AxiomXa
Especificaciones Técnicas

Table of Contents

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

1. General

1.1. Propósito

1.1.1. Establecer los requisitos técnicos, funcionales, jurisdiccionales, regulatorios y de calidad para los sistemas de seguridad y control de acceso que deben ser adquiridos de proveedores. Las especificaciones técnicas aprobadas definen el suministro e instalación de todos los sistemas de seguridad y control de acceso e identifican fabricantes y modelos aprobados.

1.1.2. El sistema de seguridad consistirá en la implementación de un Sistema Integrado de Control de Acceso y Evaluación de Video (ACAMVAS) que controlará el acceso del personal, proporcionará monitoreo de alarmas de detección de intrusiones en tiempo real y ofrecerá vigilancia por video activada por alarmas para los edificios y operaciones designadas de acuerdo con los requisitos y especificaciones prescritos en estos documentos y los planos aprobados. El sistema de seguridad incluirá lo siguiente, donde sea aplicable:

1.1.2.1. Integración perfecta de un sistema de gestión de video digital que permitirá a los operadores del sistema controlar y mantener la seguridad de las instalaciones desde múltiples estaciones de trabajo designadas.

1.1.2.2. Instalación y/o reemplazo de hardware de puertas y cerraduras para habilitar el acceso con lectores RFID en aperturas designadas. Las aperturas designadas con acceso de lector RFID también permitirán el desbloqueo manual utilizando el sistema de llave maestra.

1.1.2.3. Suministro e instalación de alarmas de detección de intrusiones en las instalaciones designadas.

1.1.2.4. Suministro e instalación de dispositivos de detección de movimiento interior y exterior para proporcionar cobertura de alarmas en las instalaciones designadas.

1.1.2.5. Integración perfecta de sistemas de vigilancia por video que proporciona evaluación activada por alarmas para el equipo de detección de intrusiones en las instalaciones designadas.

1.1.2.6. Suministro e instalación de acceso con lector RFID para barreras de vehículos en las instalaciones designadas.

1.1.2.7. Suministro e instalación de todo el cableado de control, señal, iluminación y distribución de energía según sea necesario para el equipo de seguridad, incluyendo cualquier trabajo de zanjeo requerido para completar la instalación.

1.1.2.8. Puesta en marcha y pruebas de los sistemas y equipos instalados según sea necesario para cumplir con las especificaciones del fabricante y los procedimientos de instalación documentados, y a satisfacción del propietario.

1.1.2.9. Capacitación del personal del propietario para operar completamente y realizar mantenimiento rutinario en los sistemas y equipos instalados.

1.1.2.10. Proveer toda la documentación asociada para las actualizaciones del sistema de seguridad.

1.2. Normas de referencia

1.2.1. Normas del Instituto Nacional Estadounidense de Estándares (ANSI)

1.2.2. CANASA (Asociación Canadiense de Alarmas y Seguridad)

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

1.2.3. Certificación CE (Conformidad de la Unión Europea)
1.2.4. CFAA (Asociación Canadiense de Alarmas de Incendio)
1.2.5. Código de Construcción de Ontario
1.2.6. RoHS (Restricción de Sustancias Peligrosas)
1.2.7. Underwriters Laboratories of Canada (ULC)

1.3. Definiciones y Acrónimos

1.3.1. Apertura – un punto de acceso como una puerta, portón, piso de ascensor u otra barrera controlada y monitoreada por un controlador.
1.3.2. Tarjetahabiente – una persona registrada con una credencial válida, como un token o tarjeta, y autorizada para acceder a aperturas controladas por el sistema asignadas.
1.3.3. CCTV – Circuito Cerrado de Televisión.
1.3.4. Controlador – Unidad de Control de Acceso; puede referirse a una unidad primaria o subordinada.
1.3.5. Credencial – una tarjeta, token, PIN, identificador biométrico u otro dispositivo presentado en un lector por un titular de tarjeta para obtener acceso a aperturas controladas por el sistema.
1.3.6. DVR/NVR – Grabador de Video Digital/Grabador de Video en Red.
1.3.7. GUI – Interfaz Gráfica de Usuario.
1.3.8. LAN/WAN – Red de Área Local/Red de Área Amplia.
1.3.9. Operador – una persona registrada con una identificación de usuario válida y contraseña autorizada con responsabilidades administrativas del sistema de control de acceso.
1.3.10. RF – Radio Frecuencia/Señalización de Radio Frecuencia.
1.3.11. RFID – Identificación por Radio Frecuencia (incluyendo tecnologías de “proximidad” de 125kHz y “tarjeta inteligente” de 13.56MHz).
1.3.12. SQL – Lenguaje de Consulta Estructurado.
1.3.13. TCP/IP – Protocolo de Control de Transmisión/Protocolo de Internet.
1.3.14. USB – Bus de Serie Universal.
1.3.15. VMS – Sistema de Gestión de Video.

1.4. Garantía

1.4.1. Garantía del Fabricante
1.4.1.1. El Proveedor deberá garantizar que todo el equipo suministrado es nuevo, sin daños, libre de defectos y conforme a las especificaciones de este documento.
1.4.2. Período de Corrección Extendido
1.4.2.1. La obligación del Proveedor incluirá la remoción, reparación o reemplazo, transporte, reinstalación y pruebas sin costo para el Comprador, de todas o cualquier parte del sistema que se encuentre defectuosa debido a materiales o mano de obra defectuosa por un período de ____ meses después de la instalación del sistema.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2. Productos

2.1. Fabricantes

2.1.1. Las especificaciones, funcionalidad, capacidades del sistema y productos presentados se basan en Controladores RBH, dispositivos de comunicación relacionados y el Sistema de Gestión de Seguridad RBH AxiomXa

2.2. Componentes de Seguridad

2.2.1. A continuación se enumeran los componentes de seguridad que se suministrarán e instalarán. También se incluye una especificación detallada de cada uno de los componentes de seguridad incluidos en esta lista.

2.2.1.1. Software de Gestión de Seguridad
2.2.1.2. Controladores
2.2.1.3. Dispositivos de Comunicación
2.2.1.4. Lectores
2.2.1.5. Credenciales
2.2.1.6. Dispositivos de bloqueo
2.2.1.7. Fuentes de alimentación
2.2.1.8. Servidores / Estaciones de trabajo

2.3. Sistema de Control de Acceso y Monitoreo de Alarmas

2.3.1. Especificaciones Generales del Sistema

2.3.1.1. El sistema de control de acceso y monitoreo de alarmas será el sistema empresarial RBH AxiomXa y cumplirá con las siguientes especificaciones de diseño y rendimiento:

2.3.1.2. El sistema será un sistema modular y en red de control de acceso y monitoreo de alarmas, compuesto por componentes comerciales probados y disponibles en el mercado, capaz de manejar grandes corporaciones con múltiples sitios remotos, monitoreo de alarmas, imágenes de video, emisión de credenciales, integración de paginación, integración de CCTV, tour de guardias interactivo, mapeo, gestión de visitantes, notificaciones por correo electrónico, sistemas de monitoreo de terceros, integración de BAS y gestión de activos.

2.3.1.3. El sistema garantizará un rendimiento duradero, capacidad de actualización rentable y permitirá una fácil expansión o modificación de entradas, salidas y estaciones de trabajo locales o remotas.

2.3.1.4. El control del sistema en la ubicación del servidor central estará bajo un único programa de software, proporcionará integración completa de todos los componentes y podrá ser alterado en cualquier momento, dependiendo de los requisitos. La reconfiguración se realizará en línea a través de la programación del sistema, sin cambios de hardware.

2.3.1.5. El software del Sistema de Gestión de Seguridad utilizará Microsoft SQL Server 2016/2017/2019 para el almacenamiento de datos y estará escrito expresamente para Microsoft SQL Server 2016/2017/2019.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.1.6. El sistema tendrá la capacidad de conectarse en red a través de una conexión LAN/WAN utilizando el protocolo de comunicación estándar TCP/IP de la industria. El sistema proporcionará encriptación a través de la conexión TCP/IP.

2.3.1.7. El sistema incorporará el uso de comunicaciones RS-485 bidireccionales y/o conexiones redundantes Clase “A” TCP/IP para redundancia y fiabilidad.

2.3.1.8. El sistema incorporará comunicaciones de "Alta Disponibilidad" para que múltiples rutas de comunicación estén disponibles para todos los controladores. Alta Disponibilidad se definirá como, "un controlador alternativo existente asumirá las comunicaciones en caso de que falle el controlador principal. El controlador debe estar ubicado en una ubicación separada del primero."

2.3.1.9. El sistema soportará tanto respuestas manuales como automáticas a las alarmas que ingresen al sistema. Cada alarma podrá iniciar una serie de diferentes acciones, como cambio de cámara, activación de dispositivos remotos y control de aperturas.

2.3.1.10. El sistema proporcionará niveles ilimitados de códigos de emergencia para permitir que el sistema opere en diferentes niveles de seguridad según el nivel de amenaza local, por ejemplo, código negro = amenaza de bomba y el edificio se bloquea.

2.3.1.11. El sistema proporcionará monitoreo de puntos de alarma supervisados y no supervisados. Al reconocer una alarma, el sistema será capaz de cambiar cámaras CCTV y crear automáticamente una ventana emergente para la visualización de video de la alarma asociada.

2.3.1.12. El sistema será capaz de armar o desarmar puntos de alarma tanto manualmente como automáticamente, según la hora del día y el día de la semana.

2.3.1.13. Las funciones de control de acceso incluirán validación basada en la hora del día, día de la semana, programación de días festivos, verificación de códigos de sitio, recuperación automática o manual de fotografías de titulares de tarjetas, y validación de acceso basada en la verificación positiva de la credencial o la credencial y verificación de video.

2.3.1.14. La programación del sistema será amigable para el operador y capaz de ser realizada por personal sin experiencia previa en computadoras. La programación será guiada por menús e incluirá "Ayuda" en línea con el uso de la tecla F1 para llamar automáticamente la información de ayuda adecuada a la pantalla. El software utilizará cuadros desplegables para todos los datos requeridos por el sistema ingresados previamente.

2.3.1.15. Después de la instalación, el Propietario podrá realizar cambios básicos en la configuración del hardware. Estos cambios en la configuración del hardware incluirán, pero no se limitarán a, tiempo de apertura de aperturas, tiempo de derivación de contacto de apertura, nombres de aperturas y lectores, cuándo y dónde es válida una credencial, y la capacidad de agregar o modificar datos de titulares de tarjetas según se desee sin los servicios del Fabricante o del Proveedor del Fabricante.

2.3.1.16. La reparación del equipo podrá realizarse en el sitio, mediante el reemplazo de módulos, utilizando componentes de repuesto. Todo el equipo tendrá conectores desenchufables para una fácil sustitución.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.1.17. Todos los componentes de control incluirán la capacidad de descargar parámetros operativos a cualquier controlador, permitiendo así que el controlador proporcione funciones operativas completas independientemente de cualquier otro componente del sistema.
2.3.1.18. El sistema será diseñado de tal manera que la inscripción de personal autorizado pueda realizarse desde una ubicación descentralizada.
2.3.1.19. El sistema proporcionará integración perfecta con múltiples fabricantes de DVRs/NVRs/VMSs al mismo tiempo.
2.3.1.20. El sistema proporcionará integración perfecta con Sistemas de Automatización de Edificios (BAS) externos, sistemas de seguridad personal, sistemas de paginación remota y sistemas de correo electrónico.
2.3.1.21. Todos los eventos del sistema, acciones del operador e información de mantenimiento se almacenarán en la(s) base(s) de datos SQL para mantener un registro permanente de la actividad del sistema. El sistema tendrá la capacidad para realizar copias de seguridad manuales y automáticas de la configuración y los eventos del sistema en medios extraíbles locales (ópticos/magnéticos) o en recursos de red remotos.
2.3.1.22. Todas las estaciones de trabajo se configurarán para actuar como un Centro de Monitoreo de Alarmas para el sistema. Todas las alarmas se configurarán según el horario y las estaciones de trabajo tendrán la capacidad de reconocer y despejar las alarmas como un proceso de dos pasos.
2.3.1.23. Todas las estaciones de trabajo tendrán la capacidad de definir el enrutamiento de alarmas con un número ilimitado de niveles de enrutamiento disponibles para el sistema.

2.3.2. Mapeo y Gráficos Interactivos

2.3.2.1. El sistema soportará un número ilimitado de pantallas de mapas gráficos en color programables por el operador capaces de mostrar el plano, la ubicación del dispositivo de alarma y las instrucciones de alarma.
2.3.2.2. Los planos se crearán en un formato aprobado y serán capaces de ser importados desde otros sistemas. Todos los mapas gráficos interactivos se mostrarán en los monitores de las estaciones de trabajo.
2.3.2.3. Los mapas serán interactivos con estado dinámico en tiempo real para que el operador pueda controlar todas las funciones del dispositivo desde el mapa.

2.3.3. Almacenamiento de Información

2.3.3.1. Toda la información programada, así como el historial de transacciones, se almacenará automáticamente en la base de datos SQL para su posterior recuperación.

2.3.4. Respaldo/Recuperación de Información

2.3.4.1. El servidor será capaz de transferir todos los datos programados y el historial de transacciones a una unidad extraíble o cualquier unidad de disco lógica. Todos los datos programados serán restaurables desde el disco en caso de falla del hardware del sistema.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.5. Velocidades de Comunicación

2.3.5.1. El sistema tendrá comunicaciones bidireccionales y se comunicará hasta 2.5mb/s.

2.3.6. Impresoras

2.3.6.1. El sistema soportará todas las impresoras del sistema configuradas y compatibles con el sistema operativo Windows®.

2.3.7. Dispositivo Señalador

2.3.7.1. El sistema utilizará el dispositivo señalador configurado y compatible con el sistema operativo Windows®.

2.3.8. Puertos de Comunicación

2.3.8.1. El sistema soportará un número ilimitado de puertos seriales o TCP/IP.

2.3.9. Estaciones de Trabajo

2.3.9.1. El sistema soportará un número ilimitado de estaciones de trabajo activas locales o remotas. Estas estaciones de trabajo serán capaces de monitorear alarmas, cambiar la base de datos y recuperar registros de transacciones en tiempo real sin afectar a otras estaciones.

2.3.10. Redes

2.3.10.1. El sistema operará con el software de redes estándar de Windows®.

2.3.11. Base de datos

2.3.11.1. La base de datos será Microsoft SQL Server 2016/2017/2019.

2.3.12. Capacidades del Software

2.3.12.1. El Servidor del Sistema tendrá los siguientes requisitos mínimos:

SO: Server 2016, 2019, Windows 10 y 11 Pro
CPU: Dual Core Min de 3.0GHz
RAM 8GB
Espacio en disco duro principal: 200GB
GPU: 512MB RAM
Dispositivo señalador

2.3.12.2. El software del sistema y el software de desarrollo de lenguaje serán existentes, aceptados por la industria y de un tipo ampliamente utilizado en sistemas comerciales. El software de la aplicación deberá haber sido escrito en un lenguaje estándar, aceptado por la industria. Todas las funciones del Sistema serán accesibles a través de menús compatibles con el sistema operativo Windows®. Los sistemas que requieran control de cadenas de comandos o sintaxis compleja no serán aceptables. Los sistemas no dependerán de entradas externas distintas del teclado.

2.3.12.3. El software del sistema incluirá las siguientes características y estará configurado como mínimo:

Expansión ilimitada de lectores
Tarjeteros ilimitados en la base de datos

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

Estaciones de trabajo clientes simultáneas ilimitadas
Zonas horarias ilimitadas
365 días festivos definidos por el operador
Niveles de acceso ilimitados
Niveles de acceso para cada titular de tarjeta
Puntos de entrada de alarma ilimitados
Puntos de control de salida ilimitados
Cuentas de operador ilimitadas con niveles de privilegio definidos
Anunciación audible de alarma en la estación de trabajo
Mapas gráficos ilimitados para ser mostrados en la estación de trabajo
Capacidad de interfaz TCP/IP o RS-232 con un sistema CCTV, que proporciona cambio de cámara activado por alarma automáticamente.
Operación verdadera de 32/64 bits
Fechas de activación/cancelación del operador
Fechas de activación/cancelación del empleado
Imagen/credencial de video opcional e impresión de código de barras

2.3.13. Operadores

2.3.13.1. Los operadores tendrán las siguientes habilidades como mínimo.

2.3.13.1.1. Cambiar cualquier configuración del cliente desde cualquier estación de trabajo en la que estén trabajando.

2.3.13.1.2. Establecer Nombres de Estación. Los nombres de las estaciones serán definidos por el operador.

2.3.13.1.3. El diálogo de Estado de la Estación estará disponible. Mostrará una lista de estaciones y su estado en línea/fuera de línea, junto con los nombres de los operadores conectados.

2.3.13.1.4. Impresoras de Reportes: Los reportes solicitados por el operador se enviarán a la(s) impresora(s) que puedan residir en cualquier lugar de la red.

2.3.14. Descripción de la Ventana de Alarma

2.3.14.1. El sistema facilitará el procesamiento de alertas mediante el uso de una ventana emergente de alarma.

2.3.14.2. La ventana mostrará las alarmas del sistema y permitirá al operador reconocer y despejar mediante un clic derecho sobre el evento.

2.3.14.3. La ventana de alarma indicará la hora de la alarma y el tiempo de respuesta del operador.

2.3.14.4. La alarma incorporará mensajes de instrucciones programables para indicar al operador qué hacer y proporcionará una ventana de acción para que el operador registre una acción en el historial de la alarma.

2.3.15. Reconocimiento Masivo de Alarmas

2.3.15.1. El sistema proporcionará un medio para reconocer masivamente las alarmas, de modo que todas las alarmas puedan ser reconocidas con una sola acción del operador.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.16. Enrutamiento de Estaciones

2.3.16.1. El sistema admitirá el enrutamiento de alarmas a cualquiera o todas las estaciones. Los horarios podrán utilizarse para determinar a qué estación se envía una alarma durante un horario determinado. Una alarma podrá ser enviada a una estación o grupo de estaciones durante un horario y reenviada a otra estación o grupo de estaciones durante otro horario.

2.3.17. Enrutamiento de Operadores

2.3.17.1. El sistema admitirá el enrutamiento de alarmas a operadores particulares, independientemente de la estación en la que el operador haya iniciado sesión.

2.3.18. Configuraciones de Menú

2.3.18.1. El sistema permitirá la configuración y programación de controladores mediante el uso de una interfaz gráfica de usuario (GUI) sencilla. Todos los dispositivos y funciones serán configurables mediante clic derecho para facilitar su operación.

2.3.19. Memoria

2.3.19.1. La memoria dentro de cada controlador se configurará automáticamente por el sistema.

2.3.20. Actualizaciones de Base de Datos

2.3.20.1. El sistema descargará y cargará información a los controladores automáticamente mientras estos estén en comunicación con el servidor. También se podrá iniciar manualmente una descarga de datos.

2.3.21. Informes

2.3.21.1. El software del sistema tendrá la capacidad de informar datos seleccionables por tipo y por zona horaria. El software permitirá al operador generar un informe para pantalla, impresora o guardar en un archivo. Los informes deberán ser exportables a al menos diez (10) formatos de archivo diferentes. El sistema incorporará el uso de un generador automático de informes.

2.3.21.2. El sistema tendrá la capacidad de informar datos seleccionables por tipo y por zona horaria a cualquier combinación de estaciones de trabajo simultáneamente.

2.3.22. Puertos Seriales

2.3.22.1. Todos los puertos seriales se configurarán desde un menú fácil de seguir. Los sistemas que requieran un conocimiento profundo del sistema operativo o la configuración de CMOS para la configuración del puerto no serán aceptables.

2.3.23. Zonas horarias

2.3.23.1. El software del sistema tendrá la capacidad para un mínimo de 255 zonas horarias definibles por el operador. Cada zona horaria permitirá un mínimo de dieciséis (16) intervalos de tiempo individuales.

2.3.23.2. Las zonas horarias se podrán asignar a:

Aperturas; tales como puertas o pisos de ascensores
Funciones de reporte de alarmas
Titulares de tarjetas

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

Entradas
Salidas
Operaciones de impresoras
Puertos de mensajería TCP/IP y RS-232
Informes
Estaciones de trabajo

2.3.24. Días feriados

2.3.24.1. El software del sistema admitirá un mínimo de 365 feriados. Los feriados se considerarán con designación H1 o H2 para que haya tres horarios distintos de feriados. Un feriado podrá comenzar en cualquier momento/hora durante un día de 24 horas. Los sistemas que requieran que el horario de inicio del feriado sea a medianoche no serán aceptables.

2.3.25. Descripciones de Aperturas

2.3.25.1. Cada apertura en el sistema se identificará usando un formato de etiquetado lógico aprobado por el propietario. A cada descripción de apertura se le asignará un texto definible por el operador de hasta cincuenta (50) caracteres.

2.3.26. Modos de Control de Acceso

2.3.26.1. Cada apertura podrá ser programada para cambiar automáticamente, basándose en un horario definido por el operador, entre los siguientes modos de operación:
"TARJETA/SOLO TAG"
"TARJETA/TAG + PIN" – Se proporcionará autenticación dual para los puntos de acceso que requieran que el titular de la tarjeta utilice su credencial e ingrese un PIN de cuatro o cinco dígitos.
"SOLO PIN" – Los teclados/lectores se utilizarán en las aperturas para otorgar acceso a personas que conozcan un PIN válido.
"ALTA SEGURIDAD"
"REGLA DE DOS PERSONAS" – Para añadir seguridad adicional, se requerirá que dos titulares de tarjetas presenten una credencial cada uno para acceder a un área segura.
"ACCESO LIBRE"

2.3.27. Coacción (Duress)

2.3.27.1. Si el lector está operando en el modo "TARJETA/ETIQUETA + PIN" o "SOLO PIN", una función de coacción permitirá ingresar un código alternativo en el teclado para acceder.

2.3.27.2. El sistema generará una alerta y podrá vincularse para controlar relés para la notificación de la alarma.

2.3.28. Alarmas

2.3.28.1. Cada apertura podrá ser programada para generar alarmas de "ENTRADA FORZADA" y "PUERTA ABIERTA" (puerta dejada abierta). Estas alarmas tendrán la capacidad de tener un retardo de tiempo definible por el operador.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.29. Anunciación de Alarmas

2.3.29.1. Además de generar un mensaje de alarma, las siguientes condiciones podrán activar una salida para anunciación:

ENTRADA FORZADA
PUERTA ABIERTA (PUERTA ENTREABIERTA)
PUERTA NO ABIERTA
SEGURIDAD
PACIENTE
RASTREO DE CÓDIGOS
COACCIÓN
TARJETA/ETIQUETA INVALIDADA
TARJETA/ETIQUETA DENEGADA
VIOLACIÓN ANTIPASSBACK
ENTRADA DE PUERTA DE ALARMA
SABOTAJE

2.3.30. Descripción de Alarma

2.3.30.1. Cada punto de alarma podrá definirse con una descripción en texto simple de hasta cincuenta (50) caracteres.

2.3.31. Habilitación de Alarmas

2.3.31.1. Las entradas de alarmas se habilitarán durante zonas horarias definibles por el operador y podrán habilitarse/deshabilitarse manualmente desde cualquier estación de trabajo.

2.3.32. Alarmas Adicionales

2.3.32.1. El sistema también deberá generar alarmas para lo siguiente:

Tampering – Acceso al gabinete
Pérdida de comunicación del controlador
Falla del Canal 1 / Falla del Canal 2
Falla de batería
Falla de corriente alterna (AC)
Falla de fusible del lector
Falla de fusible auxiliar
Falla de fusible de cerradura
Manipulación de alarmas (supervisada)

2.3.33. Supervisión de Alarmas

2.3.33.1. Al usar entradas de alarma supervisadas, el sistema debe monitorear condiciones de “ABIERTO”, “CORTO”, además de “NORMAL/ANORMAL”.

2.3.34. Salida ASCII

2.3.34.1. Las entradas de alarmas deberán emitir un mensaje ASCII a través de un comando RS-232 o TCP/IP para la integración con cualquier otro dispositivo comandable por IP. Este comando/salida será opcional, definible por el operador

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

y transmitido en puntos de alarma que entren en estado anormal, regresen a un estado normal, o ambos.

2.3.35. Salidas

2.3.35.1. Relés de derivación: Las salidas definibles por el operador podrán asignarse como relés de derivación, permitiendo que las aperturas de acceso sean monitoreadas por sistemas de alarma de terceros.

2.3.35.2. Tiempo de “encendido” del relé: Las salidas asignadas para controlar aperturas serán definibles por el operador de 1 a 127 segundos o minutos.

2.3.36. Encriptación

2.3.36.1. Las contraseñas estarán encriptadas en la base de datos del operador usando encriptación para facilitar la confidencialidad de las contraseñas individuales de los operadores.

2.3.37. Niveles de Acceso del Operador

2.3.37.1. El sistema proporcionará niveles de acceso ilimitados para el operador del sistema. Todas las acciones del operador se registrarán en la base de datos del sistema.

2.3.38. Seguridad de Contraseñas

2.3.38.1. La contraseña del operador estará encriptada para evitar que los operadores vean las contraseñas. Las contraseñas podrán tener hasta veinte (20) caracteres alfanuméricos y ser sensibles a mayúsculas y minúsculas. Los operadores tendrán derecho a editar su propia contraseña para mantenerla en secreto.

2.3.39. Particionamiento

2.3.39.1. El sistema incorporará un verdadero particionamiento de base de datos por operador. Un operador podrá iniciar sesión en cualquier lugar del sistema y tener la misma funcionalidad en cualquier estación de trabajo. Los operadores estarán limitados a la vista y el control del sistema por su nivel de acceso de operador.

2.3.40. Roles del Operador

2.3.40.1. El sistema tendrá la capacidad de definir roles ilimitados de operadores. Como mínimo, los roles del operador serán:

Administrador General
Supervisor
Operador General

2.3.40.2. Los niveles de privilegio serán asignables a pero no limitados a las siguientes funciones del menú:

Ver
Editar
Editar cualquier campo dentro del menú
Seleccionar

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.41. Actividad del Operador

2.3.41.1. Toda la actividad del operador, incluidos los cambios específicos en la base de datos, se almacenará para su recuperación posterior y a los operadores se les asignará una zona horaria para el propósito de iniciar sesión.

2.3.42. Pista de Auditoría de Cambios en la Base de Datos

2.3.42.1. El sistema registrará cambios en la base de datos, incluyendo la fecha, hora, nombre del operador y descripción del registro modificado.

2.3.42.2. os mensajes de eventos de la pista de auditoría registrarán adiciones, eliminaciones y revisiones. El registro contendrá una marca de fecha/hora para el cambio, el nombre del operador que ha iniciado sesión, el nombre de la tabla, un carácter que identifique el cambio, y una descripción basada en el campo Nombre del registro, como el ID del operador, nombre del operador, nombre del controlador, nombre del dispositivo.

2.3.42.3. El sistema hará una restauración completa o parcial, dependiendo de la selección del operador de los datos o archivos de historial durante el proceso de respaldo.

2.3.42.4. El sistema permitirá la visualización de la pista de auditoría.

2.3.42.5. El sistema NO permitirá que la tabla de Pista de Auditoría sea editada.

2.3.43. Definiciones de Empleados

2.3.43.1. Ingreso de datos de tarjetahabientes - El ingreso de datos de titulares de tarjetas será sencillo para que se requiera una capacitación mínima. Se permitirá la entrada de credenciales y cambios a través de la interfaz directa con la pantalla del visor de eventos.

2.3.43.2. Credenciales - Las credenciales podrán tener múltiples niveles de acceso o niveles de acceso especiales asignados.

2.3.43.3. Desactivación de tarjetas - Las tarjetas podrán desactivarse en el sistema mientras los datos permanecen para su reactivación en una fecha posterior.

2.3.43.4. Datos de Credenciales - El sistema permitirá números de credenciales de hasta 18 dígitos.

2.3.43.5. Registros de tarjetahabientes - Los registros de tarjetahabientes consistirán, como mínimo, en lo siguiente:

Número de credencial
Nivel de emisión
Dos (2) grupos de nivel de acceso y zona horaria
Código PIN definible por el operador
Código de la instalación
Ubicación y estado de antipassback
Fecha de vencimiento
Alta seguridad
Privilegio de bloqueo/desbloqueo
Enlaces de códigos
Estado de seguimiento
Última puerta accesada
22 campos de texto y datos definibles por el operador
Duración de uso

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

Escolta
Shunt extendido (para cumplimiento con ADA)
Anulación de antipassback

2.3.43.6. Carga en lote - El software del sistema permitirá la entrada de grupos de tarjetas/etiquetas mediante el uso de un rango de números de tarjetas/etiquetas o por un campo de empleado de carga en lote.

2.3.44. Reportes/Informes

2.3.44.1. Almacenamiento de datos - Todo el historial programado y transaccional se almacenará automáticamente en la base de datos para su recuperación posterior.

2.3.44.2. Función del sistema - El software del sistema será capaz de generar informes sin afectar la operación en tiempo real del sistema.

2.3.44.3. Medios - Los informes se generarán a partir de la base de datos y serán exportables a al menos 10 formatos de archivo, incluidos PDF, DOC, XLS y otros.

2.3.44.4. Criterios de búsqueda - La base de datos estará estructurada de tal manera que el operador podrá determinar los parámetros de búsqueda en función de las variables disponibles en el menú de informes individual. No se aceptarán sistemas que requieran que el operador escriba cadenas de búsqueda complicadas.

2.3.44.5. Tipos de reportes:

2.3.44.5.1. Informes de datos definibles por el operador estarán disponibles para la siguiente información:

Datos del tarjetahabiente
Grupos de puertas
Zonas horarias
Puertas
Entradas
Relés
Enlaces
Controladores
Operadores
Configuración del hardware del sistema
Configuración de ajustes del sistema

2.3.44.5.2. Informes de transacciones - Los informes de transacciones estarán disponibles para lo siguiente:

Transacciones de credenciales
Transacciones de alarmas
Transacciones de eventos
Actividad del operador
Tiempo y asistencia

2.3.44.5.3. Programación de informes - El software del sistema tendrá la capacidad de agrupar informes para:

Informe en pantalla
Informe a una impresora de red
Guardar un informe en un archivo sin iniciación del operador

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.45. Guías del Sistema

2.3.45.1. Ayuda en línea - El software del sistema tendrá ayuda en línea disponible en cualquier punto que requiera la entrada del operador.

2.3.45.2. Sistema de ayuda estándar de Windows® - La pantalla de ayuda será accesible utilizando los sistemas de ayuda estándar de Windows®.

2.3.45.3. Información contextual - Estas pantallas de ayuda contendrán información contextual que permitirá al operador ingresar datos correctos sin consultar el manual.

2.3.45.4. Acceso al menú de ayuda - El menú de ayuda será accesible hasta el punto exacto en el software mediante la tecla de acceso rápido “F1”.

2.3.46. Estado del sistema

2.3.46.1. Estado en tiempo real - El operador podrá monitorear, a través de pantallas gráficas, el estado de los dispositivos, incluidas aperturas, entradas de alarmas y salidas en tiempo real.

2.3.46.2. Monitor de alarmas - Habrá una pantalla disponible para monitorear alarmas y ver, como mínimo, noventa y nueve (99) de los eventos más recientes. El operador también tendrá la capacidad de ver detalles adicionales de cualquier evento mediante el uso de una sola tecla o un clic del ratón.

2.3.47. Gráficos

2.3.47.1. Formato de archivo gráfico - Los planos de planta se configurarán en formato Bitmap, GIF, JPEG o PNG.

2.3.47.2. Programación - El software del sistema podrá importar planos de planta guardados como un archivo de tipo imagen.

2.3.47.3. Operación - Al activarse una entrada o salida de alarma seleccionada, el mapa se abrirá y mostrará el dispositivo en alarma con un icono de alarma. El operador podrá hacer clic en el mapa y borrar la alarma o controlar el dispositivo desde la interfaz del mapa interactivo.

2.3.48. Identificación con Video

2.3.48.1. Capacidad de imágenes y credenciales con video - El sistema tendrá la capacidad de permitir la captura de imágenes y credenciales con video, que funcionarán como un sistema integrado de control de acceso e identificación con video cuando se utilicen junto con el software del sistema.

2.3.48.2. Entrada de datos única - El sistema utilizará una sola estación de trabajo para ingresar datos tanto para el acceso como para la identificación con video. El sistema no requerirá que el operador ingrese los datos más de una vez.

2.3.48.3. Información de credenciales - La información de las credenciales, incluidos nombre, número de credencial, firma, huella digital, texto definido por el operador, código de barras y hasta cinco (5) campos de datos estarán disponibles para cada plantilla de credencial.

2.3.48.4. Fondos definibles por el operador - El sistema proporcionará fondos definibles por el operador. Estos fondos pueden ser una imagen "capturada" o un fondo de color. El sistema será compatible con impresoras de video compatibles con Windows 10 o 11 Pro.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.48.5. Configuraciones de credenciales - Las credenciales podrán crearse en configuraciones tanto horizontales como verticales.
2.3.48.6. Cambio de credenciales - Para cambiar la credencial de un titular de tarjeta, se podrá seleccionar un nuevo fondo de la tabla de fondos. No se requiere una nueva captura de imagen.
2.3.48.7. Captura de eventos por cámara - El sistema permitirá que cualquier entrada o lector sea programado de tal manera que un evento en esa ubicación sea capturado por una cámara remota y mostrado mientras se almacena en la base de datos para su posterior visualización o impresión. Los eventos en el lector se mostrarán en tiempo real y almacenarán una "pantalla dividida" que mostrará la imagen del titular de la tarjeta almacenada junto a la imagen "capturada".
2.3.48.8. Control de cámaras - El control de las cámaras se logrará a través de una interfaz serial o TCP/IP compatible desde el sistema a un conmutador de video. La programación del conmutador de cámara para las entradas y lectores individuales no requerirá salir del programa de control de acceso.
2.3.48.9. Estaciones de trabajo adicionales - Se podrán agregar estaciones de trabajo adicionales para credenciales y/o alarmas a través de LAN.

2.3.49. Captura de Imágenes

2.3.49.1. Importación y almacenamiento de imágenes - El sistema tendrá la capacidad de importar imágenes de empleados y almacenarlas en la base de datos. Estas imágenes podrán ser recuperadas y mostradas por el operador.
2.3.49.2. Captura de imágenes desde cámaras IP - El sistema tendrá la capacidad de capturar y guardar imágenes desde cámaras IP.
2.3.49.3. Respaldo y restauración de imágenes - El sistema proporcionará el respaldo y la restauración de imágenes capturadas.

2.3.50. Integración con VMS y NVR/DVR

2.3.50.1. Integración con dispositivos VMS, NVR y DVR - El sistema se integrará sin problemas vía TCP/IP con dispositivos VMS, NVR y DVR de múltiples fabricantes simultáneamente.
2.3.50.2. Asociación de cámaras con dispositivos - El operador tendrá la opción de asociar cualquier cámara con un dispositivo y, a través de una ventana de video común, controlar y operar cualquier dispositivo con visualización en tiempo real.
2.3.50.3. Acceso a video - El video será accesible desde cualquier dispositivo mediante un clic derecho. El historial de video de cualquier evento será accesible mediante un clic derecho. La ventana de video se abrirá automáticamente al activarse la alarma del dispositivo asociado.
2.3.50.4. Vista de video común - El video será común para todos los sistemas de los fabricantes, de modo que el operador solo verá una vista.

2.3.51. Tour Interáctivo de Guardias

2.3.51.1. Módulo de tour interactivo de guardia - El sistema incorporará un módulo interactivo de tour de guardia para proporcionar el estado en tiempo real de la progresión del guardia. El incumplimiento de completar un tour activará alarmas en el sitio y fuera del sitio para operaciones de seguridad de vida.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.3.52. Gestión de Activos

2.3.52.1. Módulo de gestión de activos - El sistema incorporará un módulo de gestión de activos para que los propietarios sean asignados a equipos o vehículos para prevenir el robo. Al activarse una alarma, el sistema notificará mediante alarma, interfaz de CCTV y estado de correo electrónico el evento inapropiado.

2.3.53. Herramientas del Sistema

2.3.53.1. Asistente de copia - El sistema proporcionará un asistente de copia para copiar rápidamente cualquier parámetro de dispositivo a cualquier otro dispositivo individual o grupo de dispositivos.

2.3.53.2. Programador de respaldo - El sistema tendrá un programador de respaldo para el respaldo automático de datos.

2.3.53.3. Campos personalizables para titulares de tarjetas - El sistema tendrá la capacidad de diseñar datos de titulares de tarjetas personalizados agregando nuevos campos a voluntad.

2.3.54. Registro de Huellas Dactilares/Biométricos

2.3.54.1. Pestaña de registro de huellas dactilares/biométricos - El software tendrá una pestaña integrada en la pantalla de titulares de tarjetas para permitir que el operador registre huellas dactilares/biométricos directamente desde el software.

2.3.55. Red de Controladores C-NET –

2.3.55.1. La C-NET es la red de comunicaciones que enlaza los controladores de red entre sí.

2.3.55.2. Cada C-NET puede soportar hasta quince (15) controladores de red. Deben estar conectados entre sí a través de una conexión RS-485 y cada panel tomará su dirección de sus interruptores tipo DIP.

2.3.56. Red de Controladores D-NET

2.3.56.1. La D-NET es la red de comunicaciones que enlaza los controladores de lectores de tarjetas (RC-2/N-IRC/N-URC) y los controladores de entrada/salida (IOC-16) a los controladores de red en la C-NET.

2.3.56.2. Hasta cuatro (4) RC-2/N-IRC/N-URCs y dieciséis (16) IOC-16s pueden conectarse a un solo controlador de red a través de una conexión RS-485 y cada panel tomará su dirección de sus interruptores tipo DIP.

2.3.57. Red de Controladores E-NET

2.3.57.1. La E-NET es la red de comunicaciones que enlaza los controladores de red entre sí.

2.3.57.2. Cada E-NET puede soportar hasta quince (15) controladores de red. Están conectados entre sí a través de TCP/IP y cada panel tomará la dirección a través de la red, sin necesidad de usar los interruptores DIP, pero deben estar en la misma LAN.

2.3.58. Cambio de Dirección IP

2.3.58.1. Al utilizar direcciones IP estáticas para los controladores y por cualquier motivo, migrar todas las direcciones IP de los dispositivos y cambiarlas, los controladores

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

detectarán este cambio y permitirán que el proceso de cambio de dirección IP se realice sin problemas.

2.3.59. Integración ACS/VMS

2.3.60. La integración debe ser a través de TCP/IP (conexiones de relé y/o RS-232 no son aceptables).

2.3.61. Todos los dispositivos dentro del sistema ACS deben tener una pestaña para asociar una cámara de video del VMS al dispositivo. Esta asociación debe permitir que la cámara se llame en la interfaz gráfica de usuario del ACS en las siguientes condiciones:

2.3.61.1. Cualquier evento entrante de un dispositivo especificado.

2.3.61.2. Cualquier alarma entrante de un dispositivo especificado.

2.3.61.3. La cámara, si es PTZ, también debe ser llamada a su posición prediseñada.

2.3.62. El ACS debe poder conectarse al sistema VMS y mostrar la ventana de video predeterminada del VMS como un cliente de visualización nativa del VMS.

2.3.63. El ACS debe tener la capacidad de mostrar cualquier evento de video designado para aparecer automáticamente sin intervención del operador.

2.3.64. El ACS debe tener la capacidad de llamar manualmente video haciendo clic en el evento en cualquier lugar que aparezca en el ACS.

2.3.65. El ACS debe tener la capacidad de colocar dinámicamente las cámaras del sistema VMS en sus mapas y llamar video desde los mapas directamente.

2.3.66. El ACS debe tener la capacidad de informar todos los eventos etiquetados con video y reproducirlos directamente desde el informe dentro de la interfaz gráfica de usuario del ACS.

2.4. Hardware – Controladores AxiomXa

2.4.1. Controlador TCP/IP UNC-500

2.4.1.1. El controlador será un dispositivo electrónico de estado sólido controlado por un microprocesador de 32 bits e incluirá un reloj/calendario en tiempo real a bordo. Las placas de circuito estarán hechas de construcción chapada en oro (no se aceptarán de cobre o con plomo) e incorporarán tecnología flash-ware.

2.4.1.2. La comunicación consistirá en un protocolo estándar LAN/WAN TCP/IP de canal único o dual.

2.4.1.3. Un subconjunto de la base de datos del sistema suficiente para soportar funciones de acceso y alarma para sus lectores y puntos designados se almacenará en el controlador.

2.4.1.4. En caso de pérdida de comunicación, el controlador continuará funcionando sin degradación de la operación y proporcionará almacenamiento de al menos 30,000 eventos y hasta un máximo de 100,000 eventos con capacidad de memoria extendida. Estos eventos almacenados se cargarán automáticamente a la base de datos al restablecerse las comunicaciones.

2.4.1.5. l controlador será capaz de realizar todas las funciones del sistema indefinidamente sin el Servidor.

2.4.1.6. El controlador debe estar listado por FCC, CE, RoHS y (c)UL.

2.4.1.7. El controlador debe tener 8MB de RAM disponibles a bordo.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.4.1.8. El controlador debe tener tres (3) puertos RS-485 programables.
2.4.1.9. El controlador debe tener dos (2) puertos de lector Wiegand a bordo para aceptar cualquier formato Wiegand y hasta cinco (5) formatos Wiegand simultáneamente.
2.4.1.10. El controlador debe tener ocho (8) entradas totalmente supervisadas capaces de configuración individual para EOL (EOL simple y doble), N.A., N.C.
2.4.1.11. El controlador debe tener ocho (8) salidas. Cuatro (4) salidas de relé tipo 'C' clasificadas para 10A-30VDC y cuatro (4) salidas de colector abierto clasificadas para 100mA.
2.4.1.12. El controlador debe tener una o dos conexiones LAN TCP/IP a bordo capaces de configurarse en modo de conmutador LAN u operación LAN dual para configuraciones de comunicación Clase 'A'.
2.4.1.13. El controlador debe tener una entrada de manipulación separada.
2.4.1.14. El voltaje de entrada debe soportar 12VDC o 30W PoE+, corriente máxima de 500mA.
2.4.1.15. El controlador debe tener un circuito de carga interna para una batería de respaldo de gel de 12VDC. El controlador deberá ser capaz de recargar una batería de respaldo desde una fuente PoE+ o una fuente de alimentación local de 12VDC.
2.4.1.16. El controlador deberá ser configurable en los siguientes métodos: dispositivo Edge, montaje en pared o montaje en rack.
2.4.1.17. El despliegue del dispositivo Edge será PoE+ y operará continuamente incluso si se pierde PoE. El controlador Edge operará una (1) o dos (2) aperturas según se desee.
2.4.1.18. La configuración de montaje en rack será de 2 controladores UNC-500 o cuatro (4) aperturas en una configuración estándar de rack de 1U – 19 pulgadas. Las conexiones LAN serán frontales como configuración de red estándar. Todas las conexiones de dispositivos serán independientes y extraíbles desde la parte trasera del rack para una desconexión rápida y una fácil resolución de problemas. Todos los gabinetes de montaje en rack tendrán rieles opcionales para configuración de deslizamiento. Todos los gabinetes de montaje en rack tendrán panel superior extraíble para acceder a los paneles de control.
2.4.1.19. El controlador, cuando se configure en modo de conmutador, permitirá el looping LAN de un dispositivo TCP/IP estándar a otro como cualquier conmutador de red estándar permite sin el uso de conmutadores externos o cableado LAN especial.
2.4.1.20. El controlador debe aceptar y controlar hasta siete (7) controladores de lectores subordinados y dieciséis (16) controladores de E/S simultáneamente.
2.4.1.21. e definen enlaces como cualquier acción que cause una reacción en el sistema. Cada controlador será capaz de iniciar 'Enlaces' independientemente del estado de la computadora.
2.4.1.22. Los lectores tendrán la capacidad de iniciar comandos de '3 deslizamientos' y/o '4 deslizamientos' basados en la programación del titular de la tarjeta para iniciar una secuencia diferente de eventos según la necesidad.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.4.1.23. El controlador será capaz de almacenar y leer hasta cinco (5) formatos de credenciales personalizados simultáneamente. El controlador podrá leer el formato de la mayoría de las credenciales codificadas con efecto Wiegand, RFID, código de barras o banda magnética.

2.4.1.24. El controlador será capaz de leer números de credenciales de hasta dieciocho (18) dígitos.

2.4.1.25. El controlador tendrá la capacidad de almacenar hasta 128 zonas horarias, cada una con hasta 16 intervalos de tiempo. Cada intervalo de tiempo consistirá en un rango de días (siete días de la semana, además de un horario de días festivos) así como un rango de tiempo. El panel controlador gestionará automáticamente las zonas horarias basándose en su reloj interno.

2.4.1.26. El controlador permitirá la definición de hasta 255 días festivos con hasta 128 calendarios de días festivos. El controlador gestionará automáticamente las zonas horarias basándose en su reloj interno.

2.4.1.27. El controlador permitirá la definición de 'Horarios Automáticos' los cuales permitirán al sistema cambiar el modo de una salida de alarma o un 'Modo de Acceso' del lector automáticamente basado en un 'Horario Diario' sin intervención del operador.

2.4.1.27.1. Solo Tarjeta / Tag
2.4.1.27.2. Solo PIN,
2.4.1.27.3. Solo Código,
2.4.1.27.4. Tarjeta/Tag más PIN,
2.4.1.27.5. Alta Seguridad
2.4.1.27.6. Libre Acceso.
2.4.1.27.7. Estos modos de operación se programarán desde el ordenador anfitrión del sistema y cambiarán automáticamente según la asignación de la zona horaria.

2.4.1.28. El sistema debe soportar grupos de interbloqueo para la operación de MAN-Traps.

2.4.1.29. El panel controlador debe permitir la operación de anti-retorno, en la cual los titulares de las tarjetas deben seguir una secuencia correcta de entrada/salida.

2.4.2. Controlador UNC-100

2.4.2.1. El controlador debe ser un dispositivo electrónico de estado sólido controlado por un microprocesador de 32 bits e incluir un reloj/calendario en tiempo real a bordo. Las placas de circuito deben ser de construcción chapada en oro (no se aceptarán de cobre o con plomo) e incorporar tecnología de firmware actualizable.

2.4.2.2. La comunicación debe consistir en un protocolo estándar de red TCP/IP de un solo canal en un entorno LAN/WAN.

2.4.2.3. Un subconjunto de la base de datos del sistema suficiente para soportar funciones de acceso y alarmas para sus lectores y puntos designados debe almacenarse en el controlador.

2.4.2.4. En caso de pérdida de comunicación, el controlador debe continuar funcionando sin degradación de la operación y debe proporcionar almacenamiento de al

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

menos 30,000 eventos. Estos eventos almacenados se cargarán automáticamente a la base de datos al restablecer las comunicaciones.

2.4.2.5. El controlador debe ser capaz de realizar todas las funciones del sistema indefinidamente sin el Servidor.

2.4.2.6. El controlador debe tener certificación FCC, CE, RoHS y (c)UL.

2.4.2.7. El controlador debe tener 2MB de RAM disponible a bordo.

2.4.2.8. El controlador debe tener un (1) puerto RS-485 programable.

2.4.2.9. El controlador debe tener dos (2) puertos de lector Wiegand a bordo para aceptar cualquier formato Wiegand y cinco (5) formatos Wiegand simultáneamente.

2.4.2.10. El controlador debe tener cuatro (4) entradas completamente supervisadas capaces de configuración individual para EOL (EOL simple y dual), operación N.O., N.C.

2.4.2.11. El controlador debe tener cuatro (4) salidas. Dos (2) salidas de relé de forma 'C' con una capacidad de 10A-30VDC y dos (2) salidas de colector abierto con una capacidad de 100mA.

2.4.2.12. El controlador debe tener una entrada de manipulación separada.

2.4.2.13. Voltaje de entrada: 12VDC o 30W PoE+, corriente máxima: 500mA.

2.4.2.14. El controlador debe tener un circuito de carga interna para una batería de respaldo de gel de 12VDC. El controlador debe ser capaz de recargar una batería de respaldo desde una fuente PoE o una fuente de alimentación local de 12VDC.

2.4.2.15. El controlador debe ser configurable de las siguientes maneras: Dispositivo de borde, Controlador montado en la pared.

2.4.2.16. El despliegue del dispositivo de borde debe ser PoE+ y operar continuamente incluso si se pierde el PoE. El controlador de borde debe operar una (1) o dos (2) aperturas según sea necesario.

2.4.2.17. El controlador debe aceptar y controlar hasta siete (7) controladores de lector subordinados y dieciséis (16) controladores de E/S simultáneamente.

2.4.3. Controlador de Entrada/Salida IOC-16

2.4.3.1. Las entradas y salidas adicionales deben estar disponibles añadiendo controladores de E/S. Cada controlador de E/S debe tener un mínimo de dieciséis (16) terminales de entrada/salida supervisados. Las entradas deben incorporar supervisión completa de siete (7) tipos de circuitos y las salidas deben ser de forma "C". Hasta dieciséis (16) controladores de E/S deben estar disponibles para cada controlador de la serie UNC.

2.4.3.2. El controlador de E/S debe ser alimentado independientemente y tener su propio suministro de energía de respaldo y circuito de carga para una operación en espera mínima de 4 horas.

2.4.4. Controlador de Lector RC-2

2.4.4.1. El controlador debe tener la certificación (c)UL y también cumplir con las regulaciones FCC y CE.

2.4.4.2. Arquitectura:

2.4.4.2.1. El controlador debe soportar dos (2) aperturas de control de acceso.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.4.4.2.2. El controlador debe soportar medios locales de control a través de enlaces de sistema y hardware, así como entrada de lector y/o teclado.
2.4.4.2.3. El controlador debe soportar interfaz de campo para ocho (8) entradas de alarma configuradas de diversas maneras
2.4.4.2.4. El controlador debe tener ocho (8) salidas.
2.4.4.3. Esta funcionalidad debe permitir que cualquier controlador fuera de línea mantenga la capacidad completa de procesamiento de control de acceso. Un tarjetahabiente no debe estar al tanto de la condición fuera de línea.
2.4.4.4. Comunicaciones:
2.4.4.4.1. La red de comunicación por cable debe estar cableada con un cable blindado de par trenzado de 18 AWG.
2.4.4.4.2. La red cableada debe tener una longitud máxima de 1220 metros.
2.4.4.4.3. Esta red debe estar cableada en una configuración lineal.
2.4.4.5. El controlador debe estar configurado para informar varios mensajes de estado de comunicación del panel al Servidor con habilidades para:
2.4.4.5.1. Suprimir tipos de mensajes individuales de una entrada de alarma específica según un horario.
2.4.4.5.2. Mostrar un mensaje predefinido para cada tipo de evento de una entrada de alarma específica.
2.4.4.6. El controlador debe proporcionar informes de eventos de los siguientes eventos: Panel en línea, Panel fuera de línea y Problemas del panel.
2.4.4.7. Configuración del Hardware:
2.4.4.7.1. Direccionamiento del Panel – La dirección del controlador debe configurarse mediante cuatro interruptores DIP a bordo. Las direcciones disponibles deben ser del uno (1) al dieciséis (16).
2.4.4.7.2. Configuraciones de velocidad de comunicación – La velocidad de comunicación del controlador debe configurarse mediante dos interruptores DIP a bordo. Las tasas disponibles deben ser 9.6, 28.8, 38.4 y 56 kbps.
2.4.4.7.3. El controlador debe proporcionar medios para la sintonización de la red RS-485, específicamente: baja polarización, alta polarización y terminación. La sintonización debe realizarse ajustando los puentes (jumpers).
2.4.4.8. Interfaz de Lector:
2.4.4.8.1. El controlador debe soportar interfaz de campo para lectores de control de acceso de varios tipos.
2.4.4.8.2. La unidad debe soportar hasta cinco (5) formatos de credenciales diferentes simultáneamente.
2.4.4.8.3. La unidad debe soportar todas las tecnologías principales de lectores:
2.4.4.8.3.1. RFID
2.4.4.8.3.2. Banda Magnética
2.4.4.8.3.3. Wiegand
2.4.4.8.3.4. Código de barras
2.4.4.8.3.5. Teclado
2.4.4.8.3.6. RFID con teclado integrado
2.4.4.8.3.7. Banda magnética con teclado integrado

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.4.4.8.3.8. Geometría de mano
2.4.4.8.3.9. Huella dactilar
2.4.4.8.4. La unidad debe proporcionar control dedicado sobre LEDs Rojo y Verde para cada punto de acceso.
2.4.4.8.5. La unidad debe proporcionar control dedicado sobre el Zumbador para cada punto de acceso.
2.4.4.8.6. Se requerirán longitudes de cable de 500 pies utilizando cables de seis (6) u ocho (8) conductores blindados.
2.4.4.9. Fuente de Energía:
2.4.4.9.1. La unidad proporcionará ocho entradas de alarma completamente programables.
2.4.4.9.2. Cada entrada de alarma admitirá todos los siguientes tipos de circuitos:
2.4.4.9.2.1. N.O. no supervisado
2.4.4.9.2.2. N.C. no supervisado
2.4.4.9.2.3. N.O. supervisado con una resistencia
2.4.4.9.2.4. N.C. supervisado con una resistencia
2.4.4.9.2.5. N.O. supervisado con dos resistencias
2.4.4.9.2.6. N.C. supervisado con dos resistencias
2.4.4.9.2.7. Combinación de N.O. y N.C. supervisado con una resistencia
2.4.4.9.3. Se requerirán longitudes de cableado de 1,000 pies utilizando cables de 20 o 22 AWG.
2.4.4.10. Salidas de alarma:
2.4.4.10.1. La unidad proporcionará ocho salidas completamente configurables (cuatro de relé de forma 'C' y cuatro de colector abierto).
2.4.4.10.2. Cada salida se configurará como segura o sin fallos.
2.4.4.10.3. Las salidas de relé tendrán una clasificación de 2A @ 30VDC.
2.4.4.10.4. Las salidas de colector abierto conmutarán -12VDC @ 100mA.
2.4.4.11. Dimensiones del Recinto:
2.4.4.11.1. El recinto para el controlador tendrá las siguientes dimensiones: 12”(30.4cm) x 14” (35.5cm) x 3½” (8.9cm)
2.4.4.12. Tolerancias Ambientales:
2.4.4.12.1. La unidad funcionará dentro de las siguientes tolerancias ambientales – Temperatura de funcionamiento: 35-150°F (1.6-65°Celsius) Humedad de funcionamiento: 20-80% HR (sin condensación)

2.5. Gabinetes de Pared RBH-ENCL2

2.5.1. El gabinete una cubierta con bisagra con cerradura de llave. Un punto de entrada del panel de control monitoreará un interruptor de sabotaje del gabinete.
2.5.2. El gabinete tendrá dimensiones de 22” (55.8cm) x 18”(45.7cm) x 4”(10.1cm) con perforaciones de ½” (12mm) y ¾” (19mm). La parte trasera del gabinete tendrá monturas para llaves para facilitar el montaje.
2.5.3. El gabinete podrá contener dos de los siguientes controladores: UNC-100, UNC-500, RC-2 e IOC-16.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.6. Lectores y Credenciales

2.6.1. El sistema empleará una tecnología de control de acceso/identificación sin contacto que utilice circuitos RF en forma de microchip. Los microchips estarán codificados y transmitirán la información codificada cuando se activen.

2.6.2. Los lectores serán de cualquier tipo de salida Wiegand o equivalente de proximidad / iCLASS / MiFARE / DESFire. Leerán el número de identificación de la credencial cuando se presente en la superficie del lector sin requerir contacto físico.

2.6.3. Un lector de ventana/marco de puerta de una sola pieza, que se montará directamente en un montante/marco de puerta de metal estándar de 1.75" (4.5cm). El lector se puede montar en interiores o exteriores en prácticamente cualquier superficie, incluido el metal. El lector funcionará entre 5-14VDC para permitir facilidad y flexibilidad en la instalación. El rango de lectura con una credencial RFID estándar será de hasta 4" (hasta 10cm) cuando se instale de acuerdo con las especificaciones del fabricante. Las dimensiones máximas del lector serán 5.5" (14.0cm) de alto x 1.6" (4.1cm) de ancho x 0.75" (1.9cm) de grosor.

2.6.4. Un lector de interruptor de pared de una sola pieza, que se montará directamente en una caja eléctrica estándar de una sola ganga de metal o plástico, o en una pared plana o superficie de metal, y funcionará en interiores o exteriores. El lector funcionará entre 5-14VDC para permitir facilidad y flexibilidad en la instalación. El rango de lectura con una credencial RFID estándar será de hasta 4" (10cm) cuando se instale de acuerdo con las especificaciones del fabricante. Las dimensiones máximas del lector serán 4.6" (11.7cm) de alto x 2.9" (7.6cm) de ancho x 0.5" (1.3cm) de grosor.

2.6.5. Un lector de una sola pieza, que se montará en cualquier superficie, incluido el metal, o se puede ocultar detrás de la mayoría de los materiales de construcción, excepto el metal. El rango de lectura con una credencial RFID estándar será de hasta 7" (17cm) cuando se instale de acuerdo con las especificaciones del fabricante. Las dimensiones máximas del lector serán 4.6" (11.7cm) de alto x 5.5" (14cm) de ancho x 1.4" (3.6cm) de grosor.

2.6.6. n lector de rango medio, que se montará en la mayoría de las superficies, excepto directamente sobre metal, o se puede ocultar detrás de la mayoría de los materiales de construcción, excepto metal. El rango de lectura con una credencial RFID estándar será de hasta 21" (42cm) cuando se instale de acuerdo con las especificaciones del fabricante. Las dimensiones máximas de la cabeza del lector serán 8.8" (22.4cm) de alto x 8.8" (22.4cm) de ancho x 1.14" (2.9cm) de grosor.

2.6.7. La credencial se leerá cuando se presente en cualquier orientación o ángulo a la superficie del lector dentro del rango de lectura adecuado.

2.6.8. El lector alimentará la credencial, procesará los datos codificados y enviará los datos al sistema de acceso en menos de 110 milisegundos.

2.6.9. No habrá una placa o cubierta extraíble que permita el acceso a la electrónica del lector.

2.6.10. Un LED rojo/verde en la superficie frontal del lector indicará al titular de la tarjeta que la credencial fue leída (controlada internamente/por el lector) y se tomó una decisión de acceso (controlada por el sistema). El LED se puede configurar en modo de línea única o de línea dual (permitiendo un estado "apagado") según lo requiera

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

el sistema anfitrión, y el lector se puede cambiar entre modos presentando una credencial de programación a la cara del lector.

2.6.11. El lector tendrá una función de tono de "pitido" audible para indicar al titular de la tarjeta que la credencial fue leída (controlada internamente/por el lector) y se tomó una decisión de acceso (controlada por el sistema). El tono de audio debe ser controlable de forma independiente y no estar vinculado al estado o color del LED. El control interno del LED y del zumbador se puede habilitar/deshabilitar mediante una credencial de programación para no requerir el ajuste de interruptores internos en el lector.

2.6.12. El lector tendrá un diagnóstico incorporado, que indicará al instalador que al encender el lector ha realizado una prueba interna y está funcionando correctamente.

2.6.13. El lector tendrá una función de diagnóstico incorporada, que permitirá a un solo técnico probar la continuidad de las líneas de datos independientemente del controlador. El lector se puede colocar en el modo de diagnóstico de línea mediante una credencial de programación, y luego el técnico podrá medir los pulsos en el extremo de la línea sin necesidad de un segundo técnico en el lector presentando credenciales.

2.6.14. Las conexiones eléctricas entre el lector y el controlador serán mediante cable blindado multiconductor con código de colores, calibre #22 AWG. No se requerirá cable coaxial ni conectores especiales. La salida será en forma de flujo de datos Wiegand.

2.6.15. El cableado desde el conjunto del lector hasta el controlador se ejecutará dentro de conduits metálicos o EMT, según lo requieran los códigos eléctricos. Todas las cajas de conexiones estarán ocultas y no serán accesibles para el público en general. No se aceptará la utilización de conduits de PVC.

2.6.16. La transmisión accidental o intencional de señales de RF al lector no comprometerá el sistema.

2.6.17. El lector funcionará en el modo normal o de antipase sin necesidad de cambios en el lector.

2.6.18. El rango de temperatura de funcionamiento del lector será de -40° a +50°C.

2.6.19. Los daños o vandalismo en el lector no dañarán ninguna otra parte del sistema.

2.6.20. La manipulación del lector no afectará la seguridad del acceso.

2.6.21. Los lectores del sistema tendrán la capacidad de aceptar códigos de cualquiera de los siguientes dispositivos RFID:

2.6.22. Una credencial de plástico moldeado estándar del tamaño de una tarjeta de crédito con dimensiones máximas de 3.41" (8.7cm) x 2.14" (5.4cm) x 0.09" (0.23cm), y un peso de no más de 0.48 oz. (13.5g). Se proporcionará una ranura perforada para una correa o clip. La credencial será capaz de tener gráficos personalizados de varios colores y números marcados permanentemente impresos directamente en ambos lados.

2.6.23. Una etiqueta con dimensiones máximas de 2.2" (5.6cm) x 1.3" (3.3cm) x 0.25" (0.6cm), y un peso de 0.36 oz. (9.9g). Se proporcionará un ojal para sujeción a un llavero.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.6.24. Una credencial del tamaño de una tarjeta de crédito fabricada en PVC, con un grosor máximo de .036", y la capacidad de aceptar gráficos e imágenes de fotografías impresas directamente y capaz de llevar una banda magnética de alta coercitividad.
2.6.25. Una credencial del tamaño de una tarjeta de crédito con un grosor máximo de .048" (1.2mm), y capaz de aceptar una fotografía y gráficos mediante una solapa laminada por el cliente.
2.6.26. La credencial será una forma basada en policarbonato que no se puede imprimir directamente. La credencial será una unidad de tecnología de sensor RFID basada en PVC dual. Cumplirá con las normas ISO en cuanto a grosor (3 mm).
2.6.27. a credencial estará hecha de plástico ABS robusto para proporcionar máxima protección para la circuitería interior y ofrecer flexión mínima que pudiera causar daños a la credencial.
2.6.28. La presencia de objetos metálicos pequeños, como llaves o monedas cerca de la credencial, no alterará el código leído por el lector, ni impedirá que el lector lea el código.
2.6.29. a credencial será de un formato propietario que estará bajo control del Propietario.
2.6.30. Las credenciales serán numeradas secuencialmente. El comprador podrá especificar códigos o números.
2.6.31. La credencial deberá tener la capacidad de tener el número codificado marcado permanentemente en la superficie exterior.
2.6.32. La credencial será un dispositivo pasivo sin batería interna, pero contendrá un elemento semiconductor, que se energizará al acercarse dentro del rango de operación del lector, causando la transmisión del código desde la credencial al lector. No se aceptarán credenciales que requieran una batería interna o una celda de energía.
2.6.33. Las credenciales podrán utilizarse de manera intercambiable y serán compatibles con todos los lectores del sistema, independientemente del tamaño o estilo físico del lector, y sin necesidad de emparejamiento de códigos o dispositivos de memoria en el lector.
2.6.34. El rango de temperatura de operación de la credencial será de -40° a +50°C.

2.7. Teclados de Alarma

2.7.1. El sistema deberá incorporar teclados de alarma que se conecten directamente al sistema para operaciones avanzadas de alarma. No se aceptará la integración con sistemas de alarma de terceros.
2.7.2. Los operadores podrán armar, desarmar, enviar mensajes y monitorear cualquier alarma en el teclado. Además, los teclados deberán tener zonas de entrada y salida y la capacidad de iniciar comandos en el sistema ingresando un código o comando.
2.7.3. os teclados tendrán la capacidad de armar o desarmar cualquier grupo de entradas en el sistema, creando un panel de intrusión de alarma sin problemas.
2.7.4. Integración de Monitoreo de Alarma:
2.7.4.1. El sistema permitirá la anunciación de alarmas de detección de intrusión. Las alarmas de detección de intrusión se informarán igual que cualquier otra alarma

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

de control de acceso y tendrán las mismas propiedades de anunciación y visualización que las alarmas de control de acceso.

2.7.4.2. Las alarmas del teclado de alarma se mostrarán en la ventana de monitoreo de alarmas y cualquier señal podrá enviarse a través de puerto de mensajes TCP/IP o RS-232.

2.7.4.3. El sistema admitirá una descripción detallada de la alarma que mostrará la "Descripción de la alarma", "Fecha/hora", "Controlador", "Dispositivo" y "Área" asociados con la alarma. La información también mostrará al operador.

2.7.4.4. El sistema admitirá el rastreo de dispositivos y áreas de detección de intrusión.

2.7.4.5. El sistema podrá informar información de estado para los dispositivos de detección de intrusión.

2.7.4.6. En caso de alarma, el sistema cambiará automáticamente al mapa que muestra la alarma, el icono que representa ese punto de alarma parpadeará y se generará una alerta audible en el sistema de sonido de la estación de trabajo. El operador deberá reconocer la alarma antes de procesarla.

2.7.4.7. En el modo de procesamiento de alarma del operador, el sistema permitirá al operador:

- 2.7.4.7.1. Borrar alarmas, tamper y alarmas de diagnóstico.
- 2.7.4.7.2. Observar vistas de cámara CCTV, individualmente o en grupos, que estén asociadas con una alarma (requiere opción de conmutador de video).

2.7.4.8. En el modo de procesamiento normal, el sistema permitirá a un operador:

- 2.7.4.8.1. Ver una lista de información de actividad y seleccionar y etiquetar cualquier evento.
- 2.7.4.8.2. Ver mapas del sitio.
- 2.7.4.8.3. Realizar una prueba de dispositivos/sensores que se pueden probar.
- 2.7.4.8.4. Cambiar el estado de los sensores a acceso o seguro.
- 2.7.4.8.5. Revisar los últimos 1,000 eventos/acciones realizados en el sistema.

2.7.4.9. En el modo de procesamiento de mantenimiento, el sistema permitirá al técnico de mantenimiento:

- 2.7.4.9.1. Asignar contraseñas y acceso de función a usuarios individuales.
- 2.7.4.9.2. Examinar los estados de los puntos de entrada/salida.
- 2.7.4.9.3. Ajustar la sensibilidad de los sensores.
- 2.7.4.9.4. Acceder al sistema operativo para diagnosticar problemas del sistema.
- 2.7.4.9.5. Configurar la fecha y la hora del reloj del calendario (en Windows).
- 2.7.4.9.6. Cambiar el formato de la fecha mostrada (en Windows).
- 2.7.4.9.7. Configurar los parámetros de comunicación para los dispositivos del sistema.
- 2.7.4.9.8. Apagar el sistema.

2.7.5. Características Especiales del Hardware del Teclado de Alarma

2.7.5.1. Combinación de Control de Acceso, Alarma contra Robos, Estaciones de Armado de Teclados y Funcionalidad de Monitoreo en un controlador sin precedentes y una solución de seguridad completa.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.7.5.2. Se adapta a cualquier aplicación de seguridad que requiera funcionalidad de Control de Acceso y Alarma contra Robos, como Hogar, Pequeñas Empresas, Corporativas, Industriales y Condominios.
2.7.5.3. Puede optimizarse para aprovechar la infraestructura del edificio para una implementación rápida y económica en el entorno LAN/WAN. Esto evita la necesidad de instalar una infraestructura de comunicación RS-485 dedicada separada, ahorrando tiempo y dinero.
2.7.5.4. xpansible y flexible con hasta 256 zonas de alarma disponibles para cada teclado y un número ilimitado de teclados, nunca será necesario instalar múltiples controladores de robo en una instalación, incluso si los edificios no están en la misma propiedad.
2.7.5.5. Empaquetado con características como Control de Acceso integrado, PoE+, notificación por correo electrónico, notificación por SMS.
2.7.5.6. ompleto con acceso remoto a través de web o aplicación.
2.7.5.7. Capacidad de credenciales: 500 para modo independiente, o hasta 50,000 en modo integrado.
2.7.5.8. Construido con 4 entradas y 2 salidas incorporadas.
2.7.5.9. Admite 32 Zonas para modo independiente, o hasta 256 zonas en modo integrado.
2.7.5.10. Contiene 1 MB de memoria para el almacenamiento de tarjetas, un solo canal RS-485, PoE+ y un solo puerto lector Wiegand.

2.8. Integración de Lectores de Huellas Dactilares/Biométricos y Software

2.8.1. El lector de huellas dactilares será de la serie RBH-BFR.
2.8.2. El software tendrá una pestaña integrada en la pantalla del titular de la tarjeta para permitir que el operador inscriba huellas dactilares/biométricas directamente desde el software. Los programas que abran software de terceros son inaceptables.
2.8.3. La plantilla de captura permitirá la captura de un dedo primario y secundario como respaldo.
2.8.4. La autenticación se descargará automáticamente al lector después de la captura exitosa de la huella dactilar sin intervención del operador. La descarga se realizará mediante comunicaciones TCP/IP a los lectores de huellas dactilares.
2.8.5. La huella dactilar debe guardarse como un algoritmo para proteger la privacidad individual.
2.8.6. El algoritmo de huellas dactilares se guardará dentro de la base de datos normal de AxiomXa para capacidades automáticas de respaldo y restauración. No se aceptan sistemas de respaldo externo para huellas dactilares.
2.8.7. El lector de huellas dactilares será configurable para operar en cualquiera de los siguientes modos: Solo dedo, solo tarjeta, Tarjeta y dedo, Dedo y código PIN, huella o tarjeta.
2.8.8. El lector tendrá una salida Wiegand para conectarse al controlador.

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

2.9. Integración de Cerraduras Inalámbricas

2.9.1. El sistema admitirá la integración de cerraduras inalámbricas de Assa Abloy Aperio, Allegion AD-400 y la plataforma Engage y SALTO System con el sistema de gestión de seguridad.

2.9.2. El sistema inalámbrico y sus componentes ofrecerán como mínimo:

2.9.2.1. Frecuencia de radio inalámbrica basada en IEEE 802.15.4 a 2.4 GHz.

2.9.2.2. La comunicación inalámbrica incorporará cifrado AES de 128 bits.

2.9.2.3. El tiempo de lectura será inferior a 150 milisegundos.

2.9.2.4. Tecnologías RFID: Proximidad, MiFARE, DESFire, HID iCLASS.

2.9.2.5. Alimentación mediante baterías comerciales estándar no propietarias. La renovación de las baterías solo será posible desde el lado seguro de cualquier puerta con acceso al compartimento de la batería, solo alcanzable utilizando conjuntos de herramientas no disponibles comercialmente proporcionados exclusivamente por el fabricante.

2.9.2.6. Todos los dispositivos de bloqueo electrónico deben poder activarse temporalmente mediante un dispositivo adecuado en caso de falla total de la batería.

2.9.2.7. El sistema de control de acceso tendrá un sistema de informes de administración de baterías completo para permitir la visualización del estado de la batería de cualquier dispositivo de bloqueo en el sistema en cualquier momento.

2.9.2.8. Los dispositivos de bloqueo mismos proporcionarán, al activarse con una credencial u otro medio, una señal audible y distinguible cuando cualquier batería se reduzca a sus últimos 1,000 ciclos utilizables.

2.9.2.9. El sistema admitirá más de 500 cerraduras inalámbricas; cada configuración de controlador UNC-100 o UNC-500 estará clasificada según la cantidad de cerraduras que puede admitir.

2.9.2.10. Once a lockset is installed and registered with the controller, it appears in the security application as a traditional access point, which can be enabled and configured to work with the controller.

2.9.3. Cuando una cerradura inalámbrica se conecte al controlador, informará su número de designación.

2.9.4. Todas las cerraduras conectadas al sistema se tratarán como una cerradura en línea y se les asignará el perfil de cerradura predeterminado (en línea).

2.9.5. Las cerraduras pueden asignarse a ubicaciones.

2.9.6. as cerraduras se pueden agregar y gestionar en planos de planta.

2.9.7. Las cerraduras se pueden desbloquear momentáneamente mediante acciones de eventos o desde el sistema a través de las estaciones de trabajo, incluida la vista del plano de planta, el cliente del navegador web o la aplicación móvil.

2.9.8. La actividad asociada con una cerradura se puede ver en tiempo real en el registro de actividad.

3. Instalación

3.1. El Contratista deberá instalar todos los componentes del sistema de acuerdo con las instrucciones del fabricante y proporcionará todas las interconexiones, servicios y

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515

ajustes necesarios para un sistema completo y operativo según se especifica y muestra. Se instalarán líneas de alimentación, control, señal y comunicaciones, y transmisión de datos, además de todas las conexiones de puesta a tierra necesarias para evitar que los bucles de tierra, ruidos y sobretensiones afecten adversamente el funcionamiento del sistema. Se proporcionará el hardware de montaje según sea necesario.

3.2. Todos los productos, software, herramientas de programación, etc., estarán registrados en El Propietario y se entregarán al completar con éxito el proyecto.

3.3. Todos los cables de baja tensión fuera de la consola de control, gabinetes, cajas y similares, deberán tener clasificación de plenum cuando lo exija el código. El cable no se debe tirar en conductos ni colocar en canalizaciones, compartimientos, cajas de salida, cajas de conexiones o accesorios similares con otros cables de edificio.

3.4. Todas las entradas estarán protegidas contra sobretensiones inducidas en el cableado del dispositivo. Las salidas estarán protegidas contra sobretensiones inducidas en el control y el cableado del dispositivo instalado en exteriores. Todo el equipo de comunicaciones estará protegido contra sobretensiones inducidas en cualquier circuito de comunicaciones. Todos los cables y conductores, excepto las fibras ópticas, que sirvan como circuitos de comunicaciones desde la consola de seguridad hasta el equipo de campo y entre el equipo de campo, tendrán circuitos de protección contra sobretensiones instalados en cada extremo.

3.5. 3.5. No se permitirá que ningún cableado esté expuesto; todo el cableado debe estar completamente encerrado en un conducto metálico roscado, que deberá instalarse subterráneamente, en paredes o en estructuras metálicas, a menos que sea físicamente imposible. Cualquier conducto que esté expuesto deberá estar completamente encerrado dentro de una jaula protectora de metal expandido que sea resistente al vandalismo y esté equipada con una alarma antimanipulación. Todo el montaje del equipo debe ser tal que el equipo no pueda ser removido ni manipulado.

END OF SECTION

RBH Access Technologies Inc.
2 Automatic Rd Suite 108, Brampton, ON L6S 6K8
905-790-1515