active daily period) during game play the GD 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 either allow the player to collect those credits (i.e. it shall permit a cashout) or permit a manual hand pay.

8.6.8 The host shall be able to enable and disable game play at any of the connected GDs at any time.

8.6.9 The host shall automatically disable the connected GDs 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.

8.6.10 If multigames are implemented, there shall be a method available so that it is possible to disable and enable individual games on multigame GDs. If it is not possible to accomplish individual game enable and disable, the entire machine shall be capable of being enabled or disabled.

8.7 Back-ups and recovery

8.7.1 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 (for example, 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 gambling equipment, deletion of gambling equipment, modification of gambling equipment (for example, 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.

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

8.7.3 Backups of the system shall be able to be made on at least a daily basis. Mirrored disk copies are not adequate for these back-ups where the "mirrors" are controlled by the same central processing unit (CPU).

8.8 Encryption of stored data

8.8.1 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.

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

a) encryption/decryption keys; and

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

8.8.3 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. For the use for encryption methods and controls the requirements of SANS 27002 are applicable. The method of disabling and the procedure to be followed shall be certified by the CA.

NOTE 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 (for example, signature and RNG);

h) transfers of money to/from player accounts;

i) transfer of money between GDs; and

j) parameters, configuration and win messages.

8.8.4 The encryption algorithm shall comply with the following characteristics:

a) encryption algorithms shall be demonstrably secure against cryptanalytic attacks;

NOTE Guidance on the suitability and use of encryption algorithms is provided in SANS 18033-1, SANS 18033-2, SANS 18033-3 and SANS 18033-4.

b) 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; and

c) 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:

1) dial-up modems;

2) cellular networks; and

3) integrated services digital network (ISDN).

8.8.5 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 gambling equipment that need to interface with the protocol.

8.8.6 The "total hand pays" 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, and any printed tickets and vouchers. It shall be designated on all reports or displays as "Total Hand Pays". If the GD keeps separate meters for "cancel credits", "voucher out" or "hand pay with jackpot" then the summation of these meters to derive a total amount for "Total hand pays" may be done by the MCS.

8.8.7 For calculation of the GGR the "total hand pay" is already included in "Total cash out", so you do not have to add it in the calculation. The "total hand pay" is in for reporting purposes that is why there is no special requirement or prerequisite in the standard for calculating the GGR.

8.9 Handling of master resets

8.9.1 The MCS shall be able to identify and properly handle the situation where master resets have been performed.

8.9.2 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.

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

8.10 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.

8.11 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:

a) The date and time of the event.

b) The identity of the GD that generated the event.

c) The venue number or name, in cases where the system controls multiple gambling venues.

d) A unique code that defines the event. The PLA 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.

8.12 Security of the significant event log

The software shall resist unauthorized access to or tampering with the significant events log by at least the following strategies:

a) access to the significant events data log shall be read-only and restricted by password security;

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

c) it is mandatory that the significant event log and software shall be so structured that it is not possible for unauthorized modifications to remain undetected.

8.13 Storage of the significant event log

8.13.1 The specific significant events, regardless of the source of these events, shall be stored in the central repository. Events may be stored temporarily at intermediate points in the system, but shall be written to the central repository as soon as possible.

8.13.2 It shall be possible to retrieve events in a chronological order.

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

8.13.4 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.

8.14 System security requirements

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

8.14.2 Where PINs and passwords are used, they shall be able to be changed periodically.

8.15 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.

NOTE If an external device is used, it should be tested by the TL to ensure that it does not interfere with CEMS.

8.16 Metering

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

8.17 Permitted software

Only programs and data files certified by the CA and approved by the PLA 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:

a) operating system programs;

b) applications programs;

c) fixed data files; and

d) software signature seeds, where applicable.

8.18 Communication with GDs

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

a) on a time schedule basis, and

b) on command, via the CEMS.

8.19 Reactivation of game play

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

a) If a door open event occurs other than a logic door open, the GD may reactivate automatically when the door is eventually closed;

b) If the PIN retry limit is exceeded for a player's account card, the GD shall remain deactivated until the card is removed; and

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

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

8.20 Signatures

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

8.20.2 Signature checking for GDs shall take place in response to type 4 significant events.

8.20.3 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 cyclic redundancy check (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.

8.21 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 at the actual time that they occurred.

8.22 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 this part of SANS 1718.

8.23 Cashout while disabled — Non-permitted occasions

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

a) during game play;

b) while the GD is in demonstration, test or audit mode;

c) while the GD is in a fault condition that requires manual activation; and

d) no cashout should be permitted while the GD communication error condition exists.

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

9 Communication requirements

9.1 General

9.1.1 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 the GD, but also applies to communication between other components or devices (or both) that form part of the system.

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

9.1.3 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 comply with SANS 60950-1.

d) All electronic data communication over the public switched telephone network (PSTN), dedicated leased lines supplied by the telecommunications PLA, 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).

9.1.4 The means of communication shall be designed and implemented to automatically and continuously ensure that all the following mandatory data

a) metering and transactional data;

b) significant events;

c) critical data;

d) system security and management data, including time synchronisation data; and

e) data the PLA may additionally specify in annex A of this part of SANS 1718

are communicated from the GD to the Host and is available for the specified accounting and reporting periods.

9.1.5 Where the means of communication is designed to carry data additional to the mandatory data, (for example, such as ″player tracking data″), the following shall apply:

a) the TL shall review and verify that this additional data has no impact on the mandatory data, or the delivery of mandatory data; and

b) ensure that the communication of the mandatory data has absolute priority over the additional data.

9.1.6 The CEMS (MCS) shall be able to effectively communicate with GD’s of different manufacture and any model or variant of these. The design or implementation of the CEMS (MCS) shall not dictate the communication means of the GD.

9.2 Cellular network communication

The following requirements apply if the user or operator intends to use a cellular network, or the equivalent, for dial-up Communication between the system and remote venues:

a) Esite that will use cellular communication shall have one or more defined clear path to a cellular relay within range.

b) Messages shall be encrypted.

c) A method shall be provided to verify that the system is communicating with the correct venue, and vice versa, if required.

NOTE Calling line identification (CLI) is not considered adequate for this purpose.

d) The time to complete daily polling of the 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.

10 Data communication requirements

10.1 Remote control of GDs

Only control functions of the 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.

10.2 Communication failure and recovery

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

a) failure of central computer local area network local area network (LAN) interfaces;

b) failure of the central LAN;

c) failure of central data communication interface devices;

d) failure of single data communication interface;

e) high data communication error rates on line;

f) a foreign or additional device placed on a LAN;

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

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

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

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

k) data communication interface failure on the GD.

10.3 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).

10.4 Error detection

10.4.1 The low level communication protocol shall cater for error detection and recovery equivalent to, at a minimum, a 16 bit CRC.

NOTE Vertical parity or simple checksum byte (logical or arithmetic sum) (or both) are not acceptable error detection schemes.

10.4.2 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.

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

10.4.4 Where critical data and information (for example, credits, metering information and information that pertain to a game outcome) are transferred between microcontrollers communicating outside of a secure area of the GD, an error check shall be done on the transferal.

NOTE Parity checking or simple check sums are not adequate.

10.4.5 Where any data (for example, credits, metering information, activation/de-activation commands, information that pertains to a game outcome and error events) are transferred between the GD and an external device, such as components of a monitoring and control system, an error detection and correction system shall be supported. Data errors shall be detectable to a minimum accuracy of 99,995 %.

10.5 Error detection and recovery

All protocols shall use communication techniques that have proper error detection and recovery functions.

NOTE Output-only pulse based or "wiring harness" interfaces are not acceptable.

10.6 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:

a) there shall be positive acknowledgement of all good data messages of a critical nature received;

b) if multiple messages have been sent it shall be clear which messages are being positively acknowledged;

c) messages received in error shall initiate automatic retry query (ARQ) functions. Implementations may include negative acknowledgement (NAK) of messages received in error, window rotation schemes, timeout recovery, etc.; and

d) secure messages (for example, credit transfer, significant events and signature results) shall not use the "broadcast" interfaces.

NOTE The above requirements are not applicable to broadcast or unconfirmed message types.

10.7 Protocol

10.7.1 The CA shall certify the message formats used for data communication.

10.7.2 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.

10.7.3 The CA shall certify a protocol only if the devices that implement the protocol are able to comply with the requirements of this part of SANS 1718.

10.8 Higher level protocol

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

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

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

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

10.9 Layered protocol

10.9.1 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).

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

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

10.10 Message authentication in low level communication

Unless full encryption is used on all messages, message authentication codes (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 (for example, password transmission).

10.11 Message framing in low level communication

10.11.1 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.

10.11.2 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.

10.12 Multi-dropping

10.12.1 Multi-dropping capability is required for all protocols that communicate with GDs except those systems that use a single or dedicated communication interface for each GD.

10.12.2 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 multi-dropped

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 (for example, 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.

10.13 Period meters

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

10.14 Software meters

10.14.1 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;

b) the protocol shall clearly state the unit of measure for each meter (for example, 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.

10.14.2 Meters forwarded by the 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.

10.15 Restart / recovery

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

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

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

NOTE These requirements do not apply to unsecured messages (for example, broadcast messages).

10.16 Simulator

If a simulator is provided to enable development of the protocol in GDs and other gambling 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:

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

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

c) 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; and

d) be provided, together with all relevant documentation, on request to all users.

11 Significant events requirements

11.1 General

11.1.1 Where this part of SANS 1718 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 part of SANS 1718 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.

11.1.2 This clause provides a summary of the significant events that are specified by the CA or the PLA. 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.

11.1.3 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 PLA audit procedures have been followed. These procedures might involve immediate approval for reactivation, or the approval could be withheld until physical inspection by the PLA inspector is completed.

11.1.4 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. By definition, all type 4 events shall be reported.

NOTE The phrase "manual reactivation" is understood to include closing of the logic door (if necessary) or turning of a reset key.

11.1.5 Significant events other than type 1 that occur on the 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.

11.1.6 The following actions shall be performed, if possible, on clearing of the fault on the 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 recommence 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.

11.1.7 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.

11.1.8 All GD fault conditions shall activate an alarm, which shall include either a tower light or sound (or both).

11.1.9 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.

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

11.2 GD/terminal events

11.2.1 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.

NOTE 1 It is acceptable if the GD only detects the changes when restarting.

NOTE 2 Reportable changes include any change to any configuration that alters the metering or the game outcome or the RTP (Return to Player) 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 GD.

11.2.2 Master reset (type 4)

Intentional memory clear of all non-volatile memory of the GD has occurred.

11.2.3 Error detected in either volatile or non-volatile memory (type 4)

Failure of internal test.

The failure of some test(s) means that the GD cannot function correctly, in which case it shall disable itself immediately after reporting the event to the monitoring and control system (if possible).

11.2.4 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).

11.2.5 Logic area closed (type 1)

A sensor registers that a logic door has been closed.

11.2.6 Power on (type 1)

Power is successfully restored and the device can operate.

11.2.7 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.

11.2.8 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.

11.2.9 "Coin in tilt" or "Coin out tilt" (type 2)

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

11.2.10 "CDD runaway", "coin out tilt" or "extra coin(s) paid" (type 2)

One or more coins are improperly paid by the CDD.

11.2.11 General enclosure access (type 2)

Opening of outer enclosure door, excluding the drop box door.

This message shall be sent by the GD 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.

11.2.12 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 monitoring and control system as an unauthorized access.

11.2.13 CDD empty/malfunction (type 2)

11.2.14 Enclosure door closed (type 2)

A sensor registers that a door has been closed.

11.2.15 Cancel credit (type 2)

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

11.2.16 Coin interference (type 2/R)

External interference with a coin/token acceptor or validator.

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

11.2.17 Reel error (type 2)

A reel position does not agree with software control.

11.2.18 Collect credit (type 1)

Cashout that exceeds the limit specified by legislation.

NOTE This significant event is not specified in South African legislation at present, but may be required later.

11.2.19 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.

11.2.20 Communication failure (type 2/R)

Failure of communication link between the GD and the next point in the monitoring system which indicate a failure rate of 100% shall be recorded at the Host, and an event shall be generated.

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

11.2.21 Printer failure (type 2)

The software has registered a printer fault.

11.2.22 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 the problem is rectified.

NOTE Equipment in a casino environment is not required to be capable of doing signature checking in response to a request from the MCS.

11.2.23 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.

11.2.24 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.

11.2.25 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.

11.2.26 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.

11.2.27 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.

11.2.28 Banknote storage area access (type 2)

This message is sent by the GD when the banknote storage area is accessed.

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.

NOTE This message is intended for use only with GDs where the banknote storage area is external.

11.2.29 Banknote acceptor mechanism is disconnected (type 1).

11.2.30 User logon/logoff (type 1)

A user logs on with a correct password or logs off, from the GD other than the GD.

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.

11.2.31 Logon failure (type 1/R)

A user incorrectly enters his/her PIN three consecutive times on the GD other than the GD.

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.

11.2.32 Software signature check failure (type 4 R)

In the event of a request to perform a software signature check failing or the signature check failing the GD shall be disabled and only once the cause of the failure has been rectified, shall the GD be enabled. The disabling shall happen automatically and the re-enabling may happen remotely without the need for onsite intervention.

11.2.33 Communication Error (type 2)

Failure of communication link between GD and the next point in the monitoring system, which indicate a failure rate of 10% or more shall be recorded at the Host, and an event shall be generated.

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

11.3 Player/staff cards (if applicable)

11.3.1 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.

NOTE It is not necessary to disable the GD or the player interface.

11.3.2 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.

NOTE It is not necessary to disable the GD or the player interface.

11.3.3 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.

11.4 Banknote acceptance

Banknote reject state (type 1)

Align with the other parts of SANS 1718 series.

The GD shall report banknote reject events to the monitoring and control system.

Need to look at a way mandating submission guidelines (manufacturer submission).

Annex A
(informative)

Guidelines for submission and scope of testing

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

A.1 General

A.1.1 SANS 1718 series of standards arise from and are underpinned by the gambling legislation in the Republic of South Africa, and so as a fundamental serve the following purposes:

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

1) fairness of the game,

2) integrity of the data associated with the above inclusive of any RNG and the results it may generate,

3) mechanical safety of any equipment,

4) electrical safety of any equipment,

5) the generation, communication/transmission, recording and recall of the required significant events event and status reporting in this regard,

6) integrity of communicated data associated with (a)(1) to (a)(5) inclusive.

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

1) the auditability of taxes and levies paid to a gambling board,

2) the integrity of the data associated with the (b)(1),

3) the generation, communication/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

1) the integrity of the associated data,

2) the integrity and accuracy of gambling 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,

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

4) the retention of current and past game status and results.

d) Fundamental 4: Compliance of the equipment, or a particular gambling game with the regulations and the rules of the appropriate gambling boards in South Africa.

e) Fundamental 5: Inherently, the highest possible level of compliance with the greatest number of requirements in SANS 1718 series of standards, and the regulations and rules that apply in the South African provinces where the equipment is intended to be used.

A.1.2 These compulsory requirements should be met by the appropriate equipment before submission for gambling testing or verification. Compliance with these requirements should be included with the submission which will be held in abeyance until such time as this requirement is met.

A.1.3 Persons making submissions to the 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 test laboratory (TL) accreditation authority and the appropriate gambling boards in South Africa.

A.2 Interpretation

A.2.1 The SANS 1718 series of 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 SANS 1718 series of standards, namely:

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

b) the intent of SANS 1718 series of standards as interpreted by an English speaking person qualified in the fundamentals given above and confirmed by the TL that is accredited against these series of standards.

A.2.2 In the event that SANS 1718 series of 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 to the responsible technical committee.

A.2.3 The query will be considered by a panel of knowledgeable persons and a written clarification or interpretation will be provided.

A.2.4 For a query to be considered, the following information should be included:

a) the applicable part of SANS 1718;

b) the publication date of the part of SANS 1718 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) the description in standardized English as to the circumstances causing the query;

f) the 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.

A.2.5 In the event of a dispute as to the interpretation of SANS 1718 series of standards or their scope of application (or both), the interpretation of the nominated panel of experts should be regarded as final.

A.3 Preparation for testing or verification

A.3.1 When gauging which hardware or software should be submitted for testing or verification by the TL, the following ambit of the SANS 1718 series of 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 MCS, recall of all data for dispute purposes, conducting and reconciling a drop or count and for audit purposes.

A.3.2 Inclusive of any processes in-between the processes in A.3.1 with the appropriate event, metering and accounting and error reporting, the accuracy and integrity of any calculation required in any of the processes in A.3.1, 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.

A.4 Minimum submission guidelines

A.4.1 The testing of equipment for compliance with SANS 1718 series of 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.

A.4.2 This matching of configurations is inclusive of every hardware configuration intended to be utilized and which should be uniquely identified for practical testing purposes.

A.4.3 The testing of the MCS takes places where the MCS and any associated GDs connected to the MCS are functioning as a whole to emulate the expected operating environment in which the combinations of equipment are expected to operate.

A.4.4 Where the GD is to be added to the MCS environment, or any form of upgrade or change of the MCS environment is to be undertaken, this likewise, should be tested in a replica environment.

A.4.5 No MCS 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.

A.4.6 Regardless of the country or test 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 South African certification authority (CA) or to a gambling board:

a) An original formal request for the equipment or software being submitted, in standardized English, formally declaring which part of SANS 1718 the equipment or software has been designed to meet, signed by the applicant.

   This declaration is specifically to include the requirements in applicable parts of SANS 1718 as to which the equipment or software meets and a detailed explanation of the requirements that the equipment/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 the GD in such a manner as to be detrimental to the public or the gambling board.

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/suppliers maintenance personnel, or those of the licensed operator.

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

   2) The TL 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/software being submitted in the environment as it is intended to be used.

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

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

   1) the assembly, set-up and configuration of the equipment,

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

   3) the correct and proper operation of the equipment by both the operator/licensee and the player,

   4) for changes to equipment previously submitted, a listing of changes to the design concept implementation/methodology in the creation or operation of equipment which has not been previously reviewed by the TL,

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

      i) 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;

      ii) 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 the SANS 1718 series of standards and which should confirm the source code implemented for this purpose;

      iii) documents that indicate whether any wire or between a logic area access device or sensor should be

- broken (open circuited),
- short circuited with another wire or conductive frame of the GD,
- partially open circuited,
- partially short circuited, or
- partially short circuited to another wire or conductive frame of the GD.

A.4.7 The appropriate logic area access significant event should be reported to the monitoring control system (MCS), and the GD should be disabled accordingly for further play.

A.5 Maintenance of a defect schedule

A.5.1 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 part of SANS 1718 or a compliance letter (see A.5.2), a schedule of all these defects for the particular manufacturer or supplier should be maintained by the TL detailed with the required part of SANS 1718 not met or undertaking in the compliance letter not correctly met.

A.5.2 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 TL and the result included in the test or evaluation report as if a requirement of the applicable part of SANS 1718. The TL is requested to report to the manufacturer or supplier any defect which reoccurs in equipment under test for the manufacturer or supplier to action.

A.6 Deviations from SANS 1718 series of standards

A.6.1 In line with international practice, provision is made for a manufacturer/supplier to apply to the technical committee charged with the maintenance of SANS 1718 series of standards, to deviate from, or be exempted from, certain requirements in the applicable part of SANS 1718, where compelling reasons to do so may exist.

A.6.2 All requests received will be reviewed by a panel of knowledgeable persons, representative of the gambling industry, nominated by the technical committee.

A.6.3 A request to deviate from a requirement in the applicable part of SANS 1718 may 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.

A.6.4 Alternately, the manufacturer or supplier may request in writing to make oral presentations to the panel at any of its meetings, where again the need to deviate should be motivated and justified.

A.6.5 The panel will respond to each request during which the applicant might be expected to answer queries from the panel, which might be technical in nature.

A.7 Deviations from the gambling boards' rules and requirements

A.7.1 These deviations are ordinarily dealt with by the appropriate gambling boards that may refer or defer the request to the panel, as it sees fit.

A.7.2 Any deviations in this regard are at the sole discretion of the particular gambling board concerned, as the standards panel or technical committee is not empowered to make any decisions in this regard.

A.8 Ancillaries to equipment (add-ons)

A.8.1 Ancillaries refer to any equipment that 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 the applicable part of SANS 1718.

A.8.2 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.

A.8.3 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, a gambling board may require that sufficient review, verification and testing in terms of the appropriate part of SANS 1718 take place to ensure that add-on in no reasonable way, affects, disrupts or alters the operation of the equipment, within the scope of the appropriate part of SANS 1718 and as approved.

A.8.4 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.

A.8.5 The TL should, in conjunction with the OE and add-on manufacturer or supplier, determine which requirements in the appropriate part of SANS 1718 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.

A.8.6 The requirements in the appropriate part of SANS 1718 utilized for this purpose should be listed in the resulting test report issued by the TL and provided to the CA for its records.

Bibliography

SANS 1718-1, *Gambling equipment – Part 1: Casino equipment.*

SANS 1718-2, *Gambling equipment – Part 2: Limited payout machines.*

SANS 1718-3, *Gambling equipment – Part 3: Monitoring and control systems for gambling equipment.*

SANS 1718-4, *Gambling equipment – Part 4: Wagering record-keeping software.*

SANS 1718-5, *Gambling equipment – Part 5: Local area and wide area jackpot and progressive jackpot equipment.*

SANS 1718-7, *Gambling equipment – Part 7: Tokens.*

SANS 1718-8, *Gambling equipment – Part 8: Roulette wheels.*

SANS 1718-10, *Gambling equipment – Part 10: Server-based gambling* systems.

SANS 18033-1, *Information technology – Security techniques – Encryption algorithms – Part 1: General.*

SANS 18033-2, *Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers.*

SANS 18033-3, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers.*

SANS 18033-4, *Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers.*

SANS 60335-2-82/IEC 60335-2-82, *Household and similar electrical appliances – Safety – Part 2-82: Particular requirements for amusement machines and personal service machines.*

SANS 60950-1/IEC 60950-1, *Information technology equipment – Safety – Part 1: General requirements.*

———————