

سامانه پیشرفته کنترل دسترسی تیزبین

نسخه ۱/۵

زمستان ۱۴۰۳

- * سامانه متمرکز و یکپارچه امنیت و کنترل دسترسی ویژه معادن
- * پایش عملکرد تاسیسات حیاتی سایت جهت پیشگیری از حملات امنیتی
- * پروتکل تشخیص چهره بومی + اثر انگشت یکپارچه + تشخیص پلاک خودروها
- * هوش مصنوعی در هشدار تردها یا توقف های مشکوک و ورود خروج غیر مجاز افراد
- * هوش مصنوعی در مهار حملات سایبری به تاسیسات به کمک سنسورها و فایروال صنعتی
- * زمانبندیهای منعطف برای دسترسی پرسنل، مهمانان و سایر با شیفت های کاری منطبق با معادن
- * دستگیره های هوشمند و یکپارچه پنل ها و کابینت های حساس سایت مجهز به اثر انگشت و دوربین
- * پشتیبانی از سنسورهای ایمنی و امنیتی با قابلیت ارتباط با دوربین ها ، تلفن داخلی و بیسیم داخلی حراست
- * کامل ترین و پیشرفته ترین سامانه مدیریتی نیروهای ویژه حفاظتی و حراستی مبتنی بر تکنولوژی بوش آلمان

مقدمه :

علیرغم اینکه صنعت استخراج از معادن تا حد زیادی زیرساخت های یک کشور را پشتیبانی میکنند، این صنعت با تهدیداتی مواجه است که نیازمند امنیت و راهکارهای امنیتی همه جانبه میباشد. امنیت معادن با سه چالش روبرو است: شرایط دشوار، مناطق بزرگ و هزینه های بالای نصب راهکارهای جامع. یکی از بزرگترین مسائل امنیتی در معادن موضوع تجاوز به فضاهای پیرامونی، استخراج غیرقانونی از معادن و سرقت است. تامین امنیت تجهیزات و اطمینان حاصل نمودن از امنیت کارکنان نیز از جمله مسائل حائز اهمیت هستند.

در مقایسه با سیستم های امنیتی بکار گرفته شده در فضاهای تجاری، سیستم های امنیتی بکار گرفته شده در معادن باید قادر به ارائه ی کارکرد در فضاهای دشوار باشند. در اعماق معادن، دمای هوا میتواند به بیشتر از ۴۵ درجه سلسیوس برسد و این فضاها دائما مرطوب و شرعی هستند که این خود باعث ایجاد محدودیت در تکنولوژی مورد استفاده میشود.

راهکارهای بکار گرفته شده باید خاص هر معدن طراحی شوند. پروفایل امنیتی یک معدن معمولا از بیرون آن به وجود می آید و امنیت فضاهای پیرامونی را به نخستین دغدغه تبدیل میسازد. با این حال، علیرغم اهمیت حصارکشی فضاهای پیرامونی، اغلب به خاطر چشم انداز بزرگ و دشوار محل قرارگیری معادن، این کار بی فایده است. سیستم های امنیتی میتوانند مقدار استخراج غیرقانونی از معادن را به حداقل برسانند، اما نمی توانند از وقوع آن جلوگیری کنند. کنترل شدیدتر از طریق سیستم های امنیتی یکپارچه سازی شده میتواند خطر استخراج غیرقانونی از معادن را به حداقل برساند. طبق آمار تا حدود ۳۰ درصد از طلای استخراج شده از معادن آفریقای جنوبی، پیش از آنکه بتوانند باعث ایجاد سود برای خود مراکز استخراج از معادن شوند، به سرقت میروند. برای جلوگیری از سرقت، بیشتر توجهات روی سیستم های کنترل دسترسی و سیستم های تشخیص ورود غیرمجاز متمرکز است؛ ورود غیر مجاز به محل ذخیره سازی مواد استخراج شده، محل پردازش آنها و جاهایی که ماشین آلات سنگین حاضر هستند. سیستم های کنترل دسترسی به همراه بیومتریک ها، درب های چرخنده، دیتکتورهای تشخیص فلزات، سیستم های مدیریت زمان حضور و غیاب و بررسی پیش زمینه همگی برای به حداقل رساندن سرقت بکار گرفته میشوند.

تامین امنیت و ایمنی کارکنان، برای فضاهای کاری دشوار در معادن یک دغدغه است. سیستم های کنترل دسترسی، سیستم های نظارتی، سنسورهای تخصصی با نرم افزارهای حرفه ای و قوانین مدیریتی متضمن امنیت و ایمنی کارکنان هستند. تایید پرسنل مجاز، نخستین گام برای تامین امنیت و ایمنی کارکنان است. راهکارهای ترکیبی و یکپارچه، فرآیندهای استخراج از معادن را خودکار میسازند، حجم کار موردنیاز را کاهش میدهند و در عین حال همان سطح از امنیت را حفظ میکنند. تلفیق و یکپارچه سازی بیشتر به معنای کارآمدی عملیاتی بیشتر و صرفه جویی درازمدت بیشتر برای مشتریان است. نرم افزار امنیتی تلفیق شده با نرم افزار برنامه ریزی منابع انسانی یک روند مطلوب است.

حفاظت فیزیکی از مراکز حساس و حیاتی نظامی، انتظامی، نیروگاه ها، پالایشگاه ها، معادن و سایر سایت های مهم ملی کشور در کنار نیروهای حفاظتی و حراستی کارکشته و باتجربه به سامانه پیشرفته و کارآمد و بروز نیازمند است. با توجه به شرایط حساس کشورمان و شیوه های نفوذ و دسترسی های غیر مجاز و نامتعارف و گاها استفاده از افراد نفوذی، دیگر روش های سنتی حفاظت فیزیکی قابل اطمینان نیستند و این مراکز در برابر مخاطرات جدی گوناگون ایمنی و امنیتی قرار دارند.

مخاطرات ایمنی شامل حوادث عمدی یا غیر عمدی ایمنی مانند آتش سوزی ، نشت دود و گاز ، خطرات برقی ، انفجار ، عملکرد معیوب تاسیسات و تجهیزات و ماشین آلات و مانند آن می باشد.

مخاطرات امنیتی مانند ورود افراد غیر مجاز به سایت یا تاسیسات ممنوعه داخلی ، سرقت یا تخریب سیستم ها و تاسیسات ، توقف مشکوک افراد در برابر تاسیسات حساس داخلی ، خرابکاری در کابینت های حساس و زیرساخت های سایت ، آسیب های شبکه ای ، الکترونیکی و نهایتا حملات سایبری در حوزه IT (شامل شبکه و سیستم های رایانه ای) و OT (شامل تاسیسات و سیستم های کنترل صنعتی مانند PLC ها و سایر تجهیزات تخصصی) می باشد.

این حوادث و مخاطرات غالباً برنامه ریزی شده و توسط افراد حرفه ای و آموزش دیده انجام می شوند. امروزه با اطمینان می توان گفت کنترل این مخاطرات بدون استفاده از سامانه های هوشمند حفاظتی غیر ممکن است. این سامانه ها امروزه مانند چشم ها و گوشهای نیروهای امنیتی ، حراستی و حفاظتی در مانیتورینگ و کنترل مراکز ، فضا ها و سایت های بزرگ عمل می کنند.

سامانه تیزبین یک سیستم حفاظت فیزیکی هوشمند یکپارچه و بومی است که کلیه مخاطرات ایمنی و امنیتی سایت های بزرگ را پوشش می دهد و حاصل سالها تجربه متخصصین داخلی در راه اندازی و پشتیبانی تاسیسات حساس ایمنی و امنیتی در سایتهای بزرگ نیروگاهی ، پالایشگاهی ، سایتی ، سازمانی و سالها تجربه در حوزه امنیت فیزیکی و سایبری و نیز تجارب کار با سیستم های موفق جهانی حفاظت فیزیکی مانند بوش آلمان و CDVI فرانسه می باشد.

مخاطرات استفاده از سامانه های غیر بومی :

- سامانه های حیاتی ما را به خود وابسته می کنند.
- احتمال افشای داده ها و نقشه ها از آنها به بیرون از کشور وجود دارد.
- با توجه به تحریم های گسترده روی کشورمان ، عاری از هر گونه پشتیبانی فنی و یا تامین لوازم جانبی هستند.
- با نیازهای داخلی هماهنگی ندارند و نمی توانند خواسته های حفاظتی و حراستی داخلی ما را کاملاً پوشش دهند.
- با توجه به شرایط حساس کشورمان در این سالها کاملاً غیر قابل اعتماد و قابل نفوذ می باشند.

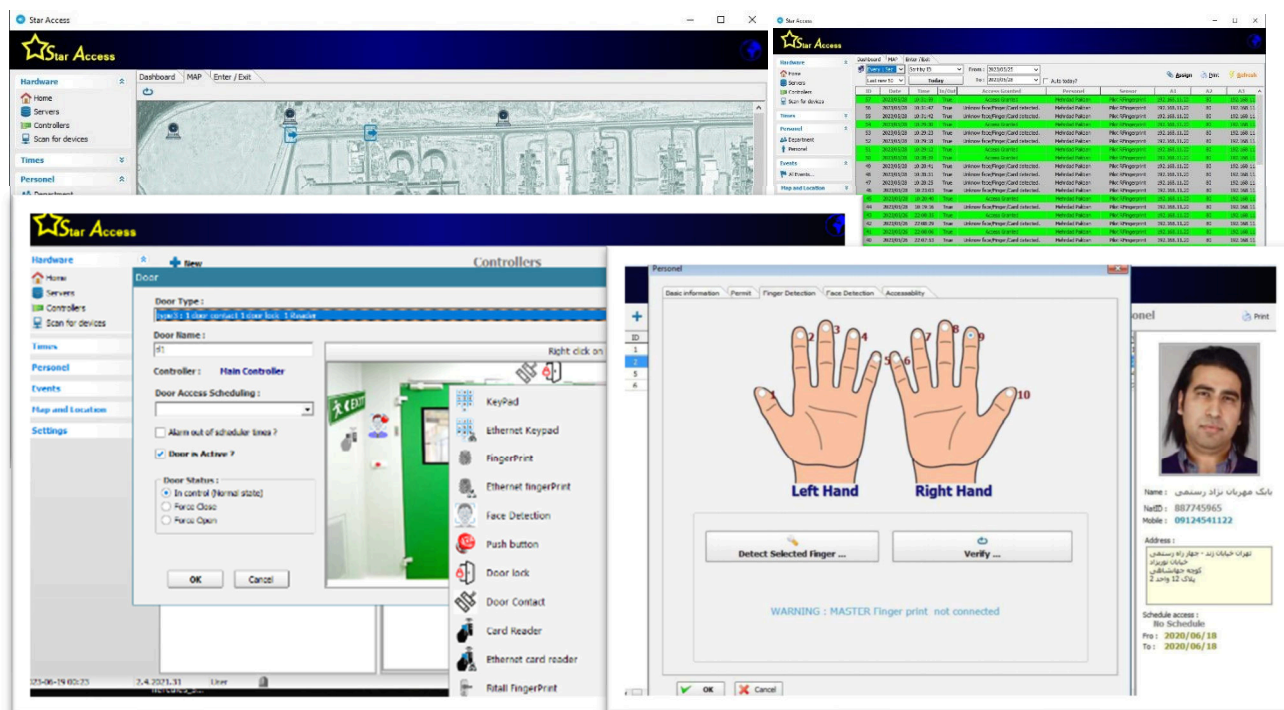
مراکز حساس و سایتهای حیاتی میهن عزیزمان طی سالهای اخیر با مخاطرات ایمنی ، امنیتی و حملات سایبری مواجه شده اند

در چنین شرایطی نیروهای متعهد تیم راد متولی سامانه یکپارچه تیزبین وظیفه میهنی خود دانستند تا از توان و دانش و تجربه فنی خود برای ایجاد ایمنی و امنیت مظاعف در سایتهای کشور عزیزمان استفاده کنند و در کنار نیروهای پرتلاش حفاظتی و حراستی در سلامت و بهره وری مراکز حیاتی ایران بزرگ نقشی کوچک داشته باشند.

سامانه یکپارچه تیزبین :

این سامانه نرم افزاری سخت افزاری به کمک ساختار یکپارچه خود و استفاده از بیومتریک های صنعتی و استاندارد و دوربین های ثابت و متحرک ، مادون قرمز و حرارتی جهت مدیریت و مانیتورینگ تردد پرسنل رسمی ، کادر ، مهمانان یا پیمانکاران معدن و گزارش در لحظه آنها است. در این خصوص از بیومتریک های استاندارد جهانی و سنسور های پیشرفته اثر انگشت شبکه ای تیزبین ، تشخیص چهره تیزبین ، پلاک خوان ، کارت خوان و RFID ، NFC ، کیبورد هوشمند بومی تیزکد ، دستگیره های صنعتی و هوشمند تولید گروه امنیتی راد سری ریتال و انواع گیت های تردد نفررو و ماشین رو ، سنسورهای مختلف تردد و تایید هویت و خروجی فرمان به قفل های مغناطیسی ، آژیر ، فلاشر و تجهیزات ایمن دیگر به مدد کنترلر بومی توانمند و صنعتی خود به صورت آنلاین و آفلاین کاملاً پشتیبانی می شود. داده های این سامانه کاملاً رمزنگاری شده هستند و انتخاب پروتکل و کلید ها توسط مسئولین امنیت قابل تعریف یا تغییر می باشند تا نفوذ به این سامانه را بسیار پیچیده و سخت کنند.

- سامانه تیزبین کاملاً داخل کشور تهیه ، تولید و پشتیبانی می شود.
 - تجهیزات تخصصی سامانه اعم از کنترلر صنعتی ، تشخیص چهره ، اثر انگشت ، دستگیره های هوشمند ، کیبورد تیزکد و غیره توسط تیم فنی و مهندسی تیزبین با کیفیت صنعتی و توسط مجموعه راد تولید و پشتیبانی می شوند.
- سامانه تیزبین قابلیت مانیتور کردن وضعیت اتصال کلیه دستگاه ها ، موقعیت لحظه ای و مسیر تردد افراد و اعلام وضعیت سنسورها مثلاً باز یا بسته بودن درب ها و کابینت ها به صورت شبکه یکپارچه را دارا می باشد .

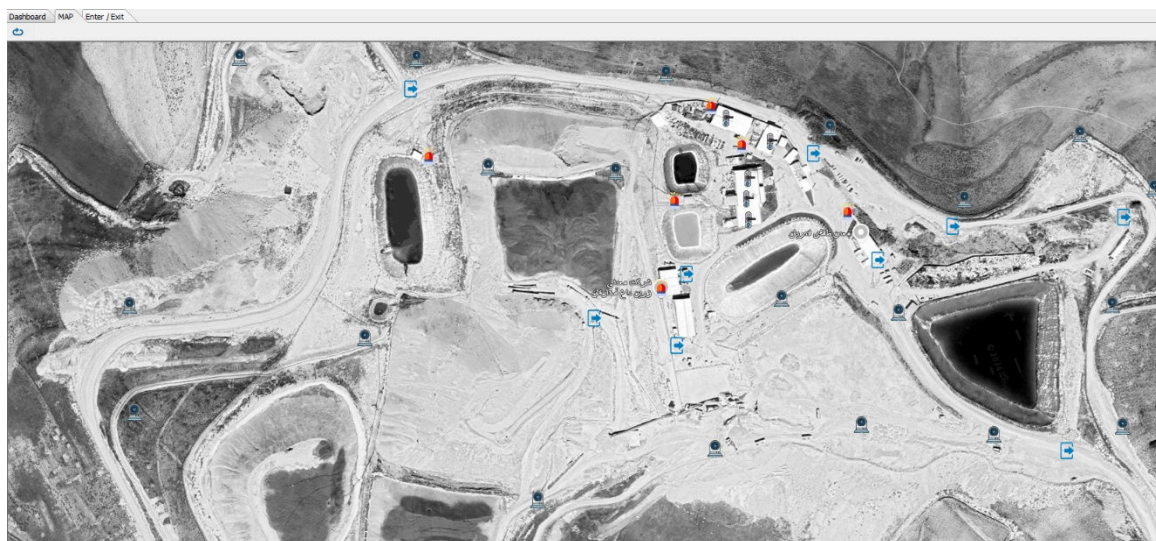


پشتیبانی از طیف وسیعی از سنسورها و سایر تجهیزات اکسس کنترل

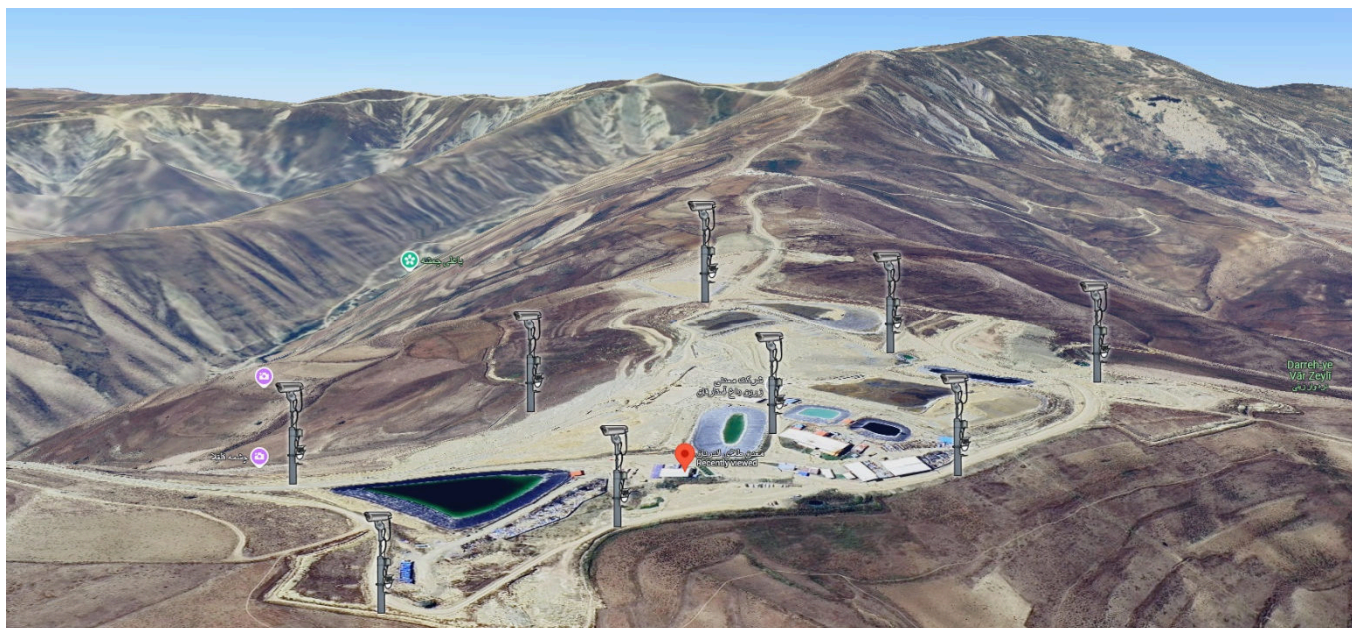
تعریف اثر انگشت و چهره برای نفرات

نقشه هوایی

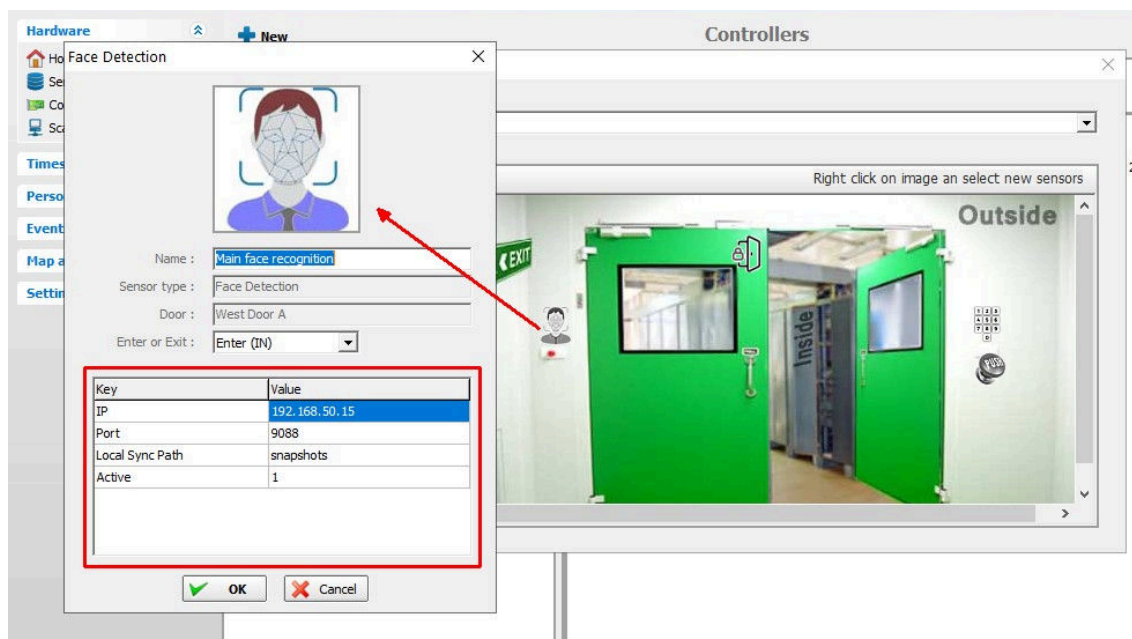
قابلیت تعریف نقشه های گوناگون و جانمایی کنترلر ها ، سنسورها ، آلازم ها ، دوربین ها و پنجره های بازپخش ویدئو ، درب ها ، دستگیره های هوشمند و سایر تجهیزات فرمان پذیر یا گزارش دهنده اکسس کنترل روی آنها با امکان زون بندی نقشه و پیاده سازی گرافیکی همه اینها جهت نمایش روی مانیتورهای بزرگ برای پرسنل حفاظتی ، حراستی و مدیران معدن به طور مجزا و بر اساس سطوح دسترسی تعیین شده .



مانیتورینگ هوایی زنده تیزبین: نمونه ای از نقشه هوایی یک معدن ، سنسورها ، آلازم ها و دوربین های چیده شده روی آن جهت مانیتورهای بزرگ اتاق حراست

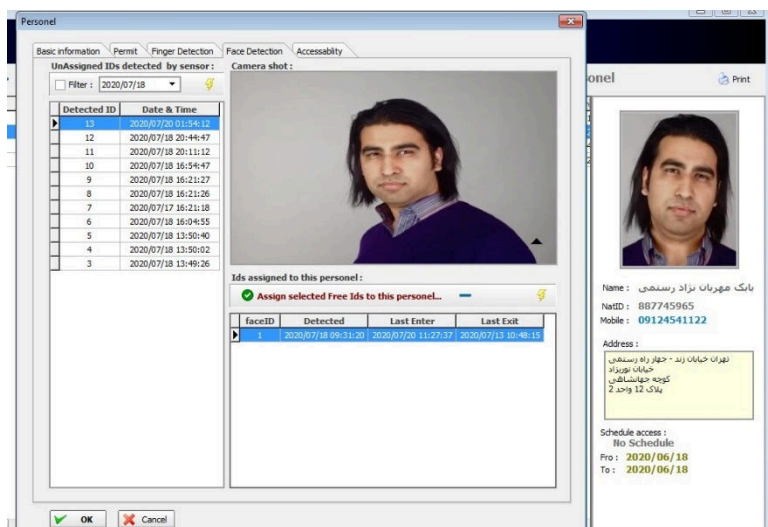


پنجره نمای سه بعدی جاگذاری دوربین ها و سایر سنسورها در نرم افزار تیزبین : نمای سه بعدی کمک می کند کار طراحی و چینش سنسورهای پیرامونی و دوربینها دقیق و بر اساس شرایط جغرافیایی واقعی انجام بگیرد.



نرم افزار تیزبین : تعریف و تنظیم کامل ورودی و خروجی ها

تنظیمات چهره ، اثر انگشت ، NFC ، کارت و...



تشخیص چهره منحصر به فرد استاراکس

برای هر نفر به طور مجزا می توان چهره ، اثر انگشت ، سنسور امن NFC ، رمز های مورد تایید سیستم تیزکد که باید به ترتیب خاصی وارد شوند و کارت مغناطیسی یا چپ دار شناسایی وی را ثبت و وارد نمود. این سیستم از کلیه موارد شخصی فوق الگو های گذشته پیشرفته ای تولید می کند و می توان این الگو ها را به صورت هوشمندانه با هم ترکیب نمود به این ترتیب شناسه تایید شناسایی یک فرد می تواند ترکیبی از آن ها باشد. برای مثال تایید یک فرد می تواند ترکیبی از چهره ، اثر انگشت ، NFC و یا تیزکد وی باشد. همچنین می توان برای برخی ورودی

های کم اهمیت تر یکی و برای برخی ورودی های با اهمیت بالا بیشتر از یکی از الگو ها را در مورد این فرد ترکیب نمود. برای مثال ورود به سایت تنها با چهره (یا اثر انگشت) ولی ورود به یک اتاق یا محدوده با چهره + اثر انگشت + تیزکد باشد . هر چه اهمیت محل ورود بیشتر باشد ترکیب پیشرفته تری از الگو ها توصیه می شود.



استفاده از NFC



کارت های چپ دار، مغناطیسی و تماسی



کیبورد هوشمند تیزکد ساخت تیزبین



نرم افزار تیزبین دارای قابلیت چند مانیتوره است. بنابراین همزمان با اینکه می توانید نقشه هوایی را داشته باشید ، قادرید لاگ تردها ، اخطاهای امنیتی ، دوربین ها و ... را بررسی کنید و یا به داشبورد مدیریت دسترسی داشته باشید. برای هر کاربر می توان سطوح دسترسی گوناگون داشت.

هوش مصنوعی Ai

هوش مصنوعی در بررسی تردهای مشکوک نفرات:

سرور تیزبین قادر است با توجه به امکانات پایشی که دارد (مانند دوربین ها ، سیستم تشخیص چهره و ...) به پایش تردد های مشکوک در سایت بپردازد. این سیستم نسبت به مواردی مانند کلاه نقاب دار ، عینک دودی ، ماسک ، سر همواره پایین و عدم نگاه درست به دوربین های تشخیص چهره موازی ، حرکت های نامتعارف به جلو و بازگشت به عقب در کوتاه مدت ، توقف مدت دار در محدوده های حساس و تعیین شده مانند جلوی تابلوها و تاسیسات مهم (که قبلا محدوده آنها انتخاب شده است) و موارد مشابه ، حساسیت نشان می دهد و مسیر تردد این افراد را بیشتر مورد بررسی قرار می دهد. چنانچه مواردی توسط هوش مصنوعی مشکوک باشد آنها را به مسئولین حراستی و حفاظتی با آلام و هشدار و میزان اهمیت گزارش می دهد و برشهای ویدیویی از حرکتهای مشکوک را برای ویدیوچک آنها به طور خودکار تهیه می نماید. این هوش مصنوعی به طور خودکار موارد مشکوک را شناسایی می کند و حالت های جدید رفتارهای مشکوک را یاد می گیرد .

هوش مصنوعی در بررسی وضعیت تجهیزات:



تصویری از تاسیسات حساس صنعتی و برقی معدن

سرور سامانه تیزبین به کمک کنترلرهای قدرتمند خود و سنسورهای تخصصی قادر است کلیه داده های مربوط به تاسیسات حساس سایت را دریافت و آنها را تحلیل کند. سپس Ai (هوش مصنوعی) داخلی سرور از داده های تاسیسات حساس سایت الگوهایی پیشرفته تولید می کند که بعدا چنانچه با مغایرتی مواجه شد گزارش می دهد، این تغییرات البته ممکن است واقعا توسط پرسنل فنی و مهندسی وارد شده باشند ولی سامانه تیزبین تایید تغییرات را از سرپرست شیفت دریافت و ثبت می کند. بنابر این مشخص می شود آیا این تغییرات مجاز بوده و در صورت مجاز بودن ، توسط کدام پرسنل در شیفت کدام سرپرست انجام گرفته است.

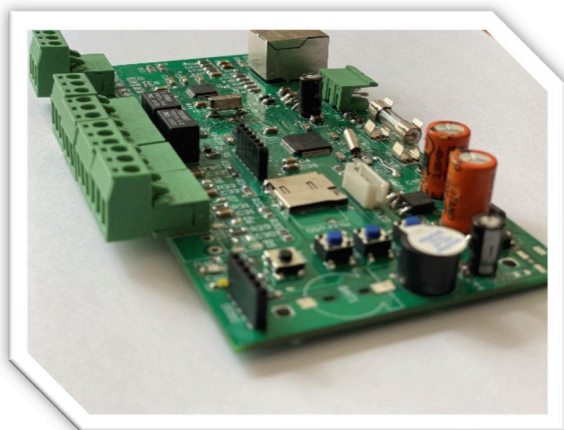
سامانه تیزبین به کمک این قابلیت ها قادر است جلوی آسیب های عمدی به سیستم ها و تجهیزات کلیدی مانند PLC ها ،

کنترلرهای HVAC ، موتورها و ژنراتورها و تاسیسات حیاتی و حساس سایت را بگیرد.



نمونه هایی از فایروال های صنعتی که تیزبین قادر به ارتباط با آنهاست

فایروال بومی تیزبین



سخت افزار کنترلر سامانه تیزبین

با توجه به حساسیت بالای کنترلر سخت افزاری در کنترل دقیق ورودی و خروجی ها و حفظ امنیت بالای آن در ارتباط با سامانه تیزبین ، سخت افزار مربوطه کاملا در داخل و توسط تیم فنی تیزبین طراحی و تولید شده است. برخی از قابلیت های این سخت افزار به شرح زیر می باشد :

- قابلیت ارتباط با کارت خوان های استاندارد، اثر انگشت ، تشخیص چهره بومی تیزبین و کیبورد هوشمند تیزکد ساخت تیزبین و ...
- قابلیت ارتباط با انواع فلاشر هشدار، آژیر و قفل مغناطیسی به صورت رمزنگاری شده (غیر قابل از کار انداختن و غیر فعال کردن)
- قابلیت ارتباط با انواع گیت های نفر رو (تریپود، استوانه ای، کشویی) و ماشین رو متصل به تشخیص چهره و پلاک)
- عملکرد به صورت آنلاین و آفلاین
- سینک خودکار و دستی با سرور
- بسیار کم مصرف همراه با دو باتری پشتیبان قدرتمند جهت حفظ عملکرد در شرایط کاری حساس
- ساختار کاملا ماژولار
- رمزنگاری پیشرفته ارتباطی با سرور که برای هر سایت اختصاصی است .
- امکان لاگ ، کانفیگ و مانیتور تنظیمات و وضعیت ارتباطی کنترلرها و سنسورها با سرور (آنلاین و آفلاین)
- هشدار های صوتی و تصویری
- قطعات صنعتی با طول عمر بالا و تست عملکرد در شرایط سخت آب و هوایی
- محافظت در برابر تزریق ولتاژ یا اتصال کوتاه به ورودی ها جهت آسیب عمده و از کار انداختن کنترلر و هشدار این موارد به مرکز

تیزبین : مانیتورینگ سلامت و کنترل عملکرد تجهیزات و تاسیسات صنعتی



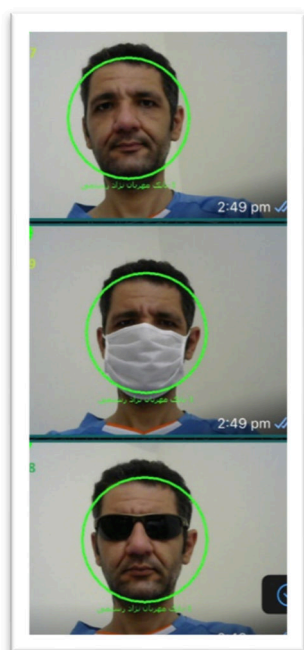
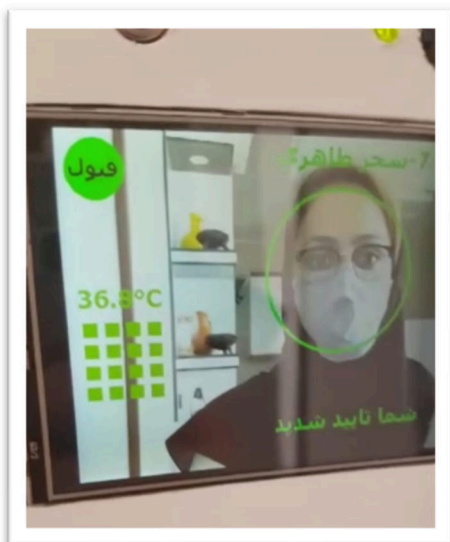
کلیه تجهیزات حساس صنعتی از تابلوهای برق گرفته تا موتورهای برق از خطوط گاز و مایعات تحت فشار تا مخازن و سایر تجهیزات مهم به واسطه سنسورهای کنترل جریان ، فشار ، دما ، لرزش و سایر ماژول های استاندارد ، در نرم افزار تیزبین به عنوان ورودی ها ایجاد و سطح مقادیر مجاز برای هر یک تعریف می شود. چنانچه در هر مورد از سطح مجاز تخطی شود قابلیت اجرای فرامینی به خروجی ها دارد ، مانند گردش دوربین به سمت تجهیز مورد آلام ، پخش هشدار صوتی ، قطع برق و یا قطع یا وصل شیرهای کنترل برقی یا فرمان به PLC و ...

بنابر این یک سیستم جامع کنترل و مانیتورینگ پروسس در تیزبین وجود دارد.

تشخیص چهره بومی سامانه تیزبین

از آنجا که نمی توان به عملکرد محدود و نامعلوم سیستم های تشخیص چهره غیر بومی اطمینان داشت و با توجه به اهمیت عدم وابستگی به نمونه های خارجی ، تیم تیزبین بر آن شد که نسخه بومی تشخیص چهره را طراحی و تولید کند. این محصول به طور مستقل تست عملکرد و کیفیت شده است. برخی از قابلیت های سیستم تشخیص چهره بومی تیزبین از قرار زیر می باشد :

- نسخه بومی و برنامه نویسی شده بر مبنای استاندارد های جهانی Ai پردازش چهره
- تشخیص دمای بدن از فاصله نیم متری با دقت بالا (افزونه سخت افزاری اختیاری)
- سرعت بالا و دقت مطلوب تشخیص چهره
- عملکرد آنلاین و آفلاین
- ثبت امن و رمزنگاری شده چهره به صورت یکپارچه در سامانه
- پیامهای صوتی چند زبانه
- هشدار دمای بالای بدن و جلوگیری از ورود افراد بیمار و داری تب
- سازگار با جداول زمان بندی پیشرفته و متنوع و منطبق با چارت کارفرما
- نمایش خروجی های مستقل مانیتورینگ بر اساس نیاز و اولویت
- نگهداری بیش از ۵۰۰۰۰ چهره (تعبیه شده در نسخه جاری و قابل توسعه)
- نگهداری و ثبت داده ها و رکوردهای بسیار زیاد به صورت کد شده
- کم مصرف با باتری قدرتمند داخلی
- تکنیک شناسایی عادی / با ماسک / با عینک (حتی عینک دودی)
- تصویربرداری از چهره ها با ظرفیت بالا برای آرشیو تمامی چهره های تشخیص داده شده یا نشده و نگهداری به صورت داخلی و سینک خودکار با سرور با کیفیت بالا
- فوکوس خودکار لنز روی چهره
- تطبیق نوری پیشرفته حتی اگر نور مزاحم پشت سر فرد باعث تیرگی صورت شود
- امکان محدودسازی زاویه دید لنز



دستگیره هوشمند بومی تیزبین مدل ریتال صنعتی

یکی از پرمخاطره ترین مکانهای دسترسی در همه سایت ها ، کابینت های شامل مواردی مانند سرورها ، سویچ ها یا تابلو های برق و تجهیزات مخابراتی حیاتی می باشد. این تابلوها ، رک ها و کابینت های مهم یکی از مهمترین اهداف در خرابکاری ها ، نفوذهای سایبری و موارد مشابه هستند. بنابر این تیم فنی و مهندسی تیزبین یکی از کارآمد ترین نمونه های صنعتی دستگیره را بر طبق استانداردهای نظامی طراحی و تولید کرده است . به کمک این دستگیره هوشمند می توان به طور دقیق دسترسی افراد را به تجهیزات و تاسیسات داخل تابلو ها و کابینت ها کنترل نمود و در صورت هرگونه رخداد می توان تاریخچه دقیقی از نفراتی که به آن کابینت دسترسی پیدا کرده اند دریافت کرد. با افزودن مازول دوربین می توان چهره فرد یا افرادی که به کابینت دسترسی پیدا کرده اند را ثبت کرد . در صورت قفل نشدن یا باز ماندن درب کابینت مربوطه هشدار همراه با آلام در اتاق کنترل مرکزی حراست به صورت صوتی و تصویری نمایش داده می شود. کلیه دستگیره ها به سامانه یکپارچه و متمرکز تیزبین متصل اند و مداوما وضعیت و عملکرد آنها پایش می شود . برخی از قابلیت های دستگیره کابینت تیزبین مدل ریتال در زیر آمده است :

- قابلیت عملکرد به صورت آنلاین و آفلاین با قابلیت نگهداری اطلاعات کلیه پرسنل ، شیفت های کاری ، تعطیلات ، جداول زمان بندی و ...

- ذخیره آفلاین اثر انگشت تا ۲۰۰۰ کاربر در مدل ریتال

- لاگ های دقیق و رمزنگاری شده

- بدنه بسیار مستحکم و قوی از آلومینیوم صنعتی ۶۰۶۱ و درپوش فولادی

- باتری و قطعات با کیفیت صنعتی مناسب شرایط نامساعد (دما و رطوبت)

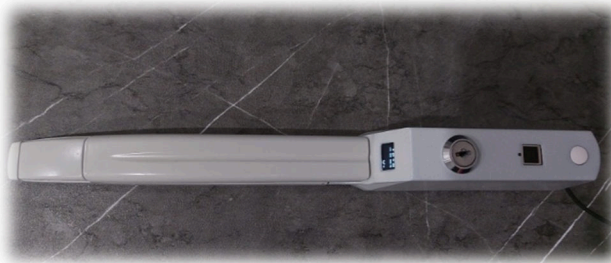
- سیستم هشدار صوتی

- خروجی آلام استاندارد و قابل تعریف جهت کاربردهای متنوع

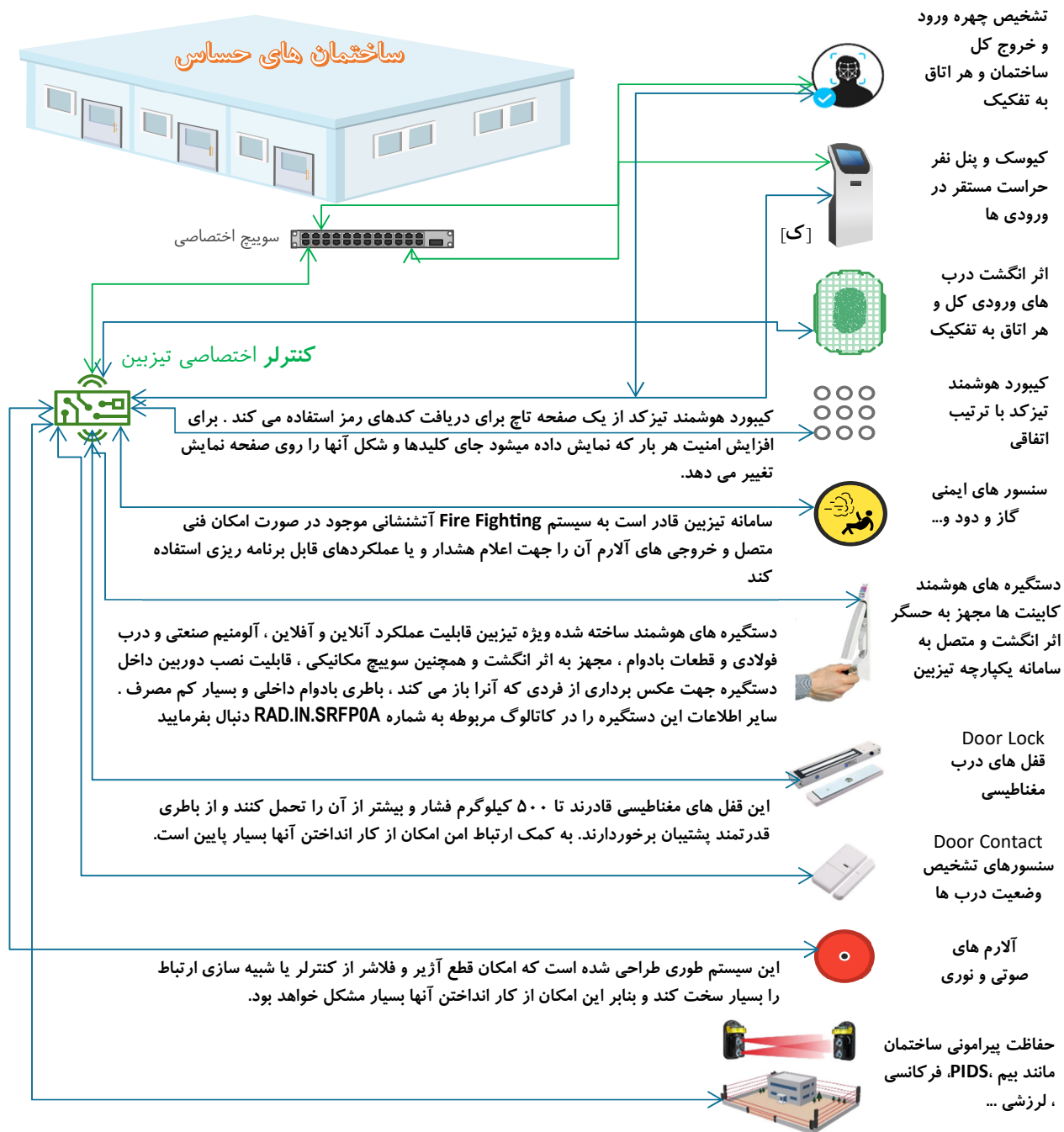
- قابل عملکرد با قفل و سویچ مکانیکی برای باز کردن در شرایط اضطراری

- قابلیت نصب دوربین درون دستگیره جهت عکس برداری از افراد

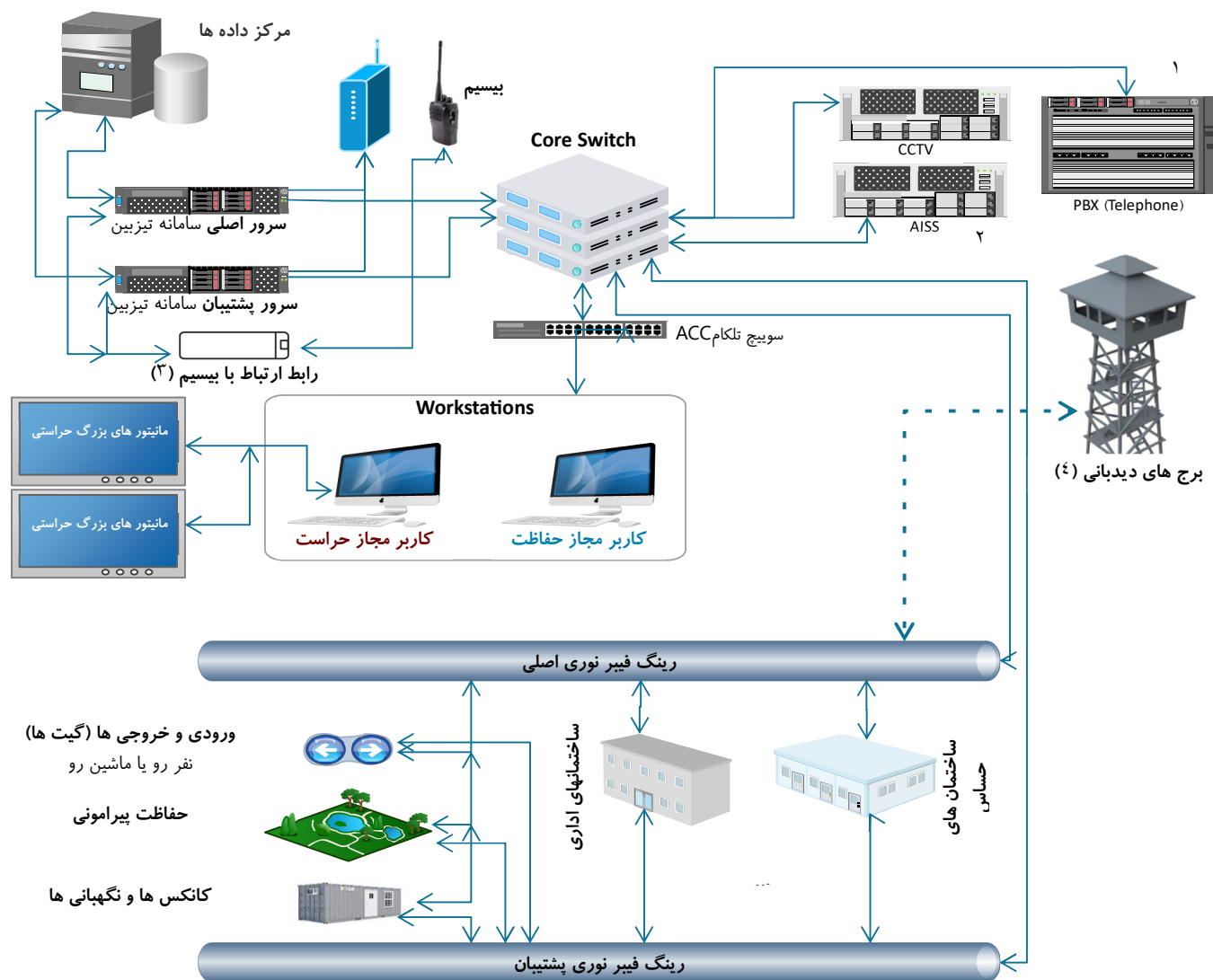
- کاملاً مازولار (فرایند تعمیر و نگهداری و پشتیبانی آسان و سریع)



این دستگیره های کابینت منحصر به فرد از قطعات صنعتی با مقاومت بالا ساخته شده است و با استاندارد ریتال آلمان کاملاً تطابق دارد



ک : کیوسک حراستی ورودی قابلیت ارتباط مستقیم صوتی، تصویری از مرکز حراست با نگهبان مستقر را دارد. ضمناً هشدارها و آلارمهای حساس ساختمان را به نگهبان نشان می دهد و به صورت تصویری و دیجیتال مجوز نفرات مجاز برای ورود به ساختمان را با اطلاعات کامل آنها مانند عکس و نام و رسته و ... را آنجا فهرست می کند و ساعت ورود و خروج افراد را ثبت می کند. این کیوسک مجهز به دوربین، میکروفون برای بررسی تصویر و صدا جهت نظارت اتاق حراست و تیم حفاظت می باشد. از این کیوسک به شکل پنلی در برج های مراقبت هم استفاده شده است. سایر اطلاعات این کیوسک را در کاتالوگ مربوطه به شماره RAD.IN.CM8100 دنبال بفرمایید.



- ۱- سامانه یکپارچه تیزبین از طریق ساختار تلفن داخلی (PBX/PABX/VOIP) در شرایط اضطراری و آلام به صورت خودکار با داخلی/داخلی های تعریف شده تماس و به صورت صوتی و گویا اعلام هشدار می کند.
- ۲- سامانه یکپارچه تیزبین با اتصال به شبکه CCTV قادر به نمایش زنده تصاویر دوربین ها در نقطه آلام روی پنل و مانیتورهای حراست است. در همان زمان سیستم عکس هایی که از دوربین های مربوطه در محیط آلام گرفته را جهت بررسی های بعدی آرشیو می کند.
- ۳- هشدارهای مهم و تعیین شده می توانند در صورت تنظیم از طریق بی سیم روی فرکانس تعریف شده اطلاع رسانی شوند
- ۴- برج های دیدبانی مجهز به پنل نظارتی و ارتباطی هستند.

گیت های ورودی و خروجی



سوییچ گیت

کنترلر تیزبین

گیت های نفر رو اداری

گیت های نفر رو ورودی اصلی

گیت ماشین رو سبک و سنگین

پلاک خودروها و چهره نفرات با هم تطبیق داده می شود و در سیستم تصاویر با کیفیت بالا ثبت میگردد

تشخیص چهره ورود و خروج

اثر انگشت ورودی اصلی

۱- کلیه ورودی های گیت های مهم و حساس یا ساختمانها یا اتاقهای مهم می توانند افرادی یا ترکیبی از بیومتریک ها استفاده کنند به این معنی که در صورت تنظیم ، هم چهره هم اثر انگشت و هم رمز (با کیبورد هوشمند تیز کد که همواره جای اعداد تغییر می کند) نیاز باشد تا ورود وی تایید گردد.

کارت خوان مجهز به دوربین

دستگیره هوشمند کابینت مدل ریتال

کنترل دسترسی به کابینت ها و تابلوهای حساس تاسیساتی همواره یک چالش بزرگ محسوب می شود. این که چه کسی و برای چه مدتی به یک تابلو دسترسی پیدا کرده ، چه مدت درب تابلو باز بوده و آیا به درستی بسته شده است یا نه. همچنین سطح دسترسی افراد در بازه های زمانی مجاز مهم است.

دستگیره هوشمند می تواند با اثر انگشت تعریف شده افراد مجاز برای کابینت های استاندارد مختلف از دسترسی غیر مجاز جلوگیری کند. دوربین تعبیه شده روی آن می تواند از هر کسی که قصد دسترسی به کابینت را دارد عکس گرفته و در حافظه خود آنرا نگهداری کند.





انواع گیت های صنعتی نفر رو ، ماشین رو با بیومتریک های مختلف از تشخیص چهره تا اثر انگشت و از کارت های تماسی تا کیبورد هوشمند با کلیدهای رندوم و NFC که داخل گوشی های هوشمند و برخی ساعت های مچی هوشمند قرار دارد پشتیبانی می کند. ضمناً همه این بیومتریک ها به همراه قفل های مغناطیسی که توان تحمل بیش از ۵۰۰ کیلو وزن و باتری داخلی دارند و نیز فلاشرها و آلارم ها از تمام اتاقها ، سالن ها ، راهروها و سوله های مد نظر حفاظت می کنند.

چالش حفاظت پیرامونی در محدوده های وسیع و غیر هم سطح

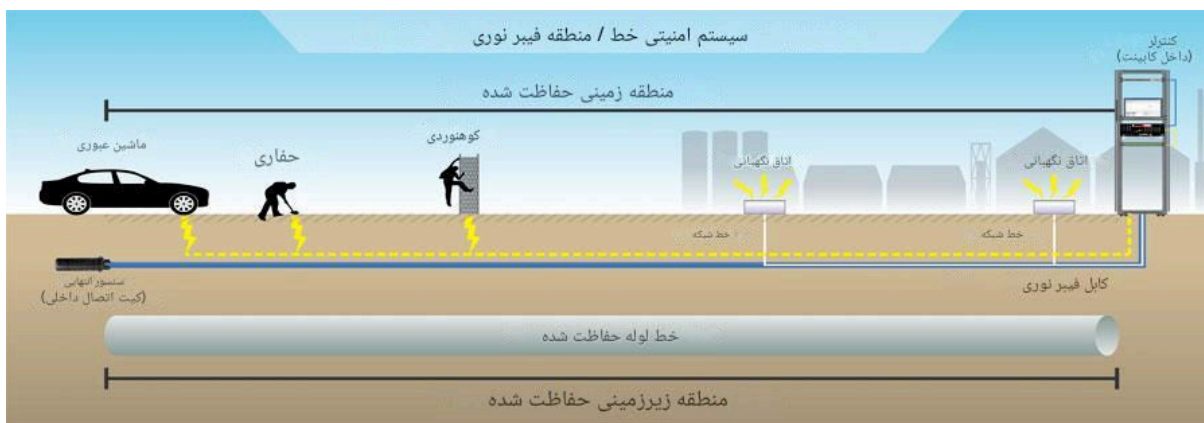
فناوری های مختلفی برای پوشش حفاظت پیرامونی محدوده های وسیع با شرایط پیچیده جغرافیایی وجود دارد. در زیر به معدودی از آنها اشاره می شود :

۱. آشکارسازهای فتوالکتریک ← برج های پرتوی (Beam) :



- استفاده از فناوری لیزر بین گیرنده و فرستنده : در بردهای متنوع ۲۰، ۶۰، ۱۰۰ و ۲۰۰ متر
- به هیچ عنوان در بین فاصله ی دو بیم هیچ مانعی وجود نداشته باشد : اعم از سنگ ، درخت ، علف...
- نباید رو به سمت نور مستقیم مثل : آفتاب و یا چراغ قرار بگیرد .
- مقاوم در برابر رطوبت ، گرما و گرد و غبار می باشد.
- قابلیت استفاده از باتری داخلی با عمر طولانی تا ۴ سال.

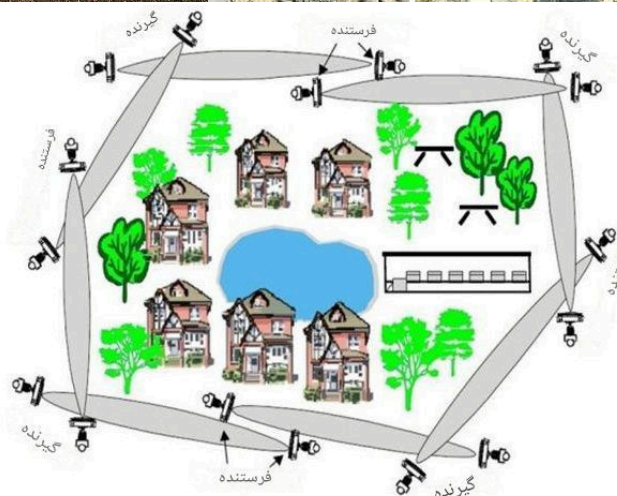
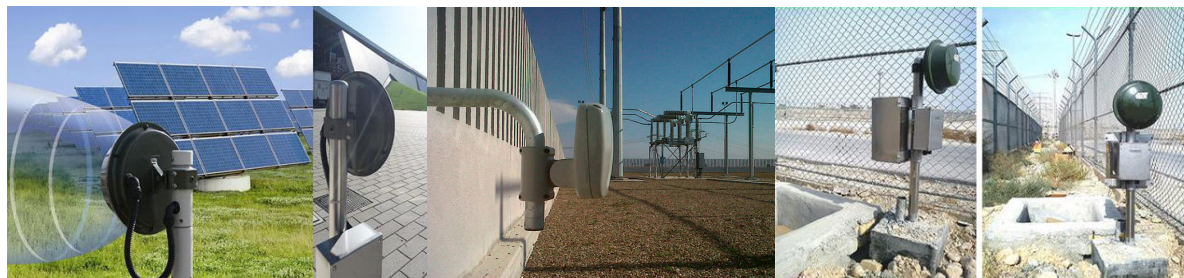
۲. فنس های ایمن شده با فیبر نوری



نمونه ای از روش دفن زیر زمینی

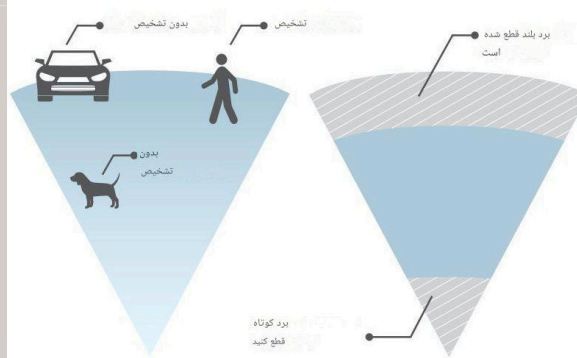
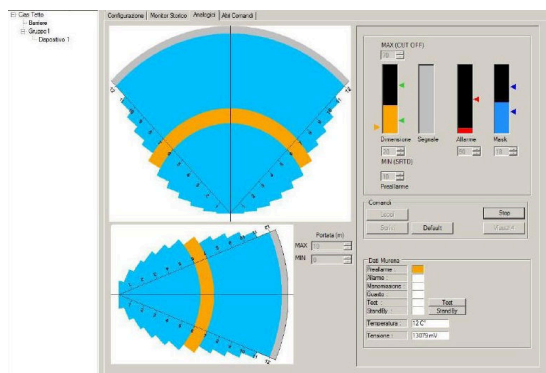
- a. سرعت بالای انتقال هشدار از فنس به مرکز
- b. پوشش نواحی و خطوط بسیار طولانی
- c. بدون نیاز به جریان الکتریکی در مسیر نصب حسگر فیبر نوری
- d. کاهش آلام های مزاحم (غیر واقعی) جهت کنترل دقیق هشدارهای دریافتی
- e. روش های نصب هوایی ، فنی ، زمینی و زیر زمینی
- f. طول عمر بالا
- g. در صورت آسیب ، نیاز به فیوژن هست که کار پشتیبانی را کمی سخت می کند

۳. فناوری های مبتنی بر امواج



a. به عنوان یک سنسور مایکروویو خالص، به سادگی در برابر مه، تغییر دما، طوفان شن، تشعشعات شدید خورشیدی مصون است.

b. بدون هیچ گونه خطری از آلارم‌های کاذب معمولی که می‌تواند توسط حیوانات کوچک یا اجسام متحرک بزرگ ایجاد شود، اجتناب کنید.



۴. فنس الکتریکی

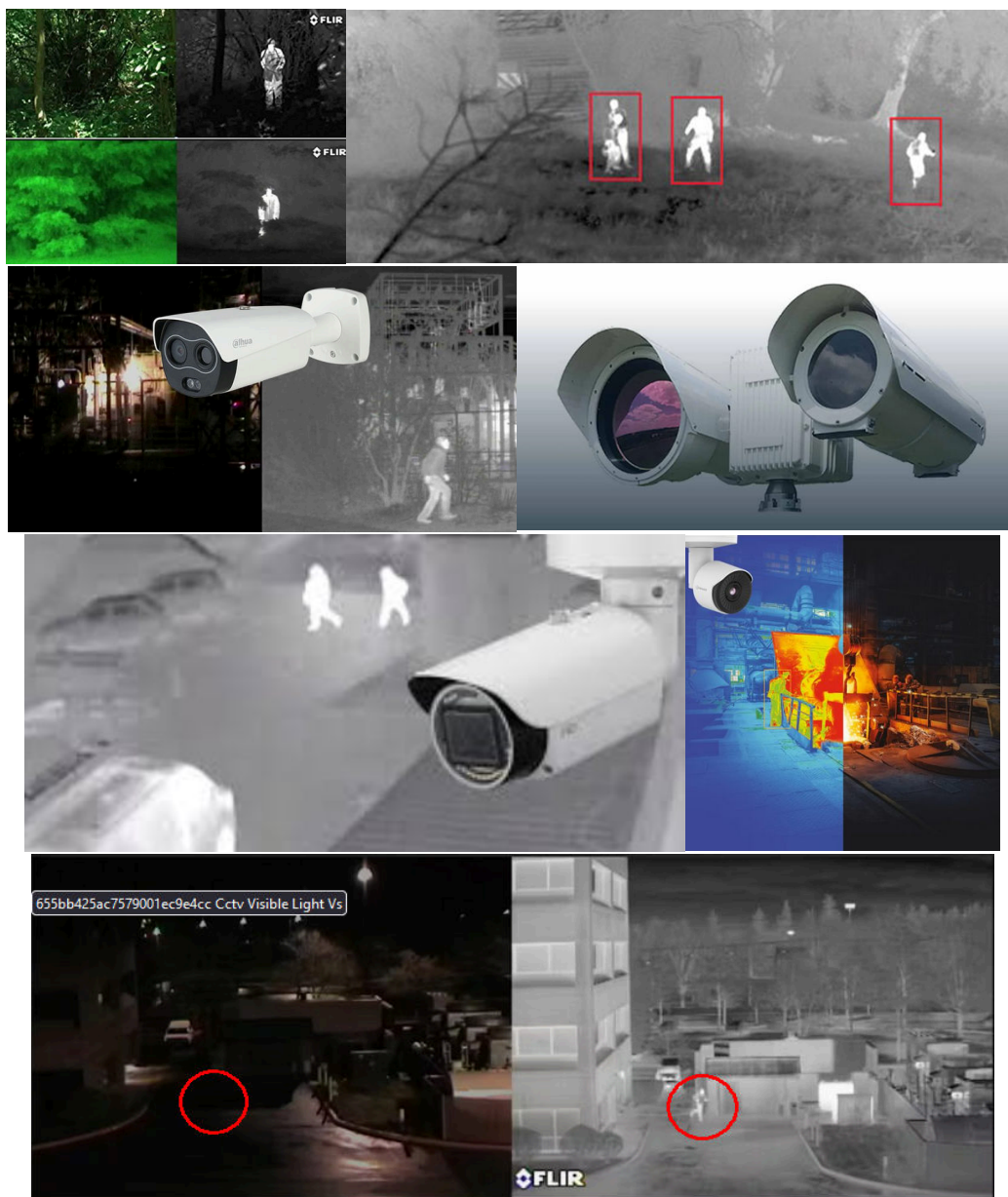


- a. سطح بالایی از حفاظت برای افراد و اموال در داخل مجموعه ها فراهم میکند.
- b. با اعمال شوک به فرد نفوذی به محدوده ، مرحله نخست بازدارندگی را ایجاد میکند.
- c. به تیم انسانی حفاظت جهت تشخیص موقعیت نفوذ احتمالی کمک میکند.
- d. قابلیت فعال سازی سیستم های امنیتی و سیستم های هشدار محیطی مثل آژیر و پروژکتور و بلد گو را دارد.
- e. شبکه الکترو فنس هیچ گونه خطر جانی برای شخص تماس گیرنده ندارد.
- f. شوک ناشی از پالس های الکتریکی تنها بر بافت پوست بدن تاثیر میگذارد و هیچ شوکی به قلب و عروق و سیستم عصبی بدن وارد نمی کند.



سامانه یکپارچه تیزبین از بسیاری از تجهیزات و سنسورهای استاندارد جهانی پشتیبانی کامل دارد. از محصولات شیاس ایتالیا تا بوش آلمان و برندهای شناخته شده و معتبر در حوزه بیومتریک ، تجهیزات پیشگیری و حفاظتی.

۵. فناوری تشخیص حرارتی

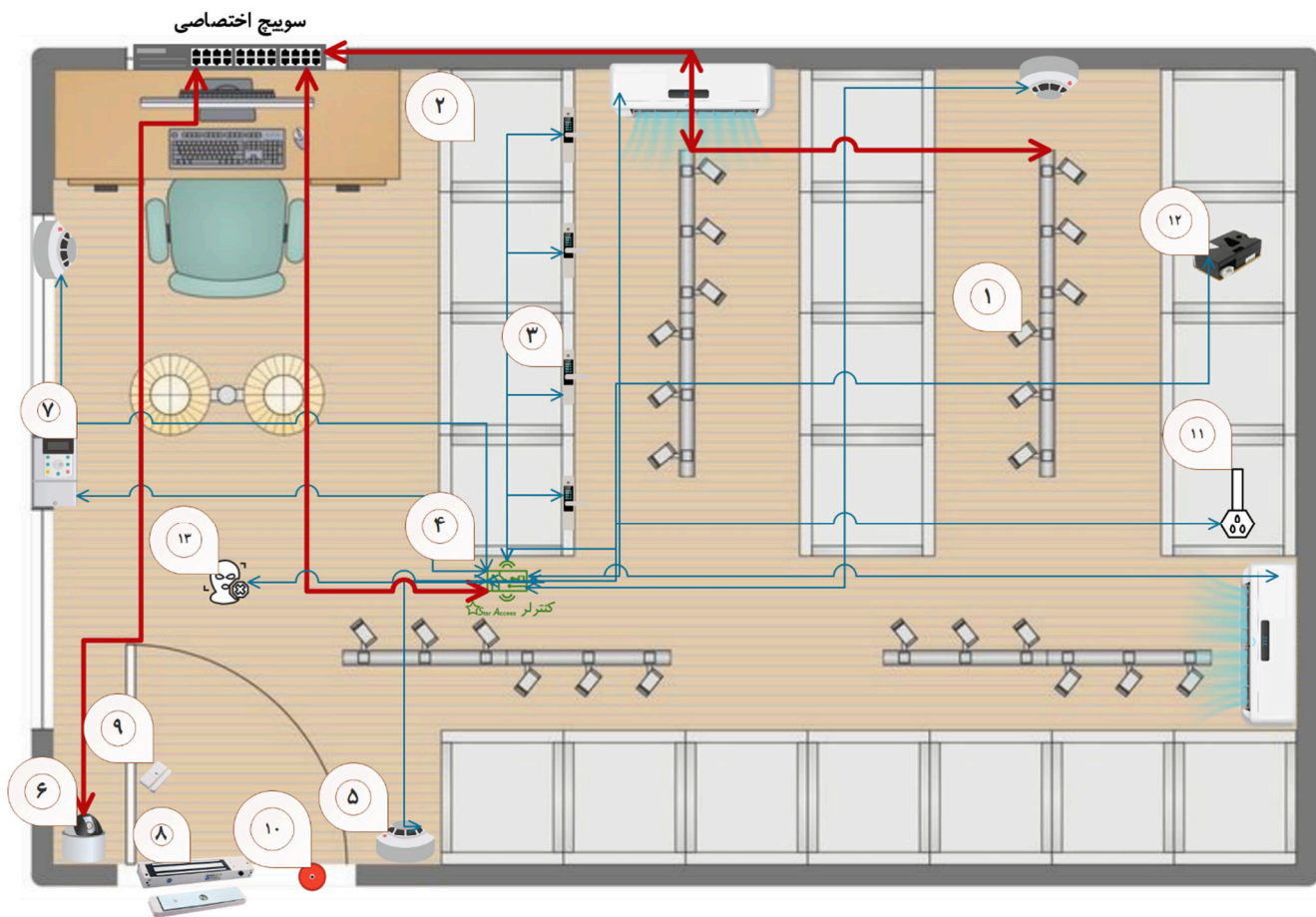


- a. تشخیص انسان از حیوان حتی در صورت استتار یا در تاریکی
- b. استفاده در شرایط آب و هوایی نامناسب.
- c. می توانند موجودات زنده و خودرو ها را تا برد بسیار بالا تشخیص بدهند
- d. کیفیت تصاویری که توسط دوربین های حرارتی ثبت می شوند، تحت تاثیر سایه یا نور تغییر نمی کند
- e. امکان تشخیص هویت افراد وجود ندارد
- f. پر هزینه بودن دوربین های Thermal
- g. برای مناطق تاریک و فضاهای باز، دوربین های حرارتی قادر به دیدن افراد متجاوز هستند. دوربین های حرارتی سبزرنگ، مستحکم بوده و دارای محفظه ای ضد انفجار هستند.

۶. فناوری پهبادهای نظارتی



از آنجا که فضاهای معدنی بسیار گسترده و بزرگند، جهت نظارت کارآمد نیروهای حفاظتی و حراستی از پهبادهای نظارتی کمک می گیرند. سامانه یکپارچه تیزبین دارای یک رابط پیشرفته سخت افزاری نرم افزاری جهت ارتباط و هدایت پهبادهای استاندارد نظارتی است. به کمک این رابط سامانه قادر است از طریق جداول زمانبندی که در اختیار دارد یا به فراخور آلارمی که از یک منطقه از معدن دریافت می کند سریعاً پهباد را به آن نقطه ارسال و تصویربرداری کرده و آنرا در اختیار مسئولین حراستی یا سرپرست های معدن قرار دهد. کلیه عملیات های پهبادی مانند سایر عملیات ها در سامانه یکپارچه و پیشرفته تیزبین ثبت و قابلیت ارجاع یا بازپخش دارند.



- ۱ دوربین های نظارتی متمرکز بر کابینت های اتاق سرور (به تعداد مورد نیاز)
- ۲ کابینت های اتاق تلکام
- ۳ دستگیره های هوشمند تیزبین کابینت مجهز به سنسور اثر انگشت RAD.IN.SRFPOA (به ازای هر کابینت وجود دارد)
- ۴ کنترلر ویژه تیزبین (به تعداد مورد نیاز بسته به بزرگی و مازولهای مورد نظر)
- ۵ سنسورهای گاز و دود (به تعداد مورد نیاز)
- ۶ دوربین اختصاصی نظارتی
- ۷ پنل برق اتاق سرور (کنترل ولتاژ ، جریان و دیتالاگر متصل به کنترلر تیزبین)
- ۸ قفل مغناطیسی درب Door Lock
- ۹ سنسور وضعیت درب Door Contact
- ۱۰ آلارم صوتی و نوری
- ۱۱ سنسور رطوبت (به تعداد مورد نیاز)
- ۱۲ سنسور ویژه گرد و غبار (به تعداد مورد نیاز)
- ۱۳ تشخیص حرکت PIR (به تعداد مورد نیاز)

سرور سامانه تیزبین

سرور سامانه تیزبین مرکز پردازش کلیه داده های کنترلرها ، سنسورها و سایر سرورهای مرتبط با خود است. با توجه به حساسیت این سرور غالبا دارای سرور پشتیبان یا redundant میباشد که داده ها و اطلاعات بین این دو با یک ابزار تخصصی مداوما سینک می شوند. سرور سامانه تیزبین **مجهز به هوش مصنوعی** در تحلیل داده ها و گزارشات و هشدارهای خود است . از هوش مصنوعی در بررسی تردهای مشکوک افراد بر مبنای رفت و آمد یا توقف در جاهای حساس تعیین شده (مانند جلوی دربها ، گذرگاه ها یا تجهیزات حساس ایمنی امنیتی) تا هوش مصنوعی در بررسی داده های مشکوک و غیر معمول تا کنترل ولتاژ و جریان و لرزش و شرایط دمایی رطوبتی و محیطی PLC ها ، HVAC یا موتورها ، ژنراتورها و ... به کمک فایروال های استاندارد صنعتی ، سنسورها و سیستم کنترلر هوشمند خود و توقف این فرامین ، تا هوش مصنوعی در بررسی وضعیت اتاق های سرور و دیتاسترها و کابینت های مهم.

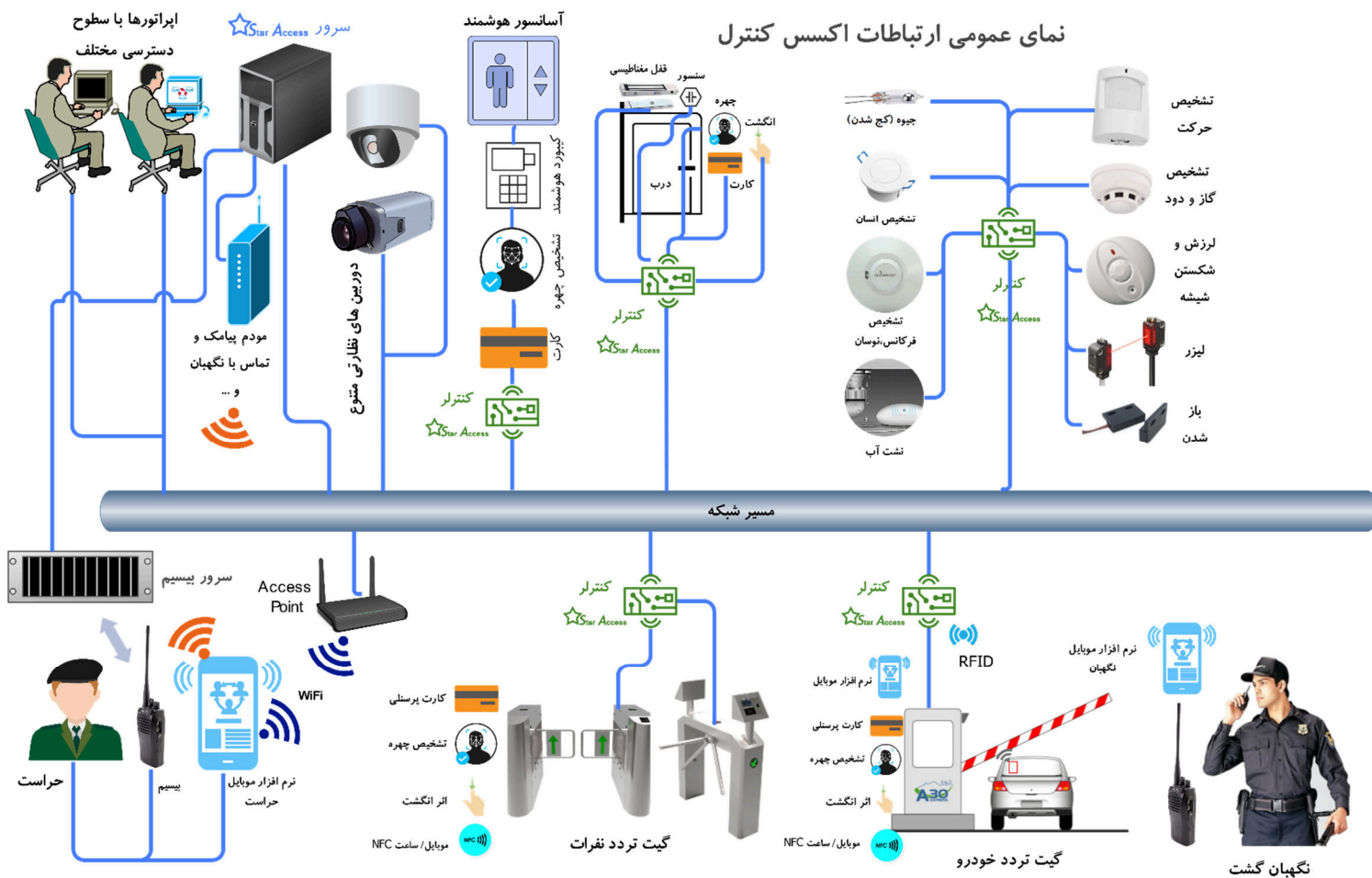
به طور کلی سرور سامانه تیزبین بنا به نیازمندی های شما قادر است با سیستم های زیر ارتباط مستمر و کارآمد داشته باشد:

VOIP PBX CCTV (پیام خودکار به تیم حراست با اعلام هشدارها به صورت پیام صوتی روی یک کانال فرکانسی تعیین شده) **PAGA** (پیجینگ هشدارها و آلارم ها یا آژیر امنیتی در صورت دریافت یک آلارم ایمنی یا امنیتی از سنسورها)

این ارتباط با سرورهای فوق تنها بر اساس سفارش و درخواست کارفرما انجام می شود و امنیت ارتباطی با نظارت کارفرما کاملا لحاظ می شود.



سرور تیزبین



شماتیک تیزبین در یک نگاه



گروه امنیتی راد
با ما در ارتباط باشید



rcgc.ir



جمهوری اسلامی ایران
وزارت صنعت، معدن و تجارت



ریاست جمهوری
معاونت علمی و فناوری

پارک فناوری پردیس
منطقه
پهشت فوری

PARDIS
Technology Park
TRAN-SILICON VALLEY



مرکز رشد فناوری نخبگان