problem z 3.5 jest taki, że to wielki na ponad 10 stron opis procesu w tabeli, który moim zdaniem jest zupełnie niezarządzalny. Nie wiem, co w takim opisem można w dyplomie zrobić. Te tabele są w standardzie, nie ma powodu dawać to całości tych opisów. Tematem dyplomu jest zarządzania dowodami argumentacji bezpieczeństwa, więc opis procesu powinien być w kontekście celu dyplomu. Żeby do tego podejść, trzeba uporządkować czym jest argumentacja bezpieczeństwa (czy ogólniej wiarygodności), w których działaniach procesu jest stosowana, a potem do czego służą dowody i jak w tych procesach są stosowane.  
Spis treści proponowany w konspekcie nie jest może idealny, ale opisuje niezły rozdział:  
    Podrozdział 1.2 Zarządzanie materiałem dowodowym w cyklu życia systemu     <9 stron>  
Czyli na 9 stronach miałby się zmieścić opis cyklu życia i jeszcze co w tym cyklu życia dzieje się z dowodami.  
Ale zacznijmy od powiedzenia, czym są te dowody. Proszę więc zacząć od uporządkowania pojęć.  
---------

1. proszę stosować dokument do wymagań edycyjnych ETI, w tym marginesy stron i formatowanie stron, styl numeracji odwołań w spisie literatury (odwołanie to numer w nawiasie kwadratowym, a nie numer przypisu)

2. We wstępie proszę podać przynajmniej cel dyplomu.

Cel z opisu tematu dyplomu był następujący: 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 miedzy innymi zarządzanie zakresem, klasyfikacją, statusem oraz zmianami. Opracowany proces będzie podlegał walidacji poprzez analizę scenariuszy zdefiniowanych dla wymagań.

Cel może zostać trochę zmodyfikowany, ale warto to mieć cały czas obecne w dyplomie.

We wstępie musi być akapit rozpoczynający się od słów "Celem dyplomu jest ..."

może warto wprowadzić pojęcie "bezpieczeństwo", "ryzyko" czy "hazard"?

- co to są "roszczenia"?

Proszę uporządkować rozdział 2, gdzie jest opisane co to jest argumentacja wiarygodności systemu (system assurance case) - dokładnie takie pojęcie jest w tytule dyplomu.

Gdy będzie opisane co to jest assurance case (safety case), a w nim postulat (claim), strategia argumentacji i dowody (evidence), to będzie można iść dalej z dyplomem.

rozdział nie opisuje jak się mają dowody do argumentacji bezpieczeństwa.

Opisując czym jest argumentacja proszę też powołać się na model argumentacji Toulmina (Toulmin's Argument Model) - to jest podstawowy model argumentacji, który jest rozszerzany o dowody (evidence).

Ale proszę nie rozbudowywać za mocno rozdziału 2 - nie ma to być długi rozdział, ma tylko konkretnie opisywać pojęcia stosowane w dyplomie.Jak będziemy mieli uporządkowany rozdział 2, to przejdziemy do uporządkowania struktury dyplomu i wypełniania kolejnych części.

------------------  
jako diagram dekompozycji rozumiem prostu podział system na komponenty. Trzeba te komponenty wyliczyć i nazwać.Jeżeli mówimy o modelach jak w UML, to może to być model klas albo model pakietów albo model przepływu danych.Diagram może być mniej lub bardziej formalny, ważne jest konkretne nazwanie komponentów i identyfikacja połączeń pomiędzy nimi.Poniżej kilka grafik z netu.  
-----------------

Co do dokumentu, to opis ABS jest szczegółowy, później nam wyjdzie na ile te informacje będą używane.  
Pisząc dyplom proszę raczej patrzeć co jest potrzebne do napisania (czyli co będzie wykorzystane w innych rozdziałach).  
W kolejnych krokach proszę o dodanie tekstu w sekcjach:  
- 2.1 - krótki opis pojęć, które będą potem stosowane w analizie bezpieczeństwa systemu (czyli ABS)  
- w 3.3 dodać prosty diagram dekompozycji analizowanego systemu (to będzie potrzebne do analizy bezpieczeństwa)  
- w 3.4 opisać (na razie szkic) analizę bezpieczeństwa, czyli w uproszczeniu:  
   - jakie hazardy  
   - jakie ich przyczyny (opisane odwołując się do elementów z modeli dekompozycji systemu)  
   - jakie zabezpieczenia i co powinno być testowane w systemie przed przekazaniem do użytkowania  
------------------  
wyjaśniając:  
1) część procesów jest zgodna i była już opisana, bo zarówno autoSPICE, jak i japoński ESPR bazują na tym samym standardzie ISO 12207.  
W dyplomie można napisać, że są różne procesy, ale należy używać tylko jeden, czyli albo ESPR albo autoSPICE.  
Obszary SYP, SWP i SUP w ESPR odpowiadają (mniej więcej) obszarom SYS, SWE i SUP w atoSPICE.  
Inne obszary (w SPICE) nie są prawdę mówiąc istotne dla wykazywania bezpieczeństwa.  
Moja uwaga do dyplomu brała się stąd, że w sekcji 3.5 najpierw są dwie strony o automotiveSPICE, a potem nagle jest rysunek 11 opisany jako "rozszerzony schemat [...] automotive SPICE", a w rzeczywistości ESPR to nie jest rozszerzenie autoSPICE, tylko to jest inny standard procesów. W dokumencie ESPR nie znalazłem informacji, że to jest rozszerzenie autoSPICE.  
To są dwa różne standardy. Oba bazują na procesach ISO 12207, więc są podobne, ale to są dwa różne standardy.

Należy wybrać JEDEN standard i w sekcji 3.5 pisać o jednym.  
Może zostać ESPR (wybór japońskiego podejścia trochę dziwi, choć może bliżej Panu do Toyoty czy Hondy).  
Jeżeli mialby to być autoSPICE, to obszary SYS, SWE i SUP są wystarczające do opisania w dyplomie (o innych można tylko wspomnieć, że są)  
2) jeżeli chodzi o polską terminologię, to tu jest kiepsko. Można stosować dowolne publikacje, jak podana przez Pana.  
AutoSPICE ma aneks C z definicjami pojęć, ale mało jest tu zagadnień bezpieczeństwa.  
Norma ISO 26262 ma część z terminologią bezpieczeństwa dla sektora automotive, ale nie mamy tej normy na ETI. Proszę zajrzeć do specyfikacji EAST-ADL: <http://www.east-adl.info/Specification/V2.1.12/EAST-ADL-Specification_V2.1.12.pdf> Tam w sekcji 17 jest model pojęć dla bezpieczeństwa. Model zawiera pojęcia takie jak hazard czy safety requirement. To są pojęcia bazowe. Nie będziemy stosować EAST-ADL w dyplomie, ale warto znać wybrane pojęcia tam stosowane. Jeżeli chodzi o metody analizy ryzyka, to autoSPICE w MAN.5.BP4 zaleca m.in. FTA i FMEA. To podstawowe metody analizy bezpieczeństwa.

//komunikacja z dnia 04.10.2018

* dobrze, że widać strukturę całego dyplomu, jest całkiem fajna
* fajny jest rozdział o safety case, w szczególności rys. 2.1 z Eurocontrol pokazuje powązanie celu (top level claim) z dowodami, warto podkreślić, że zwykle jest wiele poziomów dekompozycji
* opis systemu (jak na razie, to rys. 3.5) powinien być spójny z poziomem szczegółowości analizy bezpieczeństwa, a w analizie (tabela 3.1) są elementy, których nie ma w modelu systemu, np. cylinder główny
* analiza bezpieczeństwa w tabeli 3.1 to bardzo dobry krok, dobrze byłoby tylko trochę to uszczegółowić. Na przykład czy jest tylko jeden rodzaj awarii sterownika "nieprawidłowa kalibracja"?
* proszę o zrobienie trochę dokładniejszej analizy w tabeli 3.1
* proszę o zapoznanie się z pojęciami takimi jak fault, failure, hazard - dobrze byłoby je stosować
* gdy tabela 3.1 będzie kompletna, dla każdego zdarzania bezpiecznego proszę określić:
  + jakie są zabezpieczenia, aby nie występowało (niezawodność elementu, okresowe przeglądy i wymiany)
  + jak diagnozować i wykrywać awarię
  + jakie działania wykonywać, gdy awaria jest wykryta
* jak to będzie gotowe, to w łatwy sposób przejdziemy do budowy argumentacji bezpieczeństwa dla ABS

//Kontekst: jesteśmy wytwórcą układów ABS, dostarczamy komponenty, nie budujemy całego samochodu

//jakie artefakty (dokumenty zarządcze i techniczne, modele, ….) powstają w cyklu życia