

Tomasz ZAUDER
Instytut Systemów Sterowania

SIECIOWY SYSTEM KONTROLI DOSTĘPU NA BAZIE TECHNOLOGII LONWORKS^{*)}

Streszczenie. Referat prezentuje wyniki projektu badawczego pn. „Otwarty Sieciowy System Komunikacyjny integrujący automatyzację budynku” w zakresie kontroli dostępu.

Zaprezentowany system kontroli dostępu, dzięki zastosowaniu sieci komunikacyjnej i sterowania na bazie technologii LonWorks, jest systemem otwartym, modułowym i łatwo rozbudowywalnym.

System kontroli dostępu po zaprojektowaniu, doświadczalnym uruchomieniu i przetestowaniu został wdrożony w zakładzie przemysłowym.

THE NETWORK ACCESS CONTROL SYSTEM BASED ON THE LONWORKS TECHNOLOGY

Summary. The paper shows the results of a research project entitled 'Open Network Communication System integrating the building automation' in the field of access control.

The presented access control system is an open, modular and easily extendable system, thanks to the application of an automation and control network that is based at the LonWorks technology.

The access control system was, after the design, experimental start-up and test, implemented in an industrial plant.

^{*)} Praca została wykonana w ramach projektu celowego zamawianego nr PCZ 13-18 finansowanego przez Ministerstwo Gospodarki i Komitet Badań Naukowych.

1. Wprowadzenie

W nowoczesnym budownictwie, poza typowymi instalacjami elektrycznymi i sieciami komputerowymi oraz instalacjami systemów bezpieczeństwa przeciwpożarowego, spotyka się coraz częściej systemy automatyki mające na celu ograniczenie zużycia energii, poprawę komfortu i zapewnienie bezpieczeństwa. Do tego typu systemów należą, przede wszystkim, systemy sterowania ogrzewaniem, oświetleniem, klimatyzacją i wentylacją oraz systemy kontroli dostępu.

Budynkami wyposażanymi w takie systemy są głównie biurowce przeznaczone na wynajem pomieszczeń dla wielu różnych firm. Niemniej jednak, rośnie liczba nowych i modernizowanych budynków mieszkalnych o podwyższonym standardzie, w których inwestorzy decydują się na stosowanie systemów automatyki. Nierzadko właściciele prywatnych nieruchomości wdrażają systemy automatyzacji w swoich domach i rezydencjach.

Nowoczesne technologie w zakresie sieci komunikacyjnych i sterowania stwarzają możliwości projektowania, budowy i wdrażania jednolitych systemów obejmujących wszystkie funkcje związane z automatyką budynkową; do niedawna poszczególne podsystemy, pochodząc zazwyczaj od różnych dostawców, bazowały na różnych technologiach i gromadzenie informacji, pochodzących z tych podsystemów, w jednym miejscu (na stacji operatorskiej) wymagało ogromnego wysiłku ze strony integratora systemów.

Jednym z najczęściej stosowanych systemów automatyzacji budynków jest system kontroli dostępu, którego funkcja zapewnienia bezpieczeństwa ludzi i mienia w budynku wyznacza mu kluczową rolę w automatyzacji budynku.

System kontroli dostępu może być jedynym zastosowanym systemem, a w przypadku kompleksowej automatyzacji budynku będzie jednym z pierwszych wdrożonych.

Referat prezentuje wyniki projektu badawczego pn. „Otwarty Sieciowy System Komunikacyjny integrujący automatyzację budynku” w zakresie kontroli dostępu. W ramach tego projektu został opracowany inteligentny system automatyzacji budynku o nazwie SABIO na bazie technologii LonWorks [1, 2], którego podsystemem jest system kontroli dostępu.

2. Technologia LonWorks

Technologia LonWorks została opracowana przez amerykańską firmę Echelon z zamysłem szerokiego zastosowania w różnych dziedzinach techniki.

Technologia LonWorks umożliwia tworzenie sieci sterowania charakteryzujących się niskim kosztem implementacji i dużą elastycznością rozwiązań. Do projektowania, realizacji i eksploatacji sieci LonWorks służą środki techniczne obejmujące wszystkie niezbędne elementy: mikroprocesorowe układy scalone Neuron zawierające pamięć z zaimplementowanym protokołem komunikacyjnym LonTalk, układy interfejsowe do różnych mediów transmisji (skrętka, światłowód, fale radiowe, przewody zasilania w energię), rutery, oprogramowanie uruchomieniowe. Protokół LonTalk zaprojektowany został w celu niezawodnego przesyłania krótkich komunikatów sterowania. Umożliwia rozproszoną komunikację typu peer-to-peer. Sieć składa się z inteligentnych węzłów (urządzeń bezpośrednio przyłączonych) realizujących funkcje zbierania danych, sterowania i komunikacji z innymi węzłami sieci [3, 4, 5].

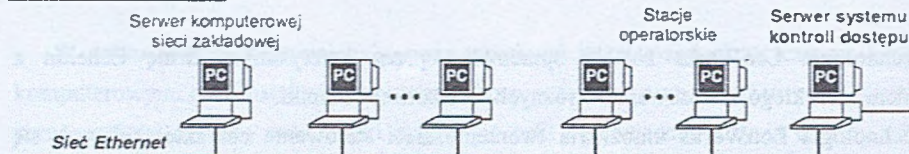
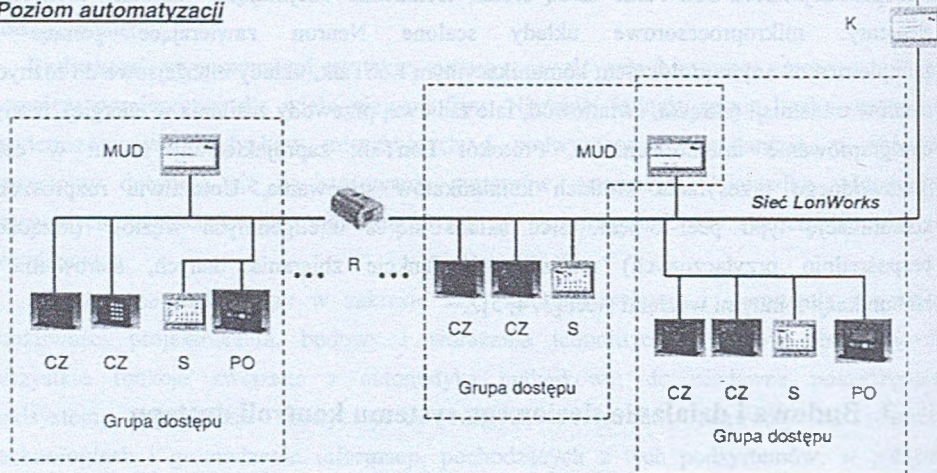
3. Budowa i działanie sieciowego systemu kontroli dostępu

3.1. Budowa systemu

Prezentowany system kontroli dostępu ma budowę dwupoziomową (rys. 1) – obejmuje poziom zarządzania i poziom automatyzacji [6]. W związku z taką budową również określenie systemu jako 'sieciowy' ma podwójne znaczenie, gdyż na każdym poziomie istnieje odrębna sieć, służąca do wymiany informacji. W przypadku poziomu zarządzania jest to sieć Ethernet, a w przypadku poziomu automatyzacji sieć LonWorks.

Poziom zarządzania obejmuje stacje operatorskie systemu, będące komputerami typu PC przyłączonymi do zakładowej sieci komputerowej Ethernet. Jedna ze stacji pełni funkcję serwera systemu kontroli dostępu, na którym zainstalowana jest wielodostępna baza danych. W bazie gromadzone są dane przychodzące z sieci LonWorks. Na serwerze i na pozostałych stacjach operatorskich znajduje się oprogramowanie aplikacji użytkowej służące do obsługi systemu kontroli dostępu. Oprócz stacji operatorskich w sieci Ethernet działają inne komputery i serwery. Na wyznaczonym serwerze sieci zakładowej serwer systemu kontroli dostępu tworzy kopię bezpieczeństwa swojej bazy danych.

Aplikacja użytkowa systemu może współpracować z modułem „Kadry-Płace” systemu zarządzania przedsiębiorstwem i wymieniać z nim informacje typu spis pracowników, bilans czasu pracy (w przypadku rozszerzenia systemu kontroli dostępu o rejestrację czasu pracy).

Poziom zarządzaniaPoziom automatyzacji

K – Konwerter LON-RS232
 MUD – Moduł Upewnien Dostępu
 R – Ruter

CZ – Czytnik
 S – Sterownik
 PO – Panel operatorski

Rys. 1. Struktura systemu kontroli dostępu

Fig. 1. The structure of the access control system

Poziom automatyzacji obejmuje sieć sterowania LonWorks i węzły sieci. Węzły pod względem funkcjonalnym tworzą grupy, które lokalnie zarządzają dostępem do pomieszczeń i obszarów chronionych. W skład grup funkcjonalnych wchodzi czytniki identyfikatorów (stykowe, zbliżeniowe), sterowniki (drzwi, bramek, kołowrotów), panele operatorские (zadajniki i nastawniki), moduły upewnien dostępu. W systemach, gdzie występuje duża liczba grup funkcjonalnych, konieczny jest podział systemu na podsieci, które są połączone ze sobą za pomocą ruterów.

Rolę sprzegającą oba poziomy spełnia serwer systemu kontroli dostępu wyposażony w interfejs do sieci LonWorks. Interfejsem może być specjalizowana karta komputerowa (np. PCLTA-10), karta podłączona do portu szeregowego (SLTA-10) albo konwerter (LON-RS232) dołączony do portu RS232.

Komunikacja w sieci sterowania odbywa się przy użyciu medium transmisyjnego, którym jest para przewodów skręconych. Wszystkie węzły wyposażone są w specjalizowany interfejs – transiwer FTT-10A, poprzez który przyłączone są do sieci LonWorks. Szybkość transmisji wynosi 78 kbit/s.

Technologia LonWorks, pozwalając stosować dowolną topologię sieci sterowania, daje projektantom i wykonawcom dużą swobodę w tworzeniu systemów najlepiej dopasowanych do potrzeb użytkowników.

W skład systemu mogą wchodzić następujące rodzaje węzłów:

- czytniki: zbliżeniowe, zbliżeniowe z klawiaturą, stykowe typu pastylka, stykowe elektroniczne (chipowe), stykowe magnetyczne; (w szczególnym przypadku czytnik może być urządzeniem bezpośrednio przyłączonym do sterownika),
- sterowniki: drzwi, bramek, kołowrotów, alarmów,
- panele operacyjne,
- moduły uprawnień dostępu,
- karty sieci LonWorks,
- konwertery LON-RS232,
- rutery.

Czytniki

Czytniki służą do odczytu zapisanej w identyfikatorze informacji i przesyłu jej do innych urządzeń (sterowników lub modułów uprawnień dostępu). Czytniki mogą być węzłami sieci LonWorks lub urządzeniami bezpośrednio przyłączonymi do sterowników. Technika odczytu informacji z identyfikatorów może być dowolna, jednakże w danym systemie zaleca się stosowanie tylko jednego typu czytników i identyfikatorów.

Identyfikatory

Identyfikatorami są dowolnego typu, kształtu i rozmiaru nośniki informacji, jednoznacznie określające właściciela identyfikatora. W przeważającej liczbie przypadków identyfikatory mają postać karty. Informacja zapisana w identyfikatorze może mieć charakter zmienny albo stały. W pierwszym przypadku w identyfikatorze wpisany jest numer, który składa się z części zawierającej oznaczenie systemu i części określającej użytkownika. W

drugim przypadku identyfikatory posiadają niezmienny numer wpisany na etapie produkcji. Jest to kolejny, unikalny numer identyfikatora danego typu.

Sterowniki drzwi, bramek, kołowrotów

W systemie sterowniki regulują ruch osób w zakresie kontroli dostępu. Współpracują z czytnikami i modułami uprawnień dostępu. Z czytników otrzymują numer identyfikatora, który następnie przesyłają do modułu uprawnień dostępu, gdzie następuje jego weryfikacja. Na podstawie informacji zwrotnej z modułu, sterownik decyduje o zezwoleniu na przejście (zwolnienie blokady bramki, kołowrotu) lub dostęp (wysterowanie elektrozaczełu drzwi) albo uruchamia alarm, gdy okazuje się, że odczytany numer identyfikatora nie należy do systemu bądź nie ma prawa dostępu w określonym miejscu.

W przypadku sterownika drzwi dołączony jest do niego bezpośrednio czujnik ruchu umieszczony wewnątrz pomieszczenia lub budynku, elektrozaczeł i buczeł. Zadaniem czujnika ruchu jest poinformowanie systemu o osobie zbliżającej się do wyjścia z pomieszczenia lub budynku. Dzięki tej informacji, system nie traktuje otwarcia drzwi od wewnątrz jak włamania. Elektrozaczeł jest elementem wykonawczym, a buczeł pełni funkcję alarmową w przypadku prób nielegalnego dostępu.

Sterowniki kołowrotów i bramek dołączane są do układów automatyki kołowrotów lub bramek i poprzez te układy pełni funkcje sterujące.

Sterownik alarmów

Zadaniem sterownika alarmów jest informowanie strażników o powstaniu alarmów (włamanie do pomieszczenia, próba nielegalnego dostępu) w konkretnym miejscu obiektu objętego przez system kontroli dostępu.

Panele operatorskie

Panele pełni rolę interfejsu użytkownika z systemem na poziomie automatyzacji. Są wyposażone w alfanumeryczny wyświetlacz i przyciski. W systemie kontroli dostępu służą do ręcznego wprowadzania rozkazów sterujących, np. blokowania lub odblokowywania kołowrotów.

Moduły uprawnień dostępu

Moduły pełni rolę koncentratorów informacji na poziomie automatyzacji. W swojej pamięci przechowują dane o ważnych identyfikatorach oraz zapisują zdarzenia zaistniałe w systemie, np. odczyty identyfikatorów, alarmy. Dane o identyfikatorach otrzymują ze stacji

operatorskiej. Zdarzenia są zapisywane we współpracy ze sterownikami, które przesyłają numery identyfikatorów do weryfikacji oraz zgłaszają wykryte nieprawidłowości.

Po nawiązaniu komunikacji ze stacją operatorską (serwerem systemu kontroli dostępu) moduły uprawnień dostępu, z udziałem konwertera albo karty sieci LonWorks, przesyłają do niej zgromadzone dane o zdarzeniach.

Karty sieci LonWorks

Karty spełniają rolę interfejsu pomiędzy siecią LonWorks a stacją operatorską serwera systemu KD. Mogą mieć postać specjalizowanej karty komputerowej (np. PCLTA-10) lub karty podłączanej do portu szeregowego komputera (SLTA-10). Karty umożliwiają wymianę informacji pomiędzy węzłami sieci a aplikacją użytkową na stacji operatorskiej.

Konwertery LON-RS232

Pełnią rolę interfejsu pomiędzy siecią LonWorks a serwerem systemu kontroli dostępu poprzez port szeregowy RS232 stacji. W sieci sterowania komunikują się z modułami uprawnień dostępu. Z modułów otrzymują informacje o zdarzeniach, które przekazują na stację, a ze stacji do modułów przesyłają zaktualizowane dane o ważnych identyfikatorach.

Rutery

W przypadku systemów o liczbie węzłów większej od określonej dla danego typu transiwera (np. 64 dla węzłów z transiwerem FTT-10A) konieczna jest segmentacja sieci i zastosowanie ruterów, które pełnią funkcję separatorów poszczególnych segmentów sieci sterowania. Rutery, z jednej strony, wzmacniają sygnały ogólnosieciowe przez nie przechodzące, a z drugiej, są filtrami dla informacji wykorzystywanych tylko w jednym segmencie.

3.2. Działanie systemu

Głównym zadaniem systemu jest zapewnienie bezpieczeństwa osobom i mieniu znajdującym się w pomieszczeniach lub obszarach objętych kontrolą dostępu.

System umożliwia dostęp do chronionych obiektów i pomieszczeń oraz przejście w określonych miejscach osobom uprawnionym, posiadającym ważne identyfikatory. Wykryte przez system próby nielegalnego dostania się do obszarów objętych nadzorem są alarmowane i pozwalają strażnikom na odpowiednie zareagowanie.

Informacje o zezwoleniach na dostęp oraz próbach nielegalnego dostępu muszą być gromadzone w celu ich późniejszej analizy.

Funkcje systemu można podzielić na wykonywane na poziomie zarządzania i na poziomie automatyzacji.

Poziom zarządzania

Ogólne funkcje aplikacji użytkowej:

- zapis zdarzeń z sieci LonWorks do bazy (np. odczyty identyfikatorów, informacje o alarmach),
- zapis danych z bazy na sieć LonWorks (np. uaktualnienie listy ważnych identyfikatorów),
- centralne zarządzanie systemem (definiowanie operatorów i ich praw dostępu do określonych funkcji aplikacji),
- rejestracja czasu pracy z aplikacją przez poszczególnych operatorów i zmian przez nich dokonywanych,
- komunikacja z serwerem zakładowej sieci komputerowej i tworzenie na nim kopii bazy danych systemu kontroli dostępu.

Funkcje przetwarzania danych:

- wprowadzanie, usuwanie osób objętych przez system, numerów identyfikatorów, urządzeń (czytników, paneli), elementów struktury zakładu (np. wydziałów, grup pracowników), stref dostępu,
- stała lub czasowa blokada użycia identyfikatora,
- uwzględnianie informacji o okresowych zmianach w czasie pracy pracowników (np. urlopy, zwolnienia lekarskie) w określaniu praw dostępu,
- tworzenie raportów zdarzeń związanych z uprawnionymi przejściami,
- tworzenie raportów sytuacji nieprawidłowych i alarmowych,
- tworzenie raportów dotyczących ręcznych sterowań bramek i kołowrotów dokonywanych przez strażników za pomocą paneli operatorskich,
- archiwizacja danych i możliwość ich późniejszego przeglądania.

Poziom automatyzacji

- odczyt identyfikatorów, sprawdzenie ich uprawnień i przesłanie informacji o odczycie na serwer systemu kontroli dostępu,
- zwolnienia blokad drzwi, bramek lub kołowrotów po odczycie identyfikatorów osób uprawnionych do dostępu lub przejścia w danym miejscu,
- alarmowanie niedozwolonych prób przejścia przez drzwi, bramki lub kołowroty,

- ręczne blokowanie i odblokowywanie bramek lub kołowrotów za pomocą paneli operatorskich,
- sygnalizacja trybu pracy bramek lub kołowrotów.

Węzły sieci sterowania, realizujące funkcję dostępu w obrębie jednego przejścia (drzwi, bramki, kołowrotu) są ze sobą związane logicznie, tworząc najmniejszą funkcjonalnie pełną jednostkę systemu. Te jednostki tworzą osnowę działania systemu i nazywają się grupami funkcjonalnymi. W dostępie do pomieszczenia, na przykład, grupa funkcjonalna składa się ze sterownika drzwi, czytnika identyfikatorów i modułu uprawnień dostępu. Każdy moduł uprawnień dostępu, z racji swojej roli, jest zazwyczaj elementem wspólnym kilku grup funkcjonalnych, ponieważ może współpracować z ośmioma sterownikami.

Liczba grup funkcjonalnych i ich konfiguracja sprzętowa zależą od konkretnych potrzeb obiektu objętego systemem kontroli dostępu. Wobec tego, system może składać się z grup dostępu do zakładu, budynku, pomieszczeń. Każda grupa działa niezależnie od pozostałych i uszkodzenie któregośkolwiek elementu jednej grupy nie powoduje zakłóceń w funkcjonowaniu pozostałych. Wyjątek stanowi moduł uprawnień dostępu, ponieważ może należeć do kilku grup funkcjonalnych.

Poziom automatyzacji funkcjonuje autonomicznie – niezależnie od poziomu zarządzania. Wyłączenie stacji operatorskich nie wpływa na działanie węzłów sieci sterowania wykonujących zapisane w ich pamięciach programy.

Sieć sterowania i jej segmenty zasilane są napięciem 24V DC. W celu zapewnienia działania systemu przez konieczny czas, w przypadku zaniku napięcia elektrycznego, zasilanie systemu powinno być podtrzymywane bateryjnie lub przez akumulatory.

4. Przykład zastosowania

System kontroli dostępu, uzupełniony o rejestrację czasu pracy, został wdrożony w zakładzie przemysłowym.

W systemie na poziomie zarządzania znajduje się jedna stacja operatorska, pełniąca funkcję serwera systemu kontroli dostępu, dołączona do ogólnozakładowej sieci komputerowej Ethernet poprzez kartę, a do sieci sterowania LonWorks poprzez konwerter LON-RS232. Na stacji znajduje się aplikacja użytkowa, która oprócz funkcji związanych z kontrolą dostępu obsługuje również rejestrację czasu pracy łącznie z przesyłem miesięcznych danych bilansowych o czasie pracy pracowników do zakładowego systemu kadrowo-płacowego znajdującego się na odrębnym komputerze podłączonym do sieci Ethernet.

Aplikacja współpracuje z serwerem sieci komputerowej, na którym tworzy kopię swojej bazy danych.

Poziom automatyzacji stanowi sieć sterowania LonWorks i 25 węzłów, którymi są: czytniki kart zbliżeniowych, panele operatorskie, sterowniki drzwi i kołowrotów, sterownik alarmów, konwerter, moduły uprawnień dostępu. Węzły sieci działają w grupach funkcjonalnych, które w miejscu swojej lokalizacji realizują zadania związane z kontrolą dostępu lub rejestracją czasu pracy oraz wymieniają między sobą informacje. Moduły uprawnień dostępu komunikują się ze stacją operatorską.

W systemie zastosowano topologię magistrali sieci. Jako medium transmisyjne wybrano kabel czterożyłowy, ekranowany. Szybkość transmisji wynosi 78 kbit/s.

Czytniki kart umieszczono przy drzwiach i kołowrotach. Odczyt uprawnionej karty powoduje zezwolenie na wejście do strefy chronionej budynku, wejście do pomieszczenia przez drzwi lub przejście przez kołowrót. Na portierni znajduje się czytnik z klawiaturą służący do rejestracji wyjść służbowych, które wymagają wprowadzenia kodu przez strażnika przed odczytem karty.

Karty zbliżeniowe, będące identyfikatorami, są podzielone na kategorie: pracownicy, praktykanci, usługodawcy i goście. Poszczególne karty mają różny czasowo i terytorialnie charakter dostępu.

Panele służą do ręcznego blokowania i odblokowywania kołowrotów.

Sterowniki drzwi we współpracy z czytnikami realizują kontrolę dostępu do budynku (2 wejścia) i pomieszczeń (4 wejścia). Do sterowników bezpośrednio przyłączone są urządzenia współpracujące: zaczep elektromagnetyczny, czujnik otwarcia drzwi i czujnik ruchu umieszczony wewnątrz pomieszczenia lub budynku. Czujnik ruchu informuje system o osobie zbliżającej się do wyjścia z pomieszczenia lub budynku, dzięki czemu system nie traktuje otwarcia drzwi od wewnątrz jako włamania.

Sterowniki kołowrotów we współpracy z czytnikami realizują kontrolę dostępu do zakładu (2 przejścia). Każdy sterownik jest dołączony do układu automatyki kołowrotu i poprzez niego steruje kołowrotem.

Na portierni znajduje się sterownik alarmów informujący strażników wizualnie i dźwiękowo o alarmach powstałych w grupach funkcjonalnych.

Grupy funkcjonalne

W systemie jest 10 grup funkcjonalnych:

- 2 grupy dostępu do zakładu,
- 2 grupy dostępu do budynku,
- 4 grupy dostępu do pomieszczeń,

- 1 grupa wyjścia służbowego,
- 1 grupa sterownika alarmów.

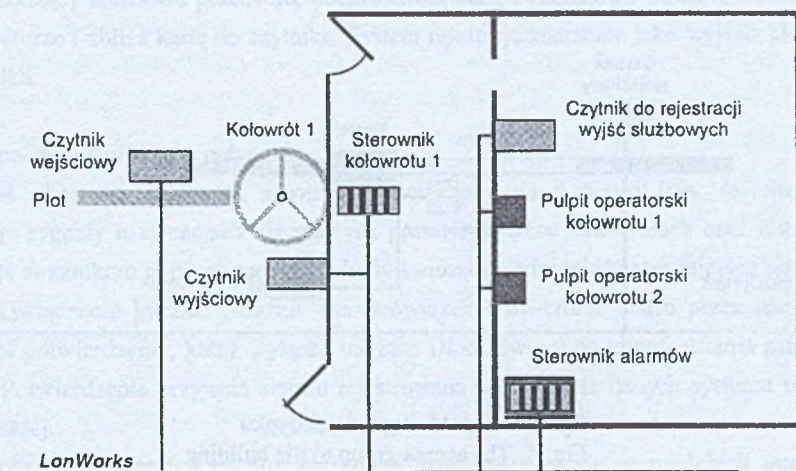
Grupy dostępu do zakładu i grupa wyjścia służbowego, oprócz kontroli dostępu, obsługują rejestrację czasu pracy.

Grupy dostępu do zakładu

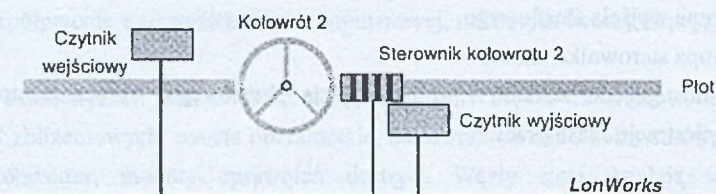
W systemie są dwie grupy dostępu do zakładu. Każda obsługuje jedno przejście i obejmuje kołowrót, czytnik wejściowy, czytnik wyjściowy, sterownik kołowrotu, panel operatorski (rys. 2 i 3).

Wejście do zakładu i wyjście z jego terenu odbywa się przez kołowroty. Odczyt ważnej karty poprzez zbliżenie jej do czytnika powoduje zwolnienie blokady kołowrotu przez sterownik, umożliwiając przejście w odpowiednim kierunku. To zdarzenie jest rejestrowane przez system i w przypadku pracowników wykorzystywane do obliczania czasu pracy. Próby nielegalnego dostępu są sygnalizowane na portierni przez sterownik alarmów i rejestrowane na stacji operatorskiej.

Do ręcznego sterowania kołowrotami przez strażnika (blokada, odblokowanie) służą panele operatorskie umieszczone na portierni.



Rys. 2. Grupy: dostępu do zakładu (kołowrót 1), wyjścia służbowego i sterownika alarmów
 Fig. 2. The groups: plant access (turnstile 1), business exit and alarm controller



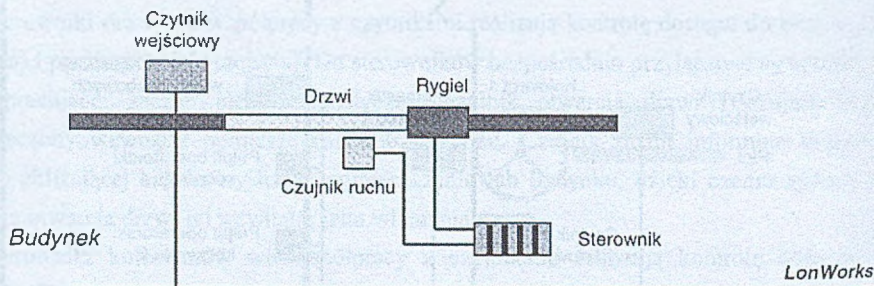
Rys. 3. Grupa dostępu do zakładu (kołowrót 2)

Fig. 3. The access group to the plant (turnstile 2)

Grupy dostępu do budynku

W systemie są dwie grupy dostępu do budynku obejmujące wejście służbowe i wejście dla gości. Każda grupa obejmuje czytnik wejściowy, sterownik drzwi, rygiel elektromagnetyczny i czujnik ruchu (rys. 4).

Osoba chcąca wejść do budynku musi zbliżyć swoją kartę do czytnika. Po odczycie ważnej karty rygiel elektromagnetyczny drzwi jest zwalniany, umożliwiając wejście. Próby nielegalnego dostępu są sygnalizowane dźwiękowo przy drzwiach, na portierni i rejestrowane na stacji operatorskiej.



Rys. 4. Grupa dostępu do budynku

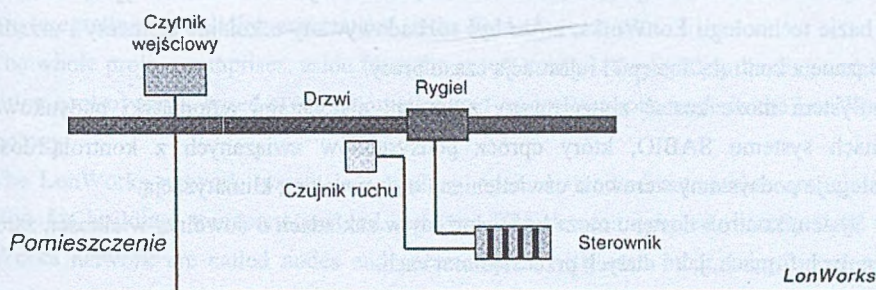
Fig. 4. The access group to the building

Grupy dostępu do pomieszczenia

W systemie są cztery grupy dostępu do pomieszczenia. Każda grupa obejmuje czytnik wejściowy, sterownik drzwi, rygiel elektromagnetyczny i czujnik ruchu (rys. 5).

Osoba chcąca wejść do pomieszczenia musi zbliżyć swoją kartę do czytnika. Po odczycie ważnej karty rygiel elektromagnetyczny drzwi jest zwalniany umożliwiając wejście. Próby

nielegalnego dostępu są sygnalizowane dźwiękowo przy drzwiach, na portierni i rejestrowane na stacji operatorskiej.



Rys. 5. Grupa dostępu do pomieszczenia

Fig. 5. The access group to a room

Grupa wyjścia służbowego

Grupa wyjścia służbowego obejmuje czytnik z klawiaturą umieszczony na portierni (rys. 4). Wychodzący służbowo pracownik podaje swoją kartę strażnikowi. Strażnik wpisuje kod na klawiaturze i zbliża kartę do czytnika. System rejestruje zdarzenie jako wyjście służbowe pracownika.

Grupa sterownika alarmów

Grupa obejmuje sterownik alarmów umieszczony na portierni (rys. 4). Sterownik otrzymuje sygnały o sytuacjach alarmowych powstałych przy kołowrotach oraz drzwiach i zgłasza je strażnikom poprzez zapalenie diody świecącej odpowiadającej miejscu powstania alarmu i włączenie buczka. Strażnik ma obowiązek potwierdzić alarm przez naciśnięcie przycisku potwierdzenia, który wyłącza buczek. Dioda świeci do chwili ustania przyczyny alarmu. Potwierdzenie przyjęcia alarmu rejestrowane jest w bazie danych systemu na stacji operatorskiej.

Uprawnienia dostępu kart dla wszystkich grup znajdują się w modułach uprawnień dostępu, z którymi komunikują się czytniki i sterowniki. W modułach gromadzone są informacje o zdarzeniach zaistniałych w grupach dostępu, skąd są przesyłane na serwer systemu kontroli dostępu.

5. Podsumowanie

System kontroli dostępu, dzięki zastosowaniu otwartej sieci komunikacyjnej i sterowania na bazie technologii LonWorks, może być rozbudowywany o kolejne elementy i urządzenia związane z kontrolą dostępu i rejestracją czasu pracy.

System może zostać zintegrowany z innymi elementami automatyki budynkowej w ramach systemu SABIO, który oprócz podsystemów związanych z kontrolą dostępu, obsługuje podsystemy sterownia oświetleniem, ogrzewaniem, klimatyzacją.

System kontroli dostępu może być wdrażany w zakładach o dowolnej wielkości, zarówno w małych firmach, jak i dużych przedsiębiorstwach.

Obecnie prace Instytutu Systemów Sterowania w zakresie kontroli dostępu będą prowadzone w kierunku rozwoju systemu do zastosowań w dużych obiektach budowlanych z zastosowaniem rozproszonych baz danych.

LITERATURA

1. Boroń W.: SABIO – inteligentny system automatyzacji budynku. *Pomiary Automatyka Kontrola*, 1999, nr 11.
2. Boroń W.: Inteligentny system automatyzacji budynku z zastosowaniem sieci sterowania LonWorks. *Materiały V Międzynarodowej Konferencji Inteligentny Budynek. Inteligentny Budynek Integracja Systemów*, 2000, nr 2 (20), s.113-116.
3. Boroń W.: Lokalna sieć sterowania LON. *Pomiary Automatyka Kontrola*, 1993, nr 10, s. 247-249.
4. Echelon LonWorks Products. Echelon Corporation. www.echelon.com
5. LonWorks Technology Device Data Book. Motorola Inc., 1997
6. Zauder T., Boroń W., Rogowski D.: Zastosowanie Internetu do nadzoru systemu automatyzacji budynku. *Wydawnictwo Politechniki Śląskiej*, 2000, *Studia Informatica* Vol. 21, No 1 (39), s. 425-433.

Recenzent: Dr inż. Wojciech Mielczarek

Wpłynęło do Redakcji 6 kwietnia 2001 r.

Abstract

The paper shows the results of a research project entitled 'Open Network Communication System integrating the building automation' in the field of access control.

The whole project comprises, aside from the access control, the lighting, heating and air-condition control and is based at the automation and control network made in the LonWorks technology.

The LonWorks network system is a leading, open, networked automation and control solution for building, transportation and industry. The devices coupled directly with the LonWorks network are called nodes and communicate with each other using a common protocol.

There are two levels in the system: a management level and automation level (Fig. 1).

The management level comprises operating stations (PC type computers), working within a local computer network (Ethernet). All the operating stations have application software for the access control system. One of them fulfils the function of an access control server with a database for collecting and logging data from the automation level nodes. The access control server is coupled with the LonWorks network with the help of a specialised card or a converter LON-RS232. The server may co-operate with the computer network server making a copy of its database on it. Another possibility is a co-operation with plant management software, installed on any computer in the Ethernet network, in the aspect of data interchange with the personal software system.

The control level comprises the LonWorks network and nodes like name tag readers (e.g. card readers), door, gate and turnstile controllers, operating panels, access rights modules, converters, routers and PC interfaces. The nodes are grouped together into so-called functional groups. Each functional group performs a local task, e.g. the access to a room.

The access control system, supplemented with time registration, was, after the design, experimental start-up and test, implemented in an industrial plant.

The practical system solution is described as an implementation example.

The implementation consists of one operating station (the access control server) on the management level and 25 nodes in 10 functional groups on the automation level.

The structures of the functional groups are shown in Figures 2 – 5.

The presented access control system is an open, modular and easily extendable system, thanks to the application of an automation and control network that is based at the LonWorks technology.