



AUTOMATYKA

ISSN 2392-1056 INDEKS 403024 AUTOMATYKAONLINE.PL

7-8/2018

Większa efektywność i elastyczność
w aplikacjach pakowania końcowego

» www.festo.com/packaging

FESTO

Dedykowane produkty i rozwiązania Festo

- siłowniki i napędy elektryczne
- sterowniki silników
- manipulatory
- systemy sterowania
- chwytaki
- oprogramowanie



Redundancja elementów

i zasadność jej stosowania

Pojęcie redundancji oznacza w inżynierii zduplikowanie lub wielokrotne powielenie wybranych elementów czy funkcji systemu, które mają krytyczne znaczenie dla jego sprawnego funkcjonowania. Celem tego zabiegu jest zapewnienie ciągłości pracy układu, przy zwiększaniu jego niezawodności. Pozwala to na zmniejszenie prawdopodobieństwa wystąpienia usterki lub uszkodzenia systemu, które mogą owocować przykrymi konsekwencjami. Powodem takiej usterki może być błędne funkcjonowanie układu, pomyłka ludzka, zużycie elementu lub inna przyczyna.

Agnieszka Hyla

Zadaniem elementów redundantnych jest zminimalizowanie zagrożenia w postaci przestoju produkcyjnego czy spowodowania uszczerbku na zdrowiu pracownika [1, 3].

Czym jest redundancja?

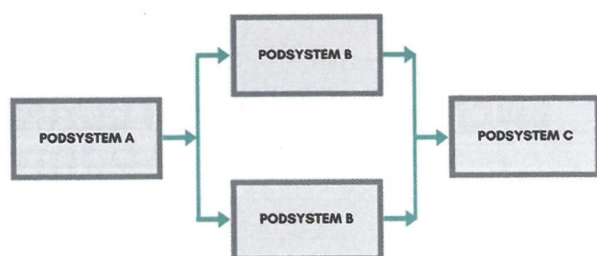
W systemach redundantnych zazwyczaj wykorzystuje się elementy zapasowe lub tak zwane rozwiązanie typu 'fail-safe', czyli układów, które na usterki reagują w sposób niezagrażający pracy maszyn, otoczeniu ani operatorom. Dodatkową zaletą systemów redundantnych może być poprawa ich parametrów lub zwiększenie szybkości pracy przez multiplikację elementów. Jest tak w przypadku procesorów komputerowych czy odbiorników nawigacji satelitarnej. Wykorzystanie kilku komponentów zamiast jednego wpływa pozytywnie na sprawność systemu. Taka redundancja jest wykorzystywana w sytuacjach, kiedy pojedyncze komponenty nie są wystarczająco niezawodne do konkretnej aplikacji [1, 2, 3].

W systemach redundantnych może dochodzić do podwojenia (rys. 1) komponentów krytycznych, lub nawet do ich potrójnienia (rys. 2). Struk-

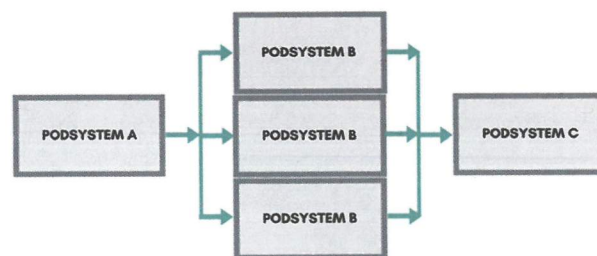
turę taką nazywamy potrójną redundancją modułową TMR (triple modular redundancy). Wówczas błąd pojedynczego elementu, który jest potrójony w układzie, może być nawet niezauważalny dla pracy całości systemu, dzięki dwóm kolejnym elementom, które mogą go zastąpić. W systemie potrójnie redundantnym występuje małe prawdopodobieństwo wystąpienia zatrzymania całego układu, ze względu na to, iż sytuacja, w której na raz usterce ulegają wszystkie trzy elementy jest bardzo rzadka. W przypadku duplikacji elementu dochodzi jedynie do podwojenia, a więc jest tylko jeden podsystem zapasowy. W wielu sytuacjach jest to jednak wystarczające rozwiązanie zabezpieczające. Aby upewnić się, że zastosowane zabezpieczenia są adekwatne do potrzeb, należy obliczyć prawdopodobieństwo awarii systemu.

$$p = \prod_{i=1}^n p_i$$

Obliczanie prawdopodobieństwa awarii systemu, gdzie n – liczba komponentów, p_i – prawdopodobieństwo awarii komponentu i -tego, p – prawdopodobieństwo jednoczesnej awarii wszystkich komponentów



Rys. 1. Duplikacja podsystemu B w układzie ABC



Rys. 2. Potrójnienie podsystemu B w układzie ABC

Najczęściej powielane komponenty

Wyróżniamy kilka podstawowych rodzajów redundancji. Pierwszy z nich to redundancja sprzętu czyli hardware. Kolejny to redundancja informacji, oparta na metodach wykrywania i eliminowania błędów. Trzeci rodzaj to redundancja czasu, polegająca na wielokrotnym wykonywaniu tych samych operacji, np. wielokrotne włączanie programu komputerowego czy tworzenie wielu kopii przekazywanych danych. W programowaniu występuje także tzw. programowanie NVP, czyli N-version programming – programowanie wielowersyjne. Ten rodzaj redundancji polega na tym, że ta sama funkcjonalność realizowana jest różnymi sposobami w celu zapewnienia ciągłości pracy systemu w przypadku niewykonania pierwszej grupy komend. W jednym z systemów informatycznych, w którym występowała funkcja weryfikowania numeru identyfikacji podatko-

wej NIP dowolnej firmy w bazie danych przedsiębiorców, weryfikacja obsługiwana była z wykorzystaniem standardowego API. Szybko jednak okazało się, że rozwiązania tego typu są zawodne. Zespół postanowił więc o implementacji dwóch dodatkowych integracji z zewnętrznymi API. W efekcie, jeśli jedna z nich zwracała błędy, np. błąd 404 (strona o podanym adresie nie istnieje), weryfikacji można było wciąż dokonać z wykorzystaniem jednej z pozostałych dwóch integracji z niezależnymi systemami. Dzięki temu użytkownicy mogli sprawnie korzystać z aplikacji, mimo występujących błędów zewnętrznych dostawców informacji.

Najczęściej powielają się elementy i podsystemy układu, które są najbardziej krytyczne. W sytuacji, kiedy operator steruje wybranym fragmentem procesu technologicznego i wykorzystuje do tego działania jeden komputer, zazwyczaj stawia obok niego drugi komputer o tym samym ustawieniu,

który w przypadku wystąpienia błędów lub usterki pierwszego komputera, przejmuje zarządzanie procesem, by nie doszło do zatrzymania pracy lub zagrożenia operatora. Podobnie w systemach safety. Redundancja polega w nich na tym, że w układzie maszyn umieszcza się dwa sterowniki safety, specjalnie dostosowane do wymagań procesu. Są one spięte w tak zwanym trybie hot standby. Oznacza to, że jeśli w pierwszym sterowniku wystąpią błędy lub zdiagnozowana zostanie nieprawidłowość, np. elektryczna, to sterownik zapasowy natychmiast przejmuje kontrolę nad procesem. Jest to meritum idei redundancji zarówno w pracy z PLC, jak i systemami SCADA. Redundantne mogą być także archiwizatory danych, takie jak Historian czy SQL Server. Bazy danych są archiwizowane w określonych odstępach czasu i jeśli dochodzi do zaburzenia pracy jednej bazy lub wystąpienia błędu, dane zapisywane są w jej kopii.

REKLAMA

EMT
SYSTEMS

CENTRUM SZKOLEŃ INŻYNIERSKICH

DOBRE WYSZKOLENIE TECHNICZNE TO PRZEPUSTKA DO GRY NA NAJWYŻSZYM POZIOMIE

- Wyselekcjonowani trenerzy z dużym doświadczeniem
- Komfortowe warunki szkoleniowe
- Dużo zajęć praktycznych

Zapraszamy do największego ośrodka szkoleń technicznych w Polsce.

EMT-SYSTEMS Sp. z o.o.
ul. Wincentego Pola 16
44-100 Gliwice

info@emt-systems.pl
32 4111 000
emt-systems.pl



Zalety bezpiecznego podejścia

De facto każdy system można uczynić redundantnym. To, czy powinno się tak zrobić zależy od kilku czynników. Użytkownicy systemu powinni przede wszystkim określić, które elementy całości wykonywanych zadań w procesie technologicznym są krytyczne. Następnie należy przeanalizować, dlaczego to właśnie te elementy są narażone na potencjalne usterki i zaprojektować system w taki sposób, aby zniwelować prawdopodobieństwo wystąpienia problemów. Problemem może być np. zasilanie. Warto pomyśleć więc o zastosowaniu kilku źródeł zasilania – już układy zasilania awaryjnego w szpitalach można potraktować jako załączek układu z elementami redundantnymi. Jest to wbrew pozorom bardzo istotna kwestia, ponieważ jeśli w zakładzie są systemy redundantne, jednak wszystkie zasilane są z tego samego źródła, jeśli to źródło przestanie dostarczać prąd, wówczas cała produkcja przestanie funkcjonować i mimo skrupulatnych przygotowań i wdrożenia układu minimalizującego usterki, tak czy inaczej dojdzie do bardzo poważnej przerwy w pracy zakładu.

Redundancja przydaje się szczególnie w warunkach wysokiego ryzyka. Za takowe uznać można elektrownie atomowe, gdzie zabezpieczenia i systemy sterowania w każdym przypadku są podwojone lub potrójone. Wszystko po to, by nie dopuścić do najmniejszego nawet prawdopodobieństwa, że dojdzie do masowej tragedii. W elektrowniach atomowych nawet tradycyjne systemy monitoringu pracy maszyn powinny być podwojone. Widać więc, że redundancja ma zastosowanie w dwóch przypadkach – kiedy proces ma słabe punkty, przez które może zostać przerwany oraz kiedy nawet bardzo dobrze przygotowany proces odbywa się w warunkach wysokiego ryzyka. W obu przypadkach użycie systemów redundantnych jest uzasadnione i wskazane. W przypadku linii produkującej samochody osobowe redundancja jest wskazana, ponieważ każda minuta przestoju to strata kilku tysięcy złotych. Z kolei w elektrowni atomowej bez redundancji nie można

się obyć, ponieważ w przypadku usterki zagrożenie jest tak ogromne, że niedopuszczalne. Tam systemy redundantne stanowią więc normę.

Wady redundancji

Dzięki zastosowaniu dodatkowych elementów układów, które zazwyczaj ulegają usterkom, zapewniamy sobie większą płynność i bezpieczeństwo procesu. Aby jednak być pewnym zaprojektowanych i wdrożonych systemów, które docelowo mają spełniać z góry określone założenia, należy przede wszystkim zwrócić uwagę na powody, dla których usterki i awarie zdarzają się w elementach powielanych. Jeśli jest to np. kwestia starzenia się urządzenia czy wytrzymałości materiałów może się okazać, że element redundantny uległ degradacji tak samo jak ten, którego usterkę miał złagodzić. W przypadku np. elementów z gumy niezwykle istotne jest, aby w podsystemach redundantnych były one wymieniane znacznie częściej niż w układzie podstawowym. Wynika to z faktu, iż guma jako polimer ulega starzeniu, nieużywana także. W związku z tym elementy zamontowane w tym samym okresie, ulegną zużyciu również w podobnym czasie [4].

Kolejnym aspektem, na który warto zwrócić uwagę przy projektowaniu systemów redundantnych jest oczywiście ich cena. Koszt powielenia systemu sterowania zbudowanego np. z trzech sterowników może się okazać dyskwalifikujący dla małego przedsiębiorcy. Zawsze należy więc przeanalizować kwestie bezpieczeństwa pracy, potencjalnych zagrożeń oraz planowanych rezultatów, aby móc ocenić, czy redundancja jest zasadna, czy nie. W przypadku redundancji informacji, czyli np. przechowywania danych w powielonej bazie, istotne jest także jej utrzymanie. Żeby rozwiązanie to miało rację bytu baza redundantna musi być często aktualizowana. Tylko wtedy przechowywane w niej dane są naprawdę przydatne w przypadku uszkodzenia bazy pierwotnej. Zbędny komputer, z którego skorzysta operator do sterowania wybranym fragmentem linii produkcyjnej w przypadku usterki komputera pierwotnego, również

musi być odpowiednio utrzymywany. Powinny się na nim znajdować najnowsze wersje oprogramowania, opisy i skrypty wszystkich niezbędnych procedur i czynności, którymi komputer ma sterować. Jeśli sprzęt ma nieaktualne informacje, staje się nieprzydatny i tak czy inaczej dochodzi do przestoju w pracy, mimo pozornie poczynionych kroków zaradczych.

Podsumowując, redundancja wybranych elementów systemów jest uzasadniona w sytuacji, kiedy patrząc na zaprojektowany układ myślimy 'to się nie może zepsuć'. To proste zdanie weryfikuje rzeczywiste przesłanki przemawiające na korzyść inwestowania w znacznie droższe i pozornie zbędne dodatkowe podsystemy. Ich obecność może stanowić o powodzeniu lub porażce misji na marsa lub codziennej pracy elektrowni atomowej. Decydować o życiu i zdrowiu pracowników oraz stanie parku maszynowego. Stąd projektując nowy proces lub modyfikując istniejący, warto pomyśleć o dodatkowych zabezpieczeniach, które skuteczniej niż tylko monitoring stanu maszyn, porządek i skrupulatność pracy eliminują zagrożenia związane z nieprzewidzianymi zdarzeniami w produkcji. ■

Agnieszka Hyla

konsultanka ds. optymalizacji produkcji
Centrum Szkoleń Inżynierskich
EMT-Systems Sp. z o.o.

Źródła:

- [1] Scott D. Sagan: Learning from normal accidents, Organization & Environment, https://web.archive.org/web/20040714202943/http://iis-db.stanford.edu/pubs/20276/sagan_oe_dec03.pdf, dostęp z dnia 26.04.2018 r.
- [2] Koren, Israel; Krishna, C. Mani. Fault-Tolerant Systems. San Francisco, CA: Morgan Kaufmann. p. 3. ISBN 0-12-088525-5, 2007.
- [3] Redundancy Management Technique for Space Shuttle Computers, IBM Research, <http://www.research.ibm.com/journal/rd/201/ibmrd2001E.pdf>, dostęp z dnia 26.04.2018 r.
- [4] Na czym polega redundancja i dlaczego warto mieć system zapasowy?, <https://www.datera.pl/blog/czym-polega-redundancja-dlaczego-warto-miec-system-zapasowy/>, dostęp z dnia 26.04.2018 r.