

Contrôle d'accès, anti-intrusion, gestion centralisée

Entreprise ou institution, toute organisation est confrontée aux problèmes de sécurité de son personnel, de protection contre le vol, l'agression, l'incendie ou l'accident, de défense de ses centres vitaux et de ses secrets, de gestion efficace de ses bâtiments. La solution efficace à ces problèmes utilise des systèmes intégrés de contrôle d'accès électronique, de gestion de sûreté et de vidéosurveillance.



Si les principes de base sont communs à tous ces systèmes, chaque application demande néanmoins une solution particulière. Maîtriser cette diversité d'applications en proposant une solution unique, cohérente et évolutive est la caractéristique du SCNET4™ de NCS®. Sa conception originale permet de construire des systèmes, petits ou grands, par l'assemblage de « cubes » identiques.

SCNET4™ est un système intégré de gestion électronique de contrôle d'accès, de sûreté d'entreprise et de centralisation technique de bâtiment. Il convient aussi bien pour de petits bâtiments que pour des installations multi sites en réseau. Il met en œuvre des concepts de très haute sécurité et des technologies innovantes, proposant une très grande puissance pour un niveau de miniaturisation inégalé.

Une innovation sans égale

Le nouveau core CP5™ qui équipe les automates SC4x5™ de NCS® conjugue une puissance et une capacité exceptionnelles avec une miniaturisation stupéfiante. Il allie une gestion complètement distribuée à la simplicité d'une solution unique.

SC4x5™ est versatile : contrôle d'accès variés, identification de badges divers, commande de tous types d'obstacles, surveillance d'alarmes de tous niveaux. C'est comme un jeu de cubes : en assemblant ces cubes identiques, miniaturisés et exceptionnellement puissants, on crée le système que l'on veut.



Il embarque aussi un serveur Web qui le rend accessible de n'importe où. Il peut être alimenté par la fonction PoE, sa consommation électrique étant extrêmement faible.

La sécurité est poussée à l'extrême : associé à l'option SECURE, cet automate permet le chiffrement des communications TCP/IP vers le serveur mais aussi des échanges de données avec les lecteurs de badges. Il allie aussi une distribution centralisée et un stockage sécurisé des clés de chiffrement liées aux badges MIFARE® DESFire EV1/EV2 avec lesquels il communique directement en mode transparent.

La liaison sur une paire des capteurs utilise MTM4™ et MTM5™, permettant des économies de câblage allée à un monitoring permanent de l'état des liens vers les entrées des automates.

Avantages techniques

L'architecture Client / Serveur de SCNET4™ est adaptée à Windows 10™ et Windows Server 2016™. La structure est optimisée pour tous les réseaux (filaire en étoile ou en bus, IP avec ou sans DHCP, ADSL, ...) et pour le pré-câblage des bâtiments. Les unités de gestion locale, appelées automates, sont équipées d'un processeur ARM® de dernière génération fonctionnant sous LINUX®.

Complet dès sa version de base, il offre nativement toutes les fonctions requises pour son exploitation aisée : gestion des alarmes, vues graphiques interactives, gestion des astreintes, accueil des visiteurs, générateur de rapports, programmeur de scénarii et de macro-commandes, assistance de dépannage, ...

Le système SCNET4 est simple, modulaire et sécurisé.

Simple

- À installer : les automates SC4x5™ (éléments miniaturisés, complets et tous identiques) sont les composants de base du système. Leur grande modularité permet leur assemblage à la manière d'un jeu de cubes.
- À mettre en œuvre : tout est affaire de paramètres, définis et modifiés à distance, directement à partir des postes de gestion. Pas de raccordements spéciaux, interrupteurs ou autres moyens localisés : le réseau de communication est lui-même auto-adressable. Tous les objets sont identifiés par des noms, labels et des descriptions personnalisables
- À utiliser : tout est automatisé et intuitif. Aucun langage technique ne doit être assimilé, chaque exploitant personnalise son système comme il l'entend.

Modulaire

- Dans sa structure : il est adapté aux installations modernes du bâtiment, aux réseaux les plus variés et au pré-câblage du bâtiment. Toutes les techniques cohabitent (IP, Token ring, bus, étoile, filaire)
- Dans sa capacité : il grandit au fur et à mesure des besoins. Une extension logicielle ne demande que l'introduction d'un code d'activation libérant les nouvelles fonctionnalités.
- Dans le choix des technologies d'identification : un même système accepte simultanément tous les codages et technologies de badge et de lecteurs. Il contient un programmeur de format.
- Dans les automatismes : tous les types d'obstacles sont pilotés de façon optimale, par scénarii prédéfinis.
- Dans sa capacité de contrôle : on choisit, pour chaque point, s'il sera simple, supervisé, de haute sécurité, ou GTC

Sécurisé

- Dans le réseau reliant les automates au serveur, les liens étant protégés contre la fraude et la substitution.
- Dans les liaisons avec les lecteurs et les capteurs, le système utilise des techniques avancées de traitement des signaux pour atteindre le plus haut niveau de sécurité.
- Dans le codage et le support des badges d'accès : l'utilisation de codes non-déchiffrables et une structure CARD-TAG (fiche de personne – code d'identification) permettent une exploitation aisée sans divulgation du code physique
- Dans la programmation des badges à lecture/écriture (MIFARE® Classic, MIFARE® DESFire EV1/EV2, ...) SCNET4™ permet à l'utilisateur de définir ses clés, ses formats et ses codes.

Avantages techniques

Technologies de badges

SCNET4™ offre une gestion simultanée de multiples technologies de codage de badges, des techniques de proximité classique (HID®, EM™, ...) jusqu'aux badges sécurisés à puce comme MIFARE® DESFire EV2, Calypso™ ou CPS3, en passant par les technologies UHF de type EPC Gen2.

Schéma directeur de sûreté

Celui-ci repose sur le principe de zones de sécurité, qui intègre le contrôle d'accès et l'anti-intrusion. L'exploitation des vues graphiques interactives facilite la télésurveillance. Un éditeur de rapports, accessible par toute station web, sécurisé, aide à la gestion du système

Système ouvert *

L'outil DBSYNC4 synchronise le système avec des bases de données externes. SCNET4REST™, l'API REST garantit un interfaçage aisé vers des systèmes tiers. XPPLUG™ offre un contrôle temps réel du système directement depuis les logiciels de la suite Milestone XProtect®. EVTSRV4™ garantit aussi l'export temps réel d'événements. Enfin, la base de données peut aussi être consultée directement via des requêtes SQL.

Système distribué

L'intelligence et les données de gestion sont distribuées jusqu'au niveau le plus proche des éléments à contrôler. Dès lors, un incident sur un de ces éléments n'influence en rien le reste du système.

Système sécurisé*

L'option SECURE offre au système SCNET4™ le plus haut niveau de sécurité requis pour un système de contrôle d'accès, alliant un chiffrement complet des communications à une gestion sécurisée des badges, de leur contenu et des clés qui les sécurisent.

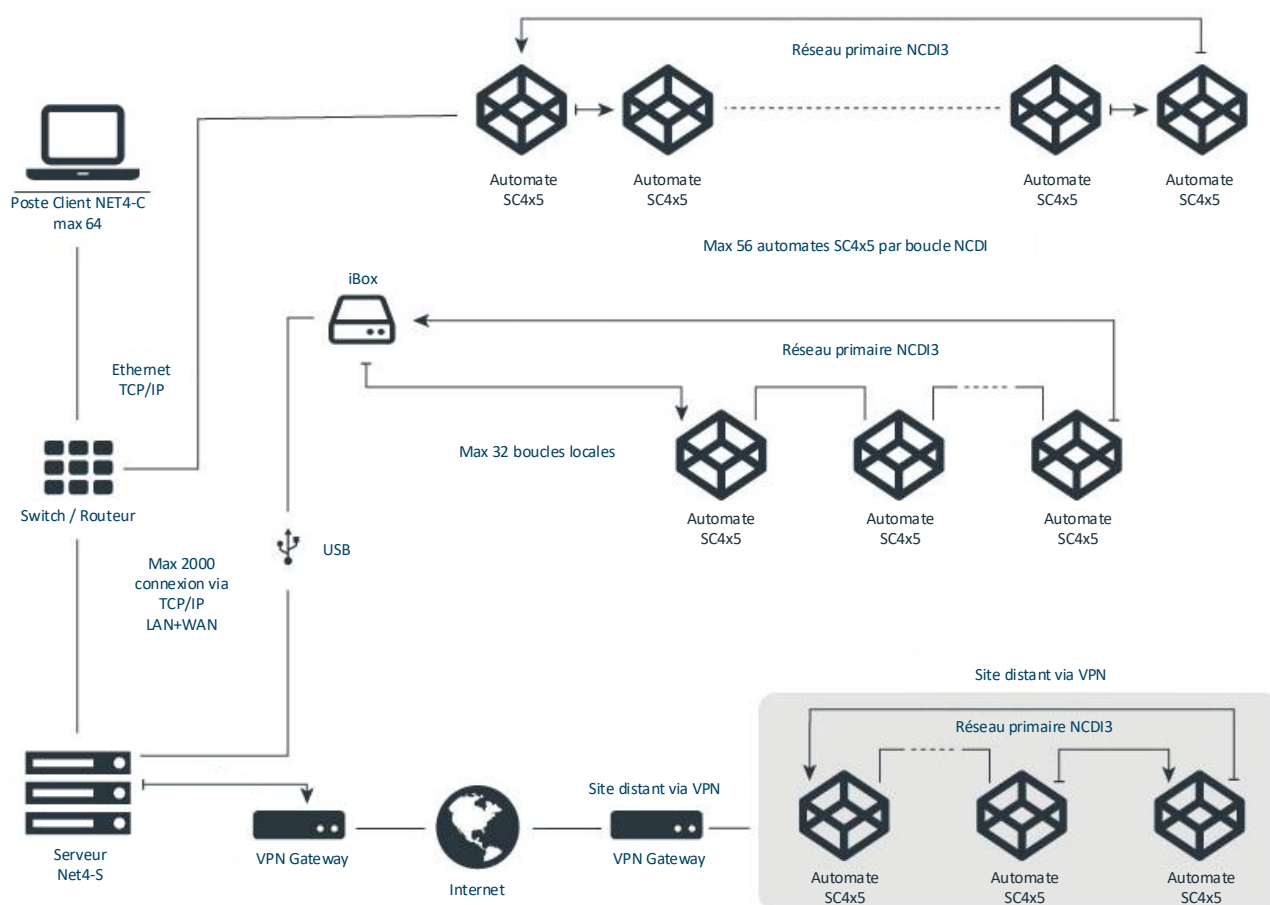
Gestion des badges intégrée*

CARDPROG4™, BADPRT4™ et SECURE™ sont autant d'options du système garantissant une gestion intégrée de la programmation, de l'enrôlement et de l'impression de vos badges de contrôle d'accès pour faciliter votre exploitation du système.

Capacités de SCNET4™

Tags ou badges en librairie	500.000	Événements	10.000.000
Tags ou badges actifs	100.000	Niveaux de priorité d'alarme	4
Accès contrôlés	16.000	Groupes d'accès	1.024
Automates	8.000	Echéanciers	256
Opérateurs	128	Périodes de temps	256
Postes clients	64	Périodes par échéancier	9
Points d'alarme	56.000	Zones de sécurité	2.400
Télécommandes	32.000	Jours de congés	50
Longueur de codage d'un TAG / badge	64 bits 24 caractères 10 chiffres	Technologies et codages de lecteurs simultanés	10

Le réseau SCNET4™



NET4-S™	Serveur de sécurité sous Windows 10™ ou Windows Server 2016
NET4-C™ Client	Postes clients d'exploitation sous Windows 10™ ou Windows Server 2016
SC4x5™	Famille d'automates sous Linux pour le contrôle des accès, alarmes et points techniques

Automates de sécurité

SC4x5™

L'un des plus compacts, l'automate SC4x5™ est aussi parmi les plus puissants. De dimensions conformes aux normes DIN, il est prévu pour un montage sur rail DIN. Les automates SC4x5™ intègrent un processeur ARM® 32 bits de dernière génération opérant sous le système Linux. La mémoire de 192 Méga octets permet de stocker un grand nombre d'informations et de données. De plus, une mémoire SD de plusieurs Giga octets peut y être intégrée*. Les programmes sont rechargeables à partir du serveur centrale ou localement. Les données sont conservées indéfiniment, bien que l'automate ne contienne pas de pile.

Canaux de communication

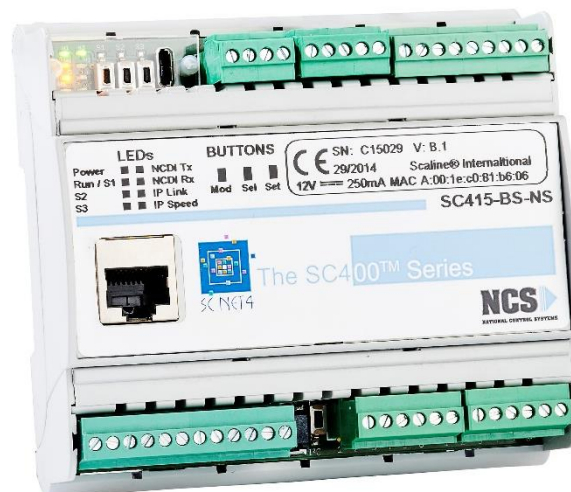
Les automates offrent simultanément des interfaces TCP/IP et filaires, et jouent aussi le rôle de routeurs dans des réseaux mixtes. Le TCP/IP en 10/100 base-T intégré (Réseau Privé, Internet ADSL...) gère aussi le protocole DHCP pour serveur DNS. Il peut aussi fonctionner en PoE*. La sécurisation des communications par l'utilisation du protocole TLS 1.2 et de certificats cryptographiques est une option.

Le canal filaire NCDI3™ est un anneau opto-isolé à jeton à haute vitesse (Jusqu'à 115 Kbauds) et à longue distance (Jusqu'à 1.200 mètres entre nœuds). Il possède des fonctions de (dé-)connexion sans interruption du canal de communication.

Une porte USB 2.0 permet la liaison avec un PC de maintenance, une tablette ou un smartphone de gestion (Interface Web embarquée*) et avec des clés mémoires de chargement

Capacité d'un SC4x5™ **

Tags actifs	100.000	Points d'alarme**	14
Accès contrôlés	4	Etats d'un point d'alarme	8
Lecteurs et/ou claviers	4	Sorties NO/NF	4
Lecteurs par accès	4	Sorties à commande transistor	4
Capacité de la mémoire d'événements	40.000		



Interfaces multiples pour lecteurs de badges

Les canaux de liaison avec les lecteurs de badges sont totalement programmables à partir du système central (Ni cavaliers, ni interrupteurs). Ils peuvent fonctionner en mode Wiegand® (Data0-Data1), en mode Iso2 (Data-Clock), en liaison série RS422 (ex : T=CL pour 14443) ou RS485 (SIA OSDP™, Aperio Online, SSCP™ ou SCDI™ - multi-lecteurs pour Scaline®). Par ailleurs, dépendamment du protocole série, le mode transparent est disponible permettant de dialoguer directement avec les cartes MIFARE DESFire EV1/EV2 ou SmartMX à partir de l'automate sans faire appel à des fonctions de sécurité des lecteurs.

D'autres modes sur mesure sont également programmables. Les modes peuvent cohabiter.

Commande de serrures

La gestion des serrures Aperio® est intégrée** au système dans tous les modes On-line. Jusqu'à 4 serrures Aperio peuvent être connectées par automate. Chaque automate peut gérer un mix de serrures online et de portes câblées.

Entrées d'alarme programmables

Par programmation à partir du système central, chacune des entrées peut être utilisée dans un mode adapté à sa fonction. Le système d'analyse de signaux permet de programmer les états et les seuils tout en veillant à assurer une marge au bruit qui élimine toute fausse alarme.

Un canal secondaire à haute vitesse permet de relier des extensions pour étendre* la capacité de 24 ou 48 entrées et de 16 relais de commande.

Mode	Détection (Une Paire)	Etats
2-S	2 niveaux	Normal-Alarme NO ou NF
3-S	Supervision 3 niveaux	Normal, Alarme, Défaut NO ou NF
6-S	MTM4™ (Multi-Tamper Mode) 6 niveaux	Normal (NO ou NF) Alarme (NO ou NF) Défaut d'autoprotection Rupture de câble Court-circuit de câble
8-S	MTM5™ (Multi Tamper Mode) pour accès	Normal (NO ou NF) Alarme Porte Autoprotection porte Bouton poussoir Autoprotection boîtier Rupture de câble Court-circuit de câble
2-D	Double point	Normal (NO ou NF) 1 et 2 Alarme (NO ou NF) 1 et 2 Rupture de câble Court-circuit de câble

Automatismes évolués de contrôle d'obstacles

Tous les automatismes, du plus simple au plus complexe sont inclus pour le contrôle d'obstacles physiques d'accès :

- Commande unique ou séparée de déverrouillage ou verrouillage dans un ou deux sens de passage
- Réglage de temps d'impulsion, de dé-condamnation, d'ouverture de porte
- Sélection des types de dispositif (émission, rupture de courant, impulsion)
- Séquences de contrôle (barrière, ascenseurs, ...)
- Modes (Surveillés, libre, verrouillé, automatique, ...).
- Contrôle de sécurité positive ou négative
- Surveillance de position.

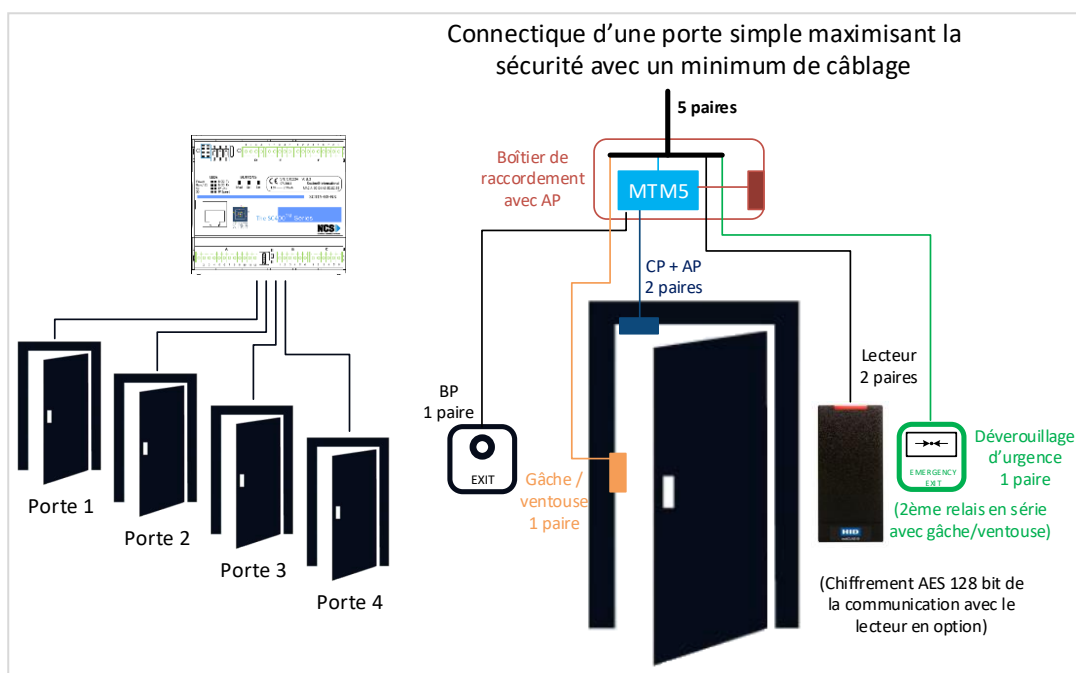
La flexibilité est encore accrue grâce aux fonctions de :

- Commande de blocage en entrée ou en sortie
- Déverrouillage forcé en entrée ou en sortie
- Définition des seuils de comptage pour déclenchement
- Gestion des sas et d'effet de sas

La programmation sélective du SC4x5™ sur échéancier ou événement d'accès ou d'alarme permet de commander des centrales d'alarme, des caméras de surveillance, des exceptions aux règles d'accès pour des groupes particuliers (pompiers, ...)

Maintenance assistée

L'échange de la SIGNATURE électronique de l'automate avec le serveur NET4™ permet de télégréer le parc (type, révision, version, numéro de pièce, ...) et les paramètres de l'installation (Date, clé système, ...)



Gestion des personnes et de l'identification

PSM : People Security Management

SCNET4™ permet d'attribuer des habilitations d'accès en fonction des niveaux de sécurité et de risque. Le contrôle est fonction d'horaires et de zones de sécurité. Le système intègre les outils pour l'accueil des visiteurs et la réservation de ressources (des salles, des parkings...)

Paramètres d'accès

Chaque fiche fait partie d'un ou de plusieurs groupes d'accès. Des groupes d'accès temporaires ou de dérogation sont possibles. L'attribution est guidée par une interface graphique. Les périodes de temps sont définies par jour et par semaine ; le système inclut le passage automatique de l'heure été / hiver et la gestion des congés, des jours fériés, des vacances.

VISIT4™ : Accueil des visiteurs

L'accueil est facilité par des fonctions de préannonce, de gestion des heures d'arrivée et de départ, de recherches multiples dans les fiches des visites antérieures, d'attribution de droits d'accès en fonction de la personne visitée et d'édition de rapports de visites. SCNET4™ inclut l'impression de tickets ou de badges codés.

CARDS & TAGS : fiches et identifiants

SCNET4 distingue les objets :

- Fiche (CARD) : personne, bien identifiable, permanent, temporaire ou visiteur. Les données sont stockées dans des fichiers extensifs comprenant de nombreux champs personnalisables.
- Identificateur (TAG) : badge, étiquette ou transpondeur, caractérisé par un numéro d'identification, une organisation de mémoire, des clés de sécurité, un format, un ou plusieurs codes. L'utilisateur crée la relation entre CARD et TAG par une opération d'enrôlement.

La structure CARD-TAG est déterminante pour assurer l'indépendance des fichiers des personnes et des badges et éviter la divulgation des codes de badges lors de l'accès aux fiches. Elle facilite la gestion de plusieurs technologies de badges comme la corrélation entre les transactions de plusieurs TAGS appartenant à une même personne, cas d'un badge personnel et d'un transpondeur de voiture.

Zones et présence

Le plan de prévention repose sur la division d'un bâtiment en zones de risques. Sa traduction en processus de contrôle est une solution sur mesure réalisée automatiquement par SCNET4™. Le processus est complété de fonctions évoluées d'anti retour local, zonal, périmétrique et temporisé, de gestion d'accès accompagné et de traçage. La prise en compte des présences dans des zones par la gestion d'événements, aboutit par exemple à l'édition automatique de listes de regroupement (Incendie, règle Seveso...).

TSM : Tag Security Management

La gestion des identificateurs pour les personnes, les véhicules, leurs occupants, les biens permet l'utilisation simultanée de plusieurs technologies d'identificateurs et formats de codage. Les outils de fabrication et de programmation ** personnalisent les badges d'identité d'entreprise.

Gestion des badges

SCNET4™ utilise un concept unique de définition du lecteur, du badge et du codage : le KPF™. Celui-ci permet de lire et d'interpréter correctement la trame d'information de tout type de badge.

La librairie standard de SCNET4™ comporte de nombreux KPF et SCNET4™ propose un outil pour définir des KPF sur mesure. Il admet 10 KPF simultanés*, sans risque de doublons. La longueur des codes peut atteindre 24 caractères, 40 chiffres ou 240 bits. SCNET4™ accepte les codages binaires, numériques et alphanumériques. Il s'adapte à tous les lecteurs du marché.

KEY	Clé éventuelle de décryptage ou de désassemblage de l'information
PROTOCOL	Langage dans lequel le lecteur envoie ses Informations
FORMAT	Masque à appliquer pour extraire l'information significative du message

Les modules BADPRT4™, IMAGE4™ et TAGENTRY4™ offrent respectivement des outils de gestion d'impression, de prise de photo d'identité et de communication avec les lecteurs de tables pour l'enrôlement et la programmation des badges.

Gestion de la surveillance

BSM : Building Security Management

La programmation horaire ou événementielle d'automatismes et la commande manuelle à distance permettent à SCNET4™ de gérer le bâtiment en fonction des zones, des droits d'accès, des échéanciers et de la corrélation entre événements.

AUDITTRAIL* - Traçage total

Cette option permet l'enregistrement horodaté et identifié et le suivi de toute modification effectuée dans la base de données d'exploitation et de toute commande

SCNET4™ SECURE

La version SECURE renforce encore la sécurité intrinsèque du SCNET4™ de base.

Dans SCNET4™ SECURE, les liaisons entre les postes informatiques, le serveur et les automates sont sécurisées par le protocole standard TLS 1.2 (Transport Layer Security). La certification des interlocuteurs et la cryptographie à clés publique/privée permet d'intégrer le système dans la politique de sécurité de l'entreprise.

La sécurité des liaisons entre les automates SC4x5™ et les lecteurs d'accès de la gamme est assurée par le chiffrement des échanges (AES) et par la signature de ces échanges. Les lecteurs sont transparents, les clés étant protégées dans les automates. La sécurité de l'accès aux automates par leur serveur web est assurée par le protocole HTTPS.

L'accès au système est sécurisé par l'authentification de chaque opérateur et la hiérarchisation des droits individualisés d'accès aux informations et aux fonctions.

NET4-S™ : Programmeur de macro-commandes

Les macro-commandes de NET4-S™ sont de trois types :

- Les Fonctions : permettent à partir de NET4-S™ d'agir sur le contrôle d'accès, de commander la sécurité et la gestion technique du bâtiment, d'éditer automatiquement des rapports ou de commander un système tiers connecté au SCNET4™
- Les Actions : commandes personnalisées définies à l'avance par l'utilisateur, pour faciliter l'exploitation par les opérateurs
- Les interactions : des scénarii programmables de fonctions (commandes, mise en/hors service, modification des habilitations d'accès, édition,) exécutées soit à un moment prédéterminé, soit en fonction d'un événement ou d'une condition.

Dans le programmeur de NET4-S™, les boucles logiques permettent de créer des scénarii chaînés. Des compteurs système et des chronomètres peuvent être associés à diverses fonctions pour activer l'exécution d'opérations. Le « Language » de programmation est toujours simple et intuitif.

Ces macro commandes peuvent créer des panneaux de commandes sur écran tactile, commander la vidéo-surveillance ou activer le DECT en fonction d'événements.

Gestion de la surveillance

MSM : Monitoring management

La fonction de télésurveillance très complète de SCNET4™ s'applique à la centralisation des états d'alarme d'accès et d'intrusion, de gestion technique et de comptages événementiels. Equipé de vues graphiques interactives, le système gère le suivi de consignes de sécurité et la gestion d'astreintes. L'accès aux informations et aux commandes est personnalisé par opérateur et par station de travail.

Surveillance sécurisée

La sélection des événements à visualiser, à mémoriser et à imprimer et le routage des informations vers des stations sont programmables par zone, en fonction de l'heure, de l'urgence, de la nature ou de la priorité.

Les habilitations d'accès des opérateurs à des fonctions, à des commandes, à des classes de badges sont personnalisables. Elles intègrent la gestion Multi-bâtiments * et Multi-sociétés *. Les écrans d'alarme affichent le contexte et gèrent la prise en compte et l'acquiescement. Ils affichent les consignes de sécurité, les astreintes, gèrent la prise de poste et sécurisent les journaux d'alarme.

La mise en veille de zones de sécurité est automatique, manuelle ou programmée.

GRAPH4™ : Vue graphiques interactives

La création des plans de bâtiment est réalisée par l'outil graphique standard sous Windows10™ ou par l'importation de fichiers Auto-Cad™ ou BMP. Une librairie de symboles (détecteurs, portes, sirènes, lampes, etc.) est fournie, ainsi qu'un outil de création graphique de symboles.

Le placement des symboles sur les plans et leur liaison avec les points créés dans SCNET4™ se font par déplacement de la souris. Bénéficiant d'un zoom avant et arrière illimités, GRAPH4™ permet de commander les éléments de l'installation (Ouvrir, mettre en veille...) directement sur les vues.

WATCH4™ : Rondier de sécurité*

Cette option gère des rondes multiples de plusieurs stations. Une station de pointage est un lecteur d'accès ou toute entrée (commutateurs à clef...). Le système génère une alarme en cas de pointage anticipé ou tardif.

Consultation à distance

SCNET4™ propose un accès sécurisé par navigateur web aux données et aux états du système ainsi qu'à des recherches sélectives.

Analyse d'incidents

Pour faciliter l'analyse d'incidents, le système affiche un événement ancien dans son contexte d'origine.

Rapports

L'éditeur de rapports traite les données du système (fiches, Tags, échéanciers, opérateurs, alarmes et relais etc..), les enregistrements historiques, l'état du système (points en alarmes, détecteurs armés, portes ouvertes, employés présents...). Il inclut un outil de transfert vers des tableurs et un générateur de rapports personnalisés

Journal de bord

Cette application INTRANET permet l'enregistrement de toute information du type « main courante » et son analyse sécurisée.

SMS4™ et EMAIL4™ : messages d'astreintes*

En plus de la gestion d'astreinte standard, ces options permettent l'envoi automatique de messages SMS (Texte) ou de courriels (email). Le choix du correspondant est sélectionné en fonction du type d'alarme et d'un échéancier.

VISION4™ : mode portier vidéo assisté*

Ce mode est activé suivant un échéancier, pour certains accès et certains postes de surveillance ; la demande d'entrée (un badgeage, un bouton d'appel) provoque la présentation des paramètres de la fiche au gardien, y compris éventuellement la photo du demandeur et la commande de la vidéosurveillance. Le gardien décide alors d'accorder ou de refuser l'accès.

Intégration des systèmes

ISM : Integrated Security Management

SCNET4™ s'intègre dans les moyens informatiques de l'entreprise. Il partage les données avec les bases des ressources humaines, les bibliothèques de photos et de plans de bâtiment. Il échange des données et des commandes avec la vidéo surveillance, la télé-surveillance, le contrôle technique du bâtiment (climatisation, GTB...), les systèmes d'appel *.

DBSYNC4™ : Synchronisation de bases de données

L'outil DBSYNC4™ permet la synchronisation du contenu de la base de données du système SCNET4™ avec des données fournies par des systèmes tiers.

Les données extérieures sont fournies de manière brute, sous diverses formes de fichiers ou de données présentées sur des URL. DBSYNC4™ compare le contenu avec celui de la base de données du système SCNET4™ et se resynchronise, propageant automatiquement tous changements vers l'intégralité du système.

Cet interface peut par ailleurs être exécuté de façon totalement automatisé afin d'asservir la gestion des fiches, identifiants et droits d'accès à une base de données maîtresse.

DCOPY4™ : Transfert de fichiers

La fonction DCOPY4™ réalise l'importation sélective de données de personnes par lot, depuis des bases de données existantes, au format ASCII délimité (sources MS Access, MSSQL™, MS Excel™...). Elle réalise l'exportation sélective de données historiques par lot, en format ASCII délimité programmable ou en format NCS SQL™ pour y créer des rapports. L'exécution est commandée par l'opérateur ou programmée automatiquement.

HARMONY : intégration complète avec des systèmes tiers

HARMONY est un concept d'intégration entre le contrôle d'accès, la vidéo-surveillance et toutes les autres techniques de sécurité du bâtiment comme l'alarme intrusion, la sécurité incendie ou la GTC.

Utilisant le plugin XPPLUG™ de NCS permettant de contrôler le système SCNET4™ directement à partir des produits de la suite logicielle Milestone XProtect®, cette intégration permet une reprise simple de tous les événements de sécurité, afin d'en faciliter le suivi et l'analyse et la définition de mécanismes d'interactions complexes entre ces techniques pour réaliser des scénarii complexes de gestion, en phase avec votre politique de sûreté.

EVTSRV4™ : Serveur de messages

EVTSER4™ réalise l'envoi de messages vers des systèmes tiers (serveurs) en fonction d'événements relatifs à SCNET4™ (client).

- Un événement est relatif aux accès (Badge accepté, porte...), aux capteurs (alarme...), aux fonctions (comptage...), au système (anomalie...).
- Le protocole d'envoi est aussi bien une interface série que TCP/IP, ADSL ou un protocole bus

EVTSER4™ assure la liaison avec

- la vidéosurveillance et la gestion technique centralisée
- la gestion des temps de présence,
 - les systèmes d'appel,
 - les centres de télé-surveillance (SIA ESPA444)

SCNET4REST™ : API REST pour le système SCNET4™

SCNET4REST™ fournit une interface d'intégration logicielle vers le système de contrôle d'accès SCNET4™ permettant son intégration dans des applicatifs extérieurs. Qu'il s'agisse de réaliser des modifications sur les usagers, leurs badges, leurs droits d'accès ou encore d'exécuter des commandes sur des objets techniques (portes, relais, points d'alarme, ...), cette interface offre tous les avantages d'une connexion aisée et standardisée vers le système.

La connexion entre le système SCNET4™ peut entièrement être sécurisée à travers l'emploi du protocole https et de token de connexion.

Système et logiciels

Les logiciels serveur et clients de SCNET4™ fonctionnent sous Windows 10™ Professionnel ou Windows Server 2016™ en 32-bits ou 64-bits. Ils utilisent MS SQL2014™, IIS 7.5. Ils sont multilingues

Distribution incrémentale du logiciel

La distribution de NET4™ comprend un CD-Rom contenant toute la librairie des programmes et des documentations, une clé unique de protection et un Wizard d'installation du logiciel. L'individualisation de l'utilisateur et du niveau de licence est réalisée par un code sécurisé d'activation. Chaque licence est donc taillée sur mesure pour chaque besoin d'exploitation. Les extensions sont mises en œuvre par un nouveau code sécurisé d'activation, sans devoir procéder à une nouvelle installation des logiciels (Pré-requis : Contrat de service NCS®).

MODSER4™ : NET4-S™ en mode service

Cette option permet le fonctionnement automatique de NET4-S™ en mode service, compatible VMware, XEN ou Hyper-V.

NET4™ Maintenance : outils et assistance

SCNET4™ possède tous les outils nécessaires à une exploitation aisée. Ils permettent les Backup et la purge de fichiers en ligne, la sauvegarde et la restauration d'historiques, le chargement, la vérification et restauration des bases de données locales. Complétant les outils de diagnostic et de log d'erreurs en ligne, des écrans de maintenance et de diagnostic facilitent la localisation des incidents.

Des outils de maintenance, de télé diagnostic et de restauration d'automates permettent une prise en main totale à distance.

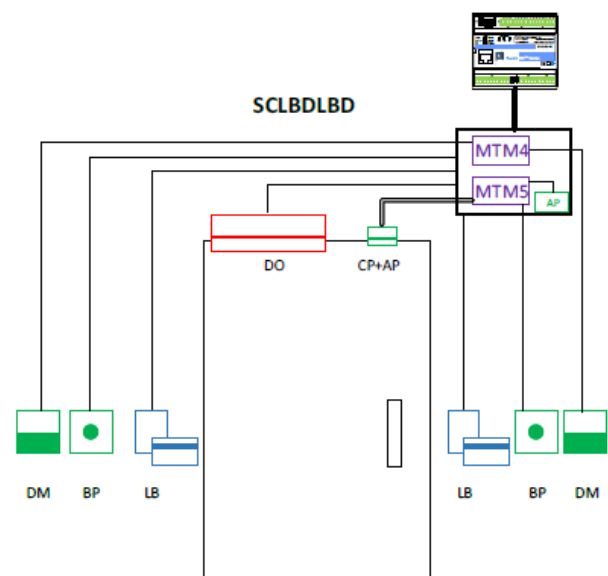
Serveur Web CP5

Par ce WEBServeur embarqué, le paramétrage et la maintenance des SC4x5(TM) et la mise à jour de leur logiciel sont très faciles et peuvent être exécutés à distance.

BUILD™ : méthodologie innovatrice en mise en œuvre

Du synoptique général d'une future installation à la mise en route finale du système installé et programmé, de nombreuses opérations d'étude, d'ingénierie, de traitement d'informations et de documentation sont exécutées. Une coordination totale est indispensable pour assurer la cohérence de la pose, du câblage, du raccordement et du paramétrage avec l'objectif fonctionnel.

La méthode BUILD™ évite les multiples traitements, automatise le transfert de données entre les disciplines (installation et programmation), accélère les processus et supprime les risques d'erreurs. Elle permet de «passer du plan bâtiment à la mise en service en une seule phase»



Exemple de schéma d'une classe fonctionnelle d'accès

NCS® - Spécialiste et innovateur

Depuis plus de vingt-cinq ans, NCS® est constructeur de systèmes de gestion et de contrôle électronique des accès physiques et de sûreté de bâtiment.

Des milliers d'installations de marque NCS® sont opérationnelles dans de nombreux pays. La société compte parmi ses clients des entreprises de l'informatique, des télécommunications, de l'énergie, de la chimie, du pétrole, de la pharmacie, des banques et des assurances, des centres de production, de distribution et de logistique, de nombreux sièges sociaux, des centres de recherche, des institutions internationales, des ministères, des centres hospitaliers, des administrations et des collectivités.

La qualité

des produits de NCS® est garantie par leur conformité vérifiée aux normes les plus sévères. Les produits ont un MTBF élevé. La traçabilité est contrôlée.

Les services

de NCS® sont à la disposition des clients et des partenaires à tous les stades des projets : étude, ingénierie de solutions, stages de formation, assistance technique, service BUILD™, aide à l'exploitation, assistance à la maintenance, « Call Center » d'assistance spécialisée.

Le support

de NCS® s'inscrit dans une politique à long terme. Une installation de sécurité évolue au fil du temps et en fonction des progrès technologiques. NCS® maintient ses produits à la pointe de la technologie en préservant la compatibilité de ses produits et systèmes.



* Non inclus dans la licence de base

** Suivant le modèle ou le type d'installation

La présente description concerne la version 3 de SCNET4™

Ce document constitue un aperçu d'ensemble sans garantie. NCS® se réserve le droit de modifier ses produits et documents sans avis préalable. © 2019 Scaline International

NCS®, le logo NCS® et Scaline® sont des marques déposées de NATIONAL CONTROL SYSTEMS S.A. SCNET4™, NET4™, SC400™, SC4x4™, NCDI™, SCDI™ et Scabus™ sont des marques de NCS®.

LINUX™ est une marque déposée de Linus Torvalds. ARM® est une marque déposée de ARM Holdings Plc. SIA et OSDP sont des marques déposées de la Security Industry Association.

Indala est une marque déposée de ASSA ABLOY AB. Aperio est une marque déposée de ASSA ABLOY AB. EM Microelectronic est une marque déposée de EM Microelectronic-Marin Ltd.

HID, Prox Card II, ISOProx II, iClass, iClass SE sont des marques déposées de HID Global. MIFARE, MIFARE Plus, MIFARE DESFire, MIFARE Classic, et SmartMX sont des marques déposées de NXP Semiconductors N.V.

Microsoft®, Windows®, Internet Explorer® sont des marques déposées de Microsoft Corporation aux Etats Unis d'Amérique et/ou dans d'autres pays du monde.

Intel et Intel Core sont des marques déposées de Intel Corporation aux Etats Unis d'Amérique et/ou dans d'autres pays du monde.

Milestone Systems et le logo Milestone sont des marques déposées de Milestone Systems aux Etats-Unis et dans d'autres pays.

Les autres marques appartiennent à leurs titulaires respectifs.