**STRONA TYTUŁOWA PRACY DYPLOMOWEJ**

//do wydrukowania z MojaPG

„Proces zarządzania materiałem dowodowym w argumentacji wiarygodności systemów”

“Evidence management process in system assurance cases.”

**OŚWIADCZENIE AUTORA PRACY**

//do wydrukowania z MojaPG

**STRESZCZENIE**

Słowa kluczowe:

**ABSTRACT**

Keywords:

SPIS TREŚCI

[WYKAZ WAŻNIEJSZYCH SKRÓTÓW I OZNACZEŃ 6](#_Toc523956397)

[1. WSTĘP I CEL PRACY 8](#_Toc523956398)

[2. BEZPIECZEŃSTWO SYSTEMÓW STEROWANIA 9](#_Toc523956399)

[*2.1* *Podstawowe pojęcia bezpieczeństwa systemów sterowania* 9](#_Toc523956400)

[*2.2* *Assurance case – definicja i struktura* 11](#_Toc523956401)

[*2.3* *Wnioskowanie o bezpieczeństwie w cyklu życia systemu* 16](#_Toc523956402)

[*2.4* *Stosowanie dowodów w safety case* 16](#_Toc523956403)

[3. SYSTEM ABS W SAMOCHODACH OSOBOWYCH 17](#_Toc523956404)

[*3.1* *Charakterystyka systemu* 17](#_Toc523956405)

[*3.2* *Budowa i działanie* 20](#_Toc523956406)

[*3.2.1* *Obwód elektroniczny* 21](#_Toc523956407)

[*3.2.2* *Obwód hydrauliczny* 22](#_Toc523956408)

[*3.3* *Wymagania* 26](#_Toc523956409)

[*3.4* *Analiza bezpieczeństwa* 28](#_Toc523956410)

[*3.5* *Proces wytwórczy ABS* 36](#_Toc523956411)

[4. ZARZĄDZANIE DOWODAMI W SAFETY CASE DLA ABS 56](#_Toc523956412)

[*4.1* *Opis podejścia* 56](#_Toc523956413)

[*4.2* *Klasyfikacja dowodów* 56](#_Toc523956414)

[*4.3* *Zbiór dowodów dla ABS w cyklu życia* 56](#_Toc523956415)

[*4.4* *Etapy zarzadzania dowodami w rozwoju safety case* 56](#_Toc523956416)

[*4.5* *Zarządzanie zmianami* 56](#_Toc523956417)

[5. Analiza procesu 57](#_Toc523956418)

[*5.1* *Skuteczność i kompletność podejścia* 57](#_Toc523956419)

[*5.2* *Korzyści – wsparcie w zarządzaniu zakresem zmian* 57](#_Toc523956420)

[*5.3* *Napotkane problemy i propozycje doskonalenia podejścia* 57](#_Toc523956421)

[*5.4* *Skalowalność* 57](#_Toc523956422)

[*5.5* *‘Ile zajęło to czasu – efektywność procesu – automatyczne / ręczne* 57](#_Toc523956423)

[6. Podsumowanie 58](#_Toc523956424)

[WYKAZ LITERATURY 59](#_Toc523956425)

[WYKAZ RYSUNKÓW 64](#_Toc523956426)

[WYKAZ TABEL 66](#_Toc523956427)

# WYKAZ WAŻNIEJSZYCH SKRÓTÓW I OZNACZEŃ

AC – Assurance Case

SC – Safety Case

SPICE - Software Process Improvement Capability Etermination

SIG – Sepcial Interest Group

EUROCONTROL – European Organization for the Safety of Air Navigation

ASIL – Automotive Safety Integrity Level

FTA – Fault tree analysis

FMEA - Failure Mode and Effects Analysis

PHA - Preliminary Hazard Analysis

RWAL - Real Wheel Anti Lock Controller

# WSTĘP I CEL PRACY

Celem dyplomu jest analiza procesu zarządzania argumentacją wiarygodności (assurance case) i opracowanie modelu zarządzania materiałem dowodowym (evidence management) w cyklu życia systemu. Wymagania na proces obejmują między innymi zarządzanie zakresem, klasyfikacją, statusem oraz zmianami. Opracowany proces będzie podlegał walidacji poprzez analizę scenariuszy zdefiniowanych dla wymagań.

# BEZPIECZEŃSTWO SYSTEMÓW STEROWANIA

## *Podstawowe pojęcia bezpieczeństwa systemów sterowania*

Bezpieczeństwo to ograniczenie do akceptowalnego poziomu ryzyka wystąpienia zagrożeń, które mogą spowodować śmierć, zranienie, chorobę zawodową, uszkodzenie lub utratę sprzętu, mienia lub szkody dla środowiska. W każdym konkretnym przypadku dokładny poziom i zakres bezpieczeństwa musi być jasno określony przez interesariuszy projektu. Ważne jest także zdefiniowanie konsekwencji wystąpienia potencjalnych zagrożeń i ich wpływ na projekt [1]. Oprócz definicji bezpieczeństwa, zrozumienie zagadnień poruszanych w dyplomie, potencjalnie niezorientowanemu odbiorcy, potrzebny jest jeszcze wykaz pojęć związanych z bezpieczeństwem systemów sterowania. Najważniejsze z tych pojęć to:

Tabela 2.1 Bezpieczeństwo systemów sterowania - pojęcia podstawowe

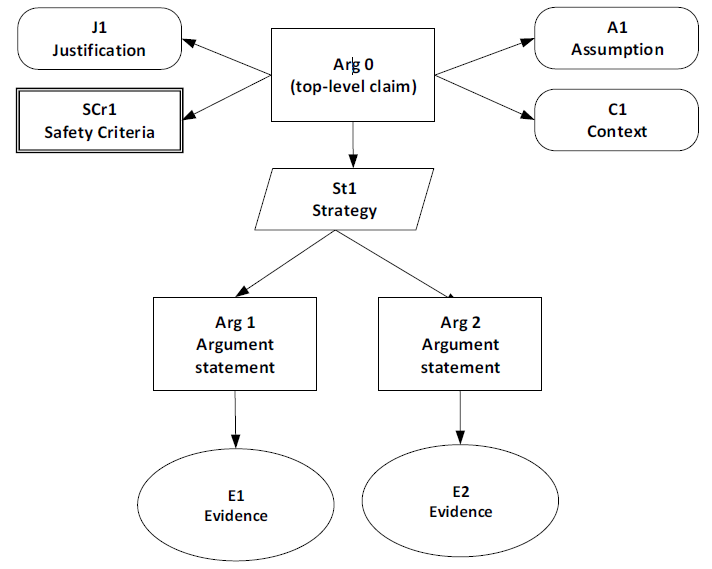
|  |  |
| --- | --- |
| ControllabiltyClassKind | klasa zawierająca numeryczne literały wskazujące na atrybuty sterowania: C0 – ogólnie sterowny, C1 – sterowanie proste, C2 – sterowanie zwykłe, C3 – utrudniona kontrola sterowania lub zupełny jej brak |
| DevelopmentCategoryKind | spis numerycznych literałów które wskazują, czy przedmiot jest modyfikacją istniejącego produktu, czy też jest to zupełnie nowa wersja. Dostępne literały to: modificationOfExistingItem, newItemDevelopment |
| ExposureClassKind | klasa zawierająca numeryczne literały wskazujące na atrybuty prawdopodobieństwa. Literały dostępne w tej klasie to E1 – rzadkie zdarzenia, występujące nie częściej niż raz w roku, ale dotyczą większości kierowców, E2 – czasami. Zdarzenia występujące kilka razy w roku, dotyczą większości kierowców, E3 – dość często. Sytuacje powtarzające się raz w miesiącu lub częściej dla w przypadku przeciętnego kierowcy, E4 – często, wszystkie sytuacje występujące średnio podczas każdej jazdy |
| FunctionalSafetyConcept | kontener, który agreguje funkcjonalne wymagania bezpieczeństwa przypisane do elementów architektury, które razem tworzą funkcjonalną koncepcję bezpieczeństwa, |
| FunctionPort | port używany do przechowywania zmiennych służących do zapewnienia interakcji komponentów |
| FunctionPrototype | reprezentuje odniesienie do wystąpienia „FunctionType” |
| FunctionType | klasa abstrakcyjna która zawiera definicje typów komponentów funkcji, które są używane do modelowania struktury funkcjonalnej. Składania FunctionTypes została zainspirowana koncepcją bloków z SysML |
| Ground | reprezentuje stwierdzenie które określa w jaki sposób dowody w SafetyCase wyjaśniają postulat |
| HardwareComponentType | reprezentuje element sprzętowy na poziomie abstrakcyjnym umożliwiając wstępne działania inżynieryjne związane ze sprzętem |
| HardwarePin | reprezentuje elektryczne punkty połączeń w architekturze sprzętowej. Zależnie od stylu modelowania architektury można rozważyć użycie rzeczywistego przewodu lub połączenie logiczne |
| Hazard | klasa reprezentująca warunek lub stan w systemie, który może być przyczyną wypadków. Zagrożenie jest spowodowane nieprawidłowym działaniem systemów bezpieczeństwa. Zagrożenie nie odnosi się bezpośrednio do zdarzeń takich jak: porażenie prądem, pożar, dym, ciepło, promieniowanie, toksyczność, palność, reaktywność, korozja, chyba że są one bezpośrednio spowodowane nieprawidłowym działaniem systemów elektrycznych i elektronicznych związanych z bezpieczeństwem |
| HazardousEvent | klasa reprezentująca połączenie poziomu ryzyka i określonej sytuacji charakteryzującej się trybem działania i sytuacją operacyjną dla określonego zastosowania systemu i środowiska |
| InternalFaultPrototype | używany do deklarowania błędów wewnętrznych komponentów w Modelu Błedu |
| Item | identyfikuje zakres informacji dotyczących oceny bezpieczeństwa |
| LifecycleStageKind | służy do definiowania etapu cyklu życia systemu dla określonego Safety Case |
| Mode | służy do reprezentowania „trybu pracy” włączając w to stan: bezpieczny (*safe*), |
| OperationalSituation | jest to stan, warunek lub scenariusz, w środowisku który może mieć wpływ na pojazd |
| ProcessFaultPrototype | używany do reprezentowania błędów procesu w komponentach Modelu Błędu. Pozwala to na deklarację wymaganego rygoru rozwojowego w kategoriach ASIL poprzez ograniczenie bezpieczeństwa |
| QuantitativeSafetyConstraint | służy do definiowania wskaźnika awarii, |
| Rationale | używany do deklaracji „uzasadnienia” w Safety Case, |
| Requirement | używany do prezentacji wymagań funkcjonalnych, technicznych, dotyczących sprzętu lub oprogramowania, |
| RequirementsContainer | służy do ułożenia wymagań w zorganizowaną strukturę |
| RequirementsRelationship | używany do reprezentowania powiązań pomiędzy wymaganiami, |
| SafetyCase | używany do prezentacji logicznie ułożonej argumentacji stanowiącej dowód, że system jest bezpieczny |
| SafetyConstraint | służy do zdefiniowania poziomu ASIL dla określonego błędu lub awarii |
| SafetyGoal | reprezentuje wymaganie bezpieczeństwa. Wskazuje w jaki sposób unikać powiązanego z nimi zagrożenia lub obniżać ryzyko wystąpienia zagrożenia do akceptowalnego poziomu |
| SystemModel | służy do organizowania modeli / architektur zgodnie z ich poziomem abstrakcji, może również utrzymywać relacje między różnymi poziomami |
| TechnicalSafetyConcept | kontener grupujący techniczne wymagania bezpieczeństwa przypisane do elementów architektury, które razem tworzą techniczną koncepcję bezpieczeństwa, |
| UseCase | używany w roli „Sytuacja Operacyjna” dla zdarzenia niebezpiecznego, |
| Warrant | reprezentuje „uzasadnienie” w Safety Case, |
| VehicleFeature | zestaw elementów pojazdu realizowanych za pomocą elementów architektury [2] |

## *Assurance case – definicja i struktura*

Głównym powodem stosowania *Assurance Case (AC)* jest konieczność potwierdzenia osiągnięcia celu lub celów, które często w terminologii, określa się jako postulaty najwyższego poziomu (*top-level claims*). *Assurance Case* jest reprezentowane w formie struktury złożonej z wielu poziomów argumentów, popartych dowodami (*evidence*) i określonymi założeniami (assumptions). Odpowiednie połączenie elementów struktury ma na celu graficzne zaprezentowanie logicznego wnioskowania o prawdziwości tezy zawartej w postulacie najwyższego poziomu, którego prawdziwość należy wykazać. AC opiera się na koncepcji systemu, który ma być wytworzony i wymaganiach przed nim stawianych. Dowody potrzebne do zapewnienia wiarygodności wskazanych argumentów mogą zatem pochodzić z artefaktów (produktów roboczych) procesu wytwarzania systemu. Zalicza się do nich m.in wytworzone analizy, używane standardy, uzyskane wyniki (np.: raporty testów), dokumenty przeglądów projektu itp.

Dekompozycja postulatu najwyższego poziomu, na poszczególne, hierarchicznie ułożone elementy niższego poziomu, pokazuje zależności pomiędzy postulatem a powiązanym materiałem dowodowym.

Rys. 2.1 prezentuje przykładowy Assurance Case zdefiniowany wg. Europejskiej Organizacji ds. Bezpieczeństwa Żeglugi Powietrznej (EUROCONTROL).



Rys. 2.1 Schemat postulatu najwyższego poziomu z powiązanymi argumentami

Każdy element Assurance Case powinien spełniać następujące wymagania:

* być jednym z dostępnych typów,
* zawierać unikalny identyfikator, posiadać określony numer w hierarchii elementów zgodny z logiczną strukturą Assurance Case. Ma to na celu ułatwienie przeprowadzania procesu wnioskowania we właściwej kolejności, dzięki uporządkowanej argumentacji,
* zwierać jednoznaczny komunikat tekstowy w celu prostej identyfikacji typu elementu w strukturze [3].

Podstawowe elementy w strukturze Asssurance Case to:

* Postulat (*claim*) – argument położony najwyżej w strukturze AC, twierdzenie dotyczące charakterystyki, właściwość lub zachowania oprogramowania lub systemu, które da się ocenić, że jest prawdziwe lub fałszywe za pomocą połączonych z nim argumentów umiejscowionych niżej, opierających się na obiektywnych dowodach [4].

Argument będący postulatem w strukturze AC powinien przedstawiać następujące informacje

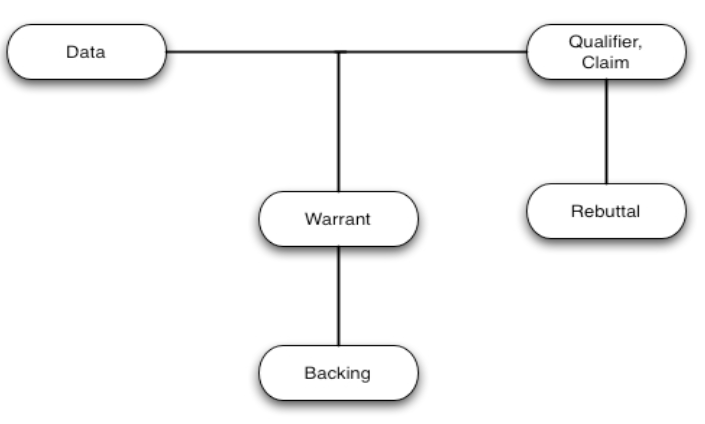
* + własności postulatu (wymagane),
  + zakres własności powiązanych z postulatem (wymagane),
  + zakres niepewności (margines błędu) co do własności związanych z postulatem (wymagane),
  + czas, w którym postulat może być stosowany (opcjonalne),
  + niepewność związana z czasem „stosowalności” postulatu (opcjonalne),
  + warunki, których spełnienie umożliwia stosowanie podanego postulatu (wymagane),
  + niepewność związana z zastosowaniem warunków umożliwiających stosowanie postulatu (opcjonalne),
  + jeżeli określona własność podana w postulacie dotyczy pewnego podzbioru systemów lub produktów lub ich elementów składowych, wymagana, pod określonymi warunkami, jest ich identyfikacja przez podanie wersji ich wystąpienia (wymagane warunkowo),
  + konsekwencje lub zagrożenia mające znaczenie dla całości twierdzenia o którym mowa w postulacie (wymagane warunkowo).
* Argument (*argument*) – element ten służy do pokazania w jaki sposób wspierające go dowody odnoszą się do postulatu, którego prawdziwość ma zostać wykazana. Argument jest szczególnie użyteczny, jeśli ma postać technicznych obliczeń lub logicznego wnioskowania, a nie charakteru dowodu.

Argument ma następujące cechy:

* + argument jest określany w sposób bezpośrednio nawiązujący do elementów z nim związanych, znajdujących się w strukturze AC pod nim,
  + argument powinien prowadzić do wniosków które odnoszą się do każdego postulatu które popiera,
  + argument określa niepewność każdego wniosku, do którego się odnosi,
  + argument zawiera informacje niezbędne do ustalenia jego wpływu na niepewność wniosku, do którego się odnosi [5].

Brytyjski filozof Stephen Toulmin zauważył, że dobry, realistyczny argument składa się z sześciu części:

* dane (*data*) – fakty lub dowody potrzebne do udowodnienia prawdziwości argumentu,
* postulat (*claim*) – twierdzenie które ma zostać uargumentowane,
* uzasadnienia (*warrants*) – ogólne, hipotetycznie (często domniemane) logiczne stwierdzenia, które łączą postulat z danymi (fakty + zebrane dowody)
* kwalifikatory (*qualifiers*) – twierdzenia, przedstawiające warunki, dla których argument jest prawdziwy
* kontrargumenty (*rebuttals*) – stwierdzenia które wskazują na okoliczności, w których argument nie jest prawdziwy
* wsparcie (*backing*) – stwierdzenia, które pomagają uznać podane uzasadnienia jako prawdziwe



Rys. 2.2 Model Argumentacji wg. Stephena Toulmina

Model argumentacji Toulmina (prezentowany na rysunku 2.2) ujawnia mocne strony oraz granice argumentacji. Głównym celem, jak wskazuje twórca modelu, nie jest zaprzeczenie wszystkim użytym kontrargumentom, lecz możliwe najbardziej wiarygodne wykazanie prawdziwości tezy postawionej w postulacie. Filozof wskazywał, że argumenty są wyrażone bardziej jako zestaw warunków określających, kiedy argument jest prawdziwy lub fałszywy, niż potwierdzone „absoluty”. Dzięki temu odbiorca może lepiej zrozumieć proces wnioskowania, ponieważ wie jaki jest zakres zastosowanych argumentów [6].

* Dowód (*evidence*) - reprezentuje informacje dotyczące systemu lub środowiska, w którym on funkcjonuje. Dowody można podzielić na dwa typy: proste, bezpośrednie – reprezentujące konkretną własność systemu oraz wspierające – dostarczające zapewnienie wiarygodności dowodów bezpośrednich.

Dowody traktowane są jako przesłanki określające, że argument z nimi powiązany jest prawdą, a więc jest wiarygodny w ogólnym procesie wnioskowania. Wszystkie informacje podawane w dowodach muszą dotyczyć wyłącznie systemu, którego cechy są poddawane pod wnioskowanie. Jeśli którykolwiek z dowodów zawiera błąd, wszystkie argumenty z nim powiązane mogą zostać uznane za błędne [7].

Dowody zarówno wspierające jak i bezpośrednie mogą pochodzić z:

* + doświadczeń związanych z systemami wytworzonym wcześniej – przydatne będą tu wszystkie wytworzone wcześniej analizy działającego systemu wytworzonego w przeszłości (źródło dowodów bezpośrednich). Istotne będzie także uzyskanie zapewnienia, że nie ma żadnych znaczących zmian pomiędzy konfiguracją poprzedniego i obecnego środowiska wytwórczego (źródło dla dowodów wspierających)
  + weryfikacji i walidacji – pozyskane dowody bezpośrednie mogą pochodzić z zapewnienia, że proces projektowania i wdrażania systemu w przeszłości był przeprowadzony prawidłowo a sam system działa zgodnie z przeznaczeniem i spełnia wymagania przed nim stawiane.
  + zgodności z normami – pozyskane dowody bezpośrednie są traktowane jako zapewnienie, że wcześniej wytworzony system był zgodny z przyjętymi standardami. Dowody wspierające, mogą być natomiast zdefiniowane w formie opisu procesu potwierdzania zgodności produktu.

Poprawnie sformułowany dowód powinien zawierać:

* + definicje,
  + zakres zastosowania,
  + Niepewność związana ze źródłem jego pochodzenia oraz dokładność pomiaru, jeśli dowód opiera się o dane liczbowe lub wyliczenia [8].

Dodatkowe elementy powiązane ze strukturą Assurance Case to:

* kryteria (*criteria*) – element definiuje pewien punkt widzenia, który wyjaśnia co rozumie się pod pojęciem cechy systemu, wskazanej w postulacie, której wiarygodność należy wykazać w procesie wnioskowania. Np. że system jest bezpieczny. Wyróżnia się trzy typy kryteriów:
  + bezwzględne (*absolute*) – odnosi się do standardowego lub ustalonego zestawu procedur,
  + względne (*relative*) – odnosi się do poziomu wiarygodności jaki zapewnia „poprzedni” system,
  + redukcyjne (*reductive*) – odnosi się do poziomu wiarygodności zapewnionego przez regułę ALARP.
* uzasadnienia (*justifications*) – element zawiera wyjaśnienie przyczyny wytworzenia lub zmiany systemu, jest bezpośrednio połączony z postulatem najwyższego poziomu,
* startegia (*strategy*) – element opisuje sposób dekompozycji argumentacji, może być połączony z postulatem najwyższego poziomu lub jednym z argumentów,
* założenia (assumptions) – element, który może być traktowany jako dowód. Nie podano informacji dotyczącej ważności tego elementu. W strukturze AC może być połączony z argumentem, strategią lub dowodem.

Praca dyplomowa dotyczyć będzie dowodzenia o bezpieczeństwie systemów. Przeprowadzenie logicznego wnioskowania o bezpieczeństwie nie byłoby możliwe bez wytworzenia Safety Case (SC). Jest to szczególny przypadek wykorzystania narzędzia Assurance Case, w którym postulat najwyższego poziomu, podlegający udowodnieniu, zawiera twierdzenie, że system jest bezpieczny w określonym kontekście użycia. Wytworzenie SC jest wymagane w celu uzyskania certyfikacji bezpieczeństwa systemów, których awaria może spowodować utratę życia, obrażenia lub szkody dla środowiska [9].

Decyzja o wytworzeniu Safety Case może być motywowana czynnikami takim jak konieczność upewnienia się, że wypuszczany na rynek produkt jest odpowiedniej jakości lub też celem może być pozyskanie certyfikatu jakości produktu od zewnętrznej instytucji.

Proces tworzenia argumentacji determinuje dokładne zbadanie kwestii np. bezpieczeństwa już na wczesnym etapie projektu. Oceny wymagają także rezultaty i skuteczność działań podjętych w celu minimalizowania ryzyka wystąpienia zagrożeń. Pozwala to uniknąć części kosztów potencjalnych awarii. Stworzenie ustrukturyzowanej argumentacji, dzięki której możemy bezsprzecznie wykazać konkretną cechę systemu np. bezpieczeństwo pozwala na łatwiejszą ocenę wpływu potencjalnych zmian na poziom bezpieczeństwa systemu. Jest to pomocne do wybrania konkretnej strategii rozwoju istniejącego systemu lub też przy gromadzeniu dowodów do argumentacji bezpieczeństwa nowych systemów, których wytworzenie jest planowane [10].

## *Wnioskowanie o bezpieczeństwie w cyklu życia systemu*

## *Stosowanie dowodów w safety case*

# SYSTEM ABS W SAMOCHODACH OSOBOWYCH

## *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 [11]. 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 [12]. Głównym zadaniami systemu ABS są:

* zapobieganie blokowaniu kół, w przypadku konieczności wykonania nagłego manewru hamowania, spowodowanego niebezpieczną sytuacja na drodze,
* wspomaganie działania hamulców, poprzez możliwość precyzyjnej symulacji hamownia „pulsacyjnego” [13].

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. 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 [14].

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 [15].

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 [16]. Na rysunku 2.1 zaprezentowane drogę hamowania pojazdu bez ABS oraz przy użyciu systemu.



Rys. 3.1 Droga hamowania pojazdu bez / z ABS

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 [17].

Jakkolwiek ABS to system elektroniczny, włączający się samoczynnie podczas hamowania, to jednak kierowca ma kluczowy wpływ na efektywność jego pracy. 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 [18]. Coraz trudniej znaleźć na drodze samochody niewyposażone fabrycznie w system ABS. To dobra informacja dla bezpieczeństwa kierowców.

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”. Na rysunku 3.2 przedstawiono długość drogi hamowania ze 100 km/h na suchej nawierzchni samochodu wyposażonego w ABS a także bez tego systemu, gdy za kierownicą siedzi „typowy” kierowca lub kierowca testowy [19].



Rys. 3.2 Droga hamowania ze 100 km/h na suchej nawierzchni

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 [20].



Rys. 3.3 Droga hamowania ze 100 km/h na mokrej nawierzchni

Porównanie długości drogi hamowania samochodu na mokrej nawierzchni w różnych przypadkach prezentuje rysunek 3.3. Bez systemu ABS samochód prowadzony przez typowego kierowcę przejechał prawie dwa razy dłuższy dystans niż pojazd z tym systemem. W chwili, gdy pojazd z 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 [21].

## *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.

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 [22].

Polska również wniosła pewien wkład w rozwój układu ABS. Na początku lat osiemdziesiątych w warszawskiej Fabryce Samochodów Osobowych (FSO) powstał Hamulcowy Układ Antypoślizgowy (HUAP), Układ ten uważa się za prototyp polskiego układu przeciwblokującego koła samochodu podczas hamowania [23].

Standardowy układ ABS można podzielić na obwód elektroniczny i hydrauliczny.

### *Obwód elektroniczny*

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 [24].

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 [25].

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

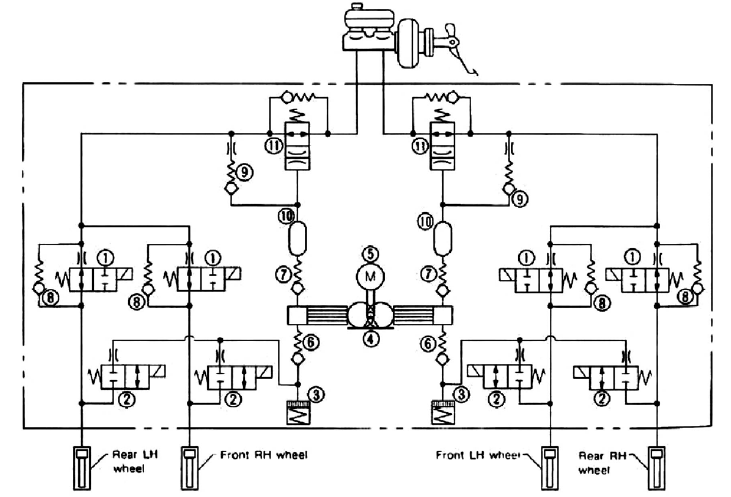
* czujniki pasywne,
* czujniki aktywne [26].

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 [27].

### *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.



Rys. 3.4 Schemat obwodu hydraulicznego w układzie ABS

Na rysunku 3.4 przedstawiono schemat układu hydraulicznego będący częścią układu ABS. Schemat ten składa się następujących elementów składowych:

1 – elektrozawory jednokierunkowe wlotowe (zwiększające ciśnienie płynu hamulcowego w układzie), 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 zaworów wlotowych i 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 - 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,
* faza utrzymania stałej wartości ciśnienia - 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,
* faza zmniejszania ciśnienia - 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.

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 [28].

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 [29]. 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 [30].

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 [31].

Akumulatory ciśnienia dostosowują swoją pracę do faz pracy elektrozaworów wylotowych i dolotowych Magazynują niewielkiej 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 [32].

## *Wymagania*

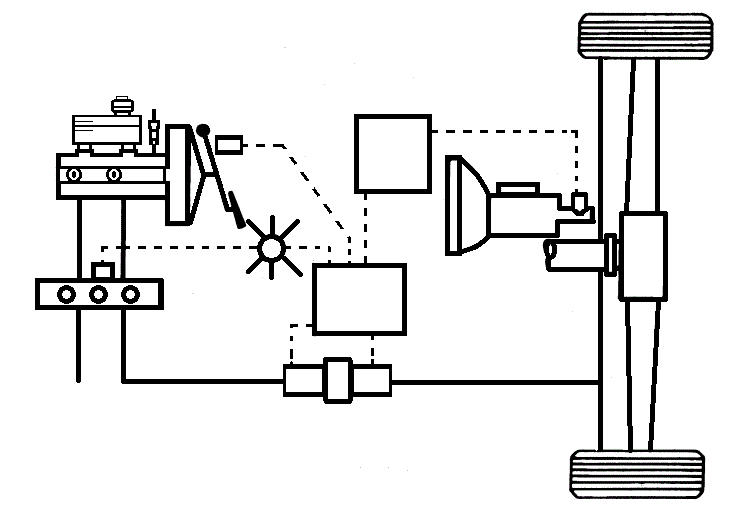
Elektroniczne systemy wsparcia kierowcy mają za zadanie podnieść poziom jego bezpieczeństwa, w nagłych i nie przewidzianych sytuacjach na drodze. ABS jako system wspierający działanie układu hamulcowego, który jest kluczowym układem pojazdu samochodowego, musi być systemem bezpiecznym. Oznacza to, że usterka systemu ABS, nie może być równoznaczna, z awarią działania układu hamulcowego, a więc 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 [33].

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*).

Ponieważ w kolejnym podrozdziale przedstawiona zostanie analiza bezpieczeństwa systemu ABS warto już teraz zapoznać się z najważniejszymi komponentami tego systemu. Przykładowy schemat systemu przeciwblokującego koła podczas hamowania dla tylnej osi przedstawiono na rysunku 3.5.



**14**

**MAX**

**MIN**

**13**

**12**

**11**

**10**

**9**

**8**

**3**

**2**

**7**

**6**

**5**

**4**

**1**

Rys. 3.5 Komponenty układu hamulcowego z systemem ABS kół tylnych

Podstawowe elementy układu ABS to: 1 – cylinder główny, 2 – zbiornik płynu hamulcowego,

3 – zawór zwrotny, 4 – włącznik świateł STOP, 5 - zestaw wskaźników, 6 – czujnik prędkości kół tylnych, 7 – przekaźnik, 8 – RWAL – sterownik systemu przeciwblokującego kół tylnych [34], 9,10 – system zaworów elektromagnetycznych składający się m.in z: zaworu odcinającego – zazwyczaj otwartego, używanego do utrzymania stałego ciśnienia płynu hamulcowego w układzie podczas akcji przeciw blokowania kół, zaworu zrzutowego – zazwyczaj zamkniętego, używanego do odprowadzania nadmiaru płynu hamulcowego i w konsekwencji obniżenie ciśnienia w układzie [35], 11 – kontrolka ostrzegawcza hamulców, 12 – urządzenie wzmacniające siłę hamowania (tzw. serwo), 13 – zawór kombinowany, 14 – pedał hamulca [36].

## *Analiza bezpieczeństwa*

Automotive Spice, to jeden ze standardów, który jest stosowany w procesie wytwarzania systemów przeznaczonych dla sektora motoryzacyjnego. Standard ten jest wspólnym językiem komunikacji zrozumiałym zarówno przez klienta (np.: producenta samochodów) jak i dostawcę systemów (np.: firmę Bosch, dostawcę m.in. systemu ABS). Dostawca powinien wykazać, że wytworzony przez niego system jest bezpieczny. Dostarczenie takiego zapewnienia wymaga m.in. identyfikacji zagrożeń, analizy ryzyka ich wystąpienia oraz oszacowania ich konsekwencji dla bezpieczeństwa systemu. Odwołam się do wspomnianego wyżej standardu, ponieważ przewiduje on implementację procesu MAN.5. Proces ten obliguje dostawcę m.in do analizy ryzyka w tym określenia priorytetów i zasobów potrzebnych do jego minimalizowania. Dowodem pomyślnej implementacji tego procesu w cyklu wytwórczym systemu, jest wytworzona dokumentacja robocza. Dzięki niej producent ma pewność, że zagrożenia zostały należycie zidentyfikowane a ryzyko ich wystąpienia odpowiednio przeanalizowane i zarządzane w czasie trwania procesu wytwarzania systemu.

Zagrożenia analizowane są pod kątem prawdopodobieństwa pojawienia się oraz konsekwencji nimi spowodowanych. Aby zrozumieć, czy istnieje ryzyko wykorzystuje się różne techniki m.in.: analizę funkcjonalną, symulację, analizę trybu i skutków awarii (FMEA) oraz analizę drzewa usterek (FTA) [37].

Ważne pojęcia wymagane do zrozumienia zagadnienia analizy bezpieczeństwa:

* zagrożenie (*hazard*) - niepożądana sytuacja, która może wyrządzić szkodę, spowodować straty materialne lub prowadzić do innych nieprzewidzianych zdarzeń.
* ryzyko (*risk*) - prawdopodobieństwo wystąpienia zagrożenia i powiązanych z nim konsekwencji,
* ocena ryzyka (*risk assessment*) - proces, w którym identyfikuje się zagrożenia dla określonego cyklu ograniczonego w czasie. Celem analizy ryzyka jest określenia odpowiednich sposobów eliminowania lub kontrolowania wspomnianych zagrożeń. Poziom ryzyka można określić wg przyjętej skali prawdopodobieństwa i skali wymiaru konsekwencji. W ten sposób tworzy się tzw. macierz ryzyka, która ma na celu pomóc w ustaleniu priorytetów zagrożeń, wymagających podjęcia natychmiastowych działań zmierzających do obniżenia poziomu prawdopodobieństwa ich powstania [38].

Realizacja dyplomu zakłada, że wykazywanie bezpieczeństwa dotyczyć będzie systemu ABS. Dlatego w tym podrozdziale zostanie zaprezentowana analiza bezpieczeństwa wspomnianego systemu. Jednym z narzędzi pozwalających na przenalizowanie ryzyka zagrożeń jakie mogą się pojawić w systemie ABS jest wspomniane wyżej drzewo usterek (FTA).

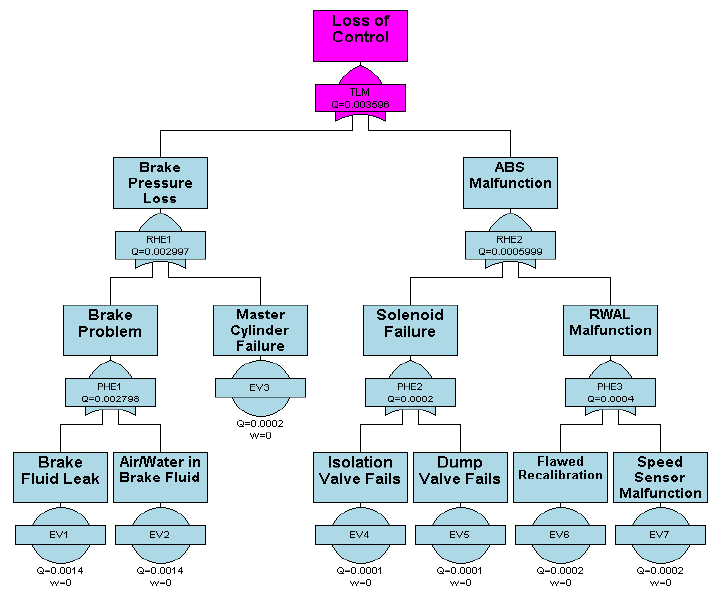
Ogólnie rzecz ujmując jakkolwiek ABS jest systemem znacznie podnoszącym bezpieczeństwo jazdy samochodem, to zmaga się z wieloma problemami które mogą się pojawić podczas okresu jego eksploatacji. Problemy te może nie powodują konieczności całkowitego zatrzymania pojazdu, ale obniżenie poziomu bezpieczeństwa powinno skłonić świadomego kierowcę do bezzwłocznego złożenia wizyty w warsztacie naprawczym.

Dostawcy systemów ABS już na etapie wytwórczym podejmują działania mające poprawić bezpieczeństwo systemu. Jednym z takich działań jest implementacja procedur dzięki którym autodiagnostyka systemu jest zdolna do przechowywania wyłącznie jednego kodu błędu. Wykrycie awarii usterki powoduje zapalnie się kontrolki ostrzegawczej „ABS” na desce rozdzielczej kierowcy. System ABS zostaje wyłączony i nie jest możliwe jego ponowne uruchomienie bez interwencji diagnosty. Kontrolka ostrzegawcza może być współdzielona z innymi elementami układu hamulcowego i zależnie od sytuacji informować kierowcę np. o awarii układu hydraulicznego lub włączeniu hamulca postojowego. Procedura autodiagnostyczna nie obejmuje wszystkich potencjalnych „ścieżek uszkodzeń” dlatego konieczna jest bardziej wszechstronna analiza. Dobrym punktem wyjścia do oceny wiarygodności jest wstępna analiza zagrożeń (PHA), identyfikująca scenariusze, w których mogą wystąpić warunki niebezpieczne. Scenariusze te obejmują zdarzenia związane z wewnętrzną konstrukcją systemu, jak również zewnętrznymi czynnikami środowiskowymi. Niezależnie od źródła pochodzenia zdarzenia mogą zahamować lub pogorszyć działanie systemu. W tabeli 3.1 zaprezentowano zidentyfikowane zagrożenia ich efekt, który może ostatecznie prowadzić do wypadku spowodowanego utratą kontroli na pojazdem podczas hamowania.

Tabela 3.1 Wstępna Analiza Zagrożeń (PHA) dotycząca systemu ABS

| Zdarzenie niebezpieczne | Podstawowy Efekt zdarzenia | Rezultat zdarzenia | Zdarzenie losowe |
| --- | --- | --- | --- |
| Wyciek płynu hamulcowego | Problem z hamulcami. Niski poziom efektywności hamowania | Utrata ciśnienia w układzie hamulcowym | Utrata kontroli nad pojazdem |
| Woda lub powietrze w płynie hamulcowym | Problem z hamulcami. Niski poziom efektywności hamowania | Utrata ciśnienia w układzie hamulcowym | Utrata kontroli nad pojazdem |
| Uszkodzenie cylindra głównego | Utrata ciśnienia w układzie hamulcowym | Utrata ciśnienia w układzie hamulcowym | Utrata kontroli nad pojazdem |
| Zawór odcinający  zapewniający stałe ciśnienie płynu hamulcowego w układzie podczas akcji przeciw blokowania kół - nie działa | Usterka solenoidu - cewki powietrznej służącej do wytwarzania jednorodnego pola elektromagnetycznego | Wadliwe działanie układu ABS | Utrata kontroli nad pojazdem |
| Zawór zrzutowy  odprowadzający nadmiar płynu hamulcowego w układzie – nie działa | Usterka solenoidu -cewki powietrznej służącej do wytwarzania jednorodnego pola elektromagnetycznego | Wadliwe działanie układu ABS | Utrata kontroli nad pojazdem |
| Nieprawidłowa kalibracja (uszkodzenie) modułu sterującego ABS (np. po wymianie czujnika prędkości) | Wadliwe działanie kontrolera sterującego - RWAL | Wadliwe działanie układu ABS | Utrata kontroli nad pojazdem |
| Wadliwe działanie czujnika prędkości (przegrzanie, zalepienie solą lub błotem drogowym, korozja) | Wadliwe działanie kontrolera sterującego – RWAL w skutek otrzymywania błędnych danych pomiarowych | Wadliwe działanie układu ABS | Utrata kontroli nad pojazdem [39] |
| Zawór zwrotny zapewniający przepływ płynu hamulcowego w jednym kierunku - nie działa | „Twardy” pedał hamulca, który w razie konieczności nie daje możliwości użycia hamulców | Utrata możliwości użycia układu hamulcowego w celu zatrzymania | Utrata kontroli nad pojazdem [40] |
| Mechaniczne uszkodzenie okablowania czujnika pomiaru prędkości | Wadliwe działanie kontrolera sterującego – RWAL Kontroler działa na niepełnych danych | Wadliwe działanie układu ABS | Utrata kontroli nad pojazdem |
| Nieprawidłowy montaż lub wybór niewłaściwego łożyska powodujący błędne umiejscowienie lub zakrycie koła dekodującego impulsy elektryczne z czujników pomiaru prędkości | Wadliwe działanie kontrolera sterującego – RWAL Kontroler otrzymuje sprzeczne lub nieprawidłowe sygnały czujników | Wadliwe działanie systemu ABS | Utrata kontroli nad pojazdem |
| Odgięcie uchwytu przytrzymującego czujnik powodujące zbyt dużą odległość miedzy czujnikiem a kołem dekodującym | Wadliwe działanie kontrolera sterującego – RWAL Kontroler otrzymuje sprzeczne lub nieprawidłowe sygnały czujników | Wadliwe działanie systemu ABS | Utrata kontroli na pojazdem [41] |
| Uszkodzenie pompy hamulcowej (korozja metalowych części, zużycie elementów uszczelniających lub przewodów | „Miękki” wpadający w podłogę pedał hamulca | Drastyczny spadek skuteczności hamowania | Utrata kontroli nad pojazdem |
| Pęknięcie metalowych lub gumowych przewodów hamulcowych | Wyciek płynu hamulcowego | „Miękki”, wpadający w podłogę pedał hamulca | Utrata kontroli nad pojazdem [42] |

Relacje między zagrożeniami można analizować za pomocą diagramu FT (*fault tree*), który prezentuje rysunek 3.6.



Rys. 3.6 Analiza drzewa błędów dla systemu ABS

Uproszczony, widoczny na rysunku poniżej, przypadek zakłada stałą częstotliwość zdarzeń powodujących problemy z hamulcami (raz w miesiącu), problemy z czujnikiem pomiarowym prędkości obrotowej koła i ponowną rekalibracją kontrolera sterującego ABS (raz na 6 miesięcy) oraz awarie zaworów hydraulicznych (raz w roku). W takim przypadku utrata kontroli nad pojazdem może nastąpić z prawdopodobieństwem 0,36% (tj. ok raz na 277 lat). Jednak np. w przypadku wadliwego działania czujnika pomiaru prędkości kół prawdopodobieństwo utraty kontroli nad pojazdem może wzrosnąć nawet dziesięciokrotnie (4,3%, raz na 23 lata) [43].

Analiza bezpieczeństwa nie będzie kompletna jeśli oprócz analizy zagrożeń przedstawionej w tabeli 3.1 nie dołączymy informacji o: diagnostyce, postepowaniu po wykryciu awarii ABS oraz możliwościach ich zapobiegania. Tabele 3.2 i 3.3 porządkują pozyskane przeze mnie informacje.

Tabela 3.2 Układ hamulcowy z ABS – Diagnostyka usterek

| Zdarzenie niebezpieczne | Diagnostyka |
| --- | --- |
| Wyciek płynu hamulcowego | * Wykonanie próby szczelności układu hydraulicznego (wynik negatywny: widoczny spadek odległości pomiędzy powierzchnią pedału hamulca a podłogą kabiny; weryfikacja przy wciśnięciu pedału hamulca do oporu) * Elementy układu hamulcowe są mokre. Na ich powierzchni stwierdzono obecność płynu hamulcowego * Widoczne wycieki płynu hamulcowego na podłożu pod podwoziem pojazdu * Nagły ubytek płynu hamulcowego w zbiorniczku w krótkim czasie (poziom płynu hamulcowego nie zawiera się w przedziale kontrolnym zaznaczonym na powierzchni zbiornika) [44] |
| Woda lub powietrze w płynie hamulcowym | * zauważono, że szybkie wciskanie pedału hamulca do oporu powoduje zmniejszanie odległości pomiędzy powierzchnią pedału hamulca a podłogą kabiny pojazdu (zmniejszenie tzw. skoku czynnego) * pedał hamulca „wpada” w podłogę kabiny przy relatywnie małej sile nacisku * zmierzono zbyt niską temperaturę wrzenia płynu hamulcowego * negatywny wynik testu pomiaru zawartości wody w płynie hamulcowym [45] |
| Uszkodzenie cylindra głównego | * uczucie „twardego” pedału hamulca podczas hamowania * zauważono że przewód podciśnienia jest nieszczelny [46] * zauważono płyn hamulcowy na powierzchni cylindra głównego * zauważono dużą ilość rdzy pomiędzy cylindrem głównym a wzmacniaczem siły hamowania * zauważono że uszczelki łączące rezerwuar płynu hamulcowego z cylindrem są zużyte * zauważono, że poziom płynu hamulcowego jest poniżej poziomu „mini” * kontrolka hamulców pozostaje cały czas zapalona [47] |
| Zawór odcinający zapewniający stałe ciśnienie płynu hamulcowego w układzie podczas akcji przeciw blokowania kół – nie działa | * wydłużony czas uruchomienia systemu ABS, zauważalnie dłuższa droga hamowania pojazdu nawet przy wsparciu systemu przeciwblokującego * elektrozawór zablokowany w pozycji otwartej – wyczuwalne „ciągnięcie” hamulców podczas hamowania z ABS [48] * identyfikacja kodu błędu lokowanego w pamięci modułu sterującego ABS wskazującego na niesprawność zaworu odcinającego [49] * Brak reakcji koła na modulowanie ciśnienia podczas hamowania w skutek zerwania przewodu do elektrozaworu [50]. |
| Zawór zrzutowy odprowadzający nadmiar płynu hamulcowego w układzie – nie działa | * zauważalnie dłuższa droga hamowania pojazdu nawet przy wsparciu systemu przeciwblokującego * elektrozawór zablokowany w pozycji otwartej – uczucie „ciągnięcia” hamulców podczas hamowania bez ABS. Wynika to z utraty ciśnienia hamowania na kole [51]. * Identyfikacja kodu błędu lokowanego w pamięci modułu sterującego ABS wskazującego na niesprawność zaworu zrzutowego [52] * Brak reakcji koła na modulowanie ciśnienia podczas hamowania w skutek zerwania przewodu do elektrozaworu [53] |
| Nieprawidłowa kalibracja (uszkodzenie) modułu sterującego ABS (np. po wymianie czujnika prędkości obrotowej koła) | * Blokowanie się zacisku hamulca podczas jazdy – blokowanie kół * Zapalona kontrolka ABS na panelu kierowcy podczas jazdy gdy pedał hamulca nie jest używany * Pedał hamulca nie reaguje * Użycie hamulców wymaga zwiększonej siły nacisku stopy kierowcy na pedał hamulca (uczucie „twardego” pedału hamulca) * Uszkodzenie prędkościomierza na panelu kierowcy. Wyświetlanie błędnych wskazań aktualnej prędkości pojazdu (usterka pojawia się bardzo rzadko) [54] |
| Wadliwe działanie czujnika prędkości (przegrzanie, zalepienie solą lub błotem drogowym, korozja) | * Inspekcja czujników ABS ujawniła ich uszkodzenie spowodowane działaniem wysokiej temperatury np.: w przypadku zwarcia w obwodzie elektrycznym * Negatywny wynik pomiaru omomierzem (tylko czujniki indukcyjne) oporu wewnętrznego czujnika na rozłączonym połączeniu wtyczkowym. Wynik pomiaru: 0 Ω – doszło do zwarcia w obwodzie elektrycznym, M Ω - wystąpienie przerwy na kole zębatym, 800 Ω – 1200 Ω – oporność czujnika jest prawidłowa * Negatywny (inny niż ∞ w przypadku badania omomierzem lub brak sygnału sinusoidalnego o odpowiedniej mocy w przypadku gdy badanie wykonano oscyloskopem) wynik badania zwarcia do masy (pomiar wykonuje się od styku przyłączeniowego przewodu czujnika do masy samochodu) * Negatywny (uzyskano przebieg sygnału inny niż prostokątny zależny od prędkości obrotowej koła) wynik pomiaru napięcia sygnału (badanie dotyczy czujników Halla w których diagnostyka za pomocą omomierza nie jest zalecana) [55] * Zauważono ogniska korozji w okolicach umiejscowienia czujnika lub wprost na nim. * Zauważono zalepienie czujnika lub koła zębatego błotem lub solą drogową. * Widoczna zapalona kontrolkę ABS na desce rozdzielczej, * Blokada kół podczas hamowania w skutek błędnych lub braku danych z czujników pomiaru prędkości * Identyfikacja zapisanego kodu błędu dotyczącego niesprawności czujników w pamięci sterownika ABS, * Awaria innych systemów korzystających z danych pomiarowych czujników prędkości [56] |
| Zawór zwrotny zapewniający przepływ płynu hamulcowego w jednym kierunku – nie działa | * zauważono wzrost skoku czynnego (odległości pomiędzy powierzchnią pedału hamulca a podłoga kabiny pojazdu) przy próbie kilkukrotnego naciśnięcia pedału hamulca [57] * „Twardy” pedał hamulca utrudniający użycie hamulców w razie konieczności zatrzymania pojazdu * Wyczucie efektu „gąbczastego” pedału hamulca. Przy niewielkiej sile nacisku pedał hamulca „zapada się” w kierunku podłogi. Zdjęcie siły nacisku na pedał hamulca powoduje powolny jego powrót do stanu wyjściowego. Usterka zaworu zwrotnego umożliwia dostawanie się powietrza do przewodów hamulcowych [58] |
| Mechaniczne uszkodzenie okablowania czujnika pomiaru prędkości obrotowej | * Podczas inspekcji czujników zauważono zły stan techniczny kabli łączących sterownik ABS z czujnikami pomiaru prędkości:   + Nastąpiło przerwanie przewodu   + Zweryfikowano nieprawidłowe podłączenie wtyków przewodów * Widoczna zapalona kontrolkę ABS na desce rozdzielczej, przy włączonym zapłonie bez naciskania pedału hamulca (po wykonaniu procedury auto diagnostycznej przy włączaniu silnika kontrolka powinna zgasnąć) * Blokada kół podczas hamowania w skutek błędnych lub braku danych z czujników pomiaru prędkości * Identyfikacja zapisanego kodu błędu dotyczącego niesprawności czujników w pamięci sterownika ABS, * Awaria innych systemów korzystających z danych pomiarowych czujników prędkości * Regulacje pozorne [59] |
| Nieprawidłowy montaż lub wybór niewłaściwego łożyska powodujący błędne umiejscowienie lub zakrycie koła dekodującego impulsy elektryczne z czujników pomiaru prędkości | * Zapalanie się kontrolki ostrzegawczej ABS podczas jazdy na desce rozdzielczej przy braku użycia hamulców * Zauważalne mechaniczne ścieranie czujnika pomiaru prędkości obrotowej spowodowane nadmiernym luzem piasty koła * Dysfunkcja ABS spowodowana błędnymi pomiarami prędkości kół (wyłączenie systemu podczas jazdy bez użycia hamulca) * Identyfikacja kodu błędu w pamięci sterownika wskazująca na dysfunkcję czujnika pomiaru prędkości * Dysfunkcja czujnika pomiaru prędkości lub koła dekodującego spowodowana zabrudzeniem opiłkami metalu ścierającego się łożyska * Samoczynne włączanie się systemu ABS przy hamowaniu z niewielkiej prędkości (przesunięcie się prawidłowo zamontowanego czujnika podczas montażu zwrotnicy) * Podczas przeglądu zauważono nieprawidłowe ułożenie magnetycznego koła dekodującego względem czujnika spowodowane błędnym montażem lub nieprawidłowym doborem łożyska * Zauważono że zastosowano zamiennik łożyska z mniejszą liczbą pól magnetycznych na pierścieniu dekodującym sygnał z czujnika pomiaru prędkości [60] |
| Odgięcie uchwytu przytrzymującego czujnik pomiaru prędkości powodujące zbyt dużą odległość pomiędzy czujnikiem a kołem dekodującym | * Uszkodzenie mechaniczne koła dekodującego (tarcie czujnika o koło dekodujące jeśli odległość jest zbyt mała) * Nieprawidłowa regulacja siły hamowania lub brak działań przeciwblokujących z powodu błędnych odczytów z czujnika (czujnik zbyt daleko od koła dekodującego) * Zablokowanie koła podczas hamowania * Zapalnie się kontrolki ostrzegawczej dotyczącej awarii ABS na desce rozdzielczej kierowcy * Identyfikacja kodu błędu w pamięci sterownika świadcząca o niesprawności czujnika pomiarowego * Stwierdzenie nieprawidłowej odległości czujnika od koła dekodującego podczas inspekcji technicznej [61] |
| Uszkodzenie pompy hamulcowej (korozja metalowych części, zużycie elementów uszczelniających lub przewodów | * Odczuwalne pogorszenie jakości hamowania. Nacisk na pedał hamulca nie przekłada się na efektywność hamowania. * Konieczne jest „pompowanie” pedału hamulca aby możliwe było użycie hamulców. [62] * Zauważono wycieki płynu hamulcowego na gwintowanych zakończeniach przewodów hamulcowych wkręconych w cylinder główny lub gumowych elementach uszczelniających * Zauważono ogniska korozji metalowych części pompy * Podczas utrzymywania wciśniętego pedału hamulca zauważono pęcherzyki powietrza no powierzchni płynu hamulcowego w zbiorniku zamontowanym do pompy hamulcowej. (Zapowietrzenie układu hamulcowego jest jedną z oznak uszkodzenia pompy hamulcowej). [63] * Brak wyczuwalnego punktu oporu pedału. Hamulec przy kilkukrotnym naciskaniu nie twardnieje lub nie wraca do położenia początkowego. Test wykonuje się na wyłączonym silniku. [64] |
| Pęknięcie metalowych lub gumowych przewodów hamulcowych | * Miękki pedał hamulca * Ubywanie lub całkowity brak płynu w zbiorniczku * Plamy płynu hamulcowego pod samochodem * Plamy płynu hamulcowego przy kołach * Ślady płynu na zaciskach * Zapalenie się kontrolki na desce rozdzielczej, ostrzegającej o małej ilości płynu hamulcowego * Ściąganie samochodu w jedną stronę podczas hamowania (skorodowane przewody hamulcowe) * Słabe działanie hamulców pomimo silnego naciskania na pedał * Widoczne otarcia i pęknięcia na metalowych przewodach hamulcowych [65] |

Tabela 3.3 Postępowanie po zdiagnozowaniu zdarzenia niebezpiecznego, przeciwdziałanie

| Zdarzenie niebezpieczne | Postępowanie w przypadku wykrycia awarii | Metody przeciwdziałania (zabezpieczenia) |
| --- | --- | --- |
| Wyciek płynu hamulcowego | * Należy udać się do warsztatu w celu identyfikacji źródła wycieku i dokonania naprawy |  |
| Woda lub powietrze w płynie hamulcowym | * Wymiana płynu hamulcowego * Wykonanie odpowietrzenia układu | * Przestrzeganie terminowej wymiany płynu hamulcowego |
| Uszkodzenie cylindra głównego |  |  |
| Zawór odcinający zapewniający przepływ płynu hamulcowego w jednym kierunku – nie działa |  |  |
| Zawór zrzutowy odprowadzający nadmiar płynu hamulcowego w układzie – nie działa |  |  |
| Nieprawidłowa kalibracja (uszkodzenie) modułu sterującego ABS (np. po wymianie czujnika prędkości obrotowej koła) | * Wykonanie diagnostyki modułu sterującego i wymiana na nowy w warsztacie naprawczym |  |
| Wadliwe działanie czujnika prędkości obrotowej koła (przegrzanie, zalepienie solą lub błotem drogowym, korozja czujnika) | * Wymiana czujnika na nowy w warsztacie naprawczym |  |
| Zawór zwrotny zapewniający stałe ciśnienie płynu hamulcowego w układzie podczas akcji przeciw blokowania kół – nie działa |  |  |
| Mechaniczne uszkodzenie okablowania czujnika pomiaru prędkości obrotowej |  |  |
| Nieprawidłowy montaż lub wybór niewłaściwego łożyska powodujący błędne umiejscowienie lub zakrycie koła dekodującego impulsy elektryczne z czujników pomiaru prędkości |  |  |
| Odgięcie uchwytu przytrzymującego czujnik pomiaru prędkości powodujące zbyt dużą odległość pomiędzy czujnikiem a kołem dekodującym |  |  |
| Uszkodzenie pompy hamulcowej (korozja metalowych części lub zużycie elementów uszczelniających) lub przewodów) |  |  |
| Pęknięcie metalowych lub gumowych przewodów hamulcowych | * Wymiana przewodów na nowe w warsztacie naprawczym | Montaż specjalnych osłon podwozia |

## *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.

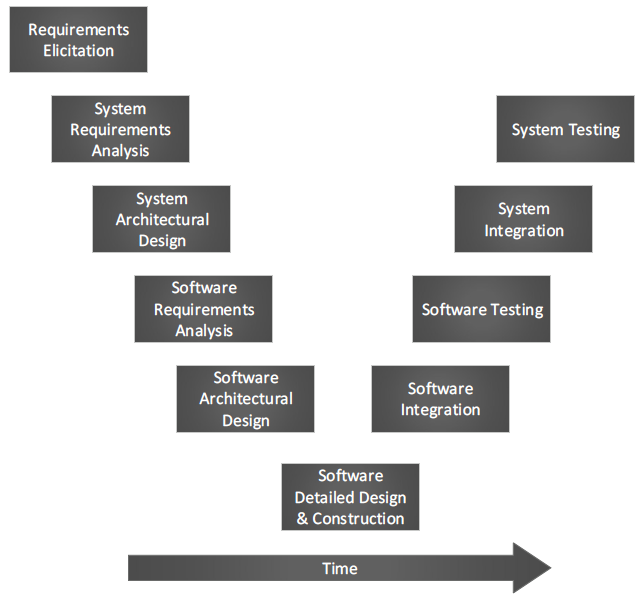
Najwięksi klienci przemysłu motoryzacyjnego w Europie, zwracają uwagę na rolę skutecznego i ustandaryzowanego zarządzania projektem, co jest wg nich równie ważne, jak wytworzenie konkretnego oprogramowania układowego. Sprawne, zarządzanie procesem wytwórczym daje odbiorcy produktu zdecydowanie więcej 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.

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.

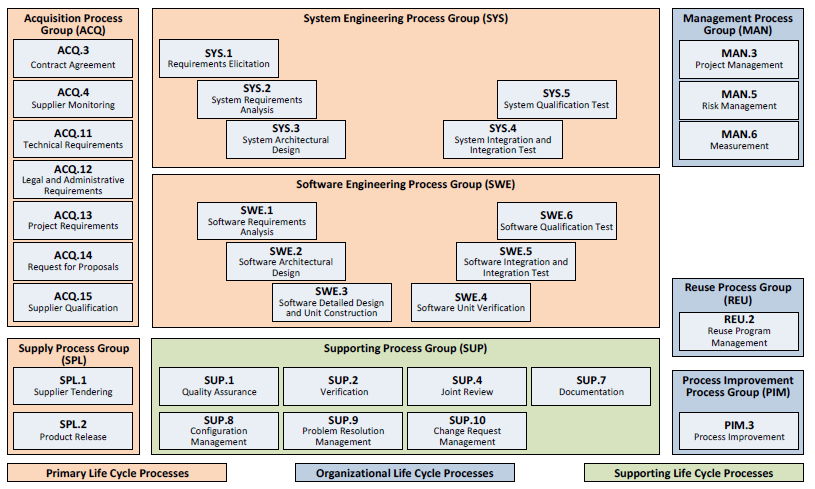
Istniejące standardy ze względu na zmieniającą się specyfikę branży motoryzacyjnej musza być ciągle rozwijane i uaktualniane w taki sposób, aby dawały najlepsze gwarancje spełniania celów, których realizacje mają wspomagać. Przykładem takiego rozwoju jest wytworzenie przez stowarzyszenie czołowych producentów samochodów (SIG – Sepcial Interest Group), standardu Automotive SPICE, zgodnego z normą ISO 12207. 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 zaprezentowany został na rys 3.5 (poniżej). Przedstawia on kolejność kroków w czasie trwania procesu wytwarzania oprogramowania. 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 klienta od początku cyklu wytwórczego [66].



Rys. 3.7 Przykładowa implementacja standardu Automotive SPICE - model V

Standard Automotive SPICE wyróżnia trzy kategorie procesów, które są integralnym częściami cyklu wytwórczego: Primary Life Cycle Processes, Organizational Life Cycle Processes and Supporting Life Cycle Processes. Rysunek 3.6 prezentuje rozmieszczenie grup procesów wg zdefiniowanych w standardzie kategorii.



Rys. 3.8 Podział procesów na kategorie wg standardu Automotive Spice

Realizacja dyplomu koncentruje się wokół kwestii dowodzenia o bezpieczeństwie systemu. Dlatego nie wszystkie procesy cyklu wytwórczego wymagają dokładnej analizy. W tym rozdziale szczegółowo omówione zostaną wyłącznie te procesy, które są kluczowe w kontekście zapewnienia, że system na etapie wytwarzania, spełnia wymagania klienta w zakresie bezpieczeństwa.

Mając na uwadze powyższe kryterium analizę cyklu wytwórczego otwierają procesy zaliczane do kategorii Primary Life Cycle Processes. Kategoria ta agreguje procesy w czterech grupach:

* System Engineering Process Group (SYS),
* Software Engineering Process Group (SWE),
* Supplay Process Group (SPL) – ta grupa dotyczy procesów wykonywanych po stronie dostawców zewnętrznych, których zadaniem jest dostarczanie produktu lub usługi, które są jedynie częścią całości wytwarzanego systemu. Wnioskowanie o bezpieczeństwie odbywa się dla systemu jako spójnej całości wszystkich komponentów także tych dostarczanych przez firmy zewnętrzne, dlatego pomijam grupę SPL w dalszej analizie procesu wytwórczego,
* Acquisition Proces Group (ACQ) – procesy tej grupy są wykonywane po stronie klienta, lub dostawcę działającego jako klient dla własnych dostawców, w celu nabycia produktu lub usługi. Procesy tej grupy, podobnie jak poprzedniej nie mają istotnego wpływu na wykazywanie bezpieczeństwa systemu, dlatego w dalszej części tego podrozdziału nie będą szerzej omawiane.

Poniżej omówione zostały procesy z grup SYS i SWE oraz SUP (procesy należące do kategorii Supporting Life Cycle Procesess) – które są ważne w kontekście dowodzenia o bezpieczeństwie systemu w cyklu wytwórczym.

|  |  |
| --- | --- |
| ***System Engineering Process Group (SYS)*** – składa się z procesów związanych z::   * Pobieraniem, zarządzaniem wymaganiami klienta i wewnętrznymi co do systemu * Definiowaniem architektury systemu * Integracją i wykonywaniem testów na poziomie systemu | |
| **Requirements Elicitation (SYS1)** | |
| Cele procesu | Gromadzenie, przetwarzanie i śledzenie wymagań interesariuszy względem produktu przez cały proces wytwórczy |
| Rezultaty implementacji  Procesu (RIP) | 1. Utrzymanie komunikacji pomiędzy zainteresowanymi stronami projektu 2. Uzgodnione wymagania interesariuszy zostały zdefiniowane i określone 3. Ustalenie mechanizmu zmian w wymaganiach które mogą następować w oparciu o zmieniające się potrzeby zainteresowanych stron projektu 4. Ustalenie mechanizmu monitorowania aktualnych potrzeb zainteresowanych stron projektu 5. Ustalenie procedury, której interesariusze powinni przestrzegać w celu określenia statusu i dyspozycji żądań zmian w wymaganiach 6. Zapewnienie, że zmiany w wymaganiach wynikające z zmieniającej się technologii i potrzeb interesariuszy są właściwie identyfikowane, powiązane a ryzyko z związane z ich wdrożeniem jest oceniane i zarządzane |
| Produkty wyjściowe | * Plan zarzadzania ryzykiem projektu (powiązane z RIP pkt. 6) * Plan ograniczania ryzyka (powiązane z RIP pkt. 6) * Korespondencja służbowa (maile, notatki ze spotkań) potwierdzająca obowiązujące uzgodnienia, dokumentująca aktualną dojrzałość projektu (powiązane z RIP pkt. 1, 4) * Dokument przeglądu projektu (powiązane z RIP pkt. 4, 5) * Dokument kontroli zmian (powiązane z RIP pkt. 3, 4) * Raport analizy (powiązane z RIP pkt. 2, 3, 6) * Wymagania Interesariuszy projektu (powiązane z RIP pkt. 1, 2) |
| **System Requirements Analysis (SYS2)** | |
| Cele procesu | Przekształcenie zdefiniowanych wymagań zainteresowanych stron projektu w zestaw wymagań systemowych, które będą pomocne przy projektowaniu systemu. |
| Rezultaty implementacji  Procesu (RIP) | 1. Wytworzenie zdefiniowanego zestawu wymagań systemowych 2. Pogrupowanie wymagań systemowych wg określonych kategorii. Analiza wymagań pod względem ich poprawności i możliwości weryfikacji 3. Przenalizowanie wpływu wymagań systemowych na środowisko operacyjne 4. Określenie priorytetów wdrażania wymagań systemowych 5. Aktualizacja wymagań systemowych, jeśli jest to potrzebne 6. Ustalenie czy wymagania interesariuszy „pokrywa” wytworzony zestaw wymagań systemowych 7. Ocena wymagań interesariuszy pod względem kosztów, harmonogramu i wpływu na projekt 8. Uzgodnienie wymagań systemowych i przekazanie wszystkim zainteresowanym stronom projektu |
| Produkty wyjściowe | * Korespondencja służbowa (maile, notatki ze spotkań) potwierdzająca obowiązujące uzgodnienia, dokumentująca aktualną dojrzałość projektu (powiązane z RIP pkt. 8) * Dokument kontroli zmian (powiązane z RIP pkt. 1) * Dokument przeglądu projektu (powiązane z RIP pkt. 6) * Dokument identyfikacji wymagań systemowych w pozyskanych wymaganiach interesariuszy (powiązane z RIP pkt. 6) * Raport analizy (powiązane z RIP pkt. 2, 3, 4, 7) * Dokument specyfikacji wymagań co do interfejsu systemu (powiązane z RIP pkt. 1, 3) * Specyfikacja wymagań systemowych (powiązane z RIP pkt. 1, 5) * Kryteria weryfikacji (powiązane z RIP pkt. 2) |
| **System Architectural Design (SYS3)** | |
| Cele procesu | * Opracowanie projektu architektury systemu * Przypisane określonych wymagań względem systemu do poszczególnych elementów w opracowanym projekcie architektury * Ocena projektu architektury systemu wg zdefiniowanych kryteriów |
| Rezultaty implementacji  Procesu (RIP) | 1. Wytworzenie projektu architektury systemu z wskazaniem elementów, z których się składa 2. Powiązanie wymagań systemowych z określonymi elementami systemu na projekcie 3. Zdefiniowanie interfejsów poszczególnych elementów systemu 4. Zdefiniowanie logiki systemu 5. Wskazanie na projekcie architektury systemu które wymagania systemowe odpowiadają pozyskanym wymaganiom od interesariuszy projektu 6. Uzgodnienie projektu architektury systemu i przekazanie go wszystkim stronom projektu |
| Produkty wyjściowe | * Projekt architektury systemu (powiązane z RIP pkt. 1, 2, 3, 4, 5) * Korespondencja służbowa (maile, notatki ze spotkań) potwierdzająca obowiązujące uzgodnienia, dokumentująca aktualną dojrzałość projektu (powiązane z RIP pkt. 6) * Dokument przeglądu projektu (powiązane z RIP pkt. 5) * Dokument identyfikacji wymagań systemowych w pozyskanych wymaganiach interesariuszy (powiązane z RIP pkt. 5) * Specyfikacja wymagań dotycząca interfejsu systemu (powiązane z RIP pkt. 3) |
| **System Integration and Integration Test (SYS4)** | |
| Cele procesu | * Integracja elementów systemu w większe moduły aż do uzyskania w pełni zintegrowanego systemu zgodnego z projektem architektury systemu * Dostarczenie dowodów, że elementy systemu zostały zintegrowane w sposób zgodny z projektem architektury |
| Rezultaty implementacji  Procesu (RIP) | 1. Wytworzenie strategii integracji systemu zgodnej planem projektu. Plan wydań kolejnych wersji systemu oraz projekt architektury systemu są opracowywane pod kątem integracji elementów systemu 2. Wytworzenie strategii testów integracji systemu, która zawiera plan testów regresyjnych, w celu przetestowania interakcji elementów systemu 3. Opracowanie specyfikacji testów integracji systemu zgodnych z strategią testów integracji, takich których pozytywne wykonanie dostarczy dowody na zgodność zintegrowanych elementów systemu w tym także interfejsów pomiędzy elementami z wytworzonym projektem architektury 4. Uzyskanie takiego zaawansowania projektu, w którym elementy systemu są zintegrowane zgodnie z dostarczoną strategia integracji 5. Wybór przypadków testowych zawartych w specyfikacji testów integracji następuje w oparciu o wytyczne strategii testów integracyjnych i planu wydań kolejnych wersji systemu 6. Zapewnienie, że interakcje poszczególnych elementów systemu są testowane przy użyciu wybranych przypadków testowych a wyniki testów są dokumentowane. 7. Zapewnienie identyfikacji przypadków testowych wraz z wynikami testów integracji przeprowadzonych na ich podstawie na projekcie architektury który obrazuje poszczególne elementy systemu 8. Zapewnienie, że wyniki testów integracji są opisywane i udostępniane wszystkim zainteresowanym stronom projektu |
| Produkty wyjściowe | * Specyfikacja testów (powiązane z RIP pkt. 3, 5) * Plan testów (powiązane z RIP pkt. 1, 2) * Wytworzony prototyp systemu (powiązane z RIP pkt. 4) * Korespondencja służbowa (maile, notatki ze spotkań) potwierdzająca obowiązujące uzgodnienia, dokumentująca aktualną dojrzałość projektu (powiązane z RIP pkt. 8) * Dokument przeglądu projektu (powiązane z RIP pkt. 7) * Dokument identyfikacji wymagań systemowych w pozyskanych wymaganiach interesariuszy (powiązane z RIP pkt. 7) * Wyniki testów (powiązane z RIP pkt. 6, 8) |
| **System Qualification Test (SYS5)** | |
| Cele procesu | Sprawdzenie czy wytworzony zintegrowany system jest zgodny z wymaganiami i czy jest gotowy do dostarczenia. |
| Rezultaty implementacji  Procesu (RIP) | 1. Opracowanie strategii testów kwalifikacji systemu, obejmującej strategie testów regresyjnych zgodnych z planem projektu i planem wydań kolejnych wersji systemu w celu kompletnego przetestowania dostarczonego zintegrowanego systemu 2. Opracowanie specyfikacji testów, zgodnie z strategią testów kwalifikacji, których celem będzie dostarczenie dowodów na zgodność systemu z wymaganiami klienta 3. Zapewnienie, że przypadki testowe uwzględnione w specyfikacji testów kwalifikacji są wybierane zgodnie z strategią testów kwalifikacyjnych i planem wydań kolejnych wersji systemu 4. Zapewnienie, że dostarczony system zintegrowany jest testowany wg wybranych przypadków testowych a wyniki są na bieżąco dokumentowane 5. Zapewnienie spójności oraz identyfikacji przypadków testowych i uzyskanych na ich podstawie wyników z wymaganiami systemowymi dostarczonymi przez klienta |
| Produkty wyjściowe | * Specyfikacja testów (powiązane z RIP pkt. 2, 3) * Plan testów (powiązane z RIP pkt. 1) * Korespondencja służbowa (maile, notatki ze spotkań) potwierdzająca obowiązujące uzgodnienia, dokumentująca aktualną dojrzałość projektu (powiązane z RIP pkt. 6) * Dokument przeglądu projektu (powiązane z RIP pkt. 5) * Dokument identyfikacji wymagań systemowych w pozyskanych wymaganiach interesariuszy (powiązane z RIP pkt. 5) * Wyniki testów (powiązane z RIP pkt. 4, 6) |

|  |  |
| --- | --- |
| ***Software Engineering Process Group (SWE)*** – składa się z procesów związanych z:   * Zarządzaniem wymaganiami klienta co do oprogramowania które wynikają z pozyskanych wymagań dotyczących systemu * Opracowaniem projektu architektury oprogramowania * Integracją i wykonywaniem testów przed wdrożeniem wytworzonego oprogramowania | |
| **Software Requirements Analysis (SWE1)** | |
| Cele procesu | Przegląd wymagań dotyczących systemu i na ich podstawie stworzenie listy wymagań względem oprogramowania wbudowanego które ma zostać wytworzone |
| Rezultaty implementacji  Procesu (RIP) | 1. Określenie wymagań względem oprogramowania i przydzielenie ich do określonych elementów oprogramowania systemu i ich interfejsów 2. Podzielenie wymagań dotyczących oprogramowania na kategorie i przeanalizowanie ich pod względem poprawności i weryfikowalności 3. Analiza wpływu wymagań względem oprogramowania na środowisko deweloperskie 4. Zdefiniowanie priorytetów wdrażania wymagań klienta względem oprogramowania podczas procesu wytwórczego. 5. Jeśli jest to konieczne wymagania względem oprogramowania mogą być aktualizowane 6. Określenie spójności i zakresu identyfikowalności wymagań dotyczących oprogramowania w dostarczonych wymaganiach względem systemu. Weryfikacja możliwości identyfikacji wymagań dotyczących oprogramowania na dostarczonym projekcie architektury systemu. 7. Ocena dostarczonych wymagań względem oprogramowania pod kątem kosztu wdrożenia, zakresu zmian w harmonogramie wdrożenia oraz wpływu na projektowany system 8. Uzgodnienie ostatecznej listy wymagań względem oprogramowania i przekazanie ich wszystkim stronom projektu których one dotyczą |
| Produkty wyjściowe | * Korespondencja służbowa (maile, notatki ze spotkań) potwierdzająca obowiązujące uzgodnienia, dokumentująca aktualną dojrzałość projektu (powiązane z RIP pkt. 8) * Dokument przeglądu projektu (powiązane z RIP pkt. 6) * Dokument kontroli zmian (powiązane z RIP pkt. 5, 7) * Dokument identyfikacji wymagań względem oprogramowania w pozyskanych wymaganiach od interesariuszy co do systemu (powiązane z RIP pkt. 1, 6) * Raport z analizy (powiązane z RIP pkt. 2, 3, 4, 7) * Specyfikacja wymagań dotyczących interfejsu oprogramowania (powiązane z RIP pkt. 1) * Specyfikacja wymagań dotyczących oprogramowania (powiązane z RIP pkt. 1) |
| **Software Architectural Design (SWE2)** | |
| Cele procesu | * Opracowanie projektu architektury oprogramowania wbudowanego * Przypisane określonych wymagań względem oprogramowania do poszczególnych elementów w opracowanym projekcie architektury * Ocena projektu architektury oprogramowania wbudowanego wg zdefiniowanych kryteriów |
| Rezultaty implementacji  Procesu (RIP) | 1. Zdefiniowanie projekt architektury oprogramowania wyodrębniając poszczególne elementy oprogramowania 2. Przydzielenie wymagań względem oprogramowania do właściwych elementów na architektury na projekcie 3. Zdefiniowanie interfejsów wszystkich elementów oprogramowania 4. Określone są zachowania dynamiczne i cele dotyczące zużycia zasobów poszczególnych elementów oprogramowania 5. Zdefiniowanie spójności między wymaganiami związanymi z oprogramowaniem a poszczególnymi elementami na projekcie architektury oprogramowania 6. Uzgodnienie ostatecznej wersji projektu architektury oprogramowania i przekazanie go zainteresowanym stronom projektu |
| Produkty wyjściowe | * Projekt architektury oprogramowania (powiązane z RIP pkt. 1, 2, 3, 4, 5) * Korespondencja służbowa (maile, notatki ze spotkań) potwierdzająca obowiązujące uzgodnienia, dokumentująca aktualną dojrzałość projektu (powiązane z RIP pkt. 6) * Dokument przeglądu projektu (powiązane z RIP pkt. 5) * Dokument identyfikacji wymagań względem oprogramowania w pozyskanych wymaganiach interesariuszy (powiązane z RIP pkt. 5) * Specyfikacja wymagań dotyczących interfejsu oprogramowania (powiązane z RIP pkt. 3) |
| **Software Detailed Design and Unit Construction (SWE3)** | |
| Cele procesu | Wytworzenie i dostarczenie elementów oprogramowania zgodnych z projektem architektury |
| Rezultaty implementacji  Procesu (RIP) | 1. Opracowanie szczegółowy projekt architektury oprogramowania z podziałem na poszczególne moduły 2. Określenie interfejsów dla wskazanych na projekcie modułów oprogramowania 3. Określenie zestawu dynamicznych zachowań poszczególnych modułów oprogramowania (określenie logiki aplikacji) 4. Określenie spójności oraz zakresu identyfikowalności pomiędzy wymaganiami względem oprogramowania a poszczególnymi modułami zdefiniowanymi w projekcie szczegółowym architektury 5. Uzgodnienie szczegółowego projektu architektury oprogramowania i przekazanie go zainteresowanym stronom projektu 6. Wytworzenie modułów oprogramowania zdefiniowanych w projekcie szczegółowym architektury |
| Produkty wyjściowe | * Szczegółowy projekt architektury oprogramowania (powiązane z RIP pkt. 1, 2, 3) * Prototyp oprogramowania wbudowanego (powiązane z RIP pkt. 6) * Korespondencja służbowa (maile, notatki ze spotkań) potwierdzająca obowiązujące uzgodnienia, dokumentująca aktualną dojrzałość projektu (powiązane z RIP pkt. 5) * Dokument przeglądu projektu (powiązane z RIP pkt. 4) * Dokument identyfikacji wymagań względem oprogramowania w pozyskanych wymaganiach interesariuszy (powiązane z RIP pkt. 4) |
| **Software Unit Verification (SWE4)** | |
| Cele procesu | * Weryfikacja wytworzonych elementów oprogramowania pod kątem ich zgodności z szczegółowym projektem architektury * Dostarczenie dowodów, że elementy oprogramowania są zgodne z zaprojektowaną architekturą oraz zdefiniowanymi wymaganiami niefunkcjonalnymi |
| Rezultaty implementacji  Procesu (RIP) | 1. Opracowanie strategii weryfikacji modułów oprogramowania 2. Opracowanie kryteriów weryfikacji modułów oprogramowania zgodnych z dostarczoną strategią weryfikacji dzięki którym możliwe będzie dostarczenie dowodów na zgodność dostarczonych modułów oprogramowania z projektem szczegółowym 3. Zapewnienie, że moduły oprogramowania są weryfikowane na podstawie strategii weryfikacji i dostarczonych kryteriów weryfikacji 4. Ustalenie spójności pomiędzy kryteriami weryfikacji modułów oprogramowania a rezultatami przeprowadzonej weryfikacji 5. Podsumowanie wyników weryfikacji modułów oprogramowania i dostarczenie ich zainteresowanym stronom projektu |
| Produkty wyjściowe | * Specyfikacja testów (powiązane z RIP pkt. 2) * Plan testów (powiązane z RIP pkt. 1) * Korespondencja służbowa (maile, notatki ze spotkań) potwierdzająca obowiązujące uzgodnienia, dokumentująca aktualną dojrzałość projektu (powiązane z RIP pkt. 5) * Dokument przeglądu projektu (powiązane z RIP pkt. 3, 4) * Dokument identyfikacji wymagań względem oprogramowania w pozyskanych wymaganiach interesariuszy (powiązane z RIP pkt. 4) * Rezultaty weryfikacji (powiązane z RIP pkt. 3, 5) * Wyniki testów (powiązane z RIP pkt. 3, 5) * Raport analizy (powiązane z RIP pkt. 3) |
| **Software Integration and Integration Test (SWE5)** | |
| Cele procesu | * Integracja elementów oprogramowania w większe moduły aż do uzyskania w pełni zintegrowanego oprogramowania wbudowanego * Dostarczenie dowodów, że elementy oprogramowania zostały zintegrowane w sposób zgodny z projektem architektury |
| Rezultaty implementacji  Procesu (RIP) | 1. Opracowanie strategii integracji oprogramowania zgodnej z planem projektu, planami wdrożeń kolejnych wersji oprogramowania oraz projektem architektury oprogramowania w celu dostarczenia dowodów poprawnego zintegrowania elementów oprogramowania 2. Opracowanie strategii testowania integracji oprogramowania obejmującą strategię testów regresji w celu przetestowania interakcji między poszczególnymi elementami oprogramowania 3. Opracowanie specyfikacji testów integracji oprogramowania zgodnie ze strategią testów integracji, której celem jest dostarczenie dowodów na zgodność zintegrowanych elementów oprogramowania z architekturą oprogramowania 4. Zapewnienie, że elementy oprogramowania są zintegrowane zgodnie ze strategią integracji oprogramowania 5. Zapewnienie, że scenariusze testowe zawarte w specyfikacji testów integracji są wybierane zgodnie ze strategią testów integracji i planem wydań kolejnych wersji oprogramowania 6. Zapewnienie, że zintegrowane elementy oprogramowania są testowane przy użyciu określonych przypadków testowych, a wyniki testów integracji oprogramowania są właściwe dokumentowane 7. Zapewnienie spójności między wskazanymi elementami na projekcie architektury oprogramowania a przypadkami testowymi zawartymi w specyfikacji testów integracji oprogramowania 8. Dokonanie posumowania wyników testów integracji oprogramowania i przekazane do wszystkich zainteresowanych stron projektu. |
| Produkty wyjściowe | * Moduł (element architektury) oprogramowania (powiązane z RIP pkt. 4) * Zintegrowane oprogramowanie (powiązane z RIP pkt. 4) * Specyfikacja testów (powiązane z RIP pkt. 3, 5) * Plan testów (powiązane z RIP pkt. 1, 2) * Korespondencja służbowa (maile, notatki ze spotkań) potwierdzająca obowiązujące uzgodnienia, dokumentująca aktualną dojrzałość projektu (powiązane z RIP pkt. 8) * Dokument przeglądu projektu (powiązane z RIP pkt. 7) * Dokument identyfikacji wymagań względem oprogramowania w pozyskanych wymaganiach interesariuszy (powiązane z RIP pkt. 7) * Wyniki testów (powiązane z RIP pkt. 6, 8) * Lista „zbudowanych” deweloperskich wersji kodu oprogramowania (powiązane z RIP pkt. 4, 7) |
| **Software Qualification Test (SWE6)** | |
| Cele procesu | Zapewnienie, że wytworzone zintegrowane oprogramowanie wbudowane jest zgodne z wymaganiami |
| Rezultaty implementacji  Procesu (RIP) | 1. Opracowanie strategii testów kwalifikacji oprogramowania, obejmującej strategie testów regresyjnych zgodnych z planem projektu i planem wydań kolejnych wersji oprogramowania w celu kompletnego przetestowania dostarczonego zintegrowanego oprogramowania 2. Opracowanie specyfikacji testów kwalifikacji oprogramowania, zgodnie z strategią testów kwalifikacji, których celem będzie dostarczenie dowodów na zgodność oprogramowania z wymaganiami klienta 3. Zapewnienie, że przypadki testowe uwzględnione w specyfikacji testów kwalifikacji są wybierane zgodnie z strategią testów kwalifikacyjnych i planem wydań kolejnych wersji oprogramowania 4. Zapewnienie, że dostarczone oprogramowanie zintegrowane jest testowane wg wybranych przypadków testowych a wyniki są na bieżąco dokumentowane 5. Zapewnienie spójności oraz identyfikacji przypadków testowych i uzyskanych na ich podstawie wyników z wymaganiami względem oprogramowania dostarczonymi przez klienta 6. Zapewnienie, że wyniki testów kwalifikacji oprogramowania zostały opisane i przekazane wszystkim stronom, projektu których dotyczą. |
| Produkty wyjściowe | * Specyfikacja testów (powiązane z RIP pkt. 2, 3) * Plan testów (powiązane z RIP pkt. 1) * Korespondencja służbowa (maile, notatki ze spotkań) potwierdzająca obowiązujące uzgodnienia, dokumentująca aktualną dojrzałość projektu (powiązane z RIP pkt. 6) * Dokument przeglądu projektu (powiązane z RIP pkt. 5) * Dokument identyfikacji wymagań względem oprogramowania w pozyskanych wymaganiach interesariuszy (powiązane z RIP pkt. 5) * Wyniki testów (powiązane z RIP pkt. 4, 6) * Strategia (powiązane z RIP pkt. 1) |

Trzecią grupą procesów które mają znaczenie w obszarze bezpieczeństwa systemu, a zatem wymagają szczegółowego omówienia to procesy z kategorii Supporting Life Cycle Processes. Kategoria ta zawiera procesy które należą do Supporting Process Group (SUP). Grupa ta składa się z procesów, które mogą być wykorzystane przez dowolny inny proces w różnych punktach cyklu życia systemu / projektu. Procesy tej grupy to:

|  |  |
| --- | --- |
| **Quality Assurance (SUP1)** | |
| Cele procesu | * Niezależne zapewnienie, że wytwarzany produkt lub trwający proces wytwórczy jest zgodny z wcześniejszymi założeniami, planami * Monitorowanie wytwarzanego produktu lub trwającego procesu wytwórczego i podejmowanie działania w przypadku stwierdzenia niezgodności |
| Rezultaty implementacji  Procesu (RIP) | 1. Opracowanie, wdrożenie i utrzymanie spójniej strategii zapewnienia jakości oprogramowania 2. Uzyskanie niezależności obiektywności oraz minimalizowanie ryzyka konfliktu interesów pomiędzy stronami projektu przy wdrażaniu strategii utrzymania jakości oprogramowania 3. Niezgodności produktów roboczych, procesów oraz czynności podejmowanych w ramach określonego procesu z powiązanymi wymaganiami są identyfikowane, dokumentowane, propagowane do wszystkich zainteresowanych stron projektu 4. Zgodność produktów roboczych, procesów i czynności w ramach procesów jest weryfikowana, dokumentowana i propagowana do wszystkich interesariuszy projektu 5. zapewnienie mechanizmów przekazywania informacji o niezgodnościach w projekcie pomiędzy osobami odpowiedzialnymi za zarządzanie projektem na różnych poziomach 6. Odpowiednie zarządzanie projektem ma na celu zapewnienie, że zidentyfikowane niezgodności zostaną rozwiązane |
| Produkty wyjściowe | * Plan zapewnienia jakości rozwiązań (powiązane z RIP pkt. 1, 2) * Korespondencja służbowa (maile, notatki ze spotkań) potwierdzająca obowiązujące zawarte uzgodnienia, dokumentująca aktualną dojrzałość projektu (powiązane z RIP pkt. 3,4,5) * Dokument z opisem problemów związanych z utrzymaniem jakości rozwiązań (powiązane z RIP pkt. 3, 5) * Dokument zawierający opis ogólnego poziomu jakości wytwarzanych rozwiązań (powiązane z RIP pkt. 2, 3, 4) * Dokument związany z przeglądem poziomu jakości wytwarzanych rozwiązań (powiązane z RIP pkt. 2, 3, 4) * Rejestr działań podjętych w celu poprawienia poziomu jakości oprogramowania (powiązane z RIP pkt. 3, 5, 6) * Dokument zawierający opis kryteriów jakie muszą zostać spełnione w celu utrzymania określonego poziomu jakości oprogramowania (powiązane z RIP pkt. 1) |
| **Verification (SUP2)** | |
| Cele procesu | * Potwierdzenie, że każdy produkt w danym procesie lub projekcie właściwie odzwierciedla określone wymagania. |
| Rezultaty implementacji  Procesu (RIP) | 1. Opracowanie, implementacja i zarządzanie strategią weryfikacji 2. Zidentyfikowanie kryteriów weryfikacji wszystkich wymaganych produktów roboczych procesu 3. Zapewnienie, że czynności w zakresie weryfikacji są wykonywane 4. Zapewnienie, że defekty są identyfikowane i dokumentowane 5. Zapewnienie, że rezultaty weryfikacji są dostępne dla klientów oraz wszystkich zainteresowanych stron projektu |
| Produkty wyjściowe | * Korespondencja służbowa (maile, notatki ze spotkań) potwierdzająca obowiązujące zawarte uzgodnienia, dokumentująca aktualną dojrzałość projektu (powiązane z RIP pkt. 5) * Korespondencja służbowa (maile, notatki ze spotkań) dokumentująca występujące problemy w zakresie implementacji procesu (powiązane z RIP pkt.3, 4, 5) * Dokumentacja wyników weryfikacji (powiązane z RIP pkt. 2, 3, 4, 5) * Dokumentacja zawierająca wykaz podjętych działań w celu rozwiązania zidentyfikowanych problemów (powiązane z RIP pkt. 4) * Dokumentacja zawierająca kryteria które musza zostać spełnione w celu zapewnienia określonego poziomu jakości (powiązane z RIP pkt. 2) * Strategia weryfikacji (powiązane z RIP pkt. 1) |
| **Joint Review (SUP3)** | |
| Cele procesu | * Potwierdzanie wspólnie z interesariuszami stanu zaawansowania projektu w odniesieniu do stawianych przed nim celów * Potwierdzanie wspólnie z interesariuszami, że produkt na obecnym etapie wytwórczym spełnia oczekiwania |
| Rezultaty implementacji  Procesu (RIP) | 1. Przeglądy zarządcze i techniczne są organizowane wg bieżących potrzeb projektu 2. Status, produkty procesu są oceniane podczas wspólnych przeglądów interesariuszy projektu 3. Wnioski uzgodnione po wspólnych przeglądach interesariuszy projektu są dostępne dla wszystkich zainteresowanych stron projektu. 4. Czynności podejmowane w następstwie uzyskanych rezultatów przeglądu projektu są monitorowane aż do ich zakończenia 5. Problemy są identyfikowane i dokumentowane |
| Produkty wyjściowe | * Korespondencja służbowa (maile, notatki ze spotkań) potwierdzająca zawarte uzgodnienia, dokumentująca aktualną dojrzałość projektu (powiązane z RIP pkt. 3,4,5) * Zapis przeglądu kontraktu (powiązane z RIP pkt. 1,2,3) * Dokumentacja występujących problemów (powiązane z RIP pkt. 3,5) * Korespondencja służbowa (maile, notatki) ze spotkań zespołów wspierających projekt (powiązane z RIP pkt. 1,2) * Dokumentacja zwierająca zapis informacji pochodzących z przeglądów projektu (powiązane z RIP pkt. 1 - 5) * Dokumentacja zawierająca wykaz podjętych działań w celu rozwiązania zidentyfikowanych problemów (powiązane z RIP pkt. 3, 4, 5) * Raporty przeprowadzonych analiz (powiązane z RIP pkt. 3, 5) * Raporty wykonanych audytów (powiązane z RIP pkt. 1, 2) * Dokumentacja dotycząca możliwości wprowadzania ulepszeń w zakresie określonego procesu (powiązane z RIP pkt. 3, 4) |
| **Documentation (SUP4)** | |
| Cele procesu | * Opracowanie materiałów projektowych * Utrzymanie aktualności zarejestrowanych informacji w procesie wytwórczym |
| Rezultaty implementacji  Procesu (RIP) | 1. Opracowanie strategii identyfikującej dokumentację, która ma powstać podczas cyklu życia produktu lub usługi 2. Identyfikacja standardów, których należy przestrzegać w celu opracowywania dokumentacji projektowej 3. Określenie rodzajów dokumentów jakie musza zostać wytworzone w trakcie trwania procesu lub projektu 4. Zawartość dokumentacji oraz cele jej wytwarzania są jasno określone 5. Określone są standardy regulujące sposób opracowania i udostępniania wytworzonej dokumentacji projektowej 6. Utrzymanie aktualności dokumentacji projektowej odbywa się wg ścisłych kryteriów |
| Produkty wyjściowe | * Plan dokumentowania czynności projektowych (powiązane z RIP pkt. 1, 2) * Dokument zawierający potwierdzenie zawartych uzgodnień (powiązane z RIP pkt. 4, 5) * Dokument przeglądu projektu (powiązane z RIP pkt. 4, 5) * Dokument zawierający historię wprowadzonych zmian w określonych obszarach projektu (powiązane z RIP pkt. 5, 6) * Lista produktów roboczych dla poszczególnych procesów (powiązane z RIP pkt. 3) |
| **Configuration Management (SUP5)** | |
| Cele procesu | * Utrzymanie integralności wszystkich produktów (np. środowiska deweloperskie) objętych procesem lub projektem * Udostępnienie ich zainteresowanym stronom zarówno po stronie klienta jak i wewnętrznie pomiędzy zespołami biorącymi udział w procesie wytwarzania oprogramowania. |
| Rezultaty implementacji  Procesu (RIP) | 1. Opracowanie strategii zarządzania konfiguracją 2. Wszystkie elementy konfiguracji wygenerowane przez proces lub projekt są zidentyfikowane i dokumentowane zgodnie ze strategią zarządzania konfiguracją 3. Modyfikacja i wydania elementów konfiguracji podlegają kontroli 4. Modyfikacje i wydania elementów konfiguracji są udostępniane zainteresowanym stronom projektu 5. Raportowany jest stan zmian elementów konfiguracji 6. Zapewniona jest kompletności i spójność podstawowych elementów konfiguracji 7. Przechowywanie elementów konfiguracji jest kontrolowane |
| Produkty wyjściowe | * Elementy konfiguracji (powiązane z RIP pkt. 2, 3, 7) * Podręcznik obsługi i przechowywania elementów konfiguracji (powiązane z RIP pkt. 3, 4, 5, 7) * Plan zarządzania konfiguracją (powiązane z RIP pkt. 1, 2, 7) * Plan naprawy konfiguracji (powiązane z RIP pkt. 1, 7) * Podstawowe dane konfiguracji (powiązane z RIP pkt. 2, 3, 4, 5, 6) * Dokument zarządzania konfiguracją (powiązane z RIP pkt. 2, 5, 7) * Historia zmian konfiguracji (powiązane z RIP pkt. 3) * System zarządzania konfiguracją (powiązane z RIP pkt. 1, 3, 4) |
| **Problem Resolution Management (SUP6)** | |
| Cele procesu | * Zapewnienie identyfikacji, analizy możliwych rozwiązań problemów * Monitoring skuteczności wdrożonych rozwiązań mających na celu usunięcie problemu |
| Rezultaty implementacji  Procesu (RIP) | 1. Opracowanie strategii zarządzania rozwiązywaniem problemów w projekcie 2. Zidentyfikowane problemy są rejestrowane i klasyfikowane 3. Zidentyfikowane problemy są analizowane w celu dobrania odpowiedniego sposobu ich rozwiązania 4. Inicjowanie rozwiązań problemu 5. Zidentyfikowane problemy są monitorowane aż do pełnego ich rozwiązania 6. Znany jest stan zgłoszonych problemów oraz okoliczności ich występowania |
| Produkty wyjściowe | * Plan zarządzania zidentyfikowanymi problemami (powiązane z RIP pkt. 1) * Dokument opisujący problem (powiązane z RIP pkt. 2, 3, 4, 5) * Raport analizy problemu (powiązane z RIP pkt. 3) * Raport zwierający ocenę skali problemu (powiązane z RIP pkt. 3) * Raport stanu problemu (powiązane z RIP pkt. 6) |
| **Change Request Management (SUP7)** | |
| Cele procesu | * Definiowanie żądań zmiany * Monitoring postępów wdrożenia żądań zmiany * Ocena skuteczności wdrożonych żądań zmian |
| Rezultaty implementacji  Procesu (RIP) | 1. Opracowanie strategii zarządzania żądaniami zmian 2. Żądania zmian są rejestrowane i identyfikowane 3. Identyfikacja zależności pomiędzy wieloma żądaniami zmian 4. Określenie kryteriów potwierdzenia realizacji żądań zmian 5. Żądania zmian są oceniane pod kątem oszacowania zasobów które są potrzebne do ich wdrożenia 6. Ustalenie priorytetów wdrożenia żądań zmian na podstawie wyników analizy ich wpływu na projekt oraz dostępności zasobów 7. Zatwierdzone żądania zmian są monitorowane aż do zakończenia ich wdrażania 8. Identyfikacja statusów żądań zmiany 9. Powiązanie żądań zmian z produktami roboczymi w procesie |
| Produkty wyjściowe | * Plan zarządzania zmianą (powiązane z RIP pkt. 1) * Żądanie zmiany (powiązane z RIP pkt. 2, 3, 4, 5, 6, 7) * Dokument przeglądu żądań zmian (powiązane z RIP pkt. 7) * Dokument kontroli wdrożonych żądań zmiany (powiązane z RIP pkt. 8, 9) |

Uzupełniając opis cyklu wytwórczego realizowany wg. standardu Automotive SPICE wspomnieć należy także o kategorii procesów *Organizational Life Cycle Processes*. Składa się ona z procesów wspierających rozwój produktów i zasobów organizacji. Właściwa implementacja i rozwój procesów tej kategorii pomagają organizacji osiągać cele biznesowe w aktualnie prowadzonych projektach. Kategoria ta dzieli procesy na trzy grupy:

* Management Proces Group (MAN) – grupa ta składa się z procesów, z których korzystać będzie każdy pracownik biorący udział w procesie wytwórczym którego rolą jest zarządzanie określony projektem lub procesem w ciągu cyklu życia systemu. Grupa MAN składa się z procesów takich jak: *project management, risk management, measurement*.
* Reuse Process Group – grupa obejmuje jeden proces stworzony w celu systematycznego wykorzystywania możliwości reużycia zasobów organizacji w cyklu życia systemu.
* Improvement Process Group (PIM) - w skład tej grupy wchodzi wyłącznie jeden proces - *process improvement*, który zawiera praktyki jakie należy stosować w celu usprawnienia innych procesów wykonywanych w ramach jednostki organizacyjnej [67].

# ZARZĄDZANIE DOWODAMI W SAFETY CASE DLA ABS

## *Opis podejścia*

## *Klasyfikacja dowodów*

## *Zbiór dowodów dla ABS w cyklu życia*

## *Etapy zarzadzania dowodami w rozwoju safety case*

## *Zarządzanie zmianami*

# Analiza procesu

## *Skuteczność i kompletność podejścia*

## *Korzyści – wsparcie w zarządzaniu zakresem zmian*

## *Napotkane problemy i propozycje doskonalenia podejścia*

## *Skalowalność*

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

# Podsumowanie

# WYKAZ LITERATURY

1. **Dezfuli H. Benjamin A. , Everett Ch. , Smith C. , Stamatelatos M. , Youngblood R.** *NASA System Safety Handbook.* Washington : National Aeronautics and Space Administration, 2011. str. 3.

2. *EAST-ADL Domain Model Specification.* strony 141 - 148.

3. **P Orwat.** *Analiza porównawcza dowodów bezpieczeństwa dla europejskich obszarów powietrznych.* Gdańsk : Politechnika Gdańska. strony 3-4.

4. Software Assurance Using Structured Assurance Case Models. [Online] [Zacytowano: 3 Wrzesień 2018.] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4548534/.

5. *ISO/IEC 15026-2 Systems and Software Assurance Case.* New York : Software & Systems Engineering Standards Committee, 2011. str. 6.

6. https://web.cn.edu/kwheeler/documents/Toulmin.pdf. [Online] [Zacytowano: 5 Wrzesień 2018.]

7. **P Orwat.** *Analiza porównawcza dowodówbezpieczeństwa dla euuropejskich obszarów powietrznych.* Gdańsk : Politechnika Gdańska. str. 5.

8. *ISO/IEC 15026-2 Systems and Software Assurance Case.* New York : Software & Systems Engineering Standards Committee, 2011. str. 6.

9. **Orwat Patryk.** *Analiza porównawcza dowodów bezpieczeństwa dla europejskich obszarów powietrznych.* Gdańsk : Politechnika Gdańska. str. 6.

10. **B.M Łuczak.** *Ocena narzędzi do budowy Assurance case.* Gdańsk : Politechnika Gdańska, 2014. str. 8.

11. **D. Smigielski.** System ABS. Co warto o nim wiedzieć? [Online] [Zacytowano: 30 Październik 2017.] http://antymoto.com.

12. Systemy elektroniczne ABS, ESP, ASR: poznaj alfabet bezpieczeństwa. *Akademia Auto Świat.* [Online] [Zacytowano: 30 Październik 2017.] http://akademia.autoswiat.pl.

13. **Właśniak R i Zamiatowski K.** *Agregat hudrauliczny Tevez MK II.* Bydgoszcz : Zespół Szkół Samochodowych, 2000. str. Rozdz. 2.1 Opis ogólny.

14. ABS (motoryzacja). *Wikipedia.* [Online] [Zacytowano: 30 Październik 2017.] https://pl.wikipedia.org.

15. How effective is ABS at reducing crashes. *Brainonboard.* [Online] [Zacytowano: 30 Październik 2017.] http://www.brainonboard.ca.

16. ABS (Anti-Blockier-System, Anti-look Break System, Anti Bloking System). [Online] [Zacytowano: 30 Październik 2017.] http://www.opony.com.pl/informacje/technologie.

17. **Foltynowicz L, Ślaski G i Kupiec J.** *Układy przeciwblokujące a diagnostyka układów hamulcowych.* Poznań  : Instytut Maszyn Roboczych i Pojazdów Samochodowych, Politechnika Poznańska, 2001. str. 2.

18. [Online] https://www.aaafoundation.org/faqs-anti-lock-braking-system-abs.

19. Kierowca lepszy niż ABS? Zapomnij. *Serwis motoryzacyjny magazynów „Motor” i „Auto Moto”.* [Online] [Zacytowano: 30 Październik 2017.] http://magazynauto.interia.pl,.

20. Bosh: ABS – historia rewolucyjnego systemu. *Serwis motoryzacyjny magazynu Auto – Swiat.* [Online] [Zacytowano: 30 Listopad 2017.] www.auto-swiat.pl.

21. Kierowca lepszy niż ABS? Zapomnij. *Serwis motoryzacyjny magazynów „Motor” i „Auto Moto”.* [Online] [Zacytowano: 30 Październik 2017.] http://magazynauto.interia.pl.

22. Bosh: ABS – historia rewolucyjnego systemu. *Serwis motoryzacyjny magazynu Auto – Swiat.* [Online] [Zacytowano: 30 Październik 2017.] www.auto-swiat.pl.

23. ABS (motoryzacja) pkt. 6 Historia. *Wikipedia.* [Online] [Zacytowano: 30 Październik 2017.] https://wikipedia.org.pl.

24. **Właśniak R i Zamiatowski K.** *Agregat hudrauliczny Tevez MK II, Rozdz. 4.1 Elektroniczny zespół sterujący.* Bydgoszcz : Zespół Szkół Samochodowych, 2000.

25. **Paszkowski J.** *Diagnostyka układu hamulcowego ABS.* Warszawa : Instytut Maszyn Elektrycznych, Politechnika Warszawska, 2003. strony 20-22.

26. Czujnik ABS. *Serwis internetowy Hella.* [Online] [Zacytowano: 30 Październik 2017.] https://www.hella.com.

27. Czujniki obrotów kół – do czego służą jak działają i jakie są objawy ich awarii? *Serwis motoryzacyjny Wirtualnej Polski.* [Online] [Zacytowano: 30 Październik 2017.] http://autokult.pl.

28. **Paszkowsk J.** *Diagnostyka układu hamulcowego ABS.* Warszawa : Instytut Maszyn Elektrycznych, Politechnika Warszawska, 2003. strony 17-19.

29. **Właśniak R i Zamiatowski K.** *Agregat hudrauliczny Tevez MK II.* Bydgoszcz : Zespół Szkół Samochodowych, 2000.

30. **Paszkowsk J.** *Diagnostyka układu hamulcowego ABS.* Warszawa : Instytut Maszyn Elektrycznych, Politechnika Warszawska, 2003.

31. **Właśniak R i Zamiatowski K.** *Agregat hudrauliczny Tevez MK II.* Bydgoszcz : Zespół Szkół Samochodowych, 2000.

32. **Paszkowsk J.** *Diagnostyka układu hamulcowego ABS.* Warszawa : Instytut Maszyn Elektrycznych, Politechnika Warszawska, 2003. str. 19.

33. **Mongiat J, i inni.** Anti-Lock Breaking System Project – Requirements Analysis Document. *Serwis Internetowy.* [Online] [Zacytowano: 30 Październik 2017.] http://www.cse.msu.edu/~cse470/F01/Projects/ABS/ABS4/web/do-requirements/do-requirements.html.

34. Autozone.com. *Sklep Autozone.com.* [Online] [Zacytowano: 20 Październik 2018.] https://www.autozone.com/repairguides/GM-Full-Size-Trucks-1988-1998-Repair-Information/REAR-WHEEL-ANTI-LOCK-RWAL-BRAKE-SYSTEM/General-Description/\_/P-0996b43f80c90ea3.

35. **Kornecki J,A i Zalewski J.** Dependability study of an antilock braking system: application of bayesian belief networks. *SemanticScholar.* [Online] 2013. [Zacytowano: 15 Wrzesień 2018.] https://www.semanticscholar.org.

36. Autozone.com. *Sklep Autozone.com.* [Online] 20 Październik 2018. https://www.autozone.com/repairguides/GM-Full-Size-Trucks-1988-1998-Repair-Information/REAR-WHEEL-ANTI-LOCK-RWAL-BRAKE-SYSTEM/General-Description/\_/P-0996b43f80c90ea3.

37. *SIG, VDA QMC Working Group 13 / Automotive.* brak miejsca : Automotive SPICE, 2015. str. 71.

38. **Pérez Ana Isabella Navarrete i Ugarelli Rita.** *Witryna sieci Web Norweskiego Stowarzyszenia Wodnego.* [Online] 2015. [Zacytowano: 3 Wrzesień 2018.] https://vannforeningen.no/wp-content/uploads/2015/06/2014\_915356.pdf.

39. **Kornecki J,A i Zalewski J.** Dependability study of an antilock braking system: application of bayesian belief networks. *Semantic Scholar.* [Online] 2013. [Zacytowano: 15 Wrzesień 2018.] https://www.semanticscholar.org.

40. Symptoms of a Bad or Failing Vacuum Brake Booster Check Valve. *YourMechanic.* [Online] [Zacytowano: 3 Listopad 2018.] https://www.yourmechanic.com/article/symptoms-of-a-bad-or-failing-vacuum-brake-booster-check-valve.

41. WP Autokult. *Witryna sieci Web Grupy WP.* [Online] [Zacytowano: 9 Październik 2018.] https://autokult.pl/28771,awarie-systemu-abs,all.

42. Auto Świat - ekspolatacja. *Witryna sieci Web magazynu Auto Świat.* [Online] [Zacytowano: 9 Październik 2018.] http://www.auto-swiat.pl/eksploatacja/objawy-typowych-awarii-hamulcow/8jqz04.

43. **Kornecki J,A i Zalewski J.** Dependability study of an antilock braking system: application of bayesian belief networks. *Semantic Scholar.* [Online] 2013. [Zacytowano: 15 Wrzesień 2018.] https://www.semanticscholar.org.

44. *Warsztat.pl.* [Online] warsztat.pl - artykuly. [Zacytowano: 22 Październik 2018.] https://warsztat.pl/artykuly.

45. warsztat.pl. *Warsztat.pl - artykuly.* [Online] [Zacytowano: 22 Październik 2018.] https://warsztat.pl/artykuly/diagnozowanie-ukladu-hamulcowego-pojazdu-samochodowego-cz-5,57680,bm9uZSE1NzY4MCEhbm93b2N6ZXNueXdhcnN6dGF0LnBsL2FydHlrdWx5L29zdGF0bmkvY3plc2NpLWktcmVnZW5lcmFjamEvMTI4.

46. Dobrymechanik.pl - artykuły. *dobrymechanik.pl.* [Online] [Zacytowano: 22 Październik 2018.] https://dobrymechanik.pl/artykuly/czytaj/544/diagnostyka/co-zrobic-gdy-pedal-hamulca-jest-twardy/.

47. YourMechanic.com. *YourMechanic Inc.* [Online] [Zacytowano: 23 Październik 2018.] https://www.yourmechanic.com/article/how-long-does-a-brake-master-cylinder-last.

48. Understanding ABS Modulator Problems. *KnowYourParts.* [Online] [Zacytowano: 25 Październik 2018.] https://www.knowyourparts.com/technical-resources/brakes-and-brake-components/understanding-abs-modulator-problems/.

49. ABS Solenoid Diagnosis: What is going on inside the HCU? *tirereview.com.* [Online] [Zacytowano: 25 Październik 2018.] http://www.tirereview.com/abs-solenoid-diagnosis-going-inside-hcu/.

50. ABS (motoryzacja). *wikipedia.org.* [Online] [Zacytowano: 23 Październik 2018.] https://pl.wikipedia.org/wiki/ABS\_(motoryzacja).

51. knowyourparts.com. *Understanding ABS Modulator Problems.* [Online] [Zacytowano: 4 Listopad 2018.] https://www.knowyourparts.com/technical-resources/brakes-and-brake-components/understanding-abs-modulator-problems/.

52. ABS Solenoid Diagnosis: What is going on inside the HCU? *http://www.tirereview.com.* [Online] [Zacytowano: 30 Październik 2018.] http://www.tirereview.com/abs-solenoid-diagnosis-going-inside-hcu/.

53. ABS (motoryzacja). *wikipedia.org.* [Online] [Zacytowano: 25 Październik 2018.] https://pl.wikipedia.org/wiki/ABS\_(motoryzacja).

54. Symptoms of a Bad ABS control module and replacement cost. *oards.com.* [Online] https://oards.com/5-symptoms-bad-abs-control-module-replacement-cost/.

55. Jak zdiagnozwoać uszkodzony czujnik ABS? *teamtotal.pl.* [Online] [Zacytowano: 5 Listopad 2018.] https://teamtotal.pl/artykul/jak-zdiagnozowac-uszkodzony-czujnik-abs.

56. Jak działa ABS? *total.com.* [Online] [Zacytowano: 24 Paździenik 2018.] http://www.total.com.pl/aktualnosci/artykuly/jak-dziala-ABS.html.

57. Sciąga.pl - układy hamulcowe. *Serwis sciaga.pl.* [Online] [Zacytowano: 19 Paździenik 2018.] https://sciaga.pl/tekst/48789-49-uklad\_hamulcowy.

58. Symptoms of a Bad or Failing Vacuum Brake Booster Check Valve. *YourMechanic.com.* [Online] [Zacytowano: 10 Listopad 2018.] https://www.yourmechanic.com/article/symptoms-of-a-bad-or-failing-vacuum-brake-booster-check-valve.

59. Jak zdiagnozować uszkodzony czujnik ABS. *teamtotal.pl.* [Online] [Zacytowano: 5 Listopad 2018.] https://teamtotal.pl/artykul/jak-zdiagnozowac-uszkodzony-czujnik-abs.

60. Wymiana łożyska koła a systemy stabilizacji ruchu. *e-autonaprawa.pl.* [Online] [Zacytowano: 5 Listopad 2018.] https://www.e-autonaprawa.pl/artykuly/5574/wymiana-lozyska-kola-a-systemy-stabilizacji-ruchu.html.

61. Jak zdiagnozować uszkodzony czujnik ABS? *teamtotal.pl.* [Online] [Zacytowano: 4 Listopad 2018.] https://teamtotal.pl/artykul/jak-zdiagnozowac-uszkodzony-czujnik-abs.

62. Co zrobić, gdy musisz pompować pedał hamulca? *DobryMechanik.* [Online] [Zacytowano: 28 Październik 2018.] https://dobrymechanik.pl/artykuly/czytaj/579/diagnostyka/co-zrobic-gdy-musisz-pompowac-pedal-hamulca/.

63. How to Diagnose a Brake Master Cylinder Failure. *itstillruns.com.* [Online] https://itstillruns.com/diagnose-brake-master-cylinder-failure-8292159.html.

64. Hamulce, czyli element ratujący nam życie. *blog.autoraport.pl.* [Online] [Zacytowano: 25 Październik 2018.] https://blog.autoraport.pl/tag/uszkodzenie-pompy-hamulcowej/.

65. Przewody hamulcowe – co się stanie w sytuacji, w której zawiodą? *motointegrator.com.* [Online] [Zacytowano: 19 Listopad 2018.] https://motointegrator.com/pl/pl/poradniki/uklad-hamulcowy/przewody-hamulcowe-co-sie-stanie-w-sytuacji-w-ktorej-zawioda.

66. **Bień A, Rzeszutko J i Szymański T.** *Systemy wbudowane do celów pomiarowo – kontrolnych w motoryzacji. Proces projektowania i wstępnej diagnostyki.* Kraków : PAK, 2014. strony 655-656. 8/2014.

67. **SIG VDA QMC Working Group 13 / Automotive.** *Automotive SPICE.* 2015.

68. Hamowanie awaryjne z ominięciem przeszkody bez systemu ABS. *Serwis Internetowy miesięcznika Szkoła Jazdy.* [Online] [Zacytowano: 30 Październik 2017.] http://www.szkola-jazdy.pl/.

69. Hamowanie z ABS-em to sztuka. *Serwis internetowy Głosu Pomorza.* [Online] [Zacytowano: 30 Październik 2017.] http://www.gp24.pl.

70. Kierowca lepszy niż ABS? Zapomnij. *Serwis motoryzacyjny magazynów „Motor” i „Auto Moto”.* [Online] [Zacytowano: 30 Październik 2017.] http://magazynauto.interia.pl.

71. Czujniki obrotów kół – do czego służą jak działają i jakie są objawy ich awarii. *Serwis motoryzacyjny portalu Wirtualna Polska.* [Online] [Zacytowano: 30 Październik 2017.] http://autokult.pl.

72. Cztery sytuacje drogowe w których ABS może wydłużać drogę hamowania. *Serwis motoryzacyjny Interii oraz magazynów „Motor” i „Auto Moto”.* [Online] [Zacytowano: 30 Październik 2017.] http://magazynauto.interia.pl.

73. Bosh: ABS – historia rewolucyjnego systemu. *Serwis motoryzacyjny magazynu Auto – Swiat.* [Online] [Zacytowano: 30 Październik 2017.] www.auto-swiat.pl.

74. ABS (motoryzacja) pkt. 6 Historia. *Wikipedia.* [Online] [Zacytowano: 30 Październik 2017.] https://pl.wikipedia.org.

75. Bosh: ABS – historia rewolucyjnego systemu. *Serwis motoryzacyjny magazynu Auto – Swiat.* [Online] [Zacytowano: 30 Październik 2017.] http://www.auto-swiat.pl.

76. ABS (motoryzacja) pkt. 6 Historia. *Wikipedia.* [Online] [Zacytowano: 30 Październik 2017.] https://pl.wikipedia.org.

77. Wikipedia - Automotive Safety Integrity Level. *Wikipedia.* [Online] [Zacytowano: 10 Wrzesień 2018.] https://en.wikipedia.org/wiki/Automotive\_Safety\_Integrity\_Level.

# WYKAZ RYSUNKÓW

[Rys. 2.1 Schemat postulatu najwyższego poziomu z powiązanymi argumentami 12](#_Toc529655622)

[Rys. 2.2 Model Argumentacji wg. Stephena Toulmina 14](#_Toc529655623)

[Rys. 3.1 Droga hamowania pojazdu bez / z ABS 18](#_Toc529655624)

[Rys. 3.2 Droga hamowania ze 100 km/h na suchej nawierzchni 19](#_Toc529655625)

[Rys. 3.3 Droga hamowania ze 100 km/h na mokrej nawierzchni 20](#_Toc529655626)

[Rys. 3.4 Schemat obwodu hydraulicznego w układzie ABS 23](#_Toc529655627)

[Rys. 3.5 Komponenty układu hamulcowego z systemem ABS kół tylnych 27](#_Toc529655628)

[Rys. 3.6 Analiza drzewa błędów dla systemu ABS 32](#_Toc529655629)

[Rys. 3.7 Przykładowa implementacja standardu Automotive SPICE - model V 39](#_Toc529655630)

[Rys. 3.8 Podział procesów na kategorie wg standardu Automotive Spice 40](#_Toc529655631)

# WYKAZ TABEL

Tabela 2.1 Bezpieczeństwo systemów sterowania - pojęcia podstawowe 9

Tabela 3.1 Wstępna Analiza Zagrożeń (PHA) dotycząca systemu ABS 29

Tabela 3.2 Układ hamulcowy z ABS – Diagnostyka usterek 32

Tabela 3.3 Postępowanie po zdiagnozowaniu zdarzenia niebezpiecznego, przeciwdziałanie 35