and new gaming software is infrequently added to an existing operational gaming machine. This differs from a PC, where users tend to buy new and different combinations of devices and software from different manufacturers, and then connect or install these new items to a PC to suit their individual needs. Therefore, the types of devices connected to a PC may vary greatly from user to user depending on their individual requirements, and may also vary significantly over time for a given PC.

[0040] Although the variety of devices available for a PC may be greater than on a gaming machine, gaming machines still have unique device requirements that differ from a PC, such as device security requirements not usually addressed by PCs. For instance, monetary devices such as coin dispensers, bill validators, ticket printers and computing devices that are used to govern the input and output of cash to a gaming machine have security requirements that are not typically addressed in PCs. Many PC techniques and methods developed to facilitate device connectivity and device compatibility do not address the emphasis placed on security in the gaming industry. To address some of these issues, a number of hardware/software components and architectures are utilized in gaming machines that are not typically found in general-purpose computing devices, such as PCs. These hardware/software components and architectures include, but are not limited to, items such as watchdog timers, voltage monitoring systems, state-based software architectures and supporting hardware, specialized communication interfaces, security monitoring, and trusted memory.

[0041] A watchdog timer is normally used in IGT gaming machines to provide a software failure detection mechanism. In a normal operating system, the operating software periodically accesses control registers in a watchdog timer subsystem to "re-trigger" the watchdog. Should the operating software not access the control registers within a preset timeframe, the watchdog timer will time out and generate a system reset. Typical watchdog timer circuits contain a loadable timeout counter register to allow the operating software to set the timeout interval within a certain time range. A differentiating feature of some preferred circuits is that the operating software cannot completely disable the function of the watchdog timer. In other words, the watchdog timer always functions from the time power is applied to the board.

[0042] IGT gaming computer platforms preferably use several power supply voltages to operate portions of the computer circuitry. These can be generated in a central power supply or locally on the computer board. If any of these voltages falls out of the tolerance limits of the circuitry they power, unpredictable operation of the computer may result. Though most modern general-purpose computers include voltage-monitoring circuitry, these types of circuits only report voltage status to the operating software. Out of tolerance voltages can cause software malfunction, creating a potential uncontrolled condition in the gaming computer. IGT gaming machines, however, typically have power supplies with tighter voltage margins than that required by the operating circuitry. In addition, the voltage monitoring circuitry implemented in IGT gaming computers typically has two thresholds of control. The first threshold generates a software event that can be detected by the operating software and an error condition generated. This threshold is triggered when a power supply voltage falls out of the tolerance range of the power supply, but is still within the operating range of the circuitry. The second threshold is set when a power supply voltage falls out of the operating tolerance of the circuitry. In this case, the circuitry generates a reset, halting operation of the computer.

[0043] The standard method of operation for IGT gaming machine game software is to use a state machine. Each function of the game (e.g., bet, play, result) is defined as a state. When a game moves from one state to another, critical data regarding the game software is stored in a custom non-volatile memory subsystem. In addition, game history information regarding previous games played, amounts wagered, and so forth also should be stored in a non-volatile memory device. This feature allows the game to recover operation to the current state of play in the event of a malfunction, loss of power, or the like. This is critical to ensure that correct wagers and credits are preserved. Typically, battery backed RAM devices are used to preserve this critical data. These memory devices are not used in typical general-purpose computers. Further, IGT gaming computers normally contain additional interfaces, including serial interfaces, to connect to specific subsystems internal and external to the gaming machine. The serial devices may have electrical interface requirements that differ from the "standard" EIA RS232 serial interfaces provided by general-purpose computers. These interfaces may include EIA RS485, EIA RS422, Fiber Optic Serial, optically coupled serial interfaces, current loop style serial interfaces, and the like. In addition, to conserve serial interfaces internally in the gaming machine, serial devices may be connected in a shared, daisy-chain fashion where multiple peripheral devices are connected to a single serial channel.

[0044] IGT gaming machines may alternatively be treated as peripheral devices to a casino communication controller and connected in a shared daisy chain fashion to a single serial interface. In both cases, the peripheral devices are preferably assigned device addresses. If so, the serial controller circuitry must implement a method to generate or detect unique device addresses. General-purpose computer serial ports are not able to do this. In addition, security-monitoring circuits detect intrusion into an IGT gaming machine by monitoring security switches attached to access doors in the gaming machine cabinet. Preferably, access violations result in suspension of game play and can trigger additional security operations to preserve the current state of game play. These circuits also function when power is off by use of a battery backup. In power-off operation, these circuits continue to monitor the access doors of the gaming machine. When power is restored, the gaming machine can determine whether any security violations occurred while power was off, such as by software for reading status registers. This can trigger event log entries and further data authentication operations by the gaming machine software.

[0045] Trusted memory devices are preferably included in an IGT gaming machine computer to ensure the authenticity of the software that may be stored on less secure memory subsystems, such as mass storage devices. Trusted memory devices and controlling circuitry are typically designed to not allow modification of the code and data stored in the memory device while the memory device is installed in the gaming machine. The code and data stored in these devices may include, for example, authentication algorithms, random number generators, authentication keys, operating system kernels, and so forth. The purpose of these trusted memory devices is to provide gaming regulatory authorities a root trusted authority within the computing environment of the gaming machine that can be tracked and verified as original.