SMART NITRO SOLUTION

Integrated Security System

V1.5

Introduction

NITRO Group is the well established security solution provider. Our group of company has started the development of our own integrated solution since 2006, and we have the R&D team for access control, video surveillance, alarm monitoring and audio analysis. Our major integration platform includes USP SecNET Door Access, YTMS Pro Time Attendance Management System, Global Monitoring Alarm Monitoring System, and GIM Audio Analysis Management System.

System Application

In our integrated system platform, the major section is USP SecNET Access Control System, and this is the key to interlink all the other sections of the system. The following features of SecNET System would be specific functions for suiting the end-users' need and their concern.

Network Connection and System Design -

USP SecNET and NAC8000N Access Controller would be a flexible TCP/IP network access control system and it can support LAN, WAN, DHCP connection types. With its own unqiue structural design, NAC8000N provides a "Master to Master" communication type for more stable and more applicable security application.

For most of the system, the hardware design would be based on Master and Slave structure. The computer would be the master and the access controller would be the slave, the slave device would mainly follow the instruction from the Master device. In this situation, the slave access controller would have limited function and a bit slower response time. If both of the access controller and the computer server would act as master, they can work individually and provide more flexible functions.

USP SecNET access control server and the NAC8000N access controller would both be in master operation mode, and they can actively communicate with each other. By using this system structure, not only the SecNET server computer can search and connect to the hardward device, but also the NAC8000N can search the SecNET server in the internet directly. NAC8000N would have the ability to actively search the computer server, this can save the number of fixed IP required in the system if there would be quite a number of access controller in different areas. Also, if some of the areas would only be able to use the mobile network (eg. 3G, GPRS), the fixed IP would not be available for usage, then only the Master/Master structurual system can be applied in the application.

Network Protection -

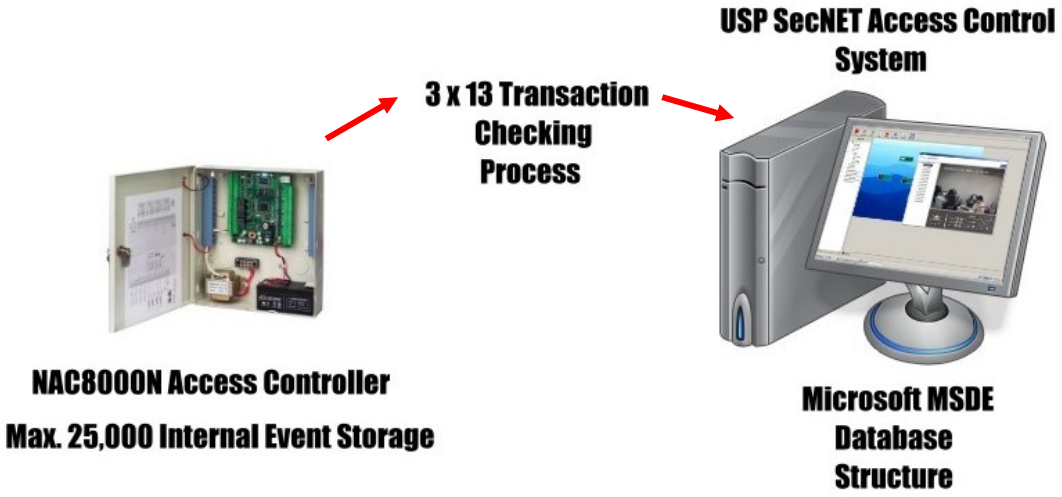
Network access control system would make use of the common TCP/IP communication protocol, most of the users would concern the security level of the system. In the NITRO NAC8000N, the system design has varies security design for network protection, so as to provide a stable operation environment for the users. The operation system would not be Windows or Linux-based, it would not be attacked by the computer virus, and this would be one of the advantages of using the specific OS.

In order to maintain the network stability, NITRO NAC8000N would have the design of “Network Auto Reconnection”. If there is any network connection problem of a Window-based computer, user would request to recover it manually, and this would be the same situation for most of the network based hardware devices. As the structure of NAC8000N access controller would be a Master control device, it would have the ability to determine the status of network environment. When the network is not favourable for system application by trial testing three (3) times of the TCP/IP connection, controller would disconnect the network and then reconnect it automatically. This can obviously help the system installer and the user for the maintaining the system in good condition.

For the same situation, NITRO NAC8000N would also be able to detect any network attracking by mass volume of network packet travelling. If this case happens, access controller would stop its internal network to prevent any chance of damage until the network problem has been fixed by the users or the IT department.

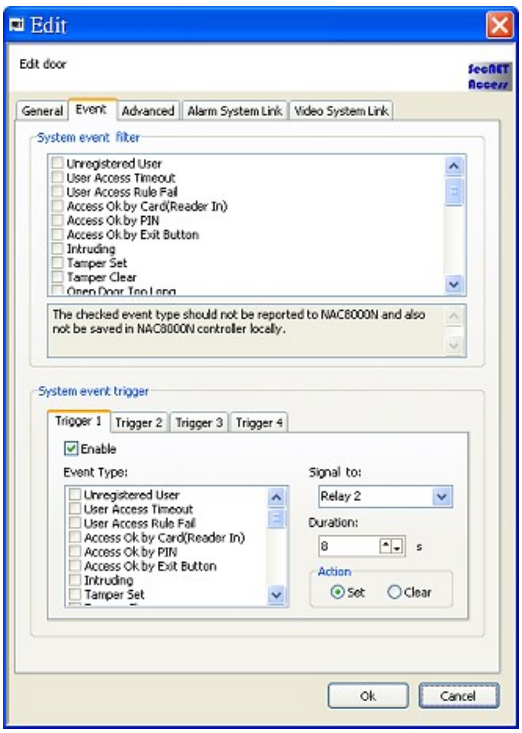
3 x 13 Transaction/ Event Protection -

Most of the users may have faced the problem of transaction/event loss during the usage of access control system, and the reason would not be easy to be found out. This can be a serious problem especially for the case of using time attendance application and the company concerning the staff behaviour. For preventing the situation of event loss, NAC8000N Master mode would undergo a unique “3 x 13 Transaction Confirmation” process. NAC8000N access controller would send the transaction or event to the SecNET server computer. Each of the transaction would be checked for 3 times before saving in the Microsoft MSDE database file, and each time of checking must fulfill 13 conditions and requirements for ensuring the transaction to be saved completely. This is one of the unique features of NITRO SecNET system for high security application.

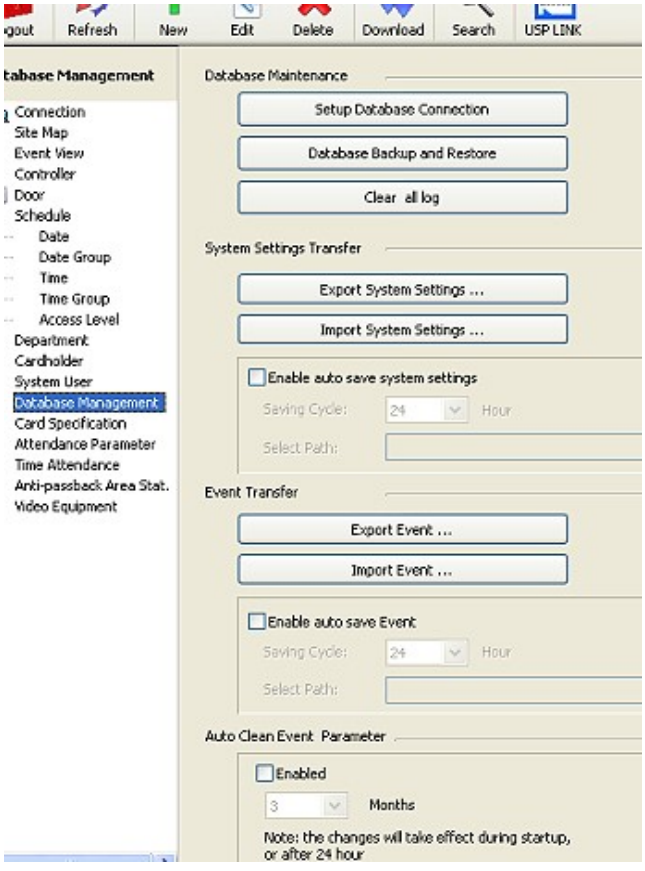


Memory/ Database Management -

Apart from the “3 x 13 Transaction Confirmation” technology, NAC8000 access controller would have the hardware memory management function for customizing the event filter function. Controller stores up to 30 types of different events, users would be able to filter the event type which would not be applicable for the actual usage. This can save the internal memory for recording those more important events.



There would be varies methods to maintain the MS MSDE database system, including both manual and auto database backup. Users can easily decide the most suitable way for keeping the required setting and the transaction/event.



High Security Door Access Function -

In the SecNET door access system, it would support varies advanced features for better control of the security level. For the lower security level requirement, users can use only the password (public pin or private pin) for door access management. The system can also support “Door Hold Per Request” function. After the door has been opened by proper access right, the door will keep the open state until the end of the pre-defined time schedule. These two methods would be the most convenient way to apply the simple door access system for the users, and the security level of them would be comparatively low.

Using the access card with different combination of functions can provide higher security applications, eg. bank, warehouse and countinghouse. These functions would include the sections as below.

i) Hardware Protection – Sector Management – Specific Reader and Card Format
ii) Multi-Card Control
iii) Remote Control – Access Card + Video + Voice Confirmation

****** Sector Reader Management -***

Sector reader is one of the major technology developed by NITRO Security. We have designed a specific card reading method for checking and verifying a predefined card sector and encrypted code. The whole process of card scanning would be highly protected, and only the pre-programmed card can be accessed by the sector reader. By using this technology, there would be benefit security protection, prevention of reading unauthorized access card for not giving unwanted card number output, customization of card number per system request, and usage of user defined site code. We concern much more than what the users want.

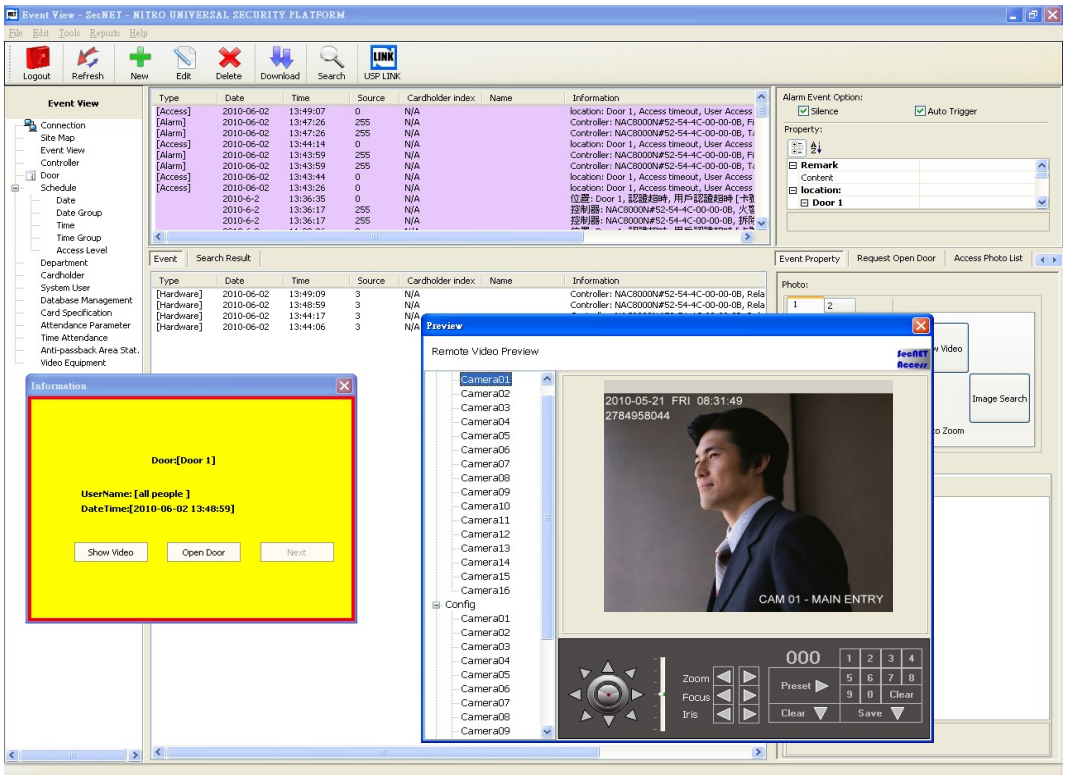
*** Multi-Card Control -

Multi-Card management is the common feature using in the high security areas, eg. warehouse with high value products and countinghouse. Within a predefined time period, it is needed to have more than one access card successfully completing the access right checking, otherwise the door cannot be opened. NITRO USP SecNET system would accept from two (2) to eight (8) multi-card management, it can support at most 8 persons using different access card to scan the reader with each of the them 10s time period. If anyone of them cannot complete the process, it should retry the whole process of 8 persons card access again.

*** Remote Control – Access Card + Video Confirmation -

Remote control is one of the functions which must have a guard operating the SecNET access control server. When the user scans the access card from the reader, NAC8000N would firstly check with the guard before opening the door. The guard would receive the request from the user, they can view the live video of the corresponding door. If it is needed, the guard can activate the voice talk function to check the user. The whole process would be done via the TCP/IP network, and it is not needed for too much extra wiring. There would be a short-cut key for the guard to open the door after confirmation of the user access right.

This application would be used for bank and treasury, and it should include a high security alarm and CCTV monitoring system and a team of security guard.



***Remote Video Confirmation feature depends on the model of DVR used. ***

Integrated Alarm Monitoring System -

For the traditional burglar alarm system, operator can use a specific code for arm or disarm the sytem. This application would be certain limitations.

i) it cannot prevent the disclose the arm/disarm code to other persons by human factors;

ii) the arm/disarm code would normally be long and complicated. Operator may sometime not easy to remember the code.

iii) there would be no record for the person who arm or disarm the alarm system.

To provide an alternative or better choice to the user, NITRO factory has designed for “Card + Pin” arm/disarm function. User would be able to choose high security mode or easy operation mode. To use the high security mode, each operator should use their own access card together with a specific predefined code to arm/disarm the system. Without the card, no any person can operate the alarm system even in the case of knowing the code. Easy operation mode can allow the operator using a very simple code or pin to arm/disarm the system with their own access card. This can prevent any cases of forgetting the code or password.

“Card + Pin” arm/disarm function would be clear indication on the NITRO NR series access control reader. After arming the system, the LED of the reader would change from red to green, so as to easy checking the status of the alarm system.

Disarm Status (RED LED) **Arm Status (GREEN LED)**

Cloakwise Extra Protection -

In the normal intruder sensing application, the passive infrared (PIR) would detect the motion of the human. For some of the specific case, the intruder would attempt to mask discovery by heat reflecting materials which can cover himself. Dual-tec sensor would also need to firstly detect the object using passive infrared, and if the intruder uses the specific umbrella or protective coating, then the alarm detection function may not work properly.

Cloakwise is a proprietory detection algorithm for distinguishing the presence of an intruder even if the unauthorized person attempts to or “cloak” their presence. Utilising advanced signal processing techniques to both microwave and PIR channels, the ***Cloakwise*** technology can recognize masking attempts and detect accordingly. By always analyzing both PIR and microwave sources with the best balance of sensitivity and stability, the ***Cloakwise*** is a ***TRUE Dual-Tec*** alarm monitoring detection function. With its exceptional stability and false alarm immunity ability, ***Cloakwise*** can the secure solution for varies installation environment.

SMART NITRO SOLUTION would integrate all the access control, alarm monitoring and CCTV video surveillance for providing all the required functions to the users.

For any further detailed information, please contact support@nitrosec.com .