TRANSCOMP – XIV INTERNATIONAL CONFERENCE
COMPUTER SYSTEMS AIDED SCIENCE, INDUSTRY AND TRANSPORT

*Systemy bezpieczeństwa,*
*Systemy Sygnalizacji Włamania i Napadu,*
*Biometryka*

Zygmunt STRZYŻAKOWSKI[1]
Waldemar SZULC[2]
Adam ROSIŃSKI[3]

# ZINTEGROWANY SYSTEM BEZPIECZEŃSTWA O STEROWANIU BIOMETRYCZNYM

*W artykule zaprezentowano koncepcję zintegrowanego złożonego systemu bezpieczeństwa dla obiektu o specjalnym przeznaczeniu, z zastosowaniem sterujących urządzeń biometrycznych w celu identyfikacji uprawnionych osób. Przedstawiono zagadnienia związane z czytnikami biometrycznymi stosowanymi w systemach Kontroli Dostępu, a następnie ich integrację z innymi systemami (w szczególności z Systemami Sygnalizacji Włamania i Napadu). Opisano przykładowy zintegrowany system bezpieczeństwa i zobrazowano go schematem blokowym. Pozwoliło to na przeprowadzanie analizy niezawodnościowo-eksploatacyjnej. W wyniku jej otrzymano zależności pozwalające wyznaczyć wartości prawdopodobieństwa przebywania rozpatrywanego systemu w określonych stanach.*

# THE INTEGRATED SECURITY SYSTEM WITH BIOMETRICAL CONTROL

*The paper covers the scheme of the integrated security system for special purpose building, the system in which biometric control devices were applied in order to indentify authorized persons. The article discusses issues of biometric readers used in Access Control System and their integration with other systems (especially with Burglary and Robbery Alarm Systems). Moreover, the paper describes the integrated security system and illustrates it on the block scheme. Thus elaborated model allows analysing reliability and exploitation issues. As a result of the analysis some relationships have been obtained that enabled to define probability values of the system operation in particular states.*

[1] Politechnika Radomska, Wydział Transportu i Elektrotechniki, Polska, 26-600 Radom, ul. Malczewskiego 29
[2] Wyższa Szkoła Menedżerska w Warszawie, Wydział Informatyki Stosowanej, Polska, 03-772 Warszawa, ul. Kawęczyńska 36, tel. 22 5900829, e-mail: waldemar.szulc@mac.edu.pl
[3] Politechnika Warszawska, Wydział Transportu, Zakład Telekomunikacji w Transporcie, Polska, 00-662 Warszawa, ul. Koszykowa 75, tel.: 22 2347038, e–mail: adro@it.pw.edu.pl

## 1. WSTĘP

Niniejszy referat jest kontynuacją badań autorów dotyczących elektronicznych systemów bezpieczeństwa o różnych stopniach komplikacji. Badania dotyczyły i nadal dotyczą procesów eksploatacyjno–niezawodnościowych rozproszonych systemów bezpieczeństwa [11,12] ze szczególnym uwzględnieniem tych, zaliczane są do wyższych kategorii zagrożeń (dawne Z3 i Z4) oraz klasyfikowanych jako (stopień 3) i (stopień 4) [8]. Szczególnym badaniom autorów poddane są obiekty specjalnego znaczenia o znacznym złożoności sprzętowej. Obiekty te zwykle posiadają bardzo rozbudowane elektroniczne systemy bezpieczeństwa o charakterze rozproszonym. Zawierają również systemy: telewizji przemysłowej wysokiej rozdzielczości z rejestracją na dyskach HDD i DVD, kontroli dostępu realizowanej jako niezależną lub stanowiącą fragment centrali (opcja), p. pożarowe niezależne lub w ograniczonym zakresie stanowiące również fragment centrali. Bardzo często elektroniczne systemy bezpieczeństwa są powiązane z systemami mechanicznymi (drzwi, okna a w nich szyby o klasyfikowanych klasach, rygle drzwiowe, trzymaki elektromagnetyczne itp.). Autorzy przedstawiają również relacje niezawodnościowo-eksploatacyjne zachodzące w elektronicznych systemach bezpieczeństwa w postaci grafów. Trzeba nadmienić, że obiekty specjalnego przeznaczenia muszą posiadać specjalne czytniki kart lub pastylek Dallas. W tym przypadku po pewnym czasie eksploatacji elektronicznego systemu bezpieczeństwa autorzy opracowali inny system sterowania tego złożonego systemu bezpieczeństwa. Autorzy zamienili pastylki Dallas na biometryczne czytniki linii papilarnych, analizę dłoni, analizę oka (źrenica) jak również bardzo nowoczesny system sterowania biometrycznego dotyczący analizy naczyń krwionośnych np. palca. Ta zamiana wynikała z bardzo ważnej funkcji jaką spełnia pomieszczenie o charakterze specjalnym. Nadal autorzy jednak pozostawili przed pomieszczeniami o charakterze specjalnym, dwie klawiatury (manipulatory) LCD za pomocą których użytkownicy wprowadzają PIN kody. Dostęp do tego pomieszczenia mają określone osoby. Metoda biometryczna sterowania złożonym systemem bezpieczeństwa dla obiektu o specjalnym przeznaczeniu wymaga dużej wiedzy dotyczącej od projektantów i potencjalnych wykonawców systemu. Wiedza ta dotyczyła budowy modelu eksploatacyjno-niezawodnościowego oraz określenia wskaźników gotowości $K_g$ na podstawie obserwacji i badań o długim czasie trwania. Podano więc analizę matematyczną w postaci równań matematycznych za pomocą których można było wyznaczyć wartości prawdopodobieństw przebywania systemów w ściśle określonych stanach eksploatacyjno-niezawodnościowych. Były to jednak propozycje teoretyczne wymagające podbudowy praktycznej. Takie badania autorzy zaczęli realizować poczynając od 2005 r. zbierając dane eksploatacyjno-niezawodnościowe z bardzo wielu elektronicznych systemów bezpieczeństwa o podobnej skomplikowanej budowie i podobnej konfiguracji (opracowano specjalne karty do zbierania danych o uszkodzeniach). W trakcie zbierania danych o uszkodzeniach autorzy napotykali na szereg problemów eksploatacyjno-niezawodnościowych ze szczególnym uwzględnieniem systemów rozproszonych zaprojektowanych i zrealizowanych w obiektach o szczególnym przeznaczeniu (ze zrozumiałych względów nie można podać jakie to są obiekty). Zintegrowany system bezpieczeństwa został zaprojektowany w oparciu o jednostkę mikroprocesorową typu INTEGRA 64 (analizując już rzeczywisty - trudny ze względu na swoje przeznaczenie - obiekt, o którym mowa w niniejszym referacie) [4]. Przedstawiono układ niezawodnościowy elektronicznego systemu bezpieczeństwa interpretujący w/w schemat

ideowy a następnie zbudowano model eksploatacyjno–niezawodnościowy w postaci grafu przejść. Autorzy uwzględnili dane zebrane podczas eksploatacji systemu bezpieczeństwa uwzględniając biometryczne czytniki linii papilarnych. Wykorzystano skomplikowany aparat matematyczny umożliwiający obliczenie przebywania systemu bezpieczeństwa w określonym stanie eksploatacyjnym. Wtedy nasunął się istotny wniosek a mianowicie: niezawodność rozproszonych systemów bezpieczeństwa (czasami zwanych nadzoru) należy kształtować już na etapie projektowania jak również już praktycznej realizacji systemu. Jak już wspomniano, dużym wyzwaniem kiedyś było wprowadzenie biometrycznych czytników linii papilarnych palca. Te zamianę czytników autorzy zrealizowali pod koniec 2008 roku. Można ją (niezawodność) również korygować podczas procesu eksploatacji (np. rozbudowa i modernizacja już istniejącego systemu), poprzez dokonywanie odpowiednich zmian w strukturze niezawodnościowej, choć niektóre bloki systemu są na taka korektę „odporne". Jest jednak wiele innych rozwiązań czytników biometrycznych, o których wspomniano powyżej.

## 2. ZASTOSOWANIE CZYTNIKÓW BIOMETRYCZNYCH W KONTROLI DOSTĘPU

Biometria to precyzyjna identyfikacja ludzi poprzez ich niepowtarzalne charakterystyczne cechy. Istotnymi cechami mogą być: wielkość i kształt dłoni, odciski palców, głos, a także budowa oka (szczególnie źrenica). Czytniki biometryczne znalazły zastosowanie w bardzo wielu instytucjach na świecie. W systemach kontroli dostępu stosuje się je od lat siedemdziesiątych. Początkowo instalowano czytniki biometryczne tylko w instytucjach wymagających specjalnych zabezpieczeń, głównie ze względu na wysoki koszt takich urządzeń. Ostatnio, dzięki tańszym mikroprocesorom i zaawansowanej elektronice, koszt czytników biometrycznych zdecydowanie spadł a ich precyzja działania ogromnie wzrosła. Obniżenie kosztów i wielka dokładność pozwoliły na rozszerzenie zastosowania wyszukanych czytników biometrycznych. Obecnie już nie tylko elektrownie atomowe (jako obiekty specjalnego przeznaczenia), lotniska, wytwórnie papierów wartościowych ale wiele firm może sobie pozwolić na biometryczna kontrolę dostępu a więc kontrolowany przepływ ludzi. Zastosowanie czytników biometrycznych w obiektach specjalnego przeznaczenia to już bardzo często obligatoryjny wymóg inwestora.

Niniejszy referat zajmuje się zagadnieniem integracji biometrii z zadaniami kontroli dostępu nie tylko samodzielnych systemów ale i elektronicznych systemów bezpieczeństwa (zintegrowanych). Celem systemu kontroli dostępu jest dopuszczenie wyłącznie uprawnionych osób do określonych miejsc. Cel można osiągnąć korzystając właśnie z urządzeń i czytników biometrycznych do sterowania systemów bezpieczeństwa. System kontroli dostępu oparty na kartach (wszelkiego typu), bardziej kontroluje dostęp tych kart niż ludzi. Nie jest więc w pełni bezpieczny. Systemy bezpieczeństwa a w nich klawiatury oraz użycie kodów PIN, pozwalają na wejście każdemu, kto zna dany kod, niezależnie od tego, czy jest to osoba uprawniona, czy nie. Tak więc tylko urządzenia z czytnikami biometrycznymi weryfikują faktycznie osobę, która wchodzi na dany teren a więc do konkretnego pomieszczenia lub ciągu pomieszczeń. Sterowanie biometryczne może również wyeliminować konieczność stosowania kart magnetycznych lub innych. Taka opcja daje znaczne oszczędności finansowe i administracyjne a więc także upraszcza logistykę. Utrata karty powoduje konieczność wystawienia nowej. Jeśli chodzi o oko (źrenica) albo rękę to trudno będzie „zgubić" te części ciała człowieka.

Najważniejszą funkcją urządzenia z czytnikiem biometrycznym sterującym systemem bezpieczeństwa jest weryfikacja autentyczności osoby. Kontrola dostępu wymaga jednak nie tylko identyfikacji osoby, lecz również otwierania drzwi, zezwalania na dostęp lub odmawiania go oraz monitorowania alarmów. Takim właśnie zadaniom musi sprostać urządzenie z czytnikami biometrycznymi do sterowania systemami bezpieczeństwa. Znakomita większość systemów kontroli pozwala na kontrolowanie więcej niż jednych drzwi (jednostronnie lub obustronnie). Tak też jest w zaproponowanej przez autorów opcji. W takiej sytuacji można co prawda zastosować kilka systemów pojedynczych, jednak częściej stosuje się rozwiązanie sieciowe. Łącząc czytniki biometryczne ze sobą, a następnie z komputerem, otrzymujemy wygodny i łatwy w obsłudze system kontroli dostępu. Główną zaletą jest możliwość centralnego monitorowania systemami. Tak też jest w zaproponowanym przez autorów elektronicznym systemie bezpieczeństwa. Do komputera, który zlokalizowany jest w pomieszczeniach ochrony, przekazywane są wszystkie zdarzenia oraz aktywowanie punktów drzwiowych (sterowanie ryglami, elektrozaczepami, siłownikami magnetycznymi). Wszystkie zdarzenia rejestrowane są w pamięci komputera i mogą być wykorzystane w dowolnym momencie. Komputer także zarządza „wzorami biometrycznymi" np. liniami papilarnymi palca użytkownika, analiza dłoni, źrenicy oka czy układami krwionośnymi co umożliwia wpisywanie się użytkowników na dowolnym czytniku, a program roześle wzory do pozostałych punktów kontrolnych. Usunięcie użytkownika lub zmiana warunków dostępu odbywa się programowo. Pewne systemy biometryczne, przechowują wszystkie informacje wyłącznie w pamięci komputera i tam też odbywa się weryfikacja wzoru biometrycznego. Inne systemy rozprowadzają wzory biometryczne do poszczególnych czytników. Niezależnie od tego w jaki sposób przechowywane są wzory, to efekt jest taki sam. W ramach sieci czytniki połączone są przez RS-232, RS485 lub przez modem. W systemach głosowych wykorzystuje się np. linie telefoniczne.

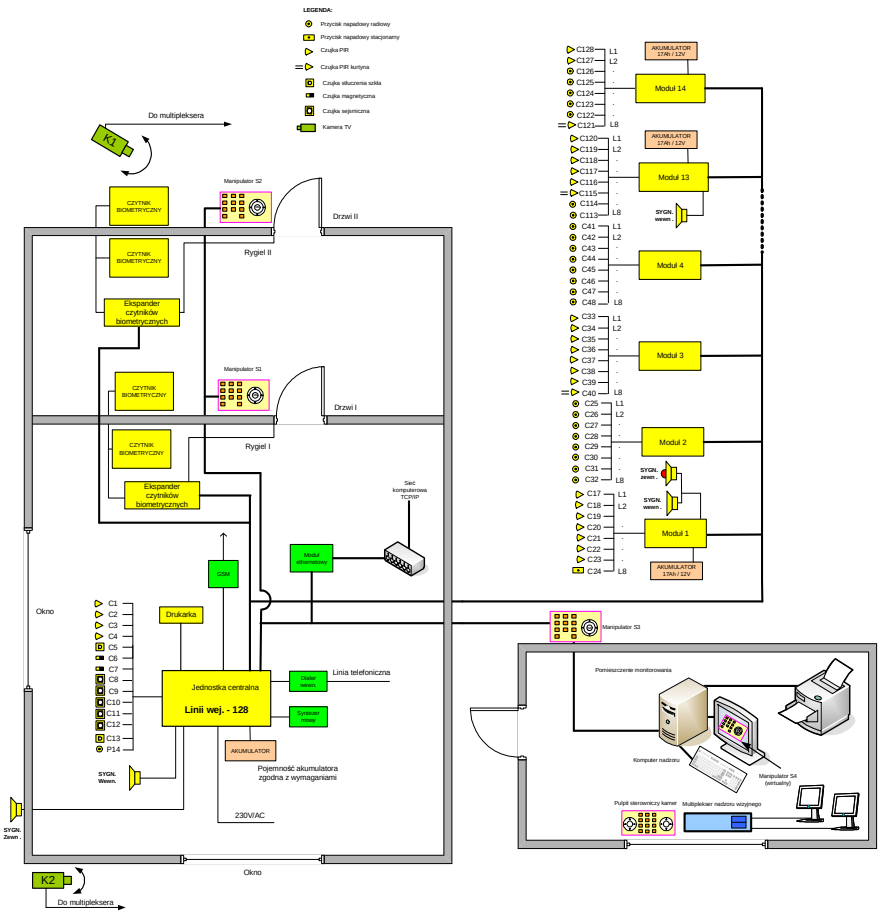
Do istotnych składników stosowania biometrycznych czytników sterujących elektronicznymi systemami bezpieczeństwa należy również zaliczyć:

- Akceptację użytkownika przez czytnik biometryczny,
- Wskaźnik Błędnych Odrzuceń,
- Zrównoważony Wskaźnik Błędu w urządzeniach z czytnikami biometrycznymi,
- Ocena danych statystycznych za zastosowaniem czytników biometrycznych,
- Przepustowość urządzeń z czytnikami biometrycznymi.

## 3. SYNTETYCZNY OPIS PRAKTYCZNEGO ROZPROSZONEGO SYSTEMU BEZPIECZEŃSTWA

Na rys. 1 przedstawiono zmodyfikowany rozproszony system bezpieczeństwa, znacznie rozbudowany i zmodernizowany poprzez wprowadzenie biometrycznych czytników linii papilarnych palca użytkownika upoważnionego. Znaczna modyfikacja systemu bezpieczeństwa, który zrealizowano na przełomie 2008/2009 roku, wynikała z potrzeb i wymagań dla obiektu specjalnego przeznaczenia. Wprowadzono jednostkę mikroprocesorową o 128 liniach wejściowych, dobudowano znaczną ilość modułów rozszerzających (na dwóch magistralach jest ich 14). Znacznie rozbudowano pomieszczenie ochrony, w którym system bezpieczeństwa jest monitorowany. Tam też znajduje się komputer nadzorujący pracę systemu bezpieczeństwa (SSWiN i KD). Kontrola Dostępu została wyposażona w urządzenia z czytnikami biometrycznymi czytającymi linie

papilarne użytkowników. W pomieszczeniu znajduje się również 16 wejściowy multiplekser cyfrowy przeznaczony do monitoringu wizyjnego CCTV z rejestracją zdarzeń na 4 dyskach HDD o pojemności po 1TB każdy [3,6,9]. Również w tym pomieszczeniu znajdują się dwie drogi monitorowania: telekomunikacyjnego i radiowego [2,7]. Elektroniczny system bezpieczeństwa został wyposażony w cztery manipulatory LCD, w tym jeden wirtualny. Dwa manipulatory LCD współpracują w systemie Kontroli Dostępu dla obsługi pomieszczenia specjalnego przeznaczenia. Również te pomieszczenia zostały wyposażone w specjalne drzwi (atestowane) z atestowanymi zamkami mechanicznymi. Kontrola Dostępu współpracuje również ze zworami elektromagnetycznymi (wynika to z logistyki obiektu). Z pomieszczenia monitorowania są sterowane szybkoobrotowe głowice kamer TV jak i ich obiektywy – zoomy z dobranymi ogniskowymi. Rezerwowe źródła zasilania (akumulatory) umożliwiają przez min. 72 godz. na pracę systemu bezpieczeństwa w przypadku awarii zasilania zasadniczego (230V). Kamery monitoringu wizyjnego współpracują z oświetlaczami podczerwonymi (wewnętrznymi) o zasięgu (od 8m do 25m) oraz zewnętrznymi o zasięgu ok. 50m i więcej.



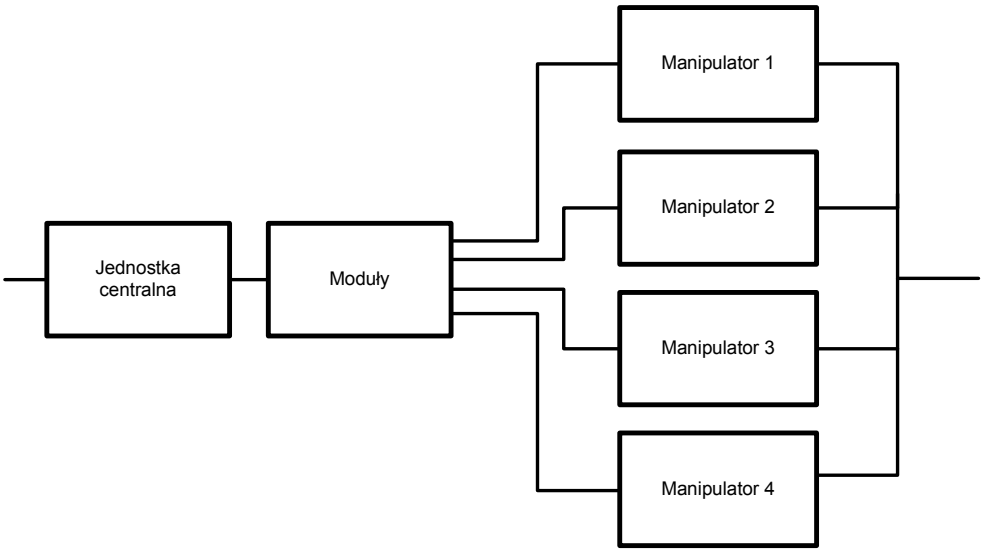

*Rys. 1. Schemat blokowy rozproszonego sytemu bezpieczeństwa*

Warto również wspomnieć o mechanicznych zabezpieczeniach zaproponowanych i zrealizowanych w obiekcie rzeczywistym specjalnego przeznaczenia. Są to specjalne okna posiadające szyby odpowiedniej kategorii. W pomieszczeniach widocznych na rys. 1 zostały zainstalowane atestowane stalowe drzwi (I i II) z szeregiem zamków z atestami. Rygle elektromagnetyczne są sterowane biometrycznymi czytnikami linii papilarnych (z rejestracją wej./wyj). System Kontroli Dostępu zastosowany w pomieszczeniu przedstawionym na rys. 1, który jest zrealizowany na tej samej jednostce mikroprocesorowej (INTEGRA 128), chroni również wybrane pomieszczenie przeciwpożarowo. Jest zrealizowana zasada współpracy KD i systemu przeciwpożarowego (względy bezpieczeństwa). Pomieszczenia posiadają specjalne konstrukcje budowlane. Ściany, podłogi, sufity są chronione czujkami sejsmicznymi. Podobnymi czujkami są chronione sejfy pancerne. Trzeba również wspomnieć o kompatybilności elektromagnetycznej a więc o zakłóceniach elektromagnetycznych, które stanowią bardzo ważny problem w systemach bezpieczeństwa o tak skomplikowanej budowie. Należy także nadmienić, że centrala alarmowa współpracuje z siecią informatyczną za pośrednictwem modułu ethernetowego. Pozwala taka metoda, zarządzać i administrować elektronicznym systemem bezpieczeństwa w sposób zdalny. Taki system jest jednak wrażliwy na zakłócenia radioelektryczne a więc powinien być wykonany bardzo starannie. Ze względów bezpieczeństwa wszystkie pomieszczenia podtynkowo, są wyposażone w metalowe siatki stanowiące barierę elektromagnetyczną.

Analizując zaproponowany układ elektronicznego systemu bezpieczeństwa ze sterowaniem biometrycznym, autorzy zbudowali model eksploatacyjno – niezawodnościowy tego skomplikowanego systemu.

## 4. MODEL EKSPLOATACYJNO-NIEZAWODNOŚCIOWY RZECZYWISTEGO SYSTEMU BEZPIECZEŃSTWA

Na rys. 2 przedstawiono model eksploatacyjno-niezawodnościowy [1,5,10,13,14], który powstał w wyniku analizy rzeczywistego elektronicznego systemu bezpieczeństwa przedstawionego na rys. 1. Ze względu na duży stopień komplikacji rzeczywistego systemu bezpieczeństwa, zastosowano metodę niezbędnych uproszczeń ale takich, które nie wypaczą logiki badań.




*Rys. 2. Schemat niezawodnościowy systemu bezpieczeństwa (model interpretujący rys.1)*

Wszystkie 14 modułów rozszerzających zostały przedstawione w postaci jednego bloku i dołączone do bloku jednostki mikroprocesorowej (centralnej). Do magistral zostały, ze względów logistycznych, dołączone 4 manipulatory LCD, w tym jeden wirtualny. Tak zbudowany schemat eksploatacyjno-niezawodnościowy stanowi tzw. mieszany model niezawodnościowy. Można tu mówić też o problemie nadmiarowości. Warto przypomnieć, że z punktu widzenia eksploatacji i niezawodności, można wyróżnić następujące rodzaje nadmiarowości:

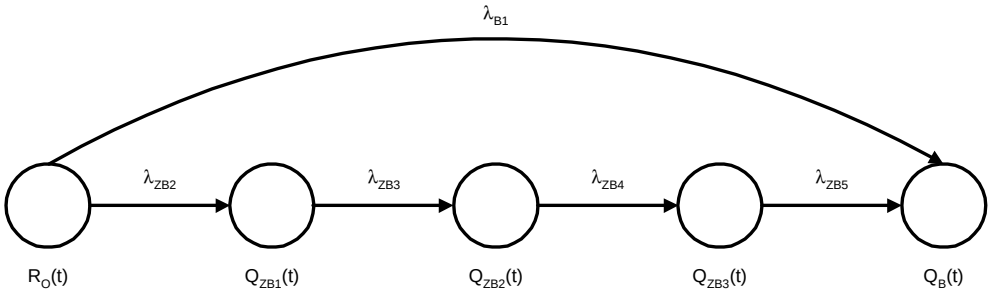
- nadmiar strukturalny,
- nadmiar funkcjonalny,
- nadmiar parametryczny,
- nadmiar informacyjny,
- nadmiar wytrzymałościowy,
- nadmiar czasowy,
- nadmiar elementowy,

Podane nadmiary mogą być spełniane jednocześnie, zwłaszcza przy tak trudnym i rozległym elektronicznym systemie bezpieczeństwa.

Analizując szczegółowo schemat przedstawiony na rys. 1 i jego uproszczony schemat niezawodnościowy (rys. 2), można stwierdzić że mogą mieć miejsce wszystkie w/w nadmiary. Jednak do badań szczególnie istotne są dwa nadmiary: strukturalny (przypadek przejścia na rezerwowe źródło zasilania w przypadku awarii źródła zasadniczego) i funkcjonalny (kilka manipulatorów LCD, w tym wirtualny). Ten ostatni nadmiar funkcjonalny jest w tym przypadku bardzo ważny ze względu na logikę i procedury obowiązujące w tego typu obiektach specjalnego znaczenia.

W wyniku analizy blokowego schematu niezawodnościowego (uproszczonego) przedstawionego na rys. 2, autorzy zaproponowali graf relacji zachodzących w

rozproszonym systemie bezpieczeństwa. Relacje zachodzące w systemie rozproszonego systemu bezpieczeństwa dla rzeczywistego obiektu zostały przedstawione na rys. 3.




*Rys. 3. Relacje zachodzące w systemie bezpieczeństwa (na podstawie rys.2)*

*gdzie:*

$R_O(t)$ *– funkcja prawdopodobieństwa przebywania systemu w stanie pełnej zdatności,*

$Q_{ZB}(t)$ *– funkcja prawdopodobieństwa przebywania systemu w stanie zagrożenia bezpieczeństwa,*

$Q_B(t)$ *– funkcja prawdopodobieństwa przebywania systemu w stanie zawodności bezpieczeństwa,*

$\lambda_{B1}$ *– intensywność przejść central i modułów,*

$\lambda_{ZB2}$ , $\lambda_{ZB3}$ , $\lambda_{ZB4}$ , $\lambda_{ZB5}$ *– intensywność przejść manipulatorów*

Jeżeli zastosuje się przekształcenia matematyczne (bardzo skomplikowane) to można otrzymać wynikowe zależności, które pozwolą wyznaczyć wartości prawdopodobieństw przebywania rozważanego (rzeczywistego) elektronicznego systemu bezpieczeństwa w odpowiednich stanach:

- stan pełnej zdatności $R_0$

$$R_0(t) = e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t} \tag{1}$$

- stan zagrożenia bezpieczeństwa $Q_{ZB1}$ przedstawiono w równaniu (2)

$$Q_{ZB1}(t) = \lambda_{ZB2} \cdot \left[ \frac{e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t} - e^{-\lambda_{ZB3}\cdot t}}{\lambda_{ZB3} - \lambda_{B1} - \lambda_{ZB2}} \right] \tag{2}$$

- stan zagrożenia bezpieczeństwa $Q_{ZB2}$ przedstawiono w równaniu (3)

$$Q_{ZB2}(t) = \lambda_{ZB2} \cdot \lambda_{ZB3} \cdot \left[ \begin{array}{l} \dfrac{e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t}}{(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3})} - \\ -\dfrac{e^{-\lambda_{ZB3}\cdot t}}{(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3})\cdot(\lambda_{ZB3}-\lambda_{ZB4})} + \\ +\dfrac{e^{-\lambda_{ZB4}\cdot t}}{(\lambda_{ZB3}-\lambda_{ZB4})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4})} \end{array} \right] \tag{3}$$

- stan zagrożenia bezpieczeństwa $Q_{ZB3}$ przedstawiono w równaniu (4)

$$Q_{ZB3}(t) = \lambda_{ZB2} \cdot \lambda_{ZB3} \cdot \lambda_{ZB4} \cdot \left[ \begin{array}{l} \dfrac{e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t}}{(-\lambda_{B1}-\lambda_{ZB2}+\lambda_{ZB5})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3})} - \\ -\dfrac{e^{-\lambda_{ZB3}\cdot t}}{(\lambda_{ZB5}-\lambda_{ZB3})(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3})\cdot(\lambda_{ZB3}-\lambda_{ZB4})} + \\ +\dfrac{e^{-\lambda_{ZB4}\cdot t}}{(\lambda_{ZB5}-\lambda_{ZB4})\cdot(\lambda_{ZB4}-\lambda_{ZB3})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4})} - \\ -\dfrac{e^{-\lambda_{ZB5}\cdot t}}{(\lambda_{ZB5}-\lambda_{ZB3})\cdot(\lambda_{ZB5}-\lambda_{ZB4})\cdot(-\lambda_{B1}-\lambda_{ZB2}+\lambda_{ZB5})} \end{array} \right] \tag{4}$$

- stan zawodności bezpieczeństwa $Q_B$ przedstawiono w równaniu (5)

$$Q_B(t) = \frac{\lambda_{B1}}{\lambda_{B1} + \lambda_{ZB2}} \cdot \left[1 - e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t}\right] + \lambda_{ZB2} \cdot \lambda_{ZB3} \cdot \lambda_{ZB4} \cdot \lambda_{ZB5} \cdot$$

$$\cdot \left[ \begin{array}{l} \dfrac{-e^{-(\lambda_{B1}+\lambda_{ZB2})\cdot t}}{(\lambda_{B1}+\lambda_{ZB2})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4})\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3})\cdot(-\lambda_{B1}-\lambda_{ZB2}+\lambda_{ZB5})} + \\ + \dfrac{e^{-\lambda_{ZB3}\cdot t}}{(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB3})\cdot\lambda_{ZB3}\cdot(\lambda_{ZB3}-\lambda_{ZB4})\cdot(\lambda_{ZB5}-\lambda_{ZB3})} - \\ - \dfrac{e^{-\lambda_{ZB4}\cdot t}}{(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZB4})\cdot(\lambda_{ZB3}-\lambda_{ZB4})\cdot\lambda_{ZB4}\cdot(\lambda_{ZB5}-\lambda_{ZB4})} + \\ + \dfrac{e^{-\lambda_{ZB5}\cdot t}}{\lambda_{ZB5}\cdot(-\lambda_{B1}-\lambda_{ZB2}+\lambda_{ZB5})\cdot(\lambda_{ZB5}-\lambda_{ZB4})\cdot(\lambda_{ZB5}-\lambda_{ZB3})} + \\ + \dfrac{1}{(\lambda_{B1}+\lambda_{ZB2})\cdot\lambda_{ZB3}\cdot\lambda_{ZB4}\cdot\lambda_{ZB5}} \end{array} \right] \quad (5)$$

Oznaczenia w powyższych zależnościach są następujące:
t – czas,
$\lambda_{B1}$ – intensywność przejść central i modułów,
$\lambda_{ZB}$ – intensywność przejść manipulatora LCD

## 5. OBLICZENIA WSKAŹNIKÓW NIEZAWODNOŚCIOWO-EKSPLOATACYJNYCH

Do obliczeń przyjęto kilka istotnych danych dotyczących badanych systemów:
Czas obserwacji systemu – 1 rok = 8760 h.
Liczba badanych systemów: 10 (takich jak na rys. 1 lub podobnych)

Otrzymane wartości prawdopodobieństw przebywania systemu w:
- stan pełnej zdatności systemu $R_0$: 0,9504
- stan zagrożenia bezpieczeństwa $Q_{ZB1}$: 0,039195
- stan zagrożenia bezpieczeństwa $Q_{ZB2}$: 0,000601
- stan zagrożenia bezpieczeństwa $Q_{ZB3}$: 0,000004
- stan zawodności bezpieczeństwa $Q_{B:}$ 0,009798

Powyższe wskaźniki zostały wyliczone na podstawie w/w równań z wykorzystaniem autorskiego programu komputerowego wspomagania Decyzji Niezawodnościowo – Eksploatacyjnych Elektronicznych Systemów Nadzoru.

## 6. WNIOSKI

Przedstawione wyniki obliczeń wymagają pewnych wyjaśnień. Gdyby przyjąć za ostateczny wynik $R_0 = 0,9504$ a więc stan pełnej zdatności zintegrowanego elektronicznego systemu bezpieczeństwa ze sterowaniem biometrycznym to wynik ten nie byłby

satysfakcjonujący. Należy brać jednak pod uwagę, czego dotyczą wskaźniki: $Q_{ZB1,}$ $Q_{ZB2,}$ $Q_{ZB3}$? Wyliczone wartości dotyczą stanu zagrożenia bezpieczeństwa wynikające z niezdatności kolejnych trzech manipulatorów LCD (w systemie bezpieczeństwa jest ich 4 szt.).

Aby więc mieć pełny obraz pełnej zdatności zintegrowanego elektronicznego systemu bezpieczeństwa przedstawionego na rys. 1 należy przyjąć pewne założenia a mianowicie:

- wszystkie manipulatory LCD (3 szt.) realizują identyczne funkcje,
- podobnie i czwarty manipulator lecz wirtualny (jednak rozpatrywany rozdzielnie),
- urządzenia z czytnikami biometrycznymi realizują zbliżone funkcje,

Jeśli przyjąć takie założenie, to całkowity stan pełnej zdatności zintegrowanego elektronicznego systemu bezpieczeństwa można wyrazić równaniem (6)

$$R_{0(całk)} = R_0 + Q_{ZB1} + Q_{ZB2} + Q_{ZB3} = 0{,}9504 + 0{,}039195 + 0{,}000601 + 0{,}000004 = 0{,}9902 \quad (6)$$

Można więc przedstawić warunek (7) wystarczający dla analizowanego elektronicznego systemu bezpieczeństwa obiektu specjalnego przeznaczenia:

$$0{,}9504 \leq R_{0całk.} \leq 0{,}9902 \quad (7)$$

Analizując nierówność (7) można odczytać, że dla granicy prawostronnej zdatny jest tylko manipulator wirtualny a dla lewostronnej zdatne są wszystkie manipulatory. Tak więc w podanym przedziale można przyjąć, że system bezpieczeństwa znajduje się w pełnej zdatności. W trakcie analizy elektronicznego systemu bezpieczeństwa posiadający urządzenia z czytnikami biometrycznymi nie były brane pod uwagę wszystkie procedury dotyczące obiektu specjalnego przeznaczenia. W przypadku gdy wszystkie cztery manipulatory są w stanie zawodności bezpieczeństwa (jest to przypadek możliwy), analizowany system bezpieczeństwa nie nadaje się do dalszej eksploatacji. W stosunku do poprzedniej wersji, w której pastylki Dallas (4 szt.) zostały zamienione na czytniki biometryczne (4 szt.), jest on znacznie bezpieczniejszy w eksploatacji i praktycznie całkowicie eliminujące manipulacje niesolidnych użytkowników.

## 7. BIBLIOGRAFIA

[1] Będkowski L., Dąbrowski T.: Podstawy eksploatacji, cz. II Podstawy niezawodności eksploatacyjnej. Wojskowa Akademia Techniczna, Warszawa 2006.
[2] Haykin S.: *Systemy telekomunikacyjne. Tom I i II*, Warszawa, WKiŁ 2004.
[3] Instrukcje programowania, serwisowe i użytkowników systemów monitoringu wizyjnego firmy SONY.
[4] Instrukcje programowania, serwisowe i użytkowników systemów sygnalizacji włamania i napadu firmy SATEL.
[5] Jaźwiński J., Ważyńska-Fiok K.: Bezpieczeństwo systemów. PWN, Warszawa 1993.
[6] Kałużny P.: Telewizyjne systemy dozorowe. WKiŁ, Warszawa 2008.
[7] Mikulik J. (praca pod red. E. Niezabitowskiej): Budynek inteligentny. T. 2, Podstawowe systemy bezpieczeństwa w budynkach inteligentnych. Wydawnictwo Politechniki Śląskiej, Gliwice 2005.

[8] Norma PN-EN 50131-1:2009: Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe.
[9] Norma PN-EN 50132-7:2003: Systemy alarmowe -- Systemy dozorowe CCTV stosowane w zabezpieczeniach -- Część 7: Wytyczne stosowania.
[10] Rosiński A.: Analiza struktur niezawodnościowych w rozproszonych systemach bezpieczeństwa. Zabezpieczenia Nr 1/2 (41/42)/2005, wyd. AAT, Warszawa.
[11] Szulc W. Rosiński A.: Prace własne dot. Elektronicznych Systemów Bezpieczeństwa w Wyższej Szkole Menedżerskiej w Warszawie, Warszawa 2008/2009.
[12] Szulc W., Rosiński A.: Badania własne dot. analizy uszkodzeń w rozproszonych systemach bezpieczeństwa (lata 2005 do 2008).
[13] Szulc W., Rosiński A.: Problemy eksploatacyjno-niezawodnościowe rozproszonego systemu bezpieczeństwa. Zabezpieczenia Nr 1 (47)/2006, wyd. AAT, Warszawa 2006.
[14] Ważyńska-Fiok K., Jaźwiński J.: Niezawodność systemów technicznych. Warszawa, PWN 1990.