Marcin MAJ, Tomasz PERZYŃSKI, Daniel PIETRUSZCZAK

MONITORING OBIEKTÓW PRZEMYSŁOWYCH NA PRZYKŁADZIE SYSTEMU KONTROLI DOSTĘPU BIBINET

W artykule przedstawiono projekt, pozwalający na rejestrację pracy oraz kontrolę dostępu do obszaru w obiekcie, w którym pracuje do 10000 osób, zbudowany w oparciu o system bibinet. System bibinet jest przeznaczony głównie do kontroli dostępu do pomieszczeń i rejestracji czasu pracy pracowników w małych, średnich i dużych firmach.

WSTĘP

Współczesne systemy monitoringu stanowią narzędzie do obserwacji, kontroli zjawisk (procesów) czy nadzoru obiektów. Monitoring pozwala na zapewnienie ochrony mienia oraz ludzkiego życia, [1], [3], [4], [5], [6], [7], [8]. Pozwala na stałą kontrolę nad procesami produkcji. W przypadku monitoringu w obiektach przemysłowych, w zamierzeniu, dąży się do zapewnienia jak największej ochrony pracownikom, zwiększenia efektywności ich pracy oraz nadzoru wszelkich procesów związanych z działalnością obiektu. Obiektem nadzoru mogą być zarówno urządzenia i maszyny, jak również skomplikowane, złożone linie technologiczne, których celem jest wyprodukowanie określonej ilości dóbr przy optymalizacji procesu ich wytwarzania.

Obiekt przemysłowy, który już podczas planów budowlanych został zaopatrzony w odpowiedni system alarmowy oraz monitoringu, pozwala na wczesne wykrycie wszelkich nadużyć związanych na przykład z kradzieżą, czy tak często występującymi w dzisiejszych czasach próbami wycieku poufnych danych. Kluczowym zagadnieniem związanym z funkcjonowaniem takiego systemu monitoringu przemysłowego jest zapewnienie ciągłości procesu w przypadku wystąpienia jakiegokolwiek nadużycia, konieczności monitorowania najważniejszych parametrów pracy procesu, czy też stanu urządzeń wchodzących w skład zadanego obszaru.

Do czynników i zagrożeń, które mogą wpłynąć na zatrzymanie bądź awarię systemu można zaliczyć awarie związane z nieautoryzowanym dostępem do urządzenia oraz zagrożenia techniczne np. brak zasilania. Skutki przestojów w takich przypadkach mogą być bardzo kosztowne, natomiast odpowiednie systemy powiadamiania pozwalają na minimalizowanie strat poprzez zastosowanie awaryjnego zasilania.

W artykule przedstawiono projekt zbudowany w oparciu o system bibinet *(bibi.net)*, [2],[3]. System pozwala na rejestrację pracy oraz kontrolę dostępu do obszaru w obiekcie, w którym pracuje do 10 000 osób.

Autorzy artykułu oświadczają, że używając w artykule w/w znaku towarowego zrobili to z myślą tylko o tej publikacji i z taką intencją, aby było to z korzyścią dla właściciela znaku, bez zamiaru naruszania znaku towarowego.

1. SYSTEM BIBINET I JEGO KONFIGURACJA

System bibinet jest przeznaczony do kontroli dostępu do pomieszczeń i rejestracji czasu pracy pracowników w małych, średnich i dużych firmach. Minimalny system składa się z pojedynczego kontrolera pełniącego funkcję kontroli dostępu bądź rejestracji czasu pracy podłączony do pojedynczego komputera. Natomiast, dzięki możliwości dołączania urządzeń do wielu komputerów i wykorzystaniu w komunikacji Internetu, maksymalne możliwości systemu bibinet są praktycznie nieograniczone. Identyfikatorami w systemie są transpondery (identyfikatory) wykonane w postaci kart plastikowych lub breloczków. Identyfikacja odbywa się poprzez zbliżenie do czytnika. Dzięki temu system jest wygodny w użyciu, niezawodny i trwały.

Ze względu na niezbyt skomplikowaną rozbudowę, związaną na przykład z koniecznością doinstalowania dodatkowych kontrolerów dla nowych powierzchni i implementacją czytników, takie rozwiązanie pozwala na zwiększenie pokrycia i zabezpieczenie większego obszaru bez dużych nakładów finansowych oraz wielu godzin poświęconym na konfigurację systemu i jego elementów.

System bibinet działa w oparciu o dwie sieci:

- sieć komputerową, która zapewnia możliwość zainstalowania systemu bibinet;
- sieć urządzeń, które umożliwiają kontrolę dostępu do obszaru i rejestrację czasu pracy.

Połączenie tych dwóch sieci ma miejsce na punktach stykowych systemy bibinet, które noszą nazwę węzłów. Takim punktem jest fizyczny komputer, który posiada zainstalowane oprogramowanie producenta. System działa w środowiskach systemów operacyjnych Microsoft Windows, od Windows XP do Windows 10 a jego konfiguracja jest zgodna ze standardami sieci Ethernet opartej na protokole TCP/IP.

2. ELEMENTY SYSTEMU BIBINET

Sieć kontroli dostępu bibinet zbudowana jest z:

- interfejsów, które znajdują się pomiędzy komputerem i kontrolerem systemu bibinet;
- kontrolerów bibinet, realizujących założenia kontrolowania dostępu i monitorowania czasu pracy;
- czytników;

pozostałych elementów, które są przez producenta dostarczane do wszystkich kontrolerów.

2.1. Interfejs

Do łączenia kontrolerów z komputerem wykorzystywany jest interfejs w standardzie RS-485 (Rys. 1.), gdzie do jednej linii takiego połączenia można zaimplementować do 100 kontrolerów systemu bibinet.

Rys. 1. *Interfejs RS232-RS485 MM-I485/bibi [2]*

2.2. Kontroler

Kontroler dostępu bibinet K-12 (Rys. 2.) stosowany jest obecnie jako jedyny mechanizm, pełniący rolę uniwersalnego modułu, a jego założenia obejmują sprawowanie pieczy nad kontrolą dostępu oraz rejestracją czasu pracy w obiektach, gdzie jest wykorzystywany. Jeden kontroler jest w stanie realizować dostęp do dwóch przejść znajdujących się w budynku i jest możliwe skonfigurowanie dla tych przejść osobnych zasad pozwalających na wejście lub wyjście z obszaru. Proces ustawiania tych kontrolerów wykonuje się z komputera, na którym zainstalowany jest program. Po tym procesie przejścia mogą działać niezależnie od faktu, czy dany komputer jest uruchomiony czy też nie. Jest to możliwe dzięki temu, iż mają one wbudowany zegar czasu rzeczywistego oraz pamięć flash. Pamięć ta umożliwia zapisanie do dziesięciu tysięcy kart dostępowych oraz ok. 32 tys. zdarzeń. Każdy kontroler systemu pozwala na dołączenie do niego dwóch czytników, gdyż w jego skład wchodzą dwa interfejsy. Kontrolery można skonfigurować w trybie niezależnym, by potrafiły komunikować się i działać z wieloma typami czytników.

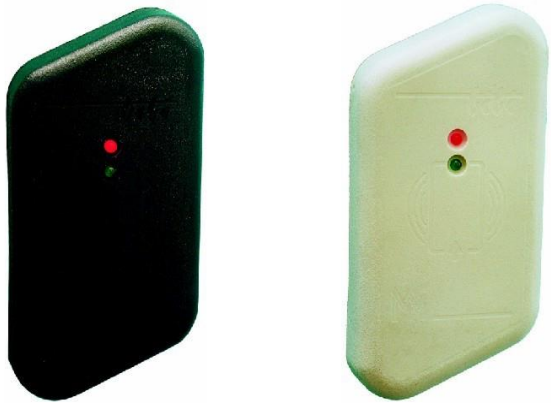
Rys. 2. *Kontroler bibi-K12 [opracowanie własne autorów]*

2.3. Czytniki

Do realizowania dostępu w omawianym systemie stosuje się dwa typy czytników, które dodatkowo wspierane są przez karty Unique:

- bibi-R32 – jest to kompaktowy czytnik, który wykazuje dużą odporność na niesprzyjające warunki pogodowe (Rys. 3.);
- bibi-R21 –model posiada wbudowany wyświetlacz, pozwalający na rejestrację czasu pracy.

Każdy czytnik w systemie ma interfejs oznaczony jako RS232, a wykorzystanie innych kart, na przykład zbliżeniowych lub magnetycznych jest możliwe poprzez zainstalowanie kompatybilnych do nich czytników innych producentów. Maksymalnie można zainstalować 4 czytniki do jednego wybranego kontrolera dostępu. Typy czytników, które mogą być wykorzystane oprócz standardowych wyposażonych w interfejs RS232, to czytniki posiadające interfejs Wieganda lub Track2.



Rys. 3. *Czytnik bibi-R32 [2]*

2.4. Klucze

Punkt zwany węzłem w systemie bibinet działa poprawnie jedynie z kluczem sprzętowym HAK2 (Rys. 4.), a ilość kluczy, którą należy wykorzystać odpowiada takiej ilości węzłów, jaka istnieje fizycznie w sieci zabezpieczającej zadany obiekt. Odpowiednie procedury bezpieczeństwa sugerują, iż klucz systemu powinien znajdować się w innym miejscu. Osoba odpowiedzialna za obsługę systemu posiada indywidualny klucz pozwalający na logowanie do systemu. Administrator ma możliwość logowania się tylko do węzłów, do których klucz ma zapisane hasło, a maksymalna ilość osób, która może być przypisana do jednego klucza wynosi 30.

Rys. 4. *Klucze bibinet [2]*

2.5. Struktura węzła sieci

Serwer pracujący w węźle sieciowym jest połączeniem, które pozwala na zestawienie sieci informatycznej z topologią sieciową urządzeń systemu bibinet. W skład topologii wchodzą takie moduły jak serwer bibinet, komponenty pozwalające na transmisje danych z innymi węzłami, kompozyt wspomagający pracę klucza HAK2/bibi oraz inne interfejsy dla pozostałych elementów systemu.

2.6. Serwer bibinet

Gromadzone przez maszynę serwerową dane zapisuje się w pliku, którego forma posiada zapis strukturalny, a dodatkowo każdy blok danych w takim pliku zabezpiecza się sumą kontrolną CRC32.

Przygotowany plik jest podpisany algorytmem MD5. Każdorazowo podczas włączania programu, odpowiednie moduły sprawdzają poprawność i spójność danych. Jakakolwiek nieuprawniona ingerencja w plik powoduje niemożność wystartowania programu. W kwestiach ogólnego bezpieczeństwa warto wspomnieć, iż każdego dnia wykonywana jest kopia zapasowa bazy w formacie .cab, a dysk komputera, który obsługuje system przechowuje dane z okresu ostatnich 15 dni. Rozproszona architektura systemu pozwala na dostęp do tych samych treści ze wszystkich komputerów wchodzących w skład systemu. Niemniej jednak, istotną procedurą jest przygotowanie regularnych kopii bezpieczeństwa przez pracownika, który administruje systemem.

2.7. Wymiana danych między węzłami

Budowa systemu pozwala na transferowanie danych między węzłami w czasie rzeczywistym, jednakże nie wymaga tego, by wszystkie punkty działały równocześnie i były włączone do sieci. W przypadku podłączenia się któregoś z nich w późniejszym czasie, zostaną do niego przesłane dane dotyczące zdarzeń. Punkty interfejsu komunikują się nie tylko przez sieć własną, ale też poprzez elementy systemu takie jak routery i sieć Internetową. Algorytm zapewniający bezpieczeństwo transmisji w sieci TCP/IP to 3DES, a wielkość klucza 3x56 bitów. Klucz jest losowo generowany dla każdej instalacji systemu.

2.8. Interfejs do kluczy

Do poprawnego działania węzła sieciowego konieczne jest posiadanie klucza sprzętowego, którego zadaniem jest realizowanie następujących funkcji:

– zachowywanie haseł dostępowych dla administratorów systemu ,
– zachowywanie algorytmów 3DES, które zapewniają szyfrowanie wymiany danych pomiędzy elementami systemu.

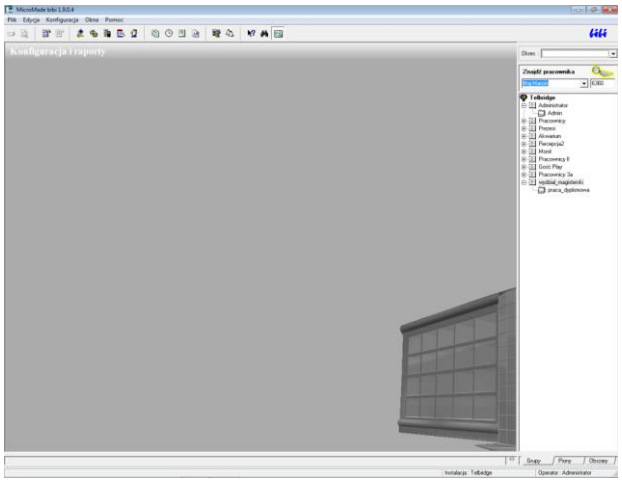
Te same klucze szyfrujące 3DES kontrolują ważność i termin wygaśnięcia licencji. Poprawne działanie programu jest możliwe tylko w przypadku posiadania aktywnej licencji na używanie produktu.

2.9. Rozbudowa urządzeń bibinet

Rozbudowę węzłów można zrealizować poprzez dodanie, z wykorzystaniem portu COM w komputerze, różnych urządzeń. Jest to możliwe zarówno poprzez zastosowanie portów fizycznych, które znajdują się na płycie głównej komputera jak i ich wirtualne odpowiedniki. Z uwagi na fakt możliwości obsługi przez systemy Windows do 256 portów COM, rozbudowa węzłów systemu bibi jest praktycznie nieograniczona, przy czym nie jest możliwe podłączenie dodatkowych urządzeń do terminala, a jedynie do węzłów.

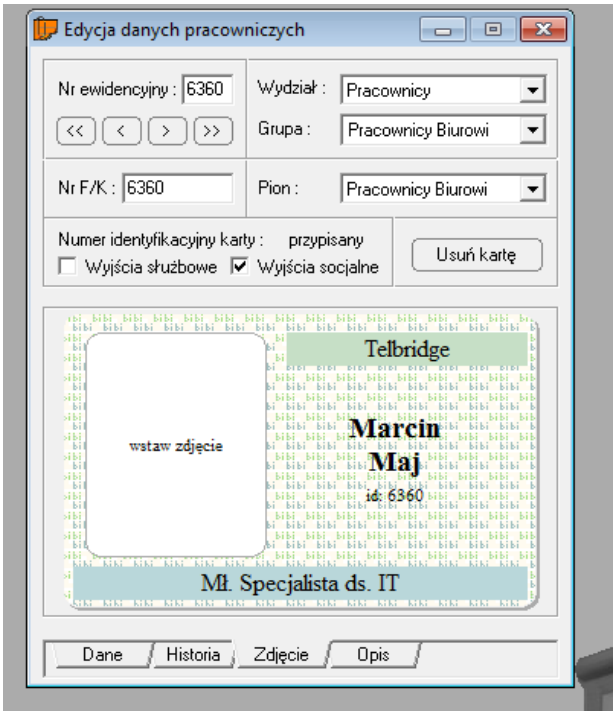
3. KONFIGURACJA PROGRAMU BIBINET

Po zainstalowaniu oprogramowania, jego interfejs główny (Rys. 5.) przedstawia się następująco: po prawej stronie znajduje się sekcja, w której istnieje struktura, składająca się z wydziałów i grup, które umożliwiają dodawanie pracowników do określonych obszarów i co za tym idzie, konfigurację dostępów do zadanych obszarów zgodnie z wytycznymi.



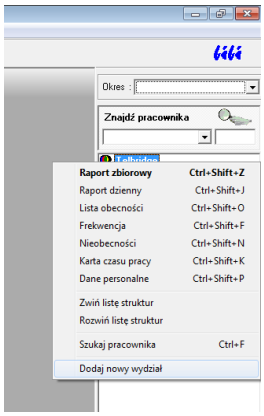
Rys. 5. *Okno główne interfejsu programu*

Dodawanie i edycja pracownika odbywa się poprzez kliknięcie na belce programu zakładki *Edycja* (Rys. 6.), a następnie zakładki *Edycja danych pracowniczych*. Nowo otwarte okno zawiera informacje dotyczące numeru ewidencyjnego, przypisanego pracownikowi, a także informacje na temat *Wydziału* oraz *Grupy*, do której w strukturze przydzielony jest użytkownik. Graficzne pole pozwala też na zaimportowanie zdjęcia pracownika oraz w dolnej sekcji przypisanie stanowiska pracy.



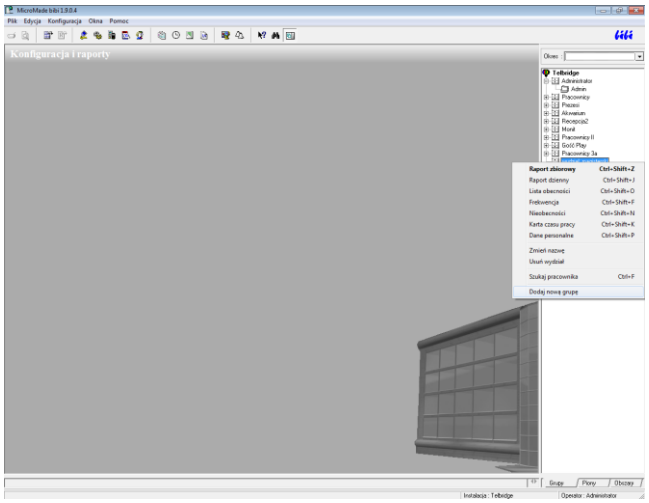
Rys. 6. *Dodawanie i edycja pracownika [opracowanie własne autorów]*

Konfigurację zaczyna się od wybrania opcji – dodaj nowy wydział (Rys. 7.). Wówczas do listy i struktury istniejących wydziałów dodany zostaje ten, który administrator programu tworzy, by dalej poddać go konfiguracji pod kątem kontroli dostępu. Widoczna na dole zakładka *Historia* pozwala na podgląd informacji o historii modyfikacji informacji dotyczących danego pracownika, na przykład zmian stanowiska lub przeniesieniu do innej grupy lub wydziału.



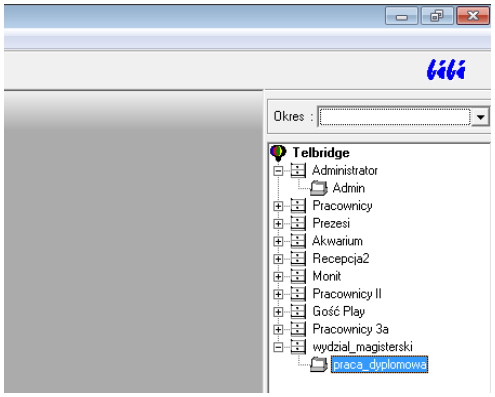
Rys. 7. *Dodawanie nowego wydziału [opracowanie własne autorów]*

W nowo utworzonym, na potrzebę projektu, *Wydziale magisterskim* należy dodać nową grupę (Rys. 8.). Rozwiniecie poprzez kliknięcie znacznika plus przy wydziale pozwoli podejrzeć strukturę drzewa wraz z dodaną nową grupą.



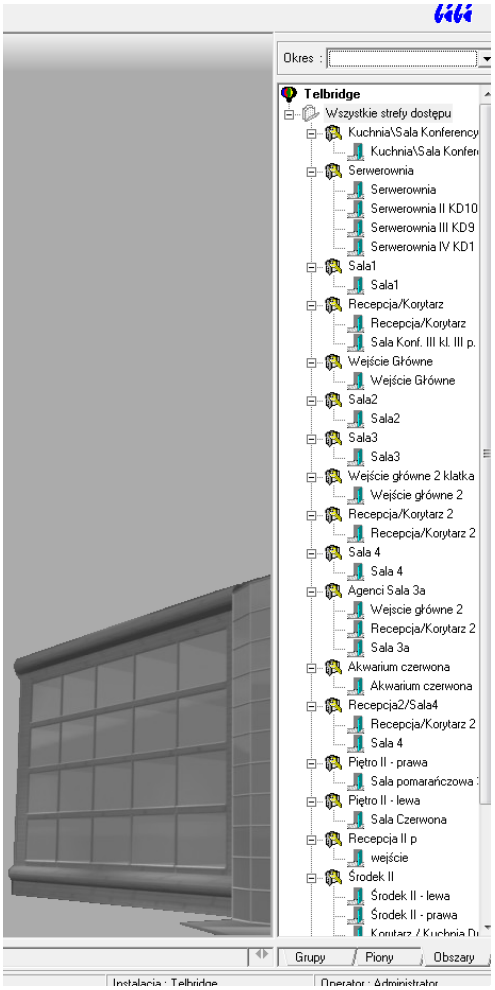
Rys. 8. *Dodawanie nowej grupy [opracowanie własne autorów]*

Strukturę drzewa kontroli dostępu przedstawiono na Rys. 9. Przejście przez ten etap pozwala na dalszą konfigurację dostępów i tworzenie lub edycję poprzez przeniesienie do danej grupy pracowników, których możliwości dostępu chce się zmodyfikować.



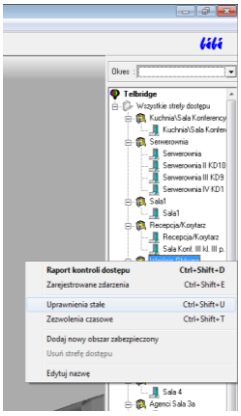
Rys. 9. *Struktura dostępu po dodaniu wydziału i grupy [opracowanie własne autorów]*

Rys. 10 przedstawia efekt uruchomienia zakładki *Obszary*, która posiada zdefiniowane strefy dostępu i przedstawia skonfigurowane pomiędzy tymi strefami czytniki otwierające rygle w drzwiach. Jest to bardzo ważna zakładka, ponieważ to na jej podstawie definiowana jest ścieżka dostępowa od drzwi wejściowych do konkretnego punktu czy sali w obiekcie. Jak można zaobserwować, niektóre strefy dostępu posiadają podpięte nawet kilka kontrolerów, co wiąże się z tym, iż na badanym obszarze występują na przykład aż 4 pomieszczenia serwerowni. Każda z nich może mieć własny dostęp poprzez zainstalowany czytnik, ale przypisane są one do jednej grupy obiektu.



Rys. 10. *Obszary stref dostępu [opracowanie własne autorów]*

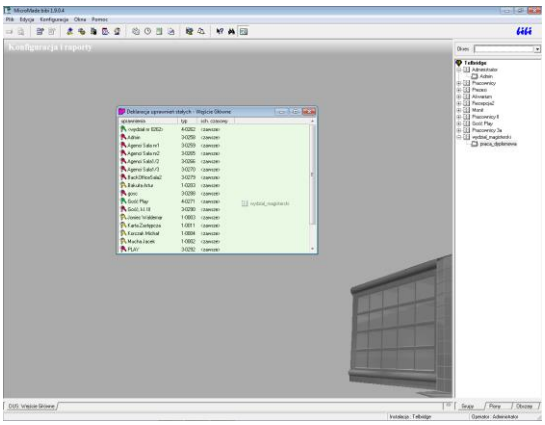
Na tym etapie możliwa jest konfiguracja uprawnień czasowym na przejściu poprzez wybranie na danym elemencie takiej opcji – uprawnienia stałe (Rys. 11.).



Rys. 11. *Dodawanie uprawnień stałych na przejściu [opracowanie własne autorów]*

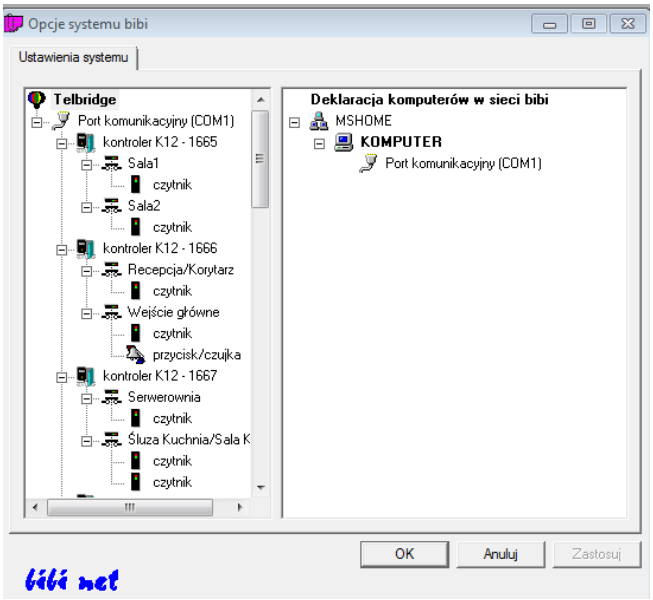
Następnie konieczne jest uruchomienie na belce programu okna dotyczącego *Deklaracji* uprawnień stałych z zakładki *Obszary* (Rys.

12.). Pozwala to przesunąć do otwartego okienka pracownika, grupę, bądź cały wydział utworzony kilka etapów wcześniej. Otworzone okno przestawia grupy dostępu, posiadające uprawnienia określone przez administratora w danym obszarze. Istnieje również możliwość konfiguracji nowych uprawnień poprzez edycję danych zawartych w oknie o nazwie *Edycja uprawnień*. Hierarchia grup w oknie jest tworzona na podstawie typu oraz numeru poszczególnych grup, które są im przydzielane. Ma to duże znaczenie, ponieważ przy zbliżeniu karty kontroler weryfikuje uprawnienia zgodnie z tym zapisem, jaki odnajdzie w oknie. W przypadku zbliżenia karty do czytnika i znalezieniu pierwszych uprawnień, które zostaną zarejestrowane na liście, kończy on swoją pracę. Uprawnienia na tej podstawie można przydzielać i rozszerzać na całe wydziały i dokonywać wyłączeń poszczególnych grup lub pracowników.



Rys. 12. *Konfiguracja uprawnień stałych dla wydziału [opracowanie własne autorów]*

Rys. 12. przedstawia wywołania z menu programu opcji. Ukazuje to sposób ustawienia i połączenia elementów systemu wchodzących w skład systemu kontroli dostępu w obiekcie. Można zauważyć, jak połączone są przejścia między pomieszczeniami. W skład elementów odblokowujących drzwi i rygiel wchodzą również przyciski mechaniczne, które umożliwiają przejście np. w przypadku wyjść ewakuacyjnych.



Rys. 13. *Okno przedstawiające interfejs komunikacyjny i połączenia między kontrolerami w obiekcie [opracowanie własne autorów]*

PODSUMOWANIE

Przedstawiony w artykule projekt kontroli dostępu oparty na systemie bibinet bardzo dobrze może się sprawdzić w przedsiębiorstwie, które zatrudnia się nawet kilkaset pracowników. Ze względu na niezbyt skomplikowaną rozbudowę oraz czytelny interfejs użytkownika, rozwiązanie takie pozwala na zabezpieczenie dużego obszaru. W pracy przedstawiono uproszczony algorytm związany z konfiguracją systemu. Przedstawione rozwiązanie stanowi wybrane narzędzie z dostępnych na rynku. Rozwiązania takie stanowią obecnie nieodzowny element wyposażenia obiektów przemysłowych.

BIBLIOGRAFIA

1. Maj M.: „*Monitoring obiektów przemysłowych*”. Praca dyplomowa magisterska, WTiE UTH Rad., Radom 2018.
2. http://www.bibinet.pl/dla_uzytkownika [25.02.2018]
3. http://pliki.micromade.pl/pdf/bibinet_ii.pdf [25.02.2018]
4. http://centrum-zabezpieczen.pl/co-to-jest-monitoring-wizyjny-i-z-czego-sie-sklada [09.02.2018]
5. http://www.nimoz.pl/baza-wiedzy/bezpieczenstwo-zbiorow-i-ludzi/ochrona-przeciwpozarowa/system-sygnalizacji-pozaru-ssp [09.02.2018]
6. http://www.systemy.pollub.pl/Dyd_MH_InteligentneInst07.pdf [11.02.2018]
7. http://www.hawrylak.pl/index.php?show=30 [11.02.2018]
8. http://www.systemy.pollub.pl/Dyd_MH_InteligentneInst07.pdf [11.02.2018]

Monitoring of industrial facilities based on the bibinet access control system

The paper presents a project that allows the registration of work and access control to the area in the facility where up to 10,000 people work, based on the bibinet system. The bibinet system is designed mainly to control access to rooms and record working time of employees in small, medium and large companies.

Autorzy:

mgr inż. Marcin Maj – student kierunku elektrotechnika, Wydział Transportu i Elektrotechniki Uniwersytetu Technologiczno-Humanistycznego im. Kazimierza Pułaskiego w Radomiu, ul. Malczewskiego 29, 26-600 Radom.

dr hab. inż. Tomasz Perzyński, prof. UTH – Wydział Transportu i Elektrotechniki Uniwersytetu Technologiczno Humanistycznego im. Kazimierza Pułaskiego w Radomiu, ul. Malczewskiego 29, 26-600 Radom, e-mail: t.perzyński@uthrad.pl

dr inż. Daniel Pietruszczak – Wydział Transportu i Elektrotechniki Uniwersytetu Technologiczno-Humanistycznego im. Kazimierza Pułaskiego w Radomiu, ul. Malczewskiego 29, 26-600 Radom, e-mail: d.pietruszczak@uthrad.pl

JEL: L96 **DOI**: 10.24136/atest.2018.138
Data zgłoszenia: 2018.05.23 **Data akceptacji**: 2018.06.15