STANDARD SERIES

GLI-25:

Dealer Controlled Electronic Table Games

Version: 1.1
Release Date: September 8, 2006

This Page Intentionally Left Blank

ABOUT THIS STANDARD

This Standard has been produced by **Gaming Laboratories International, Inc.** for the purpose of providing independent certifications to suppliers under this Standard and complies with the requirements set forth herein.

A supplier should submit equipment with a request that it be certified in accordance with this Standard. Upon certification, Gaming Laboratories International, Inc. will provide a certificate of compliance evidencing the certification to this Standard.

Dealer Controlled Electronic Table Games

GLI-25 Revision 1.1

REVISION HISTORY

Rev 1.1

3.2.3 Changed 'update' to 'synchronize'
3.2.7 added verbiage for clarity of rule
3.2.9 added definition and original rule became **3.2.9.1**
3.4.2 changed verbiage for clarity

Rev 1.0

V1.0 release date: June 16, 2006
Date Created: June 16, 2006

Table of Contents

This Page Intentionally Left Blank

CHAPTER 1

1.0 Standard Overview

1.1 Introduction

1.1.1 General Statement. **Gaming Laboratories International, Inc. (GLI)** has been testing gaming equipment since 1989. Over the years, we have developed numerous standards for jurisdictions all over the world. In recent years, many jurisdictions have opted to ask for technical standards without creating their own standards. In addition, with technology changing almost monthly, new technology is not being incorporated quickly enough into existing standards due to the long process of administrative rulemaking. This document, *GLI Standard 25*, will set forth the technical Standards for Dealer Controlled Electronic Table Games (ETG).

This standard and all others may be obtained by downloading it from our website at www.gaminglabs.com or by writing to us at:

Gaming Laboratories International, Inc.
600 Airport Road
Lakewood, NJ 08701
(732) 942-3999 Tel
(732) 942-0043 Fax

1.2 Purpose of Technical Standards

1.2.1 ***General Statement***. The Purpose of this Technical Standard is as follows:

a) To eliminate subjective criteria in analyzing and certifying Dealer Controlled Electronic Table Games.
b) To only test those criteria that impact the credibility and integrity of Dealer Controlled Electronic Table Games from both the Revenue Collection and Player's play point of view.
c) To create a standard that will ensure that the Dealer Controlled Electronic Table Games are fair, secure, and able to be audited and operated correctly.
d) To distinguish between local public policy and laboratory criteria. At GLI, we believe that it is up to each local jurisdiction to set their own public policy with respect to gaming.
e) To recognize that non-gaming testing (such as Electrical Testing) should not be incorporated into this standard but left to appropriate test laboratories that specialize in that type of testing.
f) Except where specifically identified in the standard, testing is not directed at health or safety matters. These matters are the responsibility of the manufacturer, purchaser, and operator of the equipment.
g) To construct a standard that can be easily changed or modified to allow for new technology.
h) To construct a standard that does not specify any particular method or algorithm. The intent is to allow a wide range of methods to be used to conform to the standards, while at the same time, to encourage new methods to be developed.

1.2.2 ***No Limitation of Technology***. One should be cautioned that this document should not be read in such a way that limits the use of future technology. The document should not be interpreted that if the technology is not mentioned, then it is not allowed. Quite to the contrary, as new technology is developed, we will review this standard, make changes and incorporate new minimum standards for the new technology.

1.3 Other Documents That May Apply

1.3.1 General Statement. The following other GLI standards may apply, depending on the features of the ETG and references throughout this document. All GLI standards are available on our website at www.gaminglabs.com:

a) GLI-11 Gaming Devices in Casinos;
b) GLI-12 Progressive Gaming Devices in Casinos;
c) GLI-13 On-Line Monitoring and Control Systems (MCS) and Validation Systems in Casinos;
d) GLI-16 Cashless Systems in Casinos;
e) GLI-17 Bonusing Systems in Casinos; and
f) GLI-18 Promotional Systems in Casinos.

NOTE: This standard covers the Technical Specifications of the operation of Dealer Controlled Electronic Table Games, as defined within section 1.4.1 below, where the table games are operated electronically, that require interaction from a live dealer. Please refer to GLI-24 for Electronic Table Game Systems that do not utilize a live dealer.

1.4 Defining Dealer Controlled Electronic Table Games

1.4.1 General Statement. Dealer Controlled Electronic Table Games (ETG) is the operation of a table game(s) that require a live dealer that utilizes electronics as part of the game's operation (i.e., game generation, electronically collecting, storing, communicating accounting and significant event data, etc.) **This standard is only to be used when the ETG requires a live dealer. This standard will not make assumptions as to the classification of a device in a particular jurisdiction as being a table game or a gaming device, as defined within the GLI-11 Gaming Devices in Casinos standard. Nor does GLI offer an opinion as to how many 'devices' the equipment encompasses.**

NOTE: For table game systems that do not utilize a live dealer, please refer to the GLI Standard 24.

1.5 Phases of Testing

1.5.1 General Statement. ETG submissions to the Test Laboratory may be performed in two phases:

a) Within the laboratory setting; and
b) On-site following the initial install of the system to ensure proper configuration of the security applications, if required.

NOTE: In addition to the on-site testing of the system, the Test Laboratory shall provide training on this new technology to the local regulators, recommended field auditing procedures, and assistance with the compilation of Internal Controls, if requested.

CHAPTER 2

2.0 SUBMISSION REQUIREMENTS

2.1 Reference Guide

Due to the variant ranges of systems and potential sizing limitations, each ETG will have to be reviewed on an individual basis for custom submission requirements. It is our recommendation that the Submission Requirements outlined within GLI-11 Gaming Devices in Casinos and GLI-13 Online Monitoring and Control and Validation Systems be observed as a guideline for ETG submissions.

CHAPTER 3

3.0 ETG REQUIREMENTS

3.1 Introduction

This chapter addresses ETG's that may or may not function as a component within a table game system. Each subchapter will distinguish when the section is applicable, depending on how the ETG functions.

3.2 Table Game System Requirements

3.2.1 ***General Statement***. The regulations of this subsection only apply when the ETG(s) operate as part of a 'table game system' that is independent of any external gaming system. ETG's that operate in conjunction with external systems shall meet the game level and communication requirements established within the appropriate GLI Standard, see also section 1.3.1.

3.2.2 ***System Clock***. The system must maintain an internal clock that reflects the current time (24hr format - which is understood by the local date/time format) and date that shall be used to provide for the following:

a) Time stamping of significant events;
b) Reference clock for reporting; and
c) Time stamping of configuration changes.

3.2.3 ***Synchronization Feature***. If multiple clocks are supported the system shall have a facility whereby it is able to synchronize those clocks in each system component, whereby conflicting information could not occur.

3.2.4 ***System Security***. All communications, including Remote Access (see 3.2.9), must pass through at least one approved application-level firewall and must not have a facility that allows for an alternate network path.

3.2.5 ***Firewall Audit Logs***. The firewall application must maintain an audit log of the following information and must disable all communications and generate an error event if the audit log becomes full:

a) All changes to configuration of the firewall;
b) All successful and unsuccessful connection attempts through the firewall; and
c) The source and destination IP Addresses, Port Numbers and MAC Addresses.

3.2.6 ***Surveillance/Security Functionality***. The system shall provide for interrogation that enables on-line comprehensive searching of the significant event log.

3.2.7 ***Access Control***. The system must support either a hierarchical role structure whereby user name and password define program access or individual menu item access or logon program /device security based strictly on user name and password or PIN. The system shall not permit the alteration of any significant log information without supervised access control. There shall be a provision for system administrator notification and user lockout or audit trail entry, after a set number of unsuccessful login attempts. The system shall record: Date and Time of the Login attempt, username supplied, and success or failure. The use of generic user accounts on servers is not permitted.

3.2.8 ***Data Alteration***. The system shall not permit the alteration of any accounting or significant event log information without supervised access controls. In the event financial data is changed, an audit log must be capable of being produced to document:

a) Data element altered;
b) Data element value prior to alteration;

c) Data element value after alteration;
d) Time and Date of alteration; and
e) Personnel that performed alteration (user login).

3.2.9 Remote Access defined:Remote access defines any access made by a component outside the 'trusted' network.

3.2.9.1 Remote access where permitted, shall authenticate all computer systems based on the authorized settings of the ETG and firewall application that establishes a connection with the ETG as long as the following requirements are met:

a) Remote Access User Activity log is maintained by both the property and the manufacturer, depicting: authorized by, purpose, logon name, time/date, duration, and activity while logged in;
b) No unauthorized remote user administration functionality (adding users, changing permissions, etc.);
c) No unauthorized access to database;
d) No unauthorized access to operating system; and
e) If remote access is to be on a continuous basis then a network filter (firewall) must be installed to protect access (dependant upon jurisdictional approval).

3.2.10 Self Monitoring. The system must implement self monitoring of all critical Interface Elements (e.g. central hosts, network devices, firewalls, links to third parties, etc.) and shall have the ability to effectively notify the system administrator of any error condition, provided the condition is not catastrophic. The system shall be able to perform this operation with a frequency of at least once in every 24-hour period.

3.2.11 System Redundancy, Backup & Recovery. The system shall have sufficient redundancy and modularity so that if any single component or part of a component fails, gaming can continue. There shall be redundant copies of each log file or system database or both on the system with open support for backups and restoration.

3.2.12 Backup & Recovery. In the event of a catastrophic failure when the system cannot be restarted in any other way, it shall be possible to reload the system from the last viable backup point and fully recover the contents of that backup, recommended to consist of at least the following information:

a) Significant events;
b) Accounting information;
c) Auditing information; and
d) Specific site information such as Device file, Employee file, game profiles, etc.

3.2.13 Communication Protocol. Each component of an ETG system must function as indicated by the communication protocol implemented. All protocols must use communication techniques that have proper error detection and/or recovery mechanisms which are designed to prevent unauthorized access or tampering, employing Data Encryption Standards (DES) or equivalent encryption with secure seeds or algorithms. Any alternative measures will be reviewed on a case-by-case basis, with regulator approval.

3.3 Integrity of the ETG(s)

3.3.1 General Statement. The Laboratory will perform certain tests to determine whether or not outside influences affect game fairness to the player or create cheating opportunities. An Electronic Table Game System shall be able to withstand the following tests, resuming game play without operator intervention:

a) Random Number Generator. If implemented, the random number generator and random selection process shall be impervious to influences from outside the device,

including, but not limited to, electro-magnetic interference, electro-static interference, and radio frequency interference;

b) Electro-Magnetic Interference. The ETG shall not create electronic noise that affect the integrity or fairness of neighboring devices or associated equipment;

c) Electro-Static Interference. Protection against static discharges requires that the table game's conductive cabinets be earthed in such a way that static discharge energy shall not damage, or inhibit the normal operation of the electronics or other components within the ETG. The ETG may exhibit temporary disruption when subjected to a significant electro-static discharge greater than human body discharge, but they shall exhibit a capacity to recover and complete any interrupted play without loss or corruption of any control or data information associated with the ETG. The tests will be conducted with a severity level of a minimum of 27KV air discharge;

d) Radio Frequency Interference (RFI). Electronic Table Game Systems shall not divert from normal operation by the application of RFI at a frequency range from twenty-seven (27) to one thousand (1000) MHZ with a field strength of three (3) volts per meter;

e) Magnetic Interference. ETG's shall not be adversely affected by magnetic interference. The manufacturer should supply any documentation if the device has had magnetic interference testing against any recognized standard; and

f) Liquid Spills. Liquid Spills applied to the outside of the Electronic Table Game System shall not affect the normal operation of the machine, the integrity of the material or information stored inside the cabinet, or the safety of the players operating the equipment.

3.3.2 Physical Security. The server or system component(s) must reside in a secure area where access is limited to authorized personnel. It is recommended that logical access to the game be logged on the system or on a computer or other logging device that resides outside the secure area and is not accessible to the individual(s) accessing the secure area. The logged data should include the time, date, and the identity of the individual accessing the secure area. The resulting logs should be kept for a minimum of 90 days.

3.4 Random Number Generator

3.4.1 ***General Statement***. The Random Number Generator (RNG) is the selection of game symbols or production of game outcomes. The regulations within section 3.4 are only applicable to ETG's that utilize an electronic RNG, which shall:

a) Be statistically independent;
b) Conform to the desired random distribution;
c) Pass various recognized statistical tests; and
d) Be unpredictable.

3.4.2 ***Selection Process***. Mechanical and Electro-Mechanical Random Number Generator, where utilized shall meet the following requirements:

a) All Combinations and Outcomes Shall Be Available. Each possible permutation or combination of game elements that produces winning or losing game outcomes shall be available for random selection at the initiation of each play, unless otherwise denoted by the game.
b) No Near Miss. After selection of the game outcome, the ETG shall not make a variable secondary decision, which affects the result shown to the player. For instance, the random number generator chooses an outcome that the game will be a loser.
c) No Corruption from Associated Equipment. An ETG shall use a communication protocol that effectively protects the random number generator and random selection process from influence by associated equipment, which may be communicating with the ETG.

3.4.3 Applied Tests. The test laboratory may employ the use of various recognized tests to determine whether or not the random values produced by the random number generator pass the desired confidence level of 95%. These tests may include, but are not limited to:

a) Chi-square test;
b) Equi-distribution (frequency) test;
c) Gap test;
d) Overlaps test;
e) Poker test;
f) Coupon collector's test;
g) Permutation test;
h) Kolmogorov-Smirnov test;
i) Adjacency criterion tests;
j) Order statistic test;
k) Runs tests (patterns of occurrences should not be recurrent);
l) Interplay correlation test;
m) Serial correlation test potency and degree of serial correlation (outcomes should be independent of the previous game); and
n) n) Tests on subsequences.

3.4.4 Background RNG Activity. The RNG shall be cycled continuously in the background between games and during game play at a speed that cannot be timed by the player. The test laboratory recognizes that some time during the game, the RNG may not be cycled when interrupts may be suspended. The test laboratory recognizes this but shall find that this exception shall be kept to a minimum.

3.4.5 RNG Seeding. The first seed shall be randomly determined by an uncontrolled event. After every game there shall be a random change in the RNG process (new seed, random timer, delay, etc.). This will verify the RNG doesn't start at the same value, every time. It is permissible not to use a random seed; however, the manufacturer must ensure that games will not synchronize.

3.4.6 Live Game Correlation. Unless otherwise denoted on the pay glass/display, where the ETG plays a game that is recognizable such as Poker, Blackjack, Roulette, etc., the same probabilities associated with the live game shall be evident in the simulated game. For example, the odds of getting any particular number in Roulette where there is a single zero (0) and a double zero (00) on the wheel, shall be 1 in 38; the odds of drawing a specific card or cards in Poker shall be the same as in the live game.

3.4.7 Card Games. The consequences for games depicting cards being drawn from a deck are the following:

a) At the start of each game/hand, it is recommended that the first hand of cards shall be drawn fairly from a randomly-shuffled deck; the replacement cards aren't drawn until needed;
b) Cards once removed from the deck shall not be returned to the deck except as provided by the rules of the game depicted;
c) As cards are removed from the deck they shall be immediately used as directed by the Rules of the Game (i.e., the cards are not to be discarded due to adaptive behavior by the ETGS)

3.5 Software/Program Authentication

3.5.1 Program Verification. The system server(s) and each component of the ETG that would have an effect on the integrity of the ETG shall have the ability to Authenticate all critical files including, but not limited to, executables, data, operating system files and other files, which may affect the game outcome or system operation, which reside on the medium utilizing a third-party industry standard secure hashing algorithm. (e.g. MD5 or SHA1) The algorithm shall use a key or seed of sufficient length and complexity. The manufacturer should be prepared to demonstrate the algorithm choice to both the testing laboratory and jurisdiction. The third-party verification process shall not include any process or security software provided by the operating system manufacturer. A secondary check may use commercially available software by the operating system manufacturer as part of the secondary verification.

NOTE: If the third-party verification tool is embedded within the Control Program, the Test Laboratory must be supplied with the tools needed to 'extract' the Control Program from the ETG component. This will enable the laboratory to perform forensic examinations, at the request of the regulator.

3.6 Maintenance of Critical Memory

3.6.1 General Statement. Critical memory storage may be maintained by the player terminal or the system, where applicable. Critical memory shall be maintained by a methodology that enables errors to be identified and corrected in most circumstances. This methodology may involve signatures, checksums, partial checksums, multiple copies, timestamps and/or effective use of validity codes.

3.6.2 Comprehensive Checks. Comprehensive checks of critical memory shall be made during each component restart (e.g., power up cycle). Upon power resumption, the integrity of all critical memory shall be checked. Control Programs (software that operates the system components) shall test for possible corruption caused by failure of the program storage medium and all critical game functions. Test methodology shall detect 99.99 percent of all possible failures.

3.6.3 Control Program. The critical components of the ETG and system components, where applicable, shall ensure the integrity of all control program components during execution of said components.

3.6.4 Program Storage Devices (PSDs). All PSDs (Program Storage Devices), in the executable address space of a main processor for all critical components, shall be validated and checked for corruption during the following conditions:

a) Any power up; and
b) The first time the files are loaded for use, even if only partially loaded.

NOTE: RAM and PSD space that is not critical to the ETG operations are not required to be validated.

3.7 Player Interface Terminal Requirements

3.7.1 ***General Statement***. The player interface terminal(s) must meet the Hardware and Software Requirements outlined within the GLI-11 Standard, where applicable, to ensure the security of the terminal and player safety. Requirements that can not be met as a result of manual intervention performed by the live dealer must be addressed in operational procedures and submitted to the Test Laboratory.