Solutions technologiques complètes d'Anixter

SYSTÈMES DE SÉCURITÉ PHYSIQUE

CADRE DE SÉCURITÉ PHYSIQUE INTÉGRÉ

On suppose souvent que les systèmes de sécurité physique fonctionnent ensemble de manière homogène. En réalité, l'intégration est complexe et nécessite une planification préalable. Toutes les technologies utilisées dans les systèmes de sécurité physique, qui se développent au fil du temps, n'évoluent pas au même rythme, leur capacité d'intégration se situe donc à des niveaux différents. Le modèle idéal est un système de sécurité physique nécessitant un minimum de personnalisation et qui prend en charge toutes les technologies sans perdre en fonctionnalité.

COMPOSANTS D'UN CADRE DE SÉCURITÉ PHYSIQUE INTÉGRÉ

Propriétaire	Les systèmes vidéo, de contrôle d'accès et d'intrusion existants, avec une intégration tierce limitée ou inexistante, qui donnent souvent lieu à plusieurs systèmes disparates fonctionnant en silos. Les systèmes propriétaires permettent une intégration de systèmes à partir d'un seul fabricant. Les intégrations tierces, les options du système et les fonctionnalités dépendent de la feuille de route et du calendrier du fabricant propriétaire.
Hybride	Technologies analogique et numérique coexistantes au sein d'un même système ou appareil. Permet à une technologie d'interface propriétaire et ouverte de coexister au sein d'un seul système ou appareil. Il s'agit d'une transition dans le processus de conversion et d'un investissement différé de l'intégration. Souvent, la première étape de la migration vers une interface ouverte et une infrastructure de câblage standard.
Interface ouverte	Une approche intégrée qui permet l'interopérabilité des systèmes grâce à l'utilisation d'API (interfaces de programmation) et de SDK (trousses de développement logiciel).
Architecture véritablement ouverte	Une solution prête à l'utilisation, soutenue par le secteur et en conformité avec les normes qui permet à plusieurs systèmes sur une infrastructure commune d'être gérés via une interface utilisateur unique. Des systèmes de sécurité physique à architecture ouverte et en conformité avec les normes intégrant des dispositifs anti-intrusion et anti-incendie doivent encore être introduits, tandis que le contrôle d'accès est en cours de développement.

NOUS CRÉONS DE LA VALEUR AJOUTÉE EN APPORTANT LES AVANTAGES SUIVANTS :

Choix de la technologie	Interopérabilité des systèmes	Déploiement de projet

« Correctement protégé, l'IoD permettra un traitement et une analyse des données plus efficaces, afin que les responsables de la sécurité puissent tirer parti d'une énorme ressource d'intelligence permettant de détecter les risques de manière proactive, de réagir aux situations en temps réel et d'accroître l'efficacité des mesures de sécurité. »

Source : SIA Megatrends Report (Rapport sur les mégatendances SIA)

DÉFIS COURANTS

Adopter les **TECHNOLOGIES ÉMERGENTES**

Réaliser une **VALEUR STRATÉGIQUE DES INVESTISSEMENTS**

Remédier aux **VULNÉRABILITÉS** du système

Développer les **CAPACITÉS TECHNOLOGIQUES**

Tirer parti des **TECHNOLOGIES DE RUPTURE**

SOLUTIONS TECHNOLOGIQUES

Adopter les technologies émergentes

La mise en œuvre de technologies émergentes avec des capacités améliorées peut améliorer l'efficacité opérationnelle et des systèmes. Comprendre ce vers quoi tend la technologie et évaluer les performances sont essentiels pour une mise en œuvre réussie.

Réaliser une valeur stratégique des investissements

Les appareils intelligents collectent davantage de renseignements et trouvent des possibilités sur leur utilisation dans le cadre de la veille économique. Les fonctionnalités avancées peuvent permettre de réduire les coûts et d'améliorer la rentabilité. Collaborer pour tirer parti de l'expérience des partenaires commerciaux et prouver l'efficacité des applications peut aider les organisations à justifier de nouveaux investissements dans les technologies.

Remédier aux vulnérabilités du système

Un système qui n'est pas régulièrement entretenu et mis à jour est exposé à une plus grande vulnérabilité. Adopter des meilleures pratiques en matière de TI et de sécurité, notamment un calendrier de gestion des correctifs tout en suivant les consignes et les politiques de renforcement du fabricant peut aider à protéger les systèmes de sécurité. S'abstenir de faire des investissements dans la maintenance continue et les mises à niveau de sécurité signifie sacrifier les performances du système, l'exposer à des cyberattaques et des attaques physiques, limiter les possibilités d'intégration avancée entre les systèmes.

Développer les capacités du système

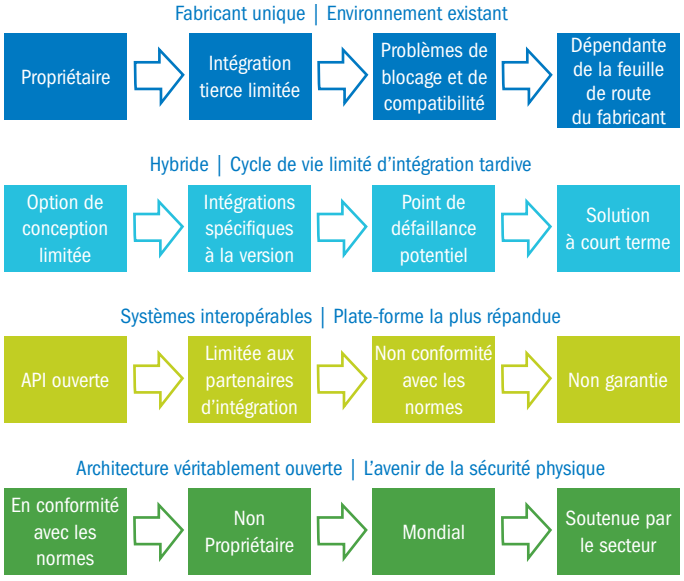
L'intégration de systèmes de sécurité physique peut permettre une collaboration de sécurité physique et logique plus poussée. L'intégration de solutions d'analyses et gestion vidéo avec un apprentissage avancé transforme les données collectées en renseignements validés et exploitables pouvant changer un système réactif en un système prédictif pour une réponse plus rapide.

Tirer parti des technologies de rupture

Le nuage et l'analyse avancée sont des technologies de rupture qui peuvent fournir de nouvelles données permettant aux clients d'extrapoler des renseignements intéressants et exploitables depuis des systèmes de sécurité physique. La collaboration avec les fabricants, les experts techniques et un réseau d'intégrateurs spécialisés est essentielle pour atteindre les objectifs de mise en œuvre de ces technologies à l'avenir.

CHEMIN VERS UNE ARCHITECTURE VÉRITABLEMENT OUVERTE

Les systèmes intégrés et ouverts sont dictés par la nécessité d'éliminer les redondances, d'améliorer l'efficacité et de gérer la sécurité physique grâce à une interface utilisateur unique. Il est possible de sélectionner les meilleurs produits pour des applications sans être confronté à des contraintes de compatibilité. L'élaboration de normes telles que l'ONVIF fournit une base de référence permet aux dispositifs IP de fonctionner ensemble. À mesure que les technologies convergent, il est essentiel de travailler avec un intégrateur de sécurité qualifié pour concevoir un cadre de sécurité physique intégré.



POUR DE PLUS AMPLES RENSEIGNEMENTS, RENDEZ-VOUS SUR ANIXTER.COM/SECURITY OU COMMUNIQUEZ AVEC VOTRE REPRÉSENTANT ANIXTER LOCAL.

Chez Anixter, nous aidons à construire, connecter, alimenter et protéger des actifs précieux et des infrastructures critiques. Des réseaux d'entreprise à la prestation de services industriels de maintenance, de réparation et de révision en passant par les applications de vidéosurveillance ou encore la distribution d'électricité, nous proposons une gamme complète de solutions et de renseignements permettant de mettre sur pied des systèmes fiables et résilients qui peuvent répondre aux besoins de votre entreprise et de votre communauté. Grâce à notre réseau de distribution mondial, notre expertise de gestion de la chaîne d'approvisionnement et notre savoir-faire technique incomparables, nous apportons l'efficacité nécessaire pour accroître vos gains.