VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ
DEPARTMENT OF COMPUTER SYSTEMS

ANALÝZA RIZIK SPOJENÝCH SE SAMOČINNĚ ŘÍZENÝMI VOZIDLY

RISK ANALYSIS OF SELF-DRIVEN VEHICLES

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE **Bc. FILIP WEIGEL**
AUTHOR

VEDOUCÍ PRÁCE **Ing. JOSEF STRNADEL, Ph.D.**
SUPERVISOR

BRNO 2022

Vysoké učení technické v Brně
Fakulta informačních technologií

Ústav počítačových systémů (UPSY) Akademický rok 2021/2022

Zadání diplomové práce

Student: **Weigel Filip, Bc.**
Program: Informační technologie a umělá inteligence
Specializace: Počítačové sítě
Název: **Analýza rizik spojených se samočinně řízenými vozidly**
Risk Analysis of Self-Driven Vehicles
Kategorie: Modelování a simulace
Zadání:

1. Zdokumentujte problematiku související s oblastí samočinně řízených vozidel a oblastí analýzy rizik; proveďte detailní rešerši současného stavu a trendů v těchto oblastech.
2. Proveďte detailní rešerši v oblasti prostředků výpočetního modelování systémů a analýzy jejich vlastností.
3. Připravte sadu výpočetních modelů samočinně řízených vozidel a jejich okolí, která umožní analyzovat dopad způsobu řízení vozidel (ovlivněného např. stupněm autonomie řízení či sběrem/zpracováním dat z čidel) a stavu/vlastností jejich podčástí (např. čidel, světel, brzdné soustavy, kol) v předem určených situacích (např. parkování, křižovatky či dálnice) a podmínkách (např. povrch vozovky, počasí či intenzita, dynamika a druh provozu).
4. Navrhněte mechanismus analýzy rizik nad sadou modelů z bodu 3, zvolte prostředky a metody vhodné pro jeho implementaci. Představte sadu situací a podmínek, ve kterých plánujete provádět analýzu rizik nad sadou modelů z bodu 3.
5. Mechanismus analýzy rizik navržený v bodě 4 implementujte.
6. S pomocí sady modelů z bodu 3 ověřte schopnost implementovaného mechanismu analyzovat rizika v několika různých situacích a podmínkách z bodu 4; identifikujte a daty dostatečně podložte zjištěná rizika, vhodně je prezentujte, interpretujte a diskutujte možnosti jejich snížení.
7. Diskutujte a zhodnoťte vlastnosti a praktickou využitelnost implementovaného mechanismu a navrhněte možné směry pokračování v řešeném tématu.

Literatura:

- Zio, E. Pedroni, N.: Uncertainty Characterization in Risk Analysis for Decision-Making Practice, 2012, 51 s.
- Bhavsar, P. et al.: Risk Analysis of Autonomous Vehicles in Mixed Traffic Streams. Transportation Research Record, Vol. 2625, No. 1, Jan. 2017, s. 51-61.
- Hansson, S.O., Belin, M., Lundgren, B. Self-Driving Vehicles-an Ethical Overview. Philosophy and Technology, 2021, 26 s.

Při obhajobě semestrální části projektu je požadováno:

- Splnění bodů 1 až 4 zadání.

Podrobné závazné pokyny pro vypracování práce viz https://www.fit.vut.cz/study/theses/

Vedoucí práce: **Strnadel Josef, Ing., Ph.D.**
Vedoucí ústavu: Sekanina Lukáš, prof. Ing., Ph.D.
Datum zadání: 1. listopadu 2021
Datum odevzdání: 18. května 2022
Datum schválení: 29. října 2021

Abstrakt

Cílem práce bylo navrhnout a implementovat systém pro analýzu rizik v samočinně řízených vozidlech. Práce se zaměřila návrh a implementaci systému pro řešení analýzy rizik založené na modelech. Požadavkem na systém byla jeho flexibilita a robustnost. Návrh analýzy rizik byl nejprve předveden v teoretické rovině a poté implementován v modelech systémů ABS a ESP v prostředí *UPPAAL*. Systém byl dále podroben různým experimentům a testům pro ověření jeho funkcionality. Na implementovaném systému byly vykonané experimenty. Experimenty byly přínosné a systém pro analýzu rizik korektně vyhodnocoval scénáře selhání a adekvátně na vzrůstající riziko reagoval. Výsledky experimentů byly prezentovány na grafech s komentářem daných scénářů selhání.

Abstract

The goal of this thesis was to design and implement system for risk analysis in self-driving cars. This thesis focused on design and implementation of system for risk analysis in models. One of the requirements for the system was to be flexible and robust. Design of the risk analysis was presented at theoretical level and then implemented in models of ABS and ESP systems in *UPPAAL* environment. The system was then tested via multiple experiments. The experiments were beneficial and the system for risk analysis correctly evaluated failure scenarios with adequate response to the rising level of risk. Experiment outputs were then presented at graphs with comment to each failure scenario.

Klíčová slova

analýza rizik, samočinně řízená vozidla, samočinné řízení, systém, modelování, počítač, ABS, ESP, riziko, rizika, vozidlo, vozidla, automobil, UPPAAL, model, komponenta, senzor, selhání, scénář selhání, parkování, hodnocení rizik, pravděpodobnost, porucha, SIMLIB, Dymola, Modelica, pravděpodobnostní hodnocení rizik, čidlo, redundantní, redundance, simulace, simulování, návrh analýzy rizik, implementace analýzy rizik

Keywords

risk analysis, self-driving cars, self-driving, system, modeling, computer, ABS, ESP, risk, cars, car, UPPAAL, model, component, sensor, failure, failure scenario, parking, risk assessment, probability, fault, SIMLIB, Dymola, Modelica, probabilistic risk assessment, redundant, redundancy, simulation, simulating, risk analysis design, risk analysis implementation

Citace

WEIGEL, Filip. *Analýza rizik spojených se samočinně řízenými vozidly.* Brno, 2022. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Josef Strnadel, Ph.D.

Analýza rizik spojených se samočinně řízenými vozidly

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana Ing. Josefa Strnadela Ph.D. Uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....
Filip Weigel
15. května 2022

Poděkování

Tímto odstavcem bych chtěl vyjádřit srdečné poděkování svému vedoucímu diplomové práce panu Josefu Strnadelovi za jeho věcné rady, ochotu a podporu při vypracovávání této práce.

Dále bych chtěl poděkovat své mamince Božence, babičce Drahušce a tatínkovi Petrovi. Jejich morální podpora, fyzická přítomnost a vložená důvěra mi byla velkým pomocníkem při studiu a následné tvorbě této práce. Taktéž bych chtěl poděkovat své sestře Kláře, bráchovi Péťovi a kamarádům za podporu.

V poslední řadě bych chtěl poděkovat své přítelkyni Sabíně za morální podporu. Rovněž se podílela významnou mírou na skvělé atmosféře při studiu a při tvorbě této práce.

Obsah

Kapitola 1

Úvod

Osobní automobily slouží lidstvu již více než 100 let. Člověk již od doby návrhu a konstrukce prvních počítačů přemýšlel nad tím, že počítače budou lidem v budoucnosti sloužit. Díky stále se zmenšujícím součástkám počítačů společně s postupným nárůstem výkonu tito digitální pomocníci pronikli do všech odvětví průmyslu, automobilového průmyslu nevyjímaje. Bez počítače by dnešní moderní osobní automobil nemohl ani nastartovat. Počítače ovládají spalování, převodovku a taktéž různé podpůrné systémy jako například ABS, ESP, systém pro hlídání mrtvého úhlu, tempomat, dokonce již automobily umí i samy zaparkovat.

S rostoucí složitostí všech systémů roste taktéž výpočetní náročnost a z toho vyplývající rizika. Práce se zabývá analýzou rizik v podpůrných systémech samočinně řízených vozidel. Analýza rizik je důležitá zejména z důvodu, že vyhledává potenciální nebezpečí pro daný systém pomocí různých metod a snaží se pro každé možné eventuální nebezpečí se snaží jej úplně eliminovat, případně redukovat dopady nebezpečí.

V kapitole 2 se práce zaměří na teoretický okruh simulace a modelování, poté budou prezentovány samočinně řízená vozidla a jejich komponenty. Dále bude prezentována teorie analýzy rizik. V analýze rizik půjde zejména o možné přístupy, metodu pravděpodobnostního hodnocení rizik a taktéž hlavní kroky při analýze rizik.
3. kapitola práce předvede prostředky pro modelování systémů včetně nástrojů pro modelování. Následovně bude práce rozebírat dostupné modely a zaměří se na jejich analýzu v prostředí *UPPAAL*.
Čtvrtá kapitola 4 bude mít za úkol představit navržený systém pro analýzu rizik v modelech, poté bude obsahovat proces hodnocení rizik v systémech ABS a ESP a rovněž bude prezentovat upravené modely ABS a ESP s implementovaným systémem pro analýzu rizik.
Předposlední kapitola 5 bude prezentovat výsledky analýzy rizik v obou systémech na grafech simulací v prostředí *UPPAAL*, společně s komentářem daných situací a okolností daného experimentu.
Poslední kapitola 6 provede zhodnocení implementace systému analýzy rizik, ohlédne se za výsledky a vydá doporučení na základě zkušeností autora po návrhu a implementaci systému pro analýzu rizik.

Kapitola 2

Rozbor řešené problematiky

2.1 Modelování a simulace

Přehled pojmů

V této kapitole budou prezentovány základní pojmy, principy a metody, které se využívají v oboru modelování a simulace na digitálních počítačích. Dále proč je výhodné vytvářet počítačové modely, problémy spojené s modely, alternativní přístupy atp. [37].

Vytváření modelů je velmi rozšířenou činností člověka. Obecně lze říct, že představa světa je modelem reality (okolní svět, který lze zkoumat). Znalosti jsou založeny na experimentování a pozorování čili to jsou výsledky mnoha experimentů s reálnými systémy. Při modelování je nutné vycházet z informací o systému, které jsou dostupné. Model, který vznikne, reprezentuje znalosti o systému z pohledu, které jsou zkoumané. Model obvykle obsahuje pouze část popisu celého systému, která je pro daný účel podstatná. Vzhledem k tomu, že model vždy vzejde vždy pouze ze znalostí, které jsou neúplné, lze modelovat pouze to, co lze pochopit a popsat [37].

Simulační modelování je transformace znalostí strojově neproveditelných na reprezentaci proveditelnou na počítači s různými úrovněmi abstrakce daného systému.

Experimentování v reálném světě je vždy zatíženo chybami měření a ostatními faktory, které mohou způsobit problémy při interpretaci výsledků. Někdy jsou experimenty s reálnými systémy neekonomické, nebezpečné, nebo neproveditelné, a proto se metody počítačové simulace hojně využívají.

Obecně je nutné neustále konfrontovat znalosti získané z reality a ze simulačního modelu a kontrolovat tak jeho platnost. Ověřování modelu je proces, ve kterém je zapotřebí dokázat, že model odpovídá modelovanému systému [37].

Lze tedy říct, že veškeré znalosti světa představují model, který odráží úroveň poznání [37].

- **Systém** lze definovat jako soubor elementárních částí - prvků systému - mající mezi sebou jisté vazby, které lze vnímat jako propojení prvků. Systémy lze rozdělit do několika kategorií dle různých kritérií. Podle existence lze systémy dělit na:
  - reálné systémy - založené na skutečném problému (počasí, uhlíková stopa, ...).
  - nereálné systémy - fiktivní, neexistující systémy. Hojně jsou využívané například v počítačových hrách.

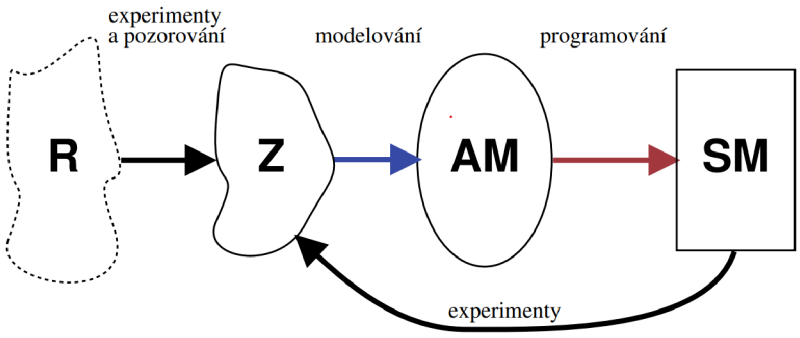
  nebo podle stavu systému v průběhu simulace:
  - statické systémy - při běhu simulace nemění svůj stav v čase.
  - dynamické systémy - při běhu simulace mění svůj stav.

  Z hlediska modelování a simulace jsou preferovanější systémy ty, které umožňují dynamické změny. Jako jednoduchý dynamický systém lze uvést zastávku MHD, přicházející cestující na zastávku, příjezd autobusu, nástup cestujících a odjezd autobusu [37].
- **Model** je napodobenina systému jiným systémem například počítačovým programem. Z hlediska modelu je důležité, aby napodoboval všechny klíčové vlastnosti systému na určité úrovni abstrakce. Modelem může být například diferenciální soustava rovnic, která popisuje chování rakety při letu a nebo ekvivalentní blokové schéma [37].
- **Abstrakce** je pohled na problém reálného světa a jeho počítačová reprezentace. Úroveň (míra) abstrakce poté udává, jak moc je model vzdálen od reálného světa. Hlavním faktorem je složitost a náročnost implementace. Je to tedy schopnost zanedbat/zjednodušit aspekty řešeného problému, které nejsou kritické z hlediska modelovaného problému. Pokud se model například zabývá problematikou kapacity dopravy ve městě, tak není nezbytně nutné model autobusu modelovat exaktně se všemi složitými fyzikálními jevy. Autobus lze poté namodelovat jako „krabičku“ s určitou rychlostí, poruchovostí atd... [32].
- **Modelování** je postup vytváření modelů na základě znalostí daného problému při zvolené úrovni abstrakce. Jedná se o nejnáročnější proces, který vyžaduje znalosti z více oborů. Kvalita výsledného modelu je kritická pro výsledky získané experimentováním s modelem [37].
- **Simulace** je proces, jehož cílem je získat znalosti o systému. Znalostí se získávají experimentováním s výsledným modelem. Ne každý model je pro simulaci vhodný. Pro získání důležitých informací o systému je třeba provádět vícenásobné simulace s různou počáteční konfigurací [37].

Princip modelování, simulací a oblasti použití

Jak již bylo popsáno v předešlé části, hlavním cílem simulace je zjištění nových poznatků o modelovaném systému. Pro provádění simulací je nezbytně nutné vytvořit vhodný model systému při určité úrovni abstrakce.

- **Abstraktní model** je první instancí, která neobsahuje všechny znalosti o modelovaném systému. Důležité je vybrání vlastností, které jsou pro model relevantní. Tím je dosaženo zjednodušení modelu na optimální úroveň.
- **Simulační model** je vytvořen z abstraktního modelu a jedná se o jeho počítačovou implementaci. Závažné je, aby simulační model obsahoval všechny vlastnosti abstraktního modelu. Hlavním rozdílem je, že s abstraktním modelem nelze provádět simulace. Simulační model je spustitelný a dle počátečního stavu, vstupů parametrů produkuje výstupy.
- **Simulační experimenty** jsou opakovaná spuštění simulačního modelu s odlišnými vstupy, stavy a parametry. Výsledkem experimentů jsou informace o chování systému při různých situacích, ze kterých lze získat nové znalosti [37].



Obrázek 2.1: Proces transformace znalostí na simulační model.[1]

Pro přiblížení lze uvést několik příkladů, ve kterých se dají techniky modelování a simulace využít [37]:

- **Automobilový průmysl** - crash testy vozidel, modely systémů ABS, ESP.
- **Doprava** - model hromadné dopravy, uhlíkové stopy.
- **Ekonomie** - model trhu s akciemi, kurzů.
- **Fyzika** - model šíření světla, tření.
- **Hvězdářství** - model galaxie, planet.
- **Kinematografie** - vizuální efekty.
- **Chemický průmysl** - model látek, reakcí, plynů.
- **Meteorologie** - modely pro předpověď počasí.
- **Vzdělávání** - model letadla, hry.

[1] https://wis.fit.vutbr.cz/FIT/st/cfs.php.cs?file=%2Fcourse%2FIMS-IT%2Ftexts%2Fopora-ims.pdf

Výhody a nevýhody simulačních metod

Výhod modelů

- **Cena:** je levnější vyrobit model automobilu, s jeho pomocí experimentovat a získávat nové znalosti, než ničit nově vyrobené automobily připravené k prodeji.
- **Rychlost:** v modelech je možné čas zrychlit, či naopak zpomalit pro účely experimentů. Zpomalení času lze využít při zkoumání deformační zóny automobilu, zrychlení při simulacích vesmíru, planet, růstu rostlin.
- **Bezpečnost:** v případě selhání simulačního modelu nehrozí žádné nebezpečí. S jejich pomocí lze simulovat například jaderný výbuch, či šíření epidemie.
- **Jediný způsob:** pro experimentální účely lze modelovat i simulovat velmi nepravděpodobné jevy, jako například srážka galaxií [37].

Nevýhody modelů

- Problémy s **validací modelu**.
- **Vysoká náročnost** na znalosti.
- **Výpočetní náročnost**.
- **Nepřesnost** modelu [37].

2.2 Samočinně řízená vozidla

V kapitole bude představena historie autonomních vozidel, rozdělení typů automobilů dle míry interakce s asistenčními systémy. Dále komponenty a z nich složené systémy, které jsou nezbytné pro určitý stupeň autonomie vozidla, současné trendy v samočinně řízených vozidlech a vyhlídky do budoucnosti.

Historie

Pravděpodobně prvními samočinně řízenými vozidly, které měly nějakou formu autonomního řízení byly plachetnice. Využívaly automatické kormidlo, které bylo spojeno s něčím jako korouhvička a díky němu plavidlo zůstalo na stejném kurzu i při měnících se větrných podmínkách [40].

V 60. letech 19. století vynalezl Robert Whitehead samo-naváděné torpédo. Využil pro udržování hloubky a kurzu revoluční systém, který nazval „tajemství“. V letadlech se první „autopilotní“ systém poprvé objevil v 10. letech 20. století. Využíval ukazatel výšky a směr letu pomocí kterého hydraulicky ovládal výškovku a kormidlo (křidélka neovládal) [40].

Za druhé světové války došlo k dalšímu vylepšení naváděcích systémů. Torpédo, vynalezené Robertem Whiteheadem, doznalo dalšího vylepšení. Tím byl sonar, díky kterému se mohlo zaměřit na svůj cíl. Dalším příkladem mohou být německé rakety „Vergeltungswaffe“, známějším pod názvy „V1/V2“. Z Francie byly schopné doletět do Londýna, kde posléze explodovaly. Naváděné byly pomocí gyroskopů, které ji udržovaly v kurzu. Průkopnická balistická střela V2 byla prvním lidským artefaktem ve vesmíru [40].

Automobilový sektor dlouho zaostával za ostatními oblastmi v autonomním řízení. Hlavním důvodem je nebývalá složitost celého systému. Zatímco letadla létají ve výškách kolem 11 kilometrů nad zemí a lodě plují po pustých oceánech a mořích, tak automobilový průmysl se musí potýkat s složitějším světem. Městské ulice plné lidí, semaforů, ostatních řidičů, kteří se občas mohou chovat nevyzpytatelně atp. Všechny tyto nástrahy se měří v metrech, centimetrech nebo milimetrech. Velkou část nebezpečí pro automobilový průmysl skýtá také to, že silnice byly (jsou) úzké, špatně značené a většinou určené jen pro lokální cestování [40].

Pokud je vzat v úvahu relativně jednoduchý hmyz, jako například šváb obecný, tak i jeho nervový systém je schopen procházet složitým prostředím poměrně velkou relativní rychlostí. Šváb, který by byl velký jako osobní automobil by se otáčel, uhýbal, běžel rychlostí přes 300 km/h. Poskytnout automobilům jen zlomek těchto navigačních schopností trvalo automobilovému průmyslu 50 let. Hlavnímu pokroku se dostalo díky číslicovým počítačům. Jedním z prvních použití byly naváděcí počítače pro jaderné střely v období studené války. Zvýšené rozpočty znamenaly, že se konstruktéři mohli uchýlit k polovodičovým součástkám, namísto křehkých elektronek [40].

Obrázek 2.2: Zabudovat do silnice ocelový drát, který by sledovaly zabudované magnety v automobilu. Zde vyobrazena „Autonomous Highway System“, jedna z vizí 50. let 20. století.[3]

V 60. letech 20. století začali nadšenci do umělé inteligence (AI) na digitálních počítačích snít o automobilech, které by byly dostatečně chytré, aby se dokázaly samostatně pohybovat v běžných ulicích. Výzva to byla obrovská. V podstatě šlo o reverzní inženýrství příslušných systémů v pohybujícím se zvířeti, jako je šváb:

1. Snímání
2. Zpracování (modelování vnějšího světa, rozhodování)
3. Reakce

První a poslední krok byl proveditelný pomocí již tehdy známých technologií. Neznámou částí bylo zpracování a mezi tím potřebná strojová inteligence. Velkou částí této výzvy byla interpretace. Automobil, jehož „mentální“ model si splete člověka s odrazem světla v louži po dešti může být skutečně nebezpečná [40].

Raní průkopníci těchto technologií snili o průlomech, kdy do konce 2. tisíciletí přinesli roboty podobné lidem. Skutečný pokrok byl ale spíše postupný než revoluční. Německý průkopník Ernst Dickmanns v 80. letech 20. století pomocí dodávky Mercedes-Benz ujel autonomně stovky kilometrů po dálnici, což byl překvapivý výkon, zvláště s přihlédnutím na výpočetní výkon dostupný v 80. letech [40].

[3] https://computerhistory.org/wp-content/uploads/2019/08/where-to-4.0_RCA_automated_highwaylores-1024x742.jpg

Obrázek 2.3: Dickmannsova laboratoř byla průkopníkem praktické samořídící technologie. Tato dodávka testovala tři generace systémů.[5]

Stupně autonomie

Autonomní vozidlo na první pohled vypadá stejně, jako vozidlo obyčejné. Je složeno ze stejných součástek, příkladem může být motor, převodovka, diferenciál, kola, pneumatiky, brzdy atd. Zásadním rozdílem je, že takové vozidlo ke svému provozu v nejlepším případě nepotřebuje žádného řidiče. Vozidlo, které tuto funkcionalitu splňuje potřebuje podstatně více senzorů, čidel a informací o svém okolí, o svém stavu, rychlosti, informací obecně. Data jsou vyhodnocována ve výpočetní jednotce, která tyto data sesbírá, vyhodnotí a s jejich pomocí je schopna ovládat natočení kol, škrtící klapku motoru, plyn, jednotlivé brzdy atp.

Automobily jsou zpravidla děleny do šesti kategorií dle stupně autonomie (aktuálně jsou dostupná vozidla mezi 2-3. úrovní) [1]:

0. **Žádný stupeň automatizace** - většina vozidel v dnešní době je stále na úrovni 0, což znamená manuální kontrolu. Člověk řídí vozidlo a má jej plně pod kontrolou. I takové vozidlo ale může mít určitý druh asistenta pro řízení, příkladem mohou být systémy rozpoznávání značek atp.

1. **Podpora řidiče** - nejnižší stupeň autonomie. Automobil obsahuje jeden systém, který pomáhá řidiči při jízdě (zatáčení, zrychlování, ...). Příkladem takového systému může být adaptivní tempomat pomáhající řidiči udržet nastavenou vzdálenost za autem před ním. Kvalifikuje se stále do první úrovně, jelikož člověk je stále zodpovědný za ostatní aspekty řízení, jako zatáčení atp.

2. **Částečná automatizace** - vozidlo může kontrolovat řízení a akceleraci/deceleraci. Auto zvládne stejné funkce jako o úroveň níž, ale s tím rozdílem, že je nyní může kombinovat. Člověk ale v jakoukoliv chvíli může převzít řízení a občas je tato interakce dokonce vyžadována. Systémy od firem Tesla (Autopilot) a Cadillac (Super Cruise) se kvalifikují jako úroveň 2.

3. **Podmíněná automatizace** - mezi úrovní 2 a 3 je z technologického hlediska obrovský skok, z hlediska lidského malý, či zanedbatelný. Vozidlo 3. úrovně již má schopnost „detekce prostředí“ a může učinit informované rozhodnutí, třeba zrychlit kolem pomalu jedoucího vozidla. Pokud systém nebude schopný některý úkol splnit, tak řidič musí převzít kontrolu nad vozidlem.

[5] https://computerhistory.org/wp-content/uploads/2019/08/where-to-vamors-merge-1024x351.jpg

4. **Vysoká automatizace** - klíčovým rozdílem je, že vozidlo 4. úrovně může zasáhnout v případě nečekané události, nebo selhání některého ze systémů. V tomto ohledu auta ve **většině** případů nepotřebují lidskou interakci při reakci na hrozící nebezpečí. Řidič stále může převzít kontrolu nad vozidlem.

5. **Plná automatizace** - řidič již není potřeba a „dynamická úloha řízení“ je eliminována. Autonomní vozidla 5. úrovně neobsahují pedály ani volant. Vozidlo je již schopno jet kamkoliv a provádět stejné činnosti jako zkušený lidský řidič. Plně autonomní vozidla jsou v testování po malých skupinkách po světě, ale žádný z nich není dostupný pro širokou veřejnost.

2.2.1 Komponenty autonomních vozidel

Jak již bylo předesláno, vozidla s autonomním řízení využívají nespočet senzorů, čidel a systémů, aby získaly přehled o svém okolí. Komponenty a z nich složené systémy budou prezentovány v následující sekci.

LIDAR

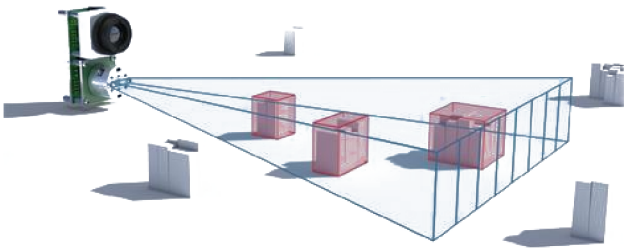
Zkratka „LIDAR“ je odvozena ze slov **Li**ght **D**etection **A**nd **R**anging. Základní koncept Lidaru se datuje do roku 1930, kdy za pomocí výkonných reflektorů společnost EH Synge zkoumala atmosféru. Samotný Lidar vznikl v raných 60. letech 20. století, krátce po vynálezu laseru díky kombinaci laseru a schopností vypočítat vzdálenost měřením času návratu signálu pomocí snímačů a elektronických součástek. První aplikací byly výzkumy atmosféry, kterou využívalo americké Národní centrum pro výzkum atmosféry. Dalším využitím se stala mise Apollo 15 v roce 1971, kdy astronauti využívali laserový výškoměr pro mapování povrchu Měsíce a díky této misi se dostal Lidar do podvědomí veřejnosti [29].

Lidar využívá ke svojí činnosti světlo ve viditelném spektru, v infračerveném, či ultrafialovém záření. Zvládne zaměřit i materiály jako horniny, chemické sloučeniny, nekovové předměty, dešťové srážky, aerosoly atp. Velmi úzký laserový paprsek je schopen zjistit fyzické vlastnosti ve velmi vysokém rozlišení. Lidary, které jsou „běžně dostupné“ využívají lasery, které jsou bezpečné pro oči. Díky tomu mohou být používány bez jakýchkoliv bezpečnostních opatření [29].

K velké popularitě Lidaru dopomohl také fakt, že je čím dál častěji nasazován v autonomních vozidlech. Zde plní činnost detektoru překážek. Implementován je jako rotující snímač, který mapuje okolí kolem vozidla. Data z Lidaru jsou zasílána řídící jednotce, která z nich vytvoří mapu prostředí, ve kterém se vozidlo nachází. V mapě jsou viditelné potencionální překážky a pozice vozidla vůči nim. Data jsou průběžně vyhodnocována softwarově a vozidlo vyhodnocuje situaci a predikuje možná rizika [29].

Spolu se softwarem dokáže systém nejen detekovat překážky v okolní, ale taktéž analyzovat potencionální dynamiku překážky, příkladem velikost, rychlost a směr pohybu. Na základě dostupných dat může řidiče upozornit, či situaci vyřešit úhybným manévrem, brzděním atp. Je tedy jedním z bezpečnostních systému. Jejich úkolem je sledovat okolní svět. Tato technologie přispívá taktéž k vyššímu komfortu a bezpečnosti. Pomáhá sledovat slepé úhly, pomáhat při parkování, varovat před srážkou při sepnutém adaptivním tempomatu

atp. Je zřejmé, že svojí přítomností ve vozidle může pomáhat velkému množství asistenčních systémů [29].



Obrázek 2.4: Základní funkcionalita Lidaru.[6]

Jeho hlavní výhodou je rychlost a zmíněná přesnost. Světlo a rádiové vlny jsou asi milionkrát rychlejší než zvuk, což je hlavní výhodou proti sonaru. Taktéž díky této vlastnosti je Lidar schopen vysílat a přijímat data z obrovského počtu impulsů. Získány jsou aktuálnější a přesnější data. Nevýhodou je stále vysoká cena (v řádech desítek tisíc až miliónů Kč.) a stálý vývoj Lidaru [29].

V roce 2015 ukázal bezpečnostní technik Jonathan Petit ze společnosti Security Innovation, že i relativně lacině a jednoduše lze Lidar zmást. Pomocí drobného laseru z laserového ukazovátka a mikropočítače Raspberry Pi sestrojil laserovou rušičku, která zmátla i komerční Lidar IBEO Lux, jenž na konferenci sloužil jako modelový příklad. Pokud by útočník s tímto jednoduchým systémem byl schopen paralyzovat Lidar v automobilech na silnici a zároveň by si koupil i GPS rušičku, tak by mohl poměrně jednoduchým a „levným“ způsobem paralyzovat část dopravy ve městě. V dnešní době zatím nic takového nehrozí, jelikož autonomní vozy netvoří velkou část dopravy. Bohužel v budoucnosti budou tyto „bizarní“ útoky automobilky a veřejnost trápit stále častěji. [24].

Radar

Slovo radar je odvozeno od **Ra**dio **D**etection **a**nd **R**anging. Jedná se o systém určený k hledání cílů, určení jejich polohy, případně i identifikaci. Mikrovlnná energie je vysílána v impulzech o jistém výkonu na určité frekvenci (MHz pro dlouhé vzdálenosti, desítky GHz pro krátké vzdálenosti), které jsou vyslány do prostoru pomocí antény. Odrazovým objektem může být vozidlo, letadlo, člověk atp. U obvyklých systémů horizontální anténa rotuje, což ale není podmínkou, protože fázované antény umožňují měnit směr vysílání a příjmu i bez pohybu. Moderní radar zpravidla využívá rotaci antény a zároveň ovlivňuje i hlavní svazek anténní vyzařovací charakteristiky [11].

Vyslané impulsy se šíří přibližně rychlostí světla. Narazí-li na předmět, tak se odrazí pod stejným úhlem, pod kterým na daný předmět dopadl. Pokud vyslaný impuls narazí na objekt v úhlu 90°, tak se odrazí tak, že se vrací přímo k anténě, která impuls vyslala. Odražené impulsy jsou přijímačem zpracovány a na indikátoru jsou viditelné. V případě, že objekt, na kterou vlna dopadá je přibližně stejných rozměrů jako vlnová délka vlny a objekt je vyroben z vhodného materiálu (kov), dochází k odrazu díky rezonanci elektromagnetického

[6] https://vtm.zive.cz/GetThumbNail.aspx?id_file=58156&width=500&height=281&q=80

vlnění a vlny se odráží zpět bez ohledu na úhel dopadu. Objekt poté zafunguje jako dipól a má efektivní odraznou plochu větší, než jsou jeho skutečné rozměry. Dosah radaru je dán výkonem vysílače, vyzářenou energií, která je dána charakteristikou antény, dále velikostí odrazné plochy, charakterem vysílaného signálu, útlumem prostředí a citlivostí přijímače. [11].

Speciálním případem radaru je radar se stálou vlnou. Negeneruje impulsy, ale stále vyzařuje, díky čemuž lze jednoznačně měřit vzdálenost, která je dána vlnovou délkou. Tento princip se využívá zejména při měření rychlosti (policejní radar RAMER), kde vzdálenost objektu není důležitá a rychlost se vypočítá podle Dopplerova jevu [11].

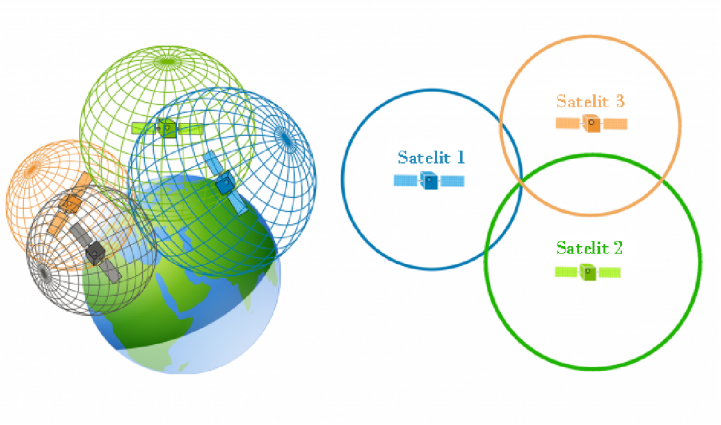
GPS

Global **P**ositioning **S**ystem je globální satelitní systém, který slouží k určení polohy, rychlosti a přesného času. V dnešní době je GPS pravděpodobně nejrozšířenějším polohovacím systémem na světě. Systém GPS lze objevit v automobilech, telefonech i chytrých hodinkách. Ke svojí funkci využívá satelity, přijímače a algoritmy určené k synchronizaci údajů. Satelitní systém je složen ze 24 satelitů umístěných v šesti orbitálních rovinách. Každá z rovin obsahuje čtyři satelity, které jsou umístěny v MEO (Medium Earth Orbit, 20 000 km nad Zemí) a pohybují se rychlostí 14 000 km/h [23].

Pro vytvoření 2D polohy na zemském povrchu jsou zapotřebí tři satelity. Za předpokladu, že přijímač má velmi přesné atomové hodiny, stačí k získání 3D polohy i nadmořské výšky satelity tři. Pokud přijímač atomové hodiny nemá (99.999% případů), tak se pro 3D polohu využije satelit čtvrtý. Získání polohy funguje pomocí techniky zvané trilaterace. Trilaterace se využívá k výpočtu polohy, rychlosti a nadmořské výšky. Občas dochází k záměně za triangulaci, ale triangulace se používá k měření úhlů, nikoliv vzdálenosti [23].

Každý satelit vysílá jedinečný signál, orbitální parametry a přesný čas z atomových hodin. Zachycený signál přijímačem GPS je použit k výpočtu vzdálenosti od zařízení GPS k satelitu. GPS zařízení poskytuje pouze informace o vzdálenosti od satelitu, proto signál z jednoho satelitu nestačí. Satelity nevydávají informace o úhlech, proto umístění může být kdekoliv na povrchu koule [23].

Pokud přijímač přijme signál z jednoho satelitu, dochází k vytvoření kruhu s poloměrem měřeným od zařízení GPS k satelitu. Dále po přijetí signálu z druhého satelitu dojde k vytvoření druhého kruhu a umístění se zpřesní průsečík dvou bodů, kde se kruhy protínají. Konečně s třetím satelitem lze určit polohu zařízení, protože zařízení je v průsečíku tří kruhu. Jelikož ve tři-rozměrném světě vytváří každý satelit kouli, nikoliv kruh, tak průsečík tří koulí vytváří dva průsečíky. Vybrán je bod blíže Zemi. S pohybem zařízení se mění poloměr. Při změně poloměru dojde k vytvoření nových koulí a jejich průsečíků. Opakovaným výpočtem je zjištěna nová pozice [23].



Obrázek 2.5: Ukázka výpočtu pozice pomocí GPS.[7]

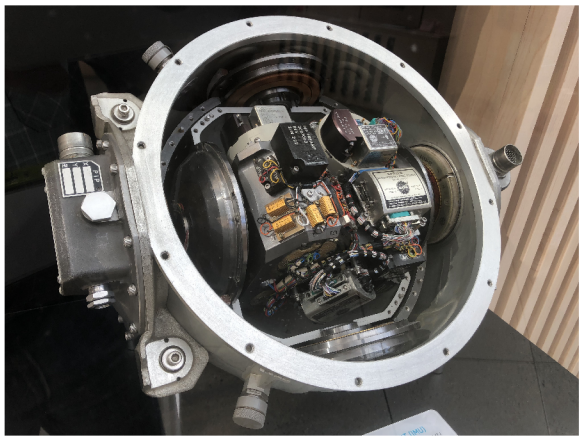
Inerciální měřící jednotka

Inerciální měřící jednotka (IMU) je elektronický systém. Pomocí kombinace gyroskopů a akcelerátorů podává informace o zrychlení a orientaci v prostoru. Akcelerometr je součástka pro měření zrychlení v jedné ose. Gyroskop je komponenta měřící otáčení v rovině. IMU vychází z klasické mechaniky, dle druhého zákonu, definovaný Isaakem Newtonem. Využívá skutečnost, že vnější síla působící na těleso způsobuje zrychlení, jenž je úměrně velké velikosti a směru výslednice daných sil. Systém IMU neustále zpracovává data o vektoru okamžitého zrychlení (pohyb objektu). Základem tohoto systému je měřící plošina, na níž je upevněna trojice navzájem kolmo orientovaných snímačů zrychlení a gyroskopy [39].

V navigačním systému jsou data z IMU zasílána do jednotky, která počítá orientaci, polohu a rychlost. Konkrétní implementace v letadle může být následující: letadlo, které se začne pohybovat po určitém směrovém vektoru. Z počátečních souřadnic x_0, y_0, z_0 a počáteční rychlosti $v_0 = 0m/s$ systém IMU změří zrychlení letadla $5m/s$ po dobu $1s$. Po půl vteřině systém vyhodnotí, že letadlo cestuje rychlostí $5m/s$ a je vzdáleno $2.5m$ od počátečních souřadnic x_0, y_0, z_0. Systém je tedy schopen i bez podpůrných systému jako například GPS zobrazit polohu letadla na mapě (pokud byla známa počáteční poloha). IMU může pracovat i v oblastech, kde je signál GPS nedostupný, což je jeho velká výhoda [39].

Hlavní nevýhodou v IMU je, že zpravidla trpí kumulovanou chybou. Systém neustále provádí výpočty s malými odchylkami a tyto malé odchylky vedou ke kumulativní chybě. Tuto chybu se dá taktéž nazvat jako „drift“ čili stále rostoucí rozdíl mezi skutečným umístěním a místem, které systém vypočítal. IMU může využít pro korekci driftové chyby systém GPS a korigovat svoji pozici [39].

[7] https://gisgeography.com/trilateration-triangulation-gps/

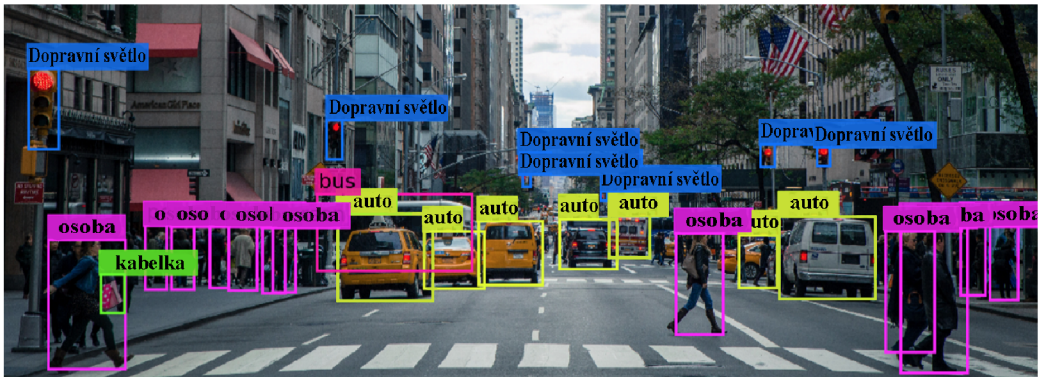


Obrázek 2.6: Inerciální měřící jednotka z kosmické lodi Apollo.[8]

Kamery

Nejen pro řidiče je zrak nejdůležitějším faktorem. Obraz z kamer umístěných na automobilu jsou taktéž skvělým vstupním parametrem pro jeho autonomii. Řidiči zadní nebo 360° kamery pomáhají při parkování, při eliminaci slepých úhlů atp. V autonomních vozidlech se využívají pro digitální mapování okolí. Díky technikám strojového učení lze z obrazu kamer získat podstatné informace. S jejich pomocí lze zjistit vzdálenost a velikost objektu, dále s použitím metod strojového učení klasifikovat objekty v obrazu dle skupin. Může se jednat o klasifikaci, zda objekt na obraze je podobný spíše na sloup veřejného osvětlení, než na sloup s dopravní značkou [38].

Kamery jsou tedy důležité pří detekci dopravních značek, detekci barvy na semaforu atp. Lidar i radar jsou schopny detekovat dopravní značku nebo semafor, ale nedokáží interpretovat žádné další informace. Z toho důvodu jsou prozatím kamery nedílnou součástí autonomních vozidel a pravděpodobně budou jejich součástí i nadále [38].



Obrázek 2.7: Klasifikace objektů pomocí strojového učení.[9]

[8] https://en.wikipedia.org/wiki/Inertial_measurement_unit

[9] https://towardsdatascience.com/everything-you-ever-wanted-to-know-about-computer-vision-heres-a-look-why-it-s-so-awesome-e8a58dfb641e

2.3 Analýza rizik

Úvod do problematiky

Analýza rizik a analýza nejistoty pro své posuzování může nabývat různých perspektiv. Existují společné a sdílené nástroje, které poskytují užitečnou podporu pro rozhodování tak, že svými výsledky informují ty, kteří mají rozhodovací pravomoc, protože technická stránka rizika je relevantní k opodstatněnému rozhodnutí [43].

Skutečný výsledek kritické situace, která může znamenat rozsáhlé následky se většinou odvozuje z procesu vznikajícím následným postupem [43]:

- **Analytický výpočet** vzniklé situace přesnými, neúprosnými a opakovatelnými metodami, jež vznikly pod dohledem odborné komunity. Dále tyto metody musí obsahovat posouzení předpokladů na kterých je analýza založena.
- **Poradní skupina**, obsahující všechny zainteresované strany a osoby s rozhodovací pravomocí (decision maker). Jejich cílem je společně zvážit jednotlivé problémy při rozhodování, prozkoumat argumenty pro podporu daného problému, zjistit výsledky technické analýzy a zahrnout i všechny ostatní faktory (např. sociální, politické, ...), které nejsou explicitně zahrnuty v technické analýze.

Zmíněný způsob postupu dovoluje, aby technická analýza byla zvládnutelná, zároveň doplněna úvahami a zajišťovala pokrytí i nemodelovaných problémů. Analytické hodnocení podporuje uvažování svými číselnými výsledky a taktéž všemi argumenty skryté za samotnou analýzou včetně všech předpokladů, hypotéz, parametrů a jejich nejistot [35].

Klíčové je zaručit, že všechny nejistoty budou brány v úvahu v **každém kroku** při postupu hodnocení rizik způsobem, který zajistí, že všechny informace a znalosti relevantní pro daný problém budou obsaženy nejvěrnějším způsobem. Nejistoty musí být [43]:

1. Uspořádaným způsobem **odhaleny a klasifikovány**.
2. Prezentovány a popsány přesnými **matematickými postupy**.
3. **Šířeny přes následné kroky** postupu hodnocení rizik, opatření rizik až do rozhodnutí.

Hlavním cílem s ohledem na nejistoty při rozhodování je poskytnutí **transparentního, jasného a informovaného obrazu** problému osobám s rozhodovací pravomocí, kteří mohou svědomitě a s jistotou uvažovat nad danou problematikou.

Po více než 40 let se pravděpodobnostní analýza využívá jako stavební kámen pro analytický proces hodnocení rizik nebo hazardních systémů a zpracování souvisejících nejistot s nimi spojenými. Běžně používaným termínem je **Probabilistic Risk Assessment** (PRA) nebo **Quantitave Risk Assessment** (QRA). První aplikace do velkých technologických systémů se datuje do 70. let 20. století, konkrétně byly implementovány v jaderných elektrárnách. Základní principy se za dobu existence analýzy rizik výrazně nezměnily [43].

Čistě pravděpodobnostní přístupy k analýze rizik a nejistoty mohou být zpochybněny za běžných podmínek z důvodu omezené nebo špatné znalosti specifického přiřazení pravděpodobnosti. V takovém kontextu nemusí být všechny zainteresované strany plně spokojené s hodnocením pravděpodobnosti na základě subjektivních úsudků, které provedla

určitá skupina analytiků. Pohled, který hledá širší popis rizik, kde jsou všechny nejistoty popsané `plain and flat`, aniž by se do analýzy rizik vkládaly jakékoliv hypotézy, které není možno potvrdit ani vyvrátit vedl řadu výzkumníků působících v poli analýzy rizik a nejistoty k vývoji alternativních modelů. Lze uvést například `probability bounds analysis` [21], `possibility theory` [19].

- **Hazard** se označuje jako potencionální zdroj poškození nebo ztráty, tj. nebezpečí pro součástku, životní prostředí, lidi atd. Za těchto nebezpečných podmínek jsou typicky implementována ochranná opatření, která mají za úkol předejít těmto nebezpečným podmínkám, nebo alespoň zmírnit a minimalizovat jejich dopady. Pouhá přítomnost nebezpečí nestačí ke splnění této podmínky. Dále je obsažena určitá **míra nejistoty**, že se může potencionální poškození přeměnit na skutečné poškození. Téma hazardu a rizika je v dnešní době tedy významným faktorem při návrhu, vývoji a provozu komponent ve všech odvětvích průmyslu. [43]

- Selhání, k němuž došlo vlivem konstrukce, či vady materiálu při výrobě se označuje jako **konstrukční selhání** (design-basis accident).

- **Aleatorní nejistoty** se týkají výskytu událostí, které definují nejistotu v různých možných scénářích havárií. Například náhodná změna skutečného geometrického rozměru materiálových vlastností součástky/součástí systému. Pro popis tohoto druhu nejistoty se využívá Poissonův model pro události náhodně se vyskytující v čase. Lze modelovat třeba náhodnou změnu provozního stavu bezpečnostního ventilu, selhání ventilu, náhodné zvýšení tlaku v nádobě atp [10].

- **Epistemické nejistoty** vznikají vlivem nedostatečné znalosti o různých vlastnostech jevů, které jsou základem pro chování systému. Projevuje se v modelové reprezentaci chování systému a to z hlediska modelové nejistoty v předpokládaných hypotézách, tak i v parametrové nejistotě (pevných, často málo známých) hodnotách parametrů modelu. Nejistoty modelu i parametrů související se současným stavem znalostí modelovaného systému jsou často reprezentovány pomocí Bayesovské sítě. [7] Zatímco epistemickou nejistotu lze poměrně dobře redukovat získáváním nových znalostí a informací o systému, aleatorní nejistotu tímto způsobem redukovat nelze. Z toho důvodu se tato nejistota občas nazývá neredukovatelná jistota [43].

  Jedním z přístupů, jak chránit systém proti nejistotě jeho scénářů selhání (fauilure scenario) je [43]:

  1. Odhalit **skupinu sekvencí** poruchových událostí, které vedou k nejhorším možným scénářům (worst-case scenario), dle konstrukčního selhání.
  2. Předpovědět jejich **důsledky**.
  3. Navrhnout odpovídající **bezpečnostní bariéry** pro předcházení těmto scénářům a pro zmírnění jejich důsledků.

- Ze základní zásady plyne, že pokud je systém navržen tak, aby odolal všem **nejhorším možným scénářům**, tak poté z definice musí být chráněn i proti nehodám, které by tento nejhorší možný scénář spustily. Proto v rámci zmíněného přístupu jsou prosazovány bezpečnostní rezervy vůči těmto scénářům pomocí konzervativních předpisů pro návrh a provoz daného systému [43].

Tento přístup se stal jedním z klíčových pro analýzu rizik a pro mnoho technologií je stále vedoucím přístupem. Provozovat systém bez zbytečného rizika s poskytnutím přiměřené záruky ochrany systému před nejistotou neznámého nezvyklého-poruchového chování jeho součástí, podsystémů, součástek a struktur bez přímé kvantifikace nejistoty, aby byl zajištěn jeho bezpečný provoz je klíčové [43].

V praxi se odkazování na „nejhorší možné případy“ obsahuje **velmi silné prvky subjektivity**, protože náhodné události mohou mít skutečně katastrofické následky, ale mohou být velice, velice nepravděpodobné. Vysoká míra subjektivity může znamenat zbytečně přísnou regulační zátěž, nadměrný konzervatismus při návrhu, provozu systému a jeho ochranných bariér s vysokou penalizací pro průmysl, zejména jaderný, letecký, vesmírný, zpracovatelský průmysl, ve kterých mohou těžké havárie vést ke skutečně vážným až katastrofickým důsledkům. Z těchto důvodů byl pro návrh, regulaci, provoz a řízení nebezpečných systémů zaveden alternativní přístup [43].

Původně byl motivován se zvyšující se **popularností jaderné energetiky** a s astronomickými investicemi do vesmírných programů v 60. letech 20. století. Přístup je založen na kvantifikaci spolehlivosti bezpečnostních systémů implementovaných za účelem předcházení nehodám a minimalizaci důsledků nehody, tak aby mohly zasahovat do míry nejistoty v analýze rizik pro rozhodovací akční členy při ochraně proti všem možným scénářům nehody. Zmíněný přístup již nerozlišuje mezi věrohodnými, nevěrohodnými, malými a velkými nehodami [43].

Ze začátku bylo provedeno mnoho studií, které měly za úkol prozkoumat přednosti `kvantitativního přístupu` založeného na pravděpodobnosti pro řešení nejistoty spojené s výskytem a vývojem scénářů. Výsledky studií byly překvapivé a motivovaly k prvnímu úplnému a plnému pravděpodobnostnímu hodnocení rizik jaderného zařízení [4].

Tato rozsáhlá studie ukázala, že hlavními přispěvateli k riziku havárie nemusí být vždy **konstrukční nehody**, což byl v té době velmi revoluční „objev“, který ukázal, že strukturální a přehnaně hloubkový přístup k bezpečnosti není ideální. Jak již bylo řečeno, „nejhorší možný případ“ je subjektivní pojem, který vedl ke zbytečně přehnaným bezpečnostním požadavkům. Pomocí těchto myšlenek a pár „bitev“ bylo dosaženo vzniku **probabilistic approach to risk analysis (PRA)**, která se ukázala jako účinná technika analýzy bezpečnosti systémů, která není omezena pouze na nejhorší možné scénáře, ale rozšiřuje se na všechny možné scénáře a jejich související důsledky. Pravděpodobnost jednotlivých scénářů je dalším z hlavních aspektů, které je třeba kvantifikovat, aby bylo možné rozumně a kvantitativně zvládnout nejistotu [4] [43].

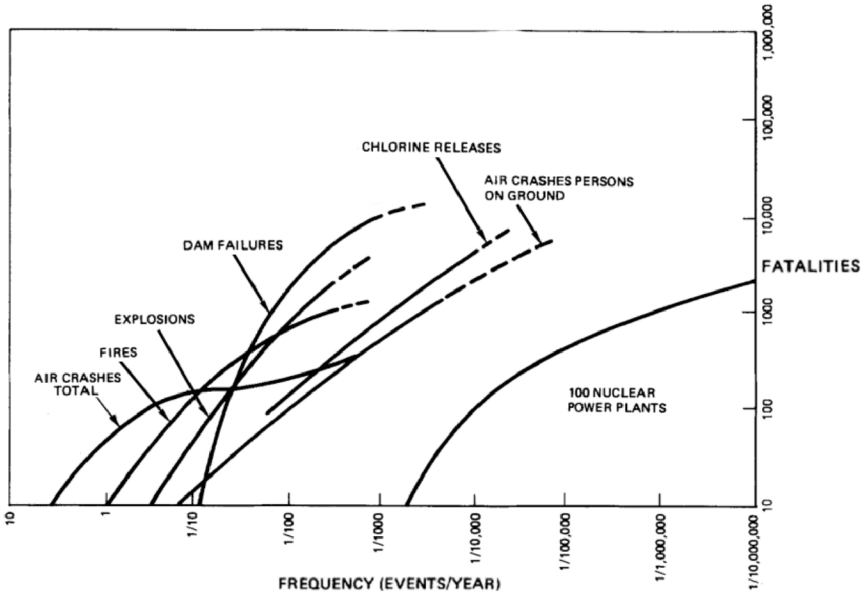
Z hlediska bezpečnostních předpisů bylo dosaženo nových kritérií. Nová kritéria zohledňují důsledky jednotlivých scénářů, ale i jejich **pravděpodobnost v rámci racionálního přístupu**, který je založen na hloubkové ochraně. V rámci tohoto přístupu ke spolehlivosti a regulaci bezpečnostní analýzy je důležitým faktorem taktéž pravděpodobnost fungování bezpečnostních bariér, implementovaných za účelem zamezení a zmírnění vzniku nebezpečných událostí, pokud by k nim došlo [43].

2.3.1 Pravděpodobnostní hodnocení rizik

Pravděpodobnostní hodnocení rizik je českým ekvivalentem pro **probabilistic risk assessment (PRA)**. Základní principy této analýzy se dají shrnout následovně. PRA systematizuje znalosti a nejistoty o studovaných jevech řešením 3 základních otázek [43]:

- Které **sekvence nežádoucích událostí** vedou ke transformaci jistého nebezpečí ve skutečné poškození systému?
- Jaká je **pravděpodobnost** každé z těchto sekvencí?
- Jaké jsou **důsledky** každé z těchto sekvencí?

Toto vede k široce uznávané technické definici rizika ve smyslu tzv. tripletů, kteří identifikují sekvence nežádoucích událostí vedoucích k poškození spolu s jejich pravděpodobnostmi a následky. Výsledkem analýzy rizika je kvantifikovaný seznam scénářů z hlediska pravděpodobnosti a důsledků, které společně představují jisté riziko. Z těchto informací, které slouží jako stavební kameny, může projektant, provozovatel, správce systému jednat tak, aby kontrolovali a případně snižovali riziko. V PRA modelu jsou znalosti o problému a s ním související nejistoty systematicky **mapovány pečlivými a opakovatelnými metodami** založenými na pravděpodobnosti. Tyto metody jsou navržené tak, aby co nejlépe charakterizovaly a poskytly transparentní výsledky. Příkladem výsledků může být očekávaný počet selhání, pravděpodobnost, že v důsledku nehody dojde k ublížení/usmrcení osoby, dále pomocí grafů, které charakterizují například frekvenci nehod (f) s alespoň n následky (n) [27].



Obrázek 2.8: Frekvence úmrtí z důvodu selhání lidského faktoru.[10]

[10] https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.323.1418&rep=rep1&type=pdf

V dnešní době jsou již metody v PRA **poměrně vyspělé**, ale i přesto byla v posledních letech vyvinuta řada nových a odlišných metod, aby lépe vyhovovaly určité problematice, s ohledem na složitosti daných problémů a reagovaly na nové technologie a systémy. Řada těchto metod umožňuje zvýšený důraz na úroveň detailů a přesností při modelování jevů a procesů, které zahrnují například podrobné fyzikální jevy, lidské faktory, ale i například dynamičnost systému. Další metody se věnují více reprezentaci a analýze rizik a s nimi souvisejících nejistot s ohledem na rozhodovací úkoly, které mají výsledky podpořit. Jako příklad lze uvést **Petriho sítě [9], Bayesovská síť [7], či metodu Monte Carlo** [8]. Analýza pravděpodobnosti v PRA modelu se opírá o dvě hlavní linie uvažování:

- **Tradiční frekventistický přístup** je aplikován, pokud máme k dispozici velké množství relevantních dat. Dále je založena na dobře známých principech statistiky, použití různých pravděpodobnostních modelů a jejich interpretace coby odhadů intervalů spolehlivosti, relativních četností, bodových hodnot, testování hypotéz atd.
- **Bayesovský přístup** je založen na použití subjektivních pravděpodobností, při absenci velkého množství dat. Postup v Bayesovském principu je následný [43]:
    1. Vytvořit pravděpodobnostní modely, které reprezentují **aleatorní nejistoty**. Př. variabilita studovaného jevu - životnost určité komponenty
    2. Vytvořit pravděpodobnostní modely, pro **epistemické nejistoty**(neúplné/nedostatek znalostí) o hodnotách parametrů modelu. Reprezentovány jsou pomocí předchozích subjektivních rozdělení pravděpodobnosti. Pokud jsou k dispozici nové údaje o jevu, tak se Bayesův vzorec použije k aktualizaci epistemických nejistot z hlediska posteriorní distribuce.
    3. Prediktivní distribuce veličin, které **považujeme za důležité** (př. životnost komponenty), jsou odvozeny aplikací zákona úplné pravděpodobnosti.

Zdroje nejistot

Za hlavní zdroje nejistot v analýze rizik se dá považovat následující [43]:

- **Nepřesné měření** fyzikálních veličin (váha, rychlost, délka atp.) je ovlivněna dvěma faktory:
    1. Analytikem, který provádí měření dané veličiny.
    2. Přesností použitého nástroje, jelikož každý přístroj má určitou tolerovanou míru přesnosti. Příkladem může být přesnost rychloměru v automobilu v kilometrech za hodinu, která je obvykle uměle nadsazena od výrobce [31].
- **Nedostatek informací/znalostí** o jevech, systémech, událostech, veličinách, dynamičnosti, které mají být analyzovány. Může být [43]:
    1. **Kvantitativního** charakteru, kdy analytik nezná přesnou hodnotu pravděpodobnosti dané události.
    2. **Kvalitativního** charakteru, kdy analytik zná pravděpodobnost události, ale i včetně dostupných informací není schopen deterministicky analyzovat popis problému.

3. **Aproximací** - pokud není dostatečně možné popsat daný jev, nebo pokud záměrně dojde k vyšší úrovni abstrakce pro zjednodušení problému, i když je nižší úroveň abstrakce dosažitelná. Někdy je aproximace skrytá, a nebo je naopak explicitně uvedena. Lze ji snížit pomocí získání více informací a dat, či podrobnějším studiem daného problému/jevu.

- **Lingvistická bariéra** vznikající významem slov v odlišných jazycích. V různých jazycích nemusejí mít slova v kontextu analýzy vždy stejný význam.

- **Množstvím informací** je druhem nejistoty plynoucí z lidské neschopnosti zpracovávat velká množství dat a informací současně. Analytik se obvykle zaměřuje na informace a parametry, které považuje za důležitější a ostatní zanedbává. Identifikace jednoznačného postupu pro výběr mezi stovkami/tisíci relevantních dat, informací a parametrů je kritickým problémem. Analytik musí tomuto druhu nejistoty čelit, když například vybírá mezi různými modely pro simulaci jevu, problému.

- **Míra subjektivity analytika**. Nejistota může taktéž pocházet ze subjektivní vnímání interpretace informací a dostupných dat analytikem. Stejná informace může být interpretována různě z důvodu subjektivity různých analytiků. Dále může mít vliv na analytika kulturní zázemí, politická orientace, kompetence analytika atp. Tento zdroj nejistoty se potlačuje pomocí sesbírání názorů různých expertů, a tím lze docílit výrazného potlačení míry subjektivity.

- Může se stát, že vznikne **rozpor v dostupných informacích/datech**. Některé z dostupných informací poukazují na chování systému a jiné informace mohou poukazovat na odlišné chování systému. V této situaci navýšení objemu dat o systému prozkoumáváním a sbíráním dalších dat nemusí znamenat potlačení této nejistoty, ale spíše vede k zvýšení tohoto rozporu. Tento rozpor může vzniknout tak, že [43]:

  1. některé informace jsou **ovlivněny chybami**, které analytik nemůže identifikovat,
  2. některé dostupné části dat **nejsou** pro daný problém zcela **relevantní**,
  3. použitý model systému analytikem **není vhodně zvoleným** a může být zkreslený.

  Pro snížení rizika zdroje nejistoty v této situaci je nutné aby analytik provedl přesnou volbu mezi dostupnými informacemi/daty. Případně některé informace/data vyřadil, aby konflikt dostatečně redukoval.

2.3.2 Hlavní kroky

Analýza rizik se skládá z částí [43]:

- **Identifikace** nesprávného chování, provozních chyb a vnějších událostí, které mohou být spouštěčem havárie ve zkoumaném systému.

- Zaměření se na **podrobnou analýzu** nehod, které jsou důležitější z hlediska jejich frekvencí a následků.

- Identifikovat a kvantifikovat **dopad nehod** na systém, výrobu, majetek, obyvatele a životní prostředí.

Díky vyhodnocení a kvantifikaci chyb, nesprávného chování, externích vlivů atp. lze poskytnout spolehlivou vazbu, aby došlo ke snížení rizika pro systém, výrobu, majetek, obyvatele a životní prostředí.

Analytický proces [43] v hodnocení rizik pro systém se dělí do pěti tradičních kroků:

- Popis systému a jeho modelování viz 2.
- Identifikace hazardů spojených s prací systému viz 2.3.2.
- Výběr spouštěcích událostí, které se mohou stát iniciátorem pro havárie viz 2.3.2,
- Kvantitativní analýza sekvencí z vybraných spouštěcích událostí, četností a následků viz 2.3.2.
- Hodnocení rizik a rozhodovací proces viz 2.3.2.

Modelování systému

V prvním kroku je nutné problematiku důkladně nastudovat a poté daný systém namodelovat, jak bylo uvedeno v kap. 2

Identifikace hazardu

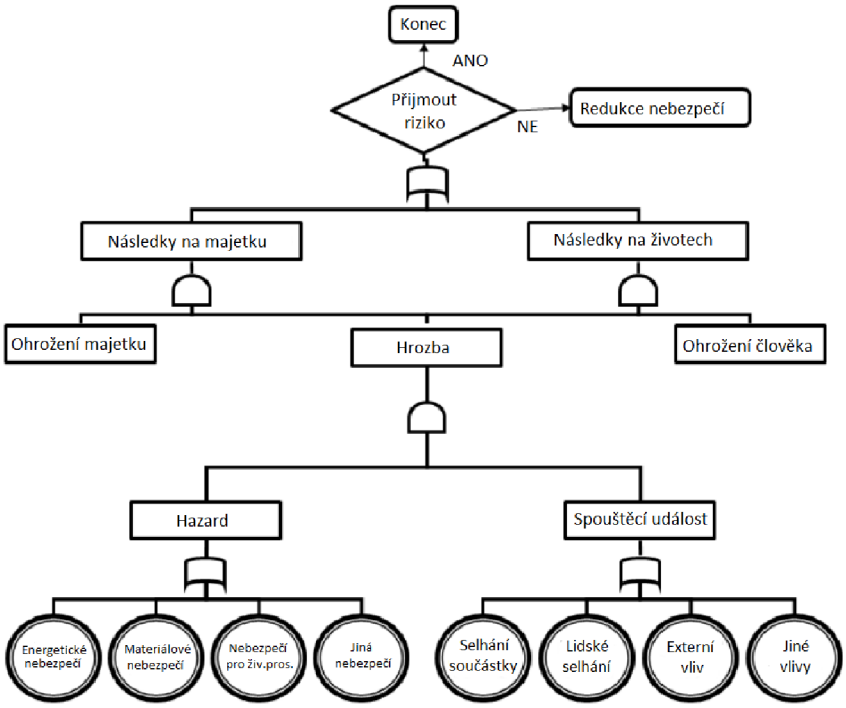
Druhým krokem v analýze určitého systému je identifikace hazardů plynoucí z jejich provozu. Lze ji definovat jako systematickou a iterativní proceduru identifikace, klasifikace a snížení hazardu. **HAZ**ard **ID**entification je zaměřena na zahrnutí všech nebezpečí, které mohou přímo i nepřímo ovlivnit správnou funkcionalitu systému [42].

Z obrázku 2.9 je zřejmý koncept, na kterých je technika HAZID založena. Nebezpečí se odhalí prostřednictvím svých projevů a je aktivováno, pokud přijde spouštěcí událost (kombinace hazardu a spouštěcí události lze nazvat jako hrozbu (mishap), které mají za následek smrt, zranění, poškození, ztrátu majetku, či ohrožení životního prostředí. Dále je nutné **rozhodnout**, zda lze riziko přijmout, či nikoliv a musí se spustit opatření pro redukci rizika [42].

HAZID studie je zpravidla prováděna pomocí **týmu kompetentních odborníků** z různých oborů pod vedením zkušeného analytika, který má s HAZID technikou zkušenosti. Každá oblast, podoblast a zóna daného systému je posuzována dle kontrolního seznamu hrozících nebezpečí. Pokud se odborníci shodnou, že v určité části systému existuje jisté nebezpečí, tak je třeba uvážit jaké riziko dané nebezpečí představuje a dále se uvažují všechny prostředky, které pomohou s eliminací, či redukcí hrozícího nebezpečí, které se uvede do HAZID protokolu. Přípustná je i situace, že v dané chvíli nelze přesně určit hrozící nebezpečí a je potřeba důkladnějšího studia daného jevu [42].

Cíle HAZID techniky [43]:

- **Identifikace hazardů** pro systém z důvodu návrhu systému a vyhodnocení následků hazardu.
- Zavést **ochranná opatření** pro řízení rizika a identifikovat oblasti, kde je zapotřebí více porozumět účinnosti ochranných opatření
- Sepsat **doporučení** k snížení pravděpodobnosti výskytu hazardu, nebo k zmírnění potencionálních následků.

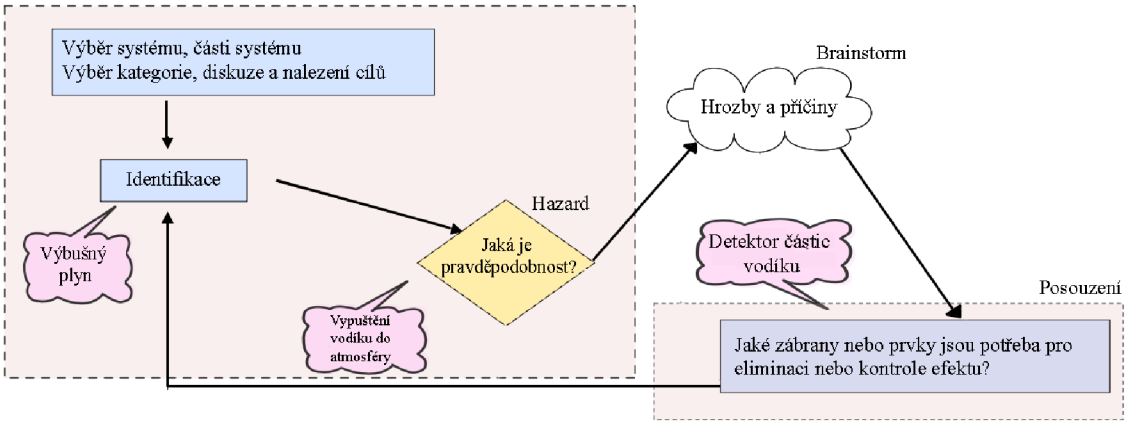


Obrázek 2.9: Základní principy HAZID techniky.[11]

Benefity

- Existující designové znalosti jsou efektivně zachyceny ve vztahu k ostatním projektům
- Procedurální doporučení, návrh zařízení, testování a doporučení k řízení procesů umožňují rychlejší vývoj standardizovaného vybavení.

[11] https://www.foncsi.org/fr/publications/cahiers-securite-industrielle/uncertainty-characterization-in-risk-analysis-for-decision-making-practice/CSI-uncertainty-QRA.pdf



Obrázek 2.10: HAZID proces.[12]

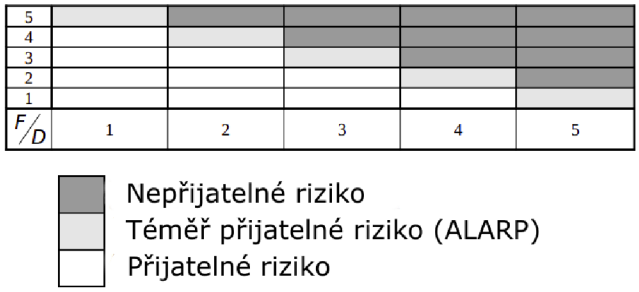
Postup

- Zjistit smysl, dosažitelné cíle a zaměření studie.
- Vybrat vhodný tým.
- Připravit samotnou studii.
- S týmem zhodnotit studii a případně korigovat problémy.
- Zdokumentovat výsledky studie [43].

Výběr spouštěcích událostí

Poté, co jsou nebezpečí identifikována jsou k nim přiděleny jednotlivé spouštěcí události (události, které mohou být potencionální příčinou hazardu a vedou přímo, nebo nepřímo k poškození systému, jejich provozovatelům, obyvatelstvu, životnímu prostředí, ztrátě výroby atd.). Výstupem této úlohy je seznam poruch, odchylek procesů, defektů, externích událostí atp. které mají nenulovou pravděpodobnost výskytu [43].

Zkušenosti analytiků, jejich poznatky a sběr dat o poruchách jsou opětovným zdrojem znalostí pro tuto část studie. Stejný hazard může být vyvolán i přes různé spouštěcí události a může vést ke stejným, či odlišným následkům. Identifikace spouštěcích událostí je tedy klíčovým aspektem celkové bezpečnostní analýzy [43].



Obrázek 2.11: Matice rizik pro identifikaci spouštěcích událostí - příklad. [13]

[12] https://www.foncsi.org/fr/publications/cahiers-securite-industrielle/uncertainty-characterization-in-risk-analysis-for-decision-making-practice/CSI-uncertainty-QRA.pdf

Dle [5] je se postup sestává z následujícího:

- Pro každé **nebezpečí** (hazard) je nutná identifikace odpovědných spouštěcích událostí. Spouštěcí události je nutné hledat mezi možnými poruchami a defekty komponent, softwarovými chybami, lidskými chybami atd.
- Klasifikovat **kritické události** identifikované v předchozím kroku na základě související úrovně rizika pomocí kvalitativní matice rizik (obr 2.10). Rizika, která jsou klasifikována jako přijatelná znamenají, že současný návrh systému zaručuje adekvátní kontrolu daného rizika. Téměř přijatelná rizika jsou rizika, pro která jsou navrženy změny v návrhu, nebo správě systému. Nepřijatelná rizika vyžadují podrobnější šetření a změnu návrhu, nebo správu systému.
- Na základě předchozího kroku je proveden výběr **nejzávažnějších** rizik.
- Mezi nejkritičtějšími událostmi je proveden výběr těch, které mají potenciál stát se **iniciátory sekvencí nehod**.
- **Seskupit** podobné spouštěcí události do homogenních skupin.
- Pro každou skupinu **vybrat** jednu spouštěcí událost, která danou skupinu bude reprezentovat.

Kvantitativní analýza

Analýza sekvencí nehod (scénářů) představuje kvantitativní fázi hodnocení daných rizik. V syntéze jsou určeny sekvence nehod, jež jsou odvozené od každé z spouštěcích událostí, které byly identifikovány v předchozím kroku. Dále je třeba kvantifikovat pravděpodobnost (frekvenci) výskytu daných sekvencí a odpovídající důsledky (související poškození) [42].
noindent **Strom událostí**
Kvantitativní analýza sekvencí [42], které vedou k nebezpečí jsou zpravidla zaznačeny pomocí stromu událostí (Event tree). Tento přístup je založen na diskretizaci vývoje skutečné nehody v několika makroskopických událostech. Identifikace spouštěcí události a události vymezující sekvence daného hazardu musí být uvedeny v chronologickém pořadí dle času a logiky výskytu. Události, vymezující jejich sled jsou obvykle charakterizovány jako z hlediska:

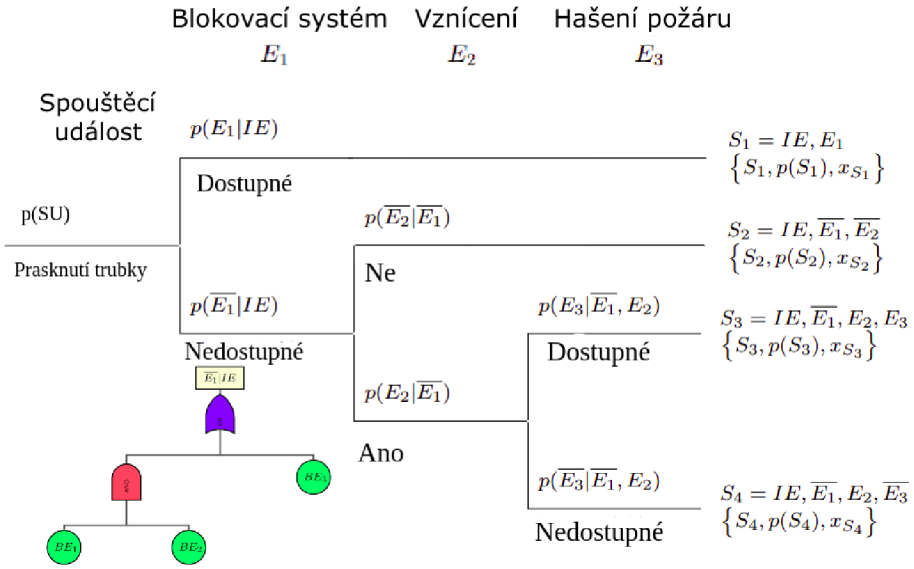
1. Zásahu (či nikoliv) ochranných systémů, které mají přijmout opatření ke zmírnění nehody,
2. plnění (neplnění) bezpečnostních funkcí
3. existence (neexistence) fyzikálních jevů

Tyto události jsou strukturovány ve formě nadpisů ve stromu událostí. Pro každou událost musí být definována a vyčíslena množina možných stavů (úspěch/selhání ochranné systému atd.) a každý stav vede k větvení stromu.

[13] http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf

Strom poruch
Analýza stromu poruch (fault-tree analysis) je systematická a deduktivní technika umožňující poodhalit vztahy, které vedou k dané nežádoucí události. Začíná od definované události selhání systému a zpětně se odvíjí příčiny až k hlavním nezávislým poruchám (lze je nazvat jako základní události). Metoda se zaměřuje na jedno konkrétní selhání systému a může poskytnout kvalitativní informace o tom, jak může daná událost nastat, její důsledky, a dále lze s její pomocí identifikovat komponenty, které hrají klíčovou roli při určování definovaného selhání systému. Danou událost kvantitativně vyjádřit díky znalosti pravděpodobnosti výskytu základní události [42].

Posloupnosti událostí jsou poté kvantifikovány z hlediska pravděpodobnosti (frekvence) výskytu, což vyžaduje stanovení pravděpodobnosti výskytu dané spouštěcí události a podmíněných pravděpodobností výskytu tvořící danou posloupnost. Každou událost (větev) ve stromu lze nazvat jako top událost, díky které lze provést výpočet pravděpodobnosti dané události. Vypočítaná hodnota představuje podmíněnou pravděpodobnost výskytu události za předpokladu, že nastaly události, které této sekvenci předcházejí [42].



Obrázek 2.12: Příklad stromu událostí s implementovaným stromem poruch. [14]

V obrázku 2.12 je ukázáno schéma stromu událostí s příkladným stromem poruch, který je použit pro vyhodnocení pravděpodobnosti $p(E_1|IE)$ události E_1, která je podmíněna výskytem spouštěcí události. Za povšimnutí stojí výpočet pravděpodobnosti $p(E_1|IE)$, jenž je vypočítána jako funkce pravděpodobnosti $p(BE_1), p(BE_2)$ a $p(BE_3)$ základních událostí BE_1, BE_2, BE_3. Násobení podmíněných pravděpodobností pro každou větev v posloupnosti dává pravděpodobnost této posloupnosti.

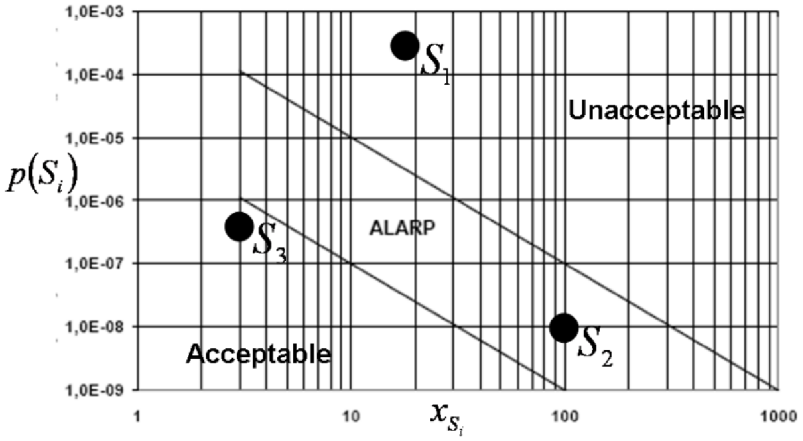
Odhad důsledků $x_Si, i \in 1, 2, ...$ každé sekvence nehod vyžaduje simulaci fyzikálních jevů zahrnutých ve větvích stromu událostí pomocí správně sestavených matematických modelů, které jsou obvykle transformovány do deterministických počítačových kódů.

[14] http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf

Hodnocení rizik a proces rozhodování

V posledním kroku postupu hodnocení rizik je nutné vyhodnotit rizika spojených se scénáři nehod identifikovanými a kvantifikovanými v předchozím kroku. V praxi je riziko spojené se scénáři klasifikované jako „přijatelné“ (současný návrh systému zaručuje kontrolu rizika),„téměř přijatelné“ (jsou navrženy změny v návrhu/řízení systému) a „nepřijatelné“ (doporučeno podrobnější šetření a změny návrhu), jak již bylo vidno z obrázku [42].

Jedním z možných přístupů ke klasifikaci scénářů nehod S_i, $i \in 1, 2, ...$ je graficky znázorněn na obrázku 2.13, kde jsou pravděpodobnosti $p(S_i)$, $i \in 1, 2, ...$ vyneseny vůči jejím důsledkům $X_{Si}, i \in 1, 2, ...$ Každý scénář je v diagramu vyobrazen jako bod. Například scénář S_1 je klasifikován jako „nepřijatelný“, scénář S_2 jako „téměř přijatelný“ (ALARP) a scénář S_3 jako „přijatelný“. Na základě této klasifikace a vizuální reprezentace osoba s rozhodující pravomocí (decision maker) nejprve identifikuje nejúčinnější strategii pro snížení rizika (prevence, snížení pravděpodobnosti úmrtí, snížení následků nehody, ...) a poté je nutná podrobná analýza systému na základě rizik, které povedou ke změně návrhu/řízení systému pro předejití nehodě, zmírnění následků atp [42].



Obrázek 2.13: Možné scénáře a jejich klasifikace. Osa X znázorňuje následky události v log. měřítku a osa Y pravděpodobnost výskytu scénáře. [16]

Nakonec je nutné zmínit, že tato operace je silně závislá na sociální, ekonomické a kulturním kontextu dané země. Úroveň přijatelnosti rizika spojená s provozem stejné typologie (jaderného, chemického, ...) se bude lišit v jednotlivých zemích [42].

[16] https://www.foncsi.org/fr/publications/cahiers-securite-industrielle/uncertainty-characterization-in-risk-analysis-for-decision-making-practice/CSI-uncertainty-QRA.pdf

2.4 Aktuální stav analýzy rizik v samočinně řízených vozidlech

Cílem studie [16] bylo identifikovat rizika spojená se selháním autonomního vozidla ve smíšeném provozu. Pro účely identifikace rizik byl systém samočinně řízeného vozidla rozebrán na součásti vozidel a součásti dopravní infrastruktury. Poté byl pro každý systém vyvinut model stromu poruch. Pravděpodobnost selhání každé součásti byla odhadnuta na základě přezkoumání publikované literatury a veřejně dostupných dat. Analýza rizik vedla k výsledku pravděpodobnosti selhání cca 14% v důsledku sekvenčního selhání samotných součástí vozidla během jeho životnosti.

Další studie [34] se zabývá hledáním poruch v autonomních vozidle. Pracuje s vysoce přesnými simulátory a s výpočetně drahými autonomními systémy s efektivním hledáním poruch, což je hlavním cílem. Práce navrhuje komplexní rámec pro hodnocení rizik samočinně řízeného vozidla. Kombinuje scénáře riskantní jízdy, modely senzorů, zásady autonomních vozidel a metody hodnocení rizik.

Studie [18] se zabývá navržením indikátoru globálního rizika pomocí lokálních informací pocházející z okolních vozidel nebo infrastruktury (komunikace V2X). Článek prezentuje zisk takového globálního ukazatele rizika v porovnání s lokálním rizikem, včetně dopadu na chování samočinně řízeného vozidla a řidiče vozidla.

Ve studii [28] autoři prezentují systém autonomního řízení jako kombinaci různých komponent, které mohou být složeny z jednotlivých operací automobilu s operací rozhodovacích systémů, jak v pravidelných časových intervalech, tak při neočekávaných situacích. Operace jsou prováděny pomocí virtuálního ovladače k provádění určitých cílů určenými uživatelem. Pro tyto systémy existují určitá bezpečnostní rizika, která je třeba otestovat a vyřešit. Studie analyzuje systémy autonomního řízení za účelem stanovení priorit rizik pomocí Pythagorových fuzzy množin, které lze využít k vyjádření nejistoty v rozhodovacím procesu. Pro analýzu rizik a jejich hodnocení je brána jako základ norma ISO 26262.

Kapitola 3

Realizační prostředky a metody

V následující kapitole bude možno nahlédnout na různé modelovací prostředky pro validaci a verifikaci modelů. Simulační modely mají vstupy, parametry, výstupy atp. s jejichž pomocí lze provádět experimenty s modely a sledovat jejich chování v čase, jak již bylo uvedeno v kapitole 2.

3.1 Dymola/Modelica

Dymola je modelovací a simulační prostředí pro komerční účely stavící na modelovacím jazyce *Modelica*. S jeho pomocí lze modelovat a simulovat různé komplexní fyzikální systémy, kterými mohou být elektrické obvody, vedení tepla, letecké systémy, automobily atp. Modely se mohou skládat z komponent z více inženýrských domén. Subsystémy jsou zpravidla reprezentovány jako propojené komponenty. Na nejnižší úrovni je chování popsáno pomocí matematických rovnic, či algoritmů. *Dymola* za účelem generování efektivního simulačního kódu zpracovává kompletní systém rovnic. Původně byla navržena v roce 1978 jako doktorandská práce [12] [3].

3.2 SIMLIB

Simulační knihovna *SIMLIB* je vyvíjena od roku 1990 na Ústavu informatiky a výpočetní techniky FEI VUT Brno, dále její vývoj pokračuje na ústavu inteligentních systémů FIT VUT Brno. Knihovna je implementována pod MS-DOS a pod operačním systémem Linux. *SIMLIB* poskytuje základní prostředky pro popis spojitých, diskrétních i kombinovaných modelů. Dále obsahuje prostředky pro řízení simulace. Při vytváření simulačních modelů a experimentování s nimi lze využít různá prostředí, která umožňují interaktivní tvorbu a prostředí pro ladění modelů [36].

Model je v *SIMLIB* reprezentován jako množina prvků, které jsou spolu navzájem propojeny různými vazbami, které spolu s chováním prvků určují chování systému jako jeden celek. Systém se dělí na jednotlivé objekty, mezi nimiž lze nalézt takové objekty, které mají podobné chování (shodné charakteristiky) a ty lze poté umístit do jedné třídy objektů. Třída definuje jejich vnitřní strukturu, reakce na vstupy a své vlastní chování v čase. Pro sběr statistických dat a informací o chování modelu při simulaci obsahuje knihovna několik tříd. Taktéž lze využít ostatní dostupné knihovny a konstrukce jazyka C++. Pomocí importovatelných knihoven lze přidat například grafické rozhraní pro lepší manipulaci s programem [36].

3.3 UPPAAL

UPPAAL je modelovací nástroj sloužící k validaci a verifikaci real-time systémů, který byl vybrán pro implementaci analýzy rizik. Nástroj je vyvíjen ve spolupráci dvou univerzit, konkrétně Uppsala University ve Švédsku a Aalborg University v Dánsku. Uživatelské rozhraní je implementováno v programovacím jazyce *Java*, verifikátor atd. jsou implementovány v jazyce *C++*. Modely jsou reprezentovány pomocí časových automatů [15].

Časový automat je šestice (L, l_0, C, A, E, I) kde:

- L je konečná množina stavů
- l_0 je počáteční stav
- C je konečná množina hodin
- A je konečná množina akcí
- E je množina hran, takových že $E \subseteq L \times A \times B(C) \times 2^C \times L$
- I je funkce přiřazující invariant stavům ve tvaru $I : L \to B(C)$ [15].

Uživatelské rozhraní

Uživatelské rozhraní je rozděleno do tří hlavních částí: Editor, Simulator (ConcreteSimulator) a Verificator.

Editor

Model systému je tvořen v editoru pomocí časových automatů. S jejich pomocí lze stochasticky modelovat systém. Časové automaty mohou být rozšířeny o proměnné, strukturované datové typy (ADT), synchronizace mezi dvěma, či více různými automaty a typy urgence. Stavy jsou reprezentovány pomocí vyplněných kruhů (kruhu lze přidělit i jednu ze třinácti různých barev) ze kterých lze vést hrany (reprezentovány čárami s šipkou) do jiných stavů, čímž lze dosáhnout přechodu mezi dvěma stavy. Stav může mít *invariant*, který určuje podmínku platící po celou dobu setrvání v daném stavu [15].

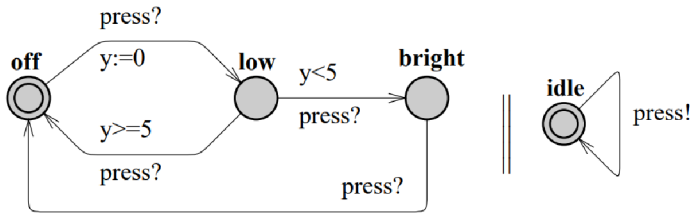
Stavy (*states*) lze rozdělit na čtyři různé druhy [15]:

- *Initial* je označen jako výchozí stav. Každý automat má právě jeden *initial* stav. Initial stav je graficky zobrazen jako kruh s menším kruhem uvnitř.
- *Urgent* je stav ve kterém dochází k zastavení času. Znázorněn jako stav s písmenem U uvnitř kruhu.
- *Commited* je stav, který rovněž jako *urgent* stav zastavuje čas s rozdílem, že další přechod musí následovat do nějakého dalšího *commited* stavu. Značen jako kruh s písmenem $\subset$ uvnitř kruhu.
- *Default* je normální stav nespadající do žádné z předchozích kategorií. Značen jako vyplněný kruh.

Přechody (*edges*) mezi jednotlivými stavy mohou mít různou funkcionalitu, konkrétně [15]:

- *Select* vymezuje interval, ze kterého potom stochasticky vybere hodnotu proměnné.
- *Guard* je omezení přechodu podmínkou. Přechod je povolen pouze v případě splnění definované podmínky, příkladem může být $x <= 1$.
- *Sync* slouží pro synchronizaci. Za pomoci synchronizačních kanálů lze přijímat a vysílat signály o signalizované synchronizaci. Lze díky nim například předat řízení mezi různými automaty. Kanály se dále dělí typy: *chan*, *urgent chan* a *broadcast chan*. Zapisuje se formou: *synchronise?* a *synchronise!*.
- *Update* provede aktualizaci proměnné, nebo může zavolat jakoukoliv funkci v kódu. Naráz lze provést více aktualizací proměnných/zavolat více funkcí.

Na následujícím obrázku bude možné prozkoumat jednoduchý automat pro ovládání žárovky. Žárovka (Lamp) má tři možné stavy: *off*, *low*, *bright* a výchozí stav má nastaven na *off*. V případě, že uživatel (User) zmáčkne tlačítko, tak se automaty synchronizují kanálem *press* a lampa se rozsvítí. Pokud uživatel zmáčkne tlačítko dostatečně rychle, dojde k další synchronizaci pomocí stejného kanálu, žárovka se dostane do stavu *bright* a rozsvítí se více. Uživatel může stisknout tlačítko náhodně v jakýkoliv čas a nebo tlačítko nezmáčknout vůbec. Hodiny y slouží k detekci, zda uživatel zmáčkl tlačítko dvakrát za sebou dostatečně rychle ($y < 5$), nebo příliš pomalu ($y >= 5$) [15].



(a) Lamp. (b) User.

Obrázek 3.1: Dva jednoduché automaty pro rozsvícení žárovky. (a) Žárovka, (b) Uživatel. [2]

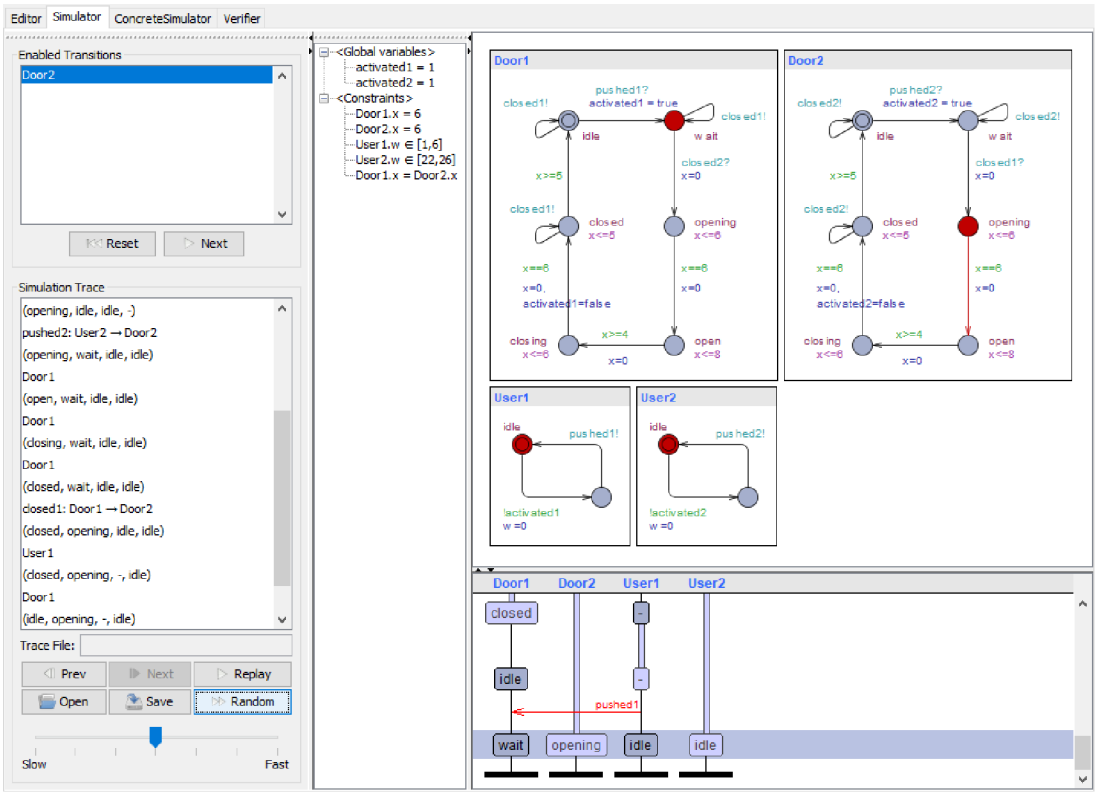
Simulátor

Simulátor může být využit třemi různými způsoby [15]:

- **Manuálně**. Uživatel si může vybrat konkrétní přechody mezi stavy.
- **Náhodně**. Simulátor náhodně vybírá přechody mezi stavy.
- **Stopování**. Uživatel může uložit/nahrát libovolnou stopu (trace) a poté sledovat, kterými stavy automat prošel.

[2] https://www.it.uu.se/research/group/darts/papers/texts/new-tutorial.pdf

V levé části simulátoru jsou umístěny vybrané a povolené přechody mezi stavy, dále stopa automatu a ovládací prvky simulace.
V prostřední části jsou umístěny kontrolní proměnné typu *integer* a proměnné typu *clock*. *UPPAAL* neukazuje konkrétní stavy s aktuálními hodnotami pro hodiny, jelikož je neomezeně mnoho takových stavů. *UPPAAL* místo toho zobrazuje množiny pro konkrétní stav známé jako symbolické stavy.
V pravé části se vyskytují všechny instanciované časové automaty, včetně aktivních stavů jednotlivých automatů.
V dolní části je možné nahlédnout na synchronizace mezi jednotlivými procesy a taktéž aktivní lokace při každém kroku automatu [15].



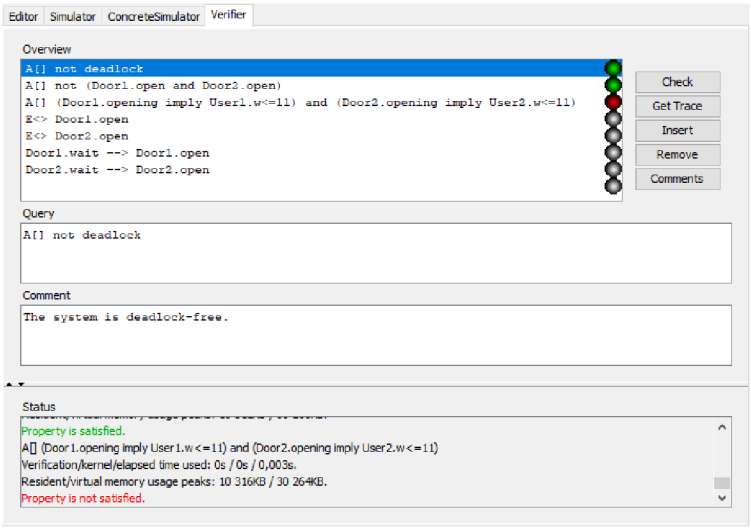
Obrázek 3.2: Uživatelské rozhraní *UPPAAL* Simulátoru. [3]

[3] Integrovaná implementace dveří v nástroji UPPAAL. /uppaal-4.1.24/demo/2doors.xml

Verifikátor

Verifikátor slouží ke kontrole požadavků na model, které jsou zapsány výrazem. Uživatel může kontrolovat jednu, více splnitelných podmínek, vkládat nové podmínky editovat/mazat podmínky a dále vytvářet k jednotlivým výrazům komentáře. Pokud je zvolen daný výraz, lze editovat jeho definici, příkladem může být podmínka $E <> Train1.Cross$ `and` $Train2.Stop$. V dolní části se nachází sekce *Status*, která slouží k přehledu komunikace se serverem [15].

Při stisku možnosti `Check` u některého z výrazů dojde k vyhodnocení podmínky v implementovaných automatech za pomocí simulace. Po konci simulace je daná podmínka označena zeleným kolečkem, pokud se ji podařilo splnit. V případě, že se podmínku splnit nepodařilo, tak je výraz označen červeným kolečkem. Simulace může taktéž skončit jako `time-lock`, kdy dojde k zastavení času v modelu z důvodu nemožné realizace jakéhokoliv přechodu. Dojde k výpisu všech automatů a jejich stavů, dále k výpisu všech proměnných. Poté je možné nahlédnout, za jaké podmínky došlo k neúspěšné simulaci a je možné model v *Editoru* opravit [15].



Obrázek 3.3: Uživatelské rozhraní *UPPAAL* Verifikátoru. [4]

Stand-alone verifikátor

Verifikaci velkých úloh často není vhodné provádět přes grafické rozhraní nástroje *UPPAAL*. Z toho důvodu je v *UPPAAL* implementován `stand-alone` verifikátor, zvaný `verifyta`, který lze spouštět pomocí příkazové řádky. Díky `stand-alone` verifikátoru je možné spouštět úlohy i na vzdáleném `UNIX` stroji, který může běžet absolutně nezávisle na uživatelově počítači. Přijímá příkazy z příkazové řádky včetně argumentů a nabízí stejné možnosti jako grafické rozhraní nástroje *UPPAAL* [15].

[4] Integrovaná implementace dveří v nástroji UPPAAL. /uppaal-4.1.24/demo/2doors.xml

UPPAAL SMC

UPPAAL SMC (Statistical Model Checking) je rozšíření prostředí *UPPAAL*, které od verze programu 4.1.4 slouží ke statistickému ověřování modelu. Jedná se o sadu technik sledující několik běhů (jednotky, stovky, tisíce, ...) s ohledem na předem definovanou zkoumanou vlastnost. Z ukončených běhů vypočítá statistiky, které lze využít pro vyhodnocení míry korektnosti návrhu daného modelu. V uživatelském rozhraní umožňuje oproti obyčejnému prostředí *UPPAAL* specifikovat rozdělení pravděpodobnosti, kterým se řídí jeho časové chování. Verifikátor poté obsahuje dodatečné dotazy, pomocí kterých lze daný model ověřovat [15].

V prostředí verifikátoru lze poté vizualizovat časový průběh hodnot jednotlivých proměnných v běžích simulace. Lze realizovat pomocí dotazu [15]:

$$\text{simulate } N \texttt{ [<= Time] } \{V_1 ..., V_k\}$$

kde N je přirozené číslo, které určuje přesný počet simulací probíhající v intervalu $[0, \texttt{Time}]$ a V_1 až V_k značí k proměnných. Hodnoty proměnných V_1 až V_k jsou zaznamenávány a vizualizovány na výsledném grafu.

Míru pravděpodobnosti na určitý jev lze zjistit za pomocí dotazu [15]:

$$\Pr \texttt{ [<= Time] } (\Psi)$$

kde v časovém intervalu $[0, \texttt{Time}]$ probíhá simulace a Ψ je zkoumaná formule.

Taktéž lze testovat hypotézy za pomocí dotazu [15]:

$$\Pr \texttt{ [<= Time] } (\Psi)\} \ >= th_0$$

kde v časovém intervalu $[0, \texttt{Time}]$ probíhá simulace, Ψ je zkoumaná formule a je zjišťováno, zda je pravděpodobnost na daný jev větší, či menší než hranice pravděpodobnosti th_0

Dostupné modely

V následující podkapitole bude následovat přehled implementovaných modelů v nástroji *UPPAAL*. Představeny budou vybrané veřejné modely absolventů FIT VUT v Brně, jejich krátké představení a shrnutí vhodnosti modelu pro analýzu rizik. Modely neimplementují komplexní autonomní vozidla z důvodu vysoké složitosti, nýbrž implementují jednotlivé podčásti autonomních vozidel, jako je například systém ABS, systém ESP, autonomní parkování atp.

3.3.1 Model ABS

Autorem modelu vozidla se systémem ABS je Bc. Dominik Holec z roku 2018 [25]. Systém ABS (**A**ntilock **B**raking **S**ystem) je systém, který zabraňuje zablokování kola a ponechává vozidlo ovladatelným v situacích prudkého brzdění. Z důvodu bezpečnosti je ovladatelnost vozidla nadřazena délce brzdné dráhy. Díky zachování ovladatelnosti vozidla je řidič schopen nouzově manévrovat s vozidlem a potencionálně se vyhnout nebezpečí/kolizi. Systém ABS funguje za jakýchkoliv povětrnostních podmínek (suchá vozovka, mokrá vozovka, zasněžená vozovka atp.). Je možné, že by vozidlo bez systému ABS zastavilo s kratší brzdnou dráhou, ale z důvodu bezpečnosti je tento systém zapnut stále. Jedná se o základní systém aktivní bezpečnosti vozidla [25].

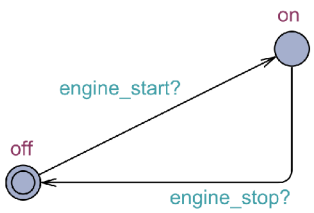
Princip systému ABS

Na kolech se nacházejí senzory, které kontrolují otáčky kola. Tyto hodnoty se porovnávají s obvodovou rychlostí kola a referenční rychlostí vozidla. Při prudkém sešlápnutí brzdového pedálu může dojít k zablokování kola. Pokud dojde k zablokování kola, tak řídící jednotka porovná hodnoty obvodových rychlostí kol a referenční rychlostí vozidla. Dojde k zjištění, že mezi referenční rychlost vozidla a obvodovou rychlostí kola je velký rozdíl, řídící jednotka situaci vyhodnotí a na krátký okamžik sníží tlak brzdové kapaliny v brzdovém okruhu. Díky tomu se sníží třecí síla mezi brzdovým kotoučem/bubnem a brzdovou deskou/čelisti. Kolo se odblokuje a je nad ním opět získána kontrola. Následně dojde opět ke zvýšení brzdného tlaku v brzdném okruhu, celý proces se opakuje. Opakování může nastat i 10-15krát za vteřinu. Systém ABS se snaží o udržení vozidla na mezi adheze čili co největší brzdný účinek bez zablokování kola. Systém ABS se vypne pouze při nízkých rychlostech ($v < 4\ kmh^{-1}$), aby mohlo dojít k úplnému zastavení vozidla [25].

Implementace modelu

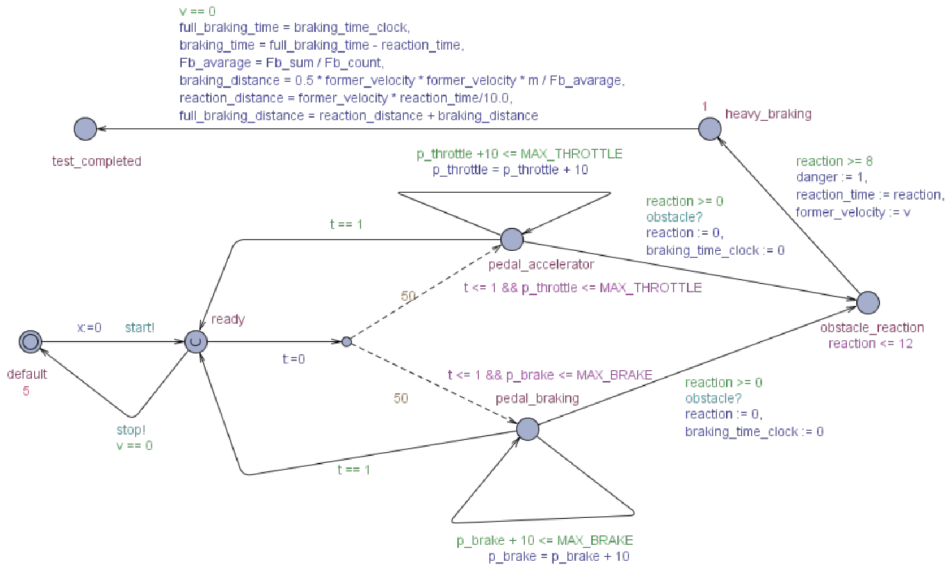
Model je rozdělen na 7 automatů, které reprezentují automobil se systémem ABS. Jednotlivé automaty budou popsány v následujících odstavcích.

Model motoru *Engine* je jednoduchý dvoustavový automat simulující funkci motoru. Signály pro změnu stavu jsou přijímané od řídící jednotky motoru a výkon, který je přímo spojen s funkcí motoru je reprezentován pomocí proměnné zrychlení a [25].



Obrázek 3.4: Automat reprezentující motor vozidla. [5]

Model řidiče *Driver* je model sloužící pro simulaci šoféra. Z pohledu celého systému se jedná o jeden z nejdůležitějších automatů. Automat cca po 5 vteřinách vyšle signál řídící jednotce vozidla ke startu vozidla, což je simulací otočení klíčku v zapalovací skříně a následnému startu motoru. Následně se automat přesune do stavu `ready`, ze kterého jsou dva možné přechody do stavů *pedal_accelerator* nebo *pedal_braking*, oba s pravděpodobností 50%. Po uskutečnění jednoho z přechodů se automat v daném stavu zacyklí (maximální počet cyklů je dán proměnnou `MAX_THROTTLE/MAX_BRAKE`). Automat cyklením náhodně zvolí polohu plynového/brzdového pedálu v rozmezí 0-100 v násobcích čísla 10 [25].



Obrázek 3.5: Automat řidiče znázorňující jeho činnost. [6]

[5] viz str 19. https://www.fit.vut.cz/study/thesis-file/20623/20623.pdf
[6] viz str 21. https://www.fit.vut.cz/study/thesis-file/20623/20623.pdf

Po uplynutí jedné časové jednotky (v modelu reprezentována jako desetina vteřiny) se automat vrátí do původního stavu `ready`. Na základě hodnot `pedal_accelerator` a `pedal_braking` se při vyhodnocení funkce *velocity()* vypočítá zrychlení `a`.
Proměnná `pedal_braking` je odečtena od proměnné `pedal_accelerator` a výsledná hodnota v intervalu [-100,100] je dále rozdělena na devět menších intervalů. Dle hodnoty z výsledného intervalu je následně vypočítáno zrychlení *a*. Jelikož je pravděpodobnost na zrychlování/brzdění stejná a snahou automatu je, aby před testem nabyl určité rychlosti, tak je ve funkci *velocity()* zvolena vhodná množina proměnných, která zabezpečuje, že auto bude s větší pravděpodobností akcelerovat. Pro zajištění simulace reálné dopravní situace na běžné komunikaci po překročení $135 kmh^{-1}$ lze automobil pouze zpomalovat. Omezením velikosti proměnné zrychlení v intervalech rychlosti vozidla od [45,55], [85,95] a [125,135] lze simulovat reálnou situaci, kdy se řidič snaží dodržovat povolené rychlosti v obci, mimo obec a na dálnici. Je žádoucí, aby vozidlo bylo testováno právě z těchto rychlostí [25].

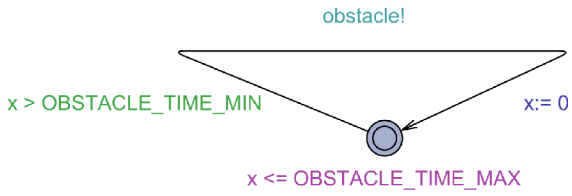
Model obsahuje rovněž vytvořenou funkci, která nastaví počáteční rychlost ze dvou důvodů.

1. Standardizované testy. Počátky všech testů mají stejnou rychlost a testy nebudou zkresleny různou počáteční rychlostí.

2. Testy jsou primárně zaměřeny na nouzové brzdění. Z toho důvodu je tedy lepší, aby tento moment nastal v dřívějším okamžiku testování. Další výhodou jsou přehlednější grafy z testování.

Při cyklení mezi stavy brzdění a akcelerace může automat obdržet signál *obstacle* značící výskyt překážky na cestě. Řidičova reakce je v rozmezí [8,12] časových jednotek a po uplynutí času reakce řidiče dochází k nouzovému brzdění. Čas reakce je opět snahou o přiblížení se reálné situaci, jelikož i řidič v reálném provozu nereaguje okamžitě, ale s určitou časovou prodlevou. Ostatní automaty se o nouzovém brzdění dozví díky nastavení proměnné `danger` na hodnotu 1. Po zastavení vozidla dojde k výpočtu statistických údajů - čas brzdění, průměrná brzdná síla, dráha brzdění s/bez reakčního času řidiče [25].

Model překážky *ObstacleSpotted* má jedinou funkcionalitu a tou je generování události *obstacle*. Automat díky signálu *obstacle* informuje řidiče o vzniku krizové situace. Událost je generována v intervalu [`OBSTACLE_TIME_MIN`,`OBSTACLE_TIME_MAX`]. V modelu jsou tyto hodnoty nastaveny na [100,105]. V případě testování vozidla před nouzovým brzděním je potřeba nastavit počáteční rychlost na nulovou, prodloužit délku simulace v testech a nastavit proměnné `OBSTACLE_TIME_MIN`/`OBSTACLE_TIME_MAX` na vyšší hodnoty [25].

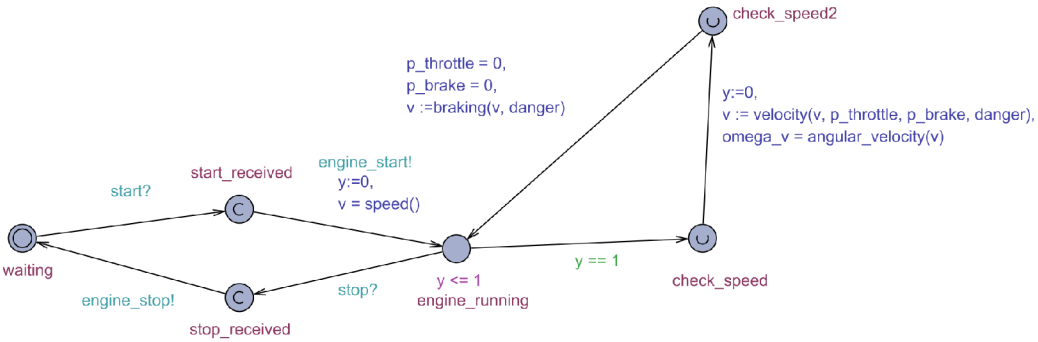


Obrázek 3.6: Automat generující překážku. [7]

[7] viz str 21. https://www.fit.vut.cz/study/thesis-file/20623/20623.pdf

Model řídící jednotky *ControlUnit* za pomocí signálů řídí startování a vypnutí motoru vozidla. Po nastartování motoru je v modelu přiřazena počáteční rychlosti funkcí *speed()*. Rychlost může být nulová, náhodná a nebo pevně definovaná uživatelem dle konstant v modelu. Následně automat cyklí mezi stavy *check_speed* a *check_speed2* ve kterém počítá rychlost, úhlovou rychlost a brzdnou sílu v případě nouzového brzdění. Funkce *velocity()* počítá zrychlení `a` na základě poměru stlačení brzdového pedálu a plynového pedálu. Dle vzorce $v = v_0 + a * t$ se na základě rychlosti z předchozího cyklu a nové hodnoty zrychlení vypočítá výsledná rychlost. Jednotkou času je opět jedna desetina vteřiny. Funkce *angular_velocity* vypočítá za pomocí vzorce $\omega = v/R$ úhlovou rychlost na základě aktuální rychlosti [25].

Funkce *braking()* v případě běžného provozu přenechává výpočet rychlosti funkci *velocity()*. V případě nouzového brzdění se hodnota decelerace a nová hodnota rychlosti vypočítá právě ve funkci *braking()*. Výpočet vychází z upraveného vzorce $F = m * a$, kde za celkovou sílu působící proti vozidlu je považována brzdná síla `F_b`, která je součtem síly tření a odporu vzduchu. Vypočtené zrychlení je následně vloženo do vzorce pro rovnoměrně zpomalený pohyb [25].



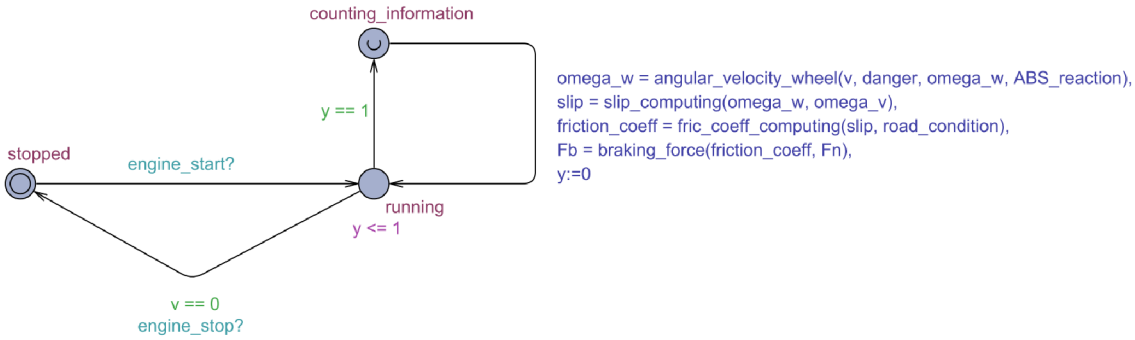
Obrázek 3.7: Automat představující práci ŘJ. [8]

Model kola *Wheel* pracuje obdobně jako model řídící jednotky ve smyslu cyklením se mezi dvěma stavy pro výpočet průběžných výsledků. Funkce *angular_velocity_wheel()* počítá úhlovou rychlost kola na základě referenční rychlosti vozidla. Při události nouzového brzdění je tato funkce zodpovědná za simulací vzniku skluzu pneumatiky a rovněž simuluje snížení tlaku elektromagnetickým ventilem ABS. Skluz kola se vytváří dělením úhlové rychlosti kola jednou ze dvou empiricky zvolených konstant $\{1.1, 1.2\}$ na základě stochastického rozhodnutí. Dělením úhlové rychlosti se snižuje úhlová rychlost kola. V případě vypnutého systému ABS a velmi vysoké počáteční rychlosti, nebo při sněžných podmínkách lze dosáhnout až k hodnotě 0, čímž je dosaženo maximálního skluzu (100%). Snižování brzdného tlaku probíhá v případě zasáhnutí systému ABS. Chování systému je zajištěno pomocí opětovného dělení původní rychlosti kola empiricky zvolenými parametry $\{0.7, 0.8, 0.9\}$. Automat se nejprve pokouší o největší redukci brzdného tlaku vydělením úhlové rychlosti kola konstantou 0.7 a poté zkouší větší konstanty. Kritériem uplatnění dané konstanty je, aby nově vypočítaná rychlost nebyla větší, než referenční rychlost vozidla, jelikož při volně se odvalujícím kole se tyto hodnoty rovnají. Při brzdění nemůže vzniknout situace, při

[8] viz str 22. https://www.fit.vut.cz/study/thesis-file/20623/20623.pdf

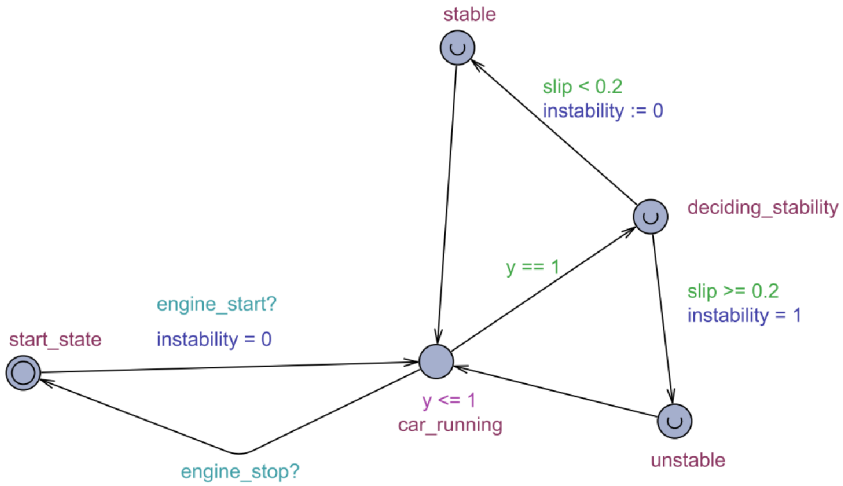
které by kolo mělo větší úhlovou rychlost než úhlová rychlost vozidla. Jediným případem, kdy daná situace může nastat je při prudkém zrychlování. Funkce *fric_coeff_computing()* počítá koeficient tření na základě křivky mu-slip, což je závislost tření na skluzu. Funkce *slip_computing()* vypočítává skluz na základě vzorce $slip = 1 - \frac{\omega_w}{\omega_v}$. Funkce *braking_force()* vypočítává brzdnou sílu jak součin tlakové síly a koeficientu tření [25]. Model dále obsahuje dva režimy [25]:

1. `DRY` - simulace suché vozovky.
2. `SNOWY` - simulace zasněžené vozovky.



Obrázek 3.8: Automat reprezentující kolo vozidla. [9]

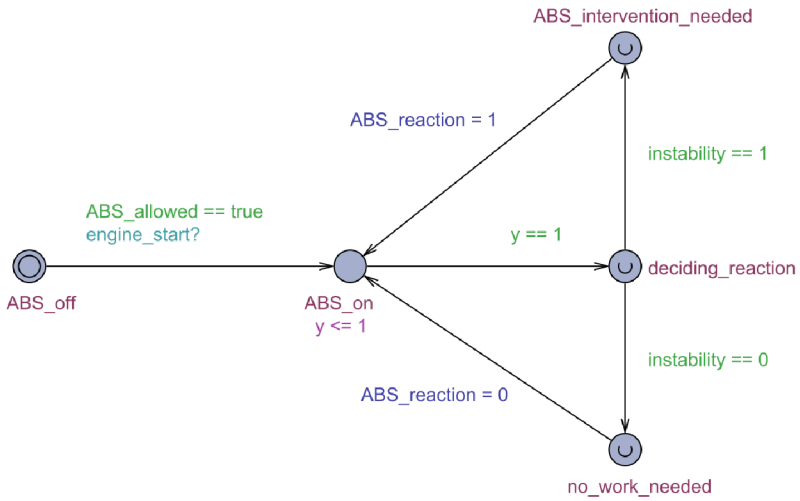
Model skluzu *Slip* se na základě hodnoty skluzu rozhoduje, zda se skluz nachází v oblasti stability (`slip` < 0.2), nebo v oblasti nestability (`slip` ≥ 0.2). Hodnota 0.2 by měla představovat zlom funkce, kdy na základě skluzu je hodnota tření nižší a brzdný účinek menší. Zmíněná hodnota se může lišit pro různé podmínky vozovky, a proto nemusí být nejvhodnější a nejefektivnější pro všechny stavy vozovky. V automatu se nastavuje proměnná `instability` značící oblast (ne)stability [25].



Obrázek 3.9: Automat pro implementaci skluzu vozidla. [10]

[9] viz str 23. https://www.fit.vut.cz/study/thesis-file/20623/20623.pdf

Model ABS *ABS* je automat implementující řídící jednotku systému ABS. Automatu je z výchozího stavu povolen přechod do následného stavu jen v případě, že je systém ABS zapnutý (*ABS_allowed == true*). Automat je ovládán proměnnou `instability`, která ovlivňuje jeho reakci. V případě, že se automat dostane do stavu *ABS_intervention_needed*, tak je to signál že se skluz dostal do oblasti nestability, brzdění se stalo neefektivním, vozidlo ztrácí kontrolu a je zapotřebí reakce systému ABS. Snížení brzdného tlaku zajišťuje již dříve popsaná funkce *angular_speed_wheel()*. V případě zapnutého systému ABS automat cyklí mezi stavy {*ABS_on*, *deciding_reaction*, *ABS_intervention_needed* , *no_work_needed*} [25].



Obrázek 3.10: Automat reprezentující činnost systému ABS.[11]

3.3.2 Model ESP

Autorem modelu vozidla se systémem ESP je Bc. Filip Weigel z roku 2020 [41]. Systém ESP (**E**lectronic **S**tability **C**ontrol) je jedním ze systémů aktivních prvků bezpečnosti vozidla. Pro jeho správnou funkcionalitu je zapotřebí přítomnosti funkčního systému ABS a ASR ve vozidle. Systém a model ABS byl představen v předchozí sekci. Systém ASR (**A**nti-**S**lip **R**egulation) je systém pro zvýšení bezpečnosti akcelerujícího vozidla. Pracuje podobně jako systém ABS s rozdílem, že se jedná o systém, který stabilizuje vozidlo při akceleraci, nikoliv deceleraci. Systém ESP zvyšuje kontrolu na vozidlem při nebezpečných situacích, příkladem může být rychlá jízda v zatáčce, jízda na kluzkém povrchu, náhlá změna směru atp. V závislosti na jízdních podmínkách snižuje nebezpečí smyku a zlepšuje stabilitu vozidla [17].

[10] viz str 23. https://www.fit.vut.cz/study/thesis-file/20623/20623.pdf
[11] viz str 23. https://www.fit.vut.cz/study/thesis-file/20623/20623.pdf

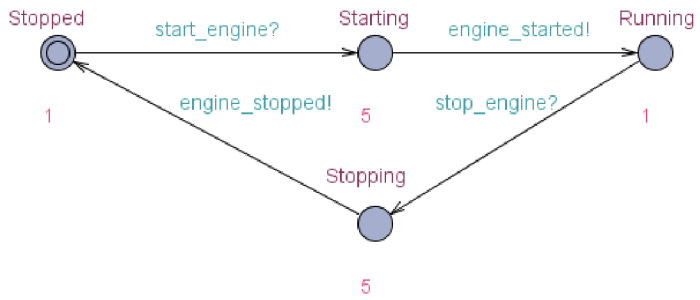
Princip systému ESP

ESP stabilizuje jízdní dynamiku a snaží se zabránit nebo minimalizovat smyk vozidla v příčném směru. Regulace jízdní dynamiky využívá prvků systémů ABS a ASR. Navíc obsahuje senzory pro snímání příčného zrychlení vozidla, senzory stáčení vozidla (úhlová rychlost kolem svislé osy), které jsou umístěny co nejblíže těžišti vozidla a dále snímač natočení volantu. Systém ESP je schopen opačného jevu jako systém ABS. Systém ABS je schopen kola odbrzdit, snížit brzdný účinek a zlepšit tím stabilitu vozidla. Systém ESP je naopak kola schopen přibrzdit a tím pomoci k větší stabilitě vozidla. Dále je systém ESP schopen omezit výkon motoru pomocí přerušení dodávky paliva, vynecháním zápalu směsi v motoru atp. Brzděním jednotlivých kol za všech okolností lze dosáhnout vyšší stability pro požadovaný směr jízdy. Jízdní nestabilitě je zabráněno pomocí přibrzďování některého z vybraných kol, nebo naopak zrychlení některého z hnaných kol [41].
Systém ESP nezasahuje do řízení, pokud je dosažena plná stabilita. Systém ESP vyhodnotí na základě rychlosti vozidla, natočení kol, zrychlení vozidla podélné/příčné překročení mezní stability vozidla a zasáhne do řízení vozidla. Moderní automobily jsou již vybaveny elektronickým natáčením volantu. V případě překročení mezní stability vozidla systém ESP nebere zřetel na požadavky řidiče, jako zvýšení natočení úhlu volantu, sešlápnutí plynového pedálu a snaží se vozidlo udržet ve stabilní oblasti [41].

Implementace modelu

Model vozidla se systémem ESP se sestává ze šesti automatů. Popis jednotlivých automatů a jejich funkcionality bude popsán v následných oddílech.

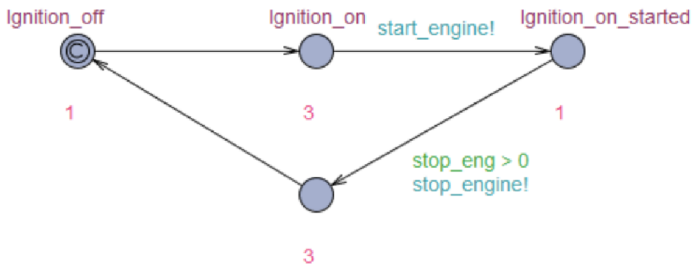
Model motoru *Engine* je jednoduchý čtyřstavový automat. Ve stavu *Stopped* je motor zastaven a nepracuje. Ze stavu *stopped* může pomocí synchronizačního signálu *start_engine* od řídící jednotky automobilu začít startovat a přejít do stavu *Starting*, přičemž tato činnost trvá cca půl vteřiny, poté motor přejde do stavu *Running* a zašle synchronizační signál *engine_started* ostatním automatům. V běžícím stavu poté čeká na signál *stop_engine* a v případě obdržení signálu provede zhašení motoru, což opět zabere asi půl vteřiny a vyšle signál *engine_stopped* [41].



Obrázek 3.11: Automat motoru vozidla. [12]

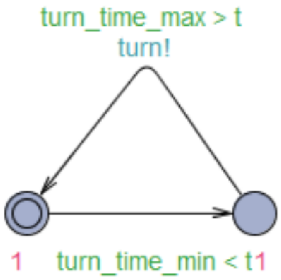
[12] viz str 24. https://www.fit.vut.cz/study/thesis-file/21569/21569.pdf

Model řídící jednoty *ECU* je implementace řídící jednotky motoru, která je opět čtyřstavová. *Initial* stavem je zde *Ignition_off* simulující vypnuté zapalování. Automat následně přejde do stavu *Ignition_on* simulující otočení klíčkem, kde setrvá přibližně tři desetiny vteřiny. Poté vysílá synchronizační signál *start_engine*, dochází ke startu motoru, motor je nastartován a automat opět poté čeká na změnu proměnné `stop_eng`, aby mohl vyslat signál *stop_engine* [41].



Obrázek 3.12: Automat řídící jednotky vozidla. [13]

Model zatáčky *Turn* je dvoustavový automat. Cílem automatu je v intervalu `turn_time_min` až `turn_time_max` vyslat synchronizační signál *turn* oznamující příchozí zatáčku. Hodnoty lze měnit, ale nastavení příliš nízkých hodnot znamená zpravidla chybnou funkcionalitu modelu, jelikož automobil nedosáhne požadované rychlosti. Rovněž je vhodné zvolit delší interval, protože při příliš krátkém intervalu nemusí synchronizační signál zachytit ostatní automaty. Výchozí hodnoty pro tyto proměnné jsou `120` a `130` [41].



Obrázek 3.13: Automat příchozí zatáčky. [14]

Model kola *Wheel* je pětistavový automat. Při obdržení synchronizačního signálu *engine_started* od automatu motoru přejde automat do nepojmenovaného stavu a přechází mezi dvěma stavy ve smyčce, dokud neobdrží signál *engine_stopped*. Pokud automat cyklí mezi dvěma stavy, tak dochází k volání funkce *speed_update()*, což je nejdůležitější funkce celého modelu ESP. Vyhodnocují se zde všechny důležité výpočty a probíhá zde rozhodování systému ESP. Ve funkci *speed_update()* dojde k zavolání funkce *stability_rate()*, která vyhodnotí míru stability vozidla. Stabilitu vozidla vyhodnocuje pouze v případě, že řidič neotáčí volantem a předpokládá, že případný prokluz při akceleraci/deceleraci vyhodnocují systémy ABS/ASR. Při otočení volantu se míra stability vyhodnocuje na nápravě, na které

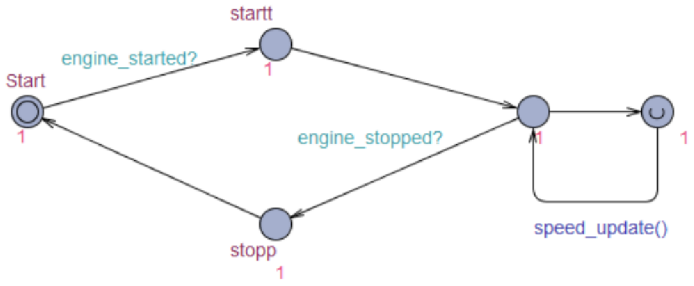
[13] viz str 25. https://www.fit.vut.cz/study/thesis-file/21569/21569.pdf
[14] viz str 24. https://www.fit.vut.cz/study/thesis-file/21569/21569.pdf

dochází k nestabilitě. Vyhodnocení stability se vypočteno jako poměr mezi potřebnou silou pro zatočení a silou, kterou jsou schopny pneumatiky přenést při zatáčení [41].

Při stabilizaci vozidla mohou nastat dvě situace:

1. Vyžadovaná brzdná síla je menší nebo rovna, než je limitní síla pneumatik (`req_moment` $\leq$ `ffk/rfk`).
2. Vyžadovaná brzdná síla je větší, než limitní síla pneumatik (`req_moment` $>$ `ffk/rfk`).

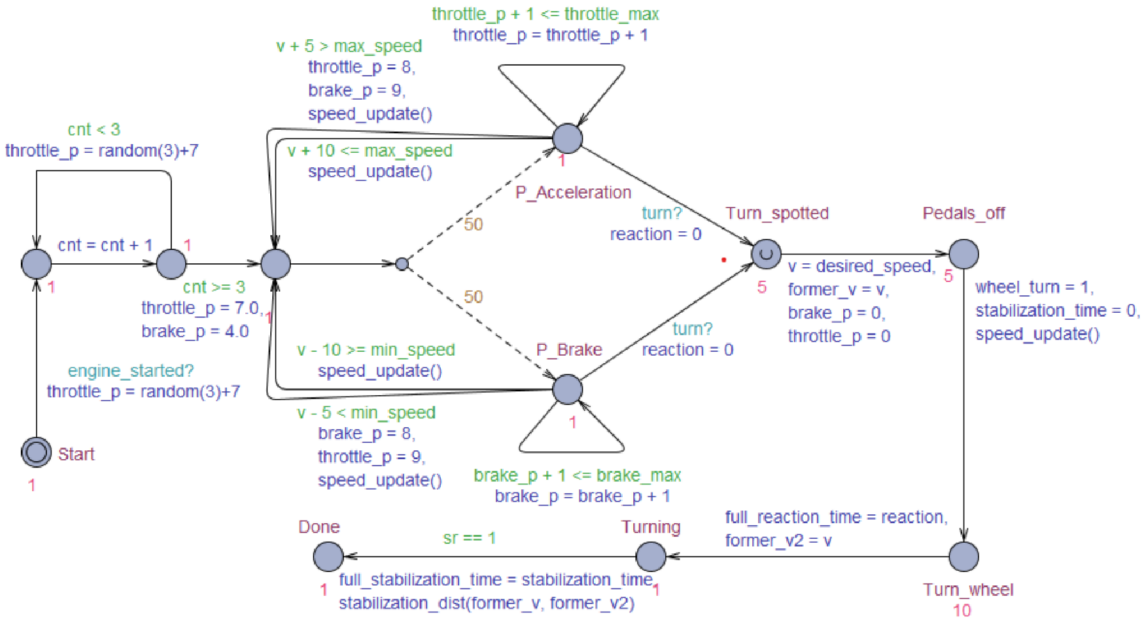
Ve funkci je vypočten moment potřebný (`req_moment`) pro získání plné stability a taktéž je vypočtena síla potřebná pro zatočení na přední a zadní nápravě (`ffk/rfk`). Pokud není volant natočen doleva, ani doprava, dochází k zavolání funkce *velocity()* a k výpočtu nové rychlosti [41].
Při zachycení signálu *turn* modelem řidiče dochází k otočení volantu řidičem a vozidlo začne zatáčet. Nyní funkce vyhodnotí, že řidič otočil volantem (`wheel_turn` $\neq 0$) a je zapotřebí zjistit míru stability. Pokud systém ESP zvládá vozidlo stabilizovat je míra stability téměř rovna 100%. Model zanedbává přenos váhy, vítr v zatáčce atd. je od míry stability odečteno náhodné číslo *random(0.05)* pro kompenzaci malé nepřesnosti modelu. Systém ESP vypočítá potřebný brzdný moment a uloží si jeho absolutní hodnotu. Pokud je vozidlo nedotáčivé je moment záporný a pokud přetáčivé, tak je naopak kladný. Na základě orientace zatáčky (pravotočivá/levotočivá) rozhodne systém ESP, které kolo přibrzdí. Příkladem může být, že ESP na základě vyhodnocení proměnných zjistilo, že je zapotřebí aplikovat brzdnou sílu na pravé zadní kolo, a tudíž zavolá funkci *ESP_brake_rr*. Ve funkci je změněn stav ESP z neaktivního na aktivní proměnnou `ESP_active` a je vypočítán potřebný brzdný moment.
Pokud nastala první situace a vyžadovaná brzdná síla je menší, než limitní síla pneumatik, tak dojde k aplikaci $\frac{1}{10}$ brzdné síly, zavolání funkce *stability_rate()* a zavolání funkce *velocity()* ve které dojde k aplikaci brzdné síly [41].
V případě druhé varianty, kdy je vyžadovaná brzdná síla větší, než limitní síla pneumatik je aplikována $\frac{1}{10}$ maximální brzdné síly za vteřinu, zavolána funkce *stability_rate()* s rozdílem, že vozidlo není plně stabilní a opět zavolána funkce *velocity()* [41].



Obrázek 3.14: Automat pro simulaci kola automobilu. [15]

[15] viz str 27. https://www.fit.vut.cz/study/thesis-file/21569/21569.pdf

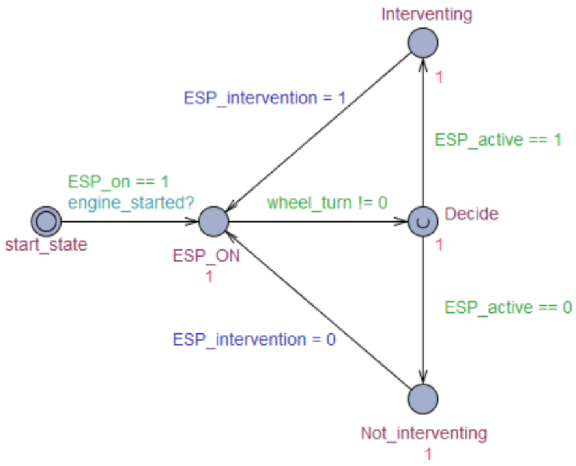
Model řidiče *Driver* obsahuje 11 stavů. Po startu motoru obdrží řidič synchronizační signál *engine_started* a je připraven k jízdě. Řidič nejprve sešlápne plynový pedál v intervalu [7,10] a dosáhne prvotní akcelerace. Řidič je nucen ve dvou iteracích cyklu držet pedál sešlápnutý ve stejné intervalu pro dosažení rozumné rychlosti. Po celkem třech iteracích je řidiči umožněno šlapat na brzdový pedál a plynový pedál. Řidič se stochasticky rozhodne s pravděpodobností 50% pro akceleraci/deceleraci. V dalším stavu má možnost plynový/brzdový pedál několikrát více sešlápnout. Poté dojde k aktualizaci rychlosti zavoláním funkce *speed_update()*. Dále pokračuje v cyklu sešlapováním brzdového/plynového pedálu, přičemž se řidič snaží dodržovat jemu povolené rychlosti (`min_speed`,`max_speed`). Při obdržení synchronizačního signálu *turn* z generátoru zatáčky může automat uskutečnit přechod do stavu *Turn_spotted* ve kterém dojde k zaznamenání nájezdové rychlosti a puštěním pedálů akcelerátoru a brzdy. Rychlost lze taktéž skokově upravit na požadovanou hodnotu `desired_speed` pro účely testování. Řidiči trvá cca půl vteřiny, než zatáčku zpozoruje, poté další půl vteřiny trvá otočení volantem. Dále řidič pouze drží volant ve směru zatáčky a dále nezasahuje do řízení. [41].



Obrázek 3.15: Automat *Driver* reprezentující řidiče. [16]

[16] viz str 28. https://www.fit.vut.cz/study/thesis-file/21569/21569.pdf

Model ESP *ESP_ECU* je automat reprezentující systém ESP. Z výchozího stavu *start_state* je povolen přechod do dalšího stavu *ESP_ON* pouze v případě, že je systém ESP zapnut (*ESP_on*) a pokud je motor nastartován *engine_started*. Dále systém vyčkává na příchozí zatáčku reprezentovanou `wheel_turn`. V momentu, kdy řidič otočí volantem a proměnná `wheel_turn` není rovna nule, dojde k aktivaci činnosti systému ESP. Systém ESP zjišťuje, zda je zapotřebí zasáhnout do řízení vozidla, či nikoliv. Pokud vyhodnotí, že je třeba zasáhnout, nastaví se hodnota proměnné `ESP_intervention` na jedničku a dojde k zásahu ESP do řízení. V opačném případě systém ESP nijak nezasahuje do řízení a hodnota `ESP_intervention` je nastavena na nulu [41].



Obrázek 3.16: Model motoru vozidla. [17]

3.3.3 Model samočinně parkujícího vozidla

Autorem modelu vozidla se systémem ESP je Bc. Marek Krucina z roku 2021 [30]. Samočinně parkující vozidlo je vozidlo s integrovaným systémem pro parkování. Jedná se o komfortní prvek výbavy vozidla se zvýšením bezpečnosti při parkování. Vozidlo by mělo být schopné zaparkovat z jízdního pruhu vedoucí parkovištěm na příslušné parkovací místo. Samotný parkovací manévr je proveden kombinací ovládání rychlosti a natočení úhlu kol. Nejčastěji se lze setkat s podélným parkováním, jelikož podélné parkování je považováno za nejtěžší druh parkování. Systémy automatického parkování by měly být schopny kolmého, šikmého i podélného parkování včetně nalezení parkovacího místa na parkovišti [30].

Princip modelu samočinně parkující vozidla

Pro orientaci vozidla na parkovišti slouží vodorovné dopravní značení. Systém automatického parkování může být realizován dvěma způsoby: [30].

1. Parkoviště bylo postaveno za účelem automatického parkování a v parkovacím systému je implementována komunikace s vozidly. Parkoviště by mělo obsahovat podpůrné senzory, které mají za cíl pomoct vozidlu v navigaci parkovištěm bez přítomnosti

[17] viz str 26. https://www.fit.vut.cz/study/thesis-file/21569/21569.pdf

řidiče. Systém parkoviště by měl dále obsahovat čidla pro detekci volných parkovacích míst a taktéž by měl vozidlo na parkovací místo navést nejrychlejším a nejkratším způsobem.

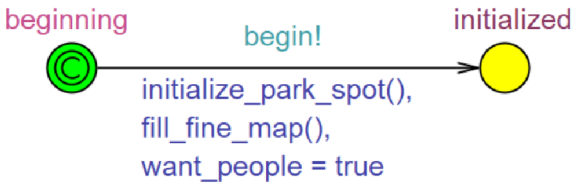
2. Parkoviště nebylo postaveno za účelem automatického parkování, tudíž se jedná o obyčejné parkoviště. Parkující vozidlo tedy nemá žádný podpůrný systém, se kterým by mohlo komunikovat a cestu k volnému parkovacímu místu, které si musí také samo vyhledat. Zde se již předpokládá, že vozidlo disponuje skutečně autonomním systémem.

Model je zaměřen na první způsob, tedy autonomně parkující vozidlo s komunikující systémem parkoviště. Systém působí, že bude spolehlivější pro rychlost a efektivitu parkování vhodnější [30].

Implementace modelu

Model samočinně parkujícího vozidla využívá několik abstrakcí reálného světa. Navržené parkoviště obsahuje vozovku, nosné konstrukce, 30 parkovacích míst, vjezd a výjezd z parkoviště. Vjezd a výjezd z parkoviště je jednosměrný, zatímco vozovka mezi parkovacími místy je obousměrná. Parkoviště je navrhnuto jako 2D pole.
Samočinně parkující vozidlo je abstrahováno jako osobní vozidlo s rozměry: délka $= 4.7m$ a šířka $= 1.9m$. v 2D poli je vozidlo reprezentováno třemi políčky na šířku a osmi na délku. Poloměr otáčení je stanoven na $5.3m$.
Zatáčení na parkovišti je realizováno pomocí Reeds-Sheppových křivek, které se využívají k výpočtu nových souřadnic. Hlavním bode je střed vozidla a krajní body se dle středových souřadnic a úhlu natočení vozidla přepočítávají. Křivky se nevyužívají pouze při zatáčení v zatáčce, ale i při (vy)parkování [30].

Model inicializátoru *Initializer* je automat pomocí kterého je spuštěn celý model. Prvním krokem je výběr náhodného místa k zaparkování zavoláním funkce *initialize_park_spot()*. Na vstupní mapě poté označí místo hodnotou 10 a vytvoří jemnější mapu parkoviště pomocí funkce `fill_fine_map()`. Proměnná `want_people = true` povolí pohyb lidí po parkovišti. Prostředí je inicializováno a lze vyslat řídící signál `begin` k předání řízení [30].

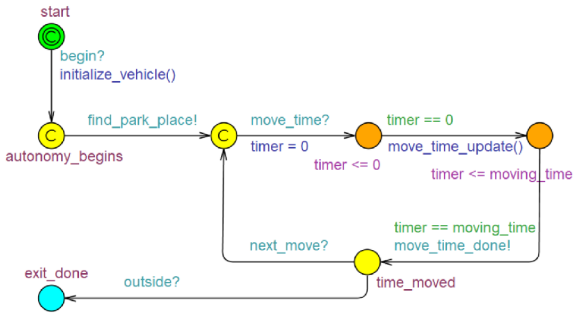


Obrázek 3.17: Automat inicializátoru. [18]

Model řídícího automatu *Car* je automat reprezentující samočinně parkující vozidlo. Automat svoji činnost začíná přijetím signálu *begin*. Prvně proběhne inicializace vozidla pomocí funkce *initialize_vehicle()*, vozidlo obdrží souřadnice a pozici na mapě u vjezdu na parkoviště. Automat se přesune do stavu *autonomy_begins* a zahájí hledání parkovacího

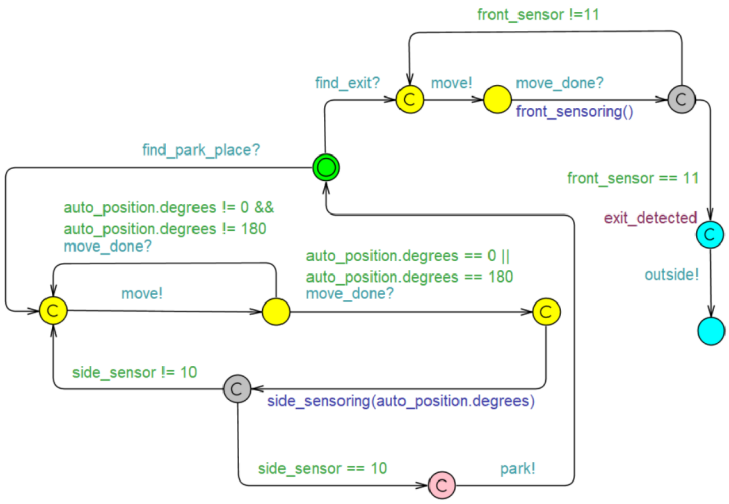
[18] viz str 26. https://www.fit.vut.cz/study/thesis-file/23481/23481.pdf

místa signálem *find_park_place*. Po přijetí signálu *move_time* automat vypočítá proměnnou `moving_time` značící trvání doby pohybu vozidla. Automat dále čeká, než daná doba uplyne. Po uplynutí časové doby se automat přesune do stavu *time_moved* a vysílá signál *move_time_done*. V případě potřeby dalšího pohybu se automat vrátí na začátek cyklu. Pokud automat přijme synchronizační signál *outside* znamená to, že je vozidlo na výjezdu a vozidlo se dostane do stavu *exit_done* [30].



Obrázek 3.18: Automat reprezentující vozidlo. [19]

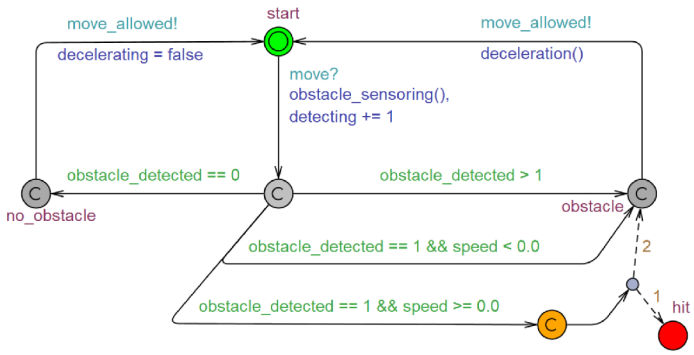
Model detekce parkovacího místa a výjezdu reprezentuje automat *Pathfinder*. Začíná přijetím signálu *find_park_place*. Automat vysílá signál *move*. Poté, co je pohyb vykonán je automat synchronizován signálem *move_done*. V této chvíli vozidlo projíždí kolem parkovacích míst a hledá jemu přiřazené parkovací místo. V případě, že senzory nedetekují dané parkovací místo, tak se automat vrací do původního stavu a opět vysílá signál *move*. Pokud senzory detekovaly určené parkovací místo, tak se automat přesune do dalšího stavu a vyšle signál *park*. Automat se vrátí do původního stavu a vyčkává na přijetí signálu *find_exit*, který znamená, že vozidlo již hledá cestu ven z parkoviště. Následně se opakuje podobný cyklus jako při hledání parkovacího místa. Při detekci výjezdu z parkoviště automat přechází do finálního stavu a vysílá signál *outside* [30].



Obrázek 3.19: Automat reprezentující *pathfinder*. [20]

[19] viz str 27. https://www.fit.vut.cz/study/thesis-file/23481/23481.pdf
[20] viz str 28. https://www.fit.vut.cz/study/thesis-file/23481/23481.pdf

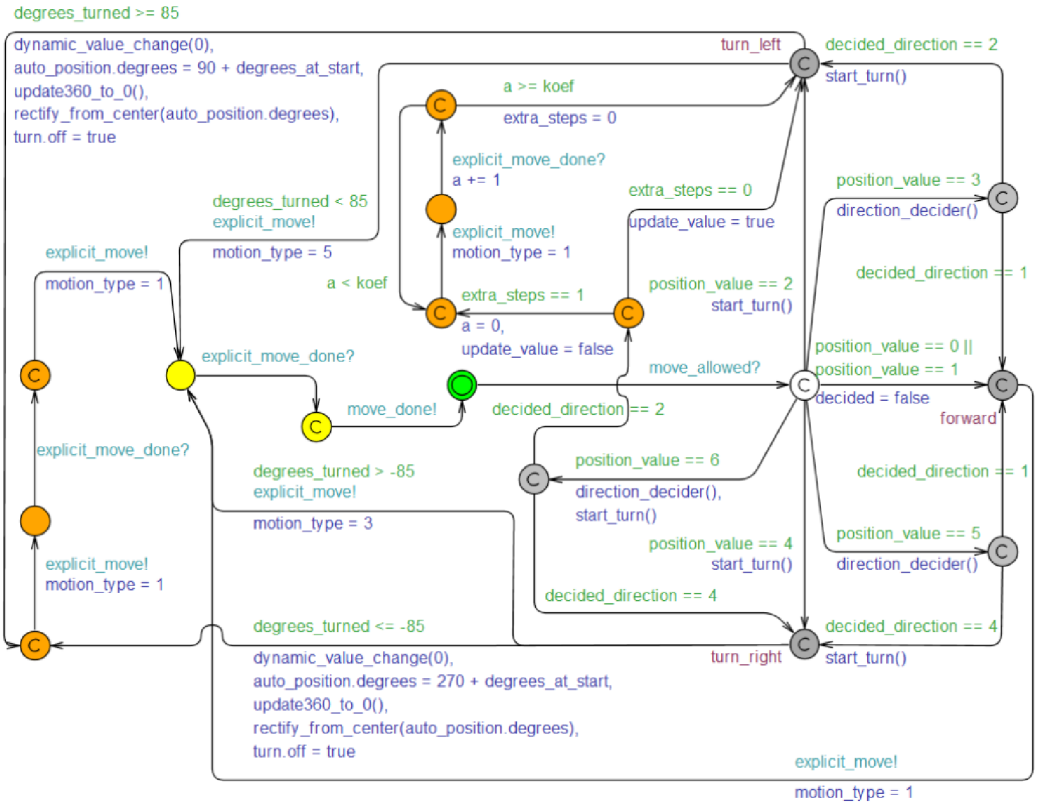
Model překážek je reprezentován automatem *ObstacleSensor*, jehož úkolem je detekovat a reagovat na překážky. Činnost automatu je zahájena pomocí synchronizačního signálu *move*. Automat snímá prostor před vozidlem v šířce $3m$ a do dálky taktéž $3m$ v pěti úrovních. Pokud není žádná překážka detekována, automat přejde do stavu *no_obstacle* odkud vyšle signál *move_allowed* a pokračuje ve snímání. V případě detekce překážky automat uskuteční přechod do stavu *obstacle*. Je-li překážka detekována v těsné blízkosti (do $60cm$) a rychlosti vozidla je nenulová je šance 1 ku 2, že nastane srážka a simulace skončí nezdarem. Jinak se srážce podaří zabránit a automat opět uskuteční přechod do stavu *obstacle*. Zašle signál *move_allowed* a sníží rychlost pomocí funkce *deceleration()* v závislosti na vzdálenosti překážky [30].



Obrázek 3.20: Automat senzoru překážky. [21]

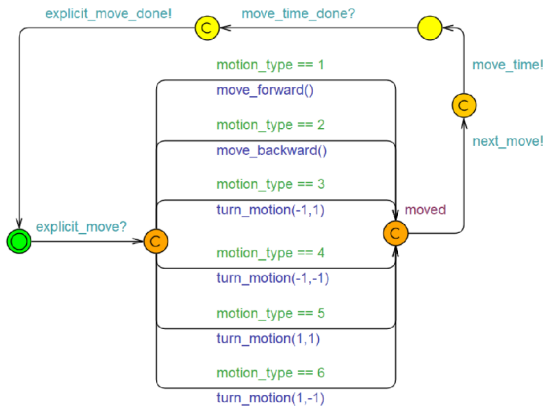
Model pohybu je reprezentován automatem *MoveConductor*. Činnost automatu začíná přijetím signálu *move_allowed*. Následuje přechod do rozhodovacího stavu dle proměnné `position_value`. Při hodnotách $\{3, 5, 6\}$ jsou následující povolené stavy šedé barvy. Pomocí funkce *direction_decider()* je nutné rozhodnout směr, dle kterého se automat rozhodne a dalšími povolenými stavy jsou *turn_left*, *turn_right* a *forward*. Pokud se vozidlo nenachází na konci zatáčky, tak následně přechází do levého žlutého stavu, vysílá signál *explicit_move* a nastavuje hodnotu proměnné `motion_type`. Pokud je pohyb vykonán, přijme signál *explicit_move_done* a vyšle signál *move_done*, kterým vrací řízení zpátky automatu *Pathfinder*.
V případě, že je vozidlo na konci zatáčky (`degrees_turned` ≥ 85 nebo `degrees_turned` ≤ -85) dojde k aktualizaci údajů a automatu je umožněn přechod do levého spodního oranžového stavu. Následně dokročí po zatáčce a poté už shodně jako v ostatních případech se dostane do prvního ze žlutých stavů a vyšle signál k poslednímu pohybu [30].

[21] viz str 29. https://www.fit.vut.cz/study/thesis-file/23481/23481.pdf



Obrázek 3.21: Automat pohybu vozidla. [22]

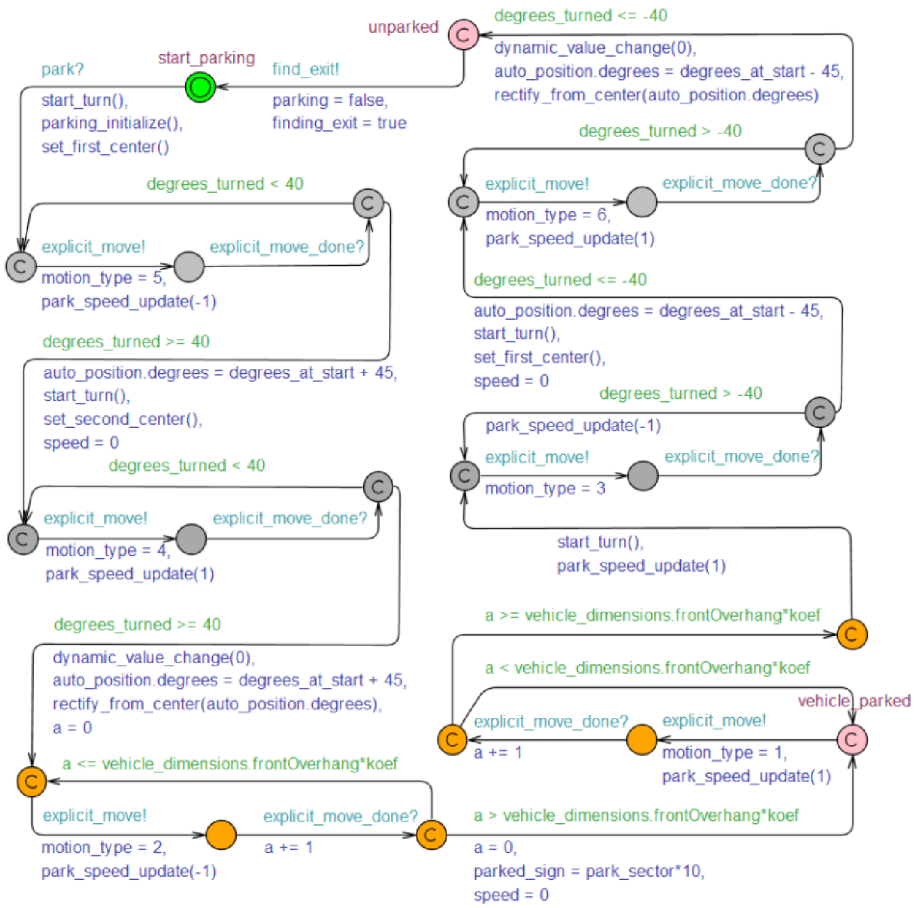
Model vykonání pohybu *Carmover* je automat, který začne svoji činnost signálem *explicit_move*. Dle hodnoty proměnné `motion_type` vykoná příslušnou funkci provádějící pohyb vozidla upravením souřadnic, dle kterých provede aktualizaci hodnot na mapě parkoviště. Automat se nachází ve stavu *moved*, vysílá signál *next_move* a *move_time*. Následuje posun času. Po posunutí času a přijetí signálu *mode_time_done* se automat může přesunout do dalšího stavu, ze kterého vysílá signál *explicit_move_done* [30].



Obrázek 3.22: Automat vykonání pohybu vozidla. [23]

[22] viz str 30. https://www.fit.vut.cz/study/thesis-file/23481/23481.pdf
[23] viz str 31. https://www.fit.vut.cz/study/thesis-file/23481/23481.pdf

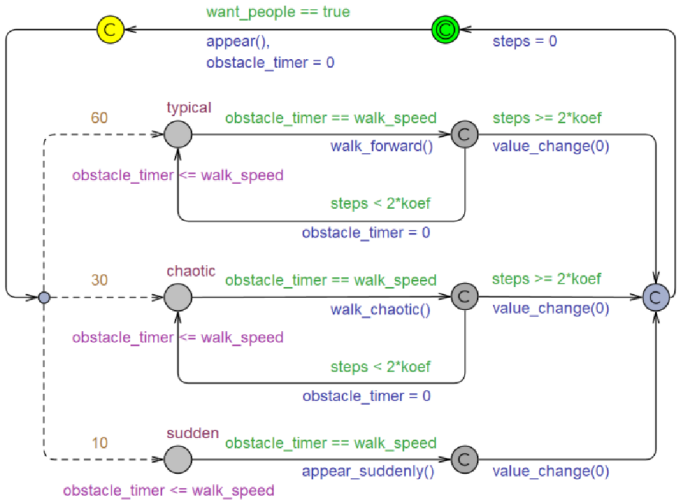
Model parkování *Parker* je spuštěn signálem *park* a dojde k volání funkce *start_turn()*. Funkce zabezpečuje nulování hodnot `degrees_turned` a nastavení proměnné `degrees_at_start` pro uložení hodnoty natočení vozidla před otáčením. Vyhodnoceny jsou také hodnoty `parking_initialize` pomocí funkce *set_first_center()* k potřebnému parkovacímu manévru. Automat provede přechod do šedých stavů začínajícího cyklu. Je vyslán signál *explicit_move* pro vykonání pohybu a funkce *park_speed_update(-1)* začne snižovat rychlost. Po příjmu signálu *explicit_move_done* je potvrzeno vykonání pohybu je nutné rozhodnout, zda v otáčení pokračovat (vozidlo se otočilo o méně než 40°), nebo přejít k další fázi parkování. Při další fázi parkování následuje další přechod do tmavě šedého stavu a začíná cyklus couvání doprava. Velikost natočení vozidla je přepočítána a funkcí *start_turn* je zahájeno další zatáčení. Funkce *set_second_center()* nastavuje novou pozici centra otáčení. Přes kanály *explicit_move* a *explicit_move_done* se komunikuje s automatem *Carmover* pro vykonání pohybu. Funkcí *park_speed_update(1)* se navyšuje rychlost [30].
Po dokončení couvání doprava je automatu umožněn přechod do prvního z oranžových stavů značící dojetí rovně na parkovací místo. Pohyb probíhá opět v cyklu a rychlost se snižuje až na nulu. Poté se automat nachází ve stavu *vehicle_parked*. Následuje vyparkování, které je složené ze stejných pohybů, ale v opačném směru. Po vyparkování je umožněn přechod do stavu *unparked*, vysílá signál *find_exit* a vozidlo hledá výjezd z parkoviště [30].



Obrázek 3.23: Automat modelu parkování vozidla. [24]

[24] viz str 32. https://www.fit.vut.cz/study/thesis-file/23481/23481.pdf

Model překážek *Peoplemaker* je automat pro reprezentaci pohybujících se překážek, zejména chodců. Automat je schopen řídit právě jednu překážku v daný moment. Pro větší hustotu provozu na parkovišti je nutné přidat automat několikrát za pomocí konstanty `N`. Funkcionalita automatu je povolena při změně hodnoty `want_people` z `false` na `true`. Pomocí funkce *appear()* se na mapě vygeneruje překážka, která je generována v oblasti zastavěných a parkovacích míst. Překážky mohou ihned vstoupit do vozovky a tím blokovat provoz [30]. Následuje rozhodnutí, zda se automat přesune do stavu *typical* s 60% pravděpodobností a simuluje chodce přecházejícího vozovku. V cyklu se vykoná určitý počet kroků pomocí funkce *walk_forward*, která aktualizuje souřadnice chodce na mapě. Cyklus se opakuje, dokud chodec vozovku nepřejde. S 30% pravděpodobností bude překážka svůj pohyb vykonávat chaoticky a automat přejde do větve *chaotic*. Zpravidla se jedná o typ chodce, který se pohybuje kolem kufru svého vozidla. S 10% pravděpodobností se překážka zjevuje ve vozovce náhle - demonstruje nepozorné lidi, děti, či zvířata, které se mohou náhle zjevit ve vozovce. Zmizení překážky je ovšem stejně rychlé, jako objevení [30].



Obrázek 3.24: Automat pro simulaci chodců ve vozovce. [25]

Vhodnost modelů pro analýzu rizik

Model systému ABS je určitě vhodným kandidátem pro analýzu rizik. Model není nijak triviální, ale zároveň není komplexní čili optimálně složitý. Mezi jeho výhody patří určitě přímočarost, dobrá funkcionalita, dále je model schopen zachovat funkčnost při limitované funkcionalitě systému ABS (výpadek ABS, selhání čidla otáček atp.). Nevýhodou by mohla být abstrakce kol, jelikož autor pracoval pouze s jedním kolem, které reprezentovalo všechna čtyři kola.

Model systému ESP je taktéž vhodným kandidátem pro analýzu rizik. Taktéž je optimálně složitý, přímočarý a funkční. Výhodou je, že model je schopen pracovat korektně i při limitované funkcionalitě systému ESP (při selhání systému ESP, při selhání čidla atp.) Nevýhodou je abstrakci brzdných a akceleračních sil, které jsou implementovány jako síly působící s/proti danému kolu.

[25] viz str 33. https://www.fit.vut.cz/study/thesis-file/23481/23481.pdf

Model samočinně parkujícího vozidla je vhodným kandidátem. Jedná se však o poměrně komplexní a netriviální model. Výhodou modelu je jeho velmi pěkná implementace a funkčnost. Dále na rozdíl od předchozích modelů není model samočinně parkujícího vozidla schopen funkčnosti při limitované funkcionalitě (selhání senzorů, selhání parkovacího asistenta atp.). Model by vyžadoval důkladnou analýzu a pravděpodobně větší změny v modelu. Což jsou jeho hlavní nevýhody.

Kapitola 4

Návrh a řešení analýzy rizik založené na modelech

V této kapitole bude prezentován navržený model analýzy rizik, hlavní kroky v analytickém procesu jednotlivých modelů a jejich případné úpravy včetně srovnání s původním modelem. V modelech bude zapotřebí identifikovat potencionální hazardy, spouštěcí události, které se mohou stát iniciátorem hazardu. Taktéž budou představeny stromy událostí vedoucí k dané spouštěcí události a jejich případné následky. Rovněž bude možné nahlédnout na implementovaný systém analýzy rizik formou modelu v prostředí *UPPAAL*.

4.1 Návrh analýzy rizik

Základním předpokladem pro analýzu rizik je dostupnost modelu v prostředí *UPPAAL* a jeho funkčnost. Dostupné modely byly představeny v předchozí kapitole.
Konkrétně: model ABS 3.3.1, model ESP 3.3.2 a model samočinně parkujícího vozidla 3.3.3.
Samotná analýza rizik bude ovlivněna subjektivním faktorem autora, jelikož pro objektivní identifikaci rizik by bylo zapotřebí analytického týmu, kde je možno subjektivní faktor potlačit.

Reálné systémy a fyzikální děje, které mají vliv na pohyb vozidla a analýzu rizik jsou velmi komplexní a ve většině případů těžko popsatelné. Je vhodné se zamyslet nad požadovanou mírou abstrakce a zvážit detaily, které je možno zanedbat a které zjednodušit. Bude zapotřebí vyvarovat se velkým zásahům do již implementovaných modelů, provedení analýzy rizik a implementace navrženého systému. Jedním z požadavků je taktéž zachování plné funkcionality modelu při vypnutí systému analýzy rizik. Systém je navržen jako *stand-alone*, tudíž aby mohl nezávisle na modelu plnit svoji funkci, odhalovat potencionální rizika a případně se s rostoucím rizikem vypořádat.

Předpokládané vstupy a výstupy

Nezbytným vstupem je samozřejmě model systému společně se stářím vozidla. Spolehlivost komponent je ovlivněna jejich stářím a dále je ovlivněna dobou, kdy byla komponenta aktivně používána. Výrobce komponenty (senzor, procesor atp.) udává její spolehlivost zpravidla hodnotou `Mean time between failures (MTBF)` [14]. Hodnota střední doby mezi

poruchami je uváděna v hodinách aktivního používání komponenty. Střední doba mezi poruchami se využívá hlavně u komponent, které se po uplynutí doby mezi poruchami opravují. Při poruše je identifikována vadná součástka komponenty/systému a je vyměněna za novou, nebo repasována. Taktéž existují komponenty, u nichž se nevyplatí vadnou součástku měnit. V takovém případě se komponenta při poruše vymění rovnou za novou, a proto výrobci zavedli nový ukazatel, který je pojmenován `Mean time to failure (MTTF)` [14].

Dalším ze vstupů do systému analýzy rizik je ohodnocení střední doby do poruchy senzoru. Senzorů je v modelu několik. Zde je uplatněna jistá míra abstrakce. Senzory otáček fungují většinou na principu elektromagnetické indukce [13]. Senzor zrychlení může být v systému implementován pomocí inerciální měřicí jednotky (2.2.1), která obsahuje akcelerometr. Dalším senzorem může být senzor rychlosti vozidla, který na základě otáček motoru a zařazeného rychlostního vypočítává celkovou rychlost vozidla. Tato hodnota může být zkreslena z důvodu zablokovaných/prokluzujících kol vozidla.
Je zřejmé, že představené senzory pracují na rozdílných principech. Druhů a typů senzorů s různou funkcionalitou existuje skutečně velmi mnoho, a proto jsou všechny typy senzorů v modelu abstrahovány jako jeden senzor, který je ohodnocený na základě hodnoty `MTTF`. Předpokladem pro užití hodnoty `MTTF` je, že vadný senzor se jakožto komponenta systému neopravuje, ale rovnou se vymění za nový.

Stáří automobilu je rovněž jistou mírou abstrahováno. Na světě neexistují dvě stejná vozidla, která „stárnou“ stejně rychle. Rozdíly ve stárnutí vozidla jsou dány výrobcem vozidla, použitými komponentami, uskladněním vyrobeného vozidla, následným prodejem vozidla jeho uživateli a poté samotné uživatelovo zacházení s vozidlem. Záleží vždy na výrobci, jak kvalitně automobil vyrábí, zda užívá vhodné technologické postupy, zda nakupuje kvalitní komponenty, dále taktéž záleží na jednotlivých zaměstnancích výrobce, s jakým nasazením a pečlivostí přistupují k výrobě vozidla.

Pokud výrobce dodržuje všechny technologické postupy, pracuje s kvalitními součástkami a i zaměstnanci přistupují k práci svědomitě, tak je zvýšena pravděpodobnost, že všechny komponenty vyrobeného vozidla budou funkční po stanovenou dobu životnosti vozidla. Dalším z faktorů je skladování vozidla před prodejem zákazníkovi. Vozy zpravidla stojí vyrobené na odstavných parkovištích u výrobce. Čas od výroby vozidla ke konečnému prodeji zákazníkovi má taktéž schopnost ovlivnit životnost vozidla.

Hlavním faktorem životnosti vozidla spolu s kvalitní výrobou je uživatelovo zacházení s vozidlem. I kvalitní výrobek může být zničen v krátkém časovém horizontu, pokud k němu uživatel nepřistupuje s respektem a neužívá jej vhodným způsobem. Příkladem nevhodného chování může být například nadměrná zátěž vozidla před dosažením provozní teploty všech komponent, nevhodné skladování - uživatel pravidelně parkuje své vozidlo na travním porostu, který zadržuje vlhkost způsobující korozi komponent/vozidla, preferovaným jízdním stylem (brzda-plyn [20]) atp.

Předpokladem tedy je, že výrobce dodržel stanovené postupy, vozidlo bylo vhodně skladováno, uživatel k němu bude přistupovat svědomitě a bude jej správně používat. Při zanedbání všech zmíněných vlivů se výpočet stáří vozidla v hodinách vypočítá následovně:

```
opotřebení [h] = (nájezd / průměrná rychlost) +
                 (stáří * stárnutí za rok)
```

kde:

- `opotřebení` je ohodnocení výsledného stáří automobilu v hodinách,
- `nájezd` je nájezd vozidla v kilometrech (stav tachometru),
- `průměrná rychlost` je průměrná rychlost vozidla v $[kmh^{-1}]$. Moderní automobily počítají průměrnou rychlost, dokud ji uživatel nevynuluje, poté se průměrná rychlost počítá znovu,
- `stáří` je stáří vozidla v letech,
- `stárnutí za rok` je ohodnocení průměrné doby stárnutí vozidla za rok v $[h]$. Komponenty vozidla podléhají stárnutí i při jeho nepoužívání.

Výstupy z modelu budou prezentovány v dalších sekcích práce. Bude se jednat zejména o experimentování s simulačními modely a z nich vycházející grafy simulace. Každý experiment bude popsán spolu s komentářem průběhu daného experimentu, zachyceny budou nejdůležitější proměnné modelu včetně ukázky funkcionality systému analýzy rizik.

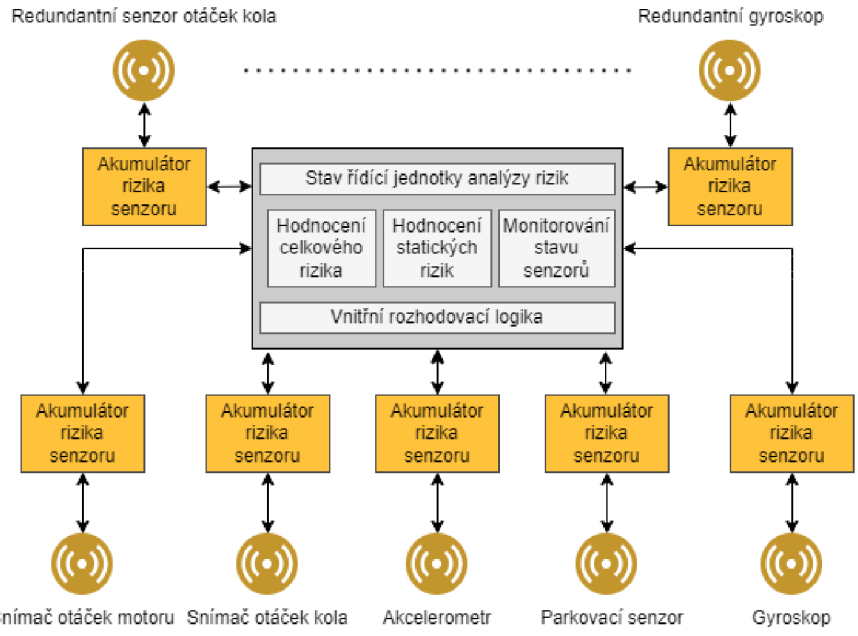
Koncept systému analýzy rizik

Při návrhu konceptu analýzy rizik byly uvažovány dva druhy nejistot, a z nich plynoucí rizika. Prvním druhem jsou epistemické nejistoty, které byly popsány v sekci. 2.3.

Epistemické nejistoty budou v systému reprezentovány staticky ohodnoceným rizikem. Riziko se vyhodnotí pouze jedenkrát za běh simulace a jeho hodnota se nebude po celý průběh měnit.
Epistemické nejistoty jsou nejistoty, které lze určitým způsobem redukovat, například opakovanými měřeními, podrobnějším zkoumáním daného jevu atp. Statické riziko bude chápáno jako riziko, které přímo souvisí s modelem daného vozidla v daném systému. Příkladem takového rizika může být chyba gravitačního zrychlení [2]. Gravitační zrychlení nemá vždy stejnou hodnotu. Dle místa na zemském povrchu se jeho velikost nepatrně mění. Nejedná se o velké odchylky od dohodnuté střední hodnoty ($a_g = 9,80665 ms^{-2}$), ale přesto se jedná o jistou míru rizika, jelikož modely pracují zpravidla s hodnotou $9,81 ms^{-2}$.
Dalším ze zástupců epistemických nejistot může být celková váha modelu vozidla. Váha vozidla má na chování vozidla velký vliv. Ovlivňuje chování vozidla při akceleraci. Dvě totožná vozidla se stejnými parametry (výkon motoru, opotřebení brzd, ...), avšak jedno z vozidel plně naložené (řidič, 4 spolujezdci a $200 kg$ v nákladovém prostoru) nemají zcela jistě totožné akcelerační zrychlení. To stejné platí i pro brzdění, kdy těžší z vozidel bude mít delší brzdnou dráhu a taktéž pro chování vozidla v zatáčce. V průběhu jízdy se váha vozidla dále může měnit vlivem čerpání paliva do motoru a jeho spalováním, umýváním skel kapalinou do ostřikovačů atd.

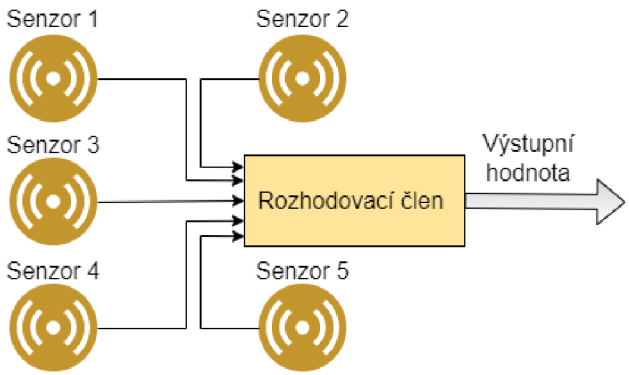
Druhým zástupcem nejistot jsou aleatorní nejistoty. Aleatorní nejistoty byly popsány v sekci. 2.3
Aleatorní nejistoty budou v modelech reprezentovány jako možná selhání jednotlivých součástek. Reprezentovány budou pomocí náhodné změny v činnosti součástky. Součástka poté nebude vykonávat požadovanou funkci a bude se projevovat nestandardním chováním. Selhávání součástky bude ohodnocováno určitou mírou rizika, která se bude kumulovat, narůstat s časem a s postupným selháváním dané součástky. Selhání součástky v reálném světě může být způsobeno mnoha faktory. Může se jednat například o únavu materiálu [22], kdy dochází k pomalu postupujícímu a kumulujícímu se poškozování materiálu. Únava materiálu vzniká z důvodu opakovaného zatěžování.
Průběh závisí na počtu opakovaných cyklů a taktéž na použitém materiálu. Při dosažení mezi únavy dochází zpravidla k únavovému lomu a destrukci materiálu/spoje. Dalším z faktorů je mechanické poškození vodiče elektrického signálu, nebo části dané komponenty. Příkladem mechanického poškození může být kamínek, který odskočí od protijedoucího vozidla a narazí do dané komponenty, čímž dojde k jejímu poškození. Mechanické poškození může způsobit i uživatel vozidla svojí nepozorností vedoucí k nehodě. Taktéž svojí nedbalostí, kdy při parkování najede na obrubník, ze kterého vozidlo následně spadne a poškodí komponentu.

Systém analýzy rizik by měl být dostatečně všeobecný a dobře škálovatelný, aby jej bylo možné aplikovat i na jiné systémy/modely, které nebudou v této práci prezentovány. Na obrázku 4.3 je možno nahlédnout na navrženou logiku systému analýzy rizik. Systém se sestává z řídící jednotky rizik, akumulátorů rizika daných senzorů a samotných senzorů. Řídící jednotka může taktéž pracovat s redundantními senzory. Na senzory jsou kladeny vysoké nároky z hlediska přesnosti a taktéž z hlediska spolehlivosti. Systém tedy může obsahovat (nemusí) redundantní senzory.



Obrázek 4.1: Schéma obecného zjednodušeného systému analýzy rizik.

Systémy s redundantními senzory jsou v reálném světě hojně rozšířeny. Redundantní čidla se mohou nacházet hned v několika různých konfiguracích.
Jedna z konfigurací je využívána v této práci. Konkrétně se jedná o konfiguraci, ve které je aktivní pouze jeden senzor, dokud je plně funkční. Při detekci nestandardního chování je senzor odpojen a jeho místo převezme senzor náhradní. Nevýhodou této konfigurace je vyžadovaná implementace detekce nestandardního chování. Další z možných konfigurací je konfigurace, při které jsou aktivní všechny senzory zároveň, každý senzor zasílá svoje naměřené hodnoty řídicí jednotce, řídící jednotka všechny přijaté hodnoty zprůměruje a vypočítá výslednou hodnotu [26].
Za zmínku stojí i zajímavá konfigurace senzorů využívající hlasovací systém. Do rozhodovacího členu systému jsou zaslány data od všech senzorů. Rozhodovací člen funguje na „demokratickém“ principu ve smyslu, kdy většina přehlasuje menšinu. Příkladem může být konfigurace s pěti senzory, které měří stejný jev. Tři nebo čtyři senzory zašlou stejnou korektní hodnotu rozhodovacímu členu a poslední senzor zašle hodnotu chybnou. Většina v tomto případě „přehlasuje“ vadný senzor a správně změřená hodnota zvítězí.
Nevýhodou je, že pokud náhle selže většina senzorů, tak poté systém pracuje s chybnými hodnotami. Pracuje s nimi i za předpokladu, že zbylá menšina senzoru zasílá správné hodnoty [6].



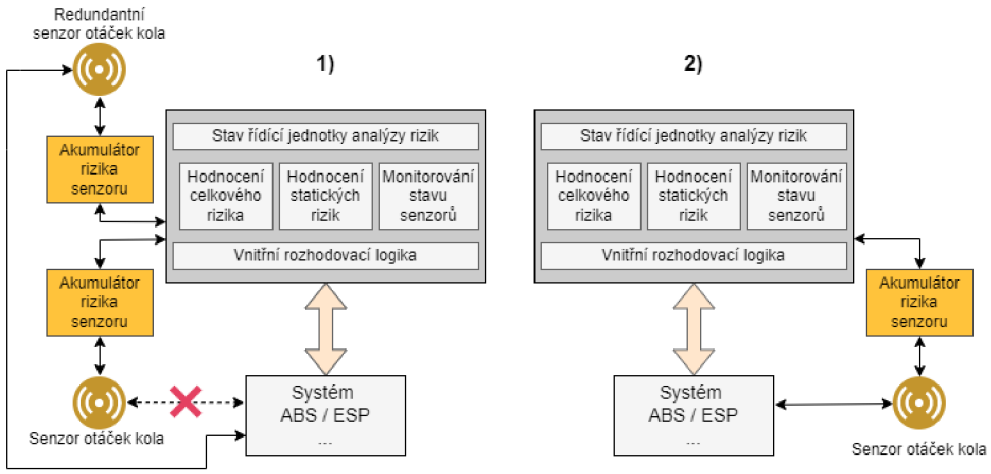
Obrázek 4.2: Implementace pěti senzorů s rozhodovacím členem.

Systém analýzy rizik komunikuje se senzory a přijímá jejich naměřené hodnoty. Naměřené hodnoty poté porovná s hodnotami, které „očekává“, neboli hodnoty, které si na základě chování vozidla, řidiče a jiných okolností předpočítá. Pokud senzor zasílá hodnoty, které se významně liší od vypočítaných hodnot, tak je to znamení nesprávného chování. Systém tedy senzor ohodnotí určitou mírou rizika, které se uloží do akumulátoru rizika daného senzoru a rovněž se uloží do akumulátoru celkového rizika.
V případě, že senzor pokračuje ve svém nesprávném chování, tak systém rizik dále ohodnocuje senzor určitou mírou rizika, až do překonání předem stanovené hranice. Po překročení předem definované hranice je zapotřebí, aby systém analýzy rizik zasáhl do funkcionality systému, který se na korektní data od senzoru spoléhá.

Navržené řešení v systému analýzy rizik dle konfigurace senzorů:

1. Systém disponuje redundantními senzory, a proto je schopen zasáhnout do funkcionality systému odpojením identifikovaného vadného senzoru a taktéž je schopen selhávající senzor nahradit redundantním senzorem.

2. Systém nedisponuje redundantními senzory. Nekorektní data ze senzoru mohou implikovat nekorektní chování některého ze systémů ABS, ESP, parkovací asistent atp.



Obrázek 4.3: 1) Detekce, odpojení vadného senzoru a připojení náhradního senzoru
2) Systém nemá k dispozici žádný náhradní senzor.

Rozhodnutí v situaci, kdy systém analýzy rizik nedisponuje náhradními senzory je složité a choulostivé. Ve vzniklé situaci by pravděpodobně bylo nejlepší, kdyby ji analyzoval člověk a ten rozhodl, co se v daný moment a situaci jeví jako nejlepší řešení. Člověk ovšem systému není schopen nijak pomoci, jelikož elektronické součástky pracují v řádech mikrosekund až nanosekund ($10^{-9}s$) a rozhodnutí je potřeba vykonat okamžitě.
Systém je tedy v rozhodnutí osamocen. Za daných okolností jsou možné pouze dvě varianty:

1. Systému ABS, ESP atp. zaslat informaci, že senzory s jejichž daty pracuje jsou nesprávná a proto by bylo vhodné systém úplně deaktivovat k předejití nesprávného chování, které může vést například k nehodě.

2. Systém ABS, ESP atp. informovat o skutečnosti, že senzory podávají nesprávná data, tudíž by bylo vhodné reakci daného systému zmírnit. V případě systému ESP to může znamenat, že systém nebude aplikovat plnou brzdnou/akcelerační sílu na zvolené kolo. Aplikovat může například polovinu dané síly po stanovenou dobu (záleží na konkrétní situaci), čímž si zachová svoji funkcionalitu, byť jen částečnou.

Systém analýzy rizik by mohl být implementován jako samostatný systém ve vozidle, který by byl zařazen na stejnou úroveň jako podpůrné systémy ABS, ESP atp. případně by mohl být integrován přímo v hlavní řídící jednotce vozidla.
V rámci kooperace s těmito systémy by mohl se systémy komunikovat, pracovat s údaji ze senzorů, monitorovat jejich stav a v případě potřeby poskytnout podpůrným systémům doporučení, jak se ve vzniklé situaci zachovat.

Výhodou by bylo, že by byl jeden systém analýzy rizik pro všechny podpůrné systémy. Dále by pracoval se všemi senzory, tudíž by měl přehled o celém vozidle. Nevýhodou je, že by se stal tzv. *single point of failure*. Dále by musel mít implementovanou konkrétní reakci na vzniklou situaci pro každý podpůrný systém zvlášť.

Systém analýzy rizik by taktéž mohl být integrován přímo do řídící jednotky daného podpůrného systému a s konkrétním systémem kooperovat. V takovém případě by systémů analýzy rizik bylo ve vozidle více, protože vozidla jsou zpravidla vybavena několika podpůrnými systémy jako ABS, ESP, hlídání jízdního pruhu, parkovací asistent atp. Hlavní výhodou integrace systému analýzy rizik přímo do podpůrného systému by bylo jeho „ušití" na míru danému systému. Dále by byla zmenšena pravděpodobnost výpadku komunikace, jelikož by se systém pro analýzu rizik nacházel přímo v daném podpůrném systému. Nevýhodou by bylo, že by poté vozidlo mělo hned několik systémů pro analýzu rizik.

4.2 Proces hodnocení rizik modelu ABS

V následující sekci bude prezentován analytický proces v hodnocení rizik pro systém ABS. Rozdělen bude do pěti kroků. Podrobné informace a doporučený postup v analytickém procesu byl popsán v sekci 2.3.2.

Popis systému a jeho modelování

V tomto kroku by měl být analytický proces zaměřen na popis systému a jeho modelování. Systém byl již Dominikem Holcem [25] popsán a namodelován. Popis modelu a jeho model byl popsán v sekci 3.3.1. Díky této skutečnosti je možné tento krok přeskočit.

Identifikace hazardu

Model systému ABS je zaměřen zejména na nouzové brzdění z důvodu nečekané události, jako může být nečekané brzdění automobilu před daným vozidel, vběhnutím dítěte na vozovku, nedání přednosti v jízdě protijedoucím vozidlem atp. Hlavním hazardem je tedy brzdění a adekvátní reakce systému ABS na blokující se kola v průběhu brzdění. Systém pracuje s několika druhy fyzikálních veličin, které mohou být zdrojem nejistot a případných hazardů. Hazard je zpravidla odhalen prostřednictvím svých projevů a je aktivován určitou spouštěcí událostí.

Identifikovaným hazardem je selhání některého ze senzorů systému ABS. Kombinace hazardu a spouštěcí události je představována pomocí určité hrozby. Z hrozby může dále vzniknout škoda na majetku, zdraví, životním prostředí atp. Špatné údaje ze senzorů, na které se spoléhá řídící jednotka systému ABS může vyvolat neadekvátní reakci systému na vzniklou událost. Následky neadekvátní reakce mohou mít lehké i vážné dopady na řidiče, jeho případné spolujezdce, protijedoucí vozidlo, na automobil jedoucí za vozidlem se systémem ABS atp.

Navrženým ochranným opatřením je implementace systému analýzy rizik do současného systému ABS pro detekci a rozhodování v krizových situacích.

Doporučením pro největší snížení pravděpodobnosti výskytu hazardu spojeným se selháním některého ze senzorů je pravidelná výměna senzorů vzhledem k jejich životnosti. O této skutečnosti by měl být uživatel vozidla informován prostřednictvím palubního počítače, který by měl uživateli sdělit, že pro správnou a bezchybnou funkcionalitu je zapotřebí senzory vyměnit.
Dalším snížením pravděpodobnosti nežádoucího chování je implementace systému analýzy rizik do vozidla.

Výběr spouštěcích událostí

V předchozí sekci byl identifikován hazard v podobě selhání senzoru při nouzovém brzdění. Nyní je zapotřebí odhalit a přidělit jednotlivé spouštěcí události k danému hazardu. Stejný hazard může být vyvolán v přes různé spouštěcí události a mít stejné, či odlišné následky.

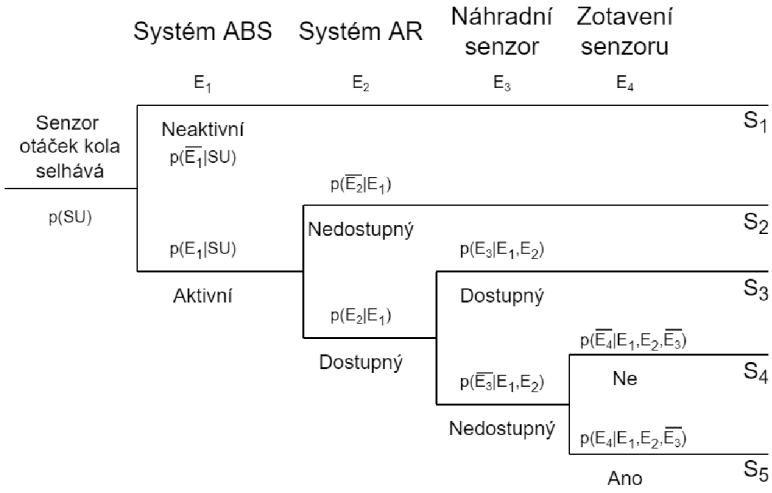
Hazard je ovlivněn zejména daty ze senzoru, jelikož velmi záleží na tom, jaká data senzor zasílá. Může se jednat o zcela nesmyslná data, kdy senzor zasílá informaci o nízkém počtu otáček kol za minutu, což je pro systém signál, že je kolo zablokované, dochází ke ztrátě kontroly nad vozidlem, je dosaženého vysokého skluzu a je zapotřebí kolo odbrzdit. Kolo však vůbec nemusí mít nízký počet otáček, a může dosahovat optimálního skluzu pro brzdění a být stále ovladatelné.
Reakce systému ABS je v tomto případě povolení brzdného tlaku, aby došlo k odblokování daného kola, byla opět získána kontrola nad vozidlem a dosaženo optimální hodnoty skluzu. Jelikož kolo není blokované a vozidlo je ovladatelné, dojde ke snížení brzdného účinku a tím i k delší brzdné dráze.

Fatálním scénářem může být podobná situace s rozdílem, kdy systém ABS díky svoji neadekvátní a špatné reakci zcela vyřadí z provozu brzdy neustálým povolováním brzdného tlaku. V takovém případě se vozidlo stává velmi nebezpečným, protože může dojít ke srážce s chodcem, protijedoucím vozidlem atp.

Strom událostí

Za pomoci stromu událostí je možné díky systematičnosti poodhalit vztahy, které vedou k dané nežádoucí události. Začátkem stromu událostí je předem definovaná událost selhání systému ABS a zpětné odvíjení příčin až k hlavním poruchám. Prezentovaný strom poruchy bude zaměřen na jedno konkrétní selhání systému. Strom poskytne informace o tom, jak může daná událost nastat a její důsledky. Dále taktéž strom poruch poskytne informaci, která porucha vedla k dané spouštěcí události.

Na níže zobrazeném stromu událostí 4.4 bude možno nahlédnout na jednotlivé větve stromu událostí. Vstupem do stromu událostí je selhávající senzor otáček kol. Vrchní větev stromu ukazuje, že systém ABS je neaktivní a selhávající senzor otáček kola nemá na systém ABS vliv. Pokud je systém ABS aktivní, dalším větvením je dostupnost systému analýzy rizik. Vrchní větev zobrazuje, že systém není dostupný. Dolní větev značí, že systém je dostupný. K dalšímu větvení dojde v případě, že systém analýzy rizik má (ne)dostupný náhradní (redundantní) senzor. V případě nedostupnosti náhradního senzoru je větev dělena naposled a sice na (ne)zotavení selhávajícího senzoru.



Obrázek 4.4: Příklad stromu událostí se spouštěcí událostí.

Hodnocení rizik a proces rozhodování

V posledním kroku je zapotřebí vyhodnotit rizika spojená se scénáři identifikovanými a kvantifikovanými v předchozím kroku. V praxi se zpravidla riziko klasifikuje jako přijatelné, téměř přijatelné a nepřijatelné.
Scénáře s přijatelnou mírou rizika jsou S_1 a S_3. V prvním scénáři je systém ABS neaktivní, tudíž selhávající senzor není rizikem. Ve třetím scénáři je systém ABS aktivní, systém analýzy rizik je dostupný a taktéž je dostupný náhradní senzor.
Scénář s téměř přijatelným rizikem je S_5, kdy je systém ABS aktivní, systém analýzy rizik dostupný, náhradní senzor nedostupný, ale senzor otáček kola přestane selhávat a zotaví se.
Scénáře s nepřijatelným rizikem jsou S_2 a S_4, kdy je aktivní systém ABS a nedostupný systém analýzy rizik, potažmo systém ABS aktivní, systém pro analýzu rizik dostupný, náhradní senzor nedostupný a nedojde k zotavení senzoru.

4.3 Proces hodnocení rizik modelu ESP

Analytický proces hodnocení rizik pro systém ESP bude tématem následující sekce. Rozdělen bude opět do pěti hlavních kroků.

Popis systému a jeho modelování

První krok by měl obsahovat návrh systému ESP, jeho modelování a verifikaci. Systém již navrhl, namodeloval a verifikoval Filip Weigel [41]. Podrobný popis systému a jeho model v prostředí *UPPAAL* byl popsán v sekci 3.3.2.

Identifikace hazardu

Systém ESP se zaměřuje na chování vozidla v zatáčce, či při nouzovém úhybném manévru. Hlavním hazardem je chování vozidla při zatáčení a případná reakce systému ESP na vzniklou událost. K aktivaci systému ESP může dojít vlivem vysoké nájezdové rychlosti do zatáčky, vběhnutím člověka na vozovku, výskytem nečekaného objektu na vozovce, úhybným manévrem před prudce brzdícím vozidlem atp. Systém vyhodnocuje a pracuje s několika typy fyzikálních veličin. Fyzikální veličiny mohou být zdrojem nejistot, rizik a z toho vyplývajících hazardů.

Hazard, na který je zaměřena implementace modelu ESP je selhání senzoru. Hrozbou při nefunkčním senzoru systému ESP může být škoda na majetku, zranění/usmrcení osoby, poškození životního prostředí atd. Řídící jednotka systému ESP se spoléhá na relevantní informace o jednotlivých součástech systému ESP. Informace pochází z kaskády senzorů, které jsou rozmístěny po celém vozidle. Nepravdivé údaje ze senzorů mohou vyvolat špatné vyhodnocení vzniklé situace systémem ESP. Špatná reakce systému ESP může znamenat například nehodu, jelikož systém ESP může zrychlovat jednotlivá poháněná kola.

Hlavní ochranné opatření spočívá v implementaci kontrolního systému, který bude přijímat informace ze senzorů, vyhodnocovat je a vydávat příslušná bezpečnostní opatření. Příkladem takového systému je navržený systém pro analýzu rizik.

K opotřebení komponent systému dochází jak při jeho používání, tak i při jeho nepoužívání. Při využívání komponent dochází k mechanickému opotřebení jednotlivých součástí dané komponenty. Při nepoužívání komponent dochází k degradaci materiálu z důvodu vnějších vlivů, jako koroze atp. Největšího snížení pravděpodobnosti selhání komponenty je jejich pravidelná výměna, kterou deklaruje výrobce daného vozidla. V případě, že nejsou komponenty pravidelně měněny je vhodné, aby vozidlo obsahovalo i systém pro analýzu rizik, který může zasáhnout do funkcionality systému ESP.

Výběr spouštěcích událostí

Hazard byl identifikován, konkrétně selhání senzoru při aktivním systému ESP, který při jízdě zasahuje do řízení vozidla. Nyní bude důležité odhalit a zároveň přidělit spouštěcí události vedoucí k hazardu.

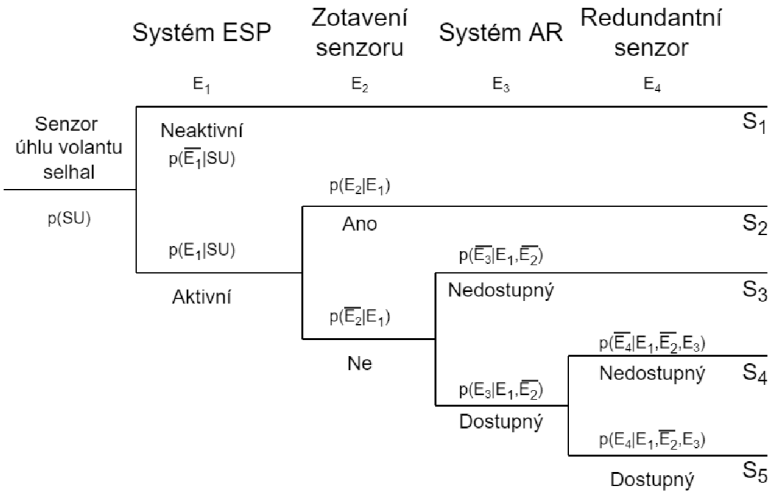
Hazardová situace a odezva systému ESP na vzniklou situaci záleží zejména na údajích, které systému ESP zasílají jednotlivá čidla. Systém ESP pracuje se senzory a spoléhá se na korektnost dat. Při posuzování údajů z senzorů kol systém ESP zajímá počet otáček kola za minutu, ze kterého vyvozuje stav kol, dále posuzuje data z akcelerometru, osazen je taktéž snímačem úhlu natočení volantu atp.

Vadným senzorem může být senzor úhlu natočení volantu, který zasílá údaje o poloze volantu řídící jednotce systému ESP. Vozidlo se vyskytuje v nebezpečné situaci, kdy je systém ESP aktivní, zasahuje do řízení a řidič má volant otočený po směru hodinových ručiček. Senzor polohy volantu ovšem zašle informaci o tom, že řidič má volant otočený na opačnou stranu. Systém ESP údaje ze všech čidel vyhodnotí a usoudí, že řidič zamýšlí jízdu doleva a přibrzdí opačné kolo, než které by měl přibrzdit. Následek se může odvíjet od situace. Nemusí hrozit žádné nebezpečí, jelikož řidič nejede příliš rychle a nachází se na prázdné křižovatce, ale taktéž může hrozit velké nebezpečí, protože se řidič spoléhá na odezvu systému ESP, protože ztratil kontrolu nad vozidlem v zasněžené zatáčce.

Strom událostí

Strom událostí je systematická a deduktivní technika, díky které je možné odhalit jednotlivé vazby mezi nežádoucími událostmi. Na jeho začátku se nachází předem určená událost selhání systému ESP, které dále pokračuje až k hlavním poruchám. Strom poruch bude vytvořen pro konkrétní spouštěcí událost a poskytne informace o tom, jak může krizová událost vzniknout, a dále jaké mohou být důsledky.

Na níže uvedeném stromu událostí 4.5 je možno nahlédnout na jednotlivé větve stromu událostí. Vstupním bodem do stromu událostí je událost, kdy selhává senzor úhlu natočení volantu. Scénář S_1 nastane, pokud senzor selhal, ale systém ESP není aktivní. Scénář S_2 je realizován, pokud je systém ESP aktivní a senzor se zotaví. Scénář S_3 se vyskytne v případě, že je systém ESP aktivní, nedojde k zotavení senzoru a systém analýzy rizik není dostupný. Poslední dva scénáře S_4 a S_5 nastanou, pokud je systém ESP aktivní, nedojde k zotavení senzoru a systém analýzy rizik je přítomen ve vozidle. Scénář S_4 znamená, že systém analýzy rizik nemá dostupný náhradní senzor a S_5 značí, že náhradní senzor přítomen je.



Obrázek 4.5: Příklad stromu událostí se spouštěcí událostí.

Hodnocení rizik a proces rozhodování

V posledním kroku je třeba zhodnotit rizika spojená s jednotlivými scénáři. Riziko se dělí do třech kategorií:

1. Přijatelné
2. Téměř přijatelné
3. Nepřijatelné

Do první kategorie lze zařadit scénář S_1, kdy není systém ESP aktivní a selhávající senzor není rizikem pro řízení vozidla. Druhým scénářem je scénář S_5, kdy je systém ESP aktivní, senzor se nezotaví, systém analýzy rizik je přítomen ve vozidle a je dostupný náhradní senzor.

Do kategorie téměř přijatelných rizik lze zařadit scénář S_2, kdy je systém ESP aktivní a dojde k zotavení senzoru.

Poslední kategorie obsahuje scénáře S_3 a S_4, kdy v prvním případě je systém ESP aktivní, nedojde k zotavení senzoru a systém AR je nedostupný. Druhý scénář je podobného charakteru s rozdílem, že systém analýzy rizik je dostupný, ale není dostupný žádný redundantní senzor.

4.4 Implementace analýzy rizik v prostředí UPPAAL

V následující sekci budou prezentovány upravené modely ABS [25] a ESP [41].

4.4.1 Modifikovaný model systému ABS

Důležitým úkolem při návrhu analýzy rizik v modelu ABS bylo zachování plné funkcionality při deaktivovaném systému analýzy rizik. Tohoto cíle bylo poměrně obtížné dosáhnout, jelikož to zpravidla znamenalo velmi časté a opakované testování modelu pomocí experimentů i při drobných úpravách. Cíle se podařilo dosáhnout a model se s vypnutým systémem chová stejně, jako model původní.

Implementované funkce

calculate_chance_to_failure() - vyhodnocení šance na selhání náhodného senzoru (stochastické)
recover_all_sensors() - provede zotavení všech senzorů v modelu
recovery_chance() - vypočítá šanci na zotavení senzoru (stochastické)
risk_ECU_intervention() - ŘJ analýzy rizik provede zásah do modelu a všechny původní senzory nahradí za senzory náhradní
fail_random_sensor() - funkce pro selhání některého ze senzorů (stochastické)
omega_w_sensor_check() - ŘJ analýzy rizik zkontroluje stav senzoru otáček kola
Fb_sensor_check() - ŘJ analýzy rizik provede kontrolu stavu senzoru brzdné síly
v_sensor_check() - ŘJ analýzy rizik zkontroluje stav senzoru celkové rychlosti vozidla
a_sensor_check() - ŘJ analýzy rizik provede kontrolu stavu senzoru celkového zrychlení vozidla
calculate_epistemic_risk() - funkce pro ohodnocení statického rizika modelu dle 4.1

Konstanty a proměnné

Konstanty datového typu `int`

`MALFUNCION_TIME_MIN` - minimální simulační čas, ve kterém může nastat porucha
`MALFUNCION_TIME_MAX` - maximální simulační čas, ve kterém může nastat porucha
`risk_ECU` - slouží k aktivaci/deaktivaci systému analýzy rizik
`redundant_sensor_available` - definuje dostupnost/nedostupnost redundantních senzorů

Konstanty datového typu `double`

`car_age` symbolizuje stáří vozidla v letech
`average_age_per_year` definuje průměrnou rychlost stárnutí vozidla za rok
`car_mileage` je nájezd vozidla v km
`average_speed` je průměrná rychlost vozidla v $[kmh^{-1}]$
`car_hours` je rovnice pro výpočet doby stáří vozidla v hodinách, dle 4.1
`sensor_mttf` je `mean time to failure` senzorů ve vozidle, dle 4.1
`threshold` slouží k definici horní hranice zákmitové hodnoty daného senzoru
`flick_risk_value` je maximální ohodnocení míry rizika při detekci jednoho zákmitu senzoru
`risk_threshold` je hranice, při které ŘJ analýzy rizik zasáhne do funkce systému ABS
`permanent_failure_risk` je ohodnocení míry rizika při detekci permanentní poruchy
`sensor_chance_to_recover` je šance na zotavení senzoru

Proměnné datového typu `int`

`recovered` slouží k detekci zotavení senzoru
`will_fail` je proměnná rozhodující, zda dojde k selhání senzoru, či nikoliv
`sensor_failure` proměnná, která ukazuje na selhávající senzor. Hodnota 0 značí, že všechny senzory jsou funkční, 1 - senzor otáčení kola, 2 - senzor brzdné síly, 3 - senzor celkové rychlosti vozidla, 4 - senzor zrychlení
`flick_failure` značí, že se jedná o zákmitovou poruchu
`permanent_failure` značí, že se jedná o permanentní poruchu
`permanent_risk_added` je pomocná proměnná, která určuje, zda již bylo připočtena míra permanentního rizika

Proměnné datového typu `double`

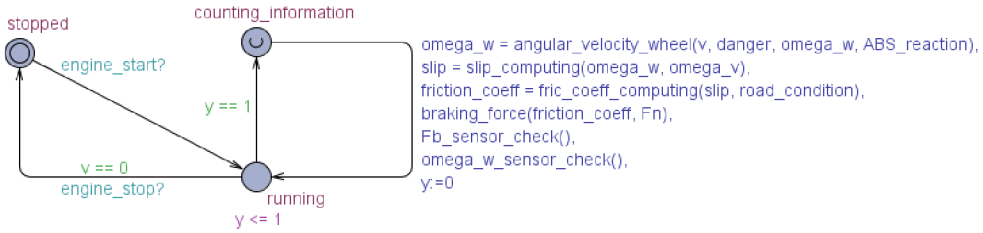
`omega_w_sensor` je senzor počtu otáček kola
`v_sensor` je senzor celkové rychlosti vozidla
`a_sensor` je senzor zrychlení
`Fb_sensor` je senzor brzdné síly
`sum_of_w_flick_risk` je akumulátor míry rizika pro senzor otáček kola
`sum_of_v_flick_risk` je akumulátor míry rizika pro senzor celkové rychlosti vozidla
`sum_of_a_flick_risk` slouží k akumulaci míry rizika pro senzor zrychlení
`sum_of_fb_flick_risk` slouží k akumulaci míry rizika pro senzor brzdné síly
`sum_of_risk` je akumulátor celkové míry rizika
`failure_chance` slouží k rozhodnutí, zda dojde k selhání některého ze senzorů, či nikoliv
`random_number` je pomocná proměnná pro generování náhodného čísla

Časové automaty

Časové automaty v modelu systému ABS byly popsány v sekci 3.3.1.
Automaty, které zůstaly bez modifikace jsou:

1. Model motoru - *Engine*
2. Model řídící jednotky - *ControlUnit*
3. Model řidiče - *Driver*
4. Model překážky - *ObstacleSpotted*
5. Model skluzu - *Slip*
6. Model ABS - *ABS*

Jediným automatem, který prošel mírnou modifikací je automat kola - *Wheel*. Automat prošel drobnou změnou, ve kterém došlo k přidání volání funkcí *Fb_sensor_check()* a *omega_w_sensor_check()*. Funkce byly původně umístěny v časovém automatu řídící jednotky rizik. Nástroj *UPPAAL* ale nesprávně přiřazoval hodnoty pro senzor brzdné síly a pro senzor otáček kola i přes to, že byly oba automaty synchronizovány pomocí implementovaných hodin *y*. Hodnoty z senzorů byly vždy o jedno časové okno zpožděné. Důsledkem bylo, že systém pro analýzu rizik tyto údaje nesprávně vyhodnocoval a taktéž nesprávně vyhodnocoval riziko. Z toho důvodu bylo nutné tyto dvě funkce volat v automatu *Wheel*, místo toho, aby byly volány v automatu *RiskECU*.



Obrázek 4.6: Modifikovaný model kola *Wheel*.

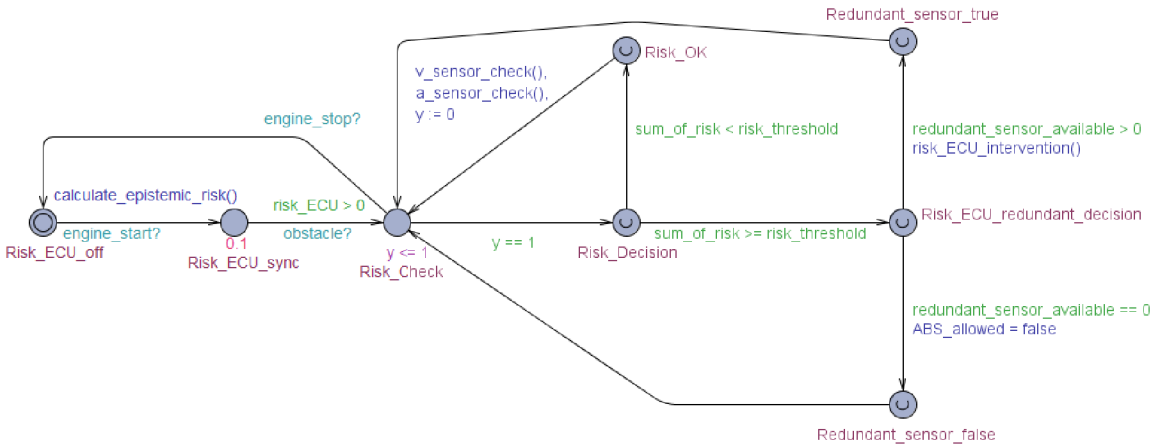
Model řídící jednotky analýzy rizik

Automat ŘJ analýzy rizik *RiskECU* začíná ve stavu *Risk_ECU_off*, při obdržení synchronizačního signálu *engine_start* je povolen přechod do stavu *Risk_ECU_sync*, kdy dojde k synchronizaci s řídící jednotkou motoru *Engine*. V případě, že je systém pro analýzu rizik aktivován, tak je povolen přechod do stavu *Risk_Check* při kterém dojde k vyhodnocení epistemických nejistot.

Dále je automat synchronizován s ostatními automaty pomocí časových hodin *y*. Při synchronizaci s ostatními automaty je povolen přechod do stavu *Risk_Decision* ve kterém je zapotřebí rozhodnutí systému, zda došlo k překročení maximální míry rizika, kterou upravuje proměnná `risk_threshold`. Pokud není maximální míra rizika překročena, tak je povolen přechod do stavu *Risk_OK* značící, že míra rizika je zatím únosná a následně dojde ke kontrole senzorů rychlosti a zrychlení pomocí funkcí *v_sensor_check()* a *a_sensor_check()*. Dále dojde k vynulování synchronizačních hodin.

V případě překročení prahu maximálního přípustného rizika je systém nucen provést rozhodnutí a je povolen přechod do stavu *Risk_ECU_redundant_decision*. Zde je zapotřebí se na základě vstupní konfigurace rozhodnout. Pokud nemá systém dostupná náhradní senzory, je nucen pro zachování bezpečnosti systém ABS deaktivovat. Systém ABS může v případě chybných dat ze senzorů provádět nežádoucí zásahy do řízení, což ohrožuje bezpečnost vozidla, a proto je bezpečnější systém deaktivovat. Systém pro analýzu rizik poté provede přechod do stavu *Redundant_sensor_false*, přičemž provede deaktivaci systému ABS pomocí modifikace proměnné *ABS_allowed* nastavením její hodnoty na 0. Poté se vrací do stavu *Risk_Check* a pokračuje v monitorování senzorů.

Systém analýzy rizik může mít k dispozici náhradní senzory (definováno konstantou `redundant_sensor_available`) poté je schopen vadný senzor nahradit senzorem redundantním. Tím je zabezpečena správná odezva systému ABS. Model řídící jednotka analýzy rizik provede přechod do stavu *Redundant_sensor_available*, přičemž provede zásah do senzoru a nahradí jej za senzor redundantní pomocí funkce *risk_ECU_intervention()*. Ve funkci *risk_ECU_intervention()* je zavolána další funkce *recover_all_sensors()*, která zabezpečuje nahrazení původního senzoru za senzor náhradní. Nastaví proměnnou `recovered` na hodnotu 1, čímž signalizuje zotavení senzoru, dále vynuluje proměnné `sensor_failure` a `flick_failure`. Provede přiřazení korektních hodnot jednotlivým senzorům a sumu celkového rizika `sum_of_risk` nastaví na hodnotu statického rizika, uloženého v proměnné `sum_of_epistemic_error`.



Obrázek 4.7: Model řídící jednotky analýzy rizik *RiskECU*.

Model generátoru poruch

Systém analýzy rizik obsahuje rovněž generátor poruch *MalfunctionGenerator*, jehož cílem je stochasticky generovat poruchy senzorů.
Generátor poruch je synchronizován s ostatními automaty pouze pomocí hodin y a signálu *engine_stop*. Začíná ve stavu *Start*, ve které stráví 0.1 desetinu časové jednotky modelu. Dalším přechodem je přechod do stavu *Will_sensor_fail*. Při vykonání přechodu je vypočtena pravděpodobnost na selhání některého ze senzorů funkcí *calculate_chance_to_failure()*. Ve funkci je nejprve vygenerováno náhodné číslo z intervalu [0,1].

Následně dojde k výpočtu šance na selhání dle vzorce:

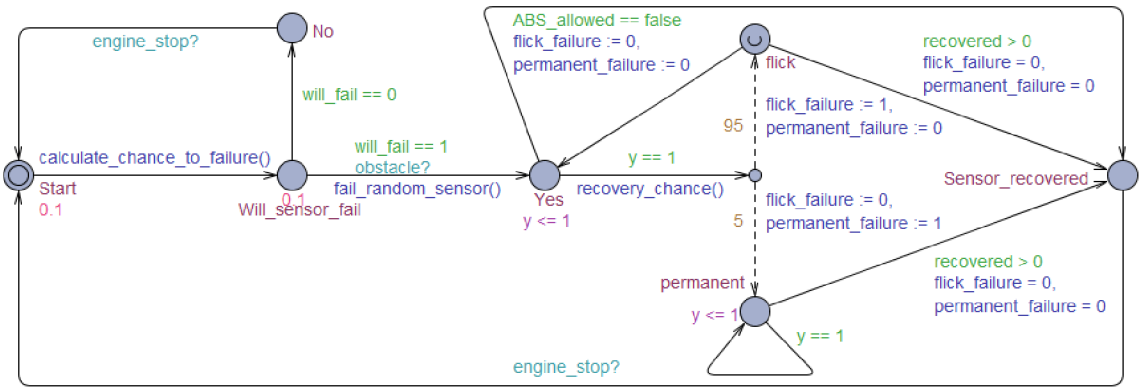
$$\texttt{failure\_chance} = 1.0 - e^{\left(\frac{\texttt{car\_hours}}{\texttt{sensor\_mttf} * -1.0}\right)}$$

Čímž dojde k výpočtu šance na selhání dle exponenciálního rozložení pravděpodobnosti [33]. Pokud je náhodně vygenerované číslo menší, než šance na selhání, tak je proměnná `will_fail` nastavena na hodnotu 1, čímž dojde k signalizaci, že některý ze senzorů selže. V případě, že žádný ze senzorů neselže, tak řídící jednotka analýzy rizik nedetekuje žádné nekorektní chování a simulace poté probíhá stejně jako v případě, kdy je analýza rizik úplně vypnuta (nastavením konstanty `risk_ECU` na 0 před začátkem simulace).

Dle hodnoty `will_fail` je automat nucen provést rozhodnutí na základě selhání senzoru. Pokud neselže, přesune se do stavu *No* a čeká na signál od řídící jednotky vozidla k zastavení motoru. V případě selhávajícího senzoru je povolen přechod do stavu *Yes* a zároveň dojde k vyhodnocení funkce *fail_random_sensor()*, která stochasticky vybere jeden ze senzorů, který bude selhávat a také nastaví proměnnou `sensor_failure` dle vybraného senzoru. Ve stavu *Yes* automat čeká na synchronizaci pomocí hodin *y*.

Po uplynutí jedné desetiny vteřiny je povolen přechod do větvícího stavu a zároveň je vyhodnocena pravděpodobnost na zotavení senzoru ve funkci *recovery_chance()*. Ve funkci *recovery_chance()* je stochasticky rozhodnuto, zda se senzor zotaví, či nikoliv. Je vygenerováno náhodné číslo v intervalu [0,1] a pokud je náhodně vygenerované číslo větší, než šance senzoru na zotavení (lze modifikovat změnou konstanty `sensor_chance_to_recover`), tak dojde k zotavení čidla a je zavolána funkce *recover_all_sensors()*.
Smyslem funkce *recovery_chance()* je, že se mohlo jednat pouze o krátkodobý výpadek senzoru, který mohl být způsoben nějakým vnějším vlivem.

Pokud se senzor nezotavil, je 95% pravděpodobnost, že se jedná o selhání senzoru kvůli zákmitu. Zákmit senzoru je reprezentován jako odchylka od očekávané hodnoty o určitou míru, ovlivněnou proměnnou `threshold`. S 5% pravděpodobností se jedná o poruchu permanentního charakteru, je proveden přechod do stavu *permanent* a je nastaven příznak permanentní poruchy pomocí proměnné `permanent_failure` = 1. Permanentní porucha by měla simulovat poruchu při níž přestal senzor zcela komunikovat. V reálné světě by se mohlo jedna o přerušení kontaktu mezi řídící jednotkou a senzorem, zkratem na komunikačním vodiči atp. V případě permanentní poruchy již automat nemá šanci na zotavení a po uplynutí jedné desetiny vteřiny provede přechod smyčkou do stejného stavu.
Pokud automat stochasticky zvolil přechod do stavu *flick*, tak se jedná o zákmit a je nastaven příznak `flick_failure` na 1. Ze stavu *flick* se poté automat vrátí do stavu *Yes* a cyklus se opakuje. Při opakovaném cyklu se může z poruchy zákmitové stát porucha permanentní. V reálném světě opět může dojít nejprve k zákmitu a poté k úplné ztrátě komunikace.
Ze stavů *flick* a *permanent* může automat vykonat přechod do stavu *Sensor_recovered*, ale to pouze v případě, že zasáhla řídící jednotka analýzy rizik pomocí nahrazení selhávajícího senzoru senzorem redundantním a nebo pokud bylo ve funkci *recovery_chance()* stochasticky rozhodnuto, že dojde k zotavení senzoru.



Obrázek 4.8: Model generátoru poruch *MalfunctionGenerator*.

4.4.2 Modifikovaný model systému ESP

Jako v případě modelu ABS, tak i v případě modelu ESP bylo důležitým předpokladem a úkolem při návrhu systému analýzy rizik zachování plné původní funkcionality modelu ESP s vypnutým systémem pro analýzu rizik. Cíle bylo dosaženo, ačkoliv bylo zapotřebí i při menším zásahu do modelu opakované testování modelů pomocí experimentů. Předpoklad se podařilo splnit a systém ESP s implementovanou a deaktivovanou analýzou rizik se chová stejně jako původní model.

Konstanty a proměnné modelu

Zde je obsažen výčet konstant a proměnných využitých v modelu s krátkým popisem jednotlivých proměnných.

Konstanty datového typu `int`

`risk_ECU` - slouží k aktivaci/deaktivaci systému analýzy rizik
`redundant_sensor_available` - definuje dostupnost/nedostupnost redundantních senzorů

Konstanty datového typu `double`

`ALARP_state_ESP_modifier` je modifikátor brzdné síly při dosažení stavu $ALARP$
`car_age` je stáří vozidla v letech
`average_age_per_year` označuje průměrnou rychlost stárnutí vozidla za rok v $[h]$
`car_mileage` je stav tachometru v km
`average_speed` je průměrná rychlost vozidla v $[kmh^{-1}]$
`car_hours` je rovnice pro výpočet doby stáří vozidla v hodinách, dle 4.1
`sensor_mttf` je `mean time to failure` senzorů ve vozidle, dle 4.1
`threshold` slouží k definici horní hranice zákmitové hodnoty daného senzoru
`flick_risk_value` je maximální ohodnocení míry rizika při detekci jednoho zákmitu senzoru
`risk_threshold` je hranice, při které ŘJ analýzy rizik aktivuje režim $ALARP$
`risk_alarp_zone_threshold` je hranice, při jejímž překročení dojde k zásahu ŘJ analýzy rizik do systému ESP.
`permanent_failure_risk` je ohodnocení míry rizika při detekci permanentní poruchy
`sensor_chance_to_recover` je šance na zotavení senzoru

Proměnné datového typu `int`

`ALARP_state` je ukazatel aktivace *ALARP* stavu
`recovered` detekuje zotavení senzoru
`will_fail` je příznak, zda dojde k selhání senzoru, či nikoliv
`sensor_failure` proměnná, která ukazuje na selhávající senzor. Hodnota 0 značí, že všechny senzory jsou funkční, 1 - senzor brzdné síly levého předního kola, 2 - senzor brzdné síly pravého předního kola, 3 - senzor brzdné síly levého zadního kola, 4 - senzor brzdné síly pravého zadního kola, 5 - senzor rychlosti vozidla, 6 - senzor zrychlení `flick_failure` značí, že se jedná o zákmitovou poruchu
`permanent_failure` značí, že se jedná o permanentní poruchu
`permanent_risk_added` je pomocná proměnná, která určuje, zda již bylo přičtena míra permanentního rizika

Proměnné datového typu `double`

`Fb_fl_sensor` - senzor brzdné síly levého předního kola
`Fb_fr_sensor` - senzor brzdné síly pravého předního kola
`Fb_rl_sensor` - senzor brzdné síly levého zadního kola
`Fb_rr_sensor` - senzor brzdné síly pravého zadního kola
`ta_sensor` - senzor zrychlení vozidla
`v_sensor` - senzor celkové rychlosti vozidla
`sum_of_fl_flick_risk` - akumulátor míry rizika senzoru brzdné síly levého předního kola
`sum_of_fr_flick_risk` - akumulátor míry rizika senzoru brzdné síly pravého předního kola
`sum_of_rl_flick_risk` - akumulátor míry rizika senzoru brzdné síly levého zadního kola
`sum_of_rr_flick_risk` - akumulátor míry rizika senzoru brzdné síly pravého zadního kola
`sum_of_v_flick_risk` slouží k akumulaci míry rizika pro senzor celkové rychlosti vozidla
`sum_of_ta_flick_risk` slouží k akumulaci míry rizika pro senzor zrychlení vozidla
`sum_of_epistemic_error` slouží k uložení míry statického rizika
`sum_of_risk` slouží k akumulaci celkové míry rizika
`recover` je proměnná k uložení šance na zotavení senzoru
`failure_chance` slouží k rozhodnutí, zda dojde k selhání některého ze senzorů, či nikoliv
`random_number` je pomocná proměnná pro generování náhodného čísla

Globální funkce modelu

Zde bude následovat výčet jednotlivých funkcí implementovaných v modelu spolu s krátkým komentářem úlohy dané funkce.
calculate_chance_to_failure() - vyhodnocení šance na selhání náhodného senzoru (stochastické)
ALARP() - pomocná funkce pro nastavení přechodu do *ALARP* režimu
recover_all_sensors() - provede zotavení všech senzorů v modelu ESP
risk_ECU_intervention() - ŘJ analýzy rizik nahradí všechny původní senzory náhradními senzory
recovery_chance() - funkce vyhodnocující šanci senzoru na zotavení
ESP_off() - funkce sloužící k deaktivaci systému ESP
Fb_fl_sensor_check() - funkce pro kontrolu stavu senzoru brzdné síly levého předního kola
Fb_fr_sensor_check() - funkce pro kontrolu stavu senzoru brzdné síly pravého předního kola
Fb_rl_sensor_check() - slouží ke kontrole stavu senzoru brzdné síly levého zadního kola
Fb_rr_sensor_check() - slouží ke kontrole stavu senzoru brzdné síly pravého zadního kola
v_sensor_check() - provede kontrolu stavu senzoru rychlosti vozidla
a_sensor_check() - provede kontrolu stavu senzoru celkového zrychlení vozidla
calculate_epistemic_risk() - funkce pro ohodnocení statického rizika modelu dle 4.1

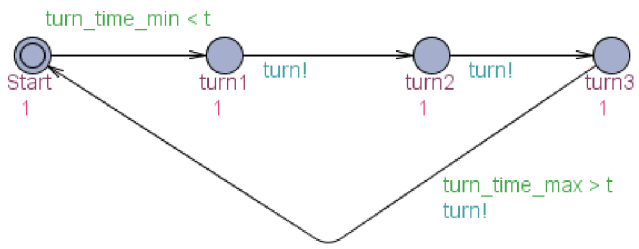
Časové automaty

Automaty, které obsahuje model ESP byly popsány v sekci 3.3.2.
Níže následuje výčet automatů, které zůstaly bez modifikace:

1. Model motoru - *Engine*
2. Model řídící jednotky - *ECU*
3. Model ŘJ ESP - *ESP_ECU*

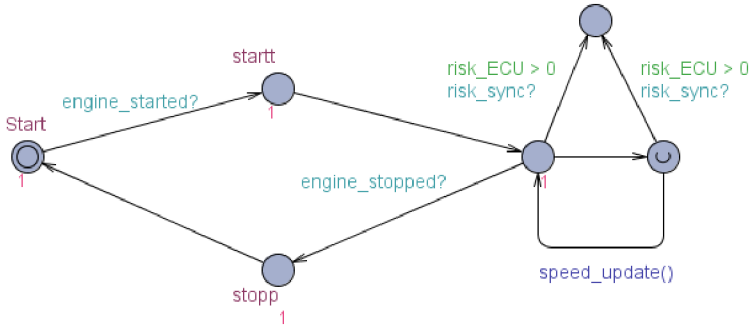
Automat řidiče *Driver* zaznamenal drobnou změnu. Došlo k přidání synchronizačního kanálu *risk_sync*, který signalizuje ostatním automatům, že již obdržel synchronizační signál *turn* a je zapotřebí spustit systém analýzy rizik. Synchronizační signál *risk_sync* je implementován mezi přechody *Pedals_off* a *Turn_wheel*, viz původní obrázek 3.15.

Automat zatáčky *Turn* prošel taktéž drobnou modifikací. Původní model systému ESP v některých případech nezaznamenal událost příchozí zatáčky. Z toho důvodu došlo k přidání více přechodů v automatu *Turn* se synchronizačním signálem *turn*. Model nyní lépe zachycuje příchozí zatáčku.



Obrázek 4.9: Modifikovaný model zatáčky *Turn*.

Mírnou modifikací prošel taktéž automat kola - *Wheel*. Došlo k přidání synchronizačního kanálu *risk_sync* v případě, že je zapnuta analýza rizik. Pokud je analýza rizik zapnuta, automat *Wheel* se již nestará o volání funkce *speed_update()* a o volání funkce *speed_update()* se stará automat analýzy rizik *Risk_ECU*, který bude popsán v následující sekci. Tato modifikace byla implementována z důvodu zachování původní funkčnosti modelu. Za předpokladu vypnutého systému analýzy rizik automat funguje stejně jako v původní implementaci čili volá funkci *speed_update()* v nekonečném cyklu, čímž dochází k aktualizaci rychlosti vozidla.



Obrázek 4.10: Modifikovaný model kola *Wheel*.

Model řídící jednotky analýzy rizik

Automat řídící jednotky analýzy rizik začne svoji úlohu ve stavu *Risk_ECU_off*. Přechod do stavu *Risk_Sync* je povolen pouze v případě, že je povolena analýza rizik pomocí proměnné `risk_ECU`, současně dojde k vyhodnocení statických rizik funkcí *calculate_epistemic_risk()*, které reprezentují epistemické nejistoty.

Pro přechod ze stavu *Risk_sync* do stavu *Risk_check* automat čeká na přijetí synchronizačního signálu *risk_sync* od automatu *Driver*. Dále automat čeká přibližně 1 desetinu vteřiny a poté mu je umožněn přechod do stavu *Risk_Decision*. Zde se systém pro analýzu rizik musí rozhodnout, zda je celková suma rizika reprezentovaná proměnnou `sum_of_risk` menší, než povolená míra rizika. Pokud ano, je povolen přechod do stavu *Update_values*, který je označen jako urgentní stav a je nutné jej neprodleně vyhodnotit. Ze stavu *Update_values* existuje jediný možný přechod, a to do stavu *Risk_check*. Při přechodu mezi těmito stavy dojde k aktualizaci rychlosti vozidla funkcí *speed_update()* a dále dojde k aktualizaci dat ze senzorů pomocí funkcí *Fb_fl_sensor_check()*, *v_sensor_check()* atd.

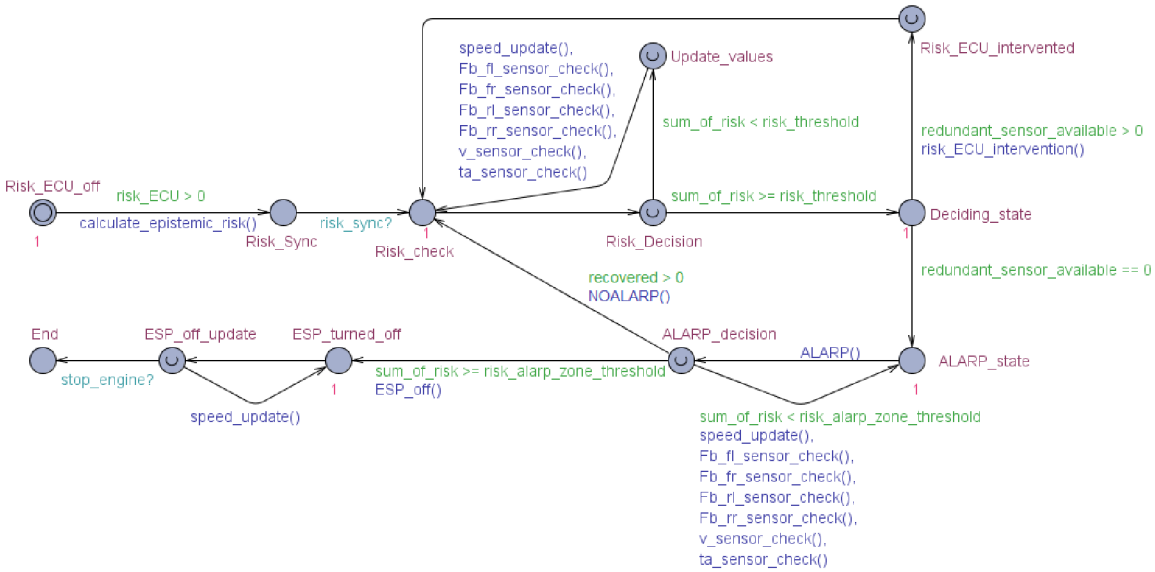
V případě, že míra rizika je větší povolená míra rizika je povolen přechod do stavu *Deciding_state*. Ve stavu *Deciding_state* je zapotřebí, aby se systém rozhodl dle dostupné vstupní konfigurace. Pokud má systém k dispozici náhradní senzory (definované proměnnou `redundant_sensor_available`) je povolen přechod do stavu *Risk_ECU_intervented*. Při přechodu dojde k zavolání funkce *risk_ECU_intervention()*, která provede nahrazení vadného senzoru senzorem náhradním. Funkce zavolá další funkci *recover_all_sensors*, která aktualizuje hodnoty všech senzorů, zredukuje míru rizika a nastaví ji na původní statickou hodnotu a označí zotavení senzorů pomocí proměnné `recovered`. Dále vynuluje detekci zákmitové/permanentní poruchy.

Pokud systém pro analýzu rizik nemá k dispozici náhradní senzory je zapotřebí jeho reakce. Zde je jeho chování rozdílné oproti implementaci v systému ABS 4.7. Povoleným přechodem je přechod do stavu *ALARP_state* a dále přechod do stavu *ALARP_decision*. Řídící jednotka analýzy rizik provede aktivaci tzv. *ALARP* stavu. Smyslem *ALARP* stavu je, že systém omezí funkcionalitu systému ESP. Neprovede úplnou deaktivaci systému ESP, ale omezí brzdnou sílu pomocí modifikátoru `ALARP_state_ESP_modifier`, čímž limituje jeho činnost pomocí volání funkce *ALARP()*.

Automat ze stavu má k dispozici tři přechody, ale záleží na konkrétní situaci. Senzor má stále šanci na zotavení, která probíhá v automatu *MalfunctionGenerator*, který bude popsán v další sekci. Pokud se senzor zotaví, tak je povolen přechod do stavu *Risk_check*.

Za situace, kdy je míra rizika menší, než hranice *ALARP* zóny je povolen přechod do stavu *ALARP_state*. Při přechodu dochází k volání stejných funkcí, jako při přechodu ze stavu *Update_values* do stavu *Risk_check*. Ze stavu *ALARP_state* je povolen přechod opět pouze do stavu *ALARP_decision*.

Pokud míra rizika již překonala i hranici zóny *ALARP* a senzor se nezotavil, tak je povolen přechod pouze do stavu *ESP_turned_off*. Při přechodu dojde k zavolání funkce *ESP_off()*, která slouží k deaktivaci celého systému ESP. Dále je deaktivován i režim *ALARP*, ESP je označeno jako neaktivní a je vynulována brzdná síla ESP. Dalším přechodem po uplynutí jedné desetiny vteřiny je přechod do stavu *ESP_off_update*. Zde jsou povoleny jen dva přechody. Při obdržení synchronizačního signálu *stop_engine* se automat přesune do stavu *End* ve kterém končí svoji funkcionalitu. Pokud signál neobdrží, je povolen přechod zpět do stavu *ESP_turned_off* a při přechodu dojde k aktualizaci rychlosti vozidla pomocí funkce *speed_update()*.



Obrázek 4.11: Model řídící jednotky analýzy rizik *RiskECU*.

Model generátoru poruch

Časový automat *MalfunctionGenerator* má stochasticky simulovat generování poruch senzorů. Začíná ve stavu *Start*. Pokud je povolena analýza rizik, tak je povolen přechod do stavu *Malfunction_decision*. Při přechodu dojde k volání funkce *calculate_chance_to_failure*, čímž dojde k stochastickému rozhodnutí, zda některý ze senzorů selže, nebo neselže. Implementace je stejná jako v případě generátoru poruch v systému ABS 4.8.

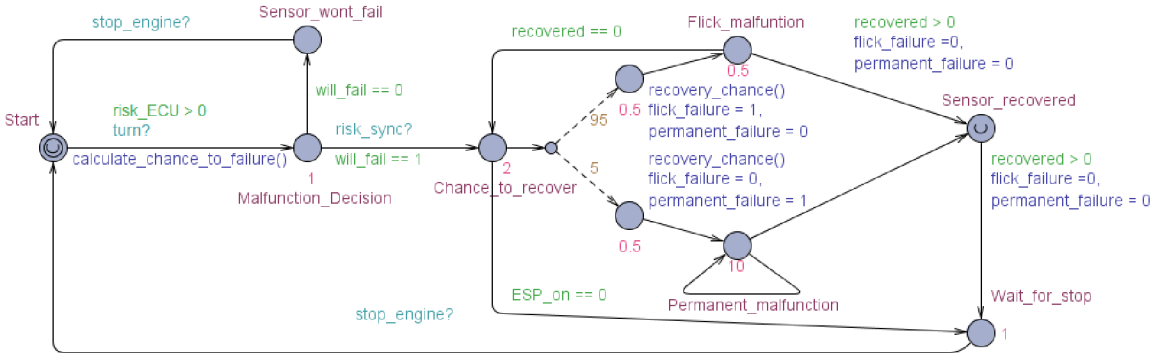
Dle hodnoty proměnné `will_fail` se automat rozhodne, který přechod zvolí. Pokud funkce *calculate_chance_to_failure* stochasticky rozhodla, že senzor neselže, tak automat provede přechod do stavu *Sensor_wont_fail*. Ve kterém dále čeká na synchronizační signál *stop_engine* od ŘJ motoru.

Za předpokladu, že je proměnná `will_fail` nastavena na hodnotu 1 dochází k selhání senzoru. Automat čeká na příjem synchronizačního signálu od automatu *Driver*, který signál zašle v případě příchozí zatáčky. Až automat zašle synchronizační signál, tak je povolen přechod do stavu *Chance_to_recover* ve kterém automat stráví dvě desetiny vteřiny. Pokud je systém ESP deaktivován řídící jednotkou analýzy rizik, nebo ani nebyl aktivní, tak automat přejde do stavu *Wait_for_stop*.

S 5% procentní pravděpodobností je porucha permanentního charakteru automat vykoná přechod do stavu *Permanent_malfunction*. Čidlo má poslední šanci na zotavení pomocí funkce *recovery_chance()*. Pokud se čidlo nezotaví, je nastaven příznak permanentní poruchy pomocí proměnné `permanent_failure` na hodnotu 1. Dále automat cyklí ve stavu *Permanent_malfunction*.

S 95% pravděpodobností se jedná o zákmit senzoru. Je uskutečněn přechod do stavu *Flick_malfunction* a při uskutečnění přechodu má senzor šanci na zotavení pomocí funkce *recovery_chance()*. Dále je nastaven příznak `flick_failure` na hodnotu 1, čímž je signalizován zákmit čidla. Pokud se senzor nezotavil, nebo řídící jednotka neprovedla zásah do systému ESP, tak jediný možný přechod je zpět do stavu *Chance_to_recover*. Automat se ocitá na začátku další smyčky, kdy se opět může stochasticky rozhodnout, kterou větev zvolí.

Ze stavů *Flick_malfunction* a *Permanent_malfunction* je možné uskutečnit přechod do stavu *Sensor_recovered* v případě, že se senzor zotavil, nebo že řídící jednotka nahradila vadný senzor senzorem redundantním. Stav *Sensor_recovered* je označen jako urgentní. Dále je možné vykonat přechod do stavu *Wait_for_stop*, ve kterém automat zůstane až do obdržení signálu *stop_engine*. Při vykonání přechodu jsou vynulovány příznaky selhání.



Obrázek 4.12: Model generátoru poruch *MalfunctionGenerator*.

Kapitola 5

Zhodnocení řešení

V této kapitole budou zkoumány klíčové vlastnosti implementované modelu analýzy rizik v modelu systému ABS [25] a v modelu systému ESP [41]. Cílem bude ukázat, jak systém analýzy rizik reaguje na různé scénáře poruch, jakým způsobem zasahuje do chování modelů a jakých rozdílů systém dosáhne. Experimenty se budou provádět i vícenásobně.

5.1 Model ABS

Testy a experimenty v této části budou dedikovány implementovanému systému analýzy rizik v modelu ABS. Nejdříve bude ověřen předpoklad, že se podařilo implementovat analýzu rizik do modelu ABS bez ztráty funkčnosti modelu a taktéž, že se model chová stále korektně a reaguje správně. Ve druhém testu bude zkoumáno chování modelu při brzdění z rychlosti $100kmh^{-1}$ na suché vozovce. Ve třetím testu bude model podroben simulaci brzdění z rychlosti $100kmh^{-1}$ na mokré vozovce. Čtvrtý test bude zaměřen na rozdílnou počáteční konfiguraci systému analýzy rizik.

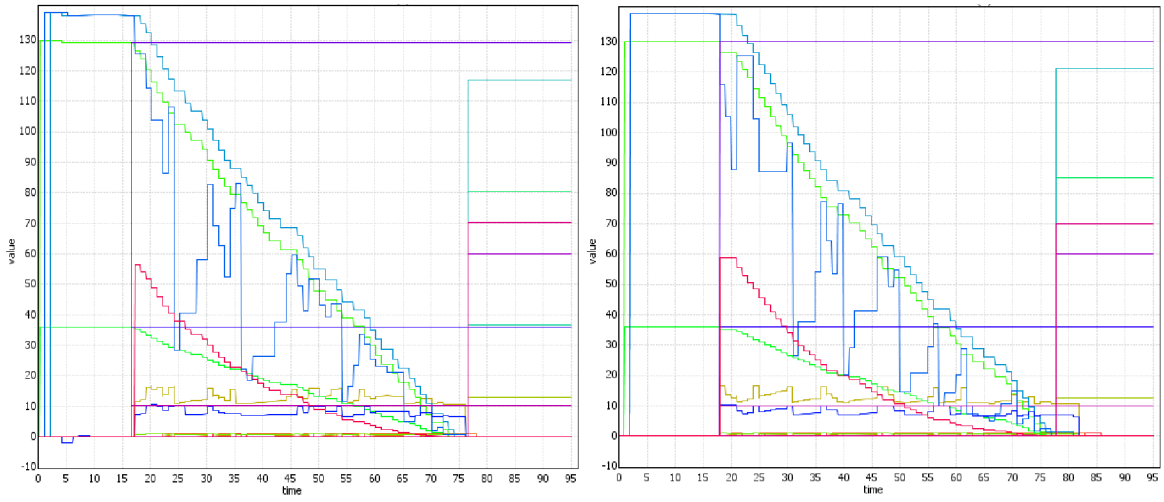
5.1.1 1. test - ověření zachování funkcionality

Prvním krokem bude porovnání původního modelu ABS bez systému analýzy rizik a výsledného modelu ABS s implementovanou analýzou rizik.
Simulace v obou modelech bude spuštěna pomocí příkazu:

```
simulate 1 [<= 95] {ABS_reaction, instability, slip, Fb/1000,
Fb_avarage/1000, friction_coeff, 3.6*v, v, braking_distance,
reaction_distance, full_braking_distance, omega_v, omega_w, a,
former_velocity, 3.6*former_velocity, braking_time, reaction_time,
full_braking_time, 0v/10.0}
```

Simulace sleduje průběh původních implementovaných proměnných v modelu. Je možné sledovat, jak se proměnné vyvíjejí v čase, jak na sobě závisí a jak se ovlivňují. Konfigurací jednotlivých proměnných a konstant lze měnit chování vozidla v různých situacích. Konstanty *OBSTACLE_TIME_MIN* a *OBSTACLE_TIME_MAX* byly nastaveny na hodnoty 5 a 10. Počáteční rychlost vozidla pro účel testu byla nastavena na hodnotu $130kmh^{-1}$ a povětrnostní podmínky a stav komunikace byl nastaven na režim `DRY`.

Z grafu byla odstraněna legenda pro lepší vizualizaci. Model bohužel není schopný přesné replikace jedné konkrétní simulace, jelikož některé jeho funkcionality jsou implementovány jako stochastický proces. Stochastická závislost je zřejmá například na proměnné `slip`, která je reprezentovaná světle modrou barvou. Rozdíl mezi zastavením ze stejné počáteční rychlosti byl řádově 7 desetin vteřiny, což je běžná odchylka vyskytující se u modelu ABS.

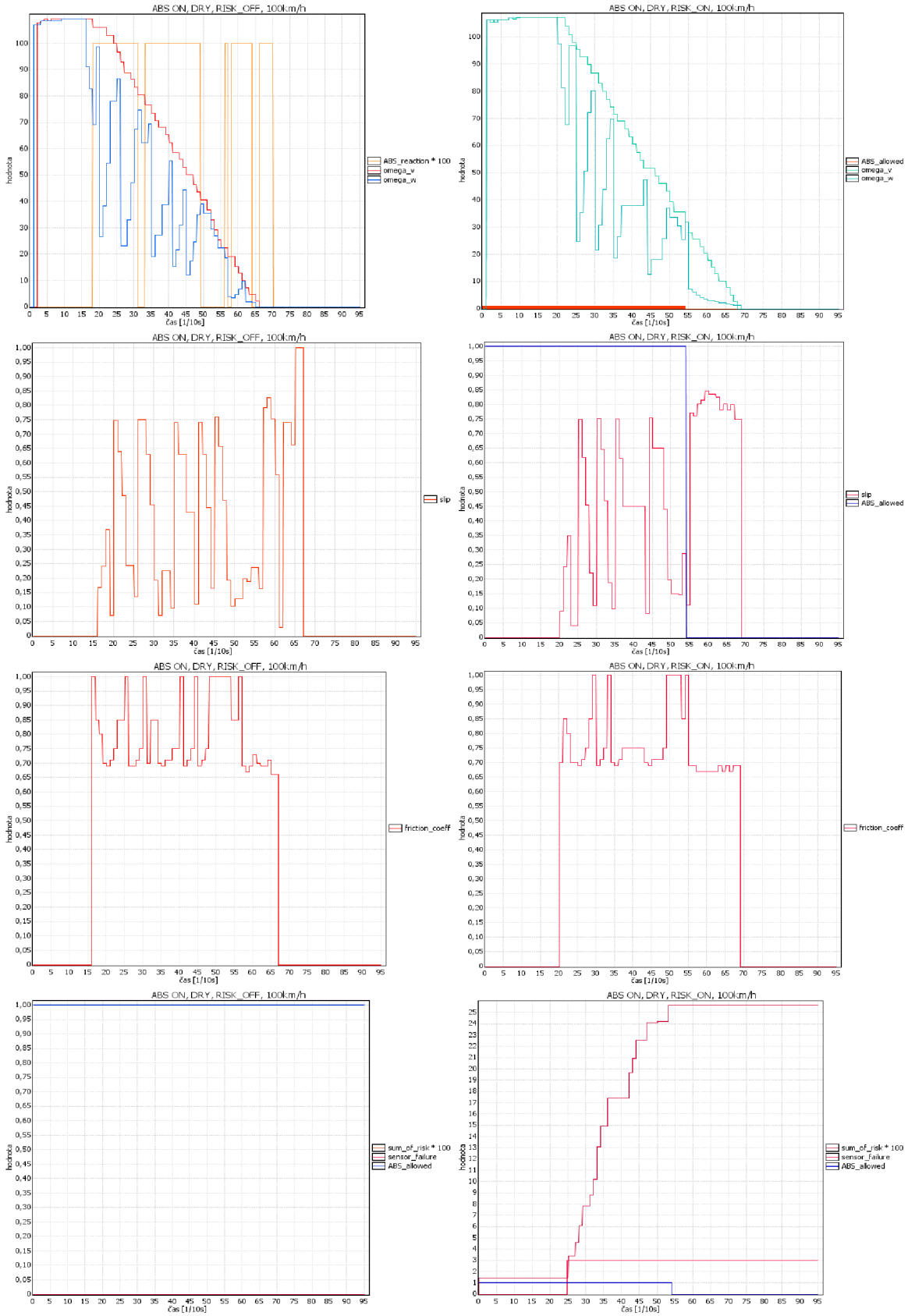


Obrázek 5.1: Vlevo simulace z původního modelu, vpravo simulace z upraveného modelu.

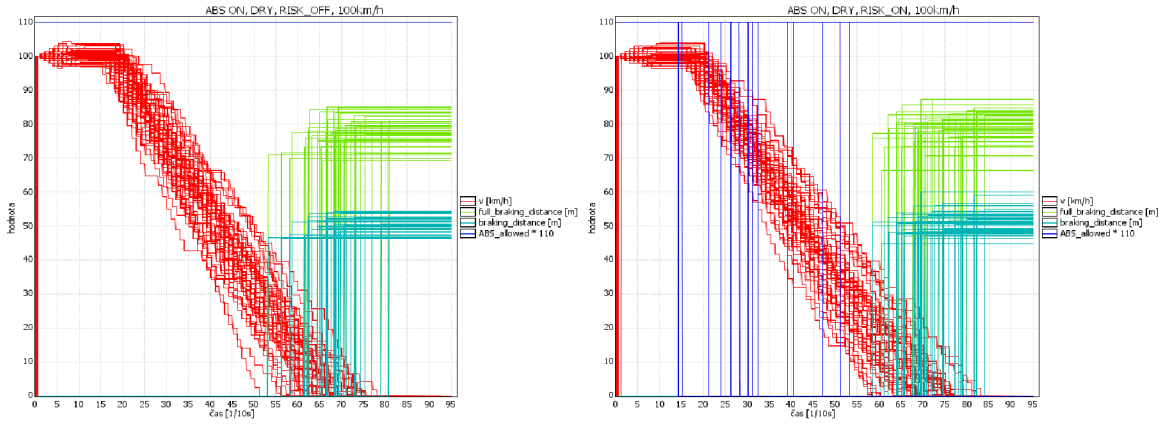
Z grafů lze tedy usoudit, že nedošlo ke změně funkcionality původního modelu a jeho funkčnost byla zachována. Jelikož se předpoklad a cíl podařilo splnit, tak všechny následující testy budou spouštěny pouze v modelu s implementovanou analýzou rizik.

5.1.2 2. test - brzdná dráha, $100 kmh^{-1}$, suchá vozovka

První test bude zaměřen na porovnání délky brzdné dráhy z počáteční rychlosti 100 km/h. Délka simulace byla nastavena na $9.5s$. Na ose X je zobrazen čas simulace a na ose Y jsou hodnoty proměnných. Na levé straně jsou zobrazeny grafy s použitím systému ABS a na pravé straně jsou grafy s zapnutým systémem ABS a taktéž se zapnutým systémem analýzy rizik. Systém analýzy rizik byl spuštěn s konstantami `risk_threshold` nastavenou na 0.25 a `flick_risk_value` na 0.03. První dvojice grafů zobrazuje průběh úhlové rychlosti vozidla a kola. Na levém obrázku je možné pozorovat, že při velkém rozdílu mezi hodnotami úhlové rychlosti vozidla a úhlové rychlosti dochází k zásahu systému ABS, reprezentovaným oranžovou čárou. Na pravém obrázku je systém ABS aktivní do hodnoty času 54 a poté systém pro analýzu rizik zasáhl do funkcionality a deaktivoval systém ABS. Vliv rostoucí míry rizika a překročení maximální míry rizika donutil systém analýzy rizik k této činnosti. Lze si povšimnout, že po deaktivaci systému ABS docházelo k větší blokaci kola, a z toho vyplývající ztráta kontroly nad vozidlem. Na druhé sadě grafů je vykreslena hodnota proměnné `slip` reprezentující skluz vozidla. Na levém grafu se hodnota skluzu drží v rozumných hodnotách, ve který je kolo na hranici smyku. V případě pravého grafu se hodnota skluzu drží opět na podobných hodnotách do deaktivace systému ABS vlivem rostoucího rizika a od té doby se hodnota skluzu pohybuje v intervalu [0.75,0.85] do úplného zastavení vozidla. Další sada grafů zobrazuje hodnotu třetího koeficientu `friction_coeff`. Opět je zřejmý rozdíl v hodnotách třecího koeficientu, který se střídavě mění z nižších hodnoty na hodnoty vyšší, které jsou výhodnější z hlediska brzdění vozidla. Ve čtvrté sadě grafů je vidět (ne)rostoucí míra rizika vyplývající z (ne)činnosti systému pro analýzu rizik.



Obrázek 5.2: Vlevo průběh simulace bez analýzy rizik. Vpravo s analýzou rizik

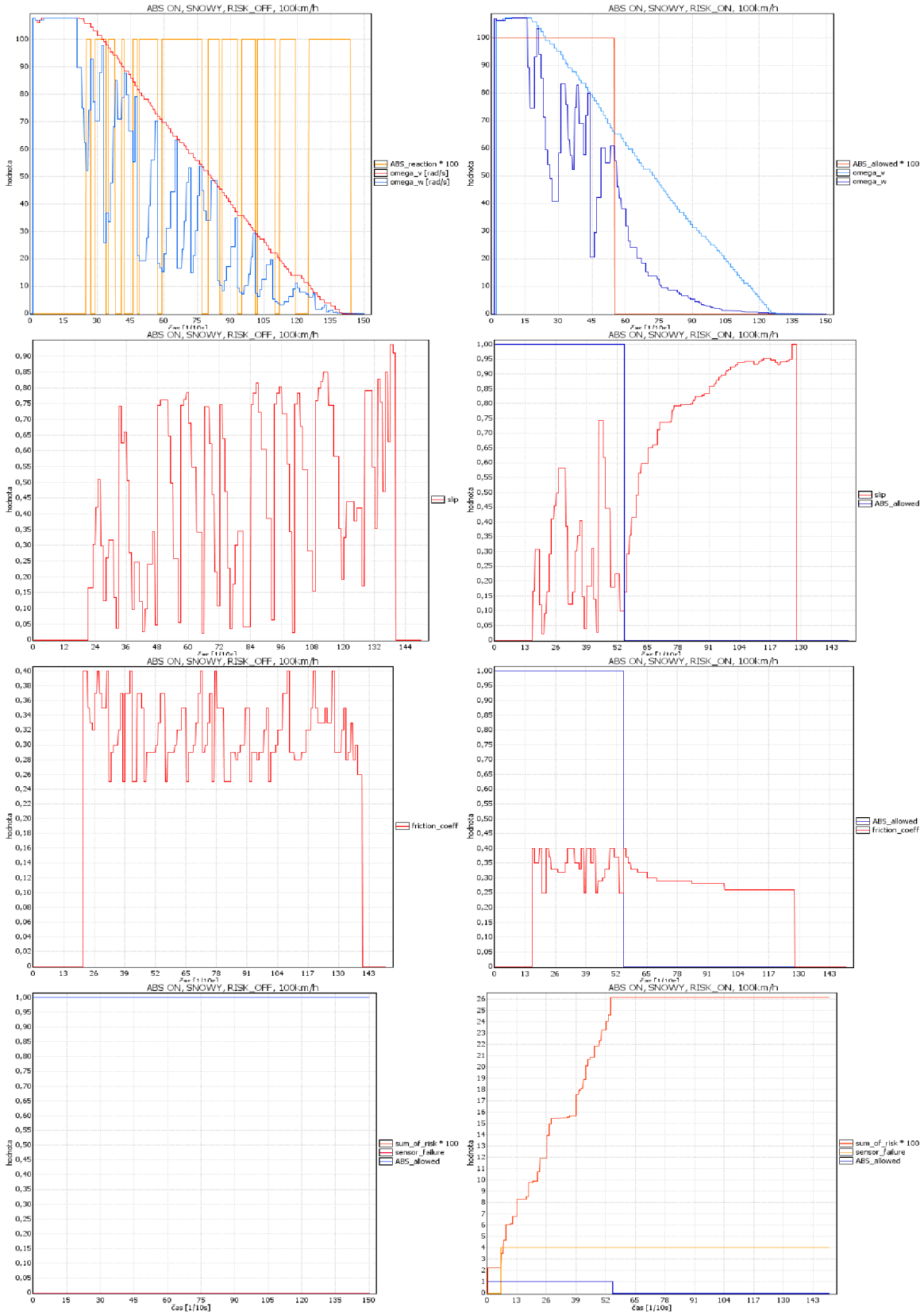


Obrázek 5.3: Test variability, 50 běhů simulací.

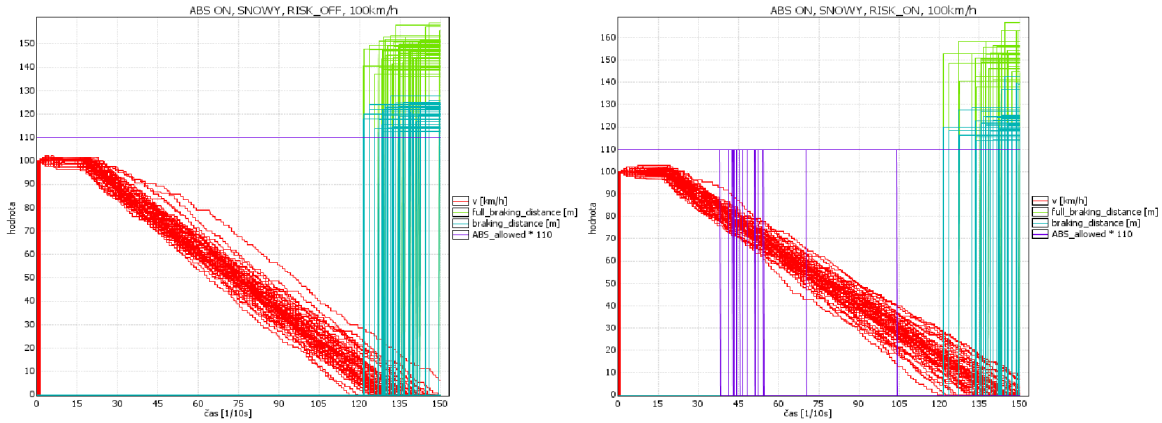
Na výše uvedených grafech je možné sledovat míru variability při běhu padesáti simulací. Na levém grafu je opět analýza rizik vypnutá a z toho důvodu v žádném z testů nedošlo k jejímu zásahu do systému ABS, jelikož z důvodu vypnuté analýzy rizik je vypnutý i generátor poruch. Na pravém grafu je možné vidět taktéž padesát simulací běhu. Konstanta `sensor_mttf` byla nastavena na hodnotu 1010 a z padesáti simulací nastala porucha ve 14 případech bez zotavení senzoru. Celkový počet poruch bude pravděpodobně vyšší. Porucha nastala tedy přibližně v každé třetí simulaci. Poruchy jsou symbolizovány na grafu nastavením hodnoty `ABS_allowed` na 0. Pro lepší čitelnost byla hodnota `ABS_allowed` vynásobena konstantou 110.

5.1.3 3. test - brzdná dráha, $100kmh^{-1}$, zasněžená vozovka

Ve třetím z testů bude možné nahlédnout na simulaci při sněžných podmínkách. Čas simulace bylo nutné prodloužit oproti předchozímu testu z $9.5s$ na $15.0s$. Grafy mají stejnou strukturu, jako v předchozím testu, aby bylo možné porovnat rozdílné podmínky testu. V levé části jsou opět umístěny grafy se zapnutým systémem ABS bez poruch a v pravé části jsou umístěny grafy s aktivním systémem ABS se zapnutým systémem analýzy rizik. Systém analýzy rizik deaktivoval systém ABS v simulačním čase 54.
Na první sadě grafů je opět zřejmé, že levý graf ukazuje činnost systému ABS, který neustále redukuje brzdný tlak vedoucí k postupné blokaci kola. V pravém grafu je vyobrazen zásah řídící jednotky analýzy rizik do systému ABS jeho deaktivací a tím i neustále se více blokujícím kolem.
Další sada grafů opět vykresluje rozdíl mezi hodnotami skluzu `slip`, kdy je zřejmé, že s deaktivovaným systémem ABS dochází k postupnému neredukovanému skluzu kola. Neredukovaný skluz kola má za následek snížení ovladatelnosti, či úplnou ztrátu kontroly a taktéž prodlužuje délku brzdné dráhy.
Třetí sada grafů zobrazuje rozdíl v třecím koeficientu, který ovlivňuje efektivitu brzdění. Z grafů lze opět snadno vyčíst, že při deaktivaci ABS nedochází k redukci brzdného tlaku a tím dochází ke stabilizaci třecího koeficientu, který nedosahuje optimálních hodnot.
Na poslední sadě grafů je znázorněn rozdíl mezi situací bez poruchy a s poruchou. V pravém grafu je prezentována celková suma rizika, která při překročení nastavené míry rizika donutí systém analýzy rizik k reakci. Dále je vykreslen selhávající senzor č. 4, kterým je senzor zrychlení.



Obrázek 5.4: Vlevo průběh simulace bez analýzy rizik. Vpravo s analýzou rizik.



Obrázek 5.5: Test variability, 50 běhů simulací.

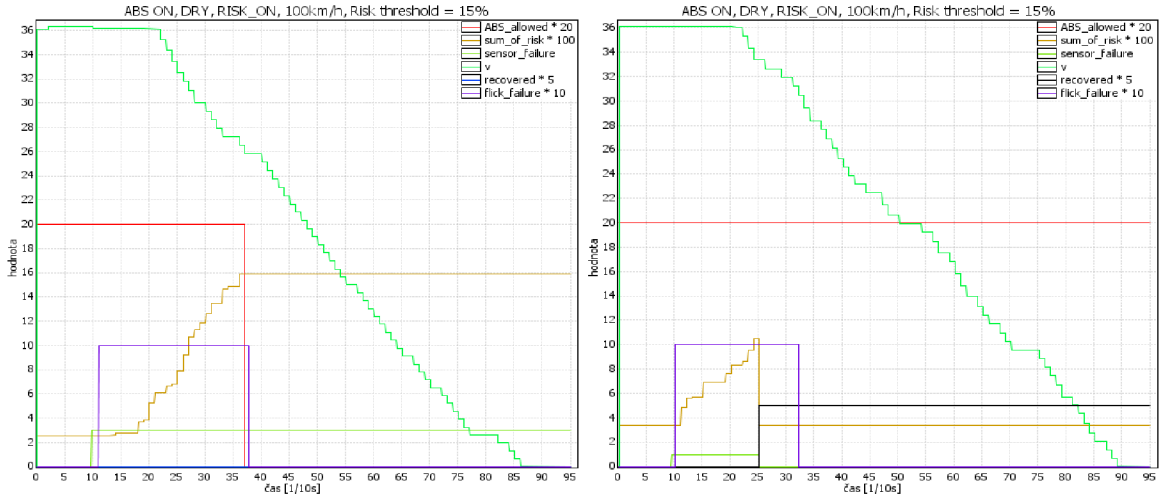
Na páté sadě grafů je zobrazena míra variability z padesáti simulací. Na levém grafu je systém pro analýzu rizik včetně generování poruch deaktivován. Na pravém grafu je zobrazen průběh padesáti simulací s celkovým počtem 17 poruch bez zotavení senzoru. Celkový počet poruch bude pravděpodobně vyšší. Konstanta `sensor_mttf` byla nastavena na hodnotu 1010. Porucha bez zotavení nastala ve více než třetině simulací. Poruchy opět symbolizuje změna stavu proměnné `ABS_allowed`.

5.1.4 4. sada testů - variabilní vlastnosti modelu

Test zásahu řídící jednotky analýzy rizik

Vlevo je zobrazen graf, ve kterém řídící jednotka analýzy rizik musí zasáhnout vlivem selhávajícího senzoru č. 3, kterým je senzor celkové rychlosti vozidla. Porucha senzoru se začne projevovat od simulačního času 10. Systémem analýzy rizik je detekována chyba značící zákmit (`flick_failure`). Senzor selhává a řídící jednotka míru rizika monitoruje. Maximální povolená míra rizika je nastavena na hodnotu 15%. Po překonání této hranice v simulačním čase 37 je z bezpečnostních důvodů systém ABS vypnut, jehož aktivita je zobrazena pomocí červené čáry.

Na pravém grafu je vyobrazena podobná situace jako v levém grafu. Hlavním rozdílem mezi těmito dvěma grafy je skutečnost, že systém ABS není řídící jednotkou analýzy rizik deaktivován po celou dobu běhu simulace. Porucha se vyskytuje v čase 1.1 vteřiny a jedná se o zákmitovou poruchu. Riziko postupně narůstá, až do času 2.5 vteřiny, kdy dojde k zotavení senzoru. Řídící jednotka tudíž nemusí zasáhnout do systému ABS a systém pokračuje v práci až do konce simulace.



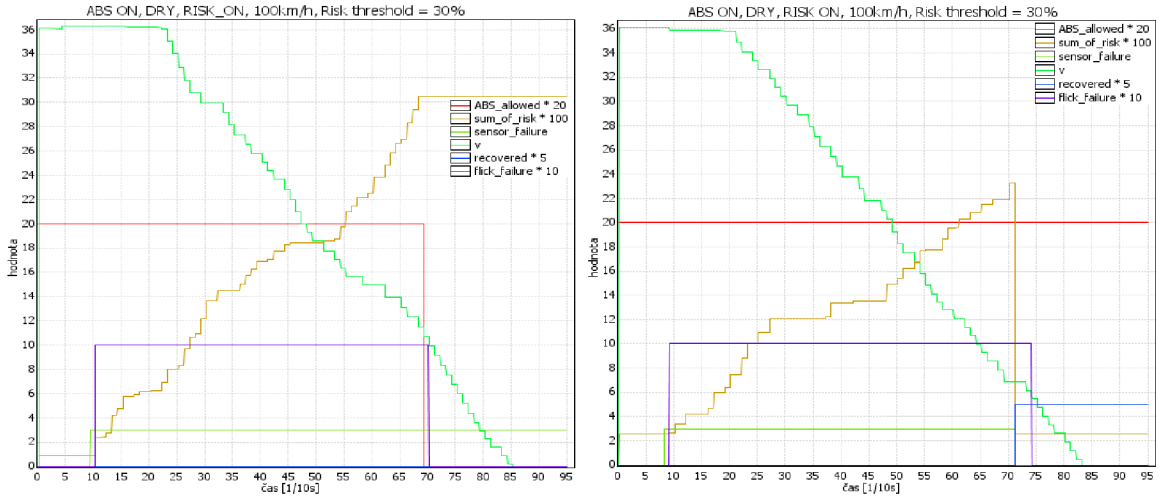
Obrázek 5.6: Grafy simulací zobrazující rozdílné chování při zotavení senzoru.

Test zásahu ŘJ analýzy rizik se zvýšenou hranicí maximálního rizika

V níže prezentovaných grafech bude možné nahlédnout na podobnou situaci, jako v předchozím testu. Hlavní rozdíl mezi těmito dvěma testy je zvýšená maximální míra rizika. Hranice rizika byla zvýšena z 15% na 30%.

Na levém grafu je signalizována porucha přibližně v čase 1.1 vteřiny. Míra rizika neustále narůstá, až do času 6.8 vteřiny, ve kterém překročí maximální povolenou hranici rizika 30%. Systém analýzy rizik proto systém ABS deaktivuje.

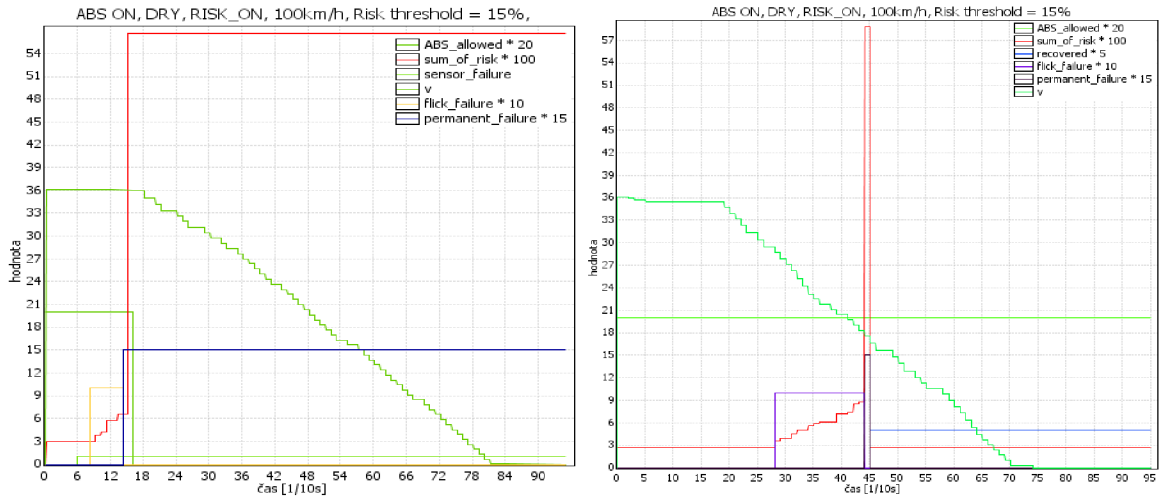
Na pravém grafu je vyobrazena podobná situace s příchozí poruchou senzoru. Rozdílem je, že senzor se v čase 7.1 vteřiny zotaví, což je signalizováno proměnnou `recovered`. Systém analýzy rizik proto do chování systému ABS nezasáhne a systém ABS je schopný pracovat až do konce simulace.



Obrázek 5.7: Grafy simulací zobrazující rozdílné chování při zotavení se zvýšenou hranicí maximálního rizika.

Test zásahu ŘJ analýzy rizik s redundantními senzory

Na níže vyobrazených grafech je možné nahlédnout na rozdílné chování jednotky analýzy rizik při dostupnosti redundantních senzorů. Na obou grafech dochází k permanentní poruše. Na levém grafu dochází k poruše v modelovém čase 8. Nejprve se jedná o zákmitovou chybu a systém analýzy rizik tuto chybu ohodnocuje a zvyšuje míru rizika. V čase 15 dochází k permanentní poruše a vlivem překročení maximální míry rizika je systém analýzy rizik nucen systém ABS deaktivovat.
Na pravém grafu dochází k poruše v čase 2.8 vteřiny. Jako v případě levého grafu dochází nejprve k zákmitu, až do času 4.4 vteřiny. Poté je porucha již permanentního charakteru a dochází ke ztrátě komunikace se senzorem. Jelikož má systém pro analýzu rizik dostupný náhradní senzor, tak provede nahrazení vazného senzoru senzorem náhradním a porucha čidla je odstraněna.



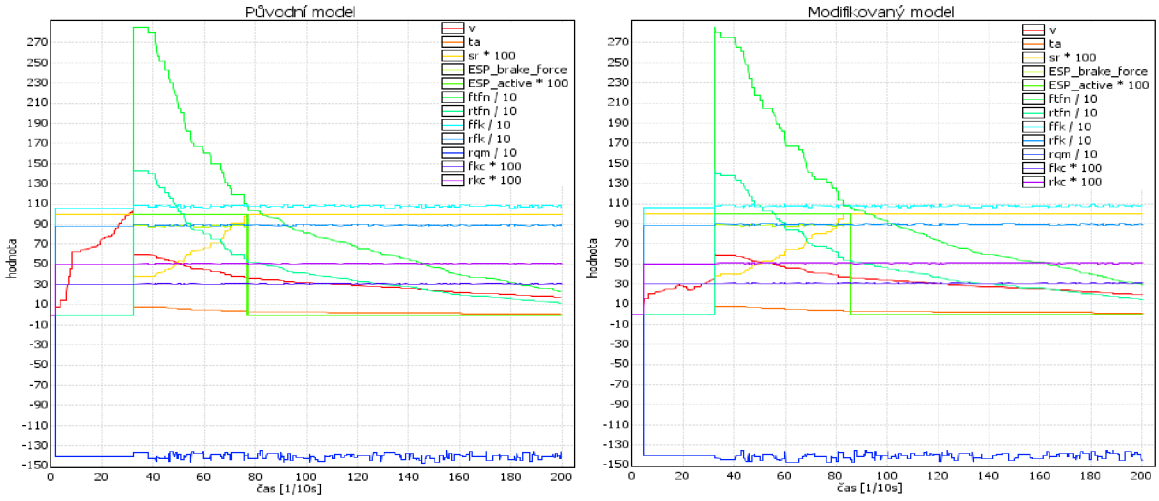
Obrázek 5.8: Grafy simulací zobrazující rozdílné chování při zotavení.

5.2 Model ESP

V následující sekci bude prezentován systém ESP s integrovanou analýzou rizik. Opět bude nejdříve ověřeno, zda nedošlo ke ztrátě funkcionality porovnáním původního modelu a modelu s implementovanou analýzou rizik.

5.2.1 1. test - ověření zachování funkcionality

Úvodním test bude spočívat v porovnání původního modelu s modelem, ve kterém je implementována analýza rizik.
Simulace bude spuštěna pomocí dotazu:
`simulate [<=200; 1] {v,ta,sr*100,ESP_brake_force,ESP_active*100,ftfn/10, rtfn/10,ffk/10,rfk/10,rqm/10,fkc*100,rkc*100}`



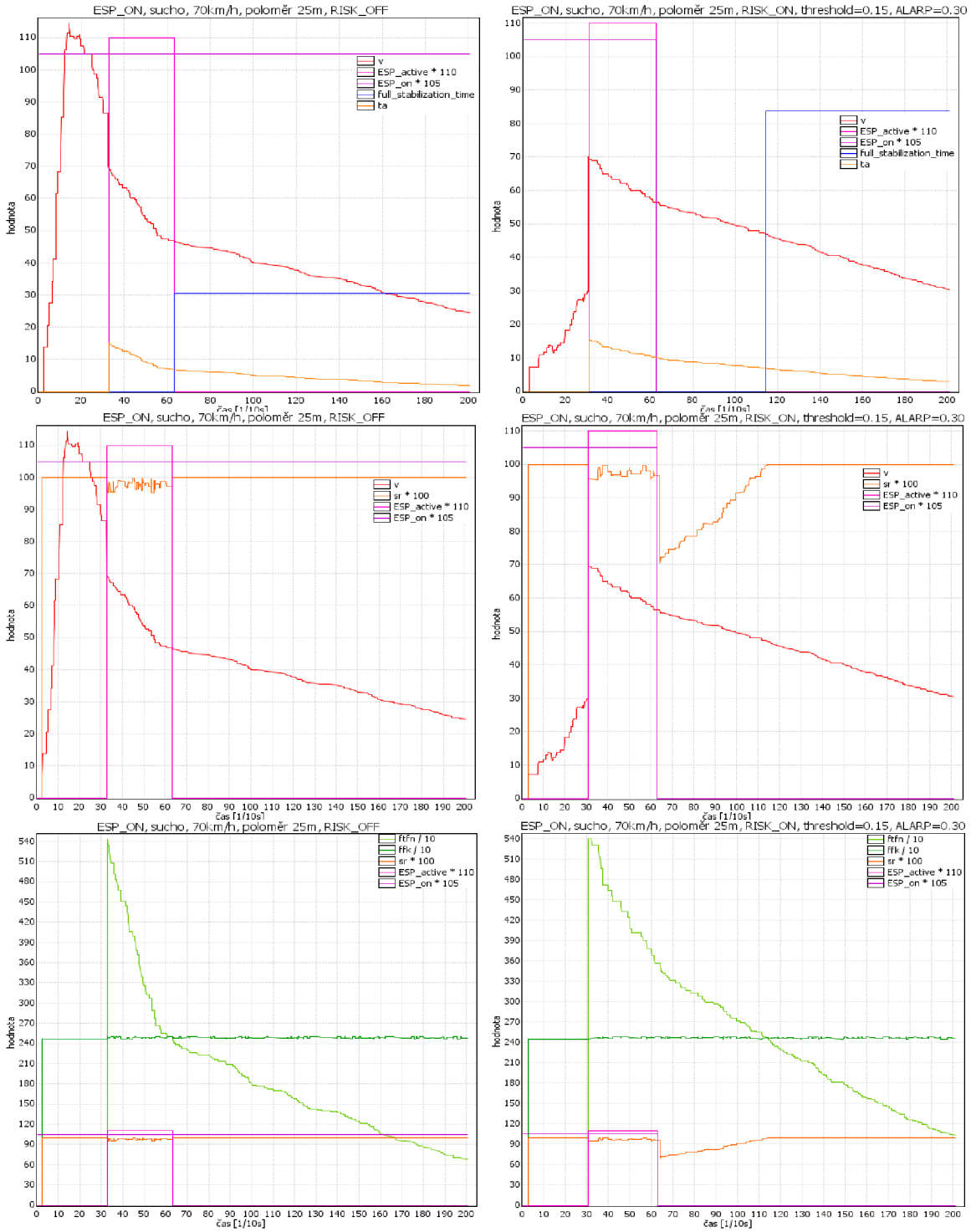
Obrázek 5.9: Vlevo simulace z původního modelu, vpravo simulace z upraveného modelu.

V obou grafech lze sledovat nejdůležitější proměnné v modelu, které ovlivňují jeho chování. Z výše uvedených grafů je zřejmé, že nedošlo ke ztrátě funkcionality, ani k jejímu zkreslení. Upravený model ESP s implementovanou analýzou rizik lze proto považovat za korektní.

5.2.2 2. test - Zatáčka s poloměrem $25m$, $70kmh^{-1}$, suchá vozovka

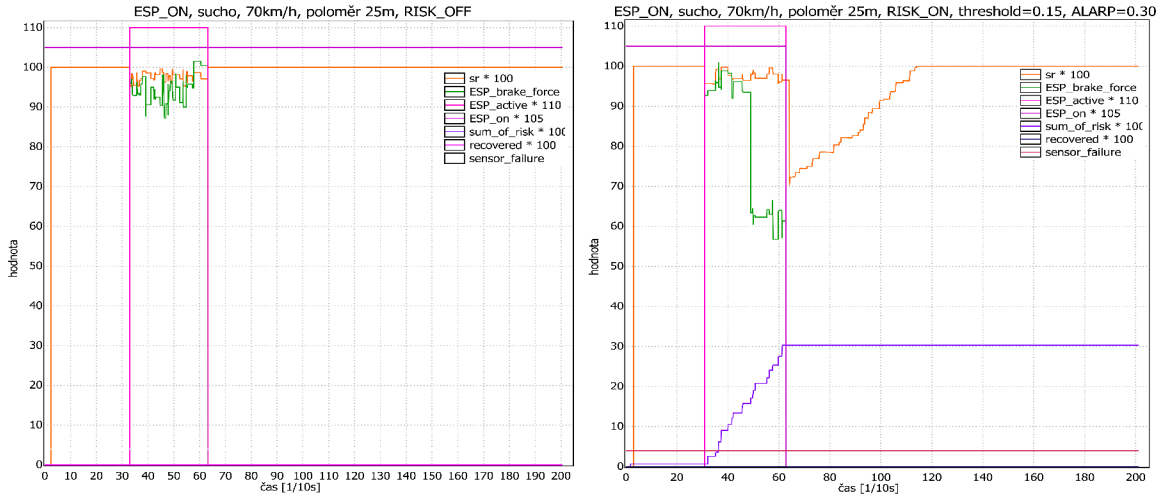
Druhý test bude zaměřen na simulaci jízdy na suché vozovce o poloměru 25 metrů s nájezdovou rychlostí $70kmh^{-1}$. Koeficient tření pod přední nápravou bude nastaven na hodnotu 0.7 a pod zadní nápravou na hodnotu 0.8 pro simulaci nedotáčivého chování vozidla. Rozložení váhy vozidla bude v poměru 66:34 a celková váha vozidla bude $1078kg$. Řidič bude projíždět pravotočivou zatáčku. Levá strana bude obsahovat grafy se zapnutým systémem ESP a vypnutým systémem pro analýzu rizik a na pravé straně budou prezentovány grafy s aktivním systémem ESP včetně implementované analýzy rizik.
První dvojice grafů je zaměřena na sledování veličiny akceleračního zrychlení v zatáčce. Na levém grafu je systém aktivní po dobu cca $3s$, poté vozidlo plně stabilizuje a již není nutné zasahovat do řízení. Na pravém grafu je zřejmé, že systém pro analýzu rizik systém ESP vypnul při překročení míry rizika.
Druhá dvojice je zaměřena na sledování míry stability. Na levém grafu je opět vidět, že

systém ESP drží po celou dobu manévru vozidlo stabilní. Na pravém grafu při vypnutí systému ESP znamená ztrátu stability, která nastává v čase 63.
Třetí dvojice grafů zobrazuje sílu potřebnou k zatočení `ftfn` a taktéž dostupnou sílu pod přední nápravou. Při překřížení těchto veličin v grafu dochází k obnovení stability vozidla.



Obrázek 5.10: Levá strana obsahuje grafy s ESP. Pravá strana obsahuje grafy s poruchou.

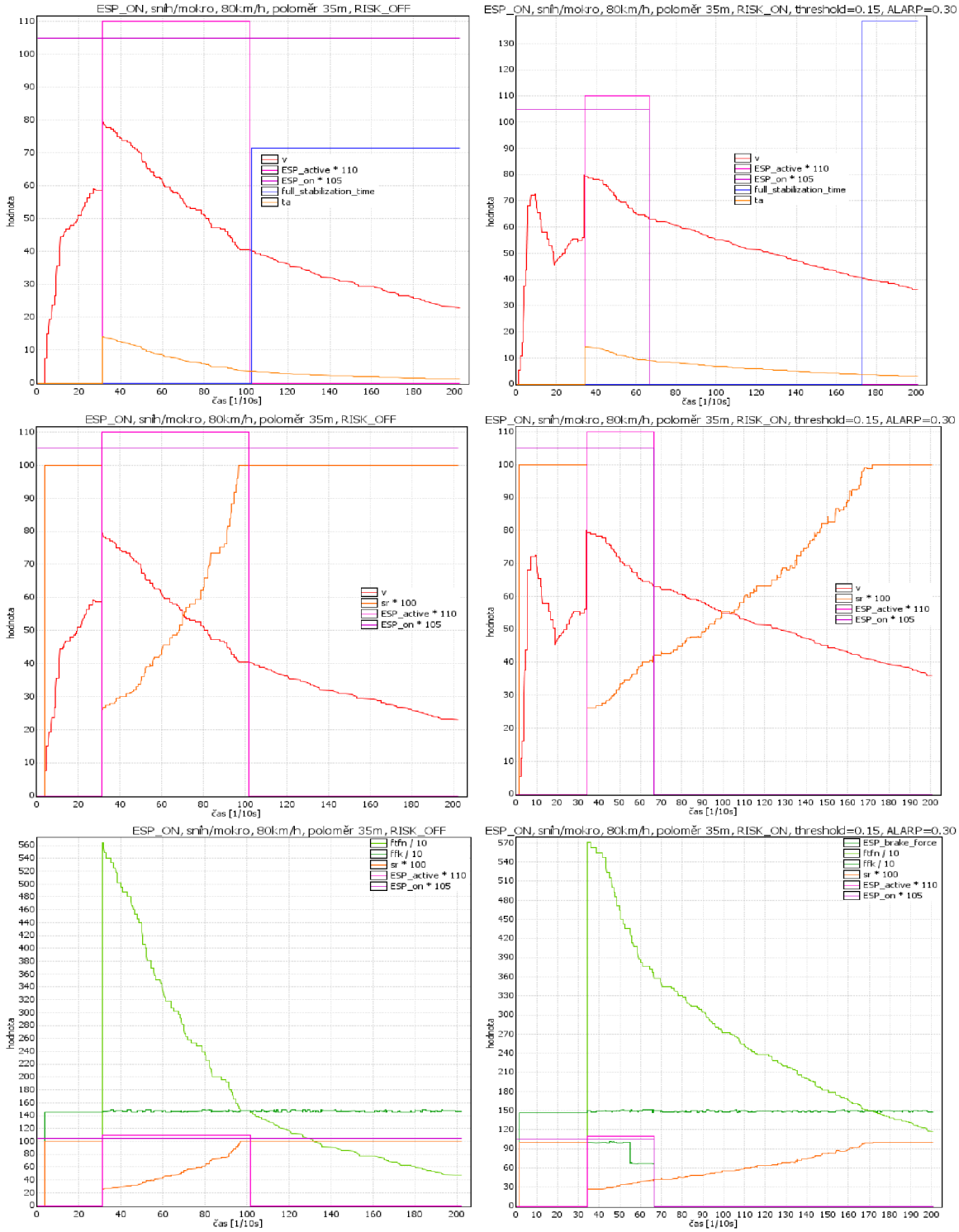
Poslední dvojice grafů sleduje průběh míry stability, brzdnou sílu vyvíjenou systémem ESP, aktivní stav ESP, celkovou míru rizika, zda se senzor zotavil (`recovered`) a senzor, který selhal.
Vlevo je možné pozorovat normální chování systému ESP bez systému analýzy rizik, a tudíž i bez poruchy.
V pravém grafu je možné vidět vylepšenou implementaci analýzy rizik oproti modelu ABS. Novou funkcionalitou je zavezení tzv. *ALARP* režimu. Při překročení maximální míry rizika definované konstantou `threshold` u systému ABS došlo k úplné deaktivaci systému. Režim *ALARP* je přechodovým stavem mezi aktivním systémem ESP a neaktivním systémem ESP. Smyslem tohoto stavu je, že systém pro analýzu rizik již ví, že dochází k selhání senzoru, avšak dává senzoru ještě možnost se zotavit. Při přechodu do režimu *ALARP* aplikuje systém ESP sílu `ESP_brake_force` vydělenou `ALARP_state_ESP_modifier`. Díky tomu je vozidlo stále stabilní. Po překročení maximální míry rizika režimu *ALARP* dochází k deaktivaci systému ESP systémem analýzy rizik. Je tedy zřejmé, že došlo k aktivaci režimu *ALARP*, senzor se nezotavil a došlo k deaktivaci systému ESP.



Obrázek 5.11: Levý obrázek - systém ESP bez poruchy. Vpravo - systém ESP s poruchou.

5.2.3 3. test - Zatáčka s poloměrem $35m$, $80kmh^{-1}$, zasněžená/mokrá vozovka

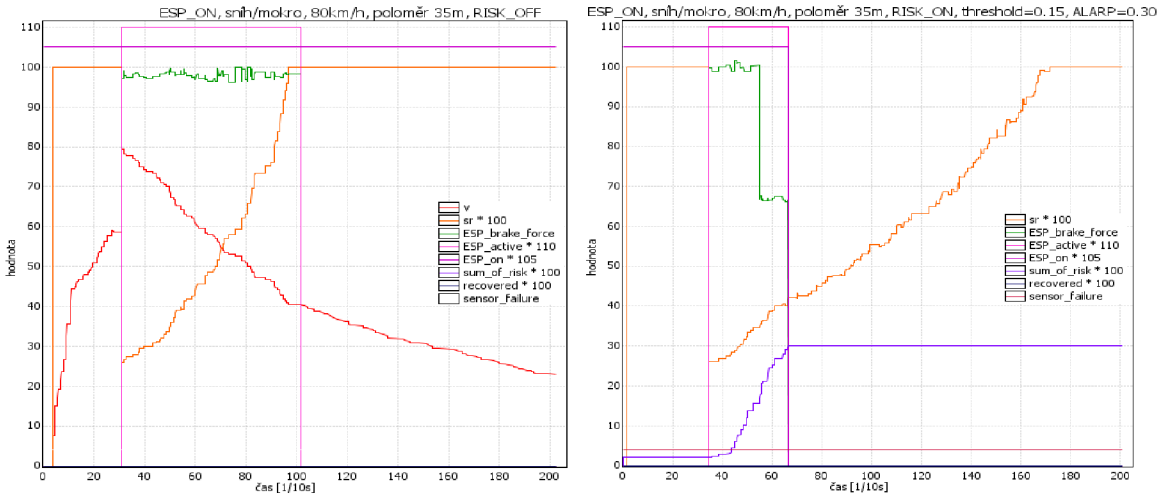
Třetí test je zaměřen na průjezd zatáčkou vozidlem za zhoršených jízdních podmínek. Pro tyto účely byly hodnoty třecího koeficientu nastaveny na hodnoty 0.37 pod přední nápravou a 0.5 pod zadní nápravou. Váha vozidla byla taktéž zvýšena na $1200kg$.
Struktura grafů je stejná jako v předchozím testu. Vlevo se nachází grafy se zapnutým systémem ESP a deaktivovaným systémem pro analýzu rizik a v pravé části jsou umístěny grafy
První graf sleduje průběh akceleračního zrychlení. V pravém grafu byl systém ESP systémem pro analýzu rizik deaktivován v čase 68.
Druhý graf sleduje míru stability vozu. Je zřejmé, že vozidlo s plně funkčním systémem ESP stabilizovalo vozidlo o cca 6.5 rychleji než vozidlo se systémem analýzy rizik.
Třetí graf opět sleduje průběh síly potřebné pro zatočení a limitní síly, kterou přenese pneumatika pod přední nápravou.



Obrázek 5.12: Vlevo průběh simulace bez analýzy rizik. Vpravo s analýzou rizik.

Na posledním grafu je opět možné nahlédnout na nejdůležitější proměnné pro systém analýzy rizik.
V levé části jsou vyobrazeny proměnné související se systémem ESP a analýzou rizik. Jelikož je systém pro analýzu rizik vypnutý, lze si povšimnout, že není analyzováno žádné

riziko, ani není aktivována možnost zotavení senzoru a taktéž nedochází k selhání žádného ze senzorů.
Pravý graf zobrazuje průběh simulace se stejnými veličinami se zapnutým systémem pro analýzu rizik. K poruše dochází v čase 36. Jelikož senzor stále vykazuje zákmitovou chybu, tak jej systém pro analýzu rizik neustále ohodnocuje zvyšující se mírou rizika. V čase 52 dochází k aktivaci režimu *ALARP*, je redukována brzdná síla systému ESP a systém pro analýzu rizik stále čeká, zda se senzor nezotaví. V modelovém čase 68 dochází k překročení maximální možné míry rizika režimu *ALARP* a deaktivaci systému ESP.

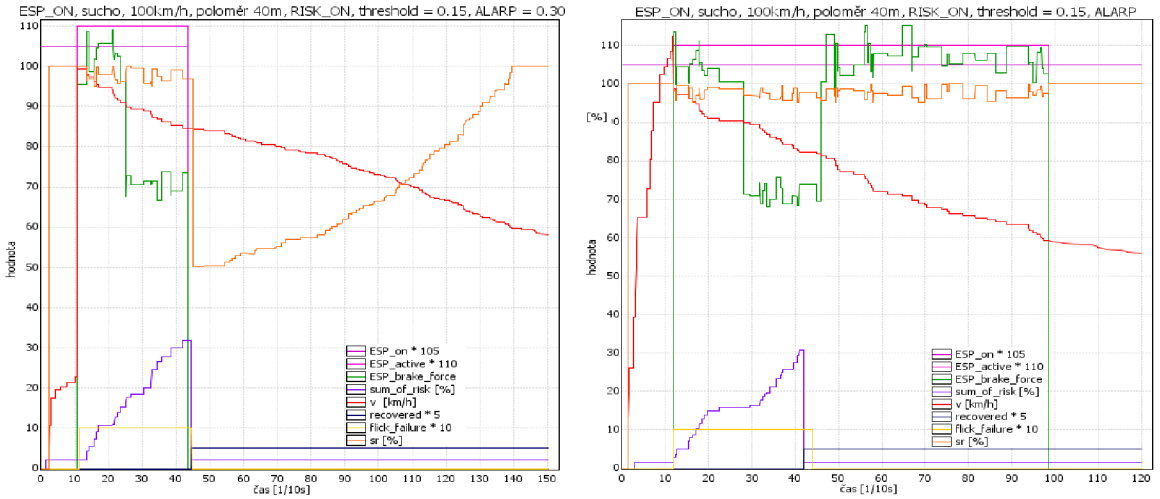


Obrázek 5.13: Vlevo průběh simulace bez analýzy rizik. Vpravo s analýzou rizik.

5.2.4 4. sada testů - konfigurovatelné vlastnosti modelu

Test zásahu řídící jednotky analýzy rizik s základní konfigurací

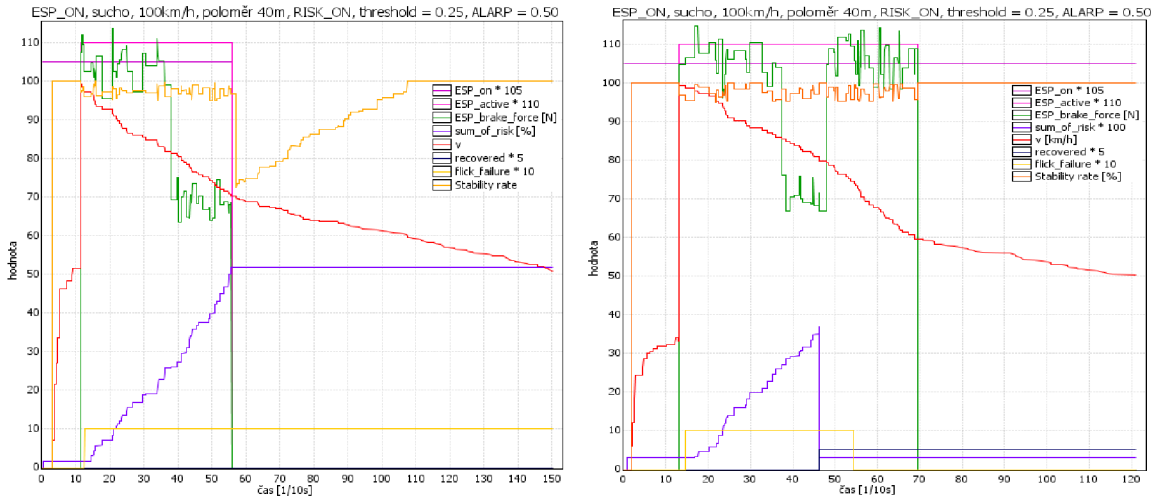
Systém pro analýzu rizik je nastaven na výchozí hodnoty.
Na levém grafu došlo ke zotavení senzoru až po vypnutí systému ESP, a proto byla míra rizika redukována. Systém ESP již aktivován nebyl. Pravý graf obsahuje zotavení senzoru těsně před překročením prahu režimu *ALARP*, a proto dochází k deaktivaci režimu *ALARP* a následné plné obnovení plné funkcionality systému ESP.



Obrázek 5.14: Grafy simulací s větší maximální mírou povoleného rizika.

Test zásahu ŘJ analýzy rizik se zvýšenou hranicí maximálního rizika

Druhý podtest obsahuje dvojici grafů, ve které byla zvýšena maximální míra rizika na 25% a taktéž byla zvýšena maximální míra rizika v režimu *ALARP*.
Levý graf obsahuje simulaci, při které nedošlo ke zotavení senzoru. Porucha nastává v čase 1.2 vteřiny a postupně pokračuje až do času 5.6 vteřiny, kdy je systém ESP deaktivován systémem pro analýzu rizik. Do času 3.4 vteřiny model pro analýzu rizik monitoruje situaci se selhávajícím senzorem a nijak nezasahuje do chování systému ESP. Od času 3.4 vteřiny ovšem dochází k překročení míry rizika a dochází k přepnutí do stavu *ALARP*, kdy model redukuje brzdnou sílu systému ESP. Od deaktivace systému ESP v čase 5.6 je možné pozorovat postupný nárůst hodnoty `Stability rate`, která vlivem vypnutí systému ESP klesla.
V pravém grafu je vyobrazena simulace, při které dojde ke zotavení senzoru. V čase 1.3 vteřiny nastává zákmitová porucha, která postupně narůstá až do času 4.7 vteřiny. V čase simulace 34 dochází k přepnutí do režimu *ALARP* a dochází k redukci brzdné síly systému ESP. V simulačním čase 47 je možné pozorovat, že se senzor zotavil, a proto systém pro analýzu rizik obnovil plnou funkcionalitu systému ESP a vozidlo pokračovalo v průjezdu zatáčkou bez ztráty stability.



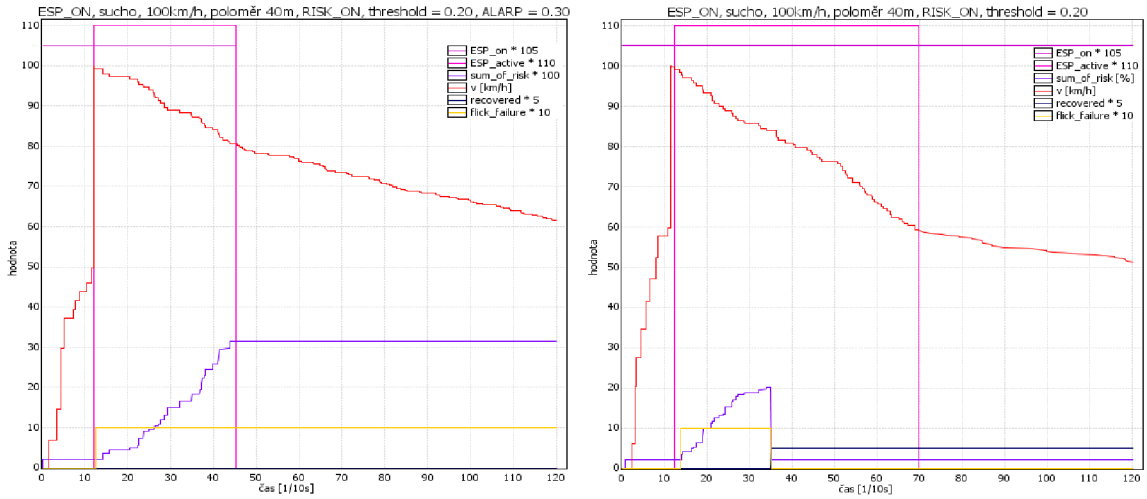
Obrázek 5.15: Grafy simulací se zásahem ŘJ analýzy rizik při zákmitu.

Test zásahu ŘJ analýzy rizik s redundantními senzory

Další dva podtesty budou zaměřeny na reakci systému pro analýzu rizik v případě dostupnosti redundantních senzorů.

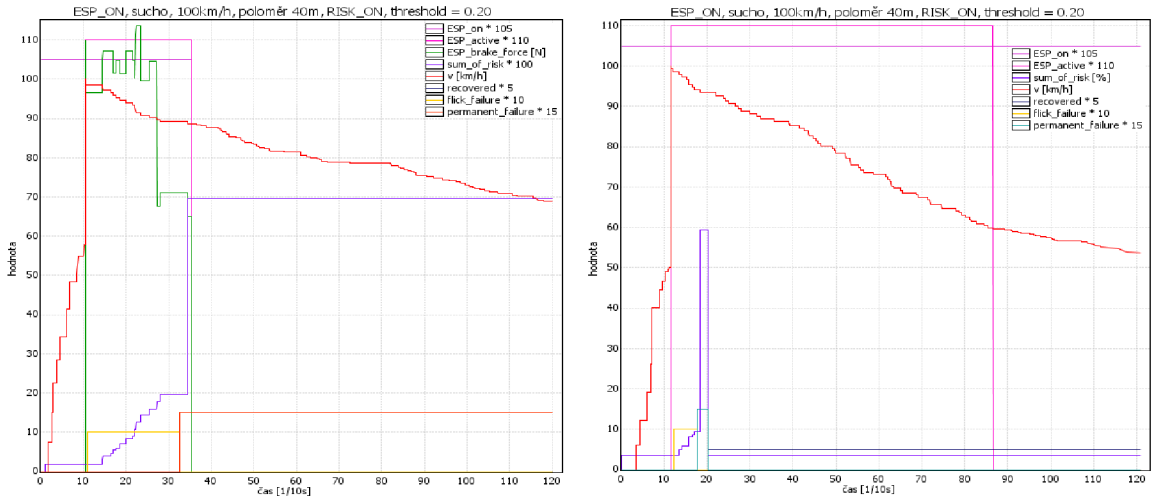
První dvojice grafů vyobrazuje dvě rozdílné chování systému pro analýzu rizik při (ne)dostupnosti redundantních senzorů při zákmitové poruše.
Levý graf zobrazuje situaci, při které nemá systém pro analýzu rizik dostupná náhradní čidla. Porucha nastává v simulačním čase 12. Senzor pokračuje ve svém nesprávném chování až do simulačního času 45, ve kterém již překročí maximální hranici rizika režimu *ALARP* a systém pro analýzu rizik deaktivuje systém ESP.
V pravém grafu nastává porucha v simulačním čase 13 a senzor pokračuje ve svojí špatné funkcionalitě až do simulačního času 35, ve kterém je překročena maximální míra rizika.

Systém pro analýzu rizik má dostupný náhradní senzor, a proto neaktivuje režim *ALARP*, ale nefunkční senzor nahradí senzorem náhradním. Nedojde k deaktivaci systému ESP, který tak může plnit svoji funkci po celou dobu běhu simulace.



Obrázek 5.16: Grafy simulací se zásahem ŘJ analýzy rizik při zákmitu.

Druhá dvojice grafů přibližuje situaci, při které dojde nejprve k zákmitové poruše, která se změní na poruchu permanentní. Opět bude možné sledovat průběh simulací a nahlédnout na chování systému pro analýzu rizik.
V levém grafu je vykreslena simulace, při které dochází v simulačním čase 10 k zákmitové poruše. Senzor pokračuje ve svém špatném chování až do času 35, ve kterém dochází k úplné ztrátě komunikace a tím i k permanentní poruše. Systém pro analýzu rizik tuto skutečnost identifikuje a z bezpečnostních důvodů deaktivuje systém ESP.
Pravý graf obsahuje podobnou simulaci jako levý graf. Hlavním rozdílem je, že systém pro analýzu rizik má dostupný náhradní senzor. V čase 13 dochází k zákmitu a senzor pokračuje v zákmitu až do času 18, kdy dojde k úplné ztrátě komunikace se senzorem. Systém pro analýzu rizik opět správně identifikuje problém ztráty komunikace, provede nahrazení nefunkčního senzoru senzorem funkčním a tím redukuje vzniklé riziko.



Obrázek 5.17: Grafy simulací se zásahem ŘJ analýzy rizik při permanentní poruše.

5.2.5 5. sada testů - pravděpodobnostní testy

Vliv parametru `sensor_mttf` na pravděpodobnost poruchy

Následující test bude zaměřen na vstupní parametr `sensor_mttf`.

Již dříve bylo řečeno, že parametr `sensor_mttf` má vliv na četnost poruch. V předchozích testech nebyl parametr podroben žádnému testu. Referenčním zdrojem pro hodnotu střední doby do poruchy byl vzat v úvahu reální senzor fungující na principu magnetické indukce viz [1], který udává střední dobu do poruchy $3010h$. Výrobci automobilových vozidel nezveřejňují hodnoty `mttf` jednotlivých senzorů a čidel, proto byl údaj převzat z uvedeného odkazu.

Důležitý je také stav vozidla, a proto byly parametry ovlivňující jeho stav zvoleny následovně:

- `car_age` - 10 let
- `average_age_per_year` - 100 hodin
- `car_mileage` - $100000km$
- `average_speed` - $60kmh^{-1}$

Z výpočtu uvedeném v 4.1 vyplývá, že opotřebení dosahuje $2666.67h$. Z následující tabulky bude tedy možné nahlédnout na pravděpodobnost poruchy vozidla při stejném opotřebení vozidla, ale s rozdílným parametrem `sensor_mttf`.

Hodnota sensor_mttf	Pravděpodobnost od: [%]	Pravděpodobnost do: [%]
1000 (118 běhů)	87.0731	97.0278
1500 (205 běhů)	80.3193	90.3169
2000 (306 běhů)	69.9289	79.9034
3010 (397 běhů)	50.6280	60.6219
6000 (383 běhů)	33.7396	43.7220
12040 (307 běhů)	20.3171	30.3094

Je zřejmé, že údaj `sensor_mttf` má značný vliv na výskyt poruch v modelu analýzy rizik. Pokud je tedy vzat v úvahu předpoklad, že výrobce použil senzor s hodnotou `mttf` $3010h$ dojde k poruše v 50-60% případů. V případě, že by výrobce použil senzor, který má čtyřnásobnou životnost, tak by k poruše došlo přibližně v 20-30% případů.

[1] shorturl.at/kszFG

Vliv opotřebení vozidla na pravděpodobnost poruchy

Následující test ověří předpoklad, že méně opotřebené vozidlo vykazuje nižší míru pravděpodobnosti poruchy stejně, jako v reálném světě.

Parametr `sensor_mttf` bude nastaven jako ve výchozí konfiguraci vozidla, a to na hodnotu $3010h$. Nastavované parametry budou: stáří vozidla v letech a nájezd vozidla v kilometrech. Parametr průměrné rychlosti zůstal na původní hodnotě $60kmh^{-1}$ a parametr průměrného stárnutí vozidla za rok taktéž zůstal na původní hodnotě $100h$.

Porovnáno bude úplně nové vozidlo, které si zákazník právě koupil u prodejce a dále vozidla s různým kilometrovým nájezdem a stářím vozidla. Starší vozidla s vyšším kilometrovým nájezdem může uživatel koupit například v automobilovém bazaru.

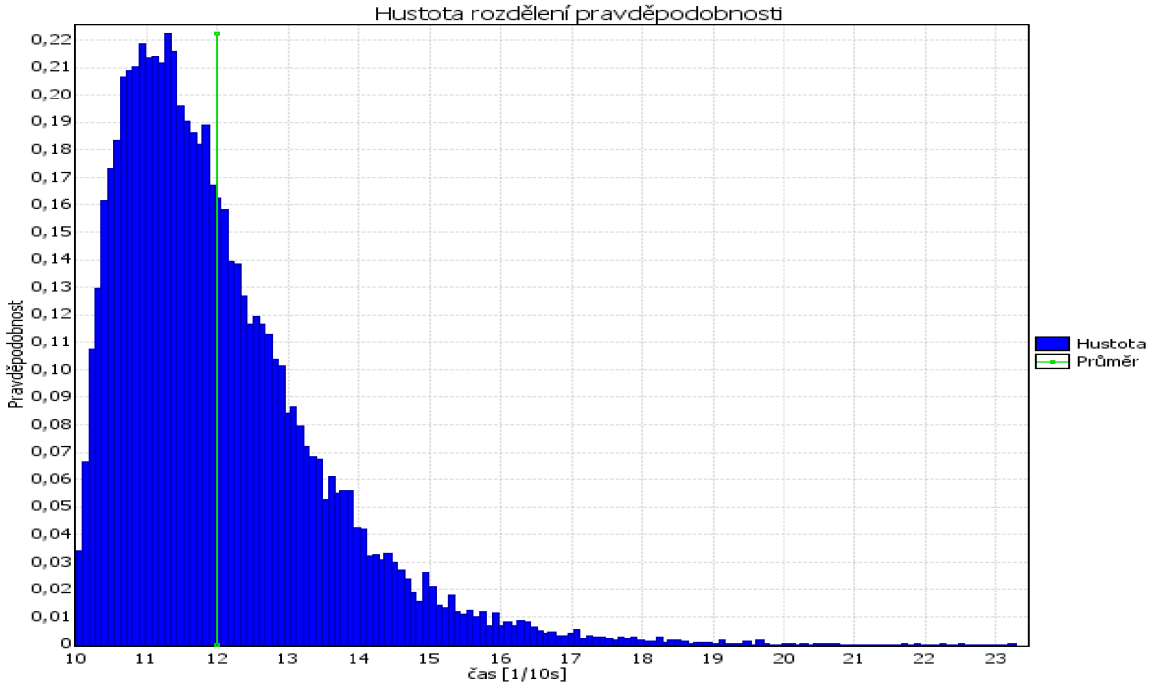
Stáří [roky]	Nájezd [km]	Pravděpodobnost od: [%]	Pravděpodobnost do: [%]
0 (98 běhů)	1	0	0.9814
3 (361 běhů)	50 000	28.6628	38.6462
7 (397 běhů)	50 000	37.5518	47.5494
3 (399 běhů)	100 000	40.8967	50.8944
7 (388 běhů)	100 000	54.4660	64.4596
10 (380 běhů)	100 000	56.7494	66.7488
10 (258 běhů)	200 000	75.2613	85.2603
20 (104 běhů)	400 000	87.8650	97.8536

Z výše uvedené tabulky je zřejmé, že stav opotřebení vozidla má na výskyt poruchy taktéž značný vliv. Testy tedy potvrdily předpoklad, že se porucha v novém vozidle téměř nevyskytla, což určitě reflektuje reálnou situaci.

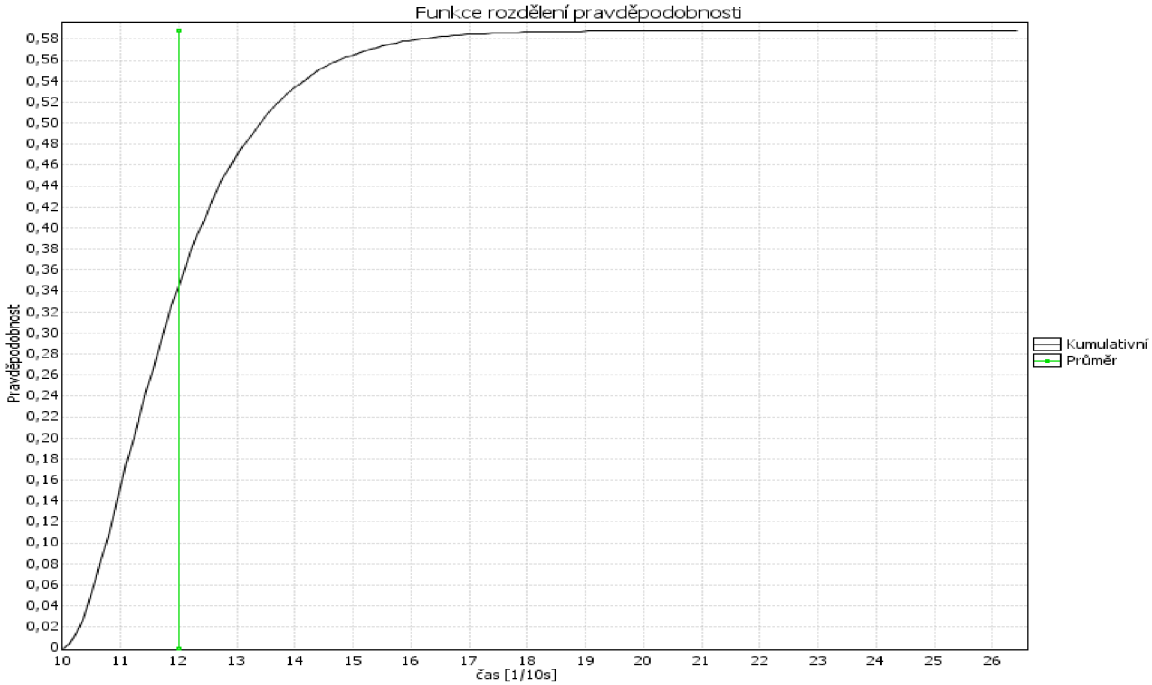
Další množinou vozidel byla méně/středně opotřebovaná vozidla. U této množiny se taktéž projevila reflexe reálného světa, že k poruchám občas dochází, a že poruchy ke středně opotřebovaným vozidlům zkrátka patří.

Poslední množinou vozidel jsou vozidla, která jsou již za zenitem a jsou již značně opotřebována. V této množině vozidel jsou poruchy velmi časté a určitě nejsou nic neobvyklého, jelikož všechny součástky a komponenty vozidla jsou již opotřebeny. Což je situace, která taktéž odpovídá reálnému světu.

Níže uvedené grafy prezentují hustotu rozdělení pravděpodobnosti a funkci rozdělení pravděpodobnosti výskytu poruchy v jednotlivých bězích simulace. Na ose x je vyobrazen čas poruchy v desetinách sekundy a na ose y je vyobrazena jeho pravděpodobnost. Z grafů lze usoudit, že k většině poruch v systému dochází do modelového času 12. Časový interval poruchy je ovlivněn zejména generátorem poruch, který generuje poruchy po příjmu synchronizačního signálu *turn*.



Obrázek 5.18: Hustota rozdělení pravděpodobnosti času poruchy.



Obrázek 5.19: Funkce rozdělení pravděpodobnosti času poruchy.

Časová náročnost

Čas potřebný k výpočtu pravděpodobnosti záleží na několika faktorech, jako je výkon procesoru, paměť, operační systém a podobně. Hlavním faktorem ovlivňujícím potřebný čas při spouštění simulací je nastavení statistického parametru nejistoty pravděpodobnosti $\mathcal{E}$ (Probability uncertainty) .

Při základním nastavení s nájezdem 100 000 km, stářím 10 let a parametrem $\mathcal{E}$ nastaveným na hodnotu 0.05 byla standardní doba běhu v rozmezí [5.2,5.9] sekundy. Konkrétní jeden běh výpočtu pravděpodobnosti potřeboval pro výpočet 385 běhů a přesný čas 5.688s.

Se stejným nastavením nájezdu kilometrů a stářím vozidla s upraveným parametrem $\mathcal{E}$ na hodnotu 0.005 byl proveden test pravděpodobnosti. Výsledky intervalu pravděpodobnosti se zúžily a pravděpodobnost byla v intervalu [58.5447, 59.5447]. Pro určení pravděpodobnosti potřeboval nástroj *UPPAAL* 504.766s a provedl při tom 37 365 běhů simulace.

Lze tedy konstatovat, že se časová složitost zvýšila zhruba stonásobně (přesněji 88.742x) při desetinásobném snížení parametru $\mathcal{E}$. Lze předpokládat, že při opětovném snížení parametru $\mathcal{E}$ na desetinu (0.0005) naroste časová závislost simulace opět přibližně stonásobně.

Testování časové náročnosti bylo provedeno také s jinými nastaveními modelu. Časová náročnost byla odlišná pouze v případě nového vozidla (nájezd 1km a stáří 0 let) a v případě velmi opotřebovaného vozidla (nájezd 400 000 km a stáří 20 let).
Za těchto podmínek proběhl test s parametrem $\mathcal{E}$ nastaveným na 0.05 v čase 0.564s při 105 vykonaných běžích simulace. Při snížení parametru $\mathcal{E}$ na desetinu původní hodnoty vzrostla časová náročnost přibližně desetinásobně (přesně 8.96 krát), jelikož čas pro vykonání testu byl 5.054s a bylo zapotřebí vykonat 345 běhů simulace.

Kapitola 6

Závěr

Cílem práce bylo zdokumentovat problematiku samočinně řízených vozidel, oblast analýzy rizik, provést rešerši z oblastí modelování systémů, připravit sadu výpočetních modelů samočinně řízených vozidel, navrhnout systém pro analýzu rizik v daných sadách modelů, systém pro analýzu rizik implementovat a ověřit jeho schopnosti analyzovat rizika.

Lze konstatovat, že cíle práce jsem dosáhl. Nejprve jsem se seznámil s okruhem samočinně řízených vozidel, analýzy rizik a prostředím *UPPAAL*. Dále jsem provedl návrhu systému analýzy rizik, jehož hlavními předpoklady byla jeho flexibilita, což znamená jeho nezávislost na konkrétní implementaci daného modelu, a taktéž možnost systém analýzy rizik deaktivovat se zachováním původního chování. Dle dostupných modelů v prostředí *UPPAAL* jsem vybral modely, které byly vhodné pro implementaci navrženého systému na základě jejich robustnosti a komplexity. Nejlepšími kandidáty se staly modely systémů ABS a ESP.

Systém analýzy rizik se mi podařilo do obou modelů implementovat s důležitým předpokladem, kterým bylo zachování původní funkčnosti modelu při deaktivování systému pro analýzu rizik. V modelu systému ABS systém pro analýzu rizik prováděl pouze deaktivaci systému ABS. V modelu systému ESP systém pro analýzu rizik dostal vylepšení oproti modelu ABS, jelikož systém ESP mohl pracovat v režimu omezené funkcionality vlivem rostoucího rizika, který jsem nazval režim *ALARP*. Pomocí experimentů a testů jsem implementovaný systém pro analýzu rizik v modelech systémů ABS a ESP ověřil v různých podmínkách a situacích.

Doporučení pro analýzu rizik v modelech:

Nejdůležitější úlohou je porozumět danému modelu, a proto je vhodné model podrobit velkému množství testů, ze kterého si člověk udělá úsudek o principu a fungování daného modelu. Vhodným pomocníkem při seznamování se s konkrétním modelem je krokování. Při krokování je vhodné sledovat jednotlivé proměnné, probíhající synchronizace mezi časovými automaty a plynoucí modelový čas. Díky krokování je možné jednodušeji a efektivněji vyhledávat případné chyby v implementaci.
Neodmyslitelnou úlohou je důkladné seznámení se s okruhem analýzy rizik. Pro správnou analýzu rizik je vhodné danou problematiku nastudovat a mít dobrý teoretický základ. K analýze rizik neodmyslitelně patří taktéž analytické myšlení neboli schopnost vyhodnocení situace a adekvátně na vzniklou situaci/okolnost zareagovat.

V práci by se dalo pokračovat analýzou a implementací systému analýzy rizik v dalších modelech. Jiným možným pokračováním by mohlo být přinesení dalších inovativních myšlenek do navrženého systému analýzy rizik a jejich následná implementace. Další variantou pokračování by bylo využití poznatků z modelů systému ABS, ESP, modelu samočinně parkujícího vozidla, modelu systému analýzy rizik, tyto modely sjednotit do jednoho většího modelu, který by obsahoval všechny uvedené modely a model podrobit vhodným testům a experimentům.

Literatura

[1] *The 6 levels of vehicle autonomy explained.* Dostupné z: https://www.synopsys.com/automotive/autonomous-driving-levels.html.

[2] *Gravitační a tíhové zrychlení.* Magda Králová. Dostupné z: http://edu.techmania.cz/cs/encyklopedie/fyzika/gravitace/gravitacni-tihove-zrychleni.

[3] *Modelica tools.* Dostupné z: https://modelica.org/tools.html.

[4] *Reactor safety study, an assessment of accident risks.* [online]. US Nuclear Regulatory Commission, 1975 [cit. 2021-11-06]. Dostupné z: https://www.nrc.gov/docs/ML0706/ML070610293.pdf.

[5] *Probabilistic risk assessment procedures guide for NASA managers and practitioners.Technical report.* NASA, 2002. Dostupné z: http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf.

[6] *Selector control functions.* Apr 2019. Dostupné z: https://instrumentationtools.com/selector-control-functions/.

[7] Bayesovská síť. In: *Wikipedie: Otevřená encyklopedie* [online]. Wikimedia Foundation, 2021. [rev. 2021-08-05]. [vid. 2021-11-08]. Dostupné z: https://cs.wikipedia.org/wiki/Bayesovsk%C3%A1_s%C3%AD%C5%A5.

[8] Metoda Monte Carlo. In: *Wikipedie: Otevřená encyklopedie* [online]. Wikimedia Foundation, 2021. [rev. 2021-09-29]. [vid. 2021-11-08]. Dostupné z: https://cs.wikipedia.org/wiki/Metoda_Monte_Carlo.

[9] Petriho sítě. In: *Wikipedie: Otevřená encyklopedie* [online]. Wikimedia Foundation, 2021. [rev. 2020-07-14]. [vid. 2021-11-07]. Dostupné z: https://cs.wikipedia.org/wiki/Petriho_s%C3%AD%C5%A5.

[10] Poissonovo rozdělení. In: *Wikipedie: Otevřená encyklopedie* [online]. Wikimedia Foundation, 2021. [rev. 2021-07-19]. [vid. 2021-11-09]. Dostupné z: https://cs.wikipedia.org/wiki/Poissonovo_rozd%C4%9Blen%C3%AD.

[11] *Radar.* Wikimedia Foundation, Oct 2021. Dostupné z: https://cs.wikipedia.org/wiki/Radar.

[12] *Dymola.* Wikimedia Foundation, Feb 2022. Dostupné z: https://en.wikipedia.org/wiki/Dymola.

[13] *Inductive sensor.* Wikimedia Foundation, Feb 2022. Dostupné z: https://en.wikipedia.org/wiki/Inductive_sensor.

[14] *Mean time between failures*. Wikimedia Foundation, Apr 2022. Dostupné z: https://en.wikipedia.org/wiki/Mean_time_between_failures.

[15] Behrmann, G., David, A. a Larsen, K. G. *A tutorial on Uppaal - Uppsala University*. Dostupné z: https://www.it.uu.se/research/group/darts/papers/texts/new-tutorial.pdf.

[16] Bhavsar, P., Das, P., Paugh, M., Dey, K. a Chowdhury, M. Risk Analysis of Autonomous Vehicles in Mixed Traffic Streams. *Transportation Research Record*. 2017, sv. 2625, č. 1, s. 51–61. DOI: 10.3141/2625-06.

[17] cesty.cz, B. *ESP (ESC)*. Bezpečné cesty.cz, Nov 2020. Dostupné z: https://www.bezpecnecesty.cz/cz/bezpecnost-automobilu/aktivni-prvky-bezpecnosti/esp-esc.

[18] Demmel, S., Gruyer, D., Burkhardt, J.-M., Glaser, S., Larue, G. et al. Global risk assessment in an autonomous driving context: Impact on both the car and the driver. *IFAC-PapersOnLine*. 2019, sv. 51, č. 34, s. 390–395. DOI: https://doi.org/10.1016/j.ifacol.2019.01.009. ISSN 2405-8963. 2nd IFAC Conference on Cyber-Physical and Human Systems CPHS 2018. Dostupné z: https://www.sciencedirect.com/science/article/pii/S2405896319300096.

[19] Didier, D. a Henri, P. *Theorie des possibilites: Applications a la representation des connaissances en informatique*. Masson, 1985.

[20] Eršil, L. *Manuál Pro Ekologickou, ekonomickou a bezpečnou jízdu*. Dostupné z: https://www.cistoustopou.cz/autem/clanek/manual-pro-ekologickou-ekonomickou-bezpecnou-jizdu-241.

[21] Ferson, S. a Ginzburg, L. *Different methods are needed to propagate ignorance and variability* [online]. Reliability Engineering and System Safety, 1996 [cit. 2021-11-06]. Dostupné z: https://www.sciencedirect.com/science/article/abs/pii/S0951832096000713?via3Dihub.

[22] Fusek, M. a Adámková, L. *Únava materiálu*. Dostupné z: https://projekty.fs.vsb.cz/463/edubase/VY_01_011/.

[23] Geotab Team, . *What is GPS?* Dostupné z: https://www.geotab.com/blog/what-is-gps/.

[24] Harris, M. *Researcher hacks self-driving car sensors*. IEEE Spectrum, Sep 2015. Dostupné z: https://spectrum.ieee.org/researcher-hacks-selfdriving-car-sensors.

[25] Holec, D. *Modelování a analýza vlivu ABS na chování vozidla*. Brno, CZ, 2018. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Dostupné z: https://www.fit.vut.cz/study/thesis/20623/.

[26] Jafari, M. a Roshanian, J. Optimal Redundant Sensor Configuration for Accuracy and Reliability Increasing in Space Inertial Navigation Systems. *Journal of Navigation*. Cambridge University Press. 2013, sv. 66, č. 2, s. 199–208. DOI: 10.1017/S0373463312000434.

[27] Kaplan, S. a Garrick, J. *On The Quantitative Definition Of Risk.* [online]. Leden 1981 [cit. 2021-11-07]. Dostupné z: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.323.1418&rep=rep1&type=pdf.

[28] Karasan, A., Kaya, I., Erdogan, M. a Budak, A. Risk Analysis of the Autonomous Vehicle Driving Systems by Using Pythagorean Fuzzy AHP. In:. Leden 2020, s. 926–934. DOI: 10.1007/978-3-030-23756-1_110. ISBN 978-3-030-23755-4.

[29] Kilián, K. *Čím Se Lidar Liší od radaru a jaká je jeho role v autonomních vozidlech.* VTM.cz, Oct 2018. Dostupné z: https://vtm.zive.cz/clanky/cim-se-lidar-lisi-od-radaru-a-jaka-je-jeho-role-v-autonomnich-vozidlech/sc-870-a-195431/default.aspx.

[30] Krucina, M. *Modelování a analýza řízení samočinně parkujícího vozidla.* Brno, CZ, 2021. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Dostupné z: https://www.fit.vut.cz/study/thesis/23481/.

[31] Káňa, L. a Slováček, P. *(Ne)přesnost automobilových tachometrů: Jsou přesnější, než byste čekali!* [online]. Prosinec 2019 [cit. 2021-11-07]. Dostupné z: https://www.auto.cz/ne-presnost-automobilovych-tachometru-jsou-presnejsi-nez-byste-cekali-132326.

[32] Křivka, Z. a Kolář, D. *Principy programovacích jazyků a objektově orientovaného programování II - Studijní opora.* 2019.

[33] Morris, S. *Exponential distribution.* Reliability analytics. Dostupné z: https://reliabilityanalyticstoolkit.appspot.com/exponential_distribution.

[34] Moss, R. J., Gupta, S., Dyro, R. a Leung, K. *Autonomous vehicle risk assessment.* Department of Aeronautics and Astronautics. Dostupné z: https://web.stanford.edu/~mossr/pdf/Autonomous_Vehicle_Risk_Assessment.pdf.

[35] Nilsen, T. a Aven, T. *Models and model uncertainty in the context of risk analysis.* [online]. Reliability Engineering and System Safety, 2003 [cit. 2021-11-05]. Dostupné z: https://www.sciencedirect.com/science/article/abs/pii/S0951832002002399?via3Dihub.

[36] Peringer, P. *SIMLIB Home Page.* Dostupné z: https://www.fit.vutbr.cz/~peringer/SIMLIB/.

[37] Peringer, P. *Modelování a simulace - Studijní opora.* 2012.

[38] Rudolph, G. a Voelzke, U. *Three sensor types drive autonomous vehicles.* Nov 2017. Dostupné z: https://www.fierceelectronics.com/components/three-sensor-types-drive-autonomous-vehicles.

[39] Toman, O. *Využití inerciální měřicí jednotky pro měření parametrů silnice.* 2014. Dostupné z: https://dspace.vutbr.cz/handle/11012/35064.

[40] Weber, M. *WHERE TO? A HISTORY OF AUTONOMOUS VEHICLES* [online]. 2014 [cit. 2021-12-30]. Dostupné z: https://computerhistory.org/blog/where-to-a-history-of-autonomous-vehicles/?key=where-to-a-history-of-autonomous-vehicles.

[41] Weigel, F. *Vliv ESP/ESC na chování vozidla.* Brno, CZ, 2020. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Dostupné z: https://www.fit.vut.cz/study/thesis/21569/.

[42] Zio, E. *An Introduction to the Basics of Reliability and Risk Analysis.* World Scientific, 2007.

[43] Zio, E. a Pedroni, N. *Uncertainty characterization in risk analysis for decision-making practice* [online]. des Cahiers de la Sécurité Industrielle, červenec 2012 [cit. 2021-11-05]. Dostupné z: https://www.foncsi.org/en/publications/collections/industrial-safety-cahiers/uncertainty-QRA/CSI-uncertainty-QRA.pdf.