

BUCZAJ Marcin ¹

Koncepcja zarządzanego przez mikrokomputer systemu alarmowego nadzorującego stan chronionego obiektu logistycznego

systemy sterowania i nadzoru, mikrokomputery
techniki zabezpieczenia mienia,
systemy alarmowe, LabVIEW

Streszczenie

Prawidłowe działanie systemu sygnalizacji włamania i napadu (I&HAS) wiąże się z szybkim przekazaniem informacji do użytkownika o stanie chronionego obiektu. W artykule przedstawiono koncepcję zastąpienia urządzenia sterującego i obrazującego (centrali alarmowej) przez komputer klasy PC wyposażony w odpowiednie oprogramowanie umożliwiające realizację funkcji sterowania, zarządzania systemem I&HAS. Do budowy takiego systemu został wykorzystany komputer PC oraz środowisko LabView. Akwizycja parametrów odbywała się na podstawie informacji i sygnałów z czujników współpracujących z kartami pomiarowymi. Zbudowany interfejs umożliwi wyświetlanie na ekranie komputera aktualnych, a także archiwalnych parametrów występujących w poszczególnych pomieszczeniach. Dzięki takiemu rozwiązaniu użytkownik ma możliwość wglądu i nadzór nad systemami alarmowym działającym w obiekcie.

CONCEPTION OF MANAGEMENT BY MICROCOMPUTER ALARM SYSTEM CONTROL CONDITION OF PROTECTION LOGISTIC OBJECT

Abstract

The correct functioning of the intrusion and hold-up alarm system (I&HAS) is connected with a quick transmitting the information about state of protect object to the user. This paper presented the concept of replaced classic hardware control and indicating equipment by computer PS with individual special software make enable realized the remote control, virtual control and indicating equipment for alarm system I&HAS. A computer PC and LabView environment have been used for the building of such system. The acquisition of parameters was carried out basing upon the information and signals received from the sensors supporting the measuring cards. The actual as well as archived parameters occurring in alarm system can be displayed on the computer screen via built-in interface. Thanks to this solution, the system user has the opportunity to review of and to supervise over the autonomous alarm systems operating in object.

1. WSTĘP

Systemy nadzoru nad stanem chronionego obiektu to systemy umożliwiające sprawowanie kontroli nad dozorowanym obiektem przez użytkowników systemu. Przez użytkowników systemu należy rozumieć zarówno osoby bezpośrednio odpowiedzialne za nadzór nad chronionym obiektem (właściciel obiektu, ochrona obiektu), jak i odpowiednie służby zewnętrzne (policja, straż pożarna). Systemy zarządzające i nadzorujące elementami zabezpieczanego obiektu to układy umożliwiające automatyczną realizację założonych w algorytmie sterowania funkcji i zadań przez układy wykonawcze na podstawie informacji pochodzących od użytkownika systemu lub od elementów detekcyjnych systemu. Systemy sterowania w obiektach budowlanych spełniają najczęściej rolę energetyczną. Odpowiadają za realizację potrzeb bytowych i technologicznych w obiekcie. Natomiast systemy nadzoru to systemy realizujący zadania dotyczące kontroli stanu obiektu, spełniają rolę informującą i umożliwiają realizację potrzeb związanych z bezpieczeństwem w obiekcie. Charakteryzują się ponadto dużo większymi wymaganiami dotyczącymi samokontroli systemu, niezawodności działania. Stanowią wyższy priorytet działania i zaspakajania potrzeb energetycznych.

Systemy nadzoru powinny zapewnić użytkownikowi zarówno realizację funkcji monitoringu aktualnego stanu obiektu (funkcje informacyjne) jak i umożliwić ingerencję w aktualne tryby pracy poszczególnych elementów systemu oraz algorytmy realizowanych przez systemu działań (funkcje sterowania). Ważne staje się również szybkie i precyzyjne skierowanie informacji o wykrytym zagrożeniu do odpowiednich komórek i grup użytkowników systemu. Systemy nadzorujące stan chronionego obiektu wyposażone w elementy odpowiedzialne za kontrolę bezpieczeństwa w obiekcie powinny charakteryzować się następującymi cechami:

- reagować na możliwie szeroką gamę mogących wystąpić w obiekcie zagrożeń;
- przekazywać użytkownikowi systemu informację o stanie zabezpieczanego obiektu;
- przekazywać informację o zidentyfikowaniu zagrożenia do konkretnej komórki odpowiedzialnej w systemie za neutralizację konkretnego zagrożenia;
- posiadać procedury neutralizacji przewidziane w przypadku wykrycia zagrożenia;

¹ Politechnika Lubelska, Katedra Inżynierii Komputerowej i Elektrycznej, 20-618 Lublin, ul. Nadbystrzycka 38A
Tel.: +48 81 53-84-301; Fax.: +48 81 53-84-301; E-mail: m.buczaj@pollub.pl

– współpracować z innymi instalacjami istniejącymi w chronionym obiekcie.

W przypadku systemów sterowania i nadzoru wyróżnić można dwie podstawowe grupy systemów:

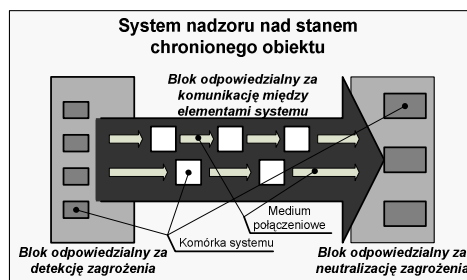
- systemy przekazywania informacji o stanie obiektu (systemy alarmowe);
- systemy bezpieczeństwa.

W przypadku systemów przekazywania informacji o stanie obiektu (systemy I&HAS, systemy DSO) głównym ich zadaniem jest detekcja rejestrowanego przez elementy detekcyjne systemu zaburzenia, zidentyfikowanie zagrożenia na podstawie analizy rejestrowanych zaburzeń w obiekcie oraz przekazanie informacji do użytkowników systemu o wykryciu zagrożenia lub stanu anomального. Natomiast systemy bezpieczeństwa (systemy oddymiania, systemy oświetlenia awaryjnego, systemy gaśnicze) wyposażone są w układy lub komórki umożliwiające realizację procesu neutralizacji zagrożenia lub ograniczenia zasięgu zidentyfikowanego zagrożenia. W tym przypadku funkcja informacyjna biegnie równoległe w stosunku do wewnętrznego procesu sterowania i przekazywania informacji między komórkami systemu wynikające z realizowanej procedury działania.

Wynika z tego, że systemy bezpieczeństwa instalowane w chronionych obiektach powinien posiadać komórki (elementy) systemu odpowiedzialne za:

- detekcję zagrożenia;
- komunikację między komórkami systemu i między systemem a użytkownikiem;
- fizyczną neutralizację zagrożeń lub przeciwdziałanie zidentyfikowanemu zagrożeniu.

Schemat funkcyjny systemu nadzoru nad stanem chronionego obiektu został przedstawiony na rys. 1.



Rys.1. Schemat funkcyjny systemu nadzoru nad stanem chronionego obiektu

W artykule zostanie zwrócona uwaga na możliwość budowy urządzeń sterujących i obrazujących (central alarmowych) opartych na sprzęcie zaliczanym do klasy mikrokomputerów. Takie rozwiązanie umożliwi, oprócz realizacji tych samych zadań i funkcji dostępnych w układach klasycznych, swobodne programowanie i tworzenie algorytmu sterującego nieograniczającego się tylko do standardowych rozwiązań. Zaproponowane rozwiązanie ma być alternatywą do obecnie stosowanych systemów wbudowanych opartych na układach mikroprocesorowych. W zarządzanym przez mikrokomputer układzie sterownia i nadzoru część decyzyjna systemu zostanie zaimplementowana, jako aplikacja stworzona w środowisku LabView. Przedstawiona koncepcja ma na celu dokonanie porównania możliwości funkcyjnych obu systemów oraz możliwości tworzenia indywidualnych procedur sterowania. Szczególna uwaga zostanie zwrócona na sposób interpretacji sygnałów pochodzących od elementów detekcyjnych systemu oraz możliwość przeniesienia procesu interpretacji wielkość rejestrowanego zaburzenie z elementu detekcyjnego (czujki) do urządzenie sterującego i obrazującego (centrali alarmowej) systemu nadzoru.

2. SYSTEMY ALARMOWE I&HAS

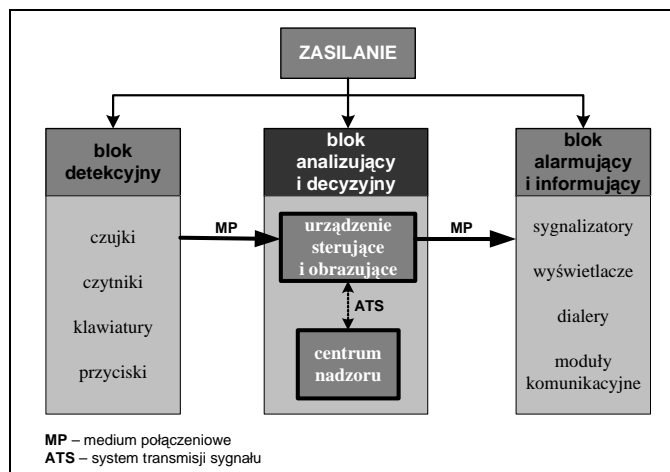
Zgodnie z wymaganiami normy PN-EN 50131-1 [1] system nadzoru umożliwiający realizację funkcji systemu alarmowego I&HAS powinien zawierać środki do wykrywania, wyzwolenia stanu alarmowego, sabotażu i rozpoznania uszkodzeń w systemie. System ten może również realizować inne funkcje pod warunkiem, że nie mają one szkodliwego wpływu na podstawowe funkcje systemu alarmowego I&HAS. Proces przekazywania informacji o wykrytym zagrożeniu w systemach I&HAS przebiega między obiektem dozorowanym a centrum odbiorczym alarmu za pośrednictwem systemu transmisji alarmu. System transmisji sygnału w zależności od stopnia zabezpieczenia systemu I&HAS powinien spełniać określone kryteria dotyczące: czasu transmisji, maksymalnej wartości czasu transmisji, czasu raportowania, dostępności i ochrony sygnału. Szczegółowe wytyczne dotyczące kryteriów stawianym systemom transmisji sygnału określa norma PN-EN 50136-1-1 [2].

Współczesne systemy alarmowe sygnalizacji włamania i napadu I&HAS (*ang. intrusion and hold-up alarm system*) to instalacja elektryczna, która odpowiada na ręczne lub automatyczne wykrycie obecności zagrożenia (włamania, napadu, próby sabotażu systemu) w zabezpieczanym obiekcie [1]. Techniczne jest to zespół współpracujących urządzeń (również z instalacją przewodową), który ma na celu wykrywanie zagrożeń, wywołanie alarmu oraz inicjowanie przedsięwzięć zmierzających do likwidacji takiego zagrożenia.

Dokonując analizy funkcjonowania takiego systemu można wyodrębnić w nim kilka podstawowych powiązanych ze sobą bloków funkcyjnych (rys. 2.):

- blok analizująco-decyzyjny (zarządzający);
- blok detekcyjny (wejściowy);
- blok alarmująco-informujący (wykonawczy);

– blok zasilający.



Rys. 2. Schemat organizacyjny systemu alarmowego I&HAS

Blok detekcyjny to zespół urządzeń, których zadaniem jest wykrycie zmian zachodzących w chronionym obiekcie lub systemie alarmowym i przekazanie informacji do urządzenia sterującego i obrazującego (centrali alarmowej) systemu. W bloku detekcyjnym nie następuje podejmowanie decyzji o wszczęciu alarmu, przekazywana jest tylko informacja o zmianie mierzonego lub kontrolowanego parametru (temperatura, zmiana położenia, dźwięk, obraz, wibracje, sabotaż) ponad dopuszczalny zakres lub ustaloną wartość.

Blok alarmujący i informujący to zespół urządzeń mających na celu przekazanie informacji pochodzącej z systemu alarmowego do otoczenia (użytkownika) po otrzymaniu sygnału pochodzącego od elementu sterującego pracą systemu. Komunikuje o zaistniałych próbach sabotażu, włamania lub naruszenia chronionej przestrzeni. Informacja ta może być przekazana na kilka sposobów: dźwiękowo, akustycznie, tekstowo, optycznie.

Blok analizująco-sterujący zawiera elementy odpowiedzialne za kontrolę pracy całego systemu oraz za podejmowanie decyzji zgodnie z ustalonymi procedurami zawartymi w algorytmie sterującym. To w nim przetwarzane są informacje pochodzące od poszczególnych elementów detekcyjnych i przekazywane są sygnały do elementów wykonawczych systemu.

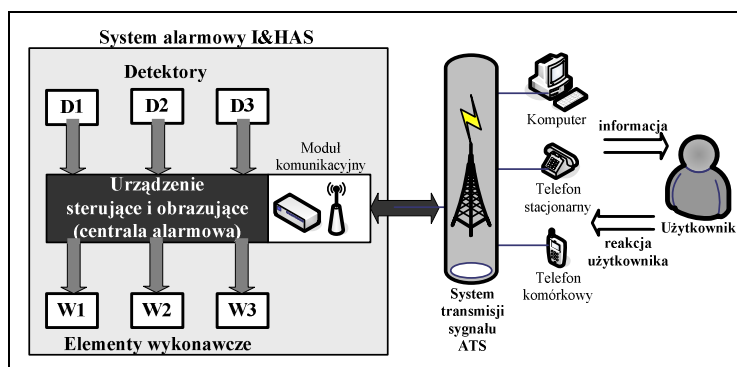
Ostatnią grupę elementów stanowiących system alarmowy są układy zasilania. Są to układy dostarczające energię elektryczną do poszczególnych urządzeń. Nie mają udziału w procesie decyzyjnym i alarmowym, jednak ze względu na fakt, że współczesne systemy alarmowe oparte są na szeroko pojętej elektronice są ich nieodzownym elementem.

Dodatkowo w systemie alarmowym występują układy odpowiedzialne za przesyłanie sygnału między poszczególnymi elementami systemu (media połączeniowe oraz systemy transmisji sygnału).

3. SYSTEM ALARMOWY Z KLASYCZNYM CENTRALĄ ALARMOWĄ

Układ nadzoru systemu alarmowego I&HAS to układ zawierający urządzenie sterujące i obrazujące (centralę alarmową) oraz współpracujące z centrami nadzoru elementy odpowiedzialne za komunikację na drodze system-użytkownik. System nadzoru to "mózg" całego systemu alarmowego, jego zadaniem jest podjęcie decyzji o wszczęciu alarmu. W tym układzie przechowywane są informacje o stanie wszystkich urządzeń współpracujących w danym systemie alarmowym, a wszystkie decyzje podejmowane są w oparciu o procedury i algorytmy zapisane w programie sterującym pracą systemu alarmowego.

Schemat organizacyjny systemu alarmowego I&HAS z klasycznym układem sterowania i nadzoru przedstawiony został na rys. 3.



Rys. 3. Schemat organizacyjny systemu alarmowego I&HAS z klasycznym układem nadzoru

Najważniejszym elementem systemu alarmowego jest urządzenie sterujące i obrazujące. Są to wyspecjalizowane urządzenia, których zadaniem jest [1, 5]:

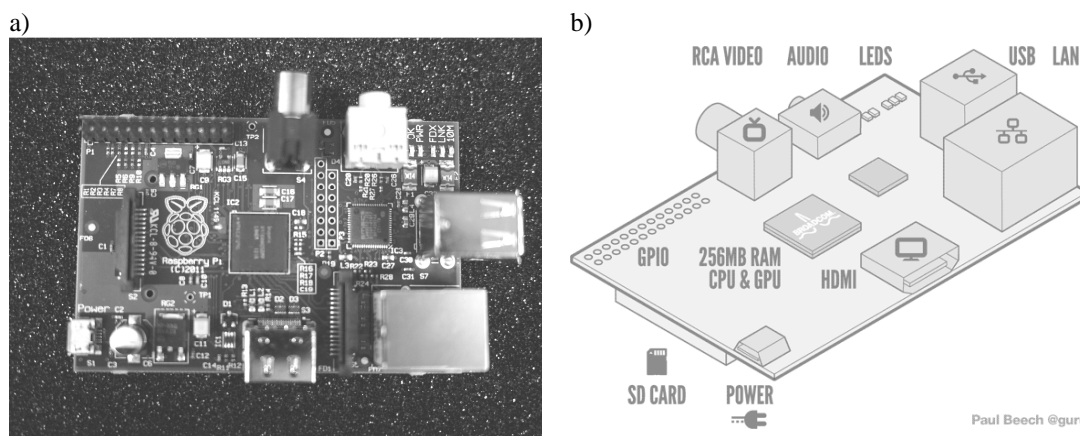
- odbieranie i przetwarzanie zgodnie z programem sterującym sygnałów informacyjnych (analogowych i/lub cyfrowych) pochodzących od poszczególnych urządzeń;
- sterowanie poprzez podanie odpowiednich sygnałów wyjściowych;
- obrazowanie zaistniałych zdarzeń na odpowiednich urządzeniach wchodzących w skład systemu sygnalizacji włamania;
- transmisja informacji do innych systemów, np. alarmowego centrum odbiorczego (w skrócie ARC, ang. *alarm receiving centre*).

Cechą klasycznych układów jest to, że całość niezbędnej do prawidłowego działania systemu infrastruktury jest fizycznie umieszczona w chronionym obiekcie. Ponadto w klasycznym rozwiązaniu istnieje wyraźne fizyczne odseparowanie układów odpowiedzialnych za sterowanie pracą systemu I&HAS (central alarmowych) od układów analizujących wielkość rejestrowanego zaburzenia oraz od układów komunikacyjnych odpowiedzialnych za przekazywanie informacji o stanie systemu między systemem a użytkownikiem. Również wymiana informacji między podsystemami większych systemów alarmowych I&HAS odbywa się na poziomie układów komunikacyjnych i urządzeń sterujących i obrazujących (central alarmowych). Podsystemy większych układów praktycznie, o ile nie są fizycznie podłączone do danego elementu detekcyjnego, to nie mają informacji jego stanie. Może to wpływać na czas reakcji na występujące w systemie zagrożenie, prawidłowość podjętej decyzji oraz na skuteczność całego procesu neutralizacji zagrożenia.

Elementy detekcyjne w klasycznym układzie systemu alarmowego działają realizując pewne ściśle określone reguły progowe. Po przekroczeniu ustalonego poziomu układ analizujący czujki zmienia tylko stan sygnału, jaki zostaje przekazany do centrali alarmowej nie przesyłając żadnej informacji o aktualnym poziomie zaburzenia. Wewnętrzne układy analizują poszczególne stany z linii detekcyjnych i realizują założone funkcje sekwencyjne, a następnie przekazują informację do użytkownika o podjętych przez urządzenie sterujące i obrazujące decyzjach. Działanie klasycznych układów zarządzających pracą systemu alarmowego ogranicza się do realizacji pewnych funkcji logicznych uzupełnionych elementami umożliwiającymi realizację procedur czasowych.

4. SYSTEM ALARMOWY Z MIKROKOMPUTEROWYM URZĄDZENIEM STERUJĄCYM

Koncepcja budowy mikrokomputerowego systemu nadzoru sterującego pracą systemu alarmowego sygnalizacji włamania i napadu I&HAS opiera się na zastąpieniu klasycznej centrali alarmowej, wyposażonej w mikroprocesorowy system wbudowany, komputerem klasy PC (o budowie klasycznej, np. desktop, o budowie specjalnej – mikrokomputerem np. Rapsberry Pi – rys. 4) z indywidualnie opracowaną aplikacją sterującą (np. w środowisku LabView).



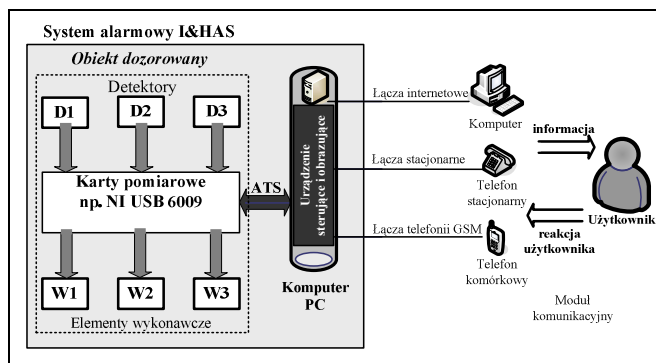
Rys. 4. Platforma mikrokomputera Rapsberry Pi model typ B, a) widok układu; b) topologia układu [8]

Organizacyjnie, z powodu braku możliwości obsługi dużej ilości elementów I/O, rozwiązanie to powoduje konieczność wyposażenia układu sterowania w układ umożliwiający odczytywanie stanów wyjść układów detekcyjnych i wysterowanie układów wejść elementów wykonawczych. W tym przypadku istnieje konieczność podniesienia roli układów komunikacyjnych z układów peryferyjnych, przekazujących na ogół tylko informację o stanie systemu alarmowego, do elementów istotnych, równorzędnych z układami sterującymi i detekcyjnymi. Dla potrzeb badawczych związanych z opisanym układem wykorzystane zostały karty pomiarowe NI USB 6009. Każda karta umożliwia obsługę 12 konfigurowalnych wejść/wyjść cyfrowych, 8 wejść analogowych i 2 wyjść analogowych. Takie wyposażenie pozwala na sprawdzenie działania systemu zarówno w konfiguracji analogicznej do klasycznej centrali alarmowej (np. Satel CA-10, Integra), a także przetestowania możliwości układu, w którym elementy detekcyjne przesyła informację o rejestrowanym zaburzeniu w ośrodku do komputera bez dokonywania analizy i oceny rejestrowanego zaburzenia.

Schemat organizacyjny systemu alarmowego I&HAS z mikrokomputerowym układem sterowania i nadzoru przedstawiony został na rys. 5. Przedstawiona organizacja systemu alarmowego umożliwia wyprowadzenie układu analizująco-decyzyjnych z elementów detekcyjnych do układu decyzyjnego.

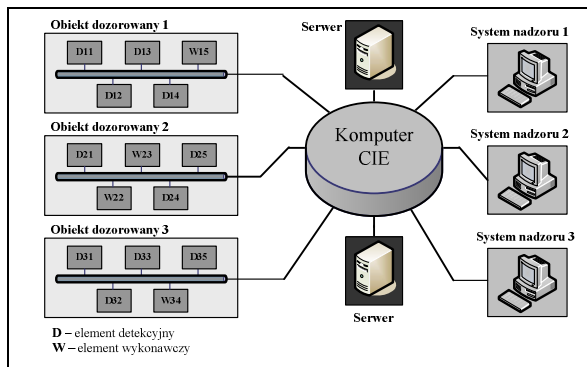
Konfiguracja systemu z przeniesioną analizą rejestrowanych parametrów zaburzenia z elementów detekcyjnych do układu zarządzania pracą systemu (układzie mikrokomputer i aplikacja sterująca) ma na celu opracowanie algorytmów opartych na zmiennych kryteriach wywoływania stanu alarmu. Takie rozwiązanie umożliwi zmianę poziomu wyzwolenia alarmu w przypadku niewielkiego zaburzenia w układzie jednej z czujek i potwierdzeniem zaburzenia również niewielkim pobudzeniem innego elementu detekcyjnego. Taka sytuacja nie jest możliwa do wykonania w klasycznym układzie, gdzie poziomy wyzwolenia alarmu są ustawione na stałe i nie ma możliwości określenia przez układ decyzyjnych aktualnych poziomów zaburzeń rejestrowanych przez poszczególne układy detekcyjne.

Tworzenie komputerowych systemów pomiarowych [4], czasami nawet pracujących niezależnie, umożliwia ukierunkowanie na różne podejście do rejestrowanego przez układy detekcyjne sygnał (rys. 7). Przesyłanie do komputera w celu dokonania analizy sygnału całego nieprzetworzonego strumienia informacji źródłowej (rejestrowanego w elemencie detekcyjnym) i jego dokładna analiza umożliwia opracowanie adaptacyjnych algorytmów wykrywania zagrożenia, w którym parametry oceny mogą się zmieniać w zależności od rejestrowanych parametrów innych elementów detekcyjnych [3].

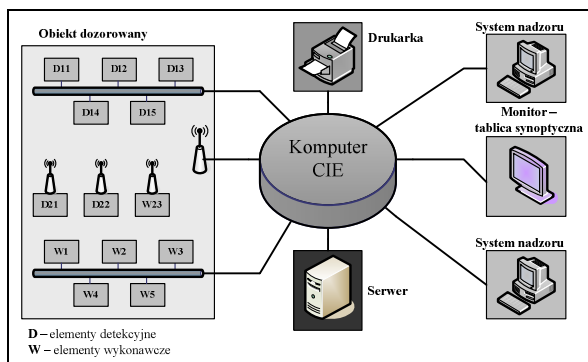


Rys. 5. Schemat organizacyjny systemu alarmowego I&HAS z wirtualnym układem sterowania i nadzoru

Zastąpienie klasycznych układów służących do zbierania i analizy informacji układami mikrokomputerowymi (rys. 6) umożliwia budowę rozproszonych układów analizująco-decyzyjnych o dowolnym stopniu powielenia. Utrudnia to proces sabotażu i praktycznie eliminuje możliwość ingerencji w proces działania rejestratora zdarzeń oraz uniemożliwia zniszczenie urządzenia sterującego podczas dokonywania włamania do obiektu [3].



Rys. 6. Topologia mikrokomputerowego systemu nadzoru nad stanem chronionego obiektu



Rys. 7. Funkcjonalność wirtualnego systemu alarmowego I&HAS

5. APLIKACJA STERUJĄCA SYSTEMEM ALARMOWY ZARZĄDZANYM PRZEZ MIKROKOMPUTER

Głównym zadaniem stawianym budowanemu komputerowo zarządzanemu systemowi alarmowemu kontrolującego stan infrastruktury w chronionym obiekcie jest umożliwienie użytkownikowi sprawowania kompleksowej kontroli parametrów bezpieczeństwa (wykrywanie zagrożeń i niebezpieczeństw). Realizacja tego celu odbywać się będzie poprzez akwizycję danych pomiarowych zbieranych przez system nadzoru z poszczególnych elementów detekcyjnych umieszczonych w poszczególnych strefach dozoru wyznaczonych na terenie zabezpieczanego obszaru lub bezpośrednio z urządzeń stanowiących wyposażenie obiektu (parametry techniczne). Najlepszym rozwiązaniem dla spełnienia tych zadań będzie wykorzystanie modelu zintegrowanego systemu nadzoru realizującego cele systemu alarmowego i systemu kontroli stanu elementów infrastruktury chronionego obiektu. Takie rozwiązanie umożliwi ograniczenie kosztów związanych z zastosowaniem dodatkowych autonomicznych systemów (kontrolującego systemu nadzoru). Taki system dodatkowo będzie charakteryzował się identycznością sygnałów dochodzących do systemu sterowania i systemu nadzoru umożliwiając prawidłową ocenę sytuacji panującej w poszczególnych obiektach lub pomieszczeniach.

Ważną funkcją aplikacji stworzonej na potrzeby realizacji zadań sterowania i kontroli przez komputerowy system nadzoru i zwiększającą możliwości funkcjonalne takiego systemu jest możliwość akwizycji danych pomiarowych i ich archiwizacja oraz możliwość zastosowania modeli matematycznych i algorytmów obliczeniowych w celu określenia stanu bezpieczeństwa w obiekcie na podstawie inteligentnych algorytmów sterowania. Taka możliwość istnieje dzięki przeniesieniu układu odpowiedzialnego za podjęcie decyzji o stanie alarmowym z elementu detekcyjnego do układu zarządzającego.

W zarządzanym za pomocą komputera PC systemie nadzoru stan bezpieczeństwa w obiekcie należy wyróżnić następujące elementy (rys. 5):

- jednostkę zarządzającą – komputer za pomocą którego odbywa się obsługa systemu;
- istniejące systemy sterujące – wydzielone autonomiczne systemy obsługujące i realizujące program wyznaczony przez użytkownika systemu (sterowniki, układy zasilające i sterujące itp.);
- elementy detekcyjne – czujniki parametrów klimatycznych i technicznych zamontowane w niewalidycznych punktach nadzorowanych pomieszczeń określające aktualny parametry w danym obszarze;
- elementy wykonawcze – urządzenia wykorzystywane do zmiany parametrów klimatycznych i technicznych w kontrolowanych pomieszczeniach (np. silniki, grzejniki, wentylatory) oraz systemy powiadamiania o wykryciu zagrożenia lub stanu awaryjnego;
- elementy pośredniczące w wymianie informacjami między autonomicznymi systemami sterowania a wirtualnym systemem nadzoru – karty pomiarowe wykorzystywane do akwizycji danych przez wirtualny system nadzoru.

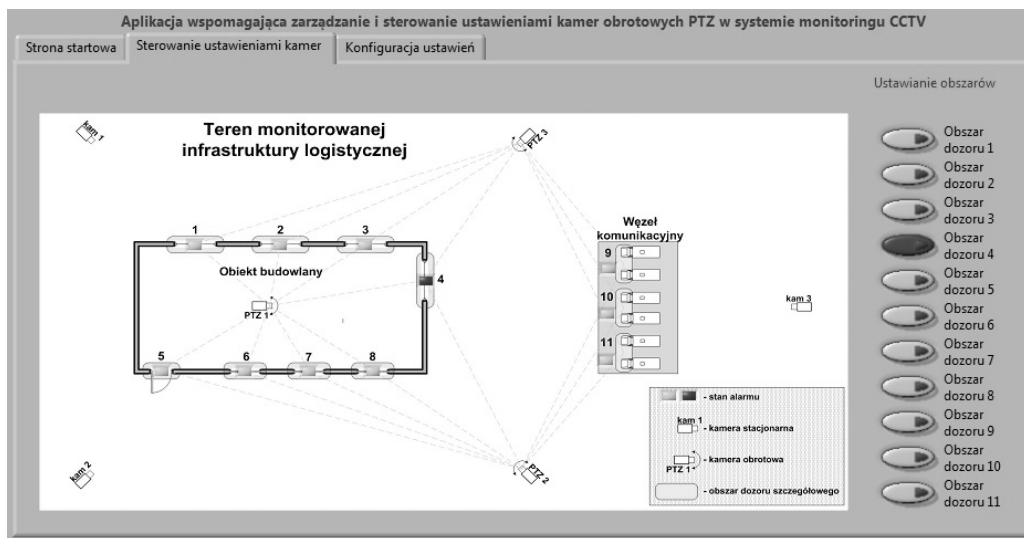
Aplikacja umożliwiająca sterowanie i kontrolę przez mikrokomputerowy system nadzoru kontrolujący stan chronionego obiektu została stworzona w oparciu o środowisko programowalne LabView. Środowisko programistyczne LabView umożliwia realizację złożonych funkcji w procesach akwizycji, archiwizacji oraz przetwarzaniu i analizie danych pomiarowych. Daje to możliwość dowolnego kreowania struktur programowych systemów pomiarowych i symulacyjnych przydatnych w projektach naukowo-badawczych, ale również tworzenie aplikacji, umożliwiających budowę nowoczesnych systemów sterowania nadzorujących procesy technologiczne. Środowisko to posiada duże możliwości obsługi procesów technologicznych zarówno w zakresie pomiarów i sterowania, ale także zindywidualizowanego podejścia do procesu tworzenia systemów obsługiwanych przez wielu użytkowników [4, 6, 7].

W zależności od uprawnień poszczególni użytkownicy mogą posiadać inny, ściśle określony dostęp do systemu. Dzięki temu system jest stabilny i odporny na działanie nieuprawnionych osób. Dodatkową zaletą stworzonych w programie LabView aplikacji jest ich indywidualność. Możliwe jest wykorzystanie zarówno pewnych schematów jak i wyposażenie programów w indywidualne rozwiązania. Umożliwia to dopasowanie aplikacji do czasami dynamicznie zmieniającej się sytuacji w zabezpieczanym obiekcie (np. zmiany architektoniczne, zmiana przeznaczenia poszczególnych pomieszczeń itp.).

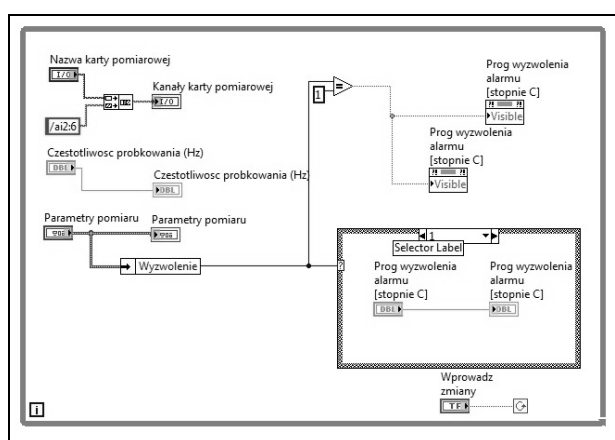
W aplikacji zarządzającej i sterującej pracą systemu można wyróżnić następujące elementy:

- interfejs użytkownika – umożliwia (w zależności od uprawnień) sterowanie, zmianę konfiguracji lub kontrolowanie pracy systemu (rys. 7);
- schemat organizacyjny – wewnętrzne powiązanie pomiędzy poszczególnymi elementami aplikacji umożliwiającą realizację zadań zadanych przez użytkownika na panelu sterującym (rys. 8);
- obsługa I/O (obsługa urządzeń wejścia i wyjścia) – część składowa systemu odpowiedzialna za akwizycję danych o elementach detekcyjnych systemu oraz wysyłanie informacji do urządzeń sterujących pracą elementów wykonawczych lub do użytkowników systemu (rys. 9).

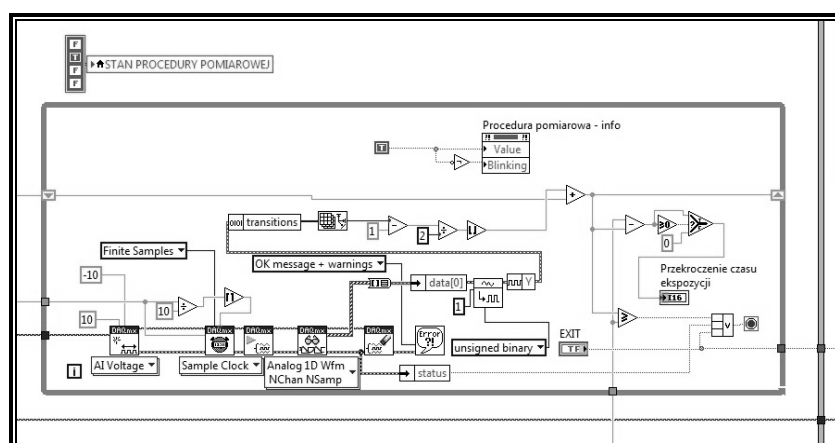
Do przedstawienia możliwości systemu sterowania pracą systemu alarmowego z poziomu komputera wykorzystano aplikację umożliwiającą przekazywanie informacji o stanie obiektu na podstawie pobudzenia układów detekcyjnych w postaci kontaktronów. Przewagą systemu zarządzanego z poziomu komputera jest możliwość dostosowania parametrów aplikacji do potrzeb użytkownika. Na rys. 7 przedstawiono interfejs programu, który umożliwiał zarówno zarządzanie pracą systemu alarmowego oraz sterował pracą kamer PTZ dostępnych w systemie monitoringu wizyjnego chronionego obiektu. Takie rozwiązanie umożliwia wykorzystanie szerokiej gamy możliwości integracji poszczególnych układów sterowania i nadzoru stosowanych w obiekcie. Umożliwia również budowę autonomicznych systemów realizujących tylko wybrany przez użytkownika zakres zadań ochrony. W prezentowane rozwiązanie umożliwia również tworzenie ściśle określonych, dostosowanych do potrzeb danego obiektu paneli kontrolnych i układów wizualizacyjnych odwzorowujących graficznie stan chronionego obiektu.



Rys. 7. Interfejs użytkownika aplikacji umożliwiającej sterowanie pracą systemu i nadzór nad stanem chronionego obiektu



Rys. 8. Procedura kalibracji danych pomiarowych – określenie poziomu wyzwolenia alarmu



Rys. 9. Procedura akwizycji danych pomiarowych – określanie parametrów detekcyjnych układu

Zaproponowany komputerowy system nadzoru umożliwiający sterowanie i kontrolujący pracę systemu alarmowego w zabezpieczanym obiekcie może działać w trybie pracy automatycznej, trybie pracy ręcznej zarządzanej przez użytkownika na stanowisku pracy oraz w trybie pracy awaryjnej zarządzanej przez użytkownika systemu za pomocą sieci Internet w sposób zdalny z poziomu innego komputera. Takie rozwiązanie umożliwia zoptymalizowanie pracy systemu w normalnych warunkach, ale także umożliwia dopasowanie się do aktualnych potrzeb w przypadku wystąpienia stanów awaryjnych lub stanów zagrożenia dla prawidłowego przebiegu procesów przechowywania i produkcji.

Oprócz sterowania i kontroli stanu poszczególnych autonomicznych systemów sterowania komputerowy system nadzoru może być wyposażony w opcję rejestracji zdarzeń. Oznacza to, że powstaje historia pracy poszczególnych elementów systemów zainstalowanych w chronionym obiekcie.

6. WNIOSKI

Systemy alarmowe I&HAS są szczególnym przypadkiem układów nadzoru. Ich wyjątkowość polega na realizacji ważnych zadań i funkcji z zakresu ochrony znajdujących się w dozorowanym obiekcie osób i mienia. Dlatego systemy te muszą spełniać rygorystyczne uwarunkowania w zakresie niezawodności działania systemu i przekazywania informacji o wykrytym zagrożeniu. Im krótszy jest czas pomiędzy chwilą wykrycia zagrożenia a reakcją użytkownika systemu na dane zagrożenie, tym większa szansa na ograniczenie szkód wywołanych tym zagrożeniem.

Istotne staje się wyposażenie systemów nadzoru w środki techniczne, w których proces przekazywania informacji o stanie obiektu na drodze "elementy systemu – układ sterowania: oraz "system – użytkownik" odbywał by się automatycznie, bez zbędnych opóźnień oraz aby informacja o stanie dozorowanego obiektu była dostępna na każde żądanie użytkownika w trybie pracy on-line i nie była ograniczona do pewnego obszaru a także by informacja ta była jak najpełniejsza.

Tym zadaniom mogą sprostać nowoczesne systemy alarmowe I&HAS. Mają one umożliwić nie tylko kontrolę i sterowanie pracą systemu alarmowego w dozorowanym obiekcie, ale umożliwiają szybsze i pełniejsze otrzymywanie informacji o występującym w obiekcie zagrożeniu. Dzięki otrzymywaniu od centrum nadzoru pełnej informacji o stanie każdego z elementów detekcyjnych systemu istnieje możliwość korygowania parametrów innych elementów w sposób ciągły na podstawie adaptacyjnego algorytmu sterowania.

Przeniesienie ośrodka podejmowania decyzji o wielkości zaburzenia i jego interpretacja z elementów detekcyjnych (czujek) do układów sterujących, pełniących rolę central alarmowych umożliwia adaptacyjne ustalanie poziomów wyzwolenia alarmów dla danych układów detekcyjnych na podstawie informacji o zaburzeniach w innych elementach detekcyjnych zainstalowanych w obiekcie. Umożliwia to także wykorzystanie w algorytmie sterowania funkcji arytmetycznych w miejsce obecnie wykorzystywanych funkcji logicznych.

W systemach zarządzanych przez układy komputerowe istnieje możliwość tworzenia procedur polegających na potwierdzeniu otrzymanych informacji i przekazywaniu informacji o aktualnie podejmowanych decyzjach i działaniach przez poszczególne ośrodki (węzły) decyzyjne o wzajemnych poczynaniach każdego z nich. W przypadku takich systemów istnieje duża możliwość tworzenia zintegrowanych układów zarządzających wszystkimi systemami sterowania i nadzoru w całym obiekcie bez konieczności dopasowywania układów komunikacyjnych między nimi, dublowanie układów i elementów oraz budowy wielu poziomowych (kaskadowych) układów nadzoru.

7. BIBLIOGRAFIA

- [1] PN-EN 50131-1 – *Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 1: Wymagania systemowe*, PKN, Warszawa, 2009.
- [2] PN-EN 50136-1-1 – *Systemy alarmowe. Systemy i urządzenia transmisji alarmu. Wymagania ogólne dotyczące systemów transmisji alarmu*, PKN, Warszawa, 2001.
- [3] Buczaj M., *Wykorzystanie telefonii mobilnej i Internetu w procesie przekazywania informacji w systemach nadzorujących stan chronionego obiektu*, Zabezpieczenia nr 1(71)/2010.
- [4] Nawrocki W., *Komputerowe systemy pomiarowe*, WKiŁ, Warszawa, 2006.
- [5] Szulc W., Rosiński A., *Systemy sygnalizacji włamania, część I – Konfiguracje central alarmowych*, Zabezpieczenia nr 2(66)/2009.
- [6] Tłaczała W., *Środowisko LabView w eksperymencie wspomaganym komputerowo*, WNT, Warszawa 2002.
- [7] Chruściel M., *LabView w praktyce*, Wydawnictwo BTC, Legionowo 2008.
- [8] www.raspberry.org.