موسوعة التيار الخفيف

نظام التحكم فى الدخول والخروج

Security Access Control System

م. أحمد محمود عيسى

Email- Eng.Ahmedessa2020@gmail.com

مقدمة

قد يتم فرض التحكم في الوصول الجغرافي من قبل بعض الأفراد (على سبيل المثال ، الحدود ، الحارس ، مدقق التذاكر) ، أو باستخدام جهاز مثل الباب الدوار قد تكون هناك أسوار لتجنب التحايل على التحكم في الوصول فإن أحد البدائل للتحكم هو ظهور نظام ACA

يشير مصطلح التحكم في الوصول أو الدخول إلى ممارسة تقييد الدخول إلى عقار أو مبنى أو غرفة على الأشخاص المصرح لهم يمكن تحقيق التحكم في الوصول المادي بواسطة الإنسان (حارس أو موظف استقبال) أو من خلال الوسائل الميكانيكية مثل الأقفال والمفاتيح ، أو من خلال الوسائل التكنولوجية مثل أنظمة التحكم .

يحدد نظام التحكم فى الدخول في وصول من يُسمح لهم بالدخول أو الخروج ، وأين يُسمح لهم بالخروج أو الدخول ، ومتى يُسمح لهم بالدخول أو الخروج تم تحقيق ذلك جزئيًا من خلال المفاتيح والأقفال عندما يتم قفل الباب ، لا يمكن إلا لمن لديه مفتاح الدخول من الباب ، اعتمادًا على كيفية تكوين القفل لا تسمح الأقفال والمفاتيح الميكانيكية بتقييد حامل المفتاح بأوقات أو تواريخ محددة .

يستخدم التحكم الإلكتروني في وصول أجهزة الكمبيوتر لحل قيود الأقفال والمفاتيح الميكانيكية يمكن استخدام مجموعة كبيرة من البيانات لاستبدال المفاتيح الميكانيكية ويمنح نظام التحكم في الوصول الإلكتروني حق الوصول بناءً على بيانات الاعتماد المقدمة عند منح الوصول ، يتم فتح الباب لفترة محددة مسبقًا ويتم تسجيل المعاملة عند رفض الوصول ، يظل الباب مغلقًا ويتم تسجيل محاولة الوصول سيقوم النظام أيضًا بمراقبة الباب والتنبيه إذا تم فتح الباب بالقوة أو فتحه لفترة طويلة بعد فتحه.

ما هو نظام التحكم فى الدخول Access Control System؟

نظام التحكم في الوصول هو تكامل لأجهزة وبرامج وأدوات الإدارة والتحكم التي تراقب إلكترونيًا

والتحكم في الدخول من خلال الأبواب والبوابات والمصاعد والعديد من نقاط الدخول الأخرى.

تم العثور على أنظمة التحكم في الوصول في كل مكان تقريبًا يمكن العثور عليها في الفنادق والمستشفيات والمطارات والبنوك ،السجون والمنشآت العسكرية والنوادي الاجتماعية والمجمعات السكنية والمكتبات والمصانع والعديد من الأماكن الأخرى

أصبحت أنظمة التحكم في الوصول اليوم أكثر تعقيدًا فالعديد من تطبيقات الأمان الأخرى يتم دمجها مع نظام التحكم في الوصول لجعلها نظام أمان كامل.

بعض أنظمة الأمان يجري دمجها مع نظام التحكم فى الدخول هى : • CCTV • كشف التسلل • HVAC • تقارير الوقت والحضور.

تستخدم العديد من أنظمة التحكم في الوصول الشبكة لأغراض الاتصال ويتم توصيل المعلومات من خلال هذه الشبكات، مثال على نظام التحكم في الوصول؛ حيث يمكن فتح الباب ببطاقة ممغنطة أو نظام RFID أو بغيرهما .

يوفر نظام التحكم عن بعد الأمان من خلال منح تحكم مرن لمن يُسمح له بدخول مقر عملك، هذا النظام أحد أكثر الأنظمة المستخدمة انتشارًا في التحكم الإلكتروني يتم وضعه أمام الأبواب باستخدام بطاقة أو شريط مغناطيسي يمكن الوصول إليه عن طريق التمرير من خلال قارئ على الباب.

يمكن التحكم في كل نقطة وصول بشكل فردي وفقًا لمتطلبات الشركة أو المؤسسات حيث يكون الأمان العالي ضروريًا أمان الشبكة مهم أيضًا، خاصة في الشركة التي تتعامل مع البيانات الحساسة.

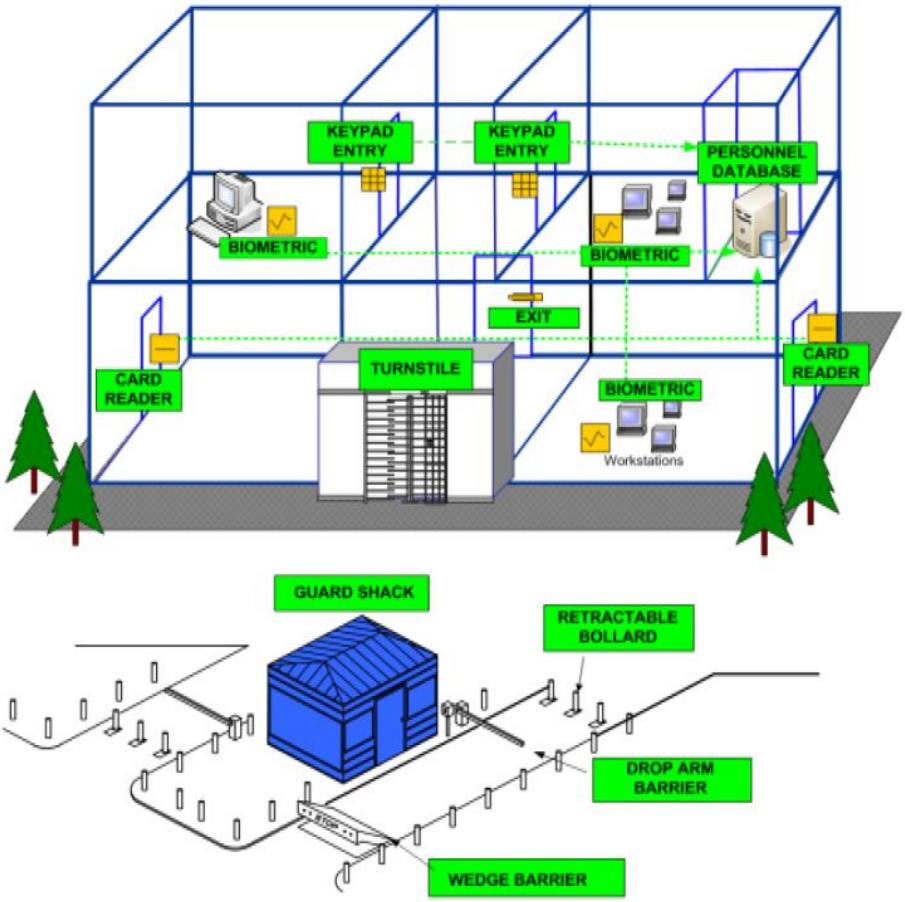
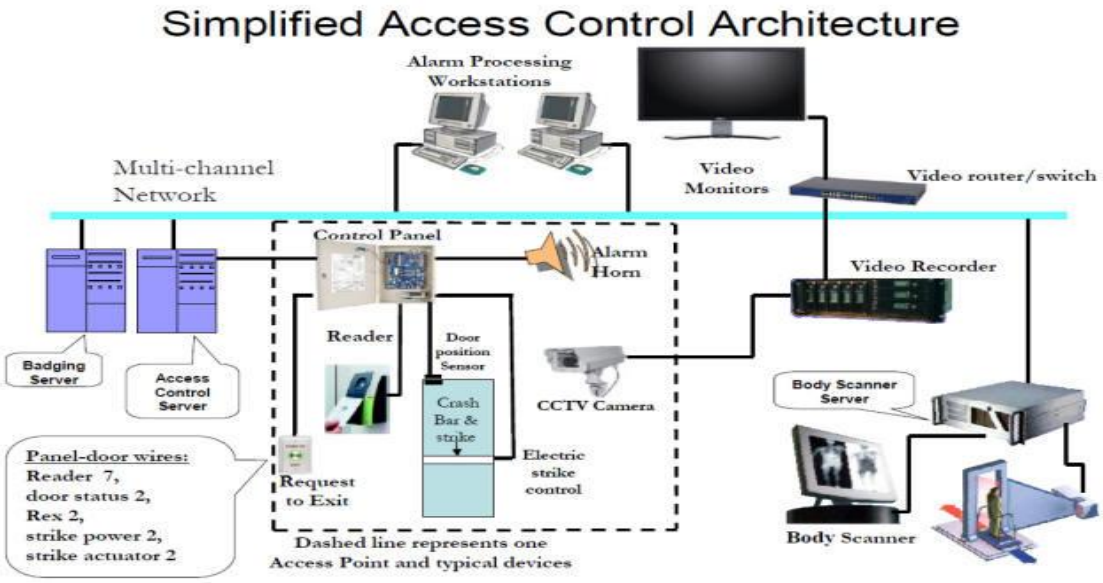


Figure 2-1. Access Control Schematic



أنواع أنظمة التحكم فى الدخول والخروج

يبدأ التحكم في دخول محيط المنشأة عالية الخطورة فهو مصمم لتقييد الوصول وحماية الموظفين والمبنى والخدمات من التهديدات الخارجية فالعنصر الرئيسي فى حماية المباني هو إنشاء مسافة مناسبة للوقوف على أساس خصائص المبنى خط الدفاع الأول هو تصميم الطرق ومواقف السيارات بالقرب من المبنى .

A-Barriers الحواجز

تتحكم أجهزة الحاجز في وصول المركبات إلى مناطق محددة مع توفير مستويات مختلفة من الأمن للمنشأة تعمل الحواجز بشكل عام على حماية نقاط دخول المركبات والتحكم فيها من خلال السماح للمركبات المصرح لها فقط و تتوفر العديد من أنماط الحواجز .

تمنع الحواجز في المقام الأول المركبات غير المصرح لها من دخول منطقة خاضعة للسيطرة عن طريق إغلاق مسار السفر يمكن استخدامها أيضًا لتوجيه أو إبطاء حركة المرور بالقرب من منطقة خاضعة للرقابة ، وردع المركبات من خلال وجودها ، وامتصاص تأثير السيارة أو إتلاف السيارة أثناء محاولات التسلل هناك عدة أنواع من الحواجز المتاحة لتطبيقات محددة ، مثل حواجز الزينة على حافة الأرصفة والحواجز القابلة للسحب لوصول المركبات في حالات الطوارئ إلى مناطق المشاة.

1-Crash Gates

هي بوابات فولاذية تنزلق عبر طريق إما على مسار أو على جانب الطريق يتم استخدامها لوقف حركة مرور المركبات غير المرغوب فيها عندما يتم ترخيص المركبة ، تفتح البوابة للسماح بمرور السيارة تعتبر بوابات الاصطدام آلية دفاع فعالة ويمكن أن تكون جذابة من الناحية المعمارية.

2-Ground Retractable Automobile Barrier

نظام حاجز السيارات القابل للسحب الأرضي (®GRAB) ، كما هو موضح في الشكل ، هو حاجز نشط للمركبة ، يستخدم الكابلات الفولاذية ومكابس امتصاص الطاقة لإيقاف المركبات و تقليل إصابة ركاب السيارة تم تصميمه ليتم إعادة ضبطه وإعادته إلى التشغيل بعد الاصطدام نظرًا لقدراته على امتصاص الإصطدام ، يوفر النظام الأمان مع الحفاظ على قدر كبير من سلامة الحاجز هذا اعتبار مهم حيث يتم تدمير العديد من الحواجز بعد اصطدام السيارة ، مما يترك الموقع معرضًا للخطر أثناء استعادة الحاجز

3-Wedge

حواجز الوتد ، كما هو موضح في الشكل ، عبارة عن أجهزة فولاذية تعمل هيدروليكيًا بزاوية لأعلى من مستوى الأرض لإنشاء حافة منيعة فوق سطح الطريق يشكل حاجز الوتد جزءًا من سطح الطريق بمجرد نشره ، يقوم الحاجز الإسفيني بعمل زاوية 45 درجة من سطح الطريق في مواجهة اتجاه حركة السيارة ويتم اقترانه بلوحة أساس لامتصاص الطاقة الحركية من الصدمة هذه الأجهزة فعالة للغاية ضد محاولة اختراق المركبات.

4-Drop Arm

تُستخدم حواجز الذراع المنسدلة ، كما هو موضح في الشكل ، بشكل شائع في مواقف السيارات والجراجات للتحكم في دخول وخروج المركبات المصرح بها إن أذرع بعض المنتجات قادرة على إيقاف المركبات غير المصرح بها عندما تكون في الوضع السفلي تتضمن بعض حواجز الذراع المتساقطة كبلًا مصممًا لربط وتدمير الطرف الأمامي للمركبة التي تحاول الاختراق.

تُستخدم الحواجز كعائق مادي لمنع أو تقييد الوصول إلى منطقة ما بعض تطبيقات الحواجز هي:

1- الحواجز الداخلية:- تعتبر مفيدة في المستودعات ومواقف السيارات والبيئات الداخلية الأخرى التي توجد بها المركبات.

قد يتم وضع حواجز لحماية البنية التحتية الحيوية ، مثل وحدات التحكم في الطاقة أو وحدات تكييف الهواء قد تحمي أيضًا مناطق وصول المشاة أو تبطئ تقدم حركة مرور المركبات عبر منطقة ما.

2- الحواجز الخارجية:- تُستخدم بشكل أساسي للتطبيقات الخارجية في أي منشأة للمساعدة في تنظيم حركة مرور المركبات وإيقاف محاولات التسلل المتعمدة.

3- الحواجز المحمولة:- مفيدة للمحيط المؤقت وحالات التحكم في الوصول وهي تغطي مجموعة من الأجهزة البلاستيكية خفيفة الوزن إلى الإصدارات الخرسانية التي يجب نقلها باستخدام معدات الرفع الميكانيكية غالبًا ما تكون الإصدارات البلاستيكية خفيفة الوزن ذات ألوان زاهية ، ويمكن ملؤها بالماء ، وتستخدم بنفس طريقة استخدام أقماع المرور لتحذير الجمهور من الظروف الخطرة أو القيود المؤقتة على الوصول إلى المركبات.

B-Bollards الحواجز البلورية

تقيد الحواجزالبلورية وصول المركبات إلى مناطق محددة مع توفير مستويات مختلفة من الأمن للمنشآت والمشاة تسمح الحواجزالبلورية بمرور المشاة دون عوائق ، على عكس الحواجز الأخرى التى تم ذكرها .

تأتي الحواجزالبلورية في عدد من الأساليب وتوفر مستويات مختلفة من الأمان مع مجموعة متنوعة من الخصائص الجمالية الأعمدة القابلة للسحب أو القابلة للإزالة متاحة للحالات التي تتطلب فقط الوصول العرضي للمركبات المصرح بها أو الطوارئ يمكن إنشاء الأعمدة من الخرسانة أو الفولاذ أو الحديد الزهر أو البلاستيك في مجموعة متنوعة من الأشكال والأحجام أصبحت الحواجزالبلورية أكثر انتشارًا في تصميمات المرافق بسبب ارتفاع مستوى قبول الجمهور لها إنهم يوجهون ويردعون المركبات من خلال وجودهم ، لكنهم لا يعيقون حركة المشاة أثناء محاولات اقتحام المركبات ، تمتص الأعمدة الطاقة الحركية وتسبب أضرارًا للمركبة

Bollards Types

1-Fixed Bollards

2-Removable Bollards

3-Retractable or Automatic Bollards

4-Manual and Semi-Automatic Removable Bollards

5-Portable Bollards

تُستخدم الحواجز البلورية في المقام الأول للتطبيقات الخارجية ، ولكنها مفيدة في التطبيقات الداخلية حيث قد تكون المركبات موجودة ، مثل المستودعات أومواقف السيارات أو الساحات أو الملاعب.

في التصميمات الداخلية للمباني ، يمكن وضع الأعمدة لحماية البنية التحتية الحيوية مثل وحدات التحكم في الطاقة أو وحدات تكييف الهواء أو مناطق وصول المشاة أو المواقع التي يلزم فيها الفصل بين حركة مرور المركبات والمشاة.

في التطبيقات الخارجية ، يمكن استخدام الأعمدة لتحديد منطقة خالية من المركبات أو لتقييد حركة مرور المركبات من طرق وطرق معينة الاستخدامات النموذجية للأعمدة المحمولة هي حماية أماكن وقوف السيارات ، أو منع المركبات من سد ممر ، أو توفير تحذير من مخاطر السلامة.

C-Turnstiles and Portals البوابات الدوارة

تدير البوابات الدوارة تدفق حركة المشاة والوصول عند نقاط التفتيش تتراوح تقنيات Turnstile من حامل ثلاثي القوائم بسيط قائم بذاته بدون وظائف محاسبية إلى حواجز يتم تنشيطها كهربائيًا باستخدام الماسحات الضوئية التي تعد مكونات لأنظمة التحكم في الوصول المؤتمنة بالكامل.

وهى عبارة عن أبواب يتم التحكم فيها كهربائيًا وتستخدم كفتحات يتم التحكم فيها في حاجز مادي يمكن استخدام البوابات منفردة أو في مجموعات لتشكيل mantraps كأداة تأخير المانترابس هو عبارة عن ترتيب للأبواب ، عادة ما يشكل ممرًا صغيرًا أو كشكًا ، والذي يسمح للشخص بالدخول والتعرف عليه قبل الشروع في منطقة خاضعة للرقابة غالبًا ما يتم استخدامها في التطبيقات عالية الأمان التي تتطلب تدقيقًا فرديًا ويمكن أن تتسامح مع معدلات الإنتاجية المنخفضة.

تشجع البوابات الدوارة الموظفين والزوار على الالتزام بإجراءات التحكم في الوصول وتقليل الحاجة إلى أفراد الأمن لمراقبة نقاط الدخول والخروج توفر بعض المنتجات معلومات حول اتجاه السفر ويمكنها حساب عدد المشاة. غالبًا ما يتم ترتيب طرق الوصول باستخدام علامات أو درابزين بحيث يشكل الأشخاص الذين ينتظرون الوصول خطاً تتضمن معظم الشركات المصنعة أجهزة مطالبة صوتية أو مرئية للإشارة إلى اتجاه السفر وأجهزة إنذار لمحاولات الدخول دون إذن.

تُستخدم البوابات الدوارة للتحكم في المشاة في المطارات ، والمدارس ، والملاعب ، والساحات ، والأمن المحيط ، والتحكم في حشود البيع بالتجزئة ، وتحصيل أجرة النقل ، والتحكم في الوصول إلى المبنى حيث تكون الإنتاجية

العالية ضرورية تُستخدم البوابات في المواقف الأمنية العالية التي تتطلب مزيدًا من التدقيق لكل فردغالبًا ما تكون البوابات متشابكة كشعار عندما يكون الفحص مطولًا مطلوبًا من كل شخص يسعى للوصول.

D-Guard Facilities أكشاك الحراسة

توفر أكشاك الحراسة المأوى لحارس المنشأة أو أفراد التحكم في الدخول ، كما هو موضح في الشكل غالبًا ما يكون كشك الحراسة هو أول ما يواجهه الزائر عند دخوله إلى منشأة آمنية تجمع العديد من الأكشاك الموجودة في السوق اليوم بين المظهر الجمالي ودرجة عالية من القوة والمتانة قد لا يكون كشك الحراسة أكثر من ملجأ مادي ضد العوامل الجوية ، أو قد يكون مكونًا من حصن آمن ضد الهجمات الجسدية تتوفر أكشاك عالية الأمان تلبي أو تتجاوز المعايير التجارية للحماية من الإنفجارات .

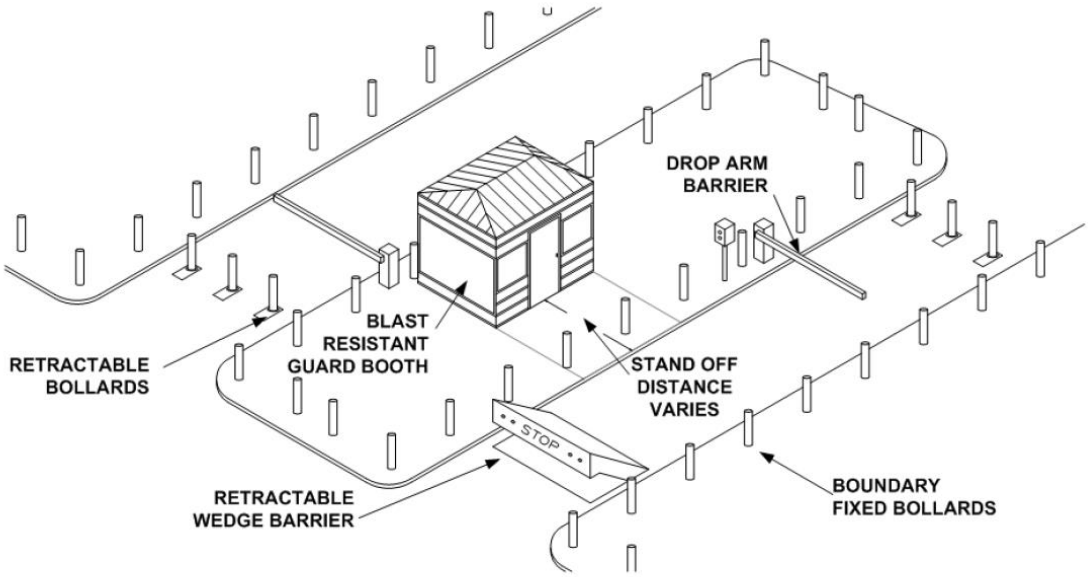


Figure 3-8. Guard Facility at Entry Point

تقع معظم أكشاك الحراسة خارج المنشأة عند مدخل السيارة ونقاط وصول الأفراد أو نقاط تسجيل الوصول للزوار غالبًا ما يتم تصنيعها مسبقًا وفقًا لاحتياجات العميل الأمنية والجمالية ويتم شحنها مباشرة إلى المنشأة تتوفر العديد من الخيارات التي تتراوح من أدراج المعاملات إلى مرافق الحمامات الكاملة تتوفر أكشاك محمولة بمستويات مختلفة من الحماية .

E-Tokens and Cipher Systems

هناك ما لا يقل عن ثلاث كتل وظيفية في أي نظام تحكم في الوصول يعتمد على الرموز الميكانيكية أو الإلكترونية الرمز المميز نفسه ، وقارئ الرمز المميز ، ولوحة التحكم في الدخول و توفر لوحة التحكم في الوصول إشارات تحكم لأجهزة الأمان ، مثل الأقفال الكهربائية أو المغناطيسية ، بناءً على المدخلات من قارئ الرموز المميزة.

الرمز المميز هو جهاز مادي (على سبيل المثال ، بطاقة الهوية أو سلسلة المفاتيح) التي تسهل المصادقة لحاملها للدخول إلى أماكن محمية قد يتم فحص الرمز المميز بواسطة أفراد الأمن أو مصادقته إلكترونيًا بواسطة قارئ الرمز المميز و الاستجابة مثل كلمة المرور الإلكترونية أو رقم التعريف الشخصي ، أو باستخدام إجراء خوارزمي آخر.

يمكن استخدام نظام التحكم في الدخول إلى الرمز المميز المصمم والمثبت بشكل صحيح لمراقبة الوصول المادي ، والوصول المنطقي (على سبيل المثال ، الكمبيوتر والشبكة) ، ووقت الموظف وحضوره ، بالإضافة إلى عدد من الوظائف الأخرى المصممة لتلبية أمن المنظمة وإدارتها تم .

1-1-Identification Cards and Badges

تعد البطاقات والشارات أكثر أشكال التعريف شيوعًا المستخدمة في صناعة التحكم في الدخول غالبًا ما يكون لديهم صورة لصاحب التسجيل واسم المالك واسم المنظمة أو شعارها وغيرها من المعلومات ذات الصلة يعد الترميز الشريطي والتصوير المجسم ووضع العلامات المائية وكيمياء انتهاء الوقت هي التقنيات الأساسية المتاحة لتخصيص نظام شارة تعريف معين يتجاوز المعلومات الأساسية والصورة يمكن أن تستوعب العديد من أنظمة البطاقات أو الشارات أكثر من واحدة من تقنيات التخصيص هذه.

-Barcoding

يمكن للبطاقات والشارات ذات الرموز الشريطية أن تحقق تحديدًا تلقائيًا بدون مفتاح وجمع البيانات لأنظمة التحكم في الوصول وتستخدم عادةً في التطبيقات ذات الأمان المنخفض تستخدم الرموز الشريطية خطوطًا عمودية ذات ارتفاع وعرض متفاوتين والتي تمثل رمز أمان يقوم القارئ بتحليل الرمز الشريطي ، والتحقق منه مقابل قائمة التحكم في الوصول ، ويسمح لحامل البطاقة أو يُمنع من الوصول إلى المنطقة حددت العديد من الصناعات ، خاصة السيارات والإلكترونيات والمواد الكيميائية ، معايير لاستخداماتها وتطبيقاتها تضمن هذه المعايير الامتثال العالمي داخل الصناعة ودقة تحديد الهوية أفضل من 99 بالمائة.

-Holographic Imaging

الصورة العاكسة ثلاثية الأبعاد هي صورة مطبوعة على بطاقة التي تستخدم تقنيات حيود الضوء لإنتاج صورة يمكن رؤيتها ولكن لا يمكن نسخها تُستخدم الصورة الثلاثية الأبعاد كتقنية لمكافحة التزوير على الشارات ؛ ومع ذلك ، فإن المعدات المستخدمة لإنشاء هذه الصور قد تكون باهظة الثمن وقد لا تكون فعالة من حيث التكلفة.

-Time Expiring Chemistry

تستخدم بطاقات أو شارات انتهاء الوقت تقنيات لإدخال مواد كيميائية تفاعلية في السطح أو التصفيح تتفاعل المواد الكيميائية في فترة زمنية معروفة وتغير لونها كيميائيا مع انتهاء الوقت وهى مفيدة للأشخاص الذين يجب أن يكون لديهم وصول مؤقت فقط إلى منشأة أو منطقة يمكن طباعة شارة منتهية الصلاحية بمعلومات أو صور ، بما في ذلك الصور ، ثم يتم تطبيق التقنية وتنشيطها تتراوح حدود الوقت من ساعة واحدة إلى شهر واحد عندما ينتهي الوقت ، يتغير اللون أو يتلاشى على كل أو جزء من البطاقة .

-Watermarking

العلامة المائية هي صورة على السطح يمكن رؤيتها ولكن لا يمكن نسخها ويمكن استخدامها كتقنية لمكافحة التزوير.

التطبيقات لهذه البطاقات والإشارات

بطاقات الهوية والشارات هي أدوات أمان من الدرجة الأولى بالنسبة للعديد من المرافق ، فهي كل ما هو مطلوب في حالة وجود حراس لمراقبة الدخول ، يجب على الأشخاص الذين يدخلون بشكل متكرر إبراز شارة المنشأة أو بطاقة الهوية ويتم إبعاد الزائرين والأشخاص الآخرين الذين يفتقرون إلى الشارات لتقديم طلب للحصول على إذن للدخول. غالبًا ما يُطلب من حاملي الشارات إظهار شارتهم بشكل بارز طوال فترة وجودهم في المنطقة الخاضعة للرقابة.

يمكن أن تكون البطاقات أو الشارات الأساس لأنظمة التحكم في الوصول عالية الأمان التي تعتمد على استخدام تقنيات الموظفين والإدارة بدلاً من البنية التحتية الإلكترونية على سبيل المثال ، تستخدم بعض المرافق شارتين لتعريف الصورة للتحكم في الوصول تُمنح الشارة الأولى إلى شخص التحكم في البوابة ، الذي يطابقها مع ملف

شارات الوصول الداخلية عند العثور على تطابق ، يتبادل الحارس الشارات ويسمح للفرد بالوصول إلى المنشأة. يجب أن تكون الشارة الثانية مرئية في جميع الأوقات في المنطقة المحمية يتم تبديل الشارات مرة أخرى عندما يغادر الفرد المنطقة المحمية في حين أن هذا النوع من النظام لا يعتمد بشكل كبير على التكنولوجيا ، إلا أنه يقدم بعض المزايا .

1-2-Keycard Door Systems

تحتوي أنظمة أبواب Keycard على قارئ متصل مباشرة بالباب وهي جزء لا يتجزأ من آلية التحكم في المزلاج غالبًا ما يتم استخدامها في الفنادق والمستشفيات لتوفير مستوى منخفض نسبيًا من الأمان لموظفي العميل في المواقف التي يحتاج فيها كل عميل إلى إذن لفتح بعض الأبواب ، وربما غرفته الخاصة ، والمبنى بعد ساعات لا تتفاعل أنظمة بطاقات المفاتيح المثبتة على الباب في الوقت الفعلي مع قاعدة بيانات مركزية يتم تخزين المعلومات المتعلقة بنشاط الباب في نظام تسجيل يعمل بالبطارية داخل الصندوق المثبت على الباب ويجب تنزيلها في قارئ محمول باليد ، والذي يمكن تنزيله بعد ذلك في جهاز كمبيوتر مركزي لحفظ السجلات.

التطبيقات لهذا النظام

لا تُستخدم أنظمة Keycard غالبًا في المواقف عالية الأمان لأن القارئ لا يتفاعل عادةً مع قاعدة بيانات مركزية للتحكم في الدخول ؛ ومع ذلك ، تسمح هذه التقنية بالمرونة والتحكم الدقيق في الوصول والقدرة على السماح أو منع الوصول من خلال باب واحد أو مجموعة من الأبواب على سبيل المثال ، يمكن بسهولة إعادة قفل الأبواب في حالة فقد المفتاح أو سرقته ، ويمكن بسهولة تعديل الوصول لتلبية المتطلبات الخاصة يمكن ترميز مفاتيح الغرفة ومفاتيح الموظفين ومفاتيح المديرين لتحسين الأمان والإنتاجية قد تقوم مفاتيح الغرفة بتشغيل قفل للغرفة وبعض المناطق المشتركة ، بينما يمكن لمفتاح الموظفين تشغيل الأقفال لسلسلة من الغرف ، ولكن فقط خلال فترة زمنية معينة.

يوفر التحكم المركزي مزايا في حالات الطوارئ يمكن تنسيق الوصول لأطقم الإطفاء والطوارئ ومنحه للمناطق المتضررة بسرعة في الأنظمة التي تكون فيها الأقفال تحت السيطرة المحلية ، قد يكون من المفيد وضع سياسات للطوارئ مسبقًا يجب حماية المفاتيح الرئيسية من سوء الاستخدام ، ولكن لا يزال من السهل الوصول إليها عند الضرورة لحماية أرواح وممتلكات شاغليها يمكن أيضًا استخدام أنظمة التحكم في الوصول الدقيقة في المدارس والكليات والمستشفيات ومباني المكاتب العامة والخاصة والمساكن تقنية Keycard مناسبة لكل من التطبيقات الداخلية والخارجية.

1-3-Cipher Lock

يتطلب الوصول باستخدام قفل مشفر حفظ رمز أو سلسلة من الأرقام قد تكون أنظمة قفل الأبواب من هذا النوع ميكانيكية أو إلكترونية أو كهروميكانيكية عادةً ما تعلق أقفال الشفرات الميكانيكية بالباب نفسه ، بينما قد يتم تثبيت أقفال الشفرات الإلكترونية على الباب أو على الحائط بجوار الباب الذي يتحكمون فيه و تتحكم أقفال التشفير الإلكترونية فى المزلاج او الكالون ، ويتم تشغيلها بالضغط على مجموعة من الأزرار أو المفاتيح المتأرجحة غالبًا ما توجد الأزرار خلف درع لمنع ملاحظة المجموعة يتم ترتيب الأزرار الموجودة على قفل تشفير ميكانيكي في دائرة أو خط عمودي بالقرب من المقبض الذي يحرك الترباس بمجرد تحرير القفل يُعرف هذا المقبض باسم دوران الإبهام أو ذراع القفل تشترك أقفال التشفير الكهروميكانيكية في ميزات الأقفال الإلكترونية والميكانيكية وقد تحتوي على قفل تركيبة من نوع الاتصال الهاتفي.

التطبيقات لهذا النظام

توجد أقفال التشفير في الغالب في تطبيقات التحكم في الوصول التي تتطلب مستويات منخفضة إلى متوسطة من الأمان يمكن أن تكون مفيدة في المواقف عالية الأمان عند استخدامها مع أنظمة التحكم في الوصول التي تتحقق من كل مستخدم تعد أرشيفات السجلات ومرافق الملفات التنظيمية وغرف البريد والاماكن التي تحتوي على مواد خطرة ، مثل الصيدليات أو غرف تخزين الطلاء ، أمثلة على التطبيقات المناسبة لأنظمة قفل التشفير هذه الأنظمة مناسبة أيضًا للاستخدام في المدارس والكليات ومباني المكاتب العامة والخاصة والمساكن يمكن استخدام أنظمة قفل التشفير في كل من التطبيقات الداخلية والخارجية.

1-4-Magnetic Stripe Cards

البطاقات الشريطية المغناطيسية هي رموز مميزة تستخدم للمصادقة والتحكم في الوصول في العديد من بيئات الأمان يمكن ربط أجهزة قراءة البطاقات ذات الشريط المغناطيسي بمجموعة متنوعة من معدات التحكم في الوصول ، بما في ذلك الأقفال الكهربائية التي يتم التحكم فيها محليًا ، أو قواعد بيانات الأمان التي يتم التحكم فيها مركزيًا. تتطابق البطاقات ذات الشريط الممغنط في تكوينها ومظهرها مع البطاقات المصرفية أو بطاقات الائتمان يحتوي الشريط عادةً على حوالي 140 رقمًا وحرفًا ، مقسمة على واحد إلى ثلاثة مسارات بتنسيق خاص يمكن أن تتضاعف كبطاقات تعريف أو شارات عند طباعتها أو نقشها باسم المستخدم ورقم التعريف وبصمات شعارات الشركة أو المنظمة والصورة.

التطبيقات لهذا النظام

تُستخدم أنظمة الشريط المغناطيسي في جميع أنحاء القطاعين العام والخاص ، نظرًا لتكلفتها المنخفضة نسبيًا وتعدد استخداماتها إنها أكثر تنوعًا من أنظمة keycard توفر أنظمة بطاقة المفاتيح بشكل أساسي تحكمًا محليًا في نقطة وصول ، ولكنها تفتقر إلى القدرة على التحكم المركزي في كثير من الأحيان ، تفتقر أنظمة keycard أيضًا إلى القدرة على حفظ الدفاتر ؛ ومع ذلك ، توفر أنظمة الشريط المغناطيسي تحكمًا دقيقًا في نقاط الوصول وإمكانية حفظ سجلات مفصلة في الوقت الفعلي.

تحقق أنظمة الشريط المغناطيسي ذلك باستخدام التحكم المركزي في النظام في الأنظمة المركزية ، يحتفظ مدير الأمن بقاعدة بيانات محوسبة للأذونات المصرح بها لكل حامل بطاقة عندما يقوم حامل البطاقة بتشغيل قارئ ، يرسل القارئ إشارة إلى وحدة التحكم ، والتي تحدد حامل البطاقة ونقطة الوصول إذا كان لحامل البطاقة إذنًا بالباب ، تفتح نقطة الوصول .

1-5-Contact Smart Card

يمكن استخدام أنظمة التحكم في الوصول التي تستخدم البطاقة الذكية لجهة الاتصال في التطبيقات عالية الأمان والتي تتضمن عددًا كبيرًا من الأشخاص الذين يحتاجون إلى قدر كبير من المرونة ، ولكنهم يحتاجون فقط إلى معدلات إنتاجية معتدلة تحل هذه الأنظمة محل العديد من أنظمة البطاقات الرئيسية والشريط المغناطيسي نظرًا لسهولة استخدامها وأمانها وموثوقيتها.

عادةً ما تبدو البطاقات الذكية كبطاقة ائتمان شائعة ، على الرغم من توفر أشكال أخرى تجاريًا في شكل مجوهرات ، مثل خاتم أو قلادة أو سوار. تعتبر الاختلافات في المظهر بين البطاقات جمالية ولا تتعلق بالسمات والوظائف الإلكترونية المتوفرة على الدوائر المتكاملة (IC) المدمجة في الهيكل البلاستيكي للبطاقات

يحدد نوع IC المضمن إمكانيات البطاقة نوعان من الدوائر المتكاملة المستخدمة في البطاقات الذكية هي دوائر المعالجات الدقيقة ودوائر الذاكرة تكافئ قدرات بطاقة المعالجات الدقيقة تقريبًا أجهزة الكمبيوتر الشخصية من الجيل الأول من حيث الذاكرة وسرعة المعالجة ؛ ومع ذلك ، تتزايد هذه القدرات مع أحدث البطاقات عادةً ما تخزن بطاقات الذاكرة كميات قليلة من البيانات ، لكن هذه البطاقات لا يمكنها إجراء عمليات معالجة أو حساب أو تنفيذ عمليات ، مثل خوارزمية دقة التصادم. يجب أن يقوم قارئ البطاقة بتطبيق أي تشفير أو تغييرات على البيانات الموجودة على بطاقة الذاكرة هناك العديد من تكوينات الذاكرة المتاحة ، والتي تسمح لأقسام معينة من الذاكرة المدمجة بالحماية ضد الكتابة أو الحجز

التطبيقات لهذا النظام

تعد البطاقات الذكية لجهات الاتصال مناسبة لأنظمة التحكم في الوصول إلى معدل النقل الداخلي والمتوسط حيث تكون مرونة النظام مهمة غالبًا ما يتم استخدامها في منشآت عالية الأمان ويمكنها التعامل مع أعداد كبيرة من المستخدمين.

تميل البطاقات الذكية لجهات الاتصال إلى أن تكون غير مناسبة للتطبيقات الخارجية بسبب تأثيرات الطقس على نقاط الاتصال الخاصة بالقارئ يمكن استخدام بطاقات الاتصال الذكية للتحكم في الوصول المادي والمنطقي ، وكذلك لتتبع وقت الموظف وحضوره. يمكن زيادة القيمة الإجمالية للنظام من خلال دعم التطبيقات الأخرى من منصة البطاقة الذكيةإلى جانب توفير الهوية والمصادقة الآمنة ، يمكن استخدام البطاقات الذكية كأدوات مالية أو محاسبية

1-6-Contactless Smart Card

تستخدم بعض أنظمة التحكم في الدخول على البطاقات الذكية التي تتمتع ، بالإضافة إلى إمكانات المعالجة أو الذاكرة ، بقدرة اتصالات ترددات الراديو (RF) التي تسمح لقارئ البطاقة بالتفاعل معها على مسافة قصيرة يشار إلى هذه البطاقات الذكية بدون تلامس يمكن استخدام أنظمة البطاقات الذكية التي لا تلامس في التطبيقات عالية الأمان التي قد تتطلب معدلات إنتاجية أكبر من أنظمة البطاقات الذكية الملامسة يمكن تجهيز بعض البطاقات الذكية بشرائط مغناطيسية ورموز شريطية وأنظمة أخرى لتسهيل التحكم في الوصول.

تشبه البطاقات الذكية غير التلامسية بطاقة ائتمان تحتوي على شريحة صغيرة مدمجة يقدم بعض البائعين أجهزة ذكية بدون تلامس في سلسلة مفاتيح والأشكال بخلاف البطاقات ، غالبًا ما يتم تضمين المكونات الإلكترونية في راتنجات الإيبوكسي بدلاً من المصفوفة البلاستيكية المستخدمة في البطاقات يجب أن تحتوي البطاقة الذكية بدون تلامس أيضًا على هوائي مدمج بجانب الشريحة الدقيقة.

بطاقة Combi هي نوع آخر من البطاقات الذكية القادرة على التردد اللاسلكي ، والتي تدعم كلاً من واجهات الاتصال والتواصل مع معالج دقيق واحد.

بطاقة التحقق من الهوية الشخصية (PIV) هي مثال على بطاقة .Combi يحدد FIPS 201 آليات المصادقة على ثلاثة مستويات ضمان للمصادقة الإلكترونية (على سبيل المثال ، بعض ، ثقة عالية وعالية جدًا) ويوحد عناصر الاعتماد الاختيارية التي توسع الثقة في نظام PIV إلى وظائف تتجاوز المصادقة

التطبيقات لهذا النظام

يعمل التشغيل بدون استخدام اليدين لأنظمة البطاقات الذكية التي لا تلامس على تقليل الوقت الذي تقضيه في بوابة الوصول هذه ميزة لأولئك العمال الذين يحملون البضائع والمواد في مساحة العمل يعد التشغيل بدون استخدام اليدين أيضًا أحد المتطلبات المرتبطة غالبًا بالأنظمة التي تعمل بمستويات عالية من الإنتاجية ، مثل المباني العامة الكبيرة

أو الأماكن الرياضية ، حيث يمر عدد كبير من الأشخاص عبر بوابات الوصول خلال فترة زمنية قصيرة في حالة الحاجة إلى مستويات عالية من الإنتاجية ، يجب توخي الحذر عند اختيار تقنية مناسبة للمصادقة ذات العاملين.

غالبًا ما يكون لدى بعض أجهزة قراءة البطاقات اللاتلامسية لوحات مفاتيح رقمية لإدخال أرقام التعريف الشخصية ، كما هو موضح في الشكل ، وأحكامًا لتوصيل أجهزة المقاييس الحيوية للمصادقة الثنائية.

تعد البطاقات الذكية بدون تلامس هي الأنسب للتطبيقات التي تتطلب تعقب الأفراد والمواد داخل منطقة محمية. يمكن استخدام هذه التقنية للتطبيقات الداخلية والخارجية.

1-7-Wiegand Cards& Key Fobs

بطاقة Wiegand عبارة عن جهاز بحجم بطاقة الائتمان من البلاستيك أو الفينيل يحتوي على صفين من الأسلاك المتوازية الصغيرة المكونة من ملكية خاصة والتي تولد رقمًا ثنائيًا عند تمرير البطاقة عبر قارئ يتم تضمين الأسلاك داخل البطاقة أثناء عملية التصنيع وتوفر الحماية ضد التزوير خارج المجال المغناطيسي للقارئ ، تكون الأسلاك المضمنة خاملة بشكل أساسي.

تم تطوير أنظمة التحكم في الوصول إلى Wiegand في أوائل السبعينيات واستخدمت في جميع أنحاء القطاعين العام والخاص ومع ذلك ، فإن العديد من أنظمة التحكم في الوصول إلى Wiegand قديمة وتتطلب صيانة متكررة. يتم استبدال بطاقة Wiegand إلى حد كبير بالبطاقة الذكية.

تُستخدم سلاسل المفاتيح كأجهزة واجهة للعديد من أنظمة التحكم في الوصول والأمن تتوفر العديد من التقنيات يمكن أن تكون مصنوعة من البلاستيك أو راتنجات الايبوكسي أو المعدن.

التطبيقات لهذا النظام

تتميز واجهة fob الرئيسية بالمرونة وهي عنصر في العديد من أنظمة التحكم في الوصول والأمان على سبيل المثال ، توفر أداة فتح باب المنزلي نظامًا أساسيًا للتحكم في الوصول للعديد من مالكي المنازل تتراوح هذه الأنظمة في التعقيد من مجرد إصدار إنذار بصوت عالٍ إلى أنظمة الاتصالات عبر الأقمار الصناعية ، ونظام تحديد المواقع العالمي (GPS) ، وتعطيل السيارة عن بُعد لمنع السرقة أو أي نشاط إجرامي آخرغالبًا ما تحتوي سلاسل المفاتيح التي تتحكم في أنظمة الإنذار بالمنشأة على لوحة مفاتيح صغيرة بها ثلاثة أو أربعة أزرار يتحكم كل زر على لوحة المفاتيح في حالة نظام الإنذار ، مثل الذراع أو نزع السلاح غالبًا ما تتضمن سلاسل المفاتيح المستخدمة في أنظمة الإنذار بالمنشأة إنذارًا بالإكراه أو زر الذعر الذي يمكن أن يطلق إنذارًا بشكل مستقل عن حالة النظام وأجهزة الاستشعار. تعد واجهة fob الرئيسية مناسبة لكل من التطبيقات الداخلية والخارجية ، وهي مفيدة بشكل خاص في تطبيقات صناعة المركبات والنقل.

F-Biometric Access Control Technologies

يشير التحكم في الوصول البيومتري إلى استخدام السمات البيولوجية البشرية للتحقق أو تحديد الهوية في أنظمة التحكم في الوصول المادي تستخدم أنظمة القياسات الحيوية قياسات البيانات المادية أو السلوكية للمقارنة بالمعلومات المسجلة مسبقًا لتحديد استجابات النظام مثل تحديد الهوية أو منح الدخول تم بناء أنظمة التحكم في الوصول البيومترية حول بعض السمات القابلة للقياس المدرجة في الجدول

Biometric	Physical	Behavioral
Facial Recognition	✓	
Fingerprint Recognition	✓	
Hand/Finger Geometry Recognition	✓	
Vein Geometry Recognition	✓	
Iris Recognition	✓	
Voice Recognition	✓	✓
Signature Dynamics Recognition		✓

تتميز معظم أنظمة التحكم في الوصول البيومترية بما يلي:

- تشمل الخصائص الفيزيائية المكونات التشريحية والوظائف الفسيولوجية لجسم الإنسان،بينما تصف الخصائص السلوكية الطريقة التي يتفاعل بها الفرد أو يتحرك داخل البيئة.

- يمكن أنظمة التحكم في الوصول البيومترية بحيث تعمل دون تدخل بشري مباشر. عادة ما ينتجون قرار التحكم في الوصول في بضع ثوانٍ أو أقل.

التطبيقات لهذا النظام

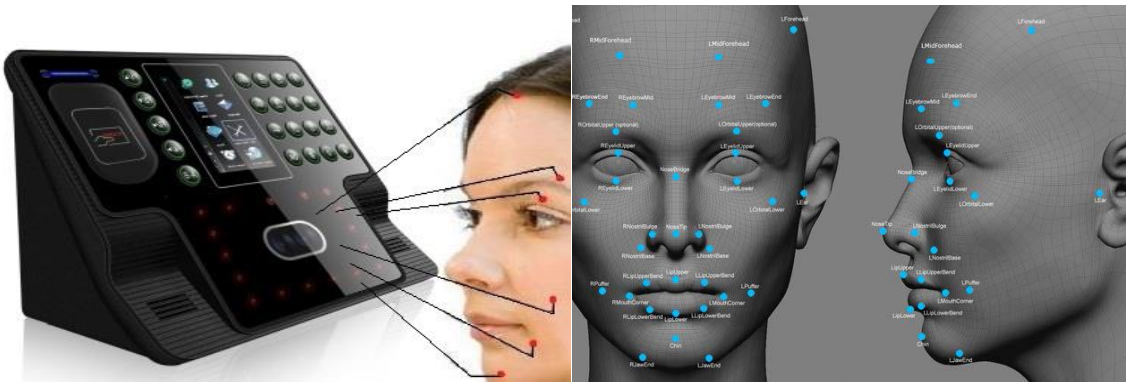
يعد التعرف على الوجه مفيدًا لتطبيقات التحقق الداخلية حيث يمكن التحكم في الإضاءة المحيطة والبيئة يجب وضع الكاميرا بحيث يمكن التقاط صور الوجه عالية الجودة لا يُنصح بالتعرف على الوجه في المناطق التي لا تكون الإضاءة فيها موحدة أو في المواقف التي تتطلب معدات حماية الأفراد (PPE) ، مثل أقنعة الوجه.

Facial Recognition

التعرف على الوجه عبارة عن تقنية للتحكم في الوصول باستخدام المقاييس الحيوية تستخدم صورة فوتوغرافية واحدة أو أكثر للتعرف على شخص من خلال قياس النقاط على وجهه في ظل ظروف خاضعة للرقابة أنظمة التعرف على الوجه ليست تطفلية ، ولا تتطلب أي اتصال جسدي مع المستخدم ، ولديها معدل عالٍ من قبول المستخدم.

لا يتأثر التعرف على الوجه بالعرق أو الاختلافات في المظهر على أساس الجنس إنها تقنية قوية قادرة على التعامل مع مجموعة واسعة من أنواع الجسم وخصائص الوجه يتم استخدام التعرف على الوجه في جميع أنحاء العالم في صناعات متنوعة مثل البنوك والألعاب والرعاية الصحية وإنفاذ القانون والجمارك وتجارة التجزئة تم اختبار التكنولوجيا بنجاح في مقارنات صناعية محايدة وهي حاليًا الجزء الأسرع نموًا في سوق التحكم في الوصول البيومتري.

التعرف على الوجه له عدد من الجوانب المرغوبة.

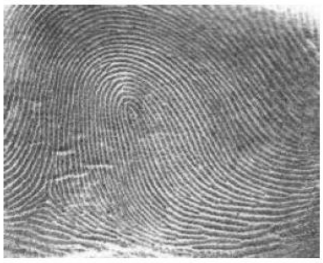


Fingerprint Recognition

يعد التعرف على بصمات الأصابع أحد أكثر القياسات الحيوية استخدامًا في صناعة التحكم في الوصول وذلك لأن بصمات الأصابع هي واحدة من أقدم أشكال تحديد الهوية الشخصية ، وغير مكلفة لجمعها وتحليلها ، كما أنها مستقرة تستخدم تطبيقات التحكم في الوصول إلى بصمات الأصابع إحدى خصائص بصمات الأصابع أو كلتيهما: أنماط التلال وتفاصيل التفاصيل الدقيقة ، وهي ميزات فريدة موجودة في الأنماط لا تتطلب بعض ماسحات بصمات الأصابع عالية التقنية بصمة الإصبع فقط لمطابقتها ، ولكنها تستخدم أجهزة مراقبة درجة الحرارة والرطوبة لضمان مسح الإصبع .

هناك ثلاثة أنماط أساسية ، كما هو موضح في الشكل ، لحواف بصمات الأصابع: القوس والحلقة والدوران.

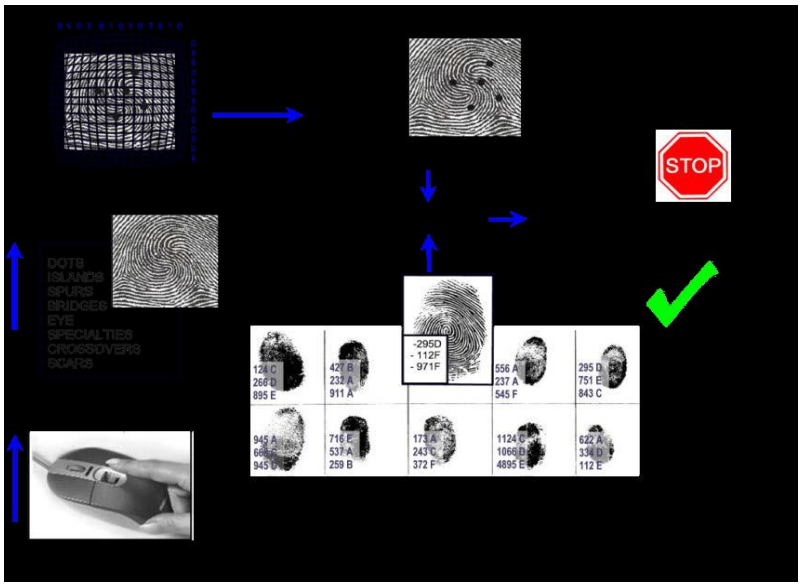
Arch



Loop

Whorl

- يتكون القوس من نتوءات تقع أحدها فوق الأخرى في شكل مقوس عام.
- تتكون الحلقة من نتوءات تدخل من جانب واحد من الإصبع وتشكل منحنى ثم تخرج من نفس الجانب.
- تتكون الزهرة من حواف تشكل نمطًا دائريًا حول نقطة مركزية



التطبيقات لهذا النظام

تُستخدم أنظمة التحكم في الوصول المستندة إلى بصمات الأصابع لأغراض تحديد الهوية والتحقق.

التكنولوجيا متاحة من مجموعة متنوعة من مصادر البائعين يمكن أن تكون الأنظمة القائمة على شرائح السيليكون وأجهزة الاستشعار التي ينبعث منها الضوء صغيرة بما يكفي لاستخدامها مع الأجهزة المحمولة ، مثل الهواتف الذكية أو الأجهزة اللوحية أو أجهزة الكمبيوتر المحمولة.

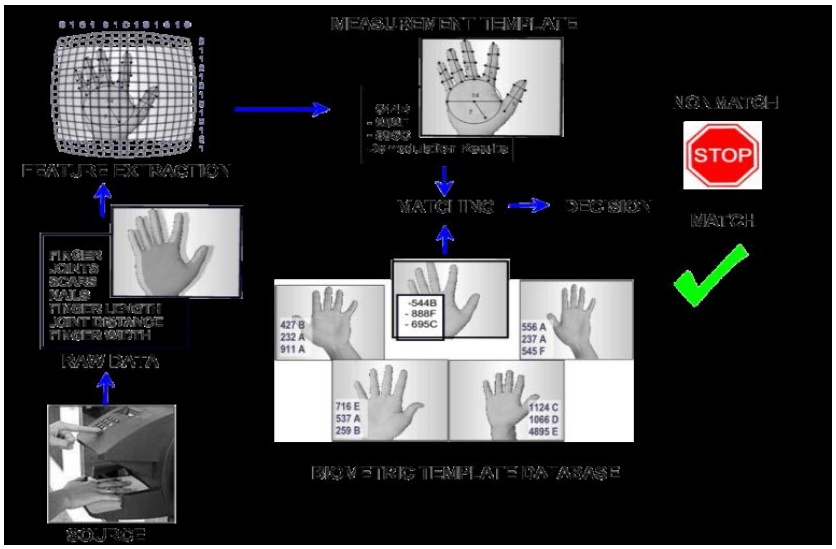
أنظمة التحكم في الوصول القائمة على بصمات الأصابع مخصصة للاستخدام الداخلي - الخارجي وتستجيب بشكل جيد لمجموعة واسعة من ظروف الرطوبة ودرجات الحرارة البيئية.

لا يوصى باستخدام هذه الأنظمة للتطبيقات التي يرتدي فيها المستخدمون قفازات أو يعملون في ظروف تسبب تآكل الأصابع واليدين قد تشمل هذه التطبيقات مواقع البناء ، أو مناطق تلوث السطح النووي - الكيميائي .

Hand/Finger Geometry Recognition

تتوفر أنظمة التعرف على هندسة اليد بشكل شائع في شكلين: أنظمة هندسة اليد الكاملة التي تقيس اليد بأكملها ، وأنظمة هندسة الإصبع التي تقيس فقط السبابة والأصابع الوسطى القياسات الحيوية لهندسة اليد والأصابع هي قياسات آلية لأبعاد اليد والأصابع مأخوذة من صورة ثلاثية الأبعاد يلتقط القارئ أو الكاميرا ما يصل إلى 96 سمة من سمات اليد مثل الشكل والعرض وطول الأصابع والمفاصل والمسافة بين المفاصل وشكل وسماكة راحة اليد. يشبه هذا بعض أنواع أنظمة التعرف على الوجه من حيث أنه يفحص الهندسة المكانية لليد والأصابع يتم تجاهل تفاصيل السطح مثل بصمات الأصابع والخطوط والندبات والأوساخ والأظافر.

أصبحت هندسة اليد الآن تقنية ناضجة ، وكانت إحدى الطرق الأولى للتحكم في الوصول البيومتري في السوق الحديث على عكس أنظمة التحكم في الوصول البيومترية الأخرى ، التي استفادت من الاختراقات التكنولوجية مثل الرقائق الدقيقة أو زيادة جودة الكاميرا ، فإن التكنولوجيا التي تدعم أنظمة التحكم في الوصول إلى هندسة اليد لم تتقدم بشكل ملحوظ لسنوات عديدة تم استخدام أنظمة التحكم في الوصول للهندسة اليدوية منذ ما يقرب من 30 عامًا في المرافق التي تشمل محطات الطاقة النووية ومراكز الرعاية الاجتماعية ومرافق الهجرة ومراكز الرعاية النهارية.



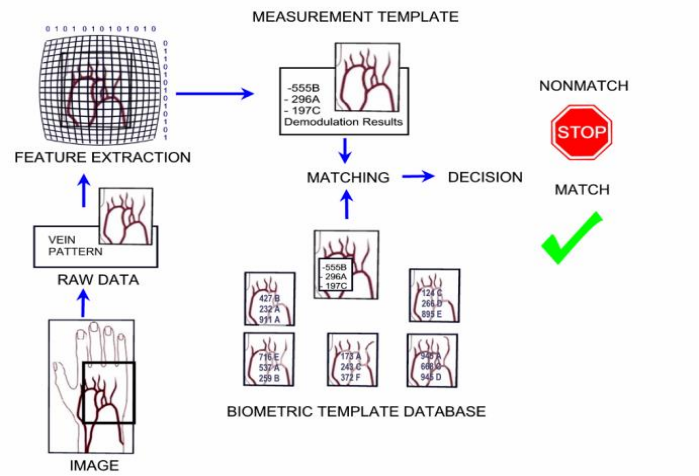
التطبيقات لهذا النظام

هندسة اليد هي تقنية دقيقة نسبيًا ، لكنها تعتمد على نقاط بيانات أقل من التعرف على بصمات الأصابع أو قزحية العين أو التعرف على الوجه تعد هندسة اليد مفيدة جدًا في التحقق ، مثل مطابقة مستخدم معروف مع نموذج تسجيل هذا المستخدم العامل الذي يحد من هندسة اليد والأصابع لتطبيقات التحقق هو أن الأيدي والأصابع لا تختلف بشكل كافٍ في الأبعاد لإنشاء قوالب فريدة في مجموعات كبيرة من المستخدمين ضمن التفاوتات المسموح بها للكاشف ، في كل مرة يسعى فيها المستخدم للوصول ، يمكن لبيانات أكثر من منتسب واحد إنشاء تطابق لذلك ، يجب أن تكون عملية تحديد الهوية ، مثل استخدام رقم التعريف الشخصي أو بصمة الإصبع أو قارئ البطاقة الذكية أو أي جهاز آخر ، مصاحبة لأنظمة هندسة اليد.

تعد أنظمة التحكم في الوصول للهندسة اليدوية مفيدة بشكل خاص في البيئات الخارجية لأن أجهزة الكشف تقاوم العديد من العوامل البيئية ، مثل الإضاءة المحيطة أو تغيرات درجة الحرارة قوالب هندسة اليد صغيرة ، مما يجعلها محمولة وتمكين نظام التحكم بأكمله من أن يتم احتوائه في وحدة كاشف واحدة. نظرًا لأن الأيدي المتسخة أو المتسخة لا تؤثر على أجهزة التحكم في الوصول للهندسة اليدوية ، يمكن استخدام هذه الأنظمة في مواقع البناء والمسابك.

Vascular Pattern Recognition

تستخدم أنظمة التحكم في الوصول للتعرف على أنماط الأوعية الدموية التي تشكلها الأوردة في أجزاء معينة من الجسم ، مثل ظهر اليد أو الإصبع أو الرسغ أو الوجه يمكن استخدام هذه الأنظمة لتحديد الهوية والتحقق يعد التعرف على أنماط الأوعية الدموية تقنية جديدة نسبيًا في صناعة التحكم في الوصول باستخدام القياسات الحيوية وتستخدم تقنيات المسح بالأشعة تحت الحمراء المصغرة على الرغم من أن هذه الأنظمة أقل نضجًا وقد تكون أكثر تكلفة من تقنيات التحكم في الوصول الأخرى ، إلا أن نضج التعرف على أنماط الأوعية الدموية آخذ في الازدياد.



التطبيقات لهذا النظام

يمكن استخدام أنظمة التعرف على أنماط الأوعية الدموية في حالات التحكم في الوصول عالية الأمان التي تتطلب تحديد الهوية أو التحقق منها يمكن برمجتها لقراءة مناطق الجسم بخلاف اليدين عندما تكون أيدي العديد من الموظفين مشغولة تنتشر تقنية التعرف على الأوعية الدموية على نطاق واسع في أجهزة الصراف الآلي في اليابان.

Iris Recognition

يلتقط نظام التعرف على قزحية العين صورة الأشعة تحت الحمراء للقزحية من مسافة 4 بوصات إلى 6 أقدام. يعتبر هذا من قبل المستخدمين ليكون غير تدخلي.

القزحية هي الحلقة الملونة المرئية بوضوح وإنها بنية عضلية تتحكم في كمية الضوء التي تدخل العين.

تتكون القزحية من تفاصيل معقدة قابلة للقياس تسمى التصدعات لا يوجد قزحتان متشابهتان ؛ حتى قزحية العين مختلفة تمامًاكمية المعلومات الفريدة التي يمكن قياسها بقزحية واحدة أكبر بكثير من بصمات الأصابع.

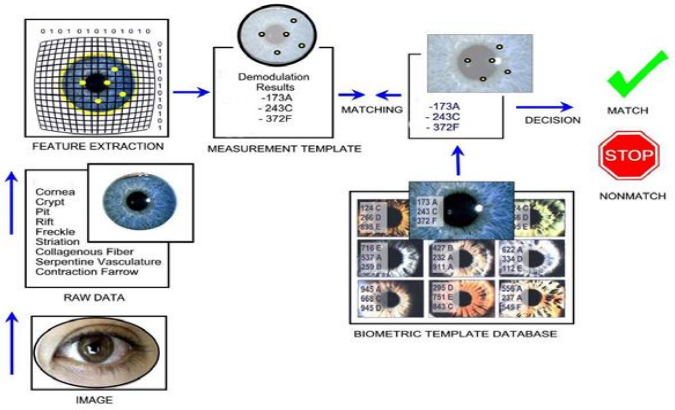
تم نشر تقنية التعرف على قزحية العين تقليديًا في المواقف عالية الأمان حيث يمكن إجراء التصوير على مسافة أقل من ثلاثة أقدام ، وهناك حاجة للبحث في قواعد البيانات الكبيرة جدًا دون تكبد مطابقات خاطئة تُستخدم هذه الأنظمة في عدد من التطبيقات البارزة ، بما في ذلك فحص المسافرين في الخطوط الجوية ، والتعرف على السجناء ، والوصول المادي إلى سجلات الرعاية الصحية. أنظمة التعرف على قزحية العين هي:

•**مستقرة** - تظل قزحية العين ثابتة على مدار حياة الشخص بأكملها. هذا يجعل التعرف على قزحية العين مقياسًا حيويًا مرغوبًا جدًا لاستخدامات التحكم في الوصول.

•**فريد** - يُنظر إلى التعرف على قزحية العين على نطاق واسع على أنه أكثر منهجية القياسات الحيوية دقة نظرًا للمستوى الغني من التفاصيل التي يمكن جمعها. تلتقط الأنظمة المتاحة أكثر من 240 خاصية فريدة في صياغة

النموذج ، وهو ما يزيد عن 10 أضعاف أنظمة القياسات الحيوية الأخرى. احتمال وجود قزحيتين لهما نفس النمط هو صفر في الأساس.

•**مرن** - على عكس بعض أنظمة التحكم في الوصول البيومترية الأخرى ، لا يتطلب التعرف على قزحية العين أي اتصال جسدي. هذا يعني أنه مناسب بشكل مثالي للاستخدام في البيئات التي تستخدم فيها القفازات أو غيرها من معدات الحماية. يمكن أن تتكامل تقنية التعرف على قزحية العين بسهولة في أنظمة التحكم في الوصول الحالية أو تعمل كنظام مستقل.



التطبيقات لهذا النظام

التحكم في الوصول للتعرف على قزحية العين دقيق للغاية وهو خيار جيد للتطبيقات عالية الأمان يمكن استخدام التعرف على قزحية العين في مهام تحديد الهوية والتحقق من السجناء هو أحد الاستخدامات الشائعة للتعرف على قزحية العين في إنفاذ القانون .

Retina Scan

شبكية العين هي عصب رقيق (50/1 بوصة) في الجزء الخلفي من العين إنه جزء من العين يستشعر الضوء ويرسل نبضات عبر العصب البصري إلى الدماغ.

يعد فحص الشبكية من أقدم القياسات الحيوية في الثلاثينيات من القرن الماضي ، أشارت الأبحاث إلى أن أنماط الأوردة الدموية في الجزء الخلفي من العين كانت فريدة من نوعها بالنسبة للفرد تم تطوير أنظمة تحديد الهوية المتاحة تجارياً في منتصف الثمانينيات.

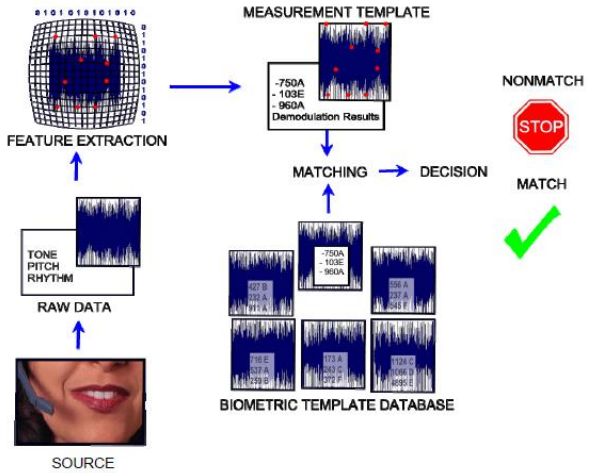
التطورات اللاحقة جعلت وحدات الماسح الضوئي أصغر حجمًا وأقل تكلفة ؛ ومع ذلك ، وبسبب تكاليف التنفيذ ، وصعوبة جمع العينات ، والتصورات السلبية المتعلقة بالتطفل ، انخفض استخدامها بشكل كبير. تعد التطبيقات عالية الأمان مع متطلبات الإنتاجية المنخفضة وعدد قليل نسبيًا من المستخدمين المصرح لهم أحد الاستخدامات القليلة المتبقية لتقنية فحص شبكية العين.

Voice Recognition

تستخدم تقنية التعرف على الصوت الجوانب الفريدة لأنماط الصوت البشري للتحقق من هوية الأفراد النظرية الأساسية للتعرف على الصوت هي أن كل صوت مميز وفريد بما يكفي للتعرف على المتحدث يتغير شكل السبيل الصوتي عندما يتحدث الشخص تساهم الأشكال المختلفة التي يفترضها الجهاز الصوتي وسلوكيات التحدث لدى الفرد في تفرد البصمة الصوتية.

حاليًا ، يتم استخدام التعرف على الصوت في عدد من قطاعات السوق بما في ذلك المستودعات والتوزيع والتجارة الإلكترونية والخدمات المالية والحكومة والرعاية الصحية والاتصالات على الرغم من أنها ليست مناسبة للحلول عالية الأمان كطريقة واحدة للتحكم في الوصول ، إلا أن تقنية التعرف على الصوت مفيدة في انخفاض مستوى الأمان وفي التطبيقات متعددة الوسائط جنبًا إلى جنب مع القياسات الحيوية الأخرى وتقنيات التحكم في الوصول الإلكتروني.

تقيس بعض الأنظمة الإيقاع والنغمة والنبرة التي يستخدمها الفرد لتكرار عبارة مرور واحدة أو أكثر تستخدم الأنظمة الأحدث خوارزميات خاصة لتحليل السبيل الصوتي لإنشاء طباعة صوتية آمنة ميزة أخرى لزيادة أمان البصمات الصوتية هي استخدام عبارات المرور العشوائية يمكن للإنسان الاستماع إلى وتكرار عبارة لا يمكن للتسجيلات تكرارها تستمر تقنية التعرف على الصوت في التقدم ، وأصبحت الأنظمة أكثر تعقيدًا بحيث يمكن أن تتكون عبارات المرور من أي عبارة يرغب الفرد في استخدامها في أي لغة العبارة نفسها ليست مهمة طالما أنها تطابق ما تتوقعه قاعدة بيانات الكمبيوتر المسجلة. إنها الخصائص الفريدة للصوت نفسه التي تم نقشها.



التطبيقات لهذا النظام

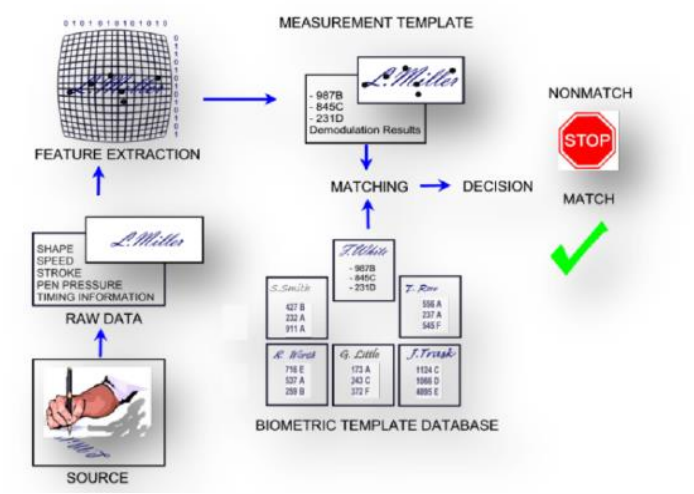
تشمل تطبيقات هذه التقنية مراقبة مخزون المستودعات والشحن ، والخدمات المصرفية ، والتسهيلات الإصلاحية ، والتحكم العام في الوصول ، وتأمين الوصول إلى المعلومات السرية ، ومراكز الاتصال ، والوصول إلى البوابات الصوتية.

Signature Dynamics Recognition

التعرف على التوقيع الديناميكي عبارة عن تقنية مقاييس حيوية تُستخدم لتحديد هوية المستخدم من خلال توقيع مكتوب بخط اليد يتم ذلك عن طريق تحليل معلومات الشكل والسرعة وضغط القلم والتوقيت أثناء عملية التوقيع . لا يتم استخدام ديناميكيات التوقيع بشكل متكرر للتحكم في الوصول المادي.

كثير من الناس على دراية بمفهوم تحليل التوقيع ، والذي يتكون من تحديد ما إذا كان التوقيع قد كتبه على الأرجح نفس الشخص الذي كتب توقيعًا مرجعيًا من ناحية أخرى ، تأخذ ديناميكيات التوقيع في الحسبان كيف تم التوقيع. التغييرات في السرعة والضغط والتوقيت (أي الإيقاعات الطبيعية) التي تحدث عندما يوقع الفرد على اسمه / اسمها هي سلوكيات مكتسبة فريدة لهذا الفرد في حين أنه من الممكن لجهاز كمبيوتر أو آلة نسخ أو مزور خبير أن يكرر مظهر التوقيع ، فإن المكونات الأخرى تكون فريدة للموقِّع الأصلي على الرغم من شيوع الاختلافات الطفيفة في توقيع الشخص بخط اليد ، فإن الاتساق الذي تخلقه الحركة الطبيعية والممارسة بمرور الوقت هو نمط فريد قابل للقياس.

التحقق من التوقيع له معدل قبول مرتفع من قبل المستخدم ، لأن التوقيع غالبًا ما يستخدم لتحديد الهوية في سياقات أخرى تستخدم المستندات القانونية ورسوم الائتمان والعديد من المعاملات اليومية الأخرى التوقيعات لتحديد الهوية والمعالجة.



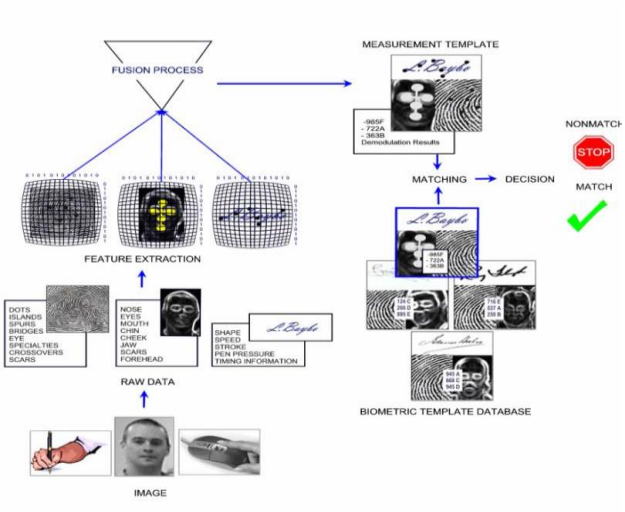
التطبيقات لهذا النظام

يمكن استخدام أنظمة التحكم في الدخول لديناميكيات التوقيع لتحديد الهوية أو التحقق غالبًا ما يتم تنفيذ هذه الأنظمة في حالات الوصول الخاضع للرقابة حيث تكون عمليات التوقيع أو الإدخال المكتوب موجودة بالفعل تشمل الأمثلة التطبيقات التي يتم فيها الاحتفاظ بسجلات وصول مكتوبة ، في المؤسسات المالية ، أو في مكاتب الوصفات الطبية في الصيدليات.

Multimodal

يجب أن تتعامل أنظمة التحكم في الوصول البيومترية الفردية غالبًا مع بيانات أجهزة الاستشعار معدلات الخطأ غير المقبولة توفر أنظمة القياسات الحيوية متعددة الوسائط القدرة على الجمع بين نمطين أو أكثر من الأنماط التكميلية للتحقق وتحديد الهوية ، كما هو موضح في الشكل التالى السبب الأكثر وضوحًا لاستخدام القياسات الحيوية متعددة الوسائط بدلاً من طريقة واحدة هو جعل عمليات التحكم في الوصول أكثر أمانًا يبدو من المنطقي أن الجمع بين الأنظمة يجب أن يجعل الانتحال أكثر صعوبة ويجب أن يؤدي إلى معدلات خطأ أقل بشكل عام. هناك طرق لدمج مخرجات أنظمة القياسات الحيوية لتحقيق هذا الهدف ، وهي عملية تسمى الاندماج.

يتمثل التحدي الحالي في تصميم نظام للتحكم في الوصول باستخدام المقاييس الحيوية مع أقل معدل خطأ ممكن ، والذي سيغطي المجموعة الكاملة من المستخدمين الفرديين ، ولا يمكن المساس به في ظل أي سيناريو معقول يعني تعدد الوسائط الحقيقي القدرة على تحليل العديد من سمات القياسات الحيوية في وقت واحد ، بدلاً من تحليل سمات القياسات الحيوية المختلفة واحدة تلو الأخرى.



التطبيقات لهذا النظام

تعد أنظمة التحكم في الوصول البيومترية متعددة الوسائط أكثر جدوى في المواقف شديدة الأمان قد تستخدم هذه الأنظمة خصائص من نفس سمات القياسات الحيوية أو من سمات مختلفة ، ولكن يتم جمع جميع العينات في نفس الوقت. على سبيل المثال ، قد يتم التقاط الوجه وبصمة الإصبع وقزحية العين وتعيين أوزان إلى نتيجة المطابقة لكل طريقة للحصول على نتيجة ثقة أعلى عدم وجود تطابق.

مثال آخر هو وريد الإصبع مع التعرف على بصمات الأصابع.

لماذا نقوم بإستخدام نظام التحكم في الدخول ؟

-السماح بالوصول فقط للموظفين المصرح لهم

-تنفيذ "بروتوكول وسياسة أمان" لجعل الموظفين والزوار والمنشأة آمنة

-تنفيذ تسلسل هرمي لمستوى الأمان والوصول بناءً على وظيفة الموظفين

-تعزيز عملية تحديد الهوية

-تتبع الموظفين الآلي

-التقليل من الخطأ البشري

-تتبع المقاولين والبائعين الخارجيين

-إنشاء تقارير الوصول لكل منطقة

- أرشفة السجلات للاستخدامات المستقبلية المحتملة

Access Control Topology

الهيكل التكوينى لنظام تحكم منع الدخول

يتم اتخاذ قرارات التحكم في الدخول من خلال مقارنة بيانات الاعتماد بقائمة التحكم في الوصول يمكن إجراء هذا البحث عن طريق خادم أو لوحة تحكم أو قارئ .

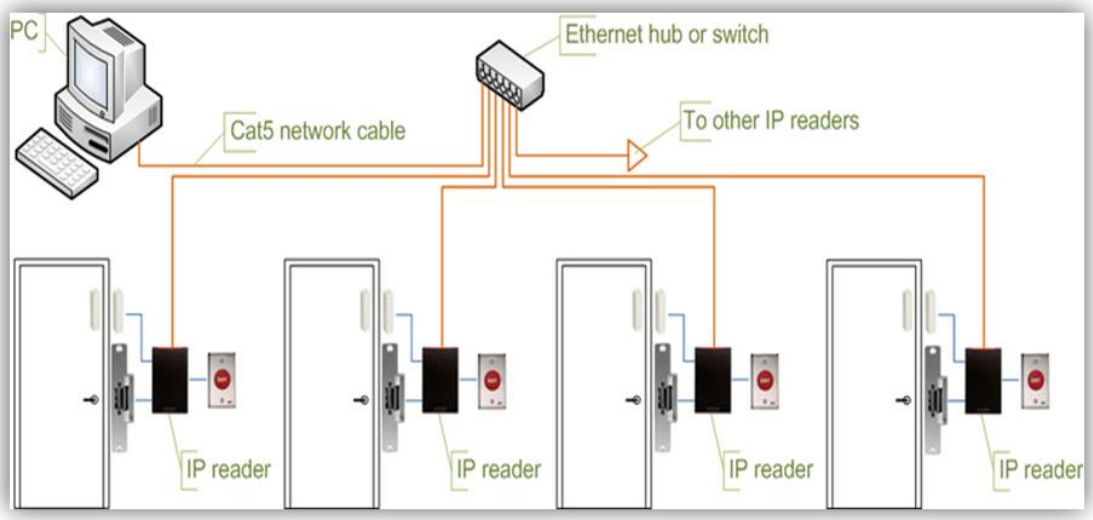
شهد تطوير أنظمة التحكم في الوصول دفعة ثابتة للبحث من مضيف مركزي إلى حافة النظام أو القارئ

الهيكل السائد حوالي عام 2009 هو المحور ويتحدث مع لوحة التحكم كمحور ، والقراء هم المتحدثين وظائف البحث والتحكم من خلال لوحة التحكم و يتواصل المتحدث من خلال اتصال تسلسلي عادة RS-485.

Access control system using serial controllers

1. Serial controllers.

يتم توصيل وحدات التحكم بجهاز كمبيوتر مضيف عبر خط اتصال تسلسلي RS-485 أو عبر حلقة تيار 20 mAفي بعض الأنظمة القديمة يجب تثبيت محولات RS-232/485 الخارجية أو بطاقات RS-485 الداخلية ، حيث لا تحتوي أجهزة الكمبيوتر القياسية على منافذ اتصالاتRS-485



Access control system using serial controllers

مميزات هذا النظام

1-يسمح معيار RS-485 بتشغيل الكابلات الطويلة ، حتى 4000 قدم (1200 متر)

2-وقت استجابة قصير نسبيًا الحد الأقصى لعدد الأجهزة الموجودة على خط RS-485 محدود بـ 32 جهازًا ، مما يعني أنه يمكن للمضيف طلب تحديثات الحالة بشكل متكرر من كل جهاز ، وعرض الأحداث في الوقت الفعلي تقريبًا.

3-موثوقية وأمان عاليان حيث لا يتم مشاركة خط الاتصال مع أي أنظمة أخرى.

عيوب هذا النظام

أ- لا يسمح RS-485 بالأسلاك من نوع Star ما لم يتم استخدام مقسمات

1-غير مناسبRS-485 تمامًا لنقل كميات كبيرة من البيانات (المستخدمين). أعلى معدل نقل ممكن هو 115.2 كيلوبت / ثانية ، ولكن في معظم الأنظمة يتم تخفيضه إلى 56.2 كيلوبت / ثانية ، أو أقل ، لزيادة الموثوقية.

2-لا يسمح RS-485 للكمبيوتر المضيف بالاتصال بالعديد من وحدات التحكم المتصلة بنفس المنفذ في وقت واحد. لذلك ، في الأنظمة الكبيرة ، قد تستغرق عمليات نقل التكوين والمستخدمين إلى وحدات التحكم وقتًا طويلاً جدًا ، مما يتداخل مع العمليات العادية.

3-لا يمكن للمراقبين بدء الاتصال في حالة وجود إنذار يعمل الكمبيوتر المضيف بمثابة خبير رئيسي في خط الاتصالRS-485 ، ويتعين على وحدات التحكم الانتظار حتى يتم استقصاءها.

4-يلزم وجود مفاتيح تبديل تسلسلية خاصة ، من أجل إنشاء إعداد فائض لجهاز الكمبيوتر المضيف.

5-يجب تثبيت خطوط RS-485 منفصلة ، بدلاً من استخدام البنية التحتية للشبكة الموجودة بالفعل.

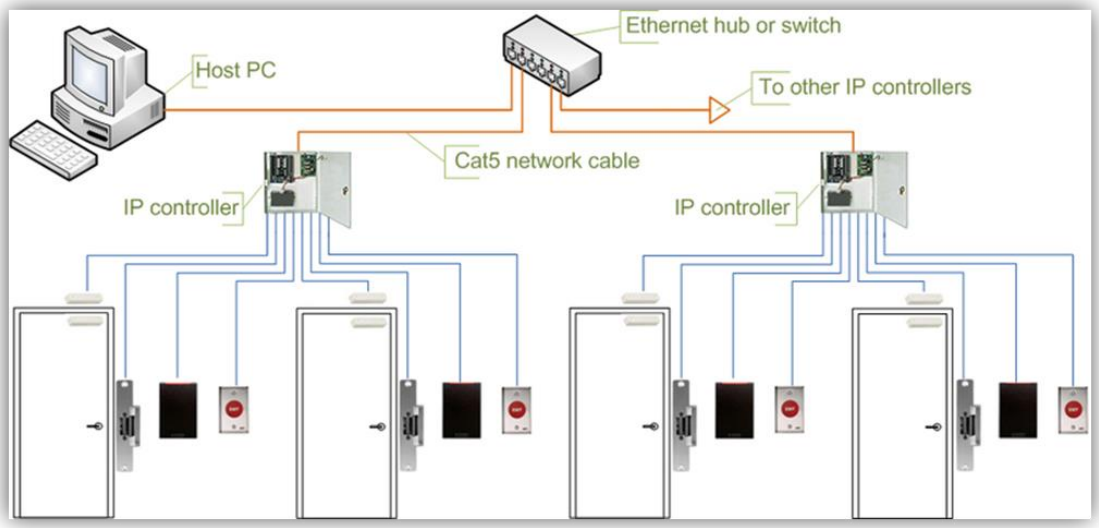
6-يعتبر الكبل الذي يفي بمعايير RS-485 أغلى بكثير من كبل شبكة UTP العادي من الفئة 5.

7-يعتمد تشغيل النظام بشكل كبير على الكمبيوتر المضيف في حالة فشل الكمبيوتر المضيف ، لا يتم استرداد الأحداث من وحدات التحكم ، وتتوقف الوظائف التي تتطلب التفاعل بين وحدات التحكم (anti-passback) عن العمل.

ب-نظام التحكم في الوصول يقوم بإستخدام وحدات التحكم الرئيسية والفرعية التسلسلية

2. Serial main and sub-controllers.

جميع أجهزة الباب متصلة بوحدات تحكم فرعية (مثل أجهزة التحكم في الأبواب أو واجهات الأبواب). عادةً لا تتخذ وحدات التحكم الفرعية قرارات الوصول ، وبدلاً من ذلك تقوم بإعادة توجيه جميع الطلبات إلى وحدات التحكم الرئيسية عادة ما تدعم وحدات التحكم الرئيسية من 16 إلى 32 وحدة تحكم فرعية.



Access control system using serial main and sub-controllers

مميزات هذا النظام

1- يتم تقليل عبئ العمل على الكمبيوتر المضيف بشكل كبير ، لأنه يحتاج فقط إلى الاتصال ببعض وحدات التحكم الرئيسية.
2- التكلفة الإجمالية للنظام أقل ، حيث أن وحدات التحكم الفرعية عادة ما تكون أجهزة بسيطة وغير مكلفة.
3- تنطبق جميع المزايا الأخرى المذكورة في الفقرة الأولى.

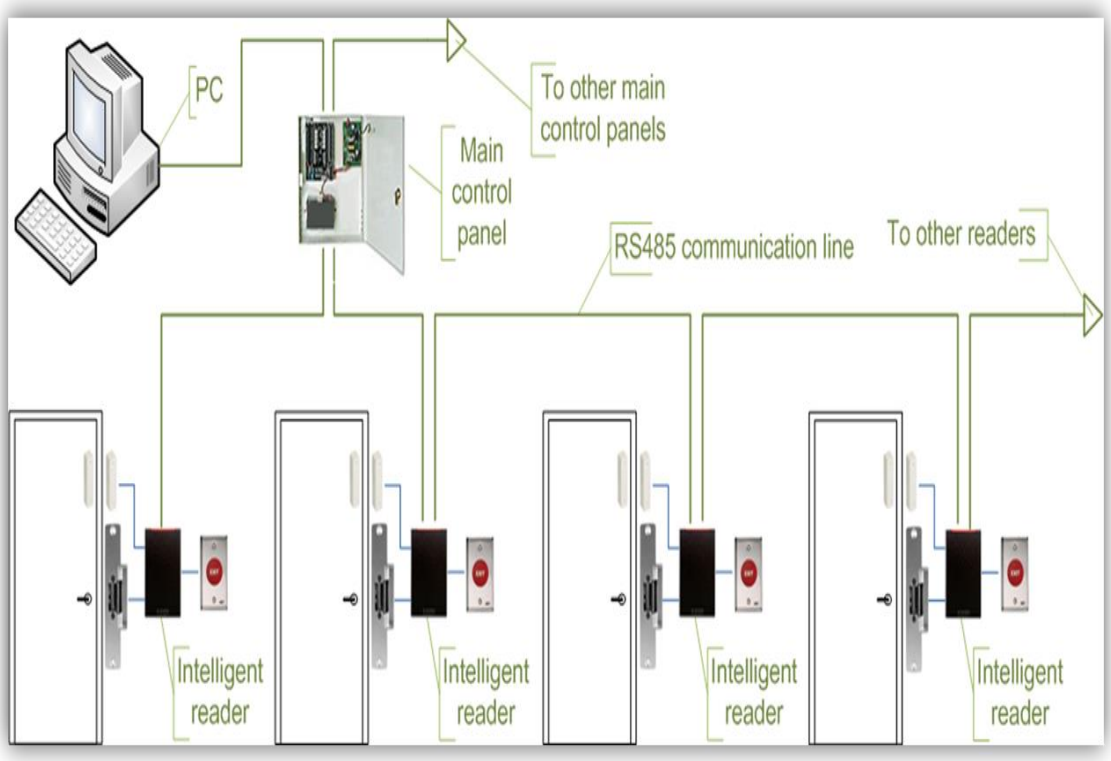
عيوب هذا النظام

1- يعتمد تشغيل النظام بشكل كبير على وحدات التحكم الرئيسية في حالة فشل أحد وحدات التحكم الرئيسية ، لا يتم استرداد الأحداث من وحدات التحكم الفرعية الخاصة بها ، وتتوقف الوظائف التي تتطلب التفاعل بين وحدات التحكم الفرعية عن العمل.
2- لا تمتلك بعض نماذج وحدات التحكم الفرعية (عادةً ما تكون منخفضة التكلفة) الذاكرة أو قوة المعالجة لاتخاذ قرارات الوصول بشكل مستقل في حالة فشل وحدة التحكم الرئيسية ، تتغير وحدات التحكم الفرعية إلى الوضع المتدهور حيث تكون الأبواب إما مقفلة أو غير مقفلة بالكامل ، ولا يتم تسجيل أي أحداث. يجب تجنب وحدات التحكم الفرعية هذه ، أو استخدامها فقط في المناطق التي لا تتطلب إجراءات أمنية مشددة.
3- تميل وحدات التحكم الرئيسية إلى أن تكون باهظة الثمن ، وبالتالي فإن مثل هذا الهيكل ليس مناسبًا تمامًا للأنظمة ذات المواقع البعيدة المتعددة التي لها أبواب قليلة فقط.
4- تنطبق جميع العيوب الأخرى المتعلقة بـ RS-485 المدرجة في الفقرة الأولى.

2. Serial main controllers & intelligent readers.

جميع أجهزة الباب متصلة مباشرة بقارئات ذكية أو شبه ذكية القراء عادة لا يتخذون قرارات الوصول ، ويعيد توجيه جميع الطلبات إلى وحدة التحكم الرئيسية فقط في حالة عدم توفر الاتصال بوحدة التحكم الرئيسية ، سيستخدم القراء قاعدة البيانات الداخلية الخاصة بهم لاتخاذ قرارات الوصول وتسجيل الأحداث. يجب استخدام القارئ شبه الذكي الذي لا يحتوي على قاعدة بيانات ولا يمكنه العمل بدون وحدة التحكم الرئيسية فقط في المناطق التي لا تتطلب درجة أمان عالية تدعم وحدات التحكم الرئيسية عادة من 16 إلى 64 قارئًا.

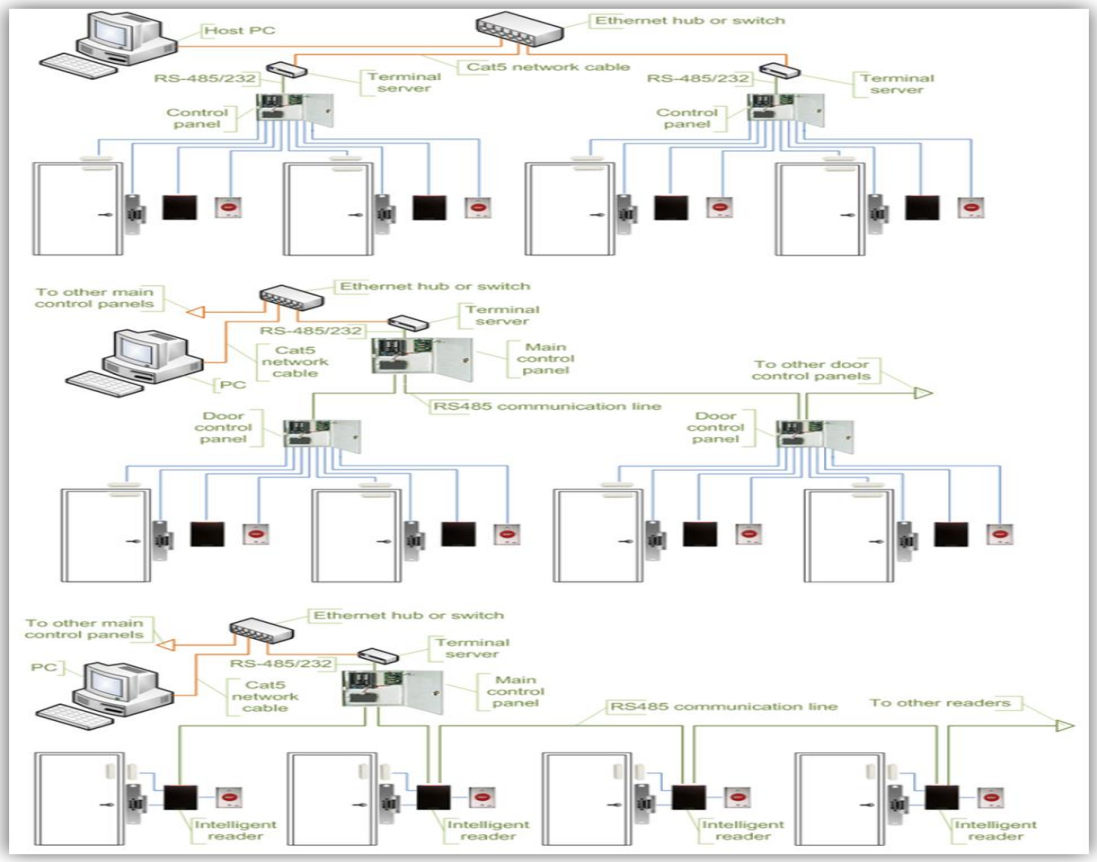
جميع المزايا والعيوب هي نفسها المذكورة في الفقرة الثانية.



Access control system using serial main controller and intelligent readers

3. Serial controllers with terminal servers.

على الرغم من التطور السريع والاستخدام المتزايد لشبكات الكمبيوتر ، ظل مصنعو التحكم في الوصول محافظين ، ولم يتسرعوا في تقديم منتجات تدعم الشبكات. عند الضغط على الحلول ذات الاتصال بالشبكة ، اختار الكثير الخيار الذي يتطلب جهدًا أقل إضافة خادم طرفي جهاز يحول البيانات التسلسلية للإرسال عبر LAN أو.WAN



Access control systems using serial controllers and terminal servers

مميزات هذا النظام

1- يسمح باستخدام البنية التحتية للشبكة الحالية لتوصيل أجزاء منفصلة من النظام.
2- يوفر حلاً مناسبًا في الحالات التي يكون فيها تركيب خط RS-485 صعبًا أو مستحيلًا.

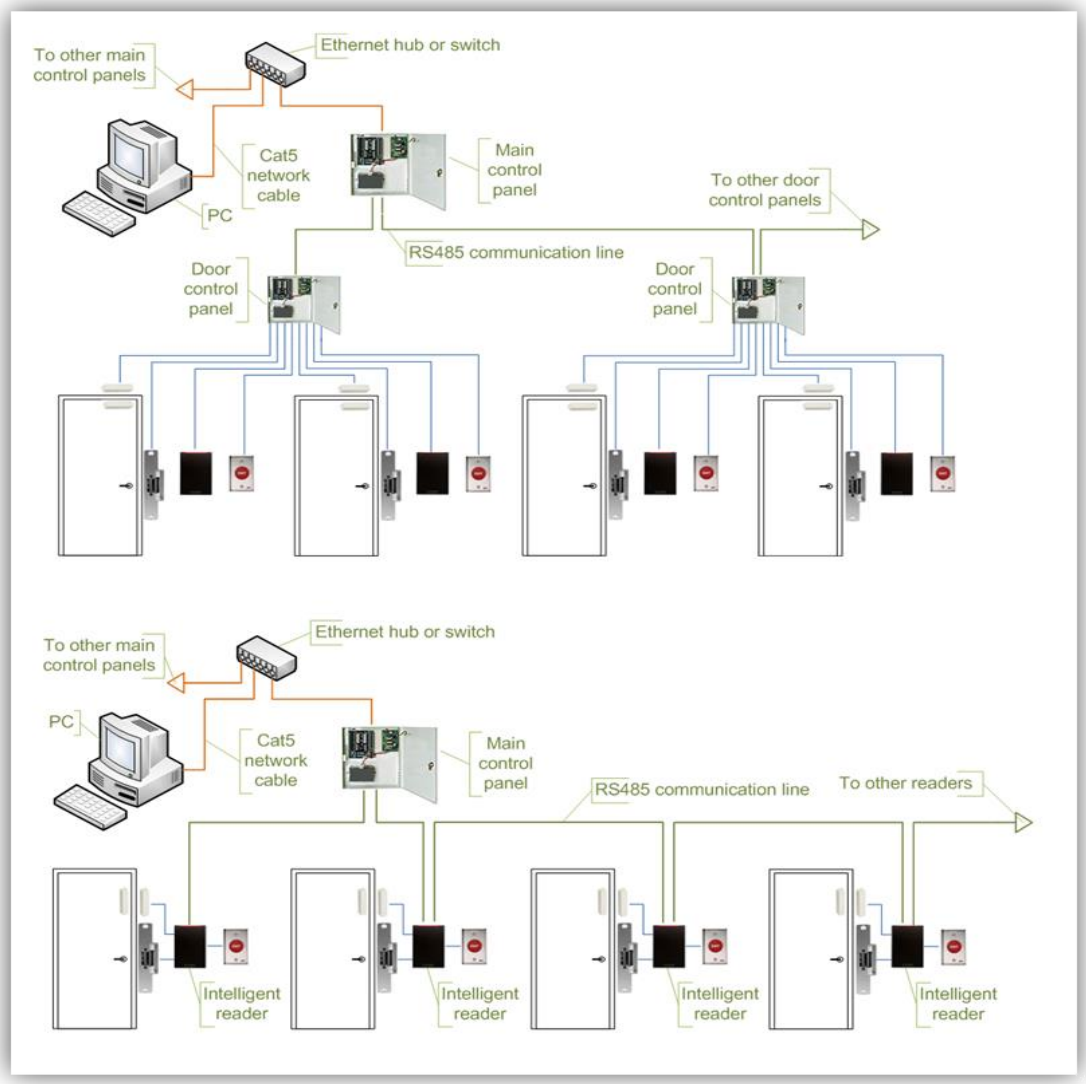
عيوب هذا النظام

1- يزيد من تعقيد النظام.
2- يخلق عملاً إضافيًا للمثبِّتين: عادةً ما يجب تكوين الخوادم الطرفية بشكل مستقل ، وليس من خلال واجهة برنامج التحكم في الوصول.

3- يعمل ارتباط الاتصال التسلسلي بين وحدة التحكم والخادم الطرفي بمثابة عنق زجاجة على الرغم من أن البيانات بين الكمبيوتر المضيف والخادم الطرفي تنتقل بسرعة شبكة 100/10 / Mbit / sec1000 ، يجب أن تتباطأ إلى السرعة التسلسلية 112.5 كيلوبت / ثانية أو أقل.
وتنطبق أيضًا جميع المزايا والعيوب المتعلقة بـ RS-485.

5-Network-enabled main controllers.

الطوبولوجيا هي نفسها تقريبًا يتم تطبيق نفس المزايا والعيوب ، ولكن واجهة الشبكة الداخلية توفر بعض التحسينات القيمة يتم نقل بيانات التكوين والمستخدم إلى وحدات التحكم الرئيسية بشكل أسرع ، ويمكن أن يتم ذلك بالتوازي. هذا يجعل النظام أكثر استجابة ، ولا يقطع العمليات العادية لا يلزم وجود أجهزة خاصة لتحقيق إعداد فائض للكمبيوتر المضيف: في حالة فشل الكمبيوتر المضيف الأساسي ، قد يبدأ الكمبيوتر المضيف الثانوي في استقصاء وحدات التحكم في الشبكة. يتم أيضًا التخلص من العيوب التي تقدمها الخوادم الطرفية



Access control system using network-enabled main controllers

6. IP controllers

يتم توصيل وحدات التحكم بجهاز كمبيوتر مضيف عبر Ethernet LAN أو.WAN

مميزات هذا النظام

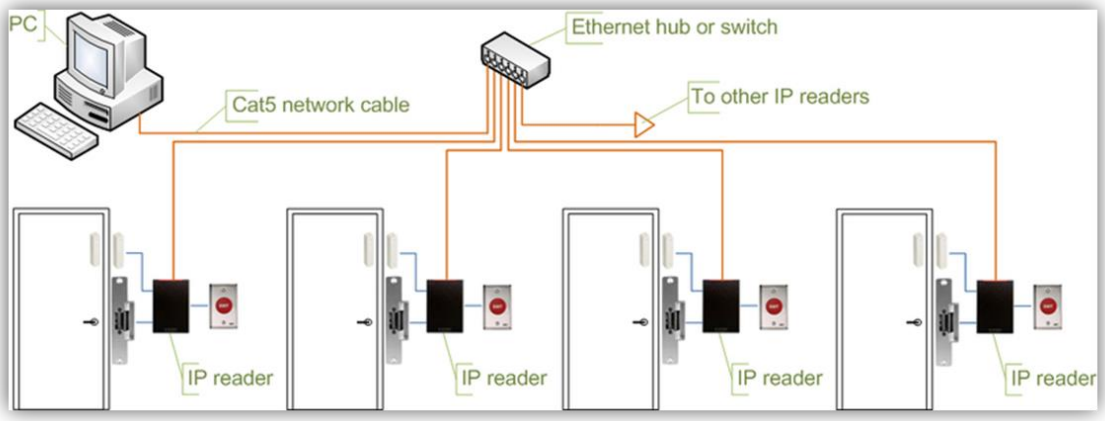
1- يتم استخدام البنية التحتية للشبكة الحالية بالكامل ، ولا توجد حاجة لتركيب خطوط اتصال جديدة.

2-لا توجد قيود فيما يتعلق بعدد وحدات التحكم مثل 32 لكل سطر في حالات.RS-485

3- لا يلزم وجود معرفة خاصة بتركيب RS-485 وإنهائها وتأريضها واستكشاف الأخطاء وإصلاحها.
4- يمكن إجراء الاتصال بوحدات التحكم بسرعة الشبكة الكاملة ، وهو أمر مهم في حالة نقل الكثير من البيانات (قواعد البيانات مع الآلاف من المستخدمين ، بما في ذلك السجلات البيومترية).
5- في حالة وجود إنذار ، قد تبدأ وحدات التحكم الاتصال بجهاز الكمبيوتر المضيف هذه القدرة مهمة في الأنظمة الكبيرة ، لأنها تعمل على تقليل حركة مرور الشبكة الناتجة عن الاستقصاء غير الضروري.
6- يبسط تركيب الأنظمة التي تتكون من عدة مواقع مفصولة بمسافات كبيرة. يعد ارتباط الإنترنت الأساسي كافياً لإنشاء اتصالات بالمواقع البعيدة.
7- تتوفر مجموعة واسعة من معدات الشبكة القياسية لتوفير الاتصال في مواقف مختلفة) ألياف ، لاسلكية ، VPN، مسار مزدوج ، PoE

عيوب هذا النظام

1- يصبح النظام عرضة للمشكلات المتعلقة بالشبكة ، مثل التأخير في حالة حركة المرور الكثيفة وتعطل معدات الشبكة.
2- قد تصبح وحدات التحكم في الوصول ومحطات العمل في متناول المتسللين إذا لم تكن شبكة المؤسسة محمية بشكل جيد يمكن القضاء على هذا التهديد عن طريق الفصل المادي لشبكة التحكم في الوصول عن شبكة المنظمة وتجدر الإشارة أيضًا إلى أن معظم وحدات التحكم في IP تستخدم إما نظام Linux الأساسي أو أنظمة تشغيل خاصة ، مما يجعل اختراقها أكثر صعوبة. يتم أيضًا استخدام تشفير البيانات القياسي في الصناعة.
3- أقصى مسافة من محور أو مفتاح إلى وحدة التحكم (في حالة استخدام كبل نحاسي) هي 100 متر (330 قدمًا).
4- تشغيل النظام يعتمد على الكمبيوتر المضيف في حالة فشل الكمبيوتر المضيف ، لا يتم استرداد الأحداث من وحدات التحكم وتتوقف الوظائف التي تتطلب التفاعل بين وحدات التحكم (مثل مكافحة التراجع) عن العمل. ومع ذلك ، تحتوي بعض وحدات التحكم على خيار اتصال من نظير إلى نظير لتقليل الاعتماد على الكمبيوتر المضيف



Access control system using IP readers

7. IP readers

القارئ متصل بجهاز كمبيوتر مضيف عبر Ethernet LAN أوWAN

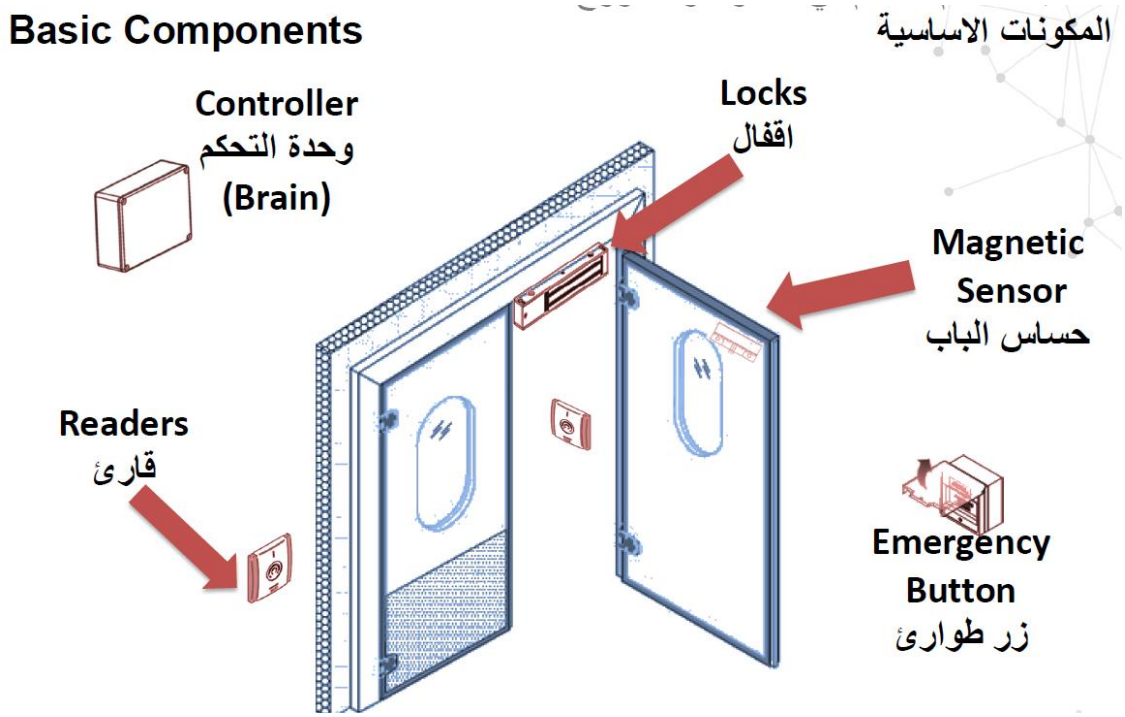
مميزات هذا النظام

1- معظم قارئات IP قادرة على PoE تجعل هذه الميزة من السهل جدًا توفير طاقة مدعومة بالبطارية للنظام بأكمله ، بما في ذلك الأقفال وأنواع مختلفة من أجهزة الكشف (في حالة استخدامها).
2- تلغي قارئات IP الحاجة إلى enclosureوحدة التحكم.
3- لا توجد سعة مهدرة عند استخدام قارئات IP على سبيل المثال ، وحدة تحكم ذات 4 أبواب ستحتوي على 25٪ من السعة غير المستخدمة إذا كانت تتحكم في 3 أبواب فقط.
4- تتوسع أنظمة قارئ IP بسهولة: ليست هناك حاجة لتثبيت وحدات تحكم رئيسية أو فرعية جديدة.
5- لا يؤثر فشل قارئ IP واحد على أي قارئ آخر في النظام

عيوب هذا النظام

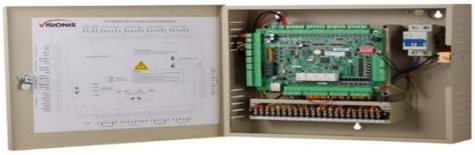
1- من أجل استخدامها في المناطق عالية الأمان ، تتطلب أجهزة قراءة بروتوكول الإنترنت وحدات إدخال / إخراج خاصة للتخلص من إمكانية التطفل عن طريق الوصول إلى أسلاك زر القفل / أو الخروج. لا تتوفر مثل هذه الوحدات النمطية لجميع مصنعي قارئIP.
2- نظرًا لكونها أكثر تعقيدًا من أجهزة القراءة الأساسية ، فإن قارئات IP هي أيضًا أكثر تكلفة وحساسية ، لذلك لا ينبغي تثبيتها في الهواء الطلق في المناطق ذات الظروف الجوية القاسية ، أو التي يحتمل أن تتعرض للتخريب ، ما لم تكن مصممة خصيصًا للتركيب الخارجي. يصنع عدد قليل من الشركات المصنعة مثل هذه النماذج.
3- تنطبق مزايا وعيوب وحدات تحكم IP على قارئات IP أيضًا.

مكونات نظام التحكم في الدخول و الخروج ACS



1-وحدة التحكمController

جهاز يخبر محرك البوابة بالعمل عندما يتلقى إشارة في حالة الاتصال الداخلي ، تكون هذه الإشارة عادةً عبارة عن اتصال إغلاق من مرحل على شكل نبضة تكمل الدائرة مؤقتًا.



The Access Control System (ACS) server

يدير البرنامج قد يحتوي على العديد من الخوادم في جهاز واحد ، أو موزعة على العديد من الأجهزة هذا الخادم مسؤول عن تعيين الوصول إلى وتتبع حركة المرور في المناطق الآمنة يحتفظ بقاعدة بيانات لأصحاب الاعتماد ومستوى وصولهم كما أنه يتواصل مع لوحات ACS لتنزيل بيانات محددة لكل لوحة لتخزين.

هناك طرق مختلفة يمكن لهذا الخادم الاتصال بها مع لوحات ACS إذا كانت اللوحات مزودة ببطاقات Ethernet ، فقد يكون الاتصال قائمًا على TCP / IP إذا كانت اللوحات مجهزة بواجهة RS-485 ، فإن الخادم (عبر محول RS-232 إلى 4) RS-485)) ، سيتواصل مع كل لوحة على الناقل التسلسلي ، واستقصاء كل لوحة ، والمعالجة بيانات اللوحة يمكن لخادم ACS أيضًا توفير "منحة المضيف" عند الطلب من اللوحات التي لا تحتوي على أحدث المعلومات يقوم خادم ACS بتحديث اللوحات على أساس مجدول ، ومع ذلك ، في غضون ذلك ، سيتم تزويد الأفراد بمنحة المضيف حتى ذلك الوقت.

The Badging Server

هو المكان الذي يتم فيه الاحتفاظ ببيانات الموظفين المصرح لهم سيقوم الخادم بمعالجة البيانات وإصدار (طباعة) بيانات الاعتماد عادةً ما يتلقى الموظف أو المقاول شارة بها العديد من المعلومات المشفرة ، بما في ذلك الصورة والاسم والعنوان والمؤسسة ومناطق الوصول وتاريخ انتهاء الصلاحية والقيود وغيرها من المعلومات الضرورية. إذا تم استخدام أجهزة القارئ في الموقع ، فقد يتم تشفير عينة من بصمات الأصابع ، أو مسح قزحية العين أيضًا.

Ethernet Router or Switch

RS-232 to RS-485 Converter

RS-232 هى واجهة تسلسلية مع خطوط تحكم متوازية للتحكم في تدفق البيانات ليست كل الإشارات ضرورية في جميع الحالات يستخدم المنفذ التسلسلي للكمبيوتر PIN 2 و 3 و 5. عادةً ما يتم ربط خط RTS إلى CTS لتطبيقات التحكم في التدفق ، وبما أنه لا يوجد مودم هاتف ، لا يتم استخدام RI و CD يستخدم RS-232 برامج تشغيل وأجهزة استقبال "أحادية الطرف". يصف الجدول أدناه أسماء الإشارات والمسامير المرتبطة بها

Pin Description	Symbol	Pin Number
Carrier Detect	CD	1
Receive Data	RD	2
Transmit Data	TD	3
Data Terminal Rdy	DTR	4
Signal Ground	SG	5
Data Set Ready	DSR	6
Request to Send	RTS	7
Clear to Send	CTS	8
Ring Indicator	RI	9

The video router/switch

يوفر القدرة على مراقبة أي كاميرا ، أو عرض متعدد الإرسال في محطة عمل عميل النظام.

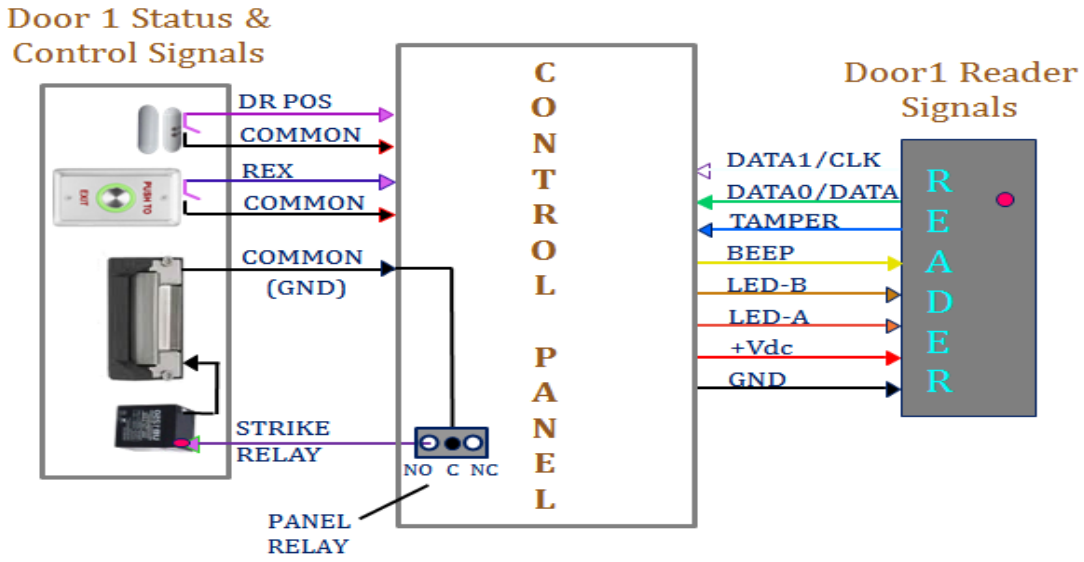
The digital video recorder

عادة ما يكون قيد التشغيل ، ويسجل الأحداث على أساس حلقة تعتمد مدة الحلقة على متطلبات العميل. هناك العديد من الكاميرات في نظام المؤسسة الكبيرة ، وربما هناك العديد من المسجلات أيضًا عادةً ما يتم تعيين المسجلات لعدد محدود من الكاميرات بناءً على سعة التخزين الخاصة بها ، ولكن ليس أقل من ذلك ، فهي ضرورية للوجود على شبكة IP نفسها بحيث يمكن استدعاء الأحداث وإعادة تشغيلها عند الطلب لكل منطقة.

The control Panel

تقوم بمعالجة بيانات القارئ ، والإبلاغ عن موضع الباب (مفتوح ، مغلق) ، ويقوم بقبول طلب الخروج من الجانب الآمن ، ويأمربفتح الباب الكهربائي ، أو البقاء مغلقًا. على جانب الخادم ، يستجيب لاستطلاعات الرأي ، وتقارير التطفل ، والإنذارات ، ومشكلات الاعتماد ، وإنذارات التلاعب ، وعدد من المعلومات الأخرى حسب الحاجة لجعل المنطقة آمنة.

تحتفظ اللوحات ببيانات اعتماد المستخدم على ذاكرة فلاش في حالة عدم توفر الاتصال بين اللوحة والخادم ستعمل اللوحات بشكل مستقل حتى يتم استعادة الاتصال. هناك العديد من اللوحات والواجهات التي تربط اللوحة بالخادم. تتصل بعض اللوحات بالخادم على بروتوكول Ethernet ، وبعضها على ناقل RS-485.



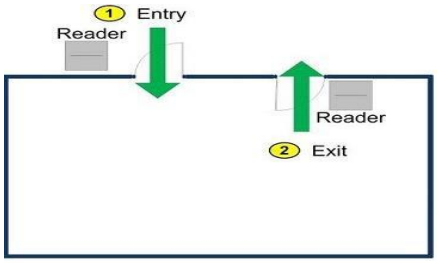
يوجد أنواع أخرى من لوحات التحكم وهى وايرلس

تتطور الأجهزة والأنظمة اللاسلكية بسرعة ، وستحل في النهاية محل الاتصالات السلكية ومع ذلك ، فإن تعقيد هذه الأنظمة يتجاوز بكثير أي تقنية سلكية بصرف النظر عن التصميم الرقمي ، يجب تصميم قسم الترددات الراديوية

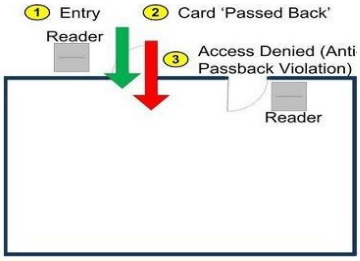
الأكثر حساسية واعتماده وترخيصه ثم هناك مشكلة التداخل والتعايش مع الأجهزة اللاسلكية الأخرى التي قد تؤثر على موثوقية التشغيل.

Global anti pass back

معنى anti-pass back هومنع حامل الكارد من تمرير الكارد اوالباسوورد الخاص به إلى شخص ثان للدخول في نفس المكان اومن نفس الباب الذي دخل فيه الشخص الاول حيث ان النظام يطلب تسجيل الخروج قبل الدخول الى نفس المكان مجددا



اما عن ال Global Anti Pass back فهو ما لا يستطيع اي نظام اخر فعله في حاله ال offline و تعريفه هو نفس تعريف ال Anti Pass back غير انه لا يسمح بدخول الشخص اي من الاماكن التى في النظام ككل وليس نفس المكان فقط و ذلك بفضل تكنولوجيا ال P2P و هي ان كل الوحدات على اتصال دائم ببعضها البعض بغض النظر عن كون السيرفر يعمل او لا.

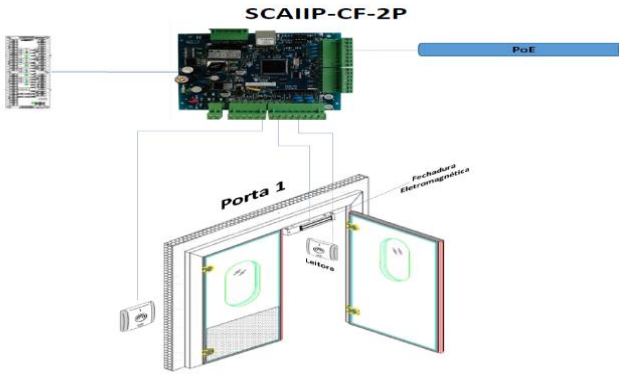


POE Controller's charge system

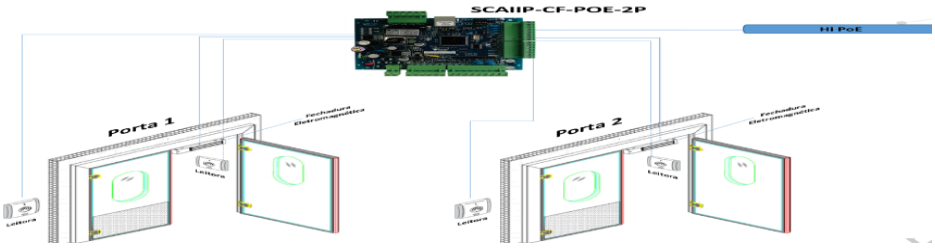
هنا نجد أن وحدات التحكم controllers تعمل اما عن طريق الكهرباء او عن طريق POE و هي عبارة عن دمج الكهرباء مع الاشارة في كابل واحد Ethernet وبذلك يصبح كل وحدة لهاكابل واحد فقط للتغذية والاشارة بدلا من كابلين لكل منهما و هنا يشترط ان توصل كل الوحدات عن طريق. POE Switch

ما هى طرق إستخدام وحدة التحكم في الابواب؟

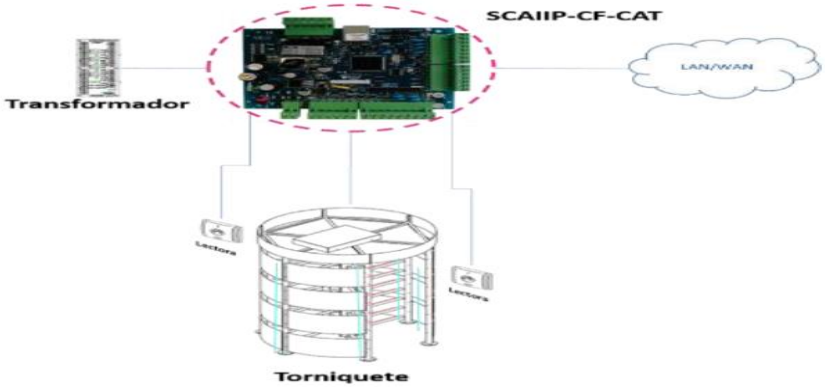
1- عند وجود باب واحد فقط



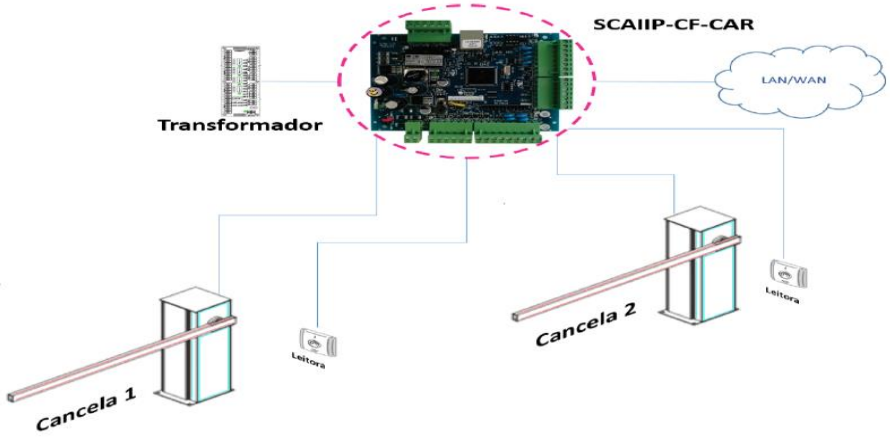
2- عند وجود مجموعة من الأبواب



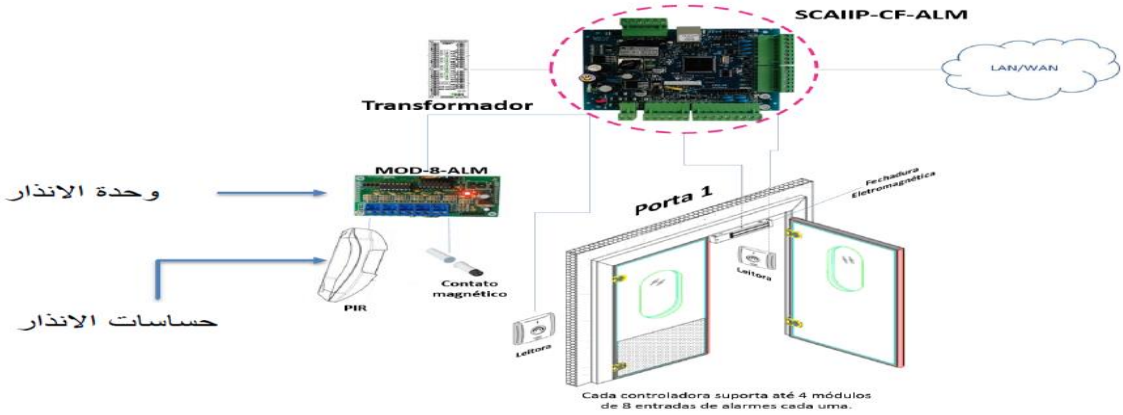
3-الابواب الدوارةTurnstile



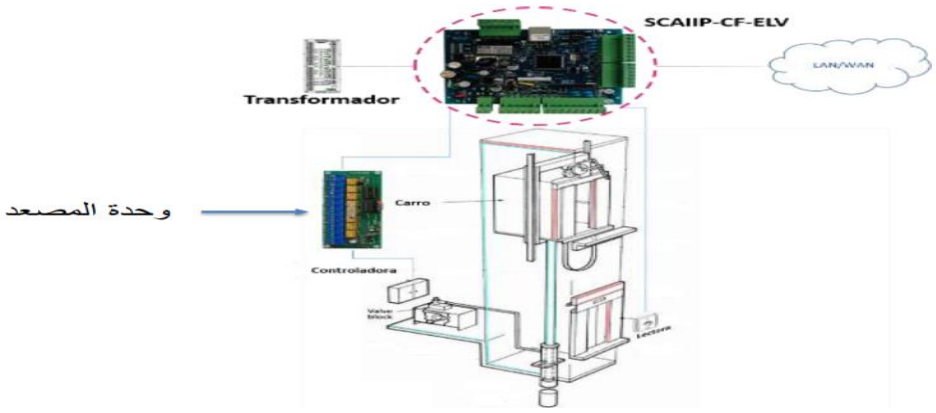
4- في الجراجاتParking area



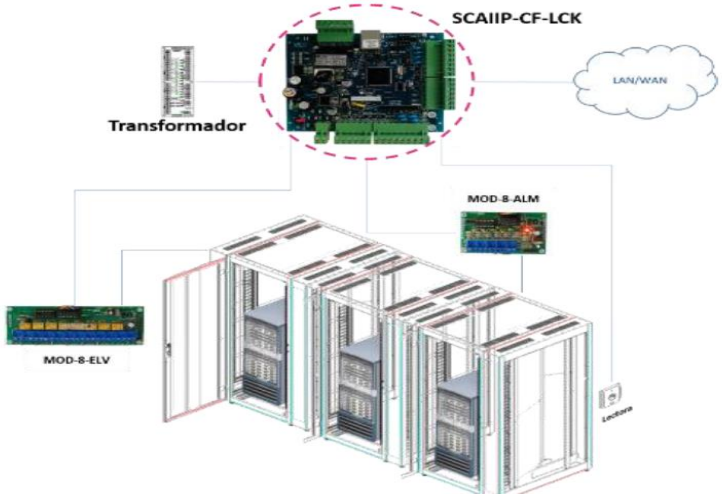
5-مع حساسات الانذار



6- في المصاعد



7-في ابواب الراك



2-القارئReader

أنواع القارئ Types of reader

يمكن تصنيف قارئات التحكم في الوصول حسب الوظائف التي يمكنهم القيام بها:

أجهزة القراءة الأساسية (غير الذكية):

ما عليك سوى قراءة رقم البطاقة أو رمز PIN ، وإعادة توجيهها إلى لوحة التحكم.

في حالة تحديد الهوية ، يخرج هؤلاء القراء رقم معرف المستخدم عادةً ما يتم استخدام بروتوكول Wiegand لنقل البيانات إلى لوحة التحكم ، ولكن الخيارات الأخرى مثل RS-232 و RS-485 و Clock / Data ليست شائعة.

اما النوع الأكثر شيوعًا من برامج قراءة التحكم في الوصول. مثل

RF Tiny by RFLOGICS و Prox Point by HID و P300 by Farpointe Data.

أجهزة القراءة الأساسية (متوسطة الذكاء):

لديهم جميع المدخلات والمخرجات اللازمة للتحكم في أجهزة الباب (القفل ، ملامسة الباب ، زر الخروج) ، لكن لا تتخذ أي قرارات تتعلق بالوصول عندما يقدم المستخدم بطاقة أو يُدخل رقم التعريف الشخصي ، يرسل القارئ المعلومات إلى وحدة التحكم الرئيسية وينتظر ردها إذا انقطع الاتصال بوحدة التحكم الرئيسية ، فإن هؤلاء القراء يتوقفون عن العمل أو يعملون في وضع متدهور.

أجهزة القراءة الأساسية (الذكية):

لديهم جميع المدخلات والمخرجات اللازمة للتحكم في أجهزة الباب ؛ لديهم أيضًا ذاكرة وقوة معالجة ضرورية لاتخاذ قرارات الوصول بشكل مستقل مثل أجهزة القراءة شبه الذكية ، فهي متصلة بلوحة تحكم عبر ناقل RS-485 ترسل لوحة التحكم تحديثات التكوين وتسترد الأحداث من القراء.

ومن الأمثلة على هؤلاء القراء: InfoProx IPO200 من CEM Systems و AP-500 من Apollo.
يوجد أيضًا جيل جديد من القراء الأذكياء يشار إليهم باسم "قراء IP". لا تحتوي الأنظمة التي تحتوي على قارئات IP عادةً على لوحات تحكم تقليدية ، ويتواصل القراء مباشرة مع جهاز كمبيوتر يعمل كمضيف.

أمثلة على هؤلاء القراء هي Foxtech FX-50UX ،

قارئ بصمات الأصابع FX-632 / جهاز التحكم في الوصول ،

نظام التحكم في الوصول PowerNet IP Reader بواسطة Isonas Security System ID ID 11 بواسطة Solus (يحتوي على خدمة ويب مضمنة لجعله سهل الاستخدام) ،

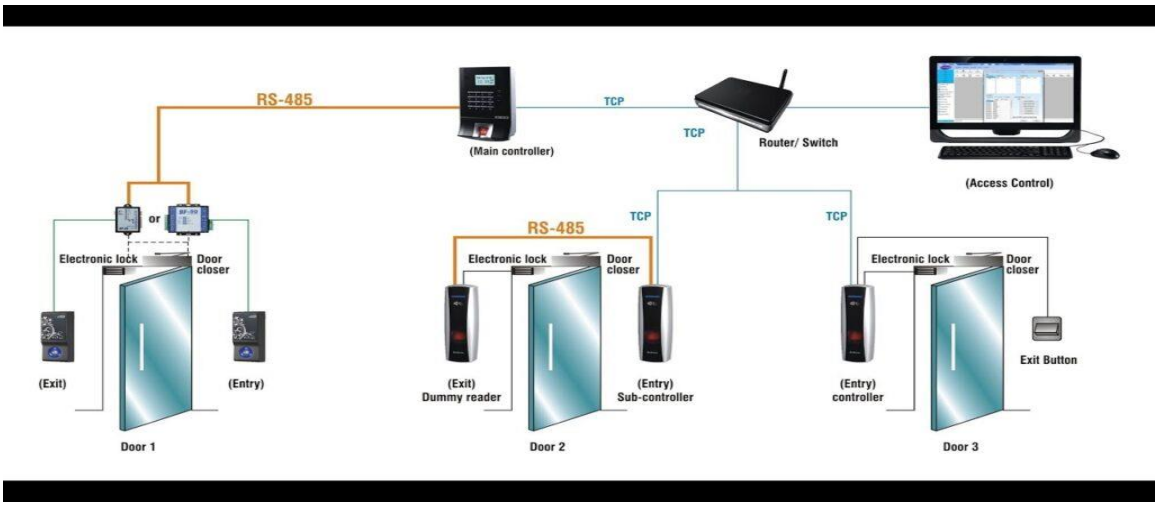
قارئ Edge ER40 بواسطة HID Global، LogLock و UNiLOCK بواسطة ASPiSYS Ltd ، وقارئ BioEntry Plus من شركة Suprema Inc. ، و G V-Station bym Bioscript In4

قد يكون لدى بعض القراء ميزات إضافية مثل شاشة LCD وأزرار الوظائف لأغراض جمع البيانات (مثل أحداث تسجيل الدخول / الخروج لتقارير الحضور) والكاميرا - مكبر الصوت - الميكروفون للاتصال الداخلي ودعم القراءة - الكتابة بالبطاقة الذكية.

يمكن أيضًا تصنيف أجهزة قراءة التحكم في الوصول حسب نوع تقنية تحديد الهوية الخاصة بهم.

برمجة جهاز Bio metric Access Control

يعد نظام التحكم في الوصول إلى Bio metric نظامًا للتحكم في الحضور والانصراف مع إمكانية الوصول إلى بصمات الأصابع ويتتبع ويسجل بيانات الزوار والموظفين من خلال برنامج الوصول الخاص به، يستخدم هذا على نطاق واسع في الأماكن السرية لسهولة التركيب والأمان العالي.



3-الأقفال والإكسسوارات Locks and Accessories

هناك أنواع مختلفة من طرق قفل الباب البوابة المتاحة اعتمادًا على مستويات الأمان المطلوبة ووظائف النظام وتطبيقه.

تُستخدم أنظمة القفل الكهربائية أو الإلكترونية جنبًا إلى جنب مع جهاز التحكم في الوصول أو جهاز الاتصال الداخلي بالباب ، حيث يرسل الوصول الاتصال الداخلي إشارة إلى القفل بمجرد تأكيد مصادقة الهوية.

Maglock (Magnetic Lock)

هو مغناطيس كهربائي قوي يتم تركيبه عادة فوق الباب ينجذب إلى لوحة الباب عند قفل الباب بالطاقة يتم فتح الباب عن طريق فتح مرحل يقطع الطاقة عن القفل.

Electric Strike Lock

هي جهاز يتم تركيبه في إطار الباب بما يتماشى مع الماسك يتحول إلى `` سلاسة " عند تشغيله للسماح للمزلاج بـ الانسحاب من خلال " الضربة والباب لفتحه في حالة تعطل الضربة الآمنة ويتحرك عندما لا يتم تشغيله في حالة الأمان (مثل maglock).

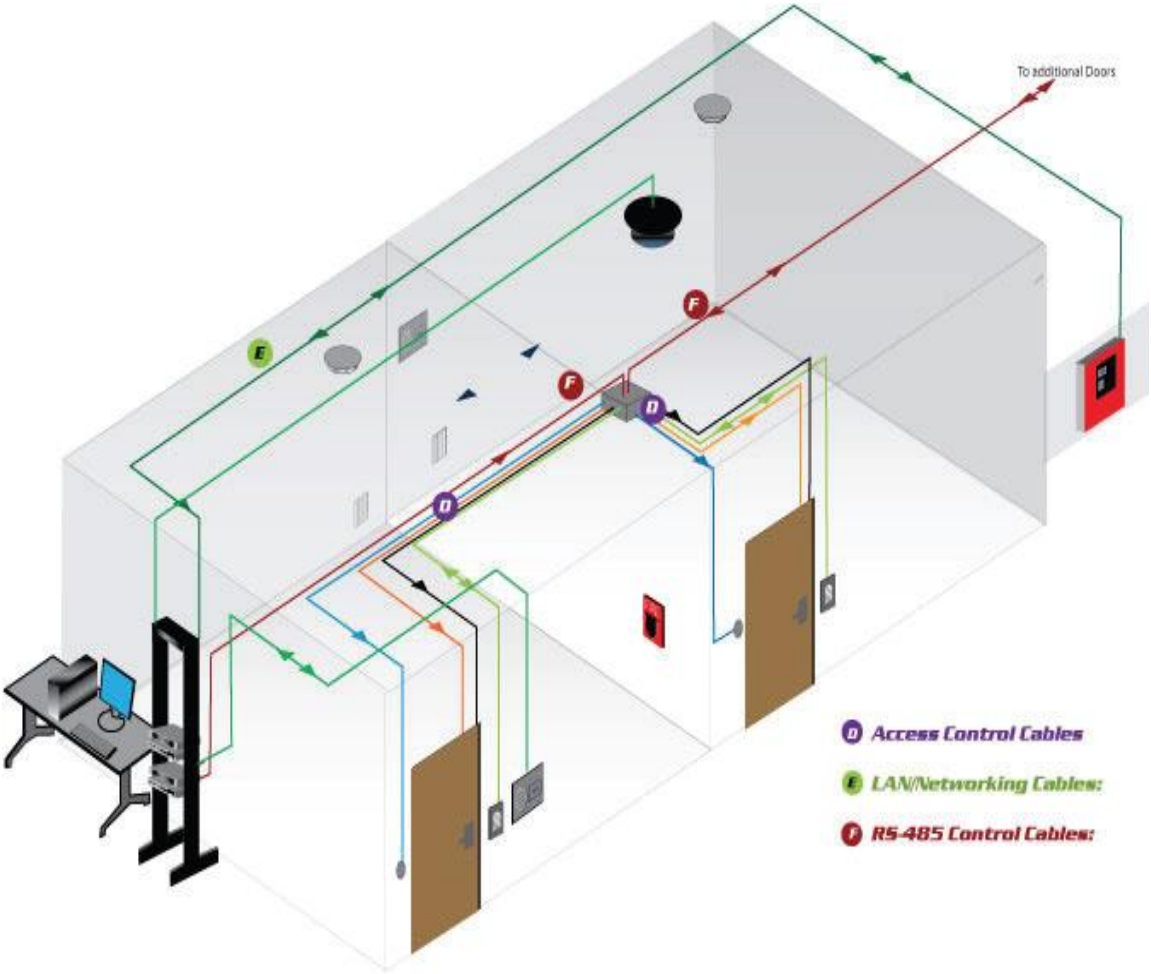
Solenoid Lock

الملف اللولبي هو جهاز يشبه الترباس يتحرك في اتجاه معين عندما يتم تشغيله كهربائيًا يعتمد كل من Maglock ، والضربة ، والملف اللولبي على المغناطيسات الكهربائية للعمل.

4-مفتاح الخروج Request to exit / Egress

هو مفتاح إغلاق مؤقت يتم عادةً إلغاء ارتداده عند الضغط عليه ، يتم إغلاق الدائرة وإشارات اللوحة لتحرير قفل الباب للسماح بالخروج من المنطقة الآمنة.

طرق تصميم أنظمةالتحكم فى دخول الأبواب



تحتوي جميع أنظمة التحكم في الوصول على نوع من القارئ ولوحة التحكم والبرامج والأجهزة الطرفية الأخرى.

Access Control Cables:

1-Reader Cables: Dependent on the type of Reader (Barcode , Magnetic Strip, Computer Chip, Biometric, and many others).

2-Door Contact Cables

3-Request to Exit Cables

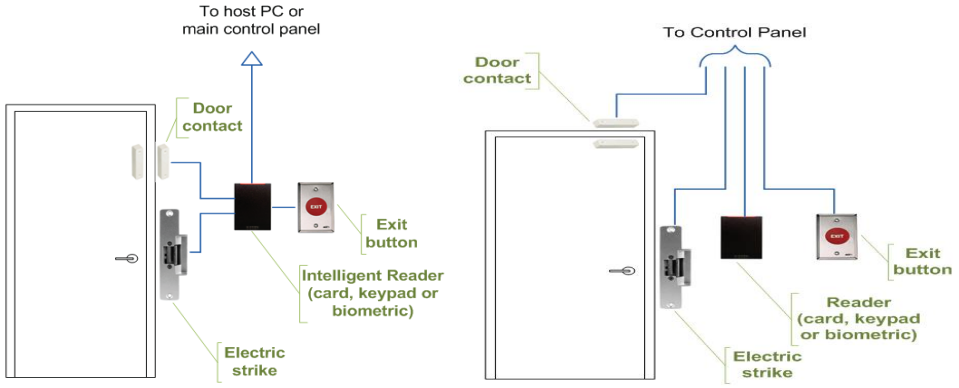
4-Lock Power Cables

5-RS-485 Cables: Communication Cables for Low Streaming Data to the Control Panels

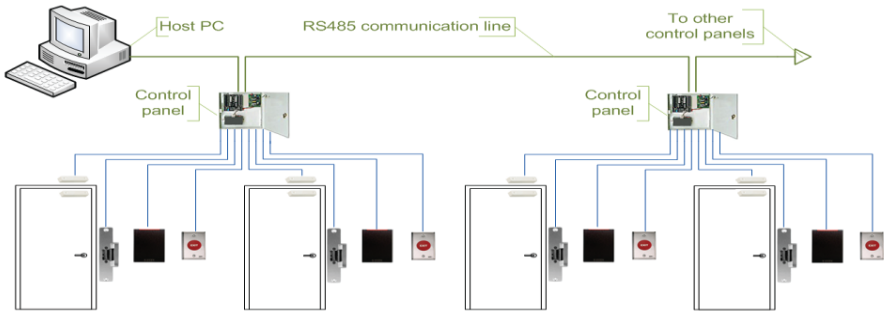
6-LAN/Networking Cables: Communication for Low/Medium/High Data Rates for Data transfer.

هناك أنواع عديدة لتصميم أنظمة التحكم في الوصول

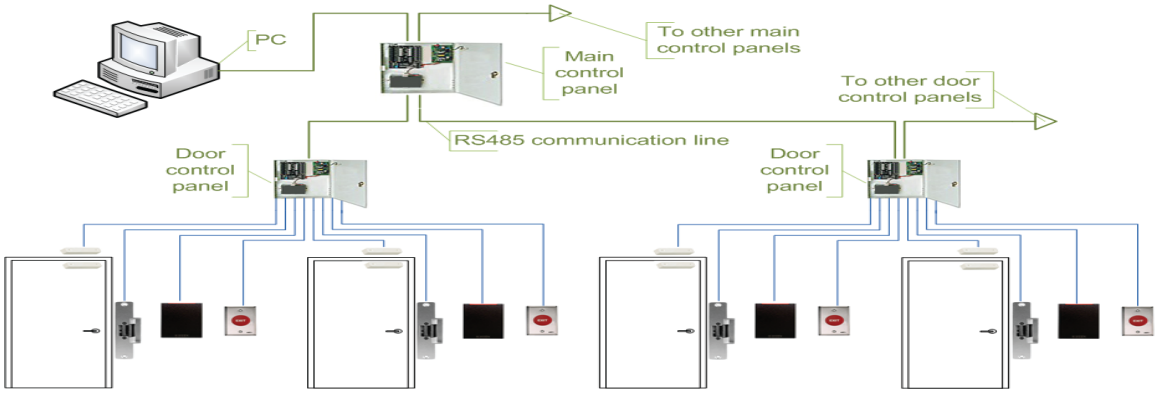
1-Typical Access Control Door Wiring Access Control Door Wiring when using host PC& Control panel



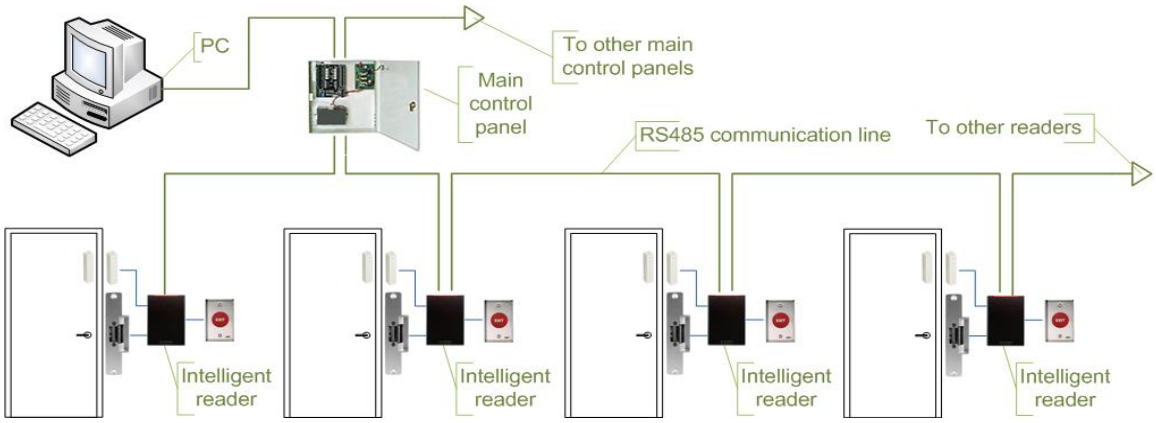
2-Access Control Systems using Serial Controllers



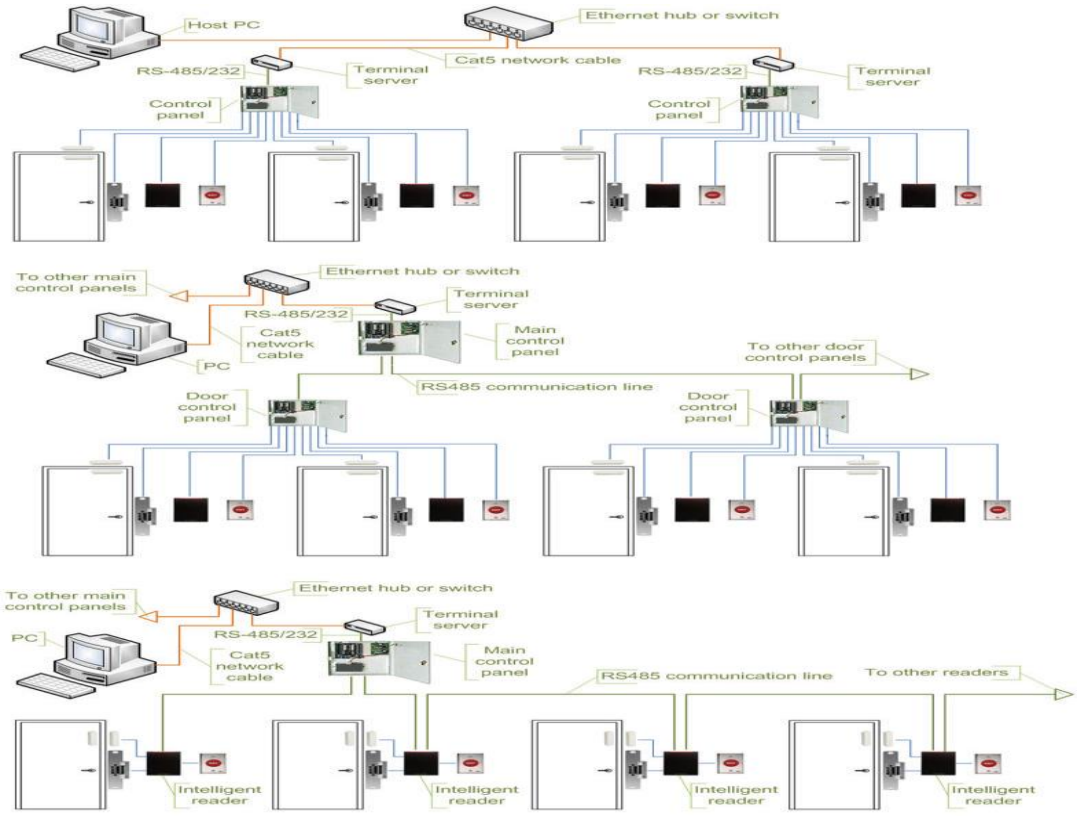
3-Access Control System using Serial main and Sub-Controllers



4-Access Control Systems using serial main controller and intelligent readers

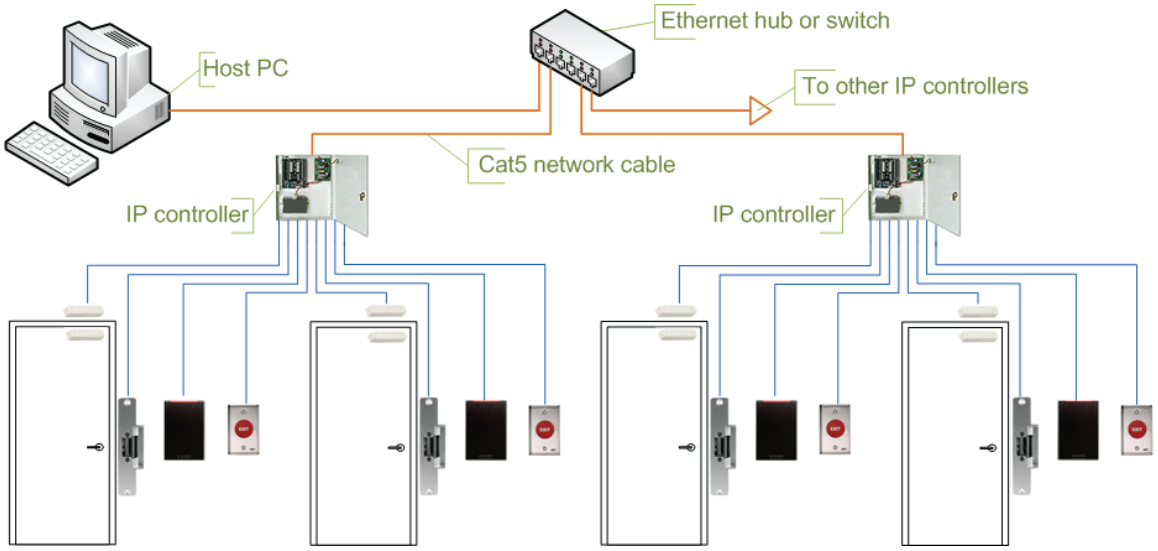


5-Access control systems using serial controllers and terminal servers

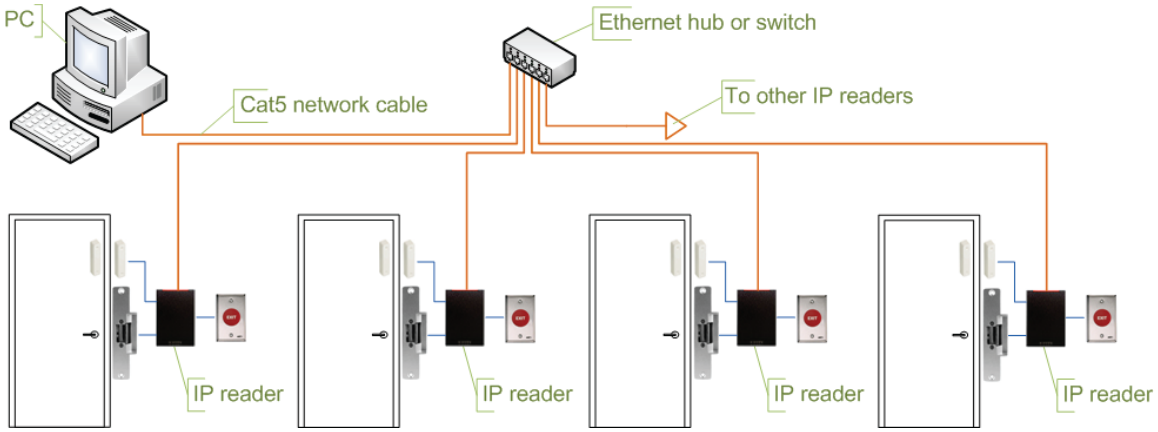


Access Control IP Design

1- Access control system using IP controllers



2-Access control system using IP Readers



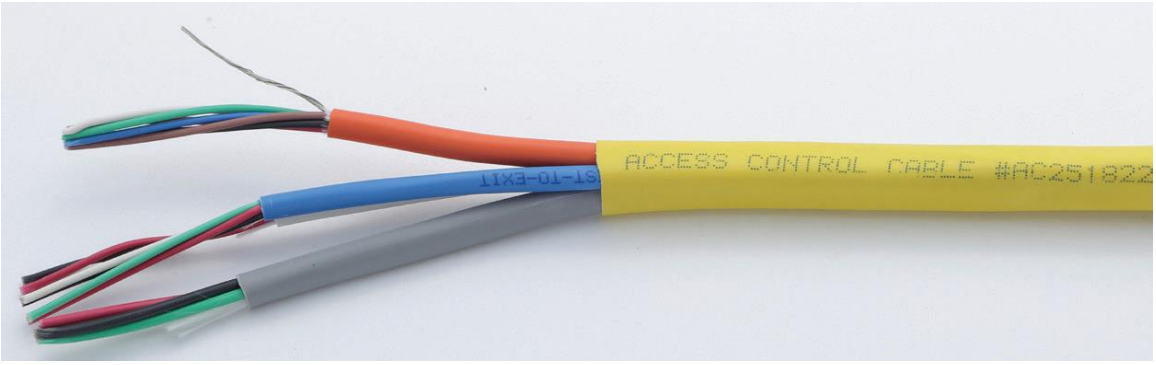
الكابلات المستخدمة لنظام التحكم فى دخول وخروج الأبواب

1-الكابلات المستخدمة للأنواع العادية فى التحكم فى دخول وخروج الأبواب

1-Reader Cable:

22/6 Shielded

3Pair 22AWG Shielded - Longer Run Orange Jacket



2-Door Contact Cable:

22/2 Unshielded White Jacket

3-Lock Power Cable:
18/4 Unshielded Gray Jacket

4-Request-to-Exit (REX):
22/4 Unshielded Blue Jacket

The Access Control All-In-One Cable is available in 3 Types of Designs:

Cable Type	AWG Size	# of Cond. or Pair	CM	CMP
Reader	22	6 or 3 Pair	AC1822	AC251822B AC251822B3P (3 Pair)
Door Contact	22	2		
Lock Power	18	4		
REX	22	4		

AC1822 - Overall Blue Jacket CM Rated
AC251822B - Overall Yellow Jacket CMP Rated
AC251822B3P - Overall Yellow Jacket CMP Rated (3Pair Reader Cable)

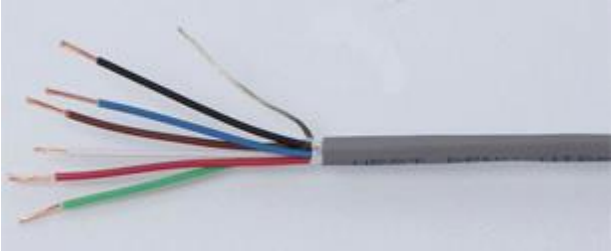
All the reader cables in the All-In-One Cable design can reach up to 250ft from Panel to Reader.
Our 3 Pair Design can reach up to 290ft.

مثال من إحدى الشركات المورد لنظام التحكم فى الدخول والخروج فى تحديد الكابلات والأسلاك المستخدمة

وهى شركة West Penn Wire

Reader Cable:

The Reader Cables range from 6 thru 15 Conductors. Most Systems are Weigand or Proximity Readers which utilize 6 Conductors, for Keypads and other devices may require a higher conductor count. The AWG Size is normally between 22-18AWG Stranded Conductors.
The insulation of standard reader cables are normally PVC (Flame Retardant)



Door Contact Cable:

The Door Contact cable is utilized to open/close door contact closures. The cable Conductor and AWG is normally 22-18AWG with 2 to 4 Conductors.
The Insulation is either PVC (Flame Retardant) or PP. The Capacitance of the cable is not an important Characteristics of the door contact cable

Lock Power Cable:

The Lock Power cable is used for the electronic locking device. The cable conductor and AWG is normally18 14 AWG and 2 to 4 Conductors

Request-to-Exit (REX):

The REX Cable is used where REX is required in an Access Control System. REX can be a Push Button or motion detection. The cable conductor and AWG is normally 22-18AWG and 2 to 4 Conductors.

Access Control RS-485 Communication

Serial controllers. Controllers are connected to a host PC via a serial RS-485 communication line. External RS-232/485 converters or internal RS-485 cards have to be installed, as standard PCs do not have RS485 communication ports.

Advantages:

• RS-485 standard allows long cable runs, up to 4000 feet (1200 m)

• Relatively short response time. The maximum number of devices on an RS-485 line is limited to 32, which means that the host can frequently request status updates from each device, and display events almost in real time.

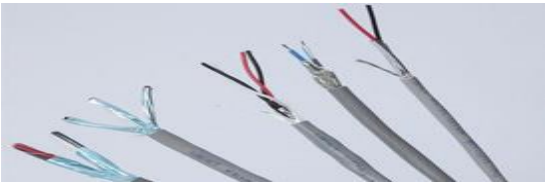
• High reliability and security as the communication line is not shared with any other systems.

Disadvantages:

• RS-485 is not well suited for transferring large amounts of data (i.e. configuration and users).

Te highest possible throughput is 115.2 kbit/sec, but in most system it is downgraded to 56.2 kbit/sec, or less, to increase reliability.

• RS-485 does not allow the host PC to communicate with several controllers connected to the same port Simultaneously. Therefore, in large systems, transfers of configuration, and users to controllers may take avery long time, interfering with normal operations.



RS-485 Cables:

Conductor

22-24 AWG Tinned Copper

Insulation:

Low Loss Insulation - Polypropylene (PP) or Polyethylene (PE) for Non-Plenum and FEP (Tefon) for Plenum

Rated Cables

Impedance: 100-120 Ohms

Capacitance: 12-16pf/f

Shield:

RS-485 cables require a shield to help in reducing the EMI/RFI interference.

A Overall Shield 100% Foil, or Overall Shield 100% Foil+ High Percetage braid

Jacket:

The jacket depends on the environment the installation is in.

General, Riser or Plenum.

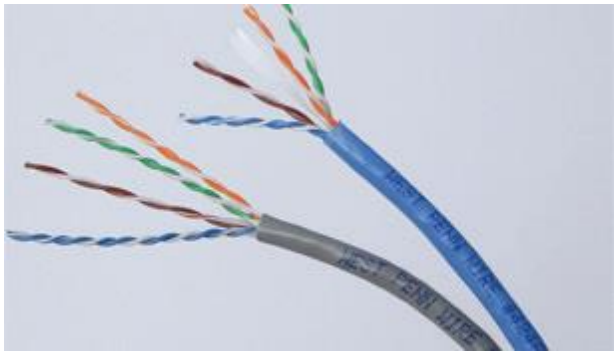
Access Control Cable List

Environment	Reader Cables	Door Contact	Lock Power Cable	REX Cables	RS-485 Cables
Non Plenum	3270 3271 3272 3263 3021	221 224 241	244 245	241 244	D2401 D4851 D2402 D4852
Plenum	253270 253271	25221B 25224B 25241B	25244B 25245B	25241B 25244B	D252401 D254851 D252402 D254852
Indoor/Outdoor	AQC3270 AQC3186 AQC3274	AQC224 AQ224	AQC44	AQ244	

-

2-الكابلات المستخدمة لأنواع IP فى التحكم فى دخول وخروج الأبواب

Cables: Category 5E and/or Category 6.



IP readers. Readers are connected to a host PC via Ethernet LAN or WAN.

Advantages:

• Most IP readers are PoE capable. Tis feature makes it very easy to provide battery backed power to the entire system, including the locks and various types of detectors (if used).

• IP readers eliminate the need for controller enclosures.

• IP reader systems scale easily: there is no need to install new main or sub-controllers.

Disadvantages:

• In order to be used in high-security areas, IP readers require special input/output modules to eliminate the possibility of intrusion by accessing lock and/or exit button wiring. Not all IP reader manufacturers have such modules available.

• Being more sophisticated than basic readers, IP readers are also more expensive and sensitive, therefore they should not be installed outdoors in areas with harsh weather conditions, or high probability of vandalism, unless specifically designed for exterior installation. A few manufacturers make such models.

Environment	Category 5E UTP	Category 5E F/UTP	Category 6 UTP	Category 6 F/UTP	Category 6A UTP	Category 6A F/UTP
Non Plenum	4245	4245F	4246	4246F	4246A	4246AF
Plenum	254245	254245F	254246	254246F	254246A	254246AF
Indoor/Outdoor	4245IO		4246IO			
Outside Plant	4245OSP		4246OSP			
Armored	M57562					

نصائح عن تصميم نظام التحكم ؟

1. Scale of project and future expansion

لا يؤثر حجم المشروع على الميزانية فقط ، ولكن أيضًا على اختيار ووظيفة أجهزة التحكم في الوصول والبنية التحتية للكابلات والقدرة على توسيع النظام مع توسع المشروع - الموقع أو الاتصال بمواقع إضافية.

2. Number of users requiring access

سيكون لحجم المشروع وتطبيقه تأثير كبير على عدد المستخدمين الذين سيحتاجون إلى الوصول إلى المبنى قد تسمح أرقام المستخدمين الأقل بأساليب مصادقة أكثر أمانًا ؛ في حين أن حركة المرور العالية والحاجة إلى سرعة نقل البيانات قد تتطلب أساليب مصادقة بسيطة وعالية السرعة وفتح وإغلاق الباب - الحاجز بسرعة عالية.

سيؤثر نوع المستخدمين أيضًا على اختيار النظام ؛ هل المستخدمون جميعهم أفراد عاديون ومسجلون (مثل المقيمين أو الموظفين) أم أن هناك عددًا كبيرًا من الزوار غير المسجلين الذين يحتاجون إلى الوصول إلى المبنى وإليه

3. What sort of identity authentication is required?

مصادقة الهوية" هي الطريقة المستخدمة لتأكيد هوية المستخدم الذي يرغب في الوصول إلى المبنىهناك مجموعة واسعة من طرق تحديد الهوية المتاحة ، من أبسط رمز PIN يتم كتابته في لوحة المفاتيح ، إلى أحدث طرق التعرف على القياسات الحيوية التي تعمل بالذكاء الاصطناعي مثل التعرف على الوجه أو قزحية العين

Identity authentication methods:

- RFID
- NFC
- PIN Code
- Bluetooth (BLE)
- QR Code Scanning
- Fingerprint Reader
- Face Recognition
- Iris Recognition
- ANPR (Automatic Number Plate Recognition)

4. Multiple-factor Authentication methods or multiple options?

يمكن تحقيق مستويات أعلى أمان الوصول باستخدام المصادقة متعددة العوامل (يشار إليها أحيانًا بالمصادقة المزدوجة) ، حيث يلزم الجمع بين طريقتين أو أكثر من طرق التحقق من الهوية للسماح بالدخولعلى سبيل المثال ، قد يطلب النظام من المستخدم مسح هاتفه الذكي بحثًا عن Bluetooth أو NFC وإدخال رقم تعريف شخصي فريد أو كلمة مرور في لوحة مفاتيح وحدة الوصول.

يجب عدم الخلط بين المصادقة متعددة العوامل وأساليب المصادقة المتعددة ؛ ستتميز العديد من أجهزة الاتصال الداخلي للأبواب وأجهزة التحكم في الوصول بمجموعة متنوعة من خيارات التحقق من الهوية للاختيار من بينها ، بينما تتطلب فقط من المستخدم توفير بطاقة واحدة للدخول - على سبيل المثال. Bluetooth أو NFC أو رمز PIN).

5. How many access location points in the system and how will they be used?

قد تحتوي المشاريع الكبيرة الحجم على عدد كبير من مواقع الوصول للموظفين والزوار والوصول إلى المركبات. يعد إجراء مراجعة تفصيلية للموقع لتأكيد جميع نقاط الوصول (الدخول والخروج) - بما في ذلك الأبواب المغلقة الخارجية والداخلية والبوابات والحواجز والوصول إلى مواقف السيارات والمباني المنفصلة المؤمنة - أمرًا ضروريًا في حساب الكمية والوظائف الصحيحة للوصول أو نهاية الاتصال الداخلي للباب نقاط.

6. Does every door or gate require access control?

تأكد من أن جميع الأبواب والبوابات التي حددتها للتحكم في الوصول تحتاج حقًا إلى آلية قفل والتحكم في الوصول. ضع في اعتبارك ما إذا كان التحكم في الوصول ضروريًا أم لا لكل باب على حدة أم أن هناك مداخل / مخارج معينة حيث سيكون ذلك عائقًا؟

على سبيل المثال ، في مناطق حركة المرور المرتفعة ، من المرجح أن تؤدي حاجة كل مستخدم إلى التوقف مؤقتًا للتحقق من هويته إلى إبطاء تدفق الحركة ؛ هل يمكن تقليل عدد نقاط الوصول الخاضعة للرقابة في الطريق عبر المبنى؟

وهل الأبواب المقفلة الآمنة مطلوبة لجميع المناطق المحددة؟ هل المراحيض أو المخازن ، على سبيل المثال ، تتطلب التحكم في الوصول ؟.

7. Internal or external access points?

سيحدد موقع التحكم في الوصول أو أجهزة الاتصال الداخلي في الباب اختيار الأجهزة ، خاصة البيئات الخارجية أو القاسية. ستوفر العلامات التجارية الخاصة بالتحكم في الوصول والاتصال الداخلي للأبواب تصنيفات IP (حماية الدخول) و IK (حماية الصدمات) لمقاومة الطقس والتخريب والظروف القاسية) كلما ارتفع تصنيف IP و IK ، زاد مستوى الحماية.

بالإضافة إلى ذلك ، يجب أيضًا مراعاة التغيرات في الضوء ودرجة الحرارة ، لا سيما في المواقع الخارجية. ستحتوي العديد من أنظمة الاتصال الداخلي للأبواب على كاميرات مدمجة للمقيم أو مسؤول الأمن (على سبيل

المثال) للتعرف على الزوار بصريًا من موقع بعيد يمكن أن تؤثر مستويات الإضاءة المنخفضة في الليل والوهج (على سبيل المثال بسبب موقع الشمس) بشكل كبير على جودة الصورة. ومع ذلك ، ستتميز العديد من أجهزة الاتصال الداخلي عالية الجودة بكاميرات منخفضة الإضاءة أو أضواء الأشعة تحت الحمراء لإعطاء جودة صورة عالية الأداء في الليل.

نظرًا لوباء الفيروس التاجي ، أصبح اكتشاف درجة حرارة الجسم شائعًا بشكل متزايد في أجهزة التحكم في الوصول وأجهزة الاتصال الداخلي للمساعدة في تحديد الأعراض الشبيهة بالحمى وتقليل انتشار الفيروس بين الموظفين أو المقيمين. ومع ذلك ، يمكن أن تتأثر دقة أنظمة الكشف الحراري بشكل ملحوظ بدرجات الحرارة المحيطة بالخارج ، وبالتالي يوصى بها للموقع الداخلي للحصول على أفضل النتائج.

8. How to exit the building? (Egress options)

عند الدخول إلى المبنى ، ضع في اعتبارك شكل الخروج على كل باب أو نقطة وصول في معظم الحالات ، سيكون مستوى الأمان عند الخروج أقل من مستوى الأمان للوصول إلى المبنى.

لذلك قد يتطلب الخروج ببساطة خيار خروج يدوي وميكانيكي مثل مقبض الباب

قد يتطلب الأمر تفاعلًا من طرف ثانٍ مثل زر طلب الخروج أو زر الاتصال الداخلي ، أو تقديم المشورة لمكتب الأمن والذي يمكن من خلاله تنشيط فتح الباب عن بُعد.

يمكن أن تكون أزرار "طلب الخروج" الآلية "RTE" مادية (اضغط للخروج) أو لا تلامس في شكل "زر عدم اللمس" الذي يتميز بمستشعر الأشعة تحت الحمراء.

أو قد تكون هناك حاجة إلى أن تكون مستويات الأمان عالية للخروج كما هي للدخول إلى المبنى ، وفي هذه الحالة قد تكون هناك حاجة إلى جهاز تحكم في الوصول مكرر على جانبي الباب.

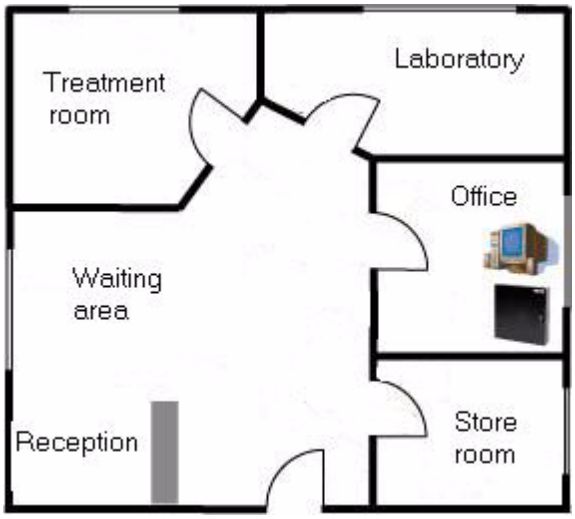
9. How will the access control points be powered? (PoE or 12v power supply?)

بالنسبة لنظام الوصول المتصل بـ IP نظام متصل عبر بروتوكول الإنترنت باستخدام البنية التحتية لشبكة LAN القياسية ، فإن معظم أجهزة التحكم في الوصول إلى IP والاتصال الداخلي بالباب وأجهزة الرد على الباب ستدعم PoE (Power-over-Ethernet)، وبالتالي باستخدام نفس كابل الفئة لكليهما اتصال البيانات والطاقة يتم توفير POEعادة من مفتاح شبكة مناسب.

يمكن أيضًا تشغيل معظم أجهزة الاتصال الداخلي والوصول إلى الباب عبر مصدر طاقة خارجي بجهد 12 فولت ، إما كبديل أو كمصدر احتياطي لـ PoE ، في حالة حدوث انقطاع في الشبكة لأي سبب من الأسباب.

مثال شامل عن نظام التحكم فى الدخول والخروج ACS

يوجد مخطط عام لمعمل طبى كالتالى نريد تركيب نظام ACA بكل مكوناته ؟



يجب أتباع الخطوات التاليه لتصميم هذا النظام

وليكن المنتج المستخدم المتفق عليه من المالك والإستشارى لنظام ACS هو BOSCH

الخطوات كالتالى :-

1-Materials Planning

Planning the doors
Low tier: Electrical components
- Card reader technologies
- Credential's technology
- Wiring for non-reader components

Middle tier: Access Controllers
High tier: Hosting the software for the final system

2-Installation with RS-485, AMC and Access PE

Mounting the access controller and associated hardware
Installing the wiring
- RS-485 bus topology for readers
- RS-485-star topology for all other components

Mounting the peripheral components
Connecting the peripheral components to the wiring
Protective diodes
Shielding data cables and avoiding ground loops
Connecting the AMC2 (Access Modular Controller)
Preparatory steps on PBC-60 power supply, AMC2 and computer
Connecting the peripheral components to the AMC2
Setting up the connection between AMC2 and the software

3-Installation with Wiegand and Access Easy Controller (AEC)

Mounting the access controller
Installing the wiring
Wiegand star topology for readers
Mounting the peripheral components
Connecting the peripheral components to the wiring
Protective diodes
Shielding data cables and avoiding ground loops
Connecting the AEC (Access Easy Controller)
Connecting the peripheral components to the AEC
Configuring the AEC hardware and network
Configuring the AEC software

سوف نقوم بشرح الخطوات السابقه

من المخطط السابق يتضح لنا التالى

1-غرفة انتظار مع منطقة استقبال ومدخل عام بين الساعة 9.00 و16.00

2- مخزن عام ، يفتح منطقة الاستقبال ، حيث توجد الضمادات والعكازات والمكتب يتم الاحتفاظ بالإمدادات ومواد المخزون غير الخطرة.

3- معمل ومخزن مؤمن يتم الاحتفاظ بالعقار والأدوات الحادة والمواد التي يحتمل أن تكون خطرة.

4- مكتب في منطقة الاستقبال ، حيث يوجد جهاز كمبيوتر وسجلات المرضى

5-غرفة treatment room

متطلبات التحكم في الدخول للغرف هي كما يلي:

Room	Access for whom	Access control requirements
1. Waiting Room with reception area	Anybody between 09:00 and 16:00	Door should be unlocked at 9:00, locked at 16:00 and requires a card outside of those hours.
2. General Storeroom	Doctor, lab technician, receptionist	Access control to prevent theft.
3. Laboratory	Doctor, lab technician	Strict access control to prevent theft and reduce danger to persons from hazardous materials and equipment.
4. Office	Doctor, receptionist	Strict access control to prevent misuse or theft of medical records and other sensitive data.
5. Treatment room	Anybody, anytime, as admitted by the doctor.	No access control as no valuables are present, and patients are always accompanied by the doctor.

1-Materials Planning

يحتوي القسم التالي على تحليل تقريبي للمتطلبات ، ويساعدك على اختيار الأجزاء المطلوبة بالكميات التي تحتاجها. من المفيد التفكير في ثلاثة مستويات:

المكونات الكهربائية ووحدة التحكم في الوصول والنظام المضيف.

هذه المستويات مغطاة بـمزيد من التفاصيل أدناه.

1-1 Planning the doors

لكل من الأبواب المذكورة في السابق نحتاج إلى تحديد الوظيفة المطلوبة بشكل عام:

1-أسهل حالة هي غرفة العلاج - لا تحتاج إلى قفل ولا تتطلب أي أجهزة تحكم في الوصول.

2-سيتم فتح المدخل الرئيسي للممارسة خلال ساعات العمل ، وسيتطلب بطاقة خارج تلك الساعات يجب أن يؤدي وصول أول موظف إلى قارئ البطاقات في الصباح إلى وضع الباب في وضع غير مقفل طوال ساعات العمل.

3-ستتطلب جميع الأبواب المزودة بقارئات البطاقات وحدة REX (طلب الخروج) والغرض منه هو توفير مخرج بدون إنذار دون الحاجة إلى بطاقة. تأتي إشارة REX عادةً من زر ضغط أو كاشف حركة داخل الغرفة ، أو مضمنة في الباب الخاص بالباب

4- هنا قررنا ربط REX بواسطة كاشف الحركة.

5-تتطلب جميع الأبواب التي يتم التحكم في الوصول إليها ملامسات مغناطيسية لإطلاق إنذار إذا تم فتح الباب بالقوة.

1-2 Low tier: Electrical components

من هذه الاعتبارات نقوم بإنشاء جدول للأبواب والمكونات الكهربائية لكل منها كالتالى

Room	Access control hardware
1. Waiting Room with reception area	Card Reader, e.g. Bosch Delta 1000 Electric door opener, e.g. Bosch Universal Electric Door Opener REX by motion detector, e.g. Bosch DS150i Magnetic contact, e.g. Bosch ISN-C devices
2. General Storeroom	Card reader Electric door opener REX by motion detector Magnetic contact
3. Laboratory	Card reader Electric door opener REX by motion detector Magnetic contact

Room	Access control hardware
4. Office	Card reader Electric door opener REX by motion detector Magnetic contact **Note**:This secured room, which already houses the computer, is the obvious place to put the access controller itself.
5. Treatment room	Nothing

1-2-1Card reader technologies

تختلف قارئات البطاقات في ناحيتين مهمتين: تردد المسح والبروتوكول.

تردد المسح:

125 كيلو هرتز مقابل 13.56 ميجا هرتز

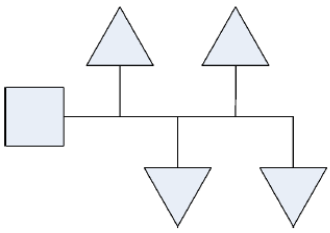
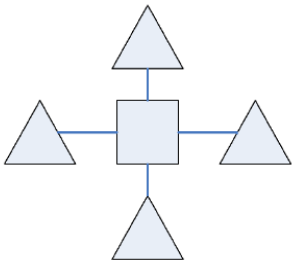
ترددات المسح الأكثر شيوعًا للقراء هي 125 كيلو هرتز و 13.56 ميجا هرتز ، و 125 كيلو هرتز هي تقنية مثبتة منتشرة في الولايات المتحدة الأمريكية وأوروبا الشرقية. تميل البطاقات والقراء إلى أن تكون أقل سعراً.

13.56ميجاهرتز هي تقنية أحدث وأكثر أمانًا منتشرة في أوروبا والشرق الأوسط وإفريقيا وبشكل متزايد في منطقة آسيا والمحيط الهادئ الدول.

RS-485مقابل Wiegand:

قرر مبكرًا ما إذا كنت ستستخدم تقنية Wiegand أو RS-485 للقراء ؛ لكل منها خاصته

المميزات والعيوب. يختلف الحد الأقصى لطول الكبل وطوبولوجيا الأسلاك ، كما يوضح الجدول التالي.

	RS-485 Readers	Wiegand Readers
Wiring topology	bus, (“chain”) 	star 
Maximum cable length	1200m	100m
Number of wires needed for the reader	4	10 (The slightly lower cost of Wiegand readers is offset by higher wiring costs and potential for wiring errors).

1-2-2 Credential's technology

حدد تقنية بيانات الاعتماد التي ترغب في استخدامها لقارئ ويجاند كالتالى

For Wiegand readers
The choice includes e.g. iCLASS (3.56MHz) and EM (125kHz) cards
For RS-485 readers
There is a wide choice: MIFARE, HITEC or LEGIC
These credentials types are available in different physical
Formats: Most common are the classic credit-card sized identity cards, and the smaller tokens and key fobs which usually carry no printed personal information.

1-2-3 Wiring for non-reader components

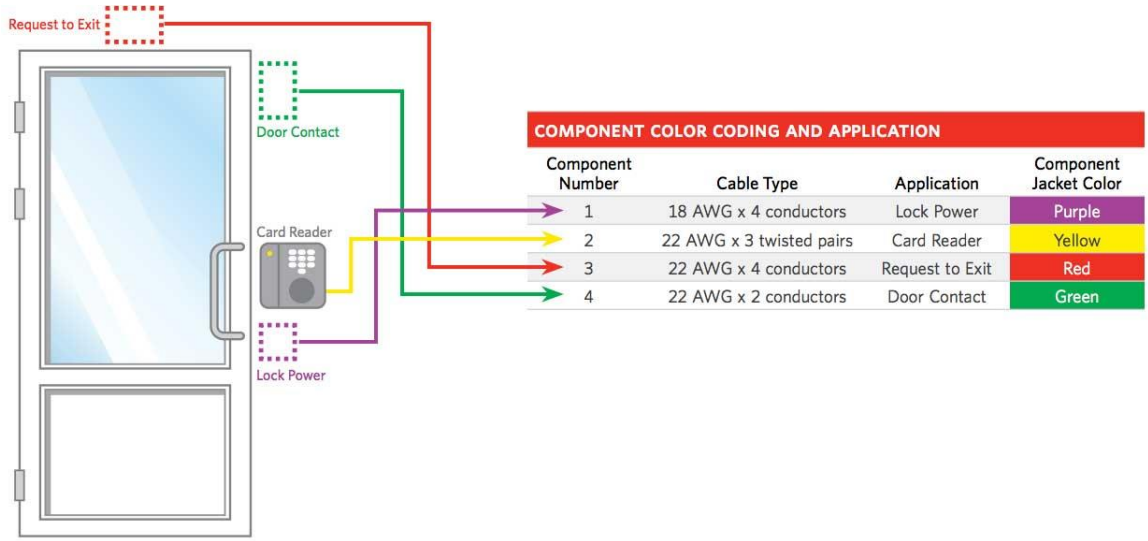
اعتمادًا على الشركة المصنعة والطراز ، سيتطلب كل مكون من هذه المكونات الكهربائية عددًا معينًا من الأسلاك للتحكم في تشغيله. يمكن العثور على القيم النموذجية لعدد الأسلاك لكل مكون في الجدول أدناه

Electrical component	Typical number of wires	Notes/explanation
Door opener	2	Power only
Magnetic contact	2	2 wires for power, but often extra wires for tamper detection
REX with push button	2	E.g. so that the receptionist can open the main entrance from her desk.
REX with motion detector	6	Highly variable depending on manufacturer: 2 wires for power, 2 to the magnetic contacts
Burglar alarm	4	(not used in this example)
Emergency exit	4	(not used in this example)

إذا كنت تعرف العدد الإجمالي للأسلاك التي يتطلبها الباب (بجميع مكوناته الكهربائية) ، وإذا كان لديك وصول إلى الموقع أثناء مرحلة البناء ، فيمكنك حينئذٍ التأثير على أنواع الكابلات الموضوعة على الأبواب.

تختلف الكابلات من حيث عدد وسماكة أسلاكها (تُعرف أيضًا باسم "core"). للمسافات التي تقل عن 25 مترًا ، كما في مثالنا ؛ سيكون سمك السلك AWG18أو 1 مم² كافياً. لمسافات أطول وتيارات أقوى ، ستكون هناك حاجة إلى أسلاك أكثر سمكًا. يتحمل AMC2 أقصى انخفاض 2 فولت من AMC إلى الأجهزة. يتم حساب انخفاض الجهد بواسطة كهربائيين وفقًا للصيغ القياسية.

يُنصح باستخدام جدول بيانات لتتبع مجموع وسمك الأسلاك المطلوبة لكل باب.



1-3 Middle tier: Access Controllers

وحدة التحكم في الوصول هي جهاز إلكتروني يتعامل مع إشارات الإدخال والإخراج من وإلى المكونات الطرفية) القارئات ، وحدات التحكم في الأبواب ، وحدات REX ، جهات الاتصال المغناطيسية ، إلخ .(إنها واجهة يتواصل من خلالها برنامج التحكم في الوصول مع المكونات ، لكن وحدة التحكم قادرة على التعامل مع بعض أحداث الإشارة من تلقاء نفسها إذا فقدت اتصالها بالبرنامج مؤقتًا.

ومن الأمثلة على ذلك وحدة التحكم المعيارية في الوصول AMC2 ووحدة التحكم في الوصول السهل من أنظمة الأمان من Bosch. Access Easy Controllerهو جهاز تحكم مع تطبيق للتحكم في الوصول المقيم AMC2 .هو برنامج / مضيف / قارئ محايد ويوفر متغيرات للتعامل مع قارئات-RS 485أو.Wiegand

1-4 High tier: Hosting the software for the final system

تقدم Bosch مجموعة واسعة من منتجات البرامج لتكوين أنظمة التحكم في الوصول ، اعتمادًا على حجم التثبيت. في مثالنا الصغير ، سيكون أحد منتجين مناسبًا

-Access Professional Edition: (Access PE)

هذا المنتج يثبت على جهاز كمبيوتر قياسي. يتحكم في الأبواب عبر وحدات الأجهزة تسمى وحدات التحكم المعيارية.(Access (E.G. AMC2 4R4

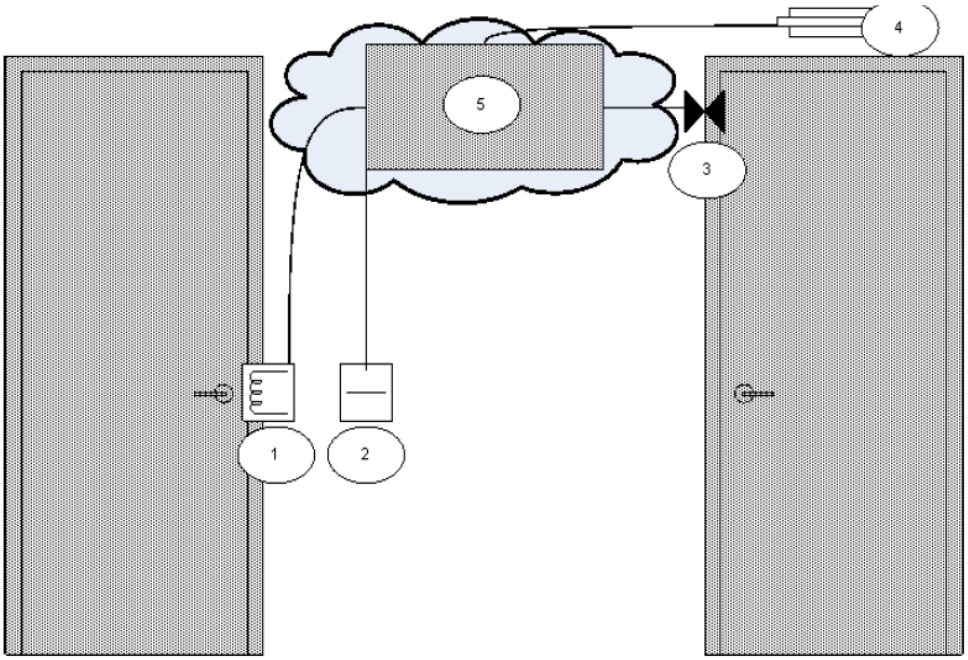
– **Access Easy Controller**: (AEC)

وجد برنامج التحكم في الوصول على وحدة تحكم الباب نفسها (أي يتم الجمع بين المستويات المتوسطة والعالية) ويتم تشغيله عبر الشبكة من جهاز كمبيوتر قياسي. يستخدم متصفح الويب لواجهة المستخدم الخاصة به.

2-Installation with RS-485, AMC and Access PE

كبرنامج Access Professional كجهاز تحكم في الوصول و AMC2 للقارئ ، و RS-485 يصف هذا الفصل تثبيت مثالنا لنظام التحكم في الوصول باستخدام اتصال تكوين. سنفترض أن جميع المكونات

1. Mounting the access controller and associated hardware.
2. Installing the wiring.
3. Mounting the peripheral components.
4. Connecting the peripheral components to the wiring.
5. Connecting the AMC to the wiring from the peripheral components.
6. Connecting the AMC to the computer and configuring the software.



Door from the outside	Same door from the inside
1: Door opener - 2 wires	3: Magnetic contact - 2 wires
2: Reader - 4 wires	4: REX with motion detector - 2 wires
5: Access controller. **NOTE: This should not be near the doors themselves, but should always be located in a secured area** (here represented by the cloud).	

2-1Connecting the AMC2 (Access Modular Controller)

The following is an illustration of a typical AMC2. Here the AMC2 4W.

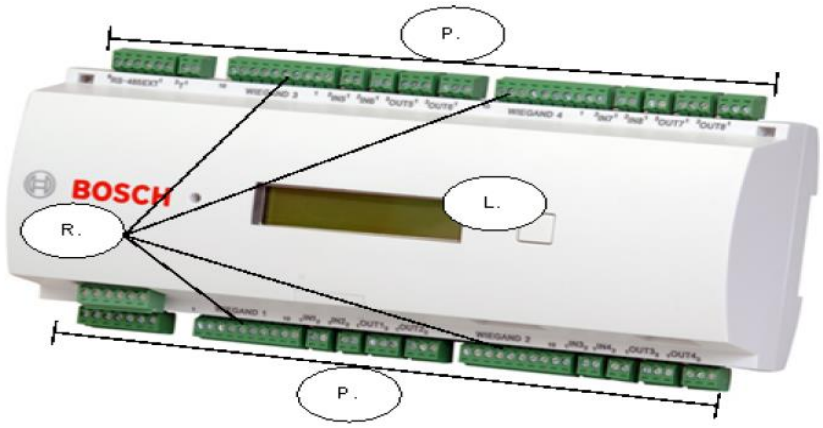


Figure 3.4 An AMC2 access controller

R: Reader connections	P: Pluggable screw terminals	L: LC Display

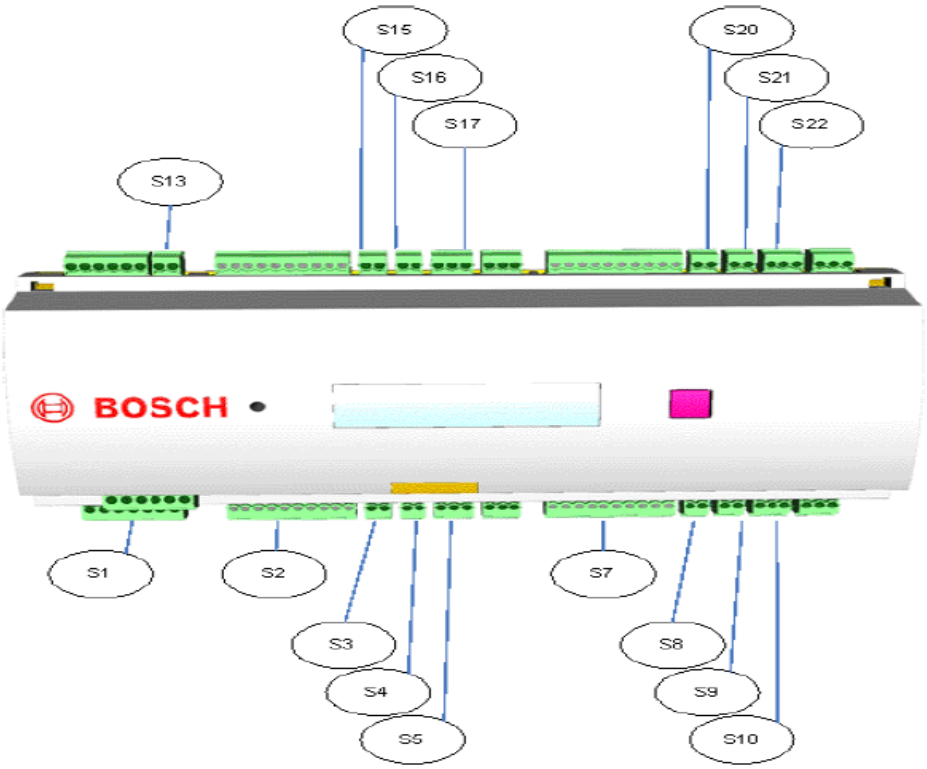
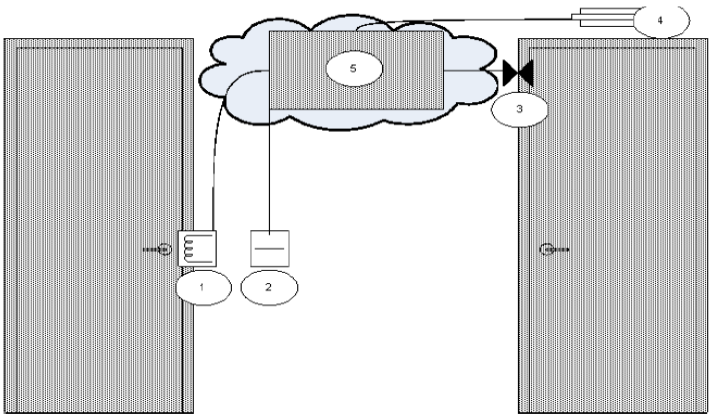


Figure 3.5 The AMC2 connections used in the 4-room surgery example.

Connector	used for...		Connector	used for...
S1 PSU	Power input		S10 Output 3	Storeroom Opener
S2 Reader port 1	Main Ent. and Lab card readers		S13 Tamper contact	(to be shorted as not in use)
S3 Input 1	Main Ent. REX		S15 Input 5	Lab. REX
S4 Input 2	Main Ent. MC		S16 Input 6	Lab. MC
S5 Output 1	Main Ent. Opener		S17 Output 5	Lab. Opener
S7 Reader port 2	Store and Office card readers		S20 Input 7	Office REX
S8 Input 3	Storeroom REX		S21 Input 8	Office MC
S9 Input 4	Storeroom MC		S22 Output 7	Office Opener

3-Installation with Wiegand and Access Easy Controller(AEC)

This chapter describes the installation of our example access control system using Wiegand communication to the readers. AEC is an access control system that uses Wiegand communication.



Door from the outside	Same door from the inside
1: Door opener - 2 wires	3: Magnetic contact - 2 wires
2: Reader - 4 wires	4: REX with motion detector - 2 wires
5: Access controller. **NOTE: This should not be near the doors themselves, but should always be located in a secured area** (here represented by the cloud).	

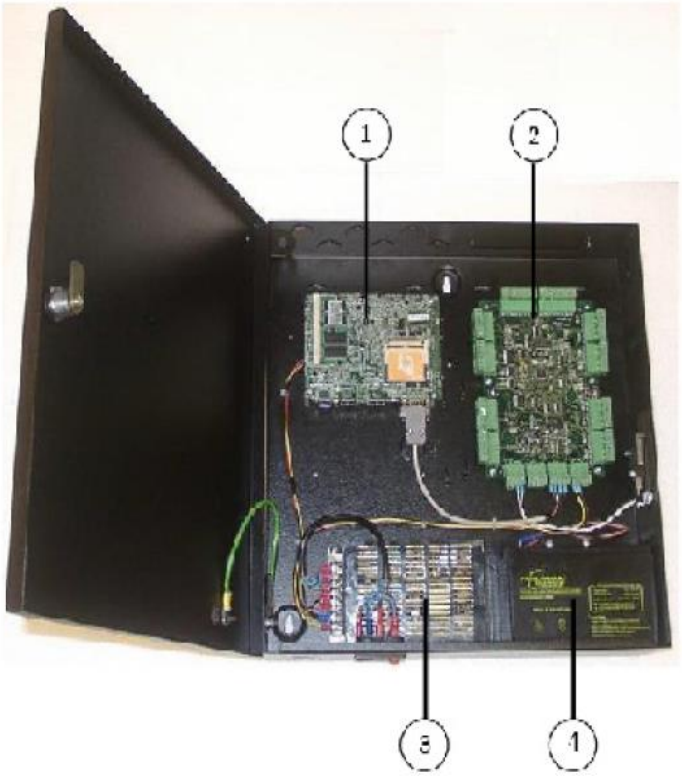
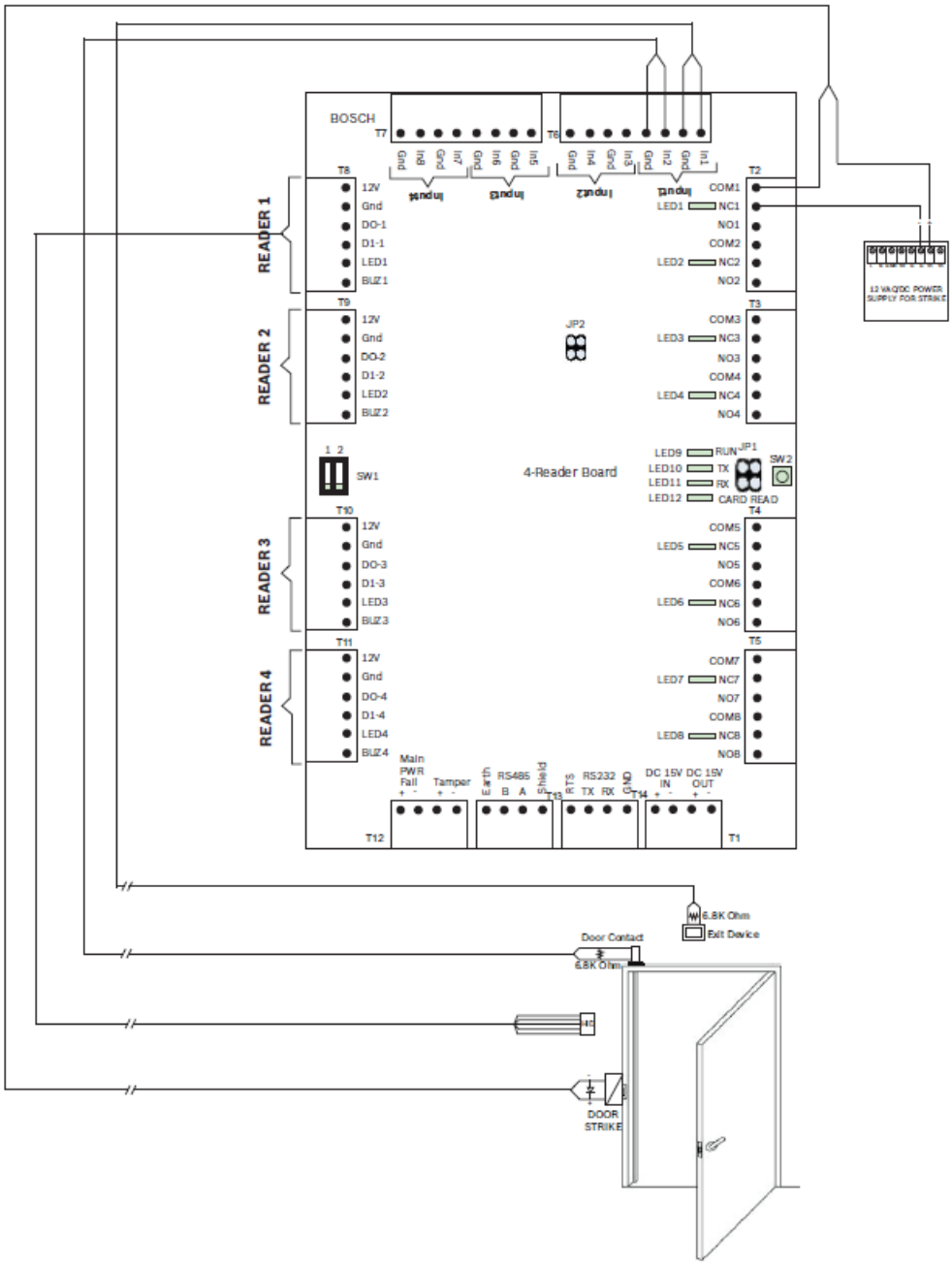


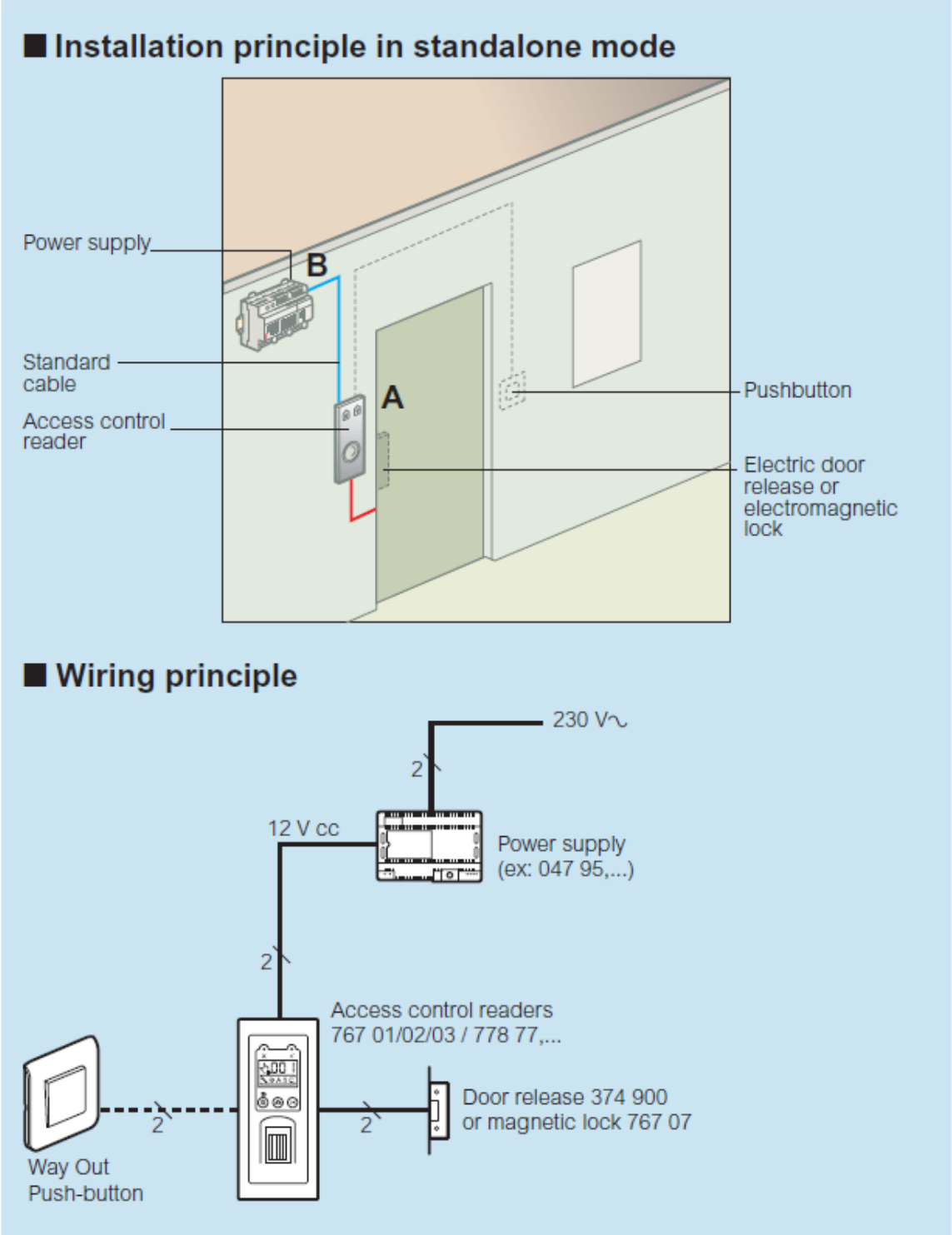
Figure 4.4 An AEC2.1 access controller

1: CPU Board	2: 4 Reader Board	3: Power Supply Unit	4: Backup Battery
Note: AEC2.1 does not come with the 12 VDC standby battery.			

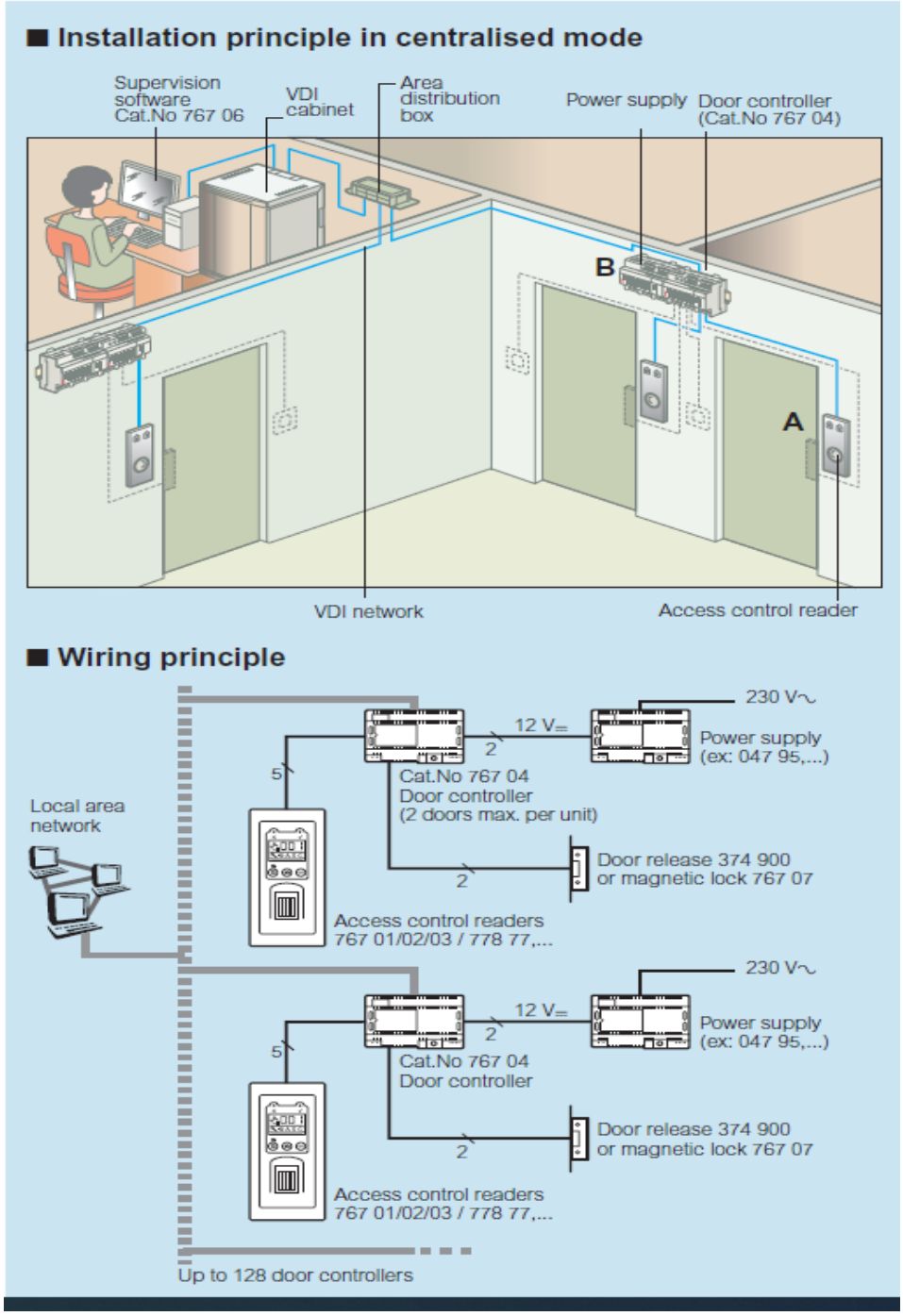

BOSCH
T7
T6
T8
T9
T10
T11
T2
T3
T4
T5
T12
T1
READER 1
READER 2
READER 3
READER 4
12V
Gnd
DO-1
D1-1
LED1
BUZ1
DO-2
D1-2
LED2
BUZ2
DO-3
D1-3
LED3
BUZ3
DO-4
D1-4
LED4
BUZ4
COM1
NC1
NO1
COM2
NC2
NO2
COM3
NC3
NO3
COM4
NC4
NO4
COM5
NC5
NO5
COM6
NC6
NO6
COM7
NC7
NO7
COM8
NC8
NO8
LED9
LED10
LED11
LED12
RUN
TX
RX
CARD READ
JP1
JP2
SW1
SW2
4-Reader Board
Main PWR Fail
Tamper
Earth
RS485
B
A
Shield
RS232
RTS
TX
RX
GND
DC 15V IN
DC 15V OUT
12 VAC/DC POWER SUPPLY FOR STRIKE
6.8K Ohm
Exit Device
Door Contact
6.8K Ohm
DOOR STRIKE

ماذا لو قمنا بإستخدام **Legrand Brand** لنظام **ACA** فى المثال السابق

1- غرفة المكتب فقط يمكن استخدام التالى

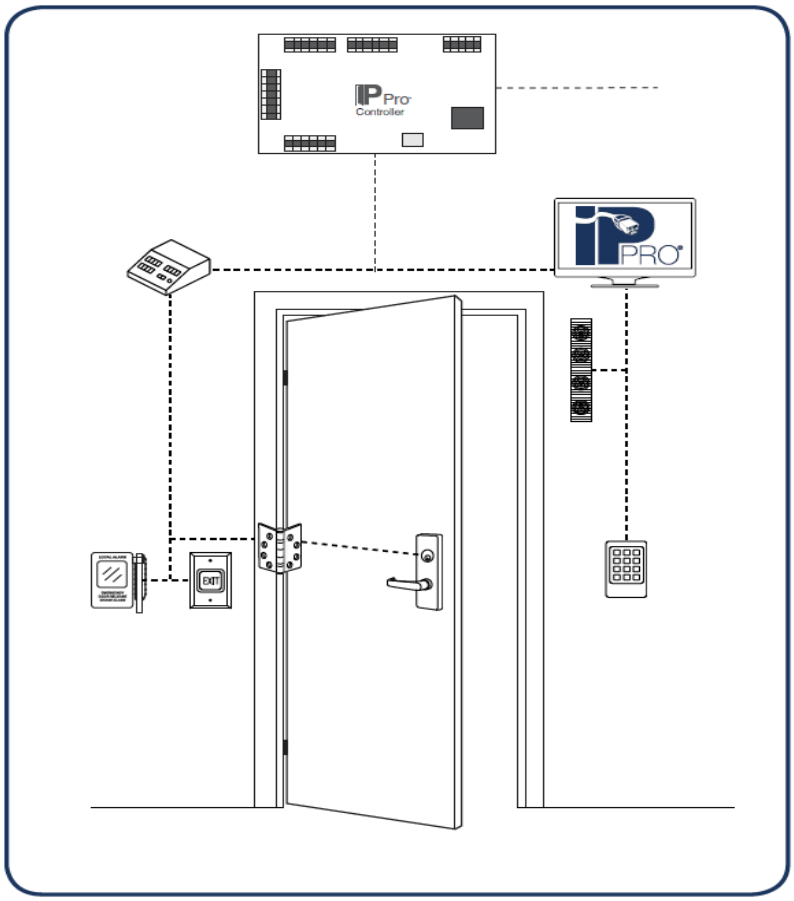


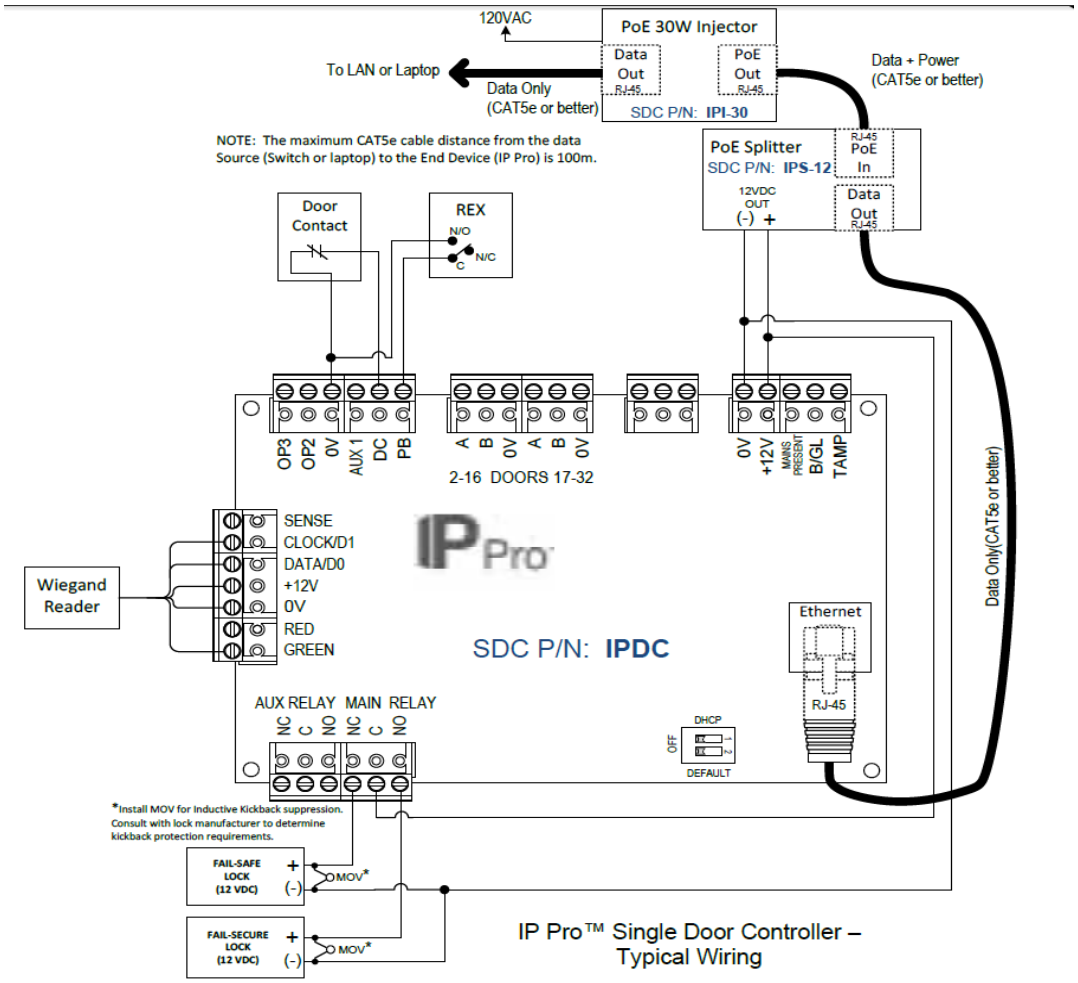
2-غرفة المكتب والمعمل والمستودع يمكن استخدام التالى



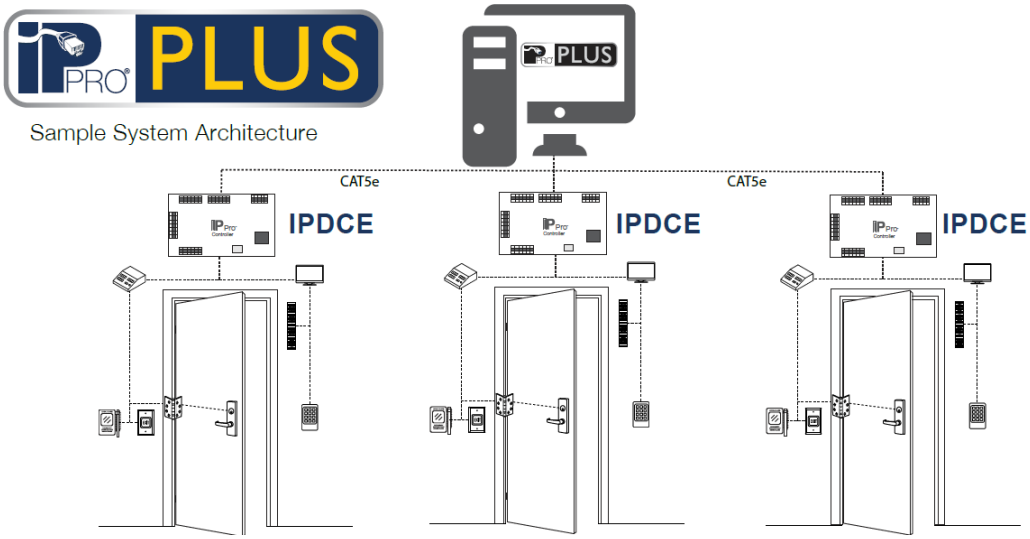
ماذا لو قمنا بإستخدام SDC Brand لنظام ACA فى المثال السابق

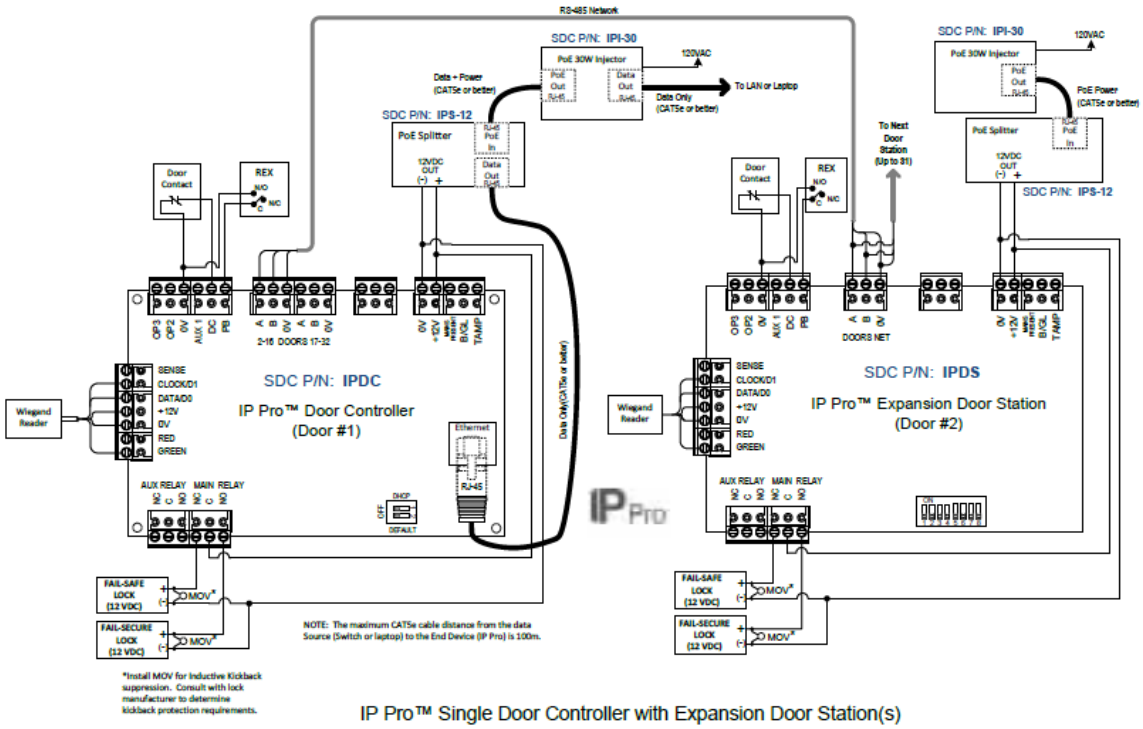
1- غرفة المكتب فقط يمكن استخدام التالى





2-غرفة المكتب والمعمل والمستودع يمكن استخدام التالى





IP Pro™ Single Door Controller with Expansion Door Station(s) – Typical Wiring

جدول كميات لنظام التحكم فى الدخول والخروج

				Supply		Installation , Testing & Comissioning	
S. No.	DESCRIPTION	Unit	Qty	Rate	Amount	Rate	Amount
	ACCESS CONTROL SYSTEM						
I	Access Intelligent Controllers (AIC)						
1	Supply, installation, testing and commissioning of Access Intelligent Controller support 4 standard Weigand Interface or up to 8 serial interface on RS 485 bus technology , 8 Input & 8 Output port as per the specification with enclosure , power supply ,& Maintenance free Batteries with 30 minutes back up . The controller should be minimum 32 bit embedded microprocessor chip and on board TCP /IP as per the Specification..The Controller Should have minimum of 2 GB of flash Memory , can store 2 Lakh Card holder Access profile & 4 lakhs transaction in offline mode. The Controller should have a 16-characters liquid crystal display (LCD), and a button provided for selective display to show all its network parameters and actual status like - IP address of the controller; MAC address of the controller as per the specificationController Should be UL 294, FCC, CE,EN as per the specification	Nos	1				
II	Readers , Cards & Tags						
1	Supply, installation, testing and commissioningBiometric Finger with Smart card(Read range Up to 9 cm) & PIN Pad Reader at Every Entry Access Doors as per the Specification	Nos	2				
2	Supply, installation, testing and commissioning Smart card(Read range Up to 4 cm) for entry of access door	Nos	2				
2	Supply, installation, testing and commissioning of contactless 16K /16Application Area Smart Card suitable for Boom Barrier , Tripod ,Flap Barrier , Biometric Reader & Access Door as per the specification	Nos	200				
III	Access Control & Attendance Software						
1	Supply, installation, testing and commissioning Access Control System Server Software consisting of Access Control system , Visitor management , 4 client License , with Attendance module as per specification	No	1				
IV	Misc Other Items for Access Control System :						
1	Single Leaf Electro Magnetic Lock of Suitable Capacity(Min 600 lbs) as per specification	Nos	2				
2	Supply, Installation, testing & commissioning of Exit push button as per the specification	Nos	2				
3	Supply and Laying of of 8 Core x 0.5 sq mm multi strand, copper, unarmoured sheilded Cable as per specification (between the every card readers & the access controllers)	Mtr	As per onsite requirement				
4	Suply and laying of PVC conduit	Mtr	As per onsite requirement				
5	Supply and Laying of 2 Core x 1.5 Sq mm, multi strand, copper, shelided, un armoured cable as per specification(between the controller and EM Lock/ door sensor/Request to exit button and)	Mtr	As per onsite requirement				

أشهر الماركات العالمية لنظام التحكم فى الدخول والخروج

BEST FOR SINGLE USERS

BEST FOR LARGE TEAMS

BEST IDENTITY AUTHENTICATION ACCESS CONTROL

BEST FOR WIRELESS ACCESS CONTROL