KRZYSZTOF
PAWELEC
AUTOMATYKA · SAFETY

RAPORT PRZYKŁADOWY

TEST PRAWDZIWEGO PROGRAMU SYMULATOREM · DANE ZAKŁADU USUNIĘTE

Sprawdziliśmy każdą kombinację, nie kilkanaście.

Program maszyny do cięcia sztang na długość: sterownik S7-1200, 23 bloki kodu, 315 sieci. Pracował latami i nikt nie zgłaszał błędów. Symulator znalazł cztery.

1 997 872

sprawdzonych kombinacji stanów i wejść



12 reguł **8** spełnionych

4 złamane

Wynik w jednej minucie

Każdy z tych błędów wymaga jednej, konkretnej sytuacji. Przy maszynie nikt jej nie próbuje, bo nikt nie naciska dwóch przycisków naraz po to, żeby zobaczyć, co się stanie.

Winda dostaje GÓRA i DÓŁ naraz

W trybie automatycznym winda jedzie w górę. Wystarczy wtedy nacisnąć „w dół” i program załącza oba styczniki.

Automat rusza mimo awarii

Trzymany przycisk RESET kasuje pamięć awarii, choć awaria trwa. START w tej chwili załącza tryb automatyczny.

Frez opuszcza się na stojąco

Przycisk z panelu opuszcza frez, gdy napęd freza nie pracuje. Program nie sprawdza przy nim ani napędu, ani trybu.

01

Program na równania

Każdą sieć drabinki zamieniamy na wyrażenie logiczne. Pracujemy na kopii projektu.

02

Reguła jednym zdaniem

Na przykład: „góra i dół nigdy jednocześnie”. Reguły ustalamy z zakładem.

03

Wszystkie stany

Symulator przechodzi każdy stan, do którego program może dojść, i w każdym podaje wszystkie kombinacje wejść.

04

Droga do błędu

Gdy reguła pęka, symulator pokazuje najkrótszą kolejność zdarzeń, która do tego prowadzi.

Dwanaście reguł, dwanaście wyników

Osiem reguł program spełnia w każdej sytuacji. To też jest wynik: te blokady są sprawdzone, a nie założone.

NR	REGUŁA	SPRAWDZONO	NARUSZEŃ	WYNIK
R1	Winda magazynka: GÓRA i DÓŁ nigdy jednocześnie	131 072	9 984	ZŁAMANA
R2	Frez: OPUSZCZANIE i PODNOSZENIE nigdy jednocześnie	43 008	0	SPEŁNIONA
R3	Łańcuch podajnika: PRZÓD i TYŁ nigdy jednocześnie	1 536	0	SPEŁNIONA
R4	Rolka podająca: OPUSZCZANIE i PODNOSZENIE nigdy jednocześnie	2 304	0	SPEŁNIONA
R5	Szczęki na końcu: PODNOSZENIE i OPUSZCZANIE nigdy jednocześnie	8 960	0	SPEŁNIONA
R6	Szczęki przed frezem: OPUSZCZANIE i PODNOSZENIE nigdy jednocześnie	4 608	0	SPEŁNIONA
R7	Zrzut sztangi: OTWIERANIE i ZAMYKANIE nigdy jednocześnie	92 160	0	SPEŁNIONA
R8	Podajnik materiału: PODNOSZENIE i OPUSZCZANIE nigdy jednocześnie	8 192	0	SPEŁNIONA
R9	Pochylnia: LEWO i PRAWO nigdy jednocześnie	48	0	SPEŁNIONA
R10	Tryb automatyczny nie jest załączony, gdy trwa awaria	788 480	179 776	ZŁAMANA
R11	Frez opuszcza się tylko przy pracującym napędzie freza	786 432	141 312	ZŁAMANA
R12	Winda nie rusza, gdy przekaźnik bezpieczeństwa jest wyłączony	131 072	32 896	ZŁAMANA
	Razem	**1 997 872**	**363 968**	

„Sprawdzono” to liczba par: osiągalny stan programu × kombinacja wejść. Cały test trwał około 3 sekund.

Złamane reguły

Po lewej fragment programu jako równanie i najkrótsza droga do błędu znaleziona przez symulator. Na czerwono to, czego w programie brakuje albo co omija warunek.

R1 Winda: GÓRA i DÓŁ jednocześnie

9 984 NARUSZEŃ

PROGRAM

```
WINDA_GÓRA = (przycisk_góra OR pamięć_góra OR (AUTOMAT AND NOT czujnik_pełny)) AND NOT krańcówka_góra  brak: AND NOT WINDA_DÓŁ
WINDA_DÓŁ = (przycisk_dół OR pamięć_dół) AND NOT krańcówka_dół  brak: AND NOT WINDA_GÓRA
```

1. Tryb automatyczny pracuje, czujnik magazynka nie zgłasza „pełny”: winda jedzie w górę.
2. Operator naciska przycisk „winda w dół”.

! **WINDA_GÓRA = 1 i WINDA_DÓŁ = 1 w tym samym cyklu.**

DLACZEGO TO WAŻNE

Dwa styczniki kierunku załączone naraz. Jeśli nie mają blokady elektrycznej lub mechanicznej, grozi to zwarciem między fazami. Rozstrzyga schemat.

DLACZEGO NIKT TEGO NIE ZAUWAŻYŁ

Łańcuch podajnika w tym samym bloku ma wzajemną blokadę (reguła R3 spełniona). W windzie ją pominięto, a w normalnej pracy nikt nie naciska „w dół” podczas jazdy w górę.

POPRAWKA

Dwa styki w dwóch sieciach. Po zmianie symulator sprawdza regułę ponownie.

R10 Automat załączony mimo awarii

179 776 NARUSZEŃ

PROGRAM

```
PAMIĘĆ_AWARII: ustaw = NOT wszystko_OK; kasuj = RESET (kasowanie ma pierwszeństwo)
AUTOMAT: ustaw = START AND NOT PAMIĘĆ_AWARII
```

1. Przekaźnik bezpieczeństwa wyłączony, frez poza położeniem wyjściowym: awaria trwa.
2. Operator trzyma RESET i naciska START.

! **AUTOMAT = 1, choć wszystko_OK = 0.**

DLACZEGO TO WAŻNE

Kasowanie nie sprawdza, czy przyczyna awarii zniknęła. Dopóki RESET jest wciśnięty, pamięć awarii pozostaje wyzerowana i nie blokuje startu.

DLACZEGO NIKT TEGO NIE ZAUWAŻYŁ

Przy odbiorze sprawdza się, że awaria zatrzymuje maszynę i że RESET ją kasuje. Nikt nie sprawdza RESET i START jednocześnie przy trwającej awarii.

POPRAWKA

Kasowanie tylko wtedy, gdy przyczyna ustąpiła: kasuj = RESET AND wszystko_OK.

R11 Frez opuszczany przy stojącym napędzie

141 312 NARUSZEŃ

PROGRAM

```
FREZ_OPUSZCZANIE = ((cykl_cięcia AND NOT krańcówka_dół) OR przycisk_z_panelu) AND NOT FREZ_PODNOSZENIE
```

1. Napęd freza stoi, maszyna w dowolnym trybie.
2. Operator dotyka na panelu „frez opuszczaj”.

! **FREZ_OPUSZCZANIE = 1 przy NAPĘD_FREZA = 0.**

DLACZEGO TO WAŻNE

Gałąź z przyciskiem panelu omija warunki cyklu. Nieobracający się frez może zostać dociśnięty do materiału.

SZERSZY OBRAZ

Z 14 komend ręcznych panelu, które sterują ruchem, tylko jedna jest blokowana w trybie automatycznym.

POPRAWKA

Komendy ręczne przez jeden warunek: tryb ręczny i brak awarii. Dla freza dodatkowo praca napędu.

R12 Winda rusza przy wyłączonym przekaźniku bezpieczeństwa

32 896 NARUSZEŃ

PROGRAM

```
WINDA_DÓŁ = (przycisk_dół OR pamięć_dół) AND NOT krańcówka_dół
brak: AND przekaźnik_bezp_OK
```

1. Przekaźnik bezpieczeństwa wyłączony (np. wciśnięty wyłącznik awaryjny).
2. Operator naciska przycisk „winda w dół”.

! **WINDA_DÓŁ = 1 przy przekaźnik_bezp_OK = 0.**

DLACZEGO TO WAŻNE

Sterownik wystawia wyjście ruchu mimo zatrzymania awaryjnego. Czy winda faktycznie ruszy, zależy od tego, czy obwód bezpieczeństwa odcina jej zasilanie. To trzeba sprawdzić na schemacie.

NIESPÓJNOŚĆ

Pamięć komendy z panelu jest kasowana tym sygnałem, a przycisk fizyczny już nie.

POPRAWKA

Sygnał przekaźnika bezpieczeństwa w obu sieciach windy.

Co jeszcze pokazał przegląd

Zanim symulator zaczął testy, program przeszedł przegląd automatyczny. To są liczby z tego przeglądu.

219 z 219
zmiennych ma nazwę domyślną Tag_x, 218 nie ma opisu

214 z 290
sieci z logiką nie ma tytułu ani komentarza

3 bloki
były niespójne: nie ma pewności, że projekt to wersja ze sterownika

51 z 94
wejść jest przepisywanych do pamięci, ale nigdzie nieużywanych

39 z 66
wyjść nie jest nigdy ustawianych przez program

9 sieci
zapisuje tę samą wartość zadaną prędkości; wygrywa ostatnia

Na plus: żaden bit nie jest przypisywany cewką w dwóch miejscach i żaden timer nie jest użyty dwa razy.

Granice testu

- Symulator sprawdza logikę dwustanową. Wartości analogowe i pozycję z enkodera traktuje jako dowolne.
- Timery mogą w modelu skończyć odliczanie w dowolnym cyklu, więc test nie zależy od nastaw czasów.
- Blokady sprzętowe poza programem ocenia się ze schematu, nie symulatorem.
- Test nie zastępuje prób na maszynie ani oceny ryzyka.

Co dostaje zakład

- [ ] listę reguł uzgodnioną z utrzymaniem ruchu
- [ ] wynik każdej reguły z liczbą sprawdzonych kombinacji
- [ ] drogę do każdego błędu, krok po kroku
- [ ] propozycję poprawki i ponowny test po zmianie
- [ ] zestaw testów do uruchomienia po każdej przyszłej zmianie programu

Ile takich sytuacji jest w Państwa programie?

Wystarczy kopia programu jednej maszyny. Test nie wymaga postoju i nie dotyka sterownika. Nazwę zakładu i dane projektu z tego przykładu usunęliśmy.

Firma Krzysztof Pawelec · NIP 9241716360
mgr inż. Krzysztof Pawelec · tel. 697 906 128
biuro.krzysztof.pawelec@gmail.com
Sensus Control · NIP 9241931839
Kasper Pawelec · tel. 794 333 028
biuro@sensuscontrol.pl
ul. Czereśniowa 6, 67-320 Małomice