Marcin JACHIMSKI[1], Zbigniew MIKOŚ[1], Grzegorz WRÓBEL[1]

AGH Akademia Górniczo-Hutnicza, Katedra Energoelektroniki i Automatyki Systemów Przetwarzania Energii (1)

doi:10.15199/48.2015.04.25

Systemy automatyki budynku realizujące funkcje bezpieczeństwa – struktury sprzętu

Streszczenie. *W artykule przedstawiono koncepcję integracji funkcji bezpieczeństwa w ramach rozproszonych systemów automatyki i sterowania budynków. Rozważono zastosowanie norm PN-EN 61508 oraz PN-EN ISO 13849. Zaproponowano zastosowanie struktury wielokanałowej z głosowaniem MooN i diagnostyką, pozwalającej na osiągnięcie poziomu nienaruszalności bezpieczeństwa SIL-3, dla poszczególnych elementów systemu sterowania realizujących funkcję bezpieczeństwa.*

Abstract*. The paper presents the concept of integration of safety functions within the distributed building automation and control system. Using the PN-EN 61508 and PN-EN ISO 13849 standards was considered. Using the multi-channel architecture of the vote MooN with diagnostics was proposed to achieve the safety integrity level SIL 3 of each control system element which performs safety function.(**Building automation systems performing safety functions - hardware structures**)*

Słowa kluczowe: automatyka budynku, bezpieczeństwo funkcjonalne, systemy rozproszone, BACS
Keywords: building automation, functional safety, distributed systems, BACS

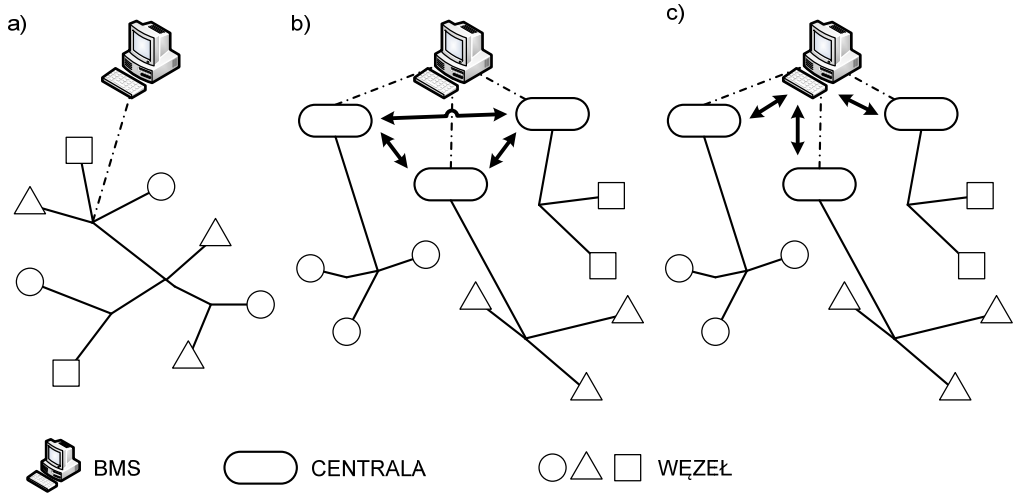
Wstęp

W systemach automatyki i sterowania budynkiem (BACS – ang. Building Automation and Control Systems) zgodnie z obowiązującymi trendami oraz normami (PN-EN 15232, PN-EN 14908, PN-EN ISO 16484, PN-EN 13321) powinno się dążyć do integracji sterowania różnych podsystemów funkcjonalnych, takich jak: system ogrzewania wentylacji i klimatyzacji (HVAC – ang. Heating, Ventilation, Air Conditioning), system sterownia oświetleniem (awaryjnym, zewnętrznym), system sygnalizacji alarmu pożaru (SAP), system kontroli dostępu (KD), dźwiękowy system ostrzegawczy (DSO), system sygnalizacji włamania i napadu (SSWIN), system sterownia oświetleniem awaryjnym (ang. emergency lighting), system monitoringu zużycia mediów (prąd, gaz, woda itp.) i innych w ramach wspólnego systemu BACS. System taki powinien współdziałać z systemem zarządzania budynkiem (BMS – ang. Building Management System).

Najlepsze rezultaty sterowania, w tym również najlepszą efektywność energetyczną można osiągnąć dzięki stosowaniu nowoczesnych, rozproszonych i otwartych systemów sterowania zgodnie z powszechnie przyjętymi standardami (LonWorks [1], BACnet [2], KNX [3]). Układy sterowania podsystemów funkcjonalnych należy integrować na niskim poziomie (obiektowym) [4] – poziomie czujników i urządzeń sterujących.

Wnioski takie zawiera miedzy innymi norma PN-EN 15232 – 2012 „Energetyczne właściwości budynków - Wpływ automatyzacji, sterowania i technicznego zarządzania budynkami" [5]. Stwierdzone zostało to również już przez wczesne badania z udziałem autorów wykonane przed publikacją normy w latach 1999-2002 w [6][7], a także późniejsze badania w latach 2010-2013 w ramach projektów badawczych NCBiR i NCN [8][9].

Jak pokazuje praktyka, na polskim rynku budowlanym regułą jest, że podsystemy bezpośrednio odpowiedzialne za bezpieczeństwo osób lub majątku znacznej wartości (np. kontroli dostępu (KD), sygnalizacji włamania i napadu (SSWIN), system sygnalizacji alarmu pożaru (SAP), oddymiania, dźwiękowy system ostrzegawczy (DSO) czy sterowania windami są realizowane jako oddzielne, certyfikowane podsystemy, a ich integracja z pozostałymi podsystemami następuje na wysokim poziomie (central podsystemów lub BMS – rys. 1). Na ogół podsystemy te są realizowane jako systemy z tzw. centralą, a nie jak wspomniane wcześniej, uznane międzynarodowymi i polskimi normami otwarte rozproszone systemy sterowania charakterystyczne dla nowoczesnych rozwiązań automatyki budynku. Powoduje to, że integracja ich jest utrudniona i możliwa wyłącznie na wyższych warstwach systemu sterowania.



Rys. 1. Systemy rozproszone BACS a) integracja na niskim poziomie, b) integracja na poziomie central, c) integracja na poziomie BMS

Czy jest możliwa prawidłowa realizacja podsystemów systemu BACS odpowiedzialnych za bezpieczeństwo osób lub majątku znacznej wartości w ramach rozproszonego systemu sterowania?

Dla prawidłowej realizacji podsystemów sterowania odpowiedzialnych za bezpieczeństwo konieczna jest integracja funkcji tych podsystemów w ramach rozproszonego systemu sterowania (zgodnie z technologią jego wykonania BACnet, LonWorks czy KNX). Aby podsystemy te spełniały swoją rolę powinny w ramach realizowanych funkcji zapewniać wysoki poziom niezawodności oraz właściwy dla nich poziom bezpieczeństwa dla użytkowników. Odpowiedni poziom bezpieczeństwa powinien być zapewniony również na styku podsystemów sterowania realizujących różne funkcje Na przykład, w aktualnej praktyce budowlanej, system powiadamiania o pożarze SAP w momencie wykrycia zagrożenia oprócz funkcji alarmowania przekazuje sygnały do systemów oddymiania, gaszenia, KD, DSO oraz HVAC. Pomimo, że podsystem SAP zapewnia pożądany poziom bezpieczeństwa użytkowników budynku, to często powiadomienia do innych podsystemów są przekazywane zwykłym sygnałem dwustanowym (poziom central podsystemów) lub poprzez komputer PC działający pod kontrolą systemu operacyjnego Windows (poziom BMS).

Dodatkowo sygnał dwustanowy jest często używany jako aktywny w momencie wystąpienia zagrożenia. W systemach sterowania przemysłowego natomiast powszechnie przyjętą i zasadną konwencją jest zadziałanie zabezpieczeń w przypadku nieaktywności (braku zasilania) sygnału.

Przy takiej praktyce awaria obwodu pojedynczego sygnału dwustanowego lub awaria komputera PC czy błąd systemu operacyjnego Windows może zablokować przejścia, podsycić pożar niewłaściwym nawiewem lub uniemożliwić nadanie odpowiedniego komunikatu DSO. Zatem nieprawidłowe działanie budynkowych systemów sterowania może zagrażać bezpieczeństwu ludzi.

Bezpieczeństwo funkcjonalne w systemach automatyki budynku.

Systemy automatyki budynku należy projektować tak aby swym nieprawidłowym działaniem nie powodowały niebezpieczeństwa dla użytkowników. Ponieważ całkowite wyeliminowanie ryzyka wynikającego z nieprawidłowego zadziałania systemów sterowania jest niemożliwe, należy dążyć do ograniczenia tego ryzyka do poziomu ryzyka tolerowanego. Systemy automatyki budynków, w zakresie elementów odpowiedzialnych za bezpieczeństwo, powinny być konstruowane w taki sposób, aby minimalizować ryzyko wystąpienia niewykrywalnych uszkodzeń, natomiast uszkodzenia wykrywalne powinny w sposób automatyczny ustawiać elementy systemu w stan bezpieczny (niezagrażający bezpieczeństwu) oraz sygnalizować uszkodzenie.

Reasumując – podsystemy automatyki budynku, które są odpowiedzialne za bezpieczeństwo osób lub mienia znacznej wartości powinny być wyposażane w funkcje bezpieczeństwa ograniczające ryzyko związane z możliwością błędnego działania mogącego temu bezpieczeństwu zagrozić.

Aktualnie najważniejszymi normami w tym obszarze są:
– PN-EN 61508: Bezpieczeństwo funkcjonalne związanych z bezpieczeństwem systemów elektrycznych / elektronicznych / programowalnych systemów elektronicznych
– PN-EN ISO 13849: Bezpieczeństwo maszyn - Elementy systemów sterowania związane z bezpieczeństwem
– PN/EN/IEC 62061: Bezpieczeństwo maszyn - Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i programowalnych elektronicznych systemów sterowania związanych z bezpieczeństwem (na bazie PN-EN 61508 - SIL)
– EN/IEC 61511: Bezpieczeństwo funkcjonalne - Przyrządowe systemy bezpieczeństwa dla sektora procesów przemysłowych (na bazie PN-EN 61508 - SIL)

Ze względu na obszar zastosowań w systemach automatyki budynku jak i sposób realizacji technicznej, jako normę wiodącą należy przyjąć PN-EN 61508 [10], ponieważ systemy sterowania automatyki budynku są budowane w oparciu o urządzenia elektryczne, elektroniczne i programowalne elektroniczne (E/E/PE – Electrical / Electronic / Programmable Electronic) i w taki też sposób będą realizowane zabezpieczenia. Norma PN-EN 61508 i pochodne określają poziom redukcji ryzyka poprzez SIL (SIL – Safety Integrity Level) a norma maszynowa PN-EN ISO 13849 [11] poprzez PL (PL – Performance Level). Zarówno SIL (poziom 1-4) jak i PL (poziom a-e) (Tab. 1) są miarami niezawodności funkcji bezpieczeństwa.

Dalsze rozważania, jako dotyczące systemów E/E/PE, zostaną odniesione do normy wiodącej w tym zakresie – PN-EN 61508.

Tabela1. Porównanie SIL (rodzaj pracy na częste przywołanie) i PL

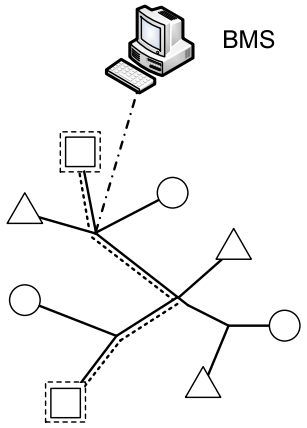
SIL (PN-EN 61508)	PL (PN-EN ISO 13849)	Średnie prawdopodobieństwo niebezpiecznego uszkodzenia na godzinę
---	a	$\geq 10^{-5}$ do $< 10^{-4}$
1	b	$\geq 3*10^{-6}$ do $< 10^{-5}$
	c	$\geq 10^{-6}$ do $< 3*10^{-6}$
2	d	$\geq 10^{-7}$ do $< 10^{-6}$
3	e	$\geq 10^{-8}$ do $< 10^{-7}$
4	---	$\geq 10^{-9}$ do $< 10^{-8}$

Zgodnie z tą normą w celu ograniczenia ryzyka należy przeprowadzić analizę ryzyka i na tej podstawie opracować wymagania bezpieczeństwa, co prowadzi z kolei do określenia wymagań dotyczących poziomu nienaruszalności bezpieczeństwa.

Składnikami rozproszonych systemów automatyki budynku są: urządzenia (sprzęt urządzeń elektronicznych programowalnych razem z oprogramowaniem) oraz sieci sterujące (protokoły transmisji danych).

Systemy automatyki budynku składają się z wielu urządzeń kompletowanych indywidualnie w momencie projektowania systemu dla konkretnego budynku, zintegrowanych w ramach jednej sieci sterującej. Nie jest zatem możliwe rozpatrzenie a priori wszystkich możliwych konfiguracji, które mogłyby być zaprojektowane w celu realizacji bezpiecznych funkcjonalności w ramach systemu automatyki. Zgodnie z wymaganiami normy każdorazowo należy rozpatrywać to oddzielnie. Można natomiast opracować elementy – podsystemy składowe (czujniki, sterowniki, urządzenia wykonawcze i protokoły sieci sterujących), które współdziałając mogłyby realizować bezpieczne funkcje sterowania (o ograniczonym ryzyku niebezpiecznego w skutkach błędu lub uszkodzenia), w ramach rozproszonego systemu sterowania automatyki budynku (rys. 2).

Zgodnie z normą ograniczenie ryzyka niebezpiecznego w skutkach błędu lub uszkodzenia może być realizowane poprzez umieszczenie w urządzeniach (podsystemach) i systemach odpowiednich funkcji bezpieczeństwa.

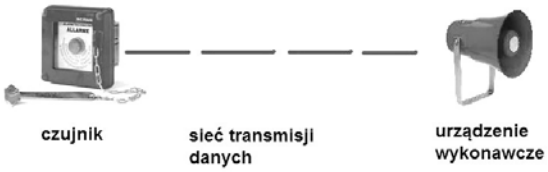


Rys. 2: Integracja funkcji bezpieczeństwa w ramach rozproszonego systemu automatyki budynku. Linią przerywaną oznaczono elementy realizujące funkcję bezpieczeństwa

Dla jakiego poziomu SIL należy opracować elementy rozproszonego systemu automatyki budynku realizujące funkcję bezpieczeństwa?

Aby ryzyko zagrażającego bezpieczeństwu ludzi błędu systemu ograniczyć do poziomu niższego od ryzyka tolerowanego, należy zastosować system sterowania automatyki budynku realizujący funkcje bezpieczeństwa o określonym poziomie SIL wynikającym z analizy ryzyka dla konkretnej funkcji bezpieczeństwa (musi spełniać odpowiedni poziom nienaruszalności bezpieczeństwa SIL). Każdorazowo należy również zdecydować czy funkcja bezpieczeństwa jest funkcją na rzadkie przywołanie (gdy jest przywoływana rzadziej niż raz na rok i nie częściej niż wynosi dwukrotność okresów między testami diagnostycznymi), czy na ciągłe przywołanie (gdy jest przywoływana częściej niż raz na rok lub częściej niż wynosi dwukrotność okresów między testami diagnostycznymi). Przy rzadkim przywołaniu SIL wyraża się średnim prawdopodobieństwem uszkodzenia wykonania funkcji bezpieczeństwa, a przy ciągłym lub częstym przywołaniu prawdopodobieństwem uszkodzenia niebezpiecznego funkcji na godzinę.

W automatyce budynkowej dominują funkcje bezpieczeństwa na rzadkie przywołanie, gdyż możliwość ich przywołania wystąpi w wyniku sporadycznych (losowych) zdarzeń (np. pożar), w przeciwieństwie do maszyn lub do automatyki procesowej, gdzie mamy do czynienia z częstymi przywołaniami.



Rys. 3. System realizujący funkcje bezpieczeństwa złożony z kilku elementów – podsystemów (czujnik, sieć transmisji danych, urządzenie wykonawcze)

Zdaniem autorów zasadnym poziomem nienaruszalności bezpieczeństwa dla urządzeń automatyki budynku (czujniki, sterowniki, sieć i protokół transmisji danych), podobnie jak dla urządzeń automatyki przemysłowej (np. PLC), jest SIL-3 [12][13]. Wymagany poziom SIL dla realizacji konkretnej funkcji musi wynikać z analizy ryzyka dla konkretnego przypadku. Decydując się na produkcję urządzeń E/E/EP przeznaczonych do realizacji funkcji bezpieczeństwa warto przyjąć SIL-3 [Tab. 2], ponieważ nawet przy tak wymagającym założeniu system złożony z kilku urządzeń oraz sieci transmisji danych może osiągać niższy poziom nienaruszalności bezpieczeństwa [14] (rys. 3). Wykonanie urządzeń dla poziomu SIL-4 jest znacznie bardziej skomplikowane i kosztowne, a realizacja tak ostrych wymagań dla sieci miejscowej byłaby trudna do spełnienia. Zalecany poziom SIL jest zawsze kompromisem pomiędzy bezpieczeństwem a kosztem zapewnienia bezpieczeństwa.

Tabela 2: Poziom SIL i prawdopodobieństwo wystąpienia błędu powodującego utratę funkcji bezpieczeństwa (rodzaj pracy na rzadkie przywołanie)

Poziom integralności bezpieczeństwa (SIL)	Prawdopodobieństwo błędu w trybie pracy na żądanie	Współczynnik redukcji ryzyka
4	$\geq 10^{-5}$ do $< 10^{-4}$	> 10,000 do ≤ 100,000 razy
3	$\geq 10^{-4}$ do $< 10^{-3}$	> 1000 do ≤ 10,000 razy
2	$\geq 10^{-3}$ do $< 10^{-2}$	> 100 do ≤ 1000 razy
1	$\geq 10^{-2}$ do $< 10^{-1}$	> 10 do ≤ 100 razy

Sprzęt sterownika automatyki budynku spełniający wymagania SIL-3

Po wykonaniu analizy ryzyka, określeniu ogólnych wymagań bezpieczeństwa, określeniu funkcji bezpieczeństwa E/E/EP oraz określeniu wymaganego poziomu nienaruszalności bezpieczeństwa, należy wytypować rodzaj sprzętu do realizacji funkcji bezpieczeństwa.

Osiągnięcie wymaganego poziomu nienaruszalności bezpieczeństwa jest możliwe poprzez zwiększenie odporności sprzętu na awarie lub zwiększenie odsetka bezpiecznych uszkodzeń tego sprzętu (takich, które nie prowadzą do sytuacji niebezpiecznych) [15]. W PN-EN 61508 proponuje się różne techniki, których zastosowanie pozwala osiągnąć pożądany poziom SIL. Na przykład odsetek bezpiecznych uszkodzeń można zwiększyć poprzez zastosowanie technik zwiększających prawdopodobieństwo wykrycia uszkodzeń i ich prawidłową obsługę (takich jak np. diagnostyka). Inną techniką jest zastosowanie sprzętu na tyle niezawodnego, że spełniającego określone wcześniej wymogi nienaruszalności bezpieczeństwa. Jeszcze inną techniką jest zastosowanie sprzętu odpornego na wewnętrzne awarie, co oznacza, że zostaną podjęte dodatkowe środki (takie jak np. redundancja) w celu uniknięcia sytuacji niebezpiecznych nawet jeśli nastąpiło uszkodzenie.

W przypadku zastosowania redundancji lub redundancji w połączeniu z diagnostyką, poszczególne struktury wielokanałowe wpływają w różny sposób na poziom bezpieczeństwa realizowanych funkcji, dostępność systemu oraz tolerancję uszkodzeń.

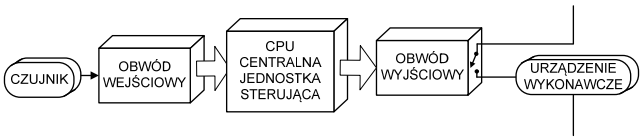
Nadmiarowe struktury wielokanałowe oznacza się kodem skrótowym MooN(D), który oznacza strukturę N kanałową o sposobie głosowania „M kanałów z N dostępnych". M oznacza liczbę sprawnych kanałów z pośród N dostępnych, która wystarcza do prawidłowej realizacji funkcji bezpieczeństwa. Opcjonalnie specyfikowana na końcu kodu skrótowego litera D oznacza kanały z diagnostyką.

Stosowane są następujące systemy:
- 1oo1 jedno wyjście z jednego,
- 1oo2 jedno wyjście z dwu,
- 2oo2 dwa wyjścia z dwu,
- 2oo3 dwa wyjścia z trzech,
- 1oo2D jedno wyjście z jednego z diagnostyką,

- 1oo2D jedno wyjście z dwu z diagnostyką,
- 2oo3D dwa wyjścia z trzech z diagnostyką.

W poniższych analizach poszczególnych struktur założono, że funkcja bezpieczeństwa w przypadku zadziałania powinna wyłączyć urządzenie wykonawcze. Struktura jednokanałowa bez diagnostyki i redundancji nie jest strukturą nadmiarową - stanowi punkt odniesienia dla struktur wielokanałowych i z diagnostyką.

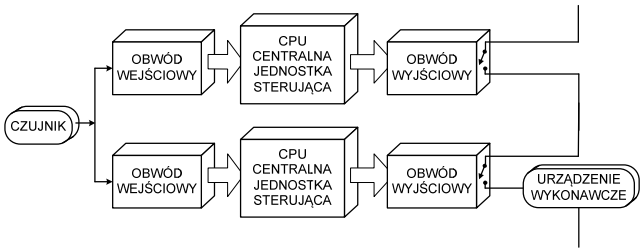
Własności struktury jednokanałowej 1oo1:
− minimalna konfiguracja,
− brak dodatkowych środków bezpieczeństwa.



Rys. 4. Struktura jednokanałowa 1oo1

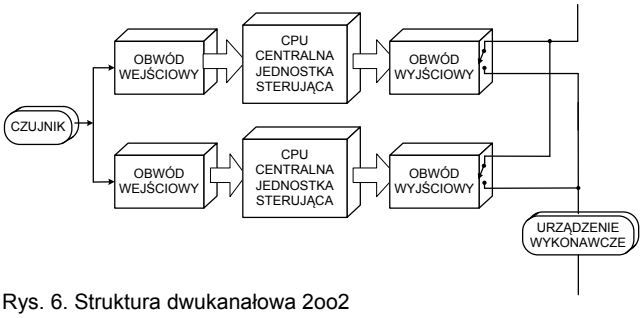
Struktura jednokanałowa (rys. 4) charakteryzuje się pojedynczym torem przetwarzania danych od czujnika do urządzenia wykonawczego. Struktura nie ma redundancji. Jedna jednostka sterująca decyduje o przełączeniu wyjścia (awaria jednostki sterującej powoduje utratę funkcji bezpieczeństwa). Błąd działania może spowodować wyłączenie wyjścia lub nie. Tolerancja na błędy wynosi zero. Oznacza to, że każdy niebezpieczny błąd prowadzi do uszkodzenia funkcji bezpieczeństwa.

Własności struktury dwukanałowej 1oo2:
− wyjścia są połączone szeregowo w celu zminimalizowania skutków uszkodzeń niebezpiecznych,
− obniżone prawdopodobieństwo niewypełnienia na żądanie funkcji bezpieczeństwa,
− zmniejszenie dostępności.



Rys. 5. Struktura dwukanałowa 1oo2

Struktura dwukanałowa (rys. 5) charakteryzuje się podwójnym torem przetwarzania danych od czujnika do urządzenia wykonawczego. System głosowania 1oo2 zwiększa bezpieczeństwo systemu w odniesieniu do 1oo1, jest również droższy w realizacji. Możliwość zadziałania funkcji z powodu uszkodzenia zwiększa się dwukrotnie zmniejszając dostępność.

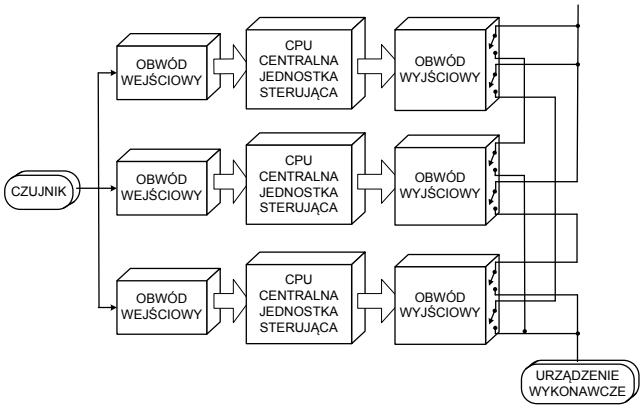


Rys. 6. Struktura dwukanałowa 2oo2

Własności struktury dwukanałowej 2oo2:
− wyjścia połączone są równolegle,
− wzrastają koszty ale nie bezpieczeństwo,
− dwa razy większe prawdopodobieństwo usterki niż w 1oo1.

W strukturze 2oo2 (rys. 6) wyjścia obu kanałów są połączone równolegle. Tylko w przypadku jednoczesnego zadziałania obu kanałów funkcja bezpieczeństwa wyłączy urządzenie wykonawcze. Uszkodzenie jednego z kanałów może prowadzić do utraty funkcji bezpieczeństwa. Dostępność systemu zmniejsza się dwukrotnie.

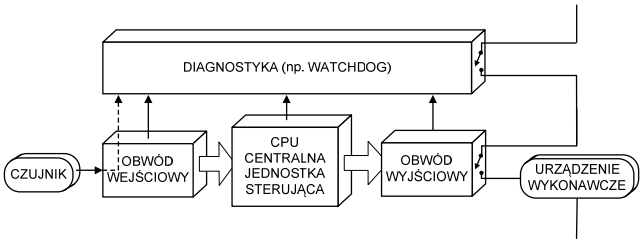
Własności struktury trójkanałowej 2oo3:
− niebezpieczne uszkodzenie może pojawić się po uszkodzeniu co najmniej 2 kanałów,
− urządzenie wykonawcze można wyłączyć poprzez jednoczesne zadziałanie co najmniej dwóch dowolnych kanałów,
− wzrost bezpieczeństwa i dostępności w stosunku do 1oo1.



Rys. 7. Struktura trójkanałowa 2oo3

Struktura trójkanałowa (rys. 7) charakteryzuje się potrójnym torem przetwarzania danych od czujnika do urządzenia wykonawczego. System głosowania 2oo3 (również nazywany TPM - Triple Modular Redundant) posiada trzy kanały, z których dwa są wymagane do poprawnej realizacji funkcji bezpieczeństwa - wyjście może być wyłączone w przypadku zadziałania przynajmniej dwóch torów. Struktura jest odporna na jedno uszkodzenie (one-fault-tolerant), zatem w przypadku uszkodzenia jednego z kanałów pozostałe dwa mogą wypełnić funkcję bezpieczeństwa. Struktura zapewnia zwiększone bezpieczeństwo oraz zwiększoną dostępność. Wadą struktury jest trzykrotnie większe prawdopodobieństwo usterki niż w 1oo1 i znaczny wzrost kosztów.

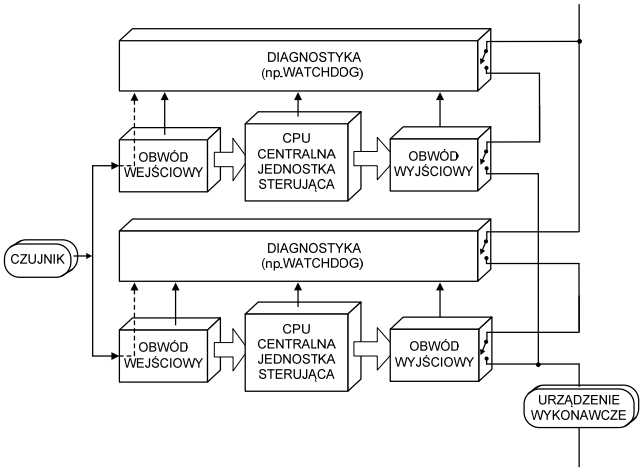
Własności struktury jednokanałowej z diagnostyką 1oo1D:
− struktura jednokanałowa z dodatkową jednostką diagnostyczną (np. watchdog),
− jednostka diagnostyczna może spowodować wyłączenie wyjścia w przypadku wykrycia awarii kanału,
− zwiększenie bezpieczeństwa
− dodatkowa elektronika



Rys. 8. Struktura jednokanałowa z diagnostyką 1oo1D

Struktura jednokanałowa z diagnostyką (rys. 8) charakteryzuje się pojedynczym torem przetwarzania danych od czujnika do urządzenia wykonawczego, uzupełnionym o diagnostykę. Struktura wprowadza automatyczną diagnostykę usterek. Dzięki autodiagnostyce w przypadku wykrycia błędu struktura może wyłączyć wyjście, ale również powiadomić o awarii zwiększając bezpieczeństwo. Dodatkowa elektronika zmniejsza dostępność. Mimo rozbudowy struktura nie jest odporna na uszkodzenia niewykrywalne.

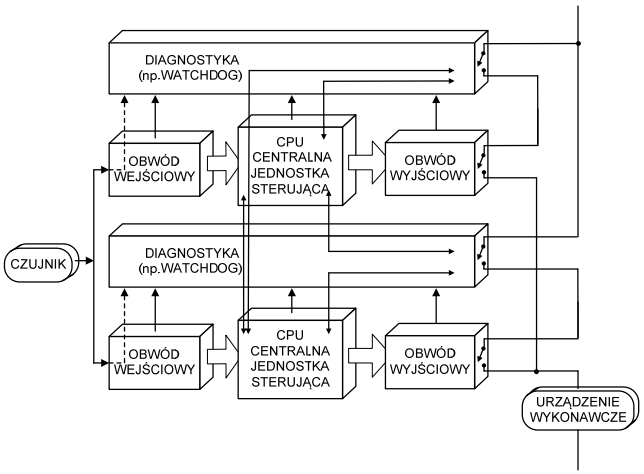
Własności struktury dwukanałowej z diagnostyką 2oo2D:
− budowa oparta na podstawie dwóch struktur 1oo1D,
− zwiększona dostępność.



Rys. 9. Struktura dwukanałowa z diagnostyką 2oo2D

W strukturze 2oo2D (rys. 9) podobnie jak w strukturze 2oo2 połączenie równoległe wyjść zwiększa dostępność. Zwiększenie bezpieczeństwa jest możliwe dzięki autodiagnostyce – w przypadku wykrytej przez diagnostykę awarii nadal drugi z kanałów może realizować funkcję bezpieczeństwa. Struktura nie jest odporna na błędy niewykrywalne.

Własności struktury dwukanałowej z diagnostyką 1oo2D:
− rozbudowana diagnostyka umożliwiająca dodatkowo porównanie kanałów,
− poziom bezpieczeństwa 1oo2 i dostępności 2oo2.



Rys. 10. Struktura dwukanałowa z diagnostyką 1oo2D

Struktura 1oo2D (rys. 10) łączy w sobie zalety systemów 1oo2 i 2oo2. Rozbudowana diagnostyka daje możliwość porównywania kanałów i stwierdzenia usterki w każdym z kanałów niezależnie przez każdy z dwóch układów diagnostycznych. Uszkodzony kanał zostaje odizolowany, podczas gdy drugi kanał nadal może realizować w pełni funkcję bezpieczeństwa. System ten posiada poziom bezpieczeństwa taki jak w 1oo2 i poziom dostępności taki jak w 2oo2. Struktura jest odporna na uszkodzenie jednego z kanałów. Nie jest odporna jedynie na błędy o wspólnej dla obu kanałów przyczynie.

Przed wyborem konkretnej struktury dla urządzenia realizującego funkcję bezpieczeństwa należy określić udział możliwych uszkodzeń bezpiecznych definiowany jako iloraz średniego wskaźnika uszkodzeń bezpiecznych podsystemu, powiększonego o wykrywalne uszkodzenia niebezpieczne do średniego całkowitego wskaźnika uszkodzeń podsystemu. Struktury bez diagnostyki nie wykrywają uszkodzeń, dlatego udział uszkodzeń bezpiecznych jest mniejszy niż w strukturach z diagnostyką. Zależność nienaruszalności bezpieczeństwa sprzętu dla odpowiednich struktur od udziału uszkodzeń bezpiecznych dla systemów elektronicznych programowalnych przedstawia Tabela 3.

Tabela 3. Nienaruszalność bezpieczeństwa sprzętu – ograniczenia dla struktur systemów elektronicznych programowalnych

Udział uszkodzeń bezpiecznych	Struktura sprzętu / tolerancja uszkodzeń	
	1oo1D, 2oo2D	1oo2D, 2oo3D
	0	1
< 60%	nie nadają się	SIL 1
≥ 60% do < 90%	SIL 1	SIL 2
≥ 90% do < 99%	SIL 2	SIL 3
≥ 99%	SIL 3	SIL 4

Według autorów odpowiednią strukturą dla urządzeń (podsystemów) systemu automatyki budynku realizujących funkcje bezpieczeństwa na poziomie SIL-3 jest struktura 1oo2D. Struktury bez tolerancji na błędy niewykrywalne dla realizacji SIL-3 wymagają trudnego do spełnienia udziału uszkodzeń bezpiecznych powyżej 99%. Wybrana struktura nadaje się do realizacji funkcji bezpieczeństwa na poziomie SIL-3 przy osiągnięciu odsetka uszkodzeń bezpiecznych w granicach od 90 do 99%. Dzięki rozbudowanej autodiagnostyce zwiększa się udział uszkodzeń bezpiecznych. Struktura ta łączy zalety struktur 1oo2 oraz 2oo2 i jednocześnie nie wymaga tak dużej rozbudowy sprzętu jak struktury trzykanałowe. Osiąga się zarówno zwiększenie poziomu bezpieczeństwa jak i dostępności systemu. Dzięki rozbudowanej diagnostyce w razie awarii urządzenie może ustawić wyjścia w stan bezpieczny oraz powiadomić o awarii systemy nadrzędne. Ze względu na to, że funkcja bezpieczeństwa w systemach automatyki budynku jest realizowana przez tor składający się z węzła związanego z czujnikiem, sieci sterującej, oraz węzła związanego z wykonaniem (rys. 4) diagnostyka może być rozszerzona o dodatkowe wykrywanie sytuacji takich jak: brak komunikacji, brak odpowiedzi węzła nadawczego czy też brak odpowiedzi węzła odbiorczego. Powiadamianie o awarii poprzez sieć sterującą może być inicjowane przez nadajnik lub odbiornik w zależności od tego, który element ulegnie awarii. Dzięki powiadamianiu możliwe jest również skrócenie udziału okresów w których system pozostaje uszkodzony.

Podsumowanie

Współczesne systemy BACS powinny być realizowane w oparciu o otwarte, rozproszone, uznane normami budynkowe systemy sterowania, które pozwalają na integrację funkcji sterowania poszczególnych podsystemów budynkowych na poziomie obiektowym. To z kolei pozwala

osiągnąć najlepsze rezultaty sterowania, w tym najwyższą poprawę efektywności energetycznej wynikającą z jakości sterowania.

Rozproszone systemy automatyki budynku powinny integrować elementy realizujące funkcje bezpieczeństwa w ramach rozproszonego systemu sterowania i automatyki BACS. Elementy tych systemów wykonujące funkcję bezpieczeństwa należy realizować w oparciu o normę PN-EN 61508 do czasu opracowania norm branżowych. Dla poszczególnych elementów należy przyjąć wymagany poziom nienaruszalności bezpieczeństwa SIL-3, co pozwoli realizować systemy złożone z kilku elementów. Odpowiednią strukturą do realizacji sprzętu jest dwukanałowa struktura z diagnostyką 1oo2D zapewniająca zwiększoną tolerancję na błędy oraz zwiększoną dostępność systemu, a także zdolność osiągania stanu bezpiecznego w przypadku wystąpienia niebezpiecznych wykrywalnych awarii. Struktura dwukanałowa nie wymusza również tak kosztownej rozbudowy jak struktury trzykanałowe. Uzupełnienie systemów składających się z kilku elementów o wzajemną diagnostykę zwiększa prawdopodobieństwo wykrycia uszkodzeń, a zdolność powiadamiania o uszkodzeniach skraca okres, w którym system pozostaje niedostępny.

Obawa przed integrowaniem w ramach BACS podsystemów sterowania mających wpływ na bezpieczeństwo osób jest nieuzasadniona. Podobna sytuacja miała miejsce w przypadku systemów sterowania w przemyśle (sterowników PLC i sterowników PLC działających w sieci sterującej), podczas gdy obecnie integracja funkcji bezpieczeństwa w takich systemach jest codzienną praktyką. W zasadzie wszyscy znaczący producenci automatyki przemysłowej oferują obecnie sterowniki PLC realizujące funkcje sterownia zapewniając określony poziom bezpieczeństwa (SIL lub/i PL). Przykładem może tu być przemysłowy system sterowania firmy ABB łączący w jednej sieci sterującej sterowniki podstawowe PLC oraz sterowniki PLC bezpieczeństwa AC500-S [16], które dodatkowo w ramach jednego sterownika PLC mogą integrować moduły podstawowe i moduły bezpieczeństwa oraz przesyłać komunikaty bezpieczeństwa poprzez podstawową sieć PROFINET i specjalizowany protokół PROFISafe. Sterowniki te spełniają wymogi specyfikacji SIL-3 (wg PN-EN 61508 oraz IEC 62061) lub PL-e (wg ISO23849). W 2013 roku rozszerzono również normę PN-EN 61131 o część 6 [17] dotyczącą bezpieczeństwa funkcjonalnego sterowników PLC [18].

Argumentem za integracją funkcji bezpieczeństwa w ramach rozproszonych systemów automatyki budynku jest też pozytywny wynik projektu SAFETYLON dla sieci sterującej LonWorks, a także uwzględnienie tematyki bezpieczeństwa funkcjonalnego w najnowszej europejskiej normie PN-EN 50491 dotyczącej systemów BACS w części 4-1:2012 [19].

LITERATURA

[1] Norma PN-EN 14908-1:2014, Otwarta transmisja danych w automatyzacji budynków, sterowaniu i zarządzaniu budynkami - Protokół sieci sterowania - Część 1: Specyfikacja protokołu, PKN, Warszawa 2014.

[2] Norma PN-EN ISO 16484-5:2014, Systemy automatyzacji i sterowania budynków (BACS) - Część 5: Protokół wymiany danych, PKN, Warszawa 2014.

[3] Norma PN-EN 13321-1:2013, Otwarta wymiana danych w automatyzacji budynków, sterowaniu i zarządzaniu budynkami - Domowe i budynkowe systemy elektroniczne - Część 1: Wymagania dotyczące wyrobów i systemów, PKN, Warszawa 2014.

[4] Jabłoński A., Zadania integracji systemów w budynkach inteligentnych, *Przegląd Elektrotechniczny*, 84 (2008), n.7, 182-185.

[5] Norma PN-EN 15232:2012, Energetyczne właściwości budynków. Wpływ automatyzacji, sterowania i technicznego zarządzania budynkami, PKN, Warszawa 2014.

[6] Racjonalizacja zużycia energii na przykładzie wybranego budynku AGH, *Grant Uczelniany Zamawiany AGH*, KANiUP AGH, 1999-2000

[7] Monitorowanie i optymalizacja zużycia energii w AGH, *Grant Uczelniany Zamawiany AGH*, KANiUP AGH, 2001-2002

[8] Zoptymalizowanie zużycia energii elektrycznej w budynkach, *Grant NCBiR SP/B/5/68017/10*, KANiUP AGH, 2010-2013

[9] Metodyka i narzędzia do oceny poprawy efektywności energetycznej budynków, *Grant NCN 3122/B/T02/2011/40*, KANiUP AGH 2011-2013

[10] Norma PN-EN 61508, Bezpieczeństwo funkcjonalne elektrycznych / elektronicznych / programowalnych elektronicznych systemów związanych z bezpieczeństwem -- Części 1-7: PKN, Warszawa 2010.

[11] PN-EN ISO 13849. Bezpieczeństwo maszyn -- Elementy systemów sterowania związane z bezpieczeństwem -- Części 1-2: PKN, Warszawa 2008, 2013.

[12] Jachimski M., Wróbel G., Mikoś Z., Hayduk G., Kwasnowski P., Ożadowicz A., Noga M., SafetyLON network protocol – safe protocol according to the EN-61508 standard, *Proceedings of 11th International Carpathian Control Conference*, Eger, 2010, 125–128.

[13] Mikoś Z., Wróbel G., Hayduk G., Kwasnowski P., Jachimski M., SafetyLON node hardware architecture according to the IEC 61508 standard, *Proceedings of 10th International Carpathian Control Conference*, Zakopane, 2009, 195–198.

[14] Langeron Y, Barros A., Grall A., Berenguer C., Combination of safety integrity levels (SILs): A study of IEC61508 merging rules, *Journal of Loss Prevention in the Process Industries*, 21 (2008), 437 – 449.

[15] Novak T., Treytl A., Palensky P., Common Approach to Functional Safety and System Security in Building Automation and Control Systems, *IEEE Conference on Emerging Technologies and Factory Automation*, Patras, 2007, 1141–1148.

[16] Welcome to AC500-S Safety PLC. Engineering Functional Safety. ABB Automation Products GmbH. 2013

[17] Norma PN-EN 61131-6:2013, Sterowniki programowalne - Część 6: Bezpieczeństwo funkcjonalne, PKN, Warszawa 2013

[18] Missala T., Nowe unormowania w zakresie bezpieczeństwa funkcjonalnego - wynik postępu technicznego, *Pomiary, Automatyka, Robotyka*, 2 (2012), 171-176.

[19] Norma PN-EN 50491-4-1:2012, Ogólne wymagania dla domowych i budynkowych systemów elektronicznych (HBES) oraz systemów automatyzacji i sterowania budynków (BACS) - Część 4-1: Ogólne wymagania bezpieczeństwa funkcjonalnego dla wyrobów przeznaczonych do zastosowania w domowych i budynkowych systemach elektronicznych (HBES) oraz w systemach automatyzacji i sterowania budynków (BACS), PKN, Warszawa 2013

***Autorzy**: dr inż Marcin Jachimski, dr inż. Zbigniew Mikoś, dr inż. Grzegorz Wróbel, AGH Akademia Górniczo-Hutnicza, Katedra Energoelektroniki i Automatyki Systemów Przetwarzania Energii, al. Mickiewicza 30, 30-059 Kraków, E-mail: jachim@agh.edu.pl, mikos@agh.edu.pl, wrobel@agh.edu.pl*