

Explain these differences, we can point to the following factors

paź 6, 2025

3 systemy bezpieczeństwa

Polepszenie porządku i obniżenie kruchości .

Porównanie 3ech systemu bezpieczeństwa: PKP, samochody, samoloty

Próbując wyjaśnić te różnice, możemy wskazać na następujące czynniki:

1. Norma ISO-2626 została zdefiniowana dla systemów samochodowych z jednym centralnym silnikiem (przynajmniej taka jest nadal dominująca architektura pojazdu). Bezpośrednią konsekwencją scentralizowanej i nieredundantnej organizacji jest to, że taki pojazd nie może być zaprojektowany jako odporny na błędy (co wymagałoby redundancji), a zatem nie może być zgodny z SIL-4 (który nakazuje konstrukcję odporną na błędy).
2. Podczas gdy norma ASIL-C mniej więcej odpowiada normie SIL-3 (w przypadku awarii system powinien przejść w stan fail-safe), norma ISO-26262 wprowadza ASIL-C wymagający architektury nadzorującej. W połączeniu z obniżonym trybem działania (np. trybem awaryjnym), tę słabszą formę redundancji można uznać za odporną na błędy, jeśli żadna awaria trybu wspólnego nie wpłynie na obie jednostki przetwarzające [13].
3. Systemy motoryzacyjne nie podlegają (jeszcze) tym samym rygorystycznym wymogom certyfikacyjnym, co systemy kolejowe i lotnicze, zgodnie z którymi producenci i organizacja eksploatująca ponoszą odpowiedzialność prawną, podczas gdy generalnie za osobę odpowiedzialną w razie wypadku często uważa się indywidualnego kierowcę. Należy zauważyć, że gdy pojazdy są użytkowane w regulowanym środowisku pracy, wymogi bezpieczeństwa są również bardziej rygorystyczne, co oznacza, że potencjalnie odpowiedzialna jest organizacja eksploatująca, a niekoniecznie operator lub kierowca. W związku z tym mniejszy wpływ finansowy produktów konsumenckich jest z pewnością czynnikiem negatywnym, nawet jeśli cena zakupu jest wysoka.
4. Sektory kolejowy i lotniczy są certyfikowane w połączeniu z regulowanym środowiskiem i infrastrukturą, która przyczynia się do ogólnego bezpieczeństwa. Pojazdy samochodowe są projektowane z bardzo niewielkimi wymaganiami dotyczącymi miejsca i czasu eksploatacji i są użytkowane w infrastrukturze drogowej opracowanej przez zewnętrzne podmioty. Infrastruktura, z której korzystają samochody, wymusza ich eksploatację w znacznie bliższej odległości fizycznej niż w przypadku samolotów. To z kolei zwiększa prawdopodobieństwo wypadków. To częściowo wyjaśnia, dlaczego wysoka liczba ofiar śmiertelnych na świecie nie znajduje odzwierciedlenia w certyfikacji ASIL.
5. Z powyższego nie należy wnioskować, że pojazd jest z definicji niebezpieczny. Wiele wypadków można przypisać nieodpowiedzialnemu zachowaniu kierowcy. Jest jednak pewną sprzecznością, że poziomy nienaruszalności bezpieczeństwa dla pojazdów samochodowych są niższe niż dla lotnictwa i kolei, biorąc pod uwagę fakt, że wypadki pojazdów zdarzają się w bardzo krótkich odstępach czasu i w ograniczonej przestrzeni, a kierowca praktycznie nie ma możliwości kontroli. W kolejnictwie i lotnictwie kierowca lub pilot często mają minuty i dużo miejsca na próbę odzyskania kontroli.
6. Norma ISO-26262 definiuje również wytyczne dotyczące dekompozycji danego poziomu ASIL. Proces ten jest jednak złożony i kieruje się podstawowym celem, jakim jest redukcja kosztów, popartym logiką, że jednoczesne awarie są mało prawdopodobne. To ostatnie założenie jest wątpliwe.

