Spis treści

[1 Wstęp [1-2] 2](#_Toc518602090)

[2 Bezpieczeństwo systemów sterowania [10+] 3](#_Toc518602091)

[2.1 Podstawowe pojęcia bezpieczeństwa systemów sterowania [2] 3](#_Toc518602092)

[2.2 Safety case – definicja i struktura [3] 3](#_Toc518602093)

[2.3 Wnioskowanie o bezpieczeństwie w cyklu życia systemu [3] 5](#_Toc518602094)

[2.4 Stosowanie dowodów w safety case 5](#_Toc518602095)

[3 System ABS w samochodach osobowych [20] 6](#_Toc518602096)

[3.1 Charakterystyka systemu 6](#_Toc518602097)

[3.2 Budowa i działanie 11](#_Toc518602098)

[3.2.1 Obwód elektroniczny 12](#_Toc518602099)

[3.2.2 Obwód hydrauliczny 15](#_Toc518602100)

[3.3 Wymagania 19](#_Toc518602101)

[3.4 Analiza bezpieczeństwa 20](#_Toc518602102)

[3.5 Proces wytwórczy ABS 21](#_Toc518602103)

[4 Zarządzanie dowodami w safety case dla ABS [15+] 33](#_Toc518602104)

[4.1 Opis podejścia 33](#_Toc518602105)

[4.2 Klasyfikacja dowodów 33](#_Toc518602106)

[4.3 Zbiór dowodów dla ABS w cyklu życia 33](#_Toc518602107)

[4.4 Etapy zarządzania dowodami w rozwoju safety case 33](#_Toc518602108)

[4.5 Zarządzanie zmianami 33](#_Toc518602109)

[5 Analiza procesu [3-5] 34](#_Toc518602110)

[5.1 Skuteczność i kompletność podejścia 34](#_Toc518602111)

[5.2 Korzyści – wsparcie w zarządzaniu zakresem zmian 34](#_Toc518602112)

[5.3 Napotkane problemy i propozycje doskonalenia podejścia 34](#_Toc518602113)

[5.4 Skalowalność 34](#_Toc518602114)

[5.5 Ile zajęło to czasu – efektywność procesu – automatyczne/ręczne 34](#_Toc518602115)

[6 Podsumowanie [1-2 strony] 35](#_Toc518602116)

[Spis literatury 36](#_Toc518602117)

# Wstęp [1-2]

# Bezpieczeństwo systemów sterowania [10+]

## Podstawowe pojęcia bezpieczeństwa systemów sterowania [2]

co to jest hazard, przyczyny, analiza bezpieczeństwa

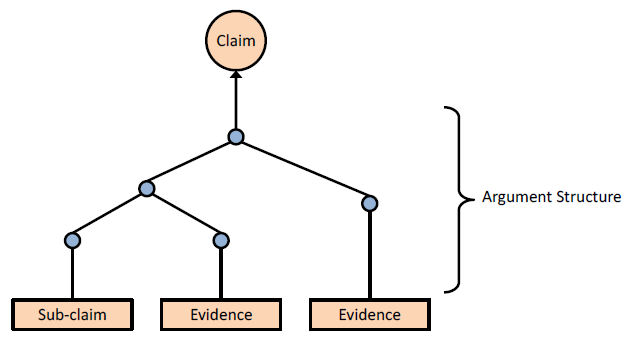
## Safety case – definicja i struktura [3]

Metodologia dotycząca wnioskowania o bezpieczeństwie – Safety Case narodziła się na terenie Wielkiej Brytanii, skąd w latach sześćdziesiątych XX w. rozprzestrzeniała się na inne kraje europejskie oraz Australię. Dowodzenie o akceptowalnym w kontekście użycia, poziomie bezpieczeństwa jest szczególnie istotne w przypadku strategicznie ważnych gałęzi przemysłu. Trudno wyobrazić sobie brak realnego dowodu bezpieczeństwa systemów komputerowych stosowanych w energetyce, dużych zakładach przemysłowych, transporcie, przemyśle zbrojeniowym, medycynie i wielu innych obszarach aktywności gospodarczej ważnych dla ludzi. Konieczność potwierdzania bezpieczeństwa systemów jest ważna także z punktu widzenia projektów związanych z eksploracją kosmosu. Wytworzenie spójnego modelu, który umożliwiałby przeprowadzenie wnioskowania o bezpieczeństwie opartego na zebranych dowodach jest niezbędne w przypadku systemów sterowania, podtrzymywania życia w wahadłowcach, które umożliwiają wykonywanie załogowych lotów w kosmos. Wysokie priorytety w zakresie bezpieczeństwa w przypadku awarii, oraz niezawodności tych systemów stanowią przyczyny dla których istotne jest przeprowadzenie dowodu bezpieczeństwa w oparciu o aktualny i reużywalny model logiczny.

Inżynierowie NASA (National Aeronautics and Space Administration) utożsamiają dowód bezpieczeństwa - Safety Case z procesem decyzyjnym w którym wykazanie roszczenia o bezpieczeństwa opiera się na identyfikacji i szacowaniu ryzyk systemu. Kluczowe według nich jest znalezienie odpowiedniego poziomu równowagi pomiędzy bezpieczeństwem systemu a jego wydajnością. Tak sformułowane wnioski na temat dowodu bezpieczeństwa zostały ujęte w zakresie koncepcji RISC: (Risc-Informed Safety Case). Zastosowanie tej metodologii ma wysyłać do klientów wyraźny sygnał, że organizacja wytwarzająca system / oprogramowanie, bierze pełną odpowiedzialność za zapewnienie akceptowalnego poziomu bezpieczeństwa. Osoby decyzyjne w procesie wnioskowania o bezpieczeństwie systemu mają pełną wiedzę na temat tego czy postawione cele w zakresie bezpieczeństwa zostały osiągnięte w każdym „kluczowym punkcie decyzyjnym”. Ważność, aktualność modelu decyzyjnego w koncepcji RISC jest uzależniona od zastosowania budowanego systemu w określonym środowisku. Konieczne jest zatem aby stosując tą koncepcję określić środowisko / otoczenie operacyjne systemu w którym jest on uważany za bezpieczny. Jeśli w trakcie przeszukiwania środowiska zostaną znalezione nieaktualne zastrzeżenia o bezpieczeństwie można wnioskować że system nie spełnia już wymogów bezpieczeństwa. Główne elementy w strukturze RISC to:

* Zestaw roszczeń lub roszczenie, spójnych pod względem zapewnienia że nadrzędne cele operacyjne określone dla bezpieczeństwa systemu zostały spełnione. Inaczej mówiąc jest to główne roszczenie (clime), że system jest odpowiednio bezpieczny.
* Dowody (evidence) stosowane jako podstawa dla argumentu o bezpieczeństwie. Przeważnie są to fakty w postaci ustalonych zasad naukowych lub dane empiryczne.
* Ustrukturyzowane argumenty o bezpieczeństwie, połączone z dowodami, używające logicznie poprawnych reguł wnioskowania. Argumenty o bezpieczeństwie mogą być deterministyczne, probabilistyczne lub jakościowe.

Dowody połączone z argumentami tworzą spójną strukturę (argument structure) obrazowaną przez digram w którym proces wnioskowania rozpoczyna się od elementów położonych najniżej. Opisaną strukturę koncepcji RiSC przedstawia poniższy schemat:



Rysunek 1. Schemat wnioskowania o bezpieczeństwie systemu wg. koncepcji RISC[[1]](#endnote-1).

Przedstawiona wyżej koncepcja RiSC to oczywiście nie jedyne podejście do Safety Case kreowane w sferze inżynierii oprogramowania.

Europejska organizacja ds. bezpieczeństwa żeglugi powietrznej (Eurocontrol) w dokumencie „Safety Case Development manual” wskazuje, że większość jeśli nie wszystkie modele Safety Case można podzielić na dwie kategorie: Unit Safety Cases – stosowane w celu wykazania bezpieczeństwa w sposób ciągły, oraz Project Safety Cases – wykorzystywane do prezentowania jedynie istotnych zmian mających wpływ na poziom bezpieczeństwa. Unit Safety Cases są produkowane i utrzymywane w celu wykazania że bieżące wykonywane z dnia na dzień operacje są bezpieczne z punktu widzenia całego systemu. Informacje w nim przechowywane zawierają określenie szacowanego poziomu bezpieczeństwa systemu / usługi (w danym czasie) oparte na zapisie monitoringu operacyjnego, ankiet czy rezultatów audytu bezpieczeństwa. Taki zbiór informacji ma na celu dokładane określenie ostatniego momentu w czasie w którym stwierdzono że system / usługa jest akceptowalnie bezpieczna w zakładanym kontekście użycia.

Project Safety Case ma na celu prezentację jedynie tych zmian które miały istotny wpływ na poziom bezpieczeństwa systemu lub obsługi. Ryzyka uwzględniane przez tą kategorię Safety Case są tworzone lub modyfikowane w wyniku zmian wprowadzanych do systemu lub usługi. Opierają się one na założeniach lub dowodach z powiązanego modelu Unit Safety Case, że konfiguracja usługi lub systemu przed wprowadzeniem zmian realizowała podstawowe cele w zakresie bezpieczeństwa[[2]](#endnote-2).

Niezależnie od wybranego rodzaju Safety Caase elementarną jego częścią jest roszczenie o bezpieczeństwie (safety case clime) które należy udowodnić w procesie wnioskowania. Wspomniana wyżej koncepcja RiSC opracowana przez inżynierów NASA zakłada istnienie dwóch niezależnych typów roszczeń o bezpieczeństwie systemu:

* Roszczenia powiązane z bieżącą lub wcześniejszą fazą wnioskowania w której podstawowe kryteria w zakresie zapewnienia bezpieczeństwa zostały spełnione

## Wnioskowanie o bezpieczeństwie w cyklu życia systemu [3]

## Stosowanie dowodów w safety case

# System ABS w samochodach osobowych [20]

## Charakterystyka systemu

Jednym z najstarszych systemów elektronicznych, stosowanych w pojazdach osobowych jest system *Anti-Lock Breaking System* (ABS). Układ ten należy się do grupy systemów typu *Advanced Vehical Control Systems* (AVCS) lub *Automated Highway Systems* (AHS).

Współczesne systemy ABS są mniejsze, lżejsze i bardziej skuteczne od swoich poprzedników. Pierwsze generacje systemu działały jednokanałowo, tzn. regulacja ciśnienia w zaciskach hamulcowych odbywała się dla czterech koła jednocześnie, co obniżało efektywność układu i wydłużało drogę hamowania pojazdu. Obecnie system jest w stanie obsługiwać każde z kół osobno, dzięki czemu wsparcie układu hamulcowego przez system ABS jest dużo lepsze[[3]](#endnote-3).

Rosnące wymagania w zakresie wsparcia kierowcy podczas prowadzenia pojazdu, zmieniająca się dynamika ruchu drogowego, stan dróg, zmienne warunki pogodowe wzmogły konieczność permanentnego rozwijania wielu innych elektronicznych systemów bezpieczeństwa. Układ ABS jest podstawą dla rozwoju innych systemów stosowanych dziś powszechnie w pojazdach drogowych, m.in. ESP – elektroniczny układ stabilizacji toru jazdy, czy ASR – system zapobiegający poślizgowi kół podczas ruszania w warunkach   
o zróżnicowanej przyczepności podłoża[[4]](#endnote-4).

Głównym zadaniami systemu ABS są:

1. Zapobieganie blokowaniu kół, w przypadku konieczności wykonania nagłego manewru hamowania, spowodowanego niebezpieczną sytuacja na drodze.
2. Wspomaganie działania hamulców, poprzez możliwość precyzyjnej symulacji hamownia „pulsacyjnego”[[5]](#endnote-5).

Zapewnienie obrotu kół podczas hamowania, eliminuje zagrożenie utraty kontroli przez kierowcę nad pojazdem. Prowadzący pojazd może w ten sposób bezpiecznie ominąć przeszkodę, której nagłe pojawienie na drodze zmusiło go do gwałtownego hamowania. System ABS nie jest w stanie sam bezpośrednio skrócić drogi hamowania pojazdu, ponieważ jest to zależne m.in. od czynników takich jak: umiejętności kierowcy, oraz warunki zewnętrzne. Niemniej jednak samochód wyposażony w system ABS podczas hamowania nie jest narażony na zjawiska występujące bezpośrednio po zablokowaniu kół takie jak wirowanie lub ściąganie w bok. Nagłe, ale w pełni kontrolowane hamowanie zwiększa szanse na uniknięcie kolizji w ruchu drogowym pomimo krótkiej odległości od przeszkody.

Utrzymanie stabilności toru jazdy poprzez wyeliminowanie niekontrolowanego poślizgu kół ma duże znaczenie w przypadku hamowania zespołu pojazdów np. samochodu ciężarowego z naczepą. Drugi człon pojazdu, gdy utraci sterowność zaczyna poruszać się w kierunku poprzecznym do osi jazdy i może spowodować przewrócenie się całego zespołu.

Hamowanie w sytuacji zagrożenia jest skuteczniejsze, jeśli pod wpływem mocnego naciśnięcia pedału hamulca uzyskana została jak największa siła hamowania dla wszystkich kół. Maksymalne skrócenie czasu do momentu aktywacji ABS jest wspierane przez system *Hydraulic Break Assist* (HBA), który gwałtowne naciskanie pedału hamulca interpretuje jako konieczność użycia maksymalnej siły hamowania dla wszystkich kół. System ten zwiększa ciśnienie w układzie hamulcowym co przyspiesza moment włączenia układu ABS[[6]](#endnote-6).

Zastosowanie systemu ABS w samochodach osobowych zmniejszyło liczbę zderzeń czołowych o 35% na mokrej nawierzchni i 9% na nawierzchni suchej. Tylko 24% kierowców samochodów, wyposażonych w system ABS i aż 58% kierowców samochodów bez tego systemu, nie było w stanie utrzymać toru jazdy po zahamowaniu[[7]](#endnote-7).

Samochody bez ABS po rozpoczęciu hamowania kontynuują jazdę w kierunku zależnym od ich osi wzdłużnej. Wszelkie próby zmiany toru jazdy mogą okazać się nieskuteczne ze względu na to iż zablokowane koła ulegają poślizgowi przez co samochód porusza się w niekontrolowany sposób. Pojazd narażony jest na wypadnięcie z drogi lub uderzenie w przeszkodę, która spowodowała zapoczątkowanie manewru hamowania przez kierowcę[[8]](#endnote-8).



Rysunek 2. Droga hamowania pojazdu z / bez ABS

Kierujący pojazdem bez ABS w sytuacji konieczności wykonania hamowania awaryjnego jest w wielu wypadkach w zdecydowanie trudniejszym położeniu. Bez wsparcia elektroniki jest zdany wyłącznie na własne umiejętności „czucia” samochodu i opanowanie. Technika hamowania awaryjnego bez wsparcia ABS polega na gwałtownym maksymalnym dociśnięciu pedałów hamulca i sprzęgła. Rozpędzone auto wpada w poślizg wzdłużny koła tracą swoją przyczepność. Samochód nie reaguje na ruchy kierownicą. Mimo to zbliżając się do przeszkody należy wykonać lekki skręt kierownicy w kierunku toru jazdy który pozwoli nam ominąć przeszkodę i jednocześnie zwolnić pedał hamulca. Spadek siły hamowania pozwoli na odzyskanie sterowności. Skręcone wcześniej koła przedniej osi spowodują szarpnięcie i zmianę toru jazdy we wskazanym przez kierowcę kierunku. Należy pamiętać o prawidłowym ułożeniu rąk na kierownicy, tak aby nie zostać zaskoczonym przez dynamiczne szarpnięcie kierownicy podczas nagłego odzyskania przyczepności. Jeśli powyższe czynności zostaną wykonane w sposób zdecydowany i odpowiednio wcześniej, istnieje duża szansa na unikniecie kolizji w ruchu drogowym[[9]](#endnote-9).

Podczas hamowania pojazdem wyposażonym w ABS następuje podniesienie poziomu ciśnienia płynu hydraulicznego, co powoduje wzrost siły hamowania na zaciskach hamulcowych. Algorytm sterujący systemu na postawie prędkości obrotowej kół oblicza oczekiwaną prędkość pojazdu. Mając dane dotyczące prędkości poruszania się pojazdu i prędkość obrotowej kół, logika obliczeniowa systemu jest w stanie obliczyć poślizg każdego z kół lub kontrolować aktualne opóźnienie kątowe koła. Przekroczenie zakładanego poziomu poślizgu powoduje rozpoczęcie regulacji siły hamowania poprzez zmniejszenie momentu tarcia mechanizmu hamującego. Zwiększenie prędkości koła, po przekroczeniu wartości oczekiwanej, rozpoczyna ponowny proces regulacji siły hamowania[[10]](#endnote-10).

Jakkolwiek ABS to system elektroniczny, włączający się samoczynnie podczas hamowania, to jednak kierowca ma kluczowy wpływ na efektywność jego pracy. Pewnym problemem dla skuteczności działania ABS jest błędne zachowanie kierowcy, który w panice, oznaki poprawnego działania systemu może intepretować jako zagrożenie, myślnie sądząc że „coś się zepsuło pod pedałem hamulca”. Efektywność działania systemu ABS podczas hamowania jest najwyższa, jeśli kierowca jak najmocniej dociska pedały hamulca i sprzęgła. Docisk pedału hamulca ma na celu jak najszybsze zwiększenie siły hamowania a przez to zatrzymanie pojazdu zanim dojdzie do kolizji z przeszkodą. Utrzymanie wciśniętego „sprzęgła” zaś, zapobiega wyłączeniu się silnika i w efekcie eliminuje możliwość wyłączenia elektronicznych systemów bezpieczeństwa samochodu. Podczas gwałtownego hamowania, kiedy ABS jest aktywny, prowadzący pojazd czuje wibracje lub szybkie pulsowanie pedału hamulca. Kierowca może odnieść wrażenie, że większy nacisk na pedał hamulca powoduje większy opór a wręcz zawracanie pedału w kierunku przeciwnym do siły nacisku. Towarzyszy temu słyszalny odgłos brzęczenia lub szlifowania. Wszystkie te sygnały świadczą o tym, że system ABS działa prawidłowo. Kierowca powinien skoncentrować swoją uwagę na utrzymaniu siły docisku pedałów hamulca i sprzęgła a także być gotowym na wykonanie manewru kierownicą w celu ominięcia przeszkody. Samochód nadal będzie w ruchu ponieważ potrzebny jest czas i odległość aby wytracił prędkość, jednak dzięki działaniu ABS, zachowa sterowność co pozwoli kierowcy utrzymać bezpieczny tor jazdy i omijać przeszkody na drodze[[11]](#endnote-11). Niestety, jak pokazują wyniki badania opublikowane przez Szkołę Jazdy Renualt, ponad połowa kierowców posiadających w swoich samochodach systemy ABS nie potrafi prawidłowo zahamować pojazdu w sytuacji zagrożenia. Decydujący jest tu brak doświadczenia i niewiedza zwłaszcza młodych kierowców, których poprawne działanie systemu ABS może wystraszyć i doprowadzić do zmniejszenia przez nich nacisku na pedał hamulca a tym samym obniżenia skuteczności hamowania[[12]](#endnote-12). Kierowcy bardziej doświadczeni, którzy także nie znają poprawnej techniki hamowania pojazdem z systemem ABS często także sami popełniają błąd próbując wykonywać wyuczone na starszej generacji samochodach hamowanie „pulsacyjne”. Niestety w takich warunkach system ABS także nie może poprawnie wykonywać swoich funkcji. Następuje „dezorientacja” systemu i w efekcie czego wydłużenie drogi hamowania. Często tez kierowcy wciskają pedał hamulca do momentu wystąpienia pierwszych sygnału poprawnego działania systemu ABS (charakterystyczne stukanie). Tymczasem może to oznaczać jedynie osiągnięcie granicy przyczepności kół na tylnej osi, podczas gdy dobrze obciążone przednie koła, maja jeszcze duże rezerwy przyczepności do podłoża.

Coraz trudniej znaleźć na drodze samochody niewyposażone fabrycznie w system ABS. To dobra informacja dla bezpieczeństwa kierowców. Negatywnym następstwem wzrostu liczby samochodów z ABS jest zwiększona liczba przypadków awarii tego systemu. Niestety, fakt, iż usterka ABS nie oddziałuje na sprawność układu hamulcowego powoduje, że wielu kierowców ją lekceważy. Problem potęgują kierowcy „starej szkoły” z długim stażem za kierownicą, aut bez ABS, którzy mylnie sądzą, iż w sytuacji krytycznej poradzą sobie wykonując hamowanie awaryjne bez wsparcia elektroniki. Niestety, fakt jest taki, że hamowanie samochodem bez systemu przeciwblokującego koła to nie jest, to samo, co awaryjne zatrzymanie pojazdu z uszkodzonym układem ABS. Brak korektora siły hamowania tylnych kół adekwatnie do intensywności wytracania prędkości może spowodować obrócenie się auta, wypadnięcie z toru jazdy i zatrzymanie na najbliższej przeszkodzie. Sytuacja kierującego pojazdem z uszkodzonym systemem ABS pogorszy się jeszcze bardziej jeśli do hamowania awaryjnego doszłoby w zakręcie. Wówczas uślizg tylnej osi spowoduję „zarzucenie” samochodu w wyniku działania siły odśrodkowej.

Warto udać się do serwisu i naprawić niesprawny system ABS ze względu na to iż nie są to wysokie koszty. Konsekwencje uderzenia w przeszkodę wynikające z nieskutecznego manewru hamowania awaryjnego są zdecydowanie wyższe, ponieważ do ceny naprawy pojazdu o ile w ogóle będzie możliwe, należy doliczyć wysokie ryzyko utraty zdrowia lub życia podczas wypadku drogowego[[13]](#endnote-13).

Szczególnie „wrażliwe” w układzie ABS są czujniki pomiaru prędkości obrotowej kół. Objawem widocznym dla kierowcy, który może wskazywać na uszkodzenie czujnika pomiarowego jest zapalona podczas jazdy kontrolka ABS, lub innych systemów z którymi system przeciwblokujący się komunikuje jak np. ESP lub ASR. Często na panelu kierowcy widoczna jest także zapalona kontrolka „check engine” co może oznaczać zapisanie informacji o awarii czujników pomiarowych w sterowniku silnika. Podobne objawy mogą także występować jeśli uszkodzeniu uległ jeden z przewodów łączących czujnik z elektryczną jednostką sterującą. Częstymi przyczynami zakłóceń w pracy czujników układu ABS są m.in. luzy powstające na zużytym łożysku koła, zbyt niskie ciśnienie w jednym z kół lub zużyte tarcze hamulcowe generujące nadmierne wibracje, przez co czujniki mogą przesyłać niepoprawne dane pomiarowe. Zimą należy zwrócić uwagę na zabrudzenia czujników lub tarczy zębatej, zalegającą na ulicach solą lub błotem śniegowym. Włączanie się systemu ABS nawet przy najmniejszym hamowaniu w ruchu miejskim może świadczyć o uszkodzeniu koła zębatego z którym ściśle współpracuje czujnik pomiarowy. Koło zębate, narażone jest na korozję, w skutek pracy w trudnych warunkach, może utracić część zębów lub całkowicie zostać zerwane. W takiej sytuacji czujnik nie będzie w stanie prawidłowo wysyłać sygnałów pomiarowych do jednostki sterującej. Uszkodzone koło zębate należy wymienić korzystając z pomocy serwisu. Wprawny diagnosta jest w stanie zidentyfikować usterkę układu ABS odczytując kod błędu zapisany w systemie co pozwala na szybsze i skuteczniejsze rozwiązanie problemu[[14]](#endnote-14).

Skuteczność awaryjnego hamowania często decyduje czy kierowca uniknie bezpośredniego uderzenia w przeszkodę, czy nie. Sprawnie działający układ ABS znacznie podnosi prawdopodobieństwo uniknięcia poważnych następstw wypadków drogowych. Możliwe, że będzie wydawać się to dziwne ale istnieją cztery sytuacje na drodze w których sprawnie działający układ przeciwblokujący koła wydłuży drogę hamowania.

Przykładem jest tu hamowanie awaryjne na drodze o „luźnej nawierzchni” np. liście na drodze. Brak bezpośredniego kontaktu z podłożem utrudnia systemowi ABS poprawne zmierzenie przyczepności kół i w efekcie poprawne dostosowanie siły hamowania. Znacznie lepszym rozwiązaniem w tej sytuacji byłoby zablokowanie kół, które w skutek wysokiej siły tarcia o podłoże mogłyby przepalić liście, aż do uzyskania pełnego kontaktu opony z drogą. Umożliwiłoby to poprawne określenie przyczepności kół przez system ABS i w efekcie jego skuteczne działanie.

Kolejną sytuacją w której ABS raczej utrudni hamowanie jest poruszania się pojazdu po kopanym piachu np. na plaży. Zablokowane koła zadziałaby jak pług wytwarzając „bandę piachu” która pomogłaby zatrzymać poruszający się pojazd. Działający układ ABS uniemożliwi zablokowanie kół przez co droga hamowania znacznie się wydłuży.

Innym przykładem, kiedy system przeciwblokujący może wydłużyć drogę zatrzymania pojazdu jest hamowanie na nawierzchni o zerowym poziomie przyczepności np. gładki lód. Niestety przy włączonym systemie ABS ze względu na brak jakiejkolwiek siły hamowania odległość do zatrzymania pojazdu wydłuża się. Zablokowane koła zdecydowanie przyspieszyłyby wytracanie prędkości samochodu i w efekcie jego zatrzymanie na lodzie. Utrudnienie pomiaru przyczepności koła, przez co zaburzenia pomiaru prędkości sprawia że hamowanie na „wyboistej” drodze należy traktować jako kolejny przykład „negatywnego” działania systemu. W tej sytuacji ważny będzie dobry stan amortyzatorów, które mogą znacząco ograniczyć momenty braku kontaktu opony z nawierzchnią a przez to wspomóc ABS w lepszym pomiarze poziomu przyczepności kół[[15]](#endnote-15).

Wskazane wyżej sytuacje to jednak tylko nieliczne przykłady, gdy elektronika nie stoi po stronie kierowcy. Zdecydowana większość przypadków hamowania awaryjnego pozwala na pełne wykorzystanie systemu ABS zapewniając krótszą drogę hamowania, stabilność toru jazdy i sterowność samochodu umożliwiającą bezpieczne ominięcie przeszkody. Korzyści działania systemu ABS najłatwiej dostrzec podczas testów hamowania awaryjnego na suchej i mokrej nawierzchni z udziałem wykwalifikowanego kierowcy testowego i typowego kierowcy jakiego często spotkamy uczestnicząc w ruchu drogowym. Elektroniczny system przeciwblokujący jest w stanie różnicować siłę hamowania na krawędzi maksymalnej przyczepności z częstotliwością kilkunastu razy na sekundę. Nawet najbardziej doświadczony kierowca nie jest w stanie robić tego tak często i równie dokładnie.

Wyższość elektroniki nad człowiekiem dokumentują testy opublikowane przez serwis motoryzacyjny Interii oraz magazynów „Motor” i „Auto Moto”.



Rysunek 3 Hamowanie ze 100 km/h na suchej nawierzchni.[16]

Najlepszy wynik podczas testu hamowania ze 100 km/h na suchej nawierzchni uzyskał typowy kierowca samochodu ze sprawnym systemem ABS. Jego droga hamowania była aż o 14 m krótsza od samochodu z wyłączonym systemem przeciwblokującym koła. Gdyby to była realna sytuacja na drodze kierowca samochodu hamując z zablokowanymi kołami uderzyłby w przeszkodę z prędkością ok 54 km/h.. Zaledwie przy nieco wyższej prędkości wykonuje się testy zderzeniowe Euro NCAP dla samochodów osobowych. Siła uderzenia przy tej prędkości powoduje nieodwracalne zniszczenia samochodu oraz groźne dla życia obrażenia pasażerów.

Przewaga w skuteczności hamowania z ABS rośnie jeszcze bardziej w sytuacji gdy kierowca musi zatrzymać pojazd na mokrej nawierzchni.



Rysunek 4 Hamowanie ze 100 km/h na mokrej nawierzchni [16]

Droga hamowania samochodu bez systemu ABS prowadzonego przez typowego kierowcę okazała się prawie dwa razy dłuższa w stosunku do pojazdu hamującego przy wsparciu elektroniki. W chwili gdy pojazd z systemem ABS zatrzymał się samochód typowego kierowcy hamujący z zablokowaniem kół poruszał się jeszcze z prędkością 69 km/h. Kierowca testowy z doświadczeniem sportowym był w stanie zahamować znacznie wcześniej, ale wynik 58,1 m uzyskany został po kilku próbach na „wyczucie” przyczepności kół. Podczas prawdziwej sytuacji na drodze hamowanie awaryjne odbywa się w stresie i jest całkowitym zaskoczeniem dla kierującego pojazdem. Typowy kierowca nie ma szans powtórzyć wyniku kierowcy testowego. Wszelkie próby chaotycznego hamowania pulsacyjnego będą tylko wydłużać drogę hamowania o kolejne metry. Mając zablokowane koła samochód nie reaguje na ruchy kierownicą przez co kierowca uderzy w przeszkodę z przy dużej prędkości[[16]](#endnote-16).

## Budowa i działanie

Współczesne urządzenia elektroniczne prawie zawsze przechodziły długą drogę rozwoju i optymalizacji. Prototypowe konstrukcje ustępowały miejsca swoim nowszym generacyjnie następcom. Część urządzeń starszej generacji zniknęła zupełnie ponieważ w toku ewolucji technologicznej uznano je za zbyt przestarzałe i nie nadające się do rozwoju lub też ich funkcje przejęły inne urządzenia działające bardzie kompaktowo. Niektóre z tych urządzeń lub układów złożonych z poszczególnych urządzeń przetrwała ścieżkę ewolucji technologicznej osiągając postać i stopień złożoności jaki znamy dzisiaj. Podobną drogę technologicznego rozwoju przeszedł układ ABS, stając się dziś mniejszym, lżejszym bardziej skutecznym układem od swoich poprzedników.

Jak zapobiegać blokowaniu kół podczas hamowania pojazdów szynowych, samochodów i samolotów? To pytanie które konstruktorzy zadawali sobie już na początku XX w. Wśród pomysłów różnych rozwiązań pojawił się układ zaprojektowany przez firmę Bosh, który w 1936 został zgłoszony do patentu jako „urządzenie zapobiegające blokowaniu kół pojazdu mechanicznego w trakcie hamowania”. Niestety, wszystkie projekty układów przeciwblokujących produkowanych w tamtym czasie, okazały się zbyt skomplikowane a przez to zbyt awaryjne i za wolne, aby można było myśleć o ich seryjnej produkcji. Pewien sukces odniosła firma Teldix (później przejęta przez Bosha) , której system „ABS 1”, realnie skracał drogę hamowania i dawał stabilność toru jazdy na zakrętach. Postęp potwierdziły testy przeprowadzone przez tą firmę w 1966r. Niestety jednak nie udało się osiągnąć satysfakcjonującego poziomu trwałości sterownika elektronicznego systemu co spowodowało że układ ten nie trafił do seryjnej produkcji. Problemem była zbyt duża (licząca ok 1000 elementów) liczba części analogowych sterownika oraz nadmiar przewodów bezpieczeństwa. Konstrukcja okazała się zbyt awaryjna by pozytywnie przejść testy bezpieczeństwa i otrzymać zgodę na rozpoczęcie seryjnej produkcji. Przy wsparciu inżynierów Bosha i zastosowaniu układów scalonych i technologii cyfrowej udało się uprościć sterownik, który od tej pory składał się z ok 140 części[[17]](#endnote-17). Pierwsze próby produkcyjnego zastosowania systemu ABS datuje się na rok 1966, kiedy to brytyjska firma Jensen wypuściła na rynek model samochodu Jensen FF wyposażony seryjnie w system ABS *Maxret* firmy Dunlop, działający na tylną oś.[[18]](#endnote-18).

Konstrukcja ABS firmy Bosh do seryjnej produkcji weszła 14 lat później kiedy to system „ABS 2”, zadebiutował jako wyposażenie dodatkowe w S-klasie Mercedesa z 1978r. oraz BMW serii 7. Pierwsze sukcesy nie zahamowały rozwoju systemu ABS. Rosnące wymagania w zakresie bezpieczeństwa powodowały że nadal pracowano nad optymalizacją układu. Znaczący sukces przyniósł rok 1989, w którym inżynierowie Bosha, zamontowali sterownik elektroniczny o budowie hybrydowej bezpośrednio przy układzie hydraulicznym. Zabieg ten pozwolił na rezygnację z części zbędnych kabli łączących sterownik z jednostką hydrauliczną oraz złączy wtykowych. Nowa generacja systemu ukazała się na rynku jako ABS 2E. Okazała się zdecydowanie lżejsza od swoich poprzedników. Pojawienie się nowych zaworów magnetycznych pozwoliło na powstanie w 1993 r układu ABS w wersji 5.0. Kolejne wersje układu ABS (wersje 5.3 oraz 5.7) wprowadzono na rynek w kolejnych latach. Nowe rozwiązania pozwoliły na kolejne obniżenia masy układu oraz wprowadzenie funkcji dodatkowych takich jak rozdział siły hamowania na cztery koła, który zastąpił używany do tej pory reduktor ciśnienia osi tylnej[[19]](#endnote-19).

Wersja ABS 5.7 była pierwszą generacją układu, która działała znacznie ciszej od swoich poprzedników ale przede wszystkim umożliwiała integracje z systemem ESP[[20]](#endnote-20).

W 2001 r zaprezentowano ABS w wersji 8.0. Modułowa konstrukcja tej generacji układu przetrwała do czasów dzisiejszych. Umożliwiała ona wytworzenie wielu wersji zaawansowania systemu obejmującego nie tylko ABS ale także ASR i ESP w dość podobny sposób. Wszystkie produkowane przez firmę Bosh systemy są produkowane przy zachowaniu jednolitego standardu obowiązującego we wszystkich zakładach produkcyjnych na świecie[[21]](#endnote-21). Polska również wniosła pewien wkład w rozwój układu ABS. Na początku lat osiemdziesiątych w warszawskiej Fabryce Samochodów Osobowych (FSO) powstał Hamulcowy Układ Antypoślizgowy (HUAP), który uznawany jest za pierwszy polski układ przeciwblokujący koła[[22]](#endnote-22).

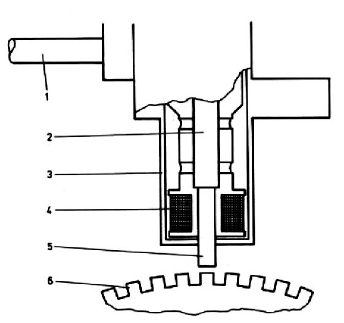
### Obwód elektroniczny

Współcześnie znane układy ABS, nie tylko firmy Bosh ale także innych producentów można zasadniczo podzielić na dwa obwody: elektroniczny i hydrauliczny.

Podstawowymi elementami obwodu elektronicznego systemu ABS są: zespół sterujący, cztery oddzielne dla każdego koła czujniki pomiaru prędkości obrotowej, czujnik położenia pedału hamulca, czujnik lampki kontrolnej, umiejscowionej na desce rozdzielczej kierowcy oraz czujniki kontroli poziomu i wartości ciśnienia płynu hamulcowego w układzie hamowania.

Elektroniczny Zespół Sterujący (EZU) jest odpowiedzialny z odbieranie i przetwarzanie sygnałów pochodzących z czujników pomiaru prędkości kół, czujnika położenia pedału hamulca, oraz czujników poziomu i wartości ciśnienia płynu hamulcowego w układzie. Zapewnienie ciągłej kontroli wyników z czujników składowych pozwala EZU m.in na ustalenie częstotliwości zmian prędkości chwilowej kół. Dokładność danych zapewniana jest przez wysoką częstotliwość pomiaru prędkości (ok 100 razy na minutę). Wykrycie nagłego spadku prędkości kół w krótkim czasie, przy jednoczesnej kwalifikacji zdarzenia, na podstawie sygnału z czujnika położenia pedału hamulca (wysłanie sygnału następuje w momencie gwałtownego dociśnięcia pedału hamulca w kierunku podwozia pojazdu) , jako hamowanie awaryjne, powoduje rozpoczęcie sterowania elektrozaworami wylotowymi i dolotowymi w taki sposób aby jak najszybciej odblokować zablokowane koła. Skuteczność działania przeciwblokującego jest interpretowana przez system, jako przywrócenie częstotliwości zmian prędkości obrotowej kół, do porównywalnych wartości, wykrywanych przed spadkiem, który zainicjował sekwencję działań przeciwblokujących. Wysoka częstotliwość wykonywania sekwencji sterujących elektrozaworami umożliwia dziesięciokrotną korekcję siły hamowania w ciągu jednej sekundy. Stwierdzenie jakichkolwiek nieprawidłowości np.: zwarcie przewodów, brak sygnału z czujników, zbyt niskie ciśnienia płynu hamulcowego lub zbyt mała jego ilość w układzie, powoduje uruchomienie przez EZU sekwencji instrukcji wyłączających system ABS wraz z zapisaniem kodu błędu w logach zdarzeń. EZU przekazuje sygnał o błędzie do czujnika lampki kontrolnej na desce rozdzielczej kierowcy. Widząc zapaloną kontrolkę ostrzegawczą, kierowca powinien udać się do serwisu w celu dokonania naprawy systemu[[23]](#endnote-23).

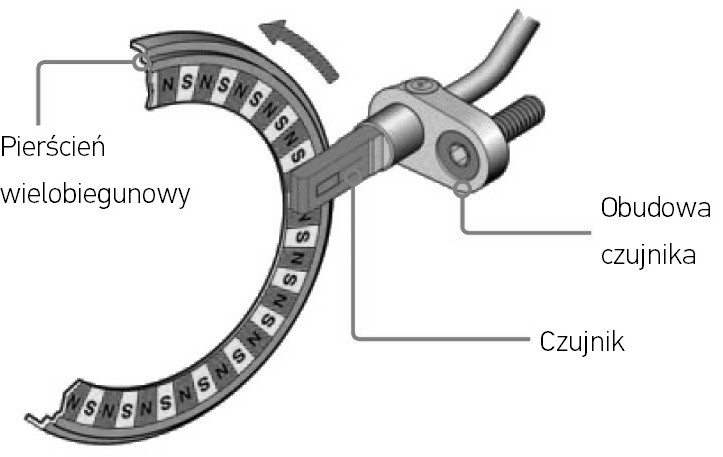
Skuteczne działanie systemu ABS jest możliwe dzięki danym o prędkości obrotowej kół które dostarczane są przez czujniki pomiarowe. Urządzenia te są generatorami prądu typu indukcyjnego. Pomiar prędkości odbywa się na podstawie sygnału o zmiennej częstotliwości proporcjonalnej do prędkości kątowej (liczby obrotów na sekundę) koła do którego czujnik jest podłączony.



Rysunek 5. Budowa pasywnego czujnika pomiaru prędkości 1 - przewód elektryczny, 2 – rdzeń magnetyczny, 3 – szczelna obudowa, 4 – uzwojenie, 5 – końcówka czujnika, 6 – tarcza z naciętymi zębami [[24]](#endnote-24).

Ze względu na sposób działania czujniki pomiaru prędkości obrotowej można podzielić na:

* Czujniki pasywne – współpracują z pierścieniem lub tarczą zębatą umieszczona na piaście koła lub przegubie napędowym zewnętrznym półosi. Podczas obracania się tarczy czujnik „liczy” ilość mijających go zębów tarczy w określonej jednostce czasu. Wewnątrz czujnika znajduje się rdzeń z uzwojeniem lub magnesem generującym pole elektromagnetyczne sięgające powierzchni koła zębatego. Obracanie się tarczy zębatej powoduje zmiany w polu elektromagnetycznym czujnika co skutkuje indukowaniem napięcia wewnątrz czujnika. Informacje o liczbie miniętych zębów na tarczy oraz wartość napięcia na rdzeniu czujnika wysyłane są w formie sygnału do EZU.
* Czujniki aktywne - współpracują z wielobiegunowym pierścieniem elektromagnetycznym umieszczonym przy kole. Na powierzchni pierścienia znajdują się wyodrębnione pola biegunowe oznaczone literami S i N. Czujnik współpracujący z tak zbudowanym pierścieniem złożony jest z elementów półprzewodnikowych które „rozpoznają” zmieniające się pole elektromagnetyczne generowane przez pierścień. Obracanie się pierścienia powoduje wygenerowanie sygnału, który przesyłany jest do sterownika EZU.



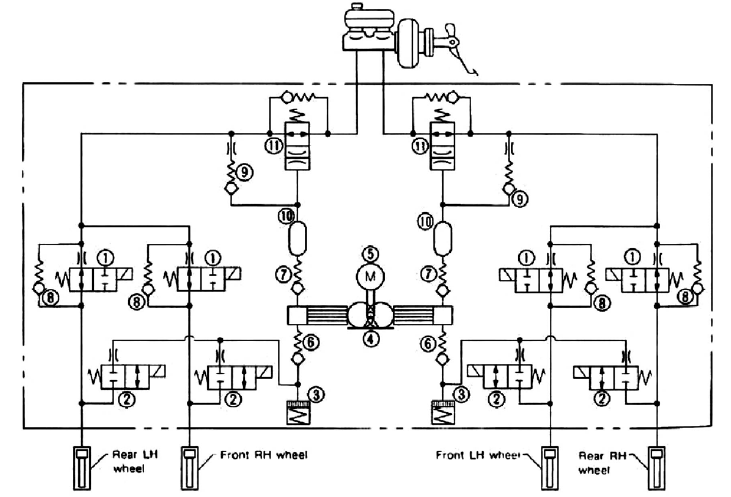
Rysunek 6 Schemat czujnika aktywnego wraz z pierścieniem elektromagnetycznym[[25]](#endnote-25)

Intensywny rozwój technologii czujników aktywnych umożliwił poprawienie wydajności ich działania poprzez wykorzystanie zjawiska Halla. Aktywny czujnik z magnesem w celu wygenerowania sygnału wyjściowego współpracuje z impulsywną tarczą tzw. kołem dekodującym, umiejscowionym na uszczelniaczu łożyska koła. Obracanie się koła powoduje powstawanie napięcia a przez to następuje zmiana natężenia pola elektromagnetycznego. Informacje o zmianach zachodzące w obrębie pola elektromagnetycznego są przesyłane do sterownika zespołu sterującego.

Mając na względzie współczesne standardy pracy układów kontrolujących tor jazdy samochodu, czujniki aktywne są zdecydowanie lepszym i bardziej precyzyjnym rozwiązaniem ponieważ wysyłają sygnały z danymi pomiarowymi już od prędkość obrotowej kół jest na poziomie 0,1 km/h. Oznacza to szybsze i bardziej dokładne dostarczanie danych do analizy przez EZU a zatem większą efektywność działań przeciwblokujących. Dla porównania czujniki pasywne rozpoczynają wysyłanie sygnałów pomiarowych od prędkości wyższych niż 3 km/h. Wykorzystanie zjawiska Halla pozwoliło na wyprodukowanie czujników rozpoznających kierunek obrotu koła, co jest ważną informacją dla poprawnej interpretacji przez EZU otrzymanych danych pomiarowych. Przewaga czujników aktywnych widoczna jest także w obszarach niezawodności, mniejszej wrażliwości na zakłócenia, oraz odporności na wysokie temperatury czy wibracje[[26]](#endnote-26).

### Obwód hydrauliczny

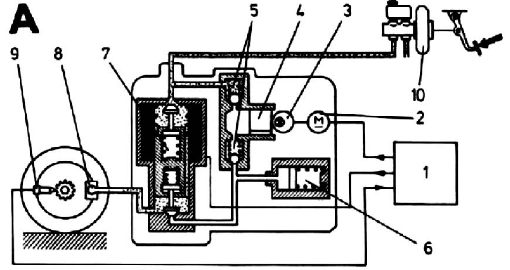
Obwód hydrauliczny, często nazywany też hydraulicznym zespołem sterującym jest całkowicie bezobsługowy. Stwierdzenie nieprawidłowości działania któregokolwiek z jego elementów powinno skutkować wymianą całego zespołu a nie poszczególnych elementów. Główne komponenty to: osiem elektrozaworów (cztery elektrozawory wylotowe i cztery elektrozawory dolotowe, po jednym z obu rodzajów dla niezależnej obsługi każdego koła), pompa hydrauliczna, akumulatory ciśnienia oraz elektrozawory główne.



Rysunek 7. Schemat obwodu hydraulicznego w układzie ABS na przykładzie samochodu Nissan Almera. Elementy składowe: 1 – elektrozawory jednokierunkowe wlotowe (zwiększające ciśnienie płynu hamulcowego), 2 – elektrozawory jednokierunkowe wylotowe (zmniejszające ciśnienie płynu hamulcowego), 3 – akumulatory ciśnienia płynu hamulcowego, 4 – pompa, 5 – silnik pompy elektrycznej, 6 – zawory wlotowe kulkowe jednokierunkowe, 7 – zawory wylotowe kulkowe jednokierunkowe, 8 – zawory zwrotne kulkowe jednokierunkowe, 8 – zawory zwrotne kulkowe jednokierunkowe, 10 – zasobniki (tłumiki pulsacji ciśnienia płynu hamulcowego), 11 – elektrozawory główne z zwrotnymi zaworami kulkowymi

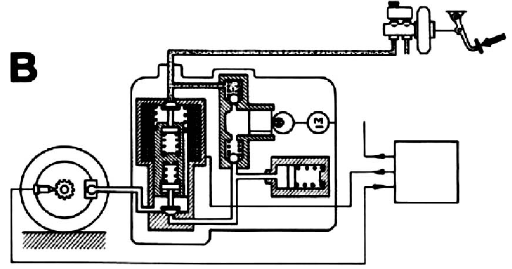
Działania przeciwblokujące dzięki którym system ABS wspiera kierowcę podczas hamowania, są wykonywane poprzez regulację ciśnienia płynu hamulcowego ,w zaciskach hamulcowych. Proces korygowania ciśnienia jest zależny od zmierzonej prędkości obrotowej kół. Rezultatem sterowania poziomem ciśnienia jest kontrola nad siłą z jaką szczęki hamulcowe dociskają powierzchnię kół. Cykl regulacji ciśnienia płynu hamulcowego jest realizowany przez precyzyjne sterowanie układem jednokierunkowych elektrozaworów wlotowych   
/ wylotowych. Zawory te są elektromagnetyczne, wyposażone w ruchomy „tłoczek”, który przyjmuje określone położenie w zależności od sposobu w który ma następować regulacja ciśnienia płynu w układzie hamulcowym. Elektrozawory są zasilane prądem zmiennym o napięciu + 12 V, za pomocą przekaźnika. Sterowanie pracą elektrozaworu odbywa się za pomocą ujemnego przerywanego sygnału pochodzącego z elektronicznego zespołu sterującego. Praca elektrozaworów odbywa się wg trzech faz:

* Faza wzrostu ciśnienia– brak sygnałów sterujących od elektronicznego zespołu sterującego. Położenie „tłoczka” wewnątrz elektrozaworu umożliwia swobodny przepływ płynu hamulcowego od pompy hamulcowej do zacisku szczeki hamulca. Ciśnienie w obwodzie jest w pełni zależne od siły z jaką kierowca naciska pedał hamulca w samochodzie. Elektrozawory pozostają w tej fazie pracy także w przypadku awarii układu ABS, co pozwala na skuteczną pracę układu hamulcowego bez wsparcia elektronicznego. Brak regulacji ciśnienia płynu hamulcowego przez elektroniczny system wspierający na podstawie pomiaru prędkości kątowej w czasie rzeczywistym sprawia, że ryzyko zablokowania kół podczas hamowania awaryjnego jest bardzo wysokie.



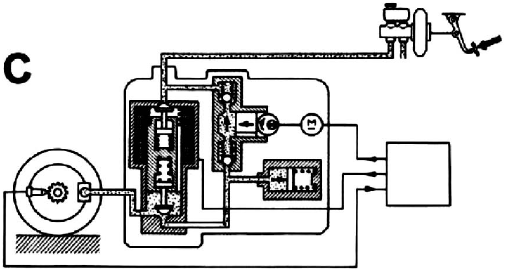
Rysunek 8 Faza wzrostu ciśnienia. Widoczny jest schemat elektrozaworu regulującego wraz z pompą elektryczną. 1 – elektroniczny zespół sterujący, 2 – silnik pompy elektrycznej, 3 – krzywka, 4 – tłoczek pompy elektrycznej, 5 - zawory kulkowe jednokierunkowe, 6 – akumulator ciśnienia, 7 – elektrozawór, 8 – zacisk hamulcowy, 9 – czujnik prędkości koła, 10 – pompa hamulcowa.

* Faza utrzymania stałej wartości ciśnienia– sterowanie w tej fazie odbywa się przy ograniczonym napięciu elektrycznym. Tłoczek blokujący, w skutek działania pola elektromagnetycznego, przesuwa się od wysokości połowy swojego skoku w celu odcięcia dopływu płynu hamulcowego, do zacisków hamulcowych. Wzrost ciśnienia nie jest możliwy bez względu na siłę jak z jaka kierowca naciska na pedał hamulca. Następuje oddzielenie mechanizmu hamującego od pompy hamulcowej i obwodu powrotnego.



Rysunek 9. Faza utrzymywania stałej wartości ciśnienia. Schemat z uwzględnieniem położenia tłoczka sterującego wewnątrz elektrozaworu oraz widok połączonej z nim pompy elektrycznej

* Faza zmniejszania ciśnienia – sterowanie odbywa się przy maksymalnej wartości napięcia elektrycznego. Następuje przyciągnięcie tłoczka blokującego przez pole elektromagnetyczne, powodując tym samym zamknięcie przewodu dolotowego, a także połączenie obwodu zacisku hamulcowego z pompą elektryczną. Uruchomienie pompy elektrycznej następuje za pomocą przekaźnika przez elektroniczny zespół sterujący. Wypompowanie płynu hamulcowego powoduje zmniejszenie ciśnienia w zacisku hamulcowym. Dzięki temu możliwy jest ponowny dopływ płynu hamulcowego przez przewody dolotowe z pompy hamulcowej w celu natychmiastowego odblokowania koła, które zostało zakwalifikowane przez system jako poślizgu.



Rysunek 10 Faza ograniczania ciśnienia. Tłoczek elektrozaworu jest uniesiony do góry poprzez przyciąganie pola elektromagnetycznego. Dzięki pracy pompy elektrycznej następuję wypompowanie płynu hamulcowego z układu a przez to zmniejszenie ciśnienia na zacisku szczęki hamulca.

Faza wzrostu i utrzymania stałej wartości ciśnienia są powtarzane za każdym razem gdy nastąpi wykrycie koła lub kół, które mogą zostać zablokowane. Fazy te następują bardzo szybko (do 10 razy nas sekundę) dzięki czemu korekcja ciśnienia na zaciskach hamulcowych jest bardziej precyzyjna Wpływa to bezpośrednio na skuteczność działań przeciwblokujących jakie ABS podejmuje w przypadku nagłego hamowania[[27]](#endnote-27).

Ważnym elementem układu hydraulicznego ABS jest pompa elektryczna. Kilka zdań na jej temat pojawiło się wcześniej przy okazji omawiania faz pracy elektrozaworów. Należy jednak ten element potraktować bardziej szczegółowo ze względu na rolę jaka spełnia w prawidłowo działającym obwodzie hydraulicznym układu ABS.

Pompa elektryczna jest typu rotacyjnego. Jej głównym zadaniem jest zasysanie płynu hamulcowego ze zbiornika i kanałów powodując wzrost ciśnienia w akumulatorze. Wydajność pompy jest ograniczona ze względu na fakt że podczas pracy wytwarza ona duże ciśnienie robocze (do 21 MPa). Rozruchem pompy steruje silnik elektryczny, zasilany prądem zmiennym przez przekaźnik pompy, oraz wyłącznik ciśnieniowy. Pompa składa się z wirnika, którego tłoczki są umieszczone w sposób promieniowy, naprzeciwko siebie oraz bieżni pierścieniowej umieszczonej niewspółosiowo. Pompa elektryczna jest bezobsługowa w przypadku zużycia sygnalizowanego np. przez nadmierny poziom hałasu podczas jej pracy albo wytwarzanie zbyt dużego ciśnienia, możliwa jest jej wymiana. Ciśnienie robocze pompy zwykle mieści się w przedziale 14 – 18 MPa i jest regulowane przez wyłącznik ciśnieniowy. Osiągniecie ciśnienia 14 MPa powoduje włączenie się pompy elektrycznej. Urządzenie jest wyłączane kiedy ciśnienie przekroczy górną granicę zakresu a więc 18 MPa. Gdy ciśnienie robocze spada poniżej 14 MPa, wyłącznik ciśnieniowy uruchamia przekaźnik pompy poprzez dostarczenie ujemnego sygnału do styku 85. Przekroczenie górnej granicy ciśnienia roboczego powoduję odcięcie dopływu sygnału ujemnego, dzięki czemu przekaźnik kończy pracę pompy. Praca pompy jest możliwa tylko przy włączonym zapłonie lub gdy silnik pracuje, ponieważ dostarczenie dodatniego sygnału o natężeniu 12 V na styku 86 odbywa się przy użyciu wyłącznika zapłonu. Wyposażenie pompy w zawór zwrotny pozwala na przepływ płynu hamulcowego w obu kierunkach z i do akumulatora ciśnienia w zależności od fazy pracy elektrozaworów układu hydraulicznego. Możliwa awaria przekaźnika lub wyłącznika ciśnieniowego, która mogłaby doprowadzić do wytworzenia ciśnienia, przez pracującą pompę, wyższego niż robocze spowodowała konieczność zastosowania zaworu bezpieczeństwa. Zawór ten ogranicza ciśnienie do wartości 21 MPa umożliwiając odpływ nadmiaru płynu do przewodu dolotowego pompy. Takie rozwiązanie ma na celu podniesienie bezpieczeństwa układu przez umożliwienie przepływu płynu hamulcowego nawet jeśli obwód jest zamknięty[[28]](#endnote-28). Uruchomienie pompy następuje równocześnie z elektrozaworami regulacyjnymi w momencie gdy nastąpi faza ograniczania ciśnienia. Połączenie pracy pompy elektrycznej z elektrozaworami dało możliwość zmniejszenia ciśnienia w zaciskach hamulcowych, co kierowca odczuwa jako lekkie pulsacje przy dociskaniu pedału hamulca[[29]](#endnote-29).

Regulacja ciśnienia płynu hamulcowego w obrębie pompy elektrycznej nie byłaby możliwa bez użycia akumulatorów ciśnienia. Akumulator ten jest zamontowany na powierzchni korpusu pompy elektrycznej i pełni rolę zbiornika przechowującego ok 150 cm3 płynu hamulcowego pod ciśnieniem 14 – 18 MPa. Zbiornik akumulatora jest podzielony na dwie komory oddzielone od siebie elastyczną membraną. Komora górna zwiera azot pod ciśnieniem wstępnym 8 MPa. Komora dolna w trakcie fazy roboczej jest wypełniona płynem hamulcowym. Pojemność każdej z komór akumulatora zmienia się w zależności faz pracy elektrozaworów wymagających zmniejszenia, utrzymania lub zwiększenia ciśnienia płynu hamulcowego. Przed dostarczeniem płynu hamulcowego pojemność dolnej komory jest równa zero. Membrana jest dociśnięta do dna zbiornika akumulatora. Wyłącznik ciśnieniowy przesyła sygnał sterujący do przekaźnika, włączając pompę elektryczną. Płyn hamulcowy pompowany przez pompę elektryczną przez przewód doprowadzający wypełnia dolną komorę zbiornika akumulatora powodując podnoszenie się membrany do góry. Po przekroczeniu ciśnienia 18 MPa wyłącznik ciśnieniowy przekazuje sygnał sterujący do przekaźnika pompy powodując jej wyłączenie. Spadek ciśnienia płynu hamulcowego znajdującego się w akumulatorze poniżej 14 MPa powoduje ponowne włączenie pompy elektrycznej w celu podniesienia ciśnienia płynu hamulcowego w komorze akumulatora. Poziom płynu hamulcowego zmniejsza się w przypadku gdy kierowca naciska pedał hamulca. Płyn hamulcowy znajdujący się w komorze akumulatora jest wówczas wykorzystywany przez obwód hydrauliczny do regulacji ciśnienia na zaciskach szczęk hamulcowych[[30]](#endnote-30).

Akumulatory ciśnienia dostosowują swoją pracę do faz pracy elektrozaworów wylotowych i dolotowych Magazynują niewielką ilości płynu hamulcowego odprowadzonego przez pompę elektryczną z zacisków hamulcowych – fazy zmniejszania ciśnienia. Płyn hamulcowy jest ponownie przekazywany do zacisków hamulcowych z rozprężonej komory akumulatora ciśnienia – zakończenie fazy zmniejszania ciśnienia[[31]](#endnote-31).

## Wymagania

Elektroniczne systemy wsparcia kierowcy maja za zadanie podnieść poziom jego bezpieczeństwa, w nagłych i nie przewidzianych sytuacjach na drodze. ABS jako system wspierający działanie układu hamulcowego, który jest kluczowym układem pojazdu samochodowego, musi być systemem bezpiecznym. Oznacza to, że usterka systemu ABS, nie może być równoznaczna, z awarią działania układu hamulcowego, a wiec pozbawieniem kierowcy możliwości zatrzymania pojazdu. Kierowca powinien być w stanie rozpocząć akcję hamowania niezależnie od tego czy system ABS pracuje prawidłowo. Zatrzymanie pojazdu nadal powinno być możliwe przy użyciu układu hamulcowego bez wsparcia elektronicznego, nawet jeśli wzrasta ryzyko zablokowania kół i w efekcie poślizgu, utraty kontroli nad pojazdem w sytuacji krytycznej. Określenie poziomu bezpieczeństwa jest możliwe poprzez zapewnienie, że system spełniania stawiane przed nim wymagania, w określonym kontekście użycia.

Główne wymagania postawione przed systemem ABS to:

* Oczekiwane jest aby włączenie systemu następowało po odebraniu sygnału z czujnika naciśnięcia pedału hamulca.
* Przy każdym uruchomieniu silnika pojazdu wymagana jest kontrola gotowości systemu do działania. W tym celu system wykona diagnostyczną procedurę testową, która sprawdzi czy nie zostały znalezione błędy blokujące jego poprawne działanie.
* Każde zdarzenie, w którym system odbierze sygnał o włączeniu hamulców zainicjuje uruchomienie podstawowej procedury testowej, której zadaniem będzie sprawdzenie czy system działa prawidłowo.
* Wykrycie błędów przez wcześniejsze procedury diagnostyczne spowoduje wykonanie metody wyłączenia systemu ABS. Układ hamulcowy nadal będzie sprawny jednak hamowanie odbywać się będzie bez wsparcia elektronicznego systemu przeciwblokującego koła.
* Wymagane jest aby system ABS przesyłał informacje dotyczące wykrytych błędów do pamięci komputera pokładowego samochodu, skąd będzie możliwe ich odczytanie przez personel podejmujący czynności naprawcze.
* Wysłanie informacji o awarii systemu ABS do komputera pokładowego samochodu spowoduje zapalenie sygnału ostrzegawczego na konsoli kierowcy. Spełnienie tego wymogu jest kluczowe w kontekście zapewnienia bezpieczeństwa kierującemu pojazdem, który wiedząc o awarii, może odpowiednio wcześniej zwrócić się do autoryzowanego serwisu, w celu dokonania czynności naprawczych.
* System będzie umożliwiał wykonanie procedury restartującej po wykonaniu czynności naprawczych przez wykwalifikowany personel serwisowy. Procedura ta, usunie status awarii w systemie, do czasu zakończenia najbliższego testu diagnostycznego, np. po uruchomieniu silnika, po którym system ABS wyśle informacje do komputera pokładowego o gotowości do pracy lub awarii jeśli błędy nadal występują.
* System ABS będzie w stanie odbierać sygnały z czujników pomiaru prędkości obrotowej dla każdego z kół.
* System będzie przeciwdziałał blokowaniu kół w oparciu o zaimplementowany algorytm służący do interpretacji odczytanych pomiarów z czujników prędkości obrotowej. Umożliwi to wcześniejsze wykrycie kół które mogą zostać zablokowane. Analiza danych odbywać się będzie na zasadzie pomiaru czy zmierzona wartość prędkości obrotowej koła zbliża się do zakładanej wartości progowej w systemie powyżej której, system zakwalifikuje koło jako potencjalnie zablokowane.
* Możliwe będzie sterowanie przez system ABS układem elektrozaworów odpowiadających za zmniejszanie lub zwiększanie ciśnienia a przez to siły hamowania w zaciskach hamulcowych kół, które mogą zostać zablokowane.
* System będzie reagował dynamicznie w zależności od wyników permanentnego pomiaru prędkości obrotowej dla każdego z kół[[32]](#endnote-32).

Wykazanie że system ABS jest bezpieczny wymaga udowodnienia że każdy z wyżej wymienionych wymogów został spełniony. Graficzną reprezentacją wnioskowania o bezpieczeństwie systemu ABS jest dowód bezpieczeństwa (*Safety Case*).

## Analiza bezpieczeństwa

hazardy / failure modes

## Proces wytwórczy ABS

Współczesny przemysł motoryzacyjny dużą część zysków inwestuje w najnowsze zdobycze nauki i techniki w celu dostarczenia użytkownikom samochodów gwarantujących jak najwyższy komfort i bezpieczeństwo podczas jazdy. Cele te osiągane są poprzez implementacje coraz większej ilości elektronicznych systemów których zadaniem jest podnoszenie standardu komfortu i bezpieczeństwa kierowcy w trakcie jazdy samochodem. Wysoki poziom zaawansowania stosowanych algorytmów komputerowych pozwala na efektywniejsze bardziej precyzyjne przetwarzanie danych pochodzących z czujników pomiarowych. Pozwala to na szybszą i skuteczniejszą „reakcję” elektronicznych systemów pokładowych samochodu na zmieniające się warunki otoczenia zewnętrznego. Podnoszenie standardów bezpieczeństwa sprawia, że czynnik błędu ludzkiego jest coraz bardziej minimalizowany. Rozbudowa funkcjonalności sterowników systemów pozwala na automatyczną aktywacje układu, który w ten sposób może reagować na zmiany w otoczeniu niezależnie od kierowcy. Szczególne znaczenie ma to w sytuacji gdy chwila nieuwagi kierującego pojazdem decyduje o tym czy stanie się on uczestnikiem wypadku drogowego czy też nie. Projektanci systemów wbudowanych sterujących elektroniką pojazdu są świadomi, że tworzony przez nich produkt ma działać tak aby być w stanie inteligentnie korygować działania kierowcy, lub zastąpić go w sytuacji gdy ten w panice podczas zagrożenia na drodze nie podejmuje żadnych działań.

Obrany kierunek rozwoju nowoczesnych technologii w motoryzacji stał się przyczyną do opracowania wyspecjalizowanych narzędzi programistycznych i standardów wytwarzania układowego oprogramowania sterującego, które powinno być niezależne od architektury sprzętowej, proste w utrzymaniu, niezawodne i łatwe do rozbudowy.

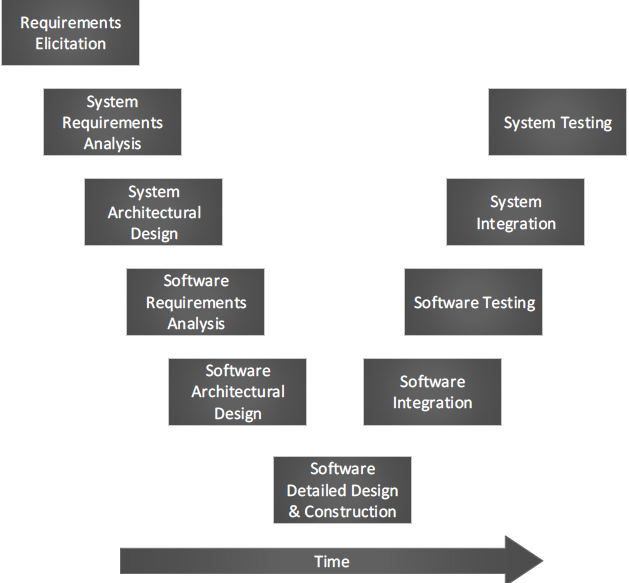
Najwięksi klienci przemysłu motoryzacyjnego w Europie, zwracają uwagę na rolę skutecznego i ustandaryzowanego zarządzania projektem, co jest wg nich równie ważne, jak wytworzenie konkretnego oprogramowania układowego. Sprawne, zarządzanie procesem wytwórczym daje odbiorcy produktu zdecydowanie więcej pewności, że zamawiany produkt będzie spełniał stawiane przed nim wymagania a przede wszystkim zostanie dostarczony w zakładanym terminie. Czas dostarczenia, produktu ma bezpośredni wpływ na proces wytwórczy w fabryce klienta, gdzie każde opóźnienie oznacza straty określonej części zysków. Dlatego klient musi mieć gwarancję minimalizacji ryzyka że produkt będzie dostarczony zbyt późno lub nie będzie spełniał oczekiwań i ostatecznie jego wdrożenie opóźni się. Jasność i przejrzystość procesu wytwórczego u dostawcy ma zatem dla klienta kluczowe znaczenie.. Standaryzacja procesu wytwórczego ma pomóc klientom na łatwiejszą kontrolę wytwarzania określonych produktów u rożnych dostawców w tym samym czasie. Ułatwia to lepsze planowanie procesu produkcyjnego po stronie klienta.

Najwięksi producenci samochodów chętniej współpracują z dostawcami systemów którzy proces wytwórczy opierają na standardzie SPICE (Software Process Improvement Capability Etermination).. Standard ten normuje proces wytwarzania, testowania systemu, oraz nakreśla sposób efektywnego zarządzania projektem tak aby produkt końcowy został dostarczony w terminie i pokrywał wymagania klienta. SPICE definiuje czym jest, jak przebiega i z jakich elementów składa się cykl wytwórczy produktu. Ważne jest to że oparcie się o tę metodologie wymusza wytwarzanie dokumentacji potwierdzającej spełnianie wyznaczonych standardów w określonych punktach czasu trwania projektu. Ułatwia to klientowi kontrolę i ocenę „dojrzałości” projektu w kluczowych momentach. Projekt prowadzony wg SPICE musi spełniać wymagania w zakresie:

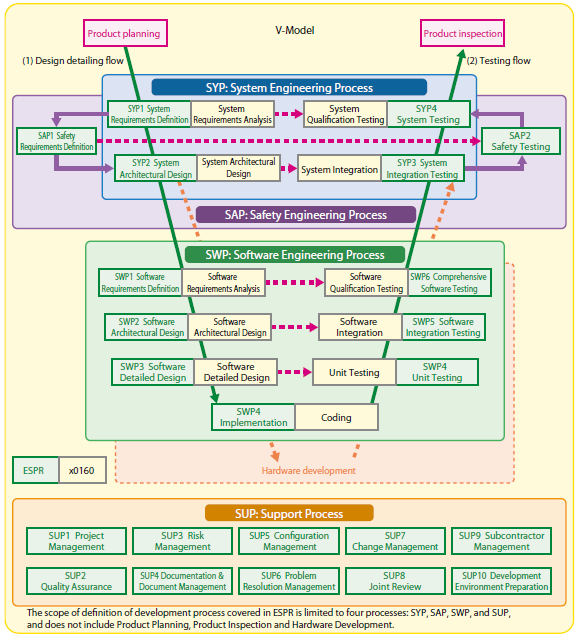
* Podstawowej praktyki która musi być wykonana dla każdego procesu zachodzącego w projekcie
* Dokumentów oraz danych, które musza zostać wytworzone w wyniku każdej podstawowej praktyki
* Atrybutów dla każdego produktu
* Wykazania że projekt jest odpowiednio zarządzany
* Wykazania że projekt jest odpowiednio wspierany

Istniejące standardy ze względu na zmieniającą się specyfikę branży motoryzacyjnej musza być ciągle rozwijane i uaktualniane w taki sposób aby dawały najlepsze gwarancje spełniania celów których realizacje maja wspomagać. Przykładem takiego rozwoju jest zaproponowany przez stowarzyszenie czołowych producentów samochodów (SIG – Sepcial Interest Group) standard Automotive SPICE. Standard ten opracowano w taki sposób aby jeszcze bardziej formalizował cykl tworzenia systemu wbudowanego zamykając etapy jej tworzenia do wspólnie przyjętych jednolitych procesów. Przyjęcie tego standardu pozwoliło na polepszenie jakość wytwarzania oprogramowania wbudowanego dla branży motoryzacyjnej przez minimalizację prawdopodobieństwa pominięcia niektórych wymagań klienta. Wykazano że dla zgodności cyklu wytwarzania systemu wbudowanego dla pojazdów mechanicznych ze standardem Automotive Spice konieczne jest aby każde wymaganie klienta pokrywał oddzielny scenariusz testowy (ang. traceability). Zachowanie zgodności ze standardem Automotive SPICE wymusza na dostawcy oprogramowania umiejętne planowanie wszystkich zadań, ciągłą analizę wymagań klienta, tworzenie architektury i specyfikacji do programów, przeglądy kodu itd. Takie prowadzenie projektu podnosi prawdopodobieństwo wczesnego wykrycia błędów a co za tym idzie niższy koszt ich naprawy. Minimalizowanie wystąpienia błędów przekłada się uzyskanie oprogramowania wyższej jakości co jest kluczowe jeśli tworzone jest ono do obsługi modułów odpowiedzialnych za funkcje bezpieczeństwa w samochodzie.

Jedną z powszechniej stosowanych implementacji standardu Automotive SPICE jest tzw. model V który opisuje kolejność kroków w procesie wytwarzania oprogramowania.



Rysunek 11. Uproszczony schemat implementacji standardu Automotive SPICE (model V) [[33]](#endnote-33)

Każdy krok ma przypisane określone zadania, których wykonanie leży w zakresie zespołów biorących udział w procesie wytwarzania oprogramowania. Realizacja uporządkowanych zadań ma zapewnić osiąganie określonych celów w zakresie realizacji wymagań stawianych przez klienta od początku cyklu wytwórczego. Poszczególne kroki w modelu V zgrupowane są w zakresie czterech podstawowych procesów:

Rysunek 11. Rozszerzony schemat implementacji standardu Automotive SPICE (model V)

* **System Engineering Process (SYP)**  - traktuje produkt wytwarzany dla klienta jako kompletny system podlegający kontrolowanemu przez klienta rozwojowi w obszarze sprzętu i oprogramowania. Proces ten składa się z kroków takich jak:

|  |  |  |
| --- | --- | --- |
| - **analiza wymagań klienta co do systemu (System Requirements Definition)** | | |
| W ramach tego kroku należy szczegółowo wyjaśnić jakie wymagania powinien spełniać system aby spełniać oczekiwania klienta. Ze wszystkich wymagań przedstawionych przez klienta wybierane są tylko te które dotyczą wytwarzanego przez dostawcę modułu. | **Zadania do wykonania:** - przygotować specyfikacje wymagań klienta co do systemu  - dokonać przeglądu wytworzonej specyfikacji wymagań klienta | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - specyfikacja wymagań co do systemu  - raport wewnętrzny z przeglądu wymagań klienta co do systemu |

|  |  |  |
| --- | --- | --- |
| - **zaprojektowanie architektury systemu (System Architectural Design)** | | |
| Krok ten wymaga zaprojektowania modelu systemu uwzględniając wymagania w zakresie sprzętu i oprogramowania. Celem powinno być określenie części składowych systemu oraz sposobu integracji pomiędzy nimi | **Zadania do wykonania:**  - przygotować projekt systemu wraz z opisem jego części składowych tj. zarówno sprzętu jaki i oprogramowania. Opis powinien zawierać informacje w jaki sposób należy zaprojektować elementy systemu, aby spełniał on wymagania zdefiniowane w specyfikacji  - dokonanie przeglądu wewnętrznego wytworzonego projektu systemu w celu określenia właściwego doboru komponentów  - dokonanie przeglądu projektu architektury systemu pod kątem poprawności opisu i integracji poszczególnych elementów | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - opis projektu architektury systemu  - raport wewnętrzny z przeglądu opisu architektury systemu – potwierdzenie, że projekt architektury systemu jest kompletną odpowiedzią na przedstawione wymagania przez klienta |

|  |  |  |
| --- | --- | --- |
| - **wykonanie testów integracyjnych systemu (System Integration Testing)** | | |
| Czynnością do wykonania w tym kroku jest potwierdzenie poprawności działania dostarczonych funkcjonalności systemu poprzez uzyskanie pozytywnych wyników z testów integracji poszczególnych modułów należących do wytwarzanego produktu | **Zadania do wykonania:**  - przygotowanie opisu testów integracji systemu  - wykonanie testów integracyjnych wg opisanych przypadków testowych  - analiza wyników testów | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - specyfikacja systemowych testów integracyjnych  - raport testów integracyjnych  - wewnętrzny dokument przeglądu raportu testów integracyjnych |

|  |  |  |
| --- | --- | --- |
| - **wykonanie testów systemowych (System testing)** | | |
| W ramach tego kroku niezbędne jest wykonanie testów systemowych mających na celu potwierdzenie, że wymagania klienta co do systemu zostały spełnione | **Zadania do wykonania:**  - przygotowanie scenariuszy testów systemowych  - przeprowadzenie testów systemowych  - przegląd wyników testów  - potwierdzenie kompletności procesu wytwórczego | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - specyfikacja testów systemowych  - raport testów systemowych  - raport końcowy procesu wytworzenia systemu uwzgledniający prezentację wytworzonego systemu i wyników testów na spotkaniu przy udziale interesariuszy projektu |

* **Software Engineering Process (SWP)** – gotowy produkt jest tu rozumiany jako oprogramowanie wbudowane sterujące pracą określonego modułu mechanicznego Proces ten składa się z kroków takich jak:

|  |  |  |
| --- | --- | --- |
| - **analiza wymagań klienta co do oprogramowania (Software Requirements Definition)** | | |
| W ramach tego kroku należy wyjaśnić i opisać wymagania które oprogramowanie musi spełniać aby być produktem jakiego oczekuje klient | **Zadania do wykonania:**  - przygotowanie specyfikacji wymagań klienta co do oprogramowania  - dokonać przeglądu wyspecyfikowanych wymagań klienta w celu selekcji tych które dotyczą oprogramowania sterującego modułem wytwarzanym przez dostawcę | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - specyfikacja wymagań co do oprogramowania  - raport wewnętrzny z przeglądu wymagań klienta co do oprogramowania |

|  |  |  |
| --- | --- | --- |
| - **zaprojektowanie architektury oprogramowania (Software Architectural Design)** | | |
| Realizacja tego kroku polega na zaprojektowaniu struktury i funkcjonalności aplikacji wbudowanej która ma zostać wytworzona | **Zadania do wykonania:**  - wykonanie opisu aplikacji wbudowanej w zakresie struktury i funkcjonalności które mają zostać wytworzone  - dokonanie przeglądu projektu struktury i planu implementacji poszczególnych funkcjonalności  - dokonanie przeglądu architektury i funkcjonalności aplikacji wbudowanej wspólnie z klientem w celu potwierdzenia zgodności z specyfikacja wymagań | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - opis projektu architektury oprogramowania  - raport wewnętrzny z przeglądu opisu architektury oprogramowania – potwierdzenie, że projekt architektury oprogramowania jest kompletną odpowiedzią na przedstawione wymagania przez klienta |

|  |  |  |
| --- | --- | --- |
| - **zaprojektowanie architektury oprogramowania /projekt szczegółowy (Software Detailed Design)** | | |
| Krok ten obejmuje wytworzenie projektu aplikacji o wyższym stopniu szczegółowości który obejmuje nie tylko zdefiniowanie poszczególnych funkcjonalności oraz modułów aplikacji odpowiedzialnych za ich obsługę, ale także projekt struktury logicznej wytwarzanego oprogramowania. | **Zadania do wykonania:**  - wykonanie opisu każdego modułu aplikacji z dokładnym uwzględnieniem funkcjonalności za jakie będzie odpowiedzialny  - dokonanie przeglądu wytworzonego projektu  - dokonanie sprawdzenia projektu pod katem spójności z specyfikacja sprzętową | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - szczegółowy opis projektu architektury oprogramowania  - raport z przeglądu wewnętrznego uszczegółowionego opisu projektu architektury oprogramowania |

|  |  |  |
| --- | --- | --- |
| **- implementacja oraz testy jednostkowe (implementation & Unit Testing)** | | |
| Ten krok w modelu procesu wytwórczego polega na Implementacji struktury aplikacji oraz wykonani testów jednostkowych na poziomie jej funkcjonalnych modułów | **Zadania do wykonania:**  - przygotowanie do wdrożenia aplikacji na środowisko testowe i przeprowadzenia testów jednostkowych  - przeprowadzenie wdrożenia i testów jednostkowych w oparciu o harmonogram wdrożeń i testów jednostkowych  - dokonanie przeglądu rezultatów wdrożenia aplikacji i testów jednostkowych | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - specyfikacja testów jednostkowych  - raport wykonania testów jednostkowych oprogramowania  - raport z przeglądu wewnętrznego rezultatów implementacji i testów jednostkowych oprogramowania |

|  |  |  |
| --- | --- | --- |
| - **Testy integracyjne oprogramowania (Software Integration Testing)** | | |
| Przeprowadzenie testów Integracyjnych aplikacji wg scenariuszy testowych | **Zadania do wykonania:**  - przygotowanie do wykonania testów integracyjnych  - przeprowadzenie testów integracyjnych wytworzonej aplikacji w celu określenia poprawności działania jej podstawowych funkcjonalności  - przegląd wyników testów | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - specyfikacja testów integracyjnych oprogramowania  - raport wykonania testów integracyjnych  - raport wewnętrzny z przeglądu rezultatów testów integracyjnych |

|  |  |  |
| --- | --- | --- |
| - **kompleksowe testy oprogramowania / testowanie kompatybilności aplikacji (Comprehensive Software Testing)** | | |
| Przeprowadzenie „kompleksowych” testów aplikacji po wdrożeniu, testach jednostkowych wszystkich modułów funkcjonalnych | **Zadania do wykonania:**  - przygotowanie do wykonania pełnego zakresu testów wytworzonej aplikacji  - przeprowadzenie pełnego cyklu testowego (wszystkie funkcjonalności aplikacji są wdrożone i udostępnione na środowisku testowym)  - dokonanie przeglądu wyników testów  - potwierdzenie zakończenia prac deweloperskich aplikacji.  Dokonanie oceny wytworzonego rozwiązania wśród interesariuszy projektu sprawdzając, czy zostały spełnione zdefiniowane na początku procesu wytwórczego wymagania systemowe. Przeprowadzanie końcowej oceny wytworzonego oprogramowania z określeniem nieprawidłowości w działaniu i wymagań które nie zostały pokryte funkcjami aplikacji. | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - specyfikacja testów w pełni wdrożonej aplikacji  - raport z wynikami przeprowadzonych testów  - raport z wewnętrznego przeglądu rezultatów testów na kompletnie wdrożonej aplikacji na środowisku testowym |

* **Safety Engineering Process (SAP)** – jest ukierunkowany na zapewnienie odpowiedniej jakości, a przez to określonego poziomu bezpieczeństwa wytwarzanego systemu. Proces ten składa się z kroków takich jak:

|  |  |  |
| --- | --- | --- |
| - **zdefiniowanie wymagań co do systemu w zakresie bezpieczeństwa (Safety Requirements**  **Definition)** | | |
| Identyfikacja wymagań systemu odnoszących się do bezpieczeństwa. | **Zadania do wykonania:**  - wytworzenie specyfikacji wymagań w zakresie bezpieczeństwa systemu  - dokonanie przeglądu specyfikacji wymagań w zakresie bezpieczeństwa | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - specyfikacja wymagań systemu w zakresie bezpieczeństwa  - wewnętrzny raport z przeglądu wyspecyfikowanych wymagań w zakresie bezpieczeństwa systemu |

|  |  |  |
| --- | --- | --- |
| **- testy bezpieczeństwa bezpieczeństwa (Safety Testing)** | | |
| Przeprowadzenie testów bezpieczeństwa wytworzonego systemu | **Zadania do wykonania:**  - przygotowanie do testów bezpieczeństwa  - przeprowadzenie testów bezpieczeństwa systemu  - dokonanie przeglądu rezultatów testów bezpieczeństwa | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - specyfikacja przypadków testowych do testów bezpieczeństwa  - raport testów bezpieczeństwa systemu  - wewnętrzy raport na temat przeglądu wyników testów bezpieczeństwa |

* **Support Process (SUP)** -składa się z czynności których wykonanie jest konieczne w celu sprawnego zarządzania zadaniami wykonywanymi podczas procesów rozwojowych opisanych wyżej. Proces ten składa się z kroków takich jak:

|  |  |  |
| --- | --- | --- |
| - **zarządzanie projektem (Project Management)** | | |
| Ogólne zdefiniowane kształtu projektu którego celem jest wytworzenie systemu wbudowanego zamawianego przez klienta. Zdefiniowanie najważniejszych zadań które musza zostać wykonane podczas trwania projektu | **Zadania do wykonania:**  - przygotowanie opisu planu projektu  - zrozumienie statusu wykonania projektu tj. zrozumienie co dla klienta jest tzw „definition of done”  - kontrola stanu projektu  - przygotowanie wstępnego raportu „kompletności” projektu | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - opis planu projektu  - raport statusu projektu  - opis planu projektu (ver 2) tylko jeśli nastąpiły istotne zmiany po ponownym zbadaniu projektu  - Raport ze stanu realizacji projektu (dotyczący tworzonego oprogramowania) |

|  |  |  |
| --- | --- | --- |
| **- zapewnienie jakości (Quality Assurance)** | | |
| Zdefiniowanie zadań potrzebnych do zapewnienia jakości wytwarzanego oprogramowania aby mieć pewność że na etapie wytwórczym produkt spełnia standardy rynku co do poziomu jakości określone dla systemów wbudowanych w trakcie procesu wytwarzania | **Zadania do wykonania:**  - zdefiniowanie celów w procesie zapewnienia jakości produktu  - wybranie metod zapewnienia jakości wytwarzanemu produktowi  - kontrola jakości w oparciu o przygotowany model procesu zapewnienia jakości oprogramowania wbudowanego | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - opis planu zapewnienia jakości wytwarzanego oprogramowania. Każda aktualizacja wymaga utworzenia nowej wersji planu. |

|  |  |  |
| --- | --- | --- |
| - **zarządzanie ryzykiem (risk management)** | | |
| Podejmowanie działań mających na celu wykrycie na wczesnym etapie projektu ryzyk które mogą być zagrożeniem dla spojności procesu wytwórczego | **Zadania do wykonania:**  - identyfikacja i określenie ryzyk projektu  - ciągła obserwacja ryzyka projektu  - określenie i wdrożenie metod mających na celu przeciwdziałanie lub minimalizację skutków ryzyka projektu | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - opis planu zarządzania ryzykiem projektu. Każda aktualizacja wymaga utworzenia nowej wersji dokumentu. |

|  |  |  |
| --- | --- | --- |
| - **wytwarzanie i zarządzanie dokumentacją (documentation, document management)** | | |
| Uporządkowane dokumentowanie wyników czynności i zadań podejmowanych w procesie rozwoju oprogramowania. Określenie osobnych zadań do wykonania dla sprawnego zarządzania dokumentacja projektu. | **Zadania do wykonania:**  - wytwarzanie i dokonywanie przeglądu dokumentacji projektu  - zapewnienie prawidłowego obiegu dokumentów wśród osób / zespołów biorących udział w projekcie  - zarządzanie przechowywaniem dokumentów projektu | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - n/d |

|  |  |  |
| --- | --- | --- |
| - **zarządzanie konfiguracją (configuration management)** | | |
| Zarządzanie poszczególnymi jednostkami i informacjami projektowymi z nimi powiązanymi, które tworzą strukturę systemu wbudowanego | **Zadania do wykonania:**  - zrozumienie celów zarzadzania konfiguracją  - tworzenie i wprowadzanie zmian do historii zarządzania zmianą konfiguracji | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - tabela zarządzania konfiguracją.  Potwierdzenie realizacji zadań w tym kroku mogą stanowić także obiekty zarządzania konfiguracją takie jak: wyniki działań wspierających zarządzanie konfiguracją, środowisko programistyczne, czy zintegrowany system |

|  |  |  |
| --- | --- | --- |
| - **zarządzanie rozwiązywaniem problemów (Problem Resolution Management)** | | |
| Omówienie różnych problemów i zagadnień związanych z rozwojem systemu wbudowanego. Zarządzanie i monitoring postępu implementacji wytworzonych rozwiązań do problemów. | **Zadania do wykonania:**  - rejestrowanie problemów i analiza przyczyn ich powstawania.  - analiza wpływu problemu na proces rozwoju systemu i opracowanie jego akceptowalnego rozwiązania  - implementacja akceptowalnego rozwiązania  - śledzenie skuteczności zaimplementowanego rozwiązania. Weryfikacja w jakim stopniu wdrożone rozwiązanie usunęło zidentyfikowany problem. | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - rejestr zarządzania incydentami  - rejestr zarzadzania problemami  Aktualizacja rejestrów wymaga wytworzenia nowej wersji dokumentu  - dokument zgłoszenia incydentu / problemu |

|  |  |  |
| --- | --- | --- |
| **- zarządzanie zmianami (Change Management)** | | |
| Zarządzanie zmianami które w trakcie procesu wytwórczego mogą pojawiać się zarówno w obszarze wymagań klienta jak i modelu wzorcowego na którym opiera się koncepcja projektowa tworzonego systemu wbudowanego. | **Zadania do wykonania:**  - rejestrowanie informacji o żądaniach wprowadzenia zmian  - analizowanie wpływu zmian na projekt systemu wbudowanego  - opracowanie i wykonanie planu zmian w projekcie  - przegląd rezultatów wprowadzonych zmian | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - rejestr zarządzania żądaniami zmian  -dokument zgłoszenia żądania wykonania zmiany |

|  |  |  |
| --- | --- | --- |
| - **wspólny przegląd (joint review)** | | |
| Dokonanie weryfikacji przy udziale interesariuszy stanu „dojrzałości” projektu. Potwierdzenie że postęp prac w poszczególnych punktach kontrolnych jest zadowalający zarówno w kontekście realizacji zadań technicznych jak i podejmowanych działań w związku z zarządzaniem projektem. | **Zadania do wykonania:**  - przygotowanie do przeglądu wykonanych zadań i stopnia ich zaawansowania  - przeprowadzenie przeglądu wykonanych zadań i omówienie aktualnie wykonywanych prac  - potwierdzenie właściwego rozumienia kwestii które wzbudzały wątpliwości interesariuszy w trakcie przeglądu | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - rejestr zadań przedstawiony do przeglądu klienta  - notatka ze spotkania z klientem |

|  |  |  |
| --- | --- | --- |
| **- zarządzanie podwykonawcami (Subcontractor Management)** | | |
| Zdefiniowanie zadań przeznaczonych do realizacji dla firm podwykonawczych | **Zadania do wykonania:**  - przygotowanie do składania zamówień i podpisywania umów  - monitorowanie realizacji zadań związanych z projektem zleconych podwykonawcom. | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - umowy podpisywanych z podwykonawcami  - rejestr zadań do realizacji dla podwykonawców |

|  |  |  |
| --- | --- | --- |
| **- Przygotowanie środowiska programistycznego (Preparation of Development Environment)** | | |
| Zbudowanie i utrzymanie środowisk, które stałyby się niezbędne do przeprowadzenia różnych etapów procesu projektowania. Rozpoczynając od projektowania, tworzenia modułów wykonywalnych, przez wdrożenie i prowadzenie testów systemu. | **Zadania do wykonania:**  - opracowanie planu przygotowania środowiska programistycznego  - zbudowanie środowiska programistycznego  - utrzymanie środowiska programistycznego | Dokumenty które powinny zostać wytworzone dla potwierdzenia realizacji zaplanowanych zadań:  - opis planu przygotowania środowisk deweloperskich  - postawione środowisko deweloperskie – jak obiekt wyjściowy potwierdzający realizacje opisywanego procesu |

Model V nie jest jedyną implementacją standardu Automotive SPICE jednakże w procesie wytwórczym systemu wbudowanego do obsługi modułu ABS jest dość powszechnie stosowany przez firmy które dostarczają ten komponent producentom samochodów osobowych[[34]](#endnote-34).

# Zarządzanie dowodami w safety case dla ABS [15+]

## Opis podejścia

## Klasyfikacja dowodów

## Zbiór dowodów dla ABS w cyklu życia

## Etapy zarządzania dowodami w rozwoju safety case

## Zarządzanie zmianami

# Analiza procesu [3-5]

## Skuteczność i kompletność podejścia

W przykładzie ABS nie znaleziono potrzeby stosowania dowodu który nie byłby ujęty w 3.5 i klasyfikacji 4.2

## Korzyści – wsparcie w zarządzaniu zakresem zmian

## Napotkane problemy i propozycje doskonalenia podejścia

## Skalowalność

## Ile zajęło to czasu – efektywność procesu – automatyczne/ręczne

# Podsumowanie [1-2 strony]

# Spis literatury

1. H.Dezfuli, A.Benjamin, Ch. Everett, C.Smith, M.Stamatelatos, R. Youngblood, "NASA system safety handbook", NASA Nov 2011 , s. 69 - 72 [↑](#endnote-ref-1)
2. „Safety Case Developement manual” s. 6 - 7 [↑](#endnote-ref-2)
3. D. Śmigielski., *System ABS. Co warto o nim wiedzieć?* <http://antymoto.com> (data dostępu: 30.10.2017) [↑](#endnote-ref-3)
4. Akademia Auto Świat, *Systemy elektroniczne ABS, ESP, ASR: poznaj alfabet bezpieczeństwa,* <http://akademia.autoswiat.pl> , (data dostępu 30.10.2017) [↑](#endnote-ref-4)
5. R. Właśniak, K. Zamiatowski *Agregat hudrauliczny Tevez MK II,* Rozdz. 2.1 *Opis ogólny*, praca dyplomowa pod kierunkiem mgr inż. I. Kulczyka, Zespół Szkół Samochodowych, Bydgoszcz 2000, (data dostępu: 30.10.2017) [↑](#endnote-ref-5)
6. ABS (motoryzacja) tekst dostępny w serwisie <https://pl.wikipedia.org>, pkt. 5 *System wspomagania nagłego hamowania ,* (data dostępu 30.10.2017) [↑](#endnote-ref-6)
7. *How effective is ABS at reducing crashes*, serwis internetowy <http://www.brainonboard.ca> , (data dostępu 30.10.2017) [↑](#endnote-ref-7)
8. ABS (Anti-Blockier-System, Anti-look Break System, Anti Bloking System), serwis internetowy <http://www.opony.com.pl/informacje/technologie> , (data dostępu: 30.10.2017) [↑](#endnote-ref-8)
9. Hamowanie awaryjne z ominięciem przeszkody bez systemu ABS, Serwis Internetowy miesięcznika Szkoła Jazdy, <http://www.szkola-jazdy.pl/> , (data dostępu: 30.10.2017) [↑](#endnote-ref-9)
10. L. Foltynowicz., G. Ślaski., J. Kupiec. *Układy przeciwblokujące a diagnostyka układów hamulcowych,* Instytut Maszyn Roboczych i Pojazdów Samochodowych, Politechnika Poznańska, 2001, s.2 [↑](#endnote-ref-10)
11. https://www.aaafoundation.org/faqs-anti-lock-braking-system-abs [↑](#endnote-ref-11)
12. Hamowanie z ABS-em to sztuka, Serwis internetowy Głosu Pomorza, <http://www.gp24.pl> , (data dostępu: 30.10.2017) [↑](#endnote-ref-12)
13. Kierowca lepszy niż ABS? Zapomnij, Serwis motoryzacyjny magazynów „Motor” i „Auto Moto”, <http://magazynauto.interia.pl>, (data dostępu: 30.10.2017) [↑](#endnote-ref-13)
14. Czujniki obrotów kół – do czego służą jak działają i jakie są objawy ich awarii?, Serwis motoryzacyjny Wp.pl, [http://autokult.pl](http://autokult.pl/25090), (data dostępu: 30.10.2017) [↑](#endnote-ref-14)
15. *Cztery sytuacje drogowe w których ABS może wydłużać drogę hamowania* , Serwis motoryzacyjny Interii oraz magazynów „Motor” i „Auto Moto”,<http://magazynauto.interia.pl> (data dostępu: 30.10.2017) [↑](#endnote-ref-15)
16. Kierowca lepszy niż ABS? Zapomnij, Serwis motoryzacyjny magazynów „Motor” i „Auto Moto”, <http://magazynauto.interia.pl>, (data dostępu: 30.10.2017) [↑](#endnote-ref-16)
17. Bosh: ABS – historia rewolucyjnego systemu, Serwis motoryzacyjny magazynu Auto – Swiat, [www.auto-swiat.pl](http://www.auto-swiat.pl) , (data dostępu 30.11.2017) [↑](#endnote-ref-17)
18. ABS (motoryzacja) tekst dostępny w serwisie <https://pl.wikipedia.org>, pkt. 6 *Historia ,* (data dostępu 30.10.2017) [↑](#endnote-ref-18)
19. Bosh: ABS – historia rewolucyjnego systemu, Serwis motoryzacyjny magazynu Auto – Swiat, [www.auto-swiat.pl](http://www.auto-swiat.pl) , (data dostępu 30.11.2017) [↑](#endnote-ref-19)
20. ABS (motoryzacja) tekst dostępny w serwisie <https://pl.wikipedia.org>, pkt. 6 *Historia ,* (data dostępu 30.10.2017) [↑](#endnote-ref-20)
21. Bosh: ABS – historia rewolucyjnego systemu, Serwis motoryzacyjny magazynu Auto – Swiat, [www.auto-swiat.pl](http://www.auto-swiat.pl) , (data dostępu 30.11.2017) [↑](#endnote-ref-21)
22. ABS (motoryzacja) tekst dostępny w serwisie <https://pl.wikipedia.org>, pkt. 6 *Historia ,* (data dostępu 30.10.2017) [↑](#endnote-ref-22)
23. R. Właśniak, K. Zamiatowski *Agregat hudrauliczny Tevez MK II,* Rozdz. 4.1 *Elektroniczny zespół sterujący*, praca dyplomowa pod kierunkiem mgr inż. I. Kulczyka, Zespół Szkół Samochodowych, Bydgoszcz 2000, (data dostępu: 30.10.2017) [↑](#endnote-ref-23)
24. J. Paszkowski *Diagnostyka układu hamulcowego ABS,* Instytut Maszyn Elektrycznych, Politechnika Warszawska, 2003, s. 20 - 22 [↑](#endnote-ref-24)
25. Czujnik ABS, Serwis internetowy, <https://www.hella.com> , (data dostępu: 30.10.2017) [↑](#endnote-ref-25)
26. Czujniki obrotów kół – do czego służą jak działają i jakie są objawy ich awarii?, Serwis motoryzacyjny Wp.pl, [http://autokult.pl](http://autokult.pl/25090), (data dostępu: 30.10.2017) [↑](#endnote-ref-26)
27. J. Paszkowsk *Diagnostyka układu hamulcowego ABS,* Instytut Maszyn Elektrycznych, Politechnika Warszawska, 2003, s. 17 - 19 [↑](#endnote-ref-27)
28. R. Właśniak, K. Zamiatowski *Agregat hudrauliczny Tevez MK II,* Rozdz. 3.1.1 *Pompa elektryczna*, praca dyplomowa pod kierunkiem mgr inż. I. Kulczyka, Zespół Szkół Samochodowych, Bydgoszcz 2000, (data dostępu: 30.10.2017) [↑](#endnote-ref-28)
29. J. Paszkowsk *Diagnostyka układu hamulcowego ABS,* Instytut Maszyn Elektrycznych, Politechnika Warszawska, 2003, s. 18 [↑](#endnote-ref-29)
30. R. Właśniak, K. Zamiatowski *Agregat hudrauliczny Tevez MK II,* Rozdz. 3.1.2 *Akumulator ciśnienia*, praca dyplomowa pod kierunkiem mgr inż. I. Kulczyka, Zespół Szkół Samochodowych, Bydgoszcz 2000, (data dostępu: 30.10.2017) [↑](#endnote-ref-30)
31. J. Paszkowsk *Diagnostyka układu hamulcowego ABS,* Instytut Maszyn Elektrycznych, Politechnika Warszawska, 2003, s. 19 [↑](#endnote-ref-31)
32. J. Mongiat, B. Lain, M. Marttin, T. Rateliff, H.S. Jung *Anti-Lock Breaking System Project – Requirements Analysis Document*, Serwis Internetowy <http://www.cse.msu.edu/~cse470/F01/Projects/ABS/ABS4/web/do-requirements/do-requirements.html> (data dostępu: 30.10.2017), [↑](#endnote-ref-32)
33. A. Bień, J. Rzeszutko, T. Szymański, *Systemy wbudowane do celów pomiarowo – kontrolnych w motoryzacji. Proces projektowania i wstępnej diagnostyki,* Akademia Górniczo – Hutnicza, Kraków, wyd. PAK vol 60 nr 8/2014, s. 655 - 656 [↑](#endnote-ref-33)
34. Espr , Embedded System development Process Reference guide, rozdz 2, Technical Section. Proces Definition Documnets, Software Engineering Center, Technology Headquarters, Information-technology Promotion Agency, Japan, 10.2012, s. 21 - 162 [↑](#endnote-ref-34)