Verslag Tinlab Advanced Algorithms

Galvin Bartes 0799967
176-671

26 oktober 2023

Inhoudsopgave

1 Inleiding

Algemeen Het ministerie van verkeer en Waterstaat wil in het kader van het klimaatakkoord en onderzoek laten uitvoeren naar de staat van het sluizenpark in Nederland. Het onderzoek moet zich richten op het ontwerpen en ontwikkelen van een geautomatiseerd sluismodel dat geschikt is voor een brede toepassing. In het onderzoek moet naar voren komen wat de huidige staat is van de sluizen met oog op veiligheid, efficiëntie, capaciteit, onderhoud, duurzaamheid en automatisering. Het onderzoek geeft aan hoe een volledig model worden opgeleverd opdat ontwerp van verschillend volledig geautomatiseerde sluizen in de toekomst geautomatiseerd kunnen worden.

Probleemanalyse Na grondige analyse van het Nederlandse sluizenpark is gebleken dat renovatie van een groot aantal sluizen noodzakelijk is. Uit een eerste verkenning is gebleken dat het gecombineerd renoveren en automatiseren van het Nederlandsesluizenpark een aanzienlijke verbetering kan opleveren t.a.v. Op het ministerie van infrastructuur enwaterstaat is helaas onvoldoende kennis van ict en systemen aanwezig om eenen ander uit te voeren

Waarom nu In het kader van het onlangs afgesloten klimaatakkoord heeft de Nederlandseoverheid daarom besloten over te gaan tot een ingrijpende renovatie van dediverse sluizen die ons land rijk is.

Gewenst resultaat Wij vragen u een model (of een onderling samenhangend aantal modellen)aan te leveren, opdat ontwerpen van verschillende, volledig geautomatiseerdesluizen in de toekomst gerealiseerd kunnen worden. Zoals gesteld in de brief is het de bedoeling dat een sluis gemodelleerd wordten dat bewezen kan worden dat de te bouwen sluis een aantal eigenschappenbezit.

Ons doel is een uppaal model van een sluis op te leveren. We wilen een fysiek systeem vastleggen in software, ofwel een domeini uit de echte wereld overplaatsen naar het conditionele. De phenomenen uit de echte wereld wprden gemonitored met sensoren. De phenomenen uit de wereld worden kenbaar gemaakt aan het softwaresysteem in de vorm van variabele data. Welke data wordt opgevangen, opgeslagen en uitgelezen wrdt vastgelegd in de requirements. De manier waarop dit gebeurt wordt vastegelegd in specificaties. De requirements worden verkregen door requirements engineers. Dit variert van concepten en best-practices uit observaties, interviews, stakehoders anaysis, focus group, document analysis, het verkennen van user requirements, task analysis, surveys en problem analysis. Requirements worden onderverdeeld in functioneel en niet-functioneel. Functionele requirements omschrijven de klantwens, ofwel functie en gedrag. Niet-functionele requirements/eisen zijn beperkt tot vereisten die aan systemen worden opgelegd. Ze hebben betrekking op kwaliteitsattributen als: schaalbaarheid, onderhoudbaarheid, beveiliging, betrouwbaarheid. Belangrijk is de vraag wat is een goed model. Voor het testen van een goed model of een specificatie zij verschillendetechnieken. In de biomedische wereld wordt er een onderscheidt gemaakt tussen in vivo "levendigïn vitro äfgeschieden experimentën insilico ëen gecomputeriseerd model".

Scope He gaat om het simuleren van een geautomatiseerde sluis. Wat voor type sluis wordt niet gemeld en ook niet uit welke onderdelen. Belangrijk is dat het model werkt en dat het voldoet aan de eisen die gebaseerd zijn op basis van literatuuronderzoek, observatie, interviews, brainstorming of een andere vorm van requirements elicitation.

Onderzoeksvragen Hoe kan een geautomatiseerde sluis worden gemodeleerd met oog op ontwikkel- en onderhoudskosten,veiligheid, efficientie en capaciteit

1. Welke requirements en kwaliteitseisen komen naar voren bij de analyse van een rampenonderzoek
2. Welke veiligheidseisen er zijn voor sluizen in nederland.
3. Hoe kan in uppaal een model worden getest dat voldoet aan de requirements/eisen volgens het rampenonderzoek?

Design goals Het systeem moet minimaal aan de volgende prestatie eisen voldoen

1. Requirements gebaseerd op rampenanalyse
2. Model testbaar in upaal

Leeswijzer In de methodologie wordt de lezer uitgelegd met welke methoden de onderzoeksvragen zijn beantwoord. In het hoofdstuk Onderzoek worden alle resultaten behandeld die naar voren zijn gekomen bij het deskresearch. De analyse van de verzamelde data wordt gedaan in het hoofdstuk analyse. Hierin wordt behandeld zoekopdracht naar IoT cloud platforms, feature extractie, prijs-berekening en prijs-feature vergelijking. In het ontwerp komen de uml diagrammen en systeemschetsen naar voren. In de de hoofdstukken Prototype, IoT cloud en Firmware wordt de implementatie behandeld van het IoT cloud platform in een bestaand project.

2 Theoretisch kader

In het eerste hoofdstuk is duidelijk geworden wat de onderzoeksvraag is, namelijk 'Hoe kan een geautomatiseerde sluis worden gemodeleerd met oog op ontwikkel- en onderhoudskosten,veiligheid, efficientie en capaciteit'. Door de toenemende complexiteit van systemen is het gebruik van modellen en de toepassing van timebased model checking op industriele controle systemen een manier van modelleren van het systeem en de requirements zodat er een bijdagre kan worden geleverd aan de acceptatie van simulatie-/modeltechniek voor de industrie.[?]. Of dit ook het geval is bij het modellereren van sluizen is nu de vraag.

De bestudering van rampen aan de hand van het vier-variabelen model biedt maakt het analyseren mogelijk van rampsituaties. Van een aantal rampen is een beschrijving gegeven met datum, plaats en oorzaak. De analyse van de 4-variabelen modellen zal gebruikt worden voor de requirementsdefinitie, ontwerp en ontwikkeling van het sluismodel.

De verschillende factoren en achtergronden die samenhangen met het modelleren van een sluis zullen in dit hoofdstuk toegelicht worden. Bovendien worden er hypotheses gevormd die de basis vormen voor debeantwoording van de onderzoeksvraag.

2.1 Begrippen, tools en literatuur

Wat is uppaal Uppaal is een geïntegreerde toolomgeving voor het modelleren, simuleren en verifiëren van real-time systemen, gezamenlijk ontwikkeld door Basic Research in Computer Science aan de Universiteit van Aalborg in Denemarken en de afdeling Informatietechnologie aan de Universiteit van Uppsala in Zweden. Het is geschikt voor systemen die kunnen worden gemodelleerd als een verzameling niet-deterministische processen met een eindige controlestructuur en klokken met reële waarde, die communiceren via kanalen of gedeelde variabelen . Typische toepassingsgebieden zijn met name real-time controllers en communicatieprotocollen, waarbij timingaspecten van cruciaal belang zijn.

Wat is statistical model checking? Dit verwijst naar verschillende technieken dfie worden gebruikt voor de monitoring van een systeem. Daarbij wordt vooral gelet op een specifieke eigenschap. Met de resultaten van de statsitieken wordt de juistheid van een ontwerp beoordeeld. Statistisch model checking wordt onder andere toegepast in systeembiologie, software engineering en industriele toepassingen. [?] [?]

Waarom gebruiken we statistisch model checking? Om de bovenstaande problemen te overwinnen stellen we voor om te werken met Statistical Model Checking , een aanpak die onlangs is voorgesteld als alternatief om een uitputtende verkenning van de toestandsruimte van het model te vermijden. Het kernidee van de aanpak is om een aantal simulaties van het systeem uit te voeren, deze te monitoren en vervolgens de resultaten uit het statistische gebied te gebruiken (inclusief het testen van sequentiële hypothesen of Monte Carlo-simulaties) om te beslissen of het systeem aan de eigenschap voldoet of niet. mate van vertrouwen. Van nature is SMC een compromis tussen testen en klassieke modelcontroletechnieken. Het is bekend dat op simulatie gebaseerde methoden veel minder geheugen- en tijdintensief zijn dan uitputtende methoden, en vaak de enige optie zijn. [?]Alternatieve tools voor Uppaal zijn Asynchronous Events,Vesta en MRMC.

MODE CONFUSION Mode confusion treed op als geobserveerd gedrag van een technisch systeem niet past in het gedragspatroon dat de gebruiker in zijn beeldvorming heeft en ook niet met

voorstellingsvermogen kan bevatten.

Wat is automatiseringsparadox Gemak dient de mens. Als er veel energie wordt gestoken in de ontwikkeling van hulmiddelen die taken van werknemers overemen heeft dat tot resultaat dat veel productieprocessen worden geautomatiseerd. De vraag is dan of vanuit mechnisch wereldpunt de robot niet de rol van de mens overneemt en of de mens nog de kwaliteiten heeft om het werk zelf te doen. [?] [?] [?]

4 variabelen model Er zijn veel veiligheidskritische computersystemen nodig voor het bewaken en besturen van fysieke processen processen. Het viervariabelenmodel, dat al bijna met succes in de industrie wordt gebruikt veertig jaar, helpt het gedrag van en de grenzen tussen het fysieke te verduidelijken processen, invoer-/uitvoerapparaten en software. [?]

Het 4 variabelen model kort toegelicht Monitored variabelen: door sensoren gekwantificeerde fenomenen uit de omgeving, bijv temperatuur

Controlled variabelen: door actuatoren bestuurde fenomenen uit de omgeving Gecontroleerde variabelen kunnen bijvoorbeeld de druk en de temperatuur zijn in een kernreactor, terwijl gecontroleerde variabelen ook visuele en hoorbare alarmen kunnen zijn als het uitschakelsignaal dat een reactorsluiting initieert; wanneer de temperatuur of druk bereikt abnormale waarden, de alarmen gaan af en de uitschakelprocedure wordt gestart

Input variabelen: data die de software als input gebruikt Hier modelleert IN de ingangshardware-interface (sensoren en analoog-naar-digitaal-omzetters) en relateert waarden van bewaakte variabelen aan waarden van invoervariabelen in de software. De invoervariabelen modelleren de informatie over de omgeving die beschikbaar is voor de software. Bijvoorbeeld, IN zou een druksensor kunnen modelleren die temperatuurwaarden omzet in analoge spanningen; Deze spanningen worden vervolgens via een A/D-omzetter omgezet in gehele waarden die zijn opgeslagen in een register dat toegankelijk is voor de computer software.

Output variabelen: data die de software levert als output De uitgangshardware-interface (digitaal-naar-analoog converters en actuatoren) is gemodelleerd door OUT, dat waarden van de uitvoervariabelen van de software relateert aan waarden van gecontroleerde variabelen. Een uitvoervariabele kan bijvoorbeeld een Booleaanse variabele zijn die door de software is ingesteld met de begrijpen dat de waarde true aangeeft dat een reactorsluiting zou moeten plaatsvinden en de waarde false geeft het tegenovergestelde aan

6 Variable model Een uitbreiding van een 4-variabelen model is het 6-variabelen model. Optitatieve statements omschrijven de omgeving zoals we het willen zien vanwege de machine. Indicatieve statements omschrijven de omgeving zoals deze is los van de machine. Een requirement is een optitatief statement omdat ten doel heeft om de klantwens uit te drukken in een softwareontwikkel project. Domein kennis bestaut uit indicatieve uitspraken die vanuit het oogpunt van software ontwikkeling relevant zijn. Een specificatie is een optitatief statement met als doel direct implementeerbaar te zijn en ter verondersteuning van het nastreven en realiseren van de requirements. Drie verschillende type domeinkennis: domein eigenschappen, domein hypothesen, en verwachtingen. Domein eingenschappen zijn beschrijvende statementsover een omgeving en zijn feiten. Domein hypotheses zijn ook beschrijvende uitspraken over een omgeving, maar zijn aannames. Verwachtingen zijn ook aannames, maar dat zijn voorschrijvende uitspraken die behaald worden door actoren als personen, sensoren en actuators.

World and machine samenvatting Inderdeel van deze cursus is de studie van het artikel World as a machine [?] Software engineering maakt het gebruik van fysieke apparaten mogelijk. Het is een beschrijving van de machine. Het doel van een machine ligt in de wereld. Commando afhandeling wordt niet beoordeeld door examinering van de software, maar door te kijken naar de kwaliteit van de geprogrammeerde documenten en het gebruik, gemak en voldoening voor de operators. Het probleem is de requirement dat ligt in de wereld en de machine is de oplossing die we bedenken. De relatie tussen machine en wereld blijkt uit de volgende 4 facetten:

- 1 modelling facet:
- interface facet:
- engineering facet:
- problem facet: requirements, specificaties en programmas zijn subsets van domeinen bestaande uit wereldlijke en machinale fenomenen. Decompositie van probleem verloopt parralel en niet hierarchisch.

denial bij knowledge: net meer het wiel uitvinden denial by hacking: obsessief toegewijs aan interactie met computers denial by abstraction: aoftwareproblemen kunnen bevangen worden in enkele simpele woorden. Het moeilijke is problemen op te splitsen. Denial by vageueness: vaag taalgebruik om probleem te verhullen

Formal recognizable description Gebruikte event als grondterm en geen english noun. Dit is reognizable. De wereld is niet strongly typed verschil tussen aannemen(optatief) en willen zien(indicatief)

Systeem vs software requirement Ter verduidelijking van het het verschil tussen systeemrequirement en softwarerequirement hieronder een overzicht:

Een system requirement is een uitspraak over wereld fenomenen (gedeeld of niet) of doelen die bereikt moeten worden. En systeem requirement is met enige regelmaat informeel, niet precies geformuleerd. Systemen gaan een zekere interactie aan met hun omgeving:Sensoren: meten fenomenen uit de omgeving (temperatuur,druk, licht, geluid, etc.). Actuatoren: veranderen iets in de omgeving (mechanische,electrisch, pneumatisch, etc.)

Een software requirement/specifcatie is een uitspraak over gedeelde fenomenen of doelen die de machine moet bereiken middels de onderdelen waar die machine uit of middels de fenomenen waar de machine controle over heeft. Is doorgaans preciezer, meetbaar, exact geformuleerd.

Software kan niet direct communiceren met de buitenwereld.Snapt derhalve niets van de buitenwereld. Kan alleen maar bestaan in en communiceren met het systeem.

Requirementsengineering Om de juiste requirements te verzamelen en selecteren hebben we meer kennis nodig van de methoden hiervoor gebruikt in het domein van requirementsengineering. [?] [?] [?] [?]

[?] [?].

what is a good software specification

- Een goed model heeft een duidelijk gespecificeerd modelleringsobject, dat wil zeggen dat het duidelijk is wat het model beschrijft.
- Een goed model heeft een duidelijk omschreven doel en draagt (idealiter) bij aan de realisatie van dat doel.

- Een goed model is traceerbaar: elk structureel element van een model (1) komt overeen met een aspect van het modelobject, of (2) codeert voor impliciete domeinkennis, of (3) codeert voor een aanvullende aanname.
- Een goed model is waarheidsgetrouw: relevante eigenschappen van het model moeten ook worden overgedragen op (behouden voor) het object van modellering.
- Een goed model is eenvoudig (maar niet te eenvoudig).
- Een goed model is uitbreidbaar en herbruikbaar, dat wil zeggen dat het is ontworpen om te evolueren en te worden gebruikt buiten het oorspronkelijke doel.
- Er is een goed model ontworpen en gecodeerd voor interoperabiliteit en het delen van semantiek.

[?]. Meer artikelen zijn: [?] [?] [?] [?] [?] [?] [?]

Wat is een sluis Een sluis is ook een scheiding tussen 2 wateren, maar met deuren. Hierdoor is het mogelijk het waterpeil te beïnvloeden. Sluizen reguleren het waterpeil zodat schepen kunnen passeren. Een stuw is een vaste of beweegbare afdamming tussen 2 wateren. [?]

[?] [?] [?] Een model van een sluispasssage kan worden gemodelleerd met procestates zoals het model aangeboden door Rijkswaterstaat

stroomschema_sluispassage.png

[?, p.79 –113] [?, p.159],

Recente ontwikkelingen op het gebied van sluisautomatisering Het ministerie van verkeer en Waterstaat wil in het kader van het klimaatakkoord en onderzoek laten uitvoeren naar de staat van het sluizenpark in Nederland. Het onderzoek moet zich richten op het ontwerpen en ontwikkelen van een geautomatiseerd sluismodel dat geschikt is voor een brede toepassing. In het onderzoek moet naar voren komen wat de huidige staat is van de sluizen met oog op veiligheid, efficiëntie, capaciteit, onderhoud, duurzaamheid en automatisering. Het onderzoek geeft aan hoe een volledig model worden opgeleverd opdat ontwerp van verschillend volledig geautomatiseerde sluizen in de toekomst geautomatiseerd kunnen worden.

2.2 Rampen

Voor deze studie is onderzoek gedaan naar verschillende rampen aan de hand van het vier variabelen model. Elke ramp op deze manier categoriseren kan ons helpen te bepalen in hoeverre requirements een rol kunnen spelen in de veiligheid van ons model.

2.2.1 Therac-25

Beschrijving In de periode van Juni 1985 and Januarie 1987 zijn er meerdere ongelukken met dodelijke afloop door de implementatie van de Therac-25 bij de behandelig van huidkanker. Dit apparaat gebruikt elektronen om stralen met hoge energie te creëren die tumoren kunnen vernietigen met minimale impact op het omliggende gezonde weefsel.

Datum en Plaats In de periode van Juni 1985 and Januarie 1987

Oorzaak Onderzoekers constateren dat er fouten zijn gemaakt tijdens de (her-)implementatie van systemen uit eerdere productiemodellen. Terwijl de therac 20 afhankelijk was van mechanische vergrendelingen werd er bij de therac-25 software gebruikt. Onderzoekers komen daarom tot de volgende conclusies Software problemen zijn onder andere:

- slechte software engineering/designing praktijken
- er is een machine gebouwd dat afhankelijk is van software voor veilgheidsoperaties
- de fout in de code is niet zo belangrijk als een geheel onveilig ontwer
- het reinigen van de buigmagneetvariabele in plaats van aan het uiteinde van het frame
- raceconditionering om aan te geven dat het invoeren van het recept nog steeds aan de gang is
- reactie van de gebruiker
- slechte subroutines voor schermvernieuwing die rommel en foutieve informatie op de werkende console achterlieten
- Problemen met het laden van tapes bij het opstarten, waarbij het gebruik van photom-tabellen werd uitgesloten om het interlock-systeem te activeren in het geval van een laadfout in plaats van een checksum

Onderzoekers zijn van mening dat de terkortkomingen in medische apparatuur niet geheel en altijd te verwijten zijn aan softwareproblemen. Zo is er ook een rol weggelegd voor fabrikanten en overheden. Klankbordgroepen klagen over het tekort aan software-evaluaties en een tekort aan hard-copy audit trials om foutmeldinen in beeld te krijgen. [?] [?] [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?],[?], [?], [?], [?], [?], [?], [?], [?], [?] , [?], [?], [?], [?].

2.2.2 Ethiopian Airlines Flight 302,boeing 737 crashes

Beschrijving Ethiopian Airlines Flight 302 was a scheduled international passenger flight from Bole International Airport in Addis Ababa, Ethiopia to Jomo Kenyatta International Airport in Nairobi, Kenya. On 10 March 2019, the Boeing 737 MAX 8 aircraft which operated the flight crashed near the town of Bishoftu six minutes after takeoff, killing all 157 people aboard.

Flight 302 is Ethiopian Airlines's deadliest accident to date, surpassing the fatal hijacking of Flight 961 resulting in a crash near the Comoros in 1996.[2][3] It is also the deadliest aircraft accident to occur in Ethiopia, surpassing the crash of an Ethiopian Air Force Antonov An-26 in 1982, which killed 73.[4]

This was the second MAX 8 accident in less than five months after the crash of Lion Air Flight 610.[2][5][6][7] Both crashes prompted a two-year worldwide long term grounding of the jet and an investigation into how the aircraft was approved for passenger service.

Datum en Plaats Op 10/03/2019 2019 stort vlucht ET302 van Ethiopian airlines neer. [?], [?],[?],[?], [?],[?].

Oorzaak De technische oorzaak ligt bij het MCAS flight control system. Dit systeem werd geimplementeerd om kosten te reduceren en opleidingen voor piloten in te korten. Deze single point of failure [?] werd getriggerd door een enkele angle-of-attack sensor[?]. Behalve de MCAS waren er nog andere failures[?], en ook deze failures [?] [?], Bij de nieuwe boeing 737 max model werden tests uitgevoerd in volledige flight simulators. Nieuwe regels van het FAA instituut vereisten ondersteuning bij het uitvoeren van enkele manouvres. Tijdens testvluchten uitgevoerd binnen een jaar voor certificatie werd het pitch-up fenomeen geconstateerd waarop het mcas systeem werd aangepast. [?],[?], [?],[?],[?],[?],[?],[?],[?],[?],[?]. In het systeem zaten nu de volgende fouten.

- MCAS wordt getriggerd woor enkele sensor zonder vertraging
- Het ontwerp staat toe dat in situaties waar de angle-of-attack fout is de mCAS wordt geactiveerd
- systeem kreeg onnidig bevoegdheid controle om de neus bij te sturen
- Waarschuwingslicht bij fouten in de angle-of-attack werkte niet door softwarefout. Het werd ook niet kritisch ebvonden door ethiopian airlines. geplande updates door boeing pas in 2020
- een losstande fout in de microprocessor va de controle computer kan vergelijkbare situaties doen voorkomen zonder dat mcas wordt geactiveerd

Fouten vielen niet op omdat FAA test uitbesteedde aan Boeing. Contact tussen de organisaties FAA en Boeing verliep op management niveau. Boeing instrueerde niet alle piloten ovver MCAS. En het MCAS systeem wwerd gezien als een achtergrond systeem.

Uit onderzoek is op te maken dat problemen bij boeing toestellen te verwijten zijn aan:

- marktdruk
- slapshot engineering
- missiekritische toepassing van technologie
- geen regelgevingsregime voor foutieve risicoanalyse

[?] [?]

2.2.3 China explosie 2015 Tianjin

Beschrijving De explosie zorgde voor de vernietiging van 12000 voertuigen, schade aan 17000 huize binnen een traal van 1 km. Er waren 173 doden inclusief brandweermensen. Een van de explosies zorgde voor een beving van 2.3 op de schaal van rigter. Opgeslagen materialen waren: calcium carbine, sodium nitraat, potassium nitraat, amminiak nitraat en cyanide. Ook is er veel kritiek geweest op de acties van de autoriteiten. Zo was er censuur vanuit de overheid op de journalistiek. Ook was er naar alle warschijnlijkheid sprake van corruptie. Zo bleek achteraf dat een van de grootste aandeelhouders Dong Shexuang de zoon te zijn van een oud-politiechef in Tanjin haven, genaamd Dong Pijun De overheid beloofde strengere toezicht en alle bedrijven moeten een risico-inventariatie maken en onderhouden .[?],[
[?].

Datum en Plaats Op 12 augustus 2015 waren er twee explosies bij de Rulthai logistiek. Deze faciliteit zorgde voor de opslag van gevaarlijke stoffen. De explosie tanjin china 12/08/2015.

Oorzaak De volgende factoren zouden een rol hebben gepeeld:

- Een onjuiste afbakening van het opslagmaeriaal
- Er was weinig kennis bij de autoriteiten over opslagmaterialen. Zo bleek er 7000 ton aan materiaal opgeslagen, dat is ruim 70 keer te maximaal toegestande hoeveelheid.
- Onverenigbaar grondgebruik in de nabije omgeving. Veel woonwijken met nar schatting 6000000 bewoners en 500 lokale bedrijvenin de buurt van de opslag gevaarlijke stoffen.

2.2.4 de malimissie

Beschrijving Aanwezige militair brengt slachtoffer naar de fransen, vervolgens naar de Tongolezen. Maar de kwaliteit van personeel liet te wensen over. Er werd een Nederlandse arts overgevlogen. De slachtoffers werden overgevlogen naar Gao omvervolgens te worden oergevolgen naar Nederland. Conclusie van de OVV[?] [?] [?] [?] [?] [?] [?] [?] [?] [?] luidt dat:

- Koopcontract werd niet goed doorgelezen
- Geen controle op kwaliteit en veiligheid
- Zwakke plekken in het ontwerp

- Opslag en gebruik in ongunstige condities
- De aanwezige medische voorzieningen waren nite volgends de nederlandse militaire richtlijnen
- Het ontbreek aan medische toetsing vanuit de defensie organisatie
- Twijfels die werden geuit binnen de defensieorganisae vonden geen wrrklank
- Ook het ongeval tijdens de mortieroefening was voor defensie geen aanleuiding om de medische voorzienignen te evalueren.
- De inrichting van veilige medische zorg voor nederlandse militairen in Kidal is ondergeschikt gemaakt aan de voortgang van de missie.

Datum en Plaats Het mortierongeluk in Mali op 06/04/2016.

Oorzaak Het ongeluk werd veroorzaakt door een kapot afsluitplaatje in de mortier. Tijdens de oefening werden de granaten warm in de zon. Granaat werd opgeslagen in niet gekoelde containers waardoor deze aan te hoge temeperaturen zijn blootgesteld. Dan was er vocht in de fatale granaat. Door de combinatie van vocht en warmte in de granaat werden zeer gevoelige explosieve stoffen werden gevormd. Het afsluitplaatje in de granaat bleek niet in staat om doorslag in veilige stand te voorkomen waarna de granaat explodeerde. De granaat stond niet op scherp en in afgegaan in veilige stand Uit onderzoek bleek dat de mortieren zijn aangeschaft bij de amerikanen. Gedurende de aanschafperiode zijn procedures en controles op kwaliteit en veiligheid deels nagelaten. Dit werd vermeld in het koopcontract.

2.2.5 schipholbrand

Beschrijving Bij de schipholbrand op 27/10/2005 . vielen zeker 11 doden onder mmigranten in de cellenclomplexen van schiphol-oost. Doodsoorzaak van de slachtffoffers is verstikking. Het gebrouw voldeed niet aan de eisen voor brandveiligheid, personeel was niet goed getraind voor dergelijke situaties en de hulpverlening kwam door verschillende factoren te laat op gang[?],[?],[?], [?],[?],[?],[?],[?],[?], [?],[?],[?],[?],[?],[?],[?],[?],[?],[?], [?],[?],[?].

Datum en Plaats Bij de vleugels j en k van cellenclomplexen van schiphol-oost op 27/10/2005 .

Oorzaak Volgens de onderzoekers van het OVV waren er geen specifieke eisen gesteld aan vleugels j en k door dienst jutitiele inrichtingen. Ook had dit instituut te weinig aandacht voor extra risicos. Daarnaast heeft de rijksgebouwendienst heeft zijn verantwoordelijkheid onvoldoende ingevuld, want vleugel j en k van het cellencomplex voldeden niet aan de eisen van de bouwregelgeving. Ook heeft de rijksgebouwendienst voorafafgaand onvoldoende gebruik gemaakt van onderzoek naar eerdere brand in de c-vleugel. De gemeente Haarlemmermeer heeft bouwvergunning gegeven terwijl vleugels j en k niet voldeden aan de bouwregelgeving.
De brandveiligheid is ook onderzocht door de OVV. In de brandmeldinstallatie is op verzoek van dienst jutitiele inrichtingen een vertraging van 3 minuten ingesteld,deze vertraging is niet formeel afgestemd met de brandweer, de vertraging is daarom door de brandweer niet vertaald in aangepast beleid. Bovendien was het inbouwen van de vertraging in strijd met de bouwvergunning waarbij werd uitgegaan van

een directte automatische doormelding bij brand.
De brandweer was niet op de hoogte van de actuele situatie op het cellencomplex, hierdoor had zij problemen met toegang te krijgen tot het complex, met als gevolg een langere opkomsttijd dan de norm. Er was geen gezamelijke oefenervaring met het personeel van het cellencomplex. De brandweer is in strijd met het calamiteitenplan niet goed opgevangen en begeleid door de aanwezige bhv'ers, hierdoor kreeg de brandweer moeilijk toegang tot de brandende vleugel en werde de bluswerkzamheden vertraagd. Bij aankomst werd de brandweer slecht geinformeerd over het aantal en de plaatst van de nog aanwezige celbewoners, de brandweer heeft tijd verloren met het zoeken anaar informatie over de situatie en de mogelijk nog aanwezige slachtoffers De bhv was onvoldoende opgeleid, geinstrueerd en geoefend voor de reddingsoperatie waar zij verantwoordelijk voor was.
Doordat de deur van cel 11 niet werd gesloten kreeg de brand zuurstof waardoor deze kont uitbreiden de aanwezigheid van grote hoeveelheid brandbare materialen, fungeerde als brandstof waardoor de brand zich verder kon ontwikkelen zowel binnen als buiten de cel.Doordat de dakluiken niet werken werd de rook en warmte niet afgevoerd, dit heeft de reddingsoperatie van de bewaarders belemmmerd en het mede onmogelijk gemaakt alle celdeuren te openen. Door de schilcontructie van het cellencomplex was het mogelijk dat de brand zich kon uitbreiden naar de andere cellen en naar de gang.
De bewoners van vleugel k zijn in eerste instantie geevacueerd naar vleugel j in plaatst van kruislings naar vleugel A. Door de evacuatie naar vleugel j bleven de bewoners geconfronteerd met de brand, waardoor er onnodig sprake was van angstgevoelens. Daarnaast werden de bewoners onvoldoende geinformeerd over de actuele situatie tijdens de brand en over de overplaatsing naar andere centra.
Er was geen evauactieplan dat voorziet in de overplaatsing van gedetineerden naar ander penetintiaire inrichtingen Bij de evacuatie naar andere detentiecentra is te weinig aandacht geweest voor ademhalingsproblemen van gedetineerden. Ook ging de grote instroom van gedetineerde in andere centra ten koste van kwaliteit van de opvang en nazorg. Zorgverlening te veel afhankelijk van ad-hoc maatregelen. De dienst jutitiele inrichtingen en de locatiedirecteur hadden geen duidelijk zicht op welke celbewoner naar welk detentiecetrum was overgeplaatst

Doordat de rechtervleugel beschadigd was, was het moeilijker om het vliegtuig recht te houden. Alleen de hoge snelheid zorgde ervoor dat er nog voldoende draagvermogen was. Toen bij het inzetten van de landing de snelheid verlaagd werd, werd het draagvermogen van de rechtervleugel echter dusdanig gering dat het toestel niet meer onder controle te houden was en een duikvlucht naar rechts maakte. [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?]

2.2.6 1951

Beschrijving Turkish Airlines-vlucht 1951 (ook bekend als TK 1951) was een passagiersvlucht die op woensdag 25 februari 2009 neerstortte in de buurt van het Nederlandse vliegveld Schiphol. Hierbij kwamen negen van de 135 inzittenden om het leven.

Het vliegtuig, een Boeing 737-800 van de Turkse maatschappij Turkish Airlines, was op weg van het vliegveld Istanbul Atatürk naar Schiphol, maar stortte om 10:26 uur,[1] kort voor de landing op de Polderbaan, neer op een akker en brak daarbij in drie stukken.[7][8]

Het officiële onderzoek van de Onderzoeksraad voor Veiligheid wees inadequaat handelen van de piloten als hoofdoorzaak aan voor het ongeluk. Ondanks een defecte hoogtemeter en onvolledige instructies van de luchtverkeersleiding hadden de piloten het ongeluk kunnen voorkomen, aldus de Onderzoeksraad.[

Datum en Plaats Op woensdag 25 februar 2009 voltrok zich de ramp met een toestel van turkisch airlines tijdensnvlucht 1951.

Oorzaak De automatische reactie van het toestel werd getriggerd door een fout gevoelige radio altimeter waardoor de automatische gashendel de energiemotot op actief stelde. Inadequaat handelen van de piloten ondanks een defecte hoogtemeter en onvolledige instructies van de luchtverkeersleiding [?] [?] [?] [?] [?] [?] [?] [?].

2.2.7 slmramp

Beschrijving Toen het toestel op 07/06/1989 de Anthony Nesty Zanderij naderde, was het daar, anders dan het weerbericht had voorspeld, mistig. Het zicht was evenwel niet zo slecht dat er niet op zicht kon worden geland. Gezagvoerder Will Rogers besloot echter via het Instrument Landing System (ILS) te landen, hoewel dit niet betrouwbaar was en hij voor zo'n landing ook geen toestemming had. De gezagvoerder brak drie landingspogingen af. Bij de vierde poging negeerde de bemanning de automatische waarschuwing (GPWS) dat het toestel te laag vloog. Het toestel raakte op 25 meter hoogte twee bomen. Het rolde om de lengteas en stortte om 04.27 uur plaatselijke tijd ondersteboven neer.

Datum en Plaats Toen het toestel op 07/06/1989 de Anthony Nesty Zanderij naderde

Oorzaak

Uit onderzoek bleek dat de papieren van de bemanning niet in orde ware door nalatigheid in de crew-member screening.Geconcludeerd werd dat de gezagvoerder roekeloos had gehandeld door voor een ILS-landing te kiezen terwijl hij daar geen toestemming voor had, en door onvoldoende op de vlieghoogte te hebben gelet. De SLM werd verweten de kwalificaties van de bemanning onvoldoende te hebben gecontroleerd. De Oorzaak van de ramp bleek achteraf het roekeloos besturen door de kapitein onder de minimum hoogte leidde tot collissie met een boom. [?],[?] [?],[?],[?], [?],[?], [?],[?],[?], [?],[?],[?],[?],[?],[?],[?],[?],[?].

2.2.8 Tsjernobyl

Beschrijving De mislukte veiligheidscontrole die 26 april 1986 01.24 uur in de SovjetUnie leiddte tot explosies in een van de reactoren in de kerncentrale. De reactoren hadden geen veiligheidsomhulling en de reactor bevat grote hoeveelheden brandbaar grafiet. Door de explosie en de brand kwamen er radioactieve stoffen vrij.het gaat helemaal mis in de kernreactor 4. De warmteproductie nam toe met een explosie tot gevolg. 31 mensen kwamen om, waaronder veel mensen dagen later door stralingsziekte.

Datum en Plaats De ramp van Tjernobyl voltrok zich op 26/04/1986 [?].

Oorzaak

Techici bij kerncentrale 4 voerden een slcht opgezet/ ontwerpen experiment uit. De kracht regulering werd uitgeschakeld evenals veiligheidssystemen. Door een bedieningsfout in een testprocedure werd het vermogen van de koelinstallaties negatief beinvloed. Mede door een ontwerpfout in de noodstopprocedure kon in het systeem niet snel genoeg schakelen om remmende invloed uit te oefenen op het toenemende vermogen van de reactorkernen. Met brand en explosies tot gevolg. [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?],[?], [?],[?], [?],[?],[?],[?],[?]

2.2.9 Safety critical systems

De kennis van de mens is veranwoordelijk voor jet scheppen van kennis. Opdoen van kennis van veiligeheidsintegriteit ten overstaan van ontwetendheid. Kennisdoelen zijn daarom altijd belangrijk en kunnen worden onderscheiden in 3 domeinen: cognitief, affectief en psychomotorisch.[?] Een Veiligheidsanalyse is een manier voor het evalueren van ongelukken en risicos op verschillende niveaus. Met een veiligheidsanalyse wordt gekeken naar mensen en systemen die worden blootgesteld aan een gevaar/risico en de mogelijkheid deze te minimaliseren. Veiligheid is moeilijk te defiinieren omdat het een vaag concept is. Een veiligheidsanalist moet kennis hebben van het systeem, maar ook ervaring met het systeem en vooral hoe een fout in het systeem zich voordoet. Volgens Stoney[?] is veiligheid een aspect dat de veiligheid van mensenleven of de omgevig niet in gevaar brengt. De interactie tussen systeem en omgeing levert kennis op door ad-hoc ervaring. Maar ook is kennis van abstractis en systeemdoelen belangrijk. Het kwalificeren van informatie moet ook op waarde geschat worden Een verkeerde schatting kan fataal zijn. Zelfs als een veiliegheidsanalse is is gedaan waarbij risicos zijn gedefinieerd en geprioretiseerd is een definitie vaneen veiligheidsnivea moetlik. Sos zijn hier richtlijnen voor en soms ook niet. Er zijn voorbeelden van tools en technieken te gebruiken voor een veiligheidsanalyse. En dat zijn

1. checklists voor critical safety items
2. fault tree analysis
3. event tree analysis
4. failure modes en critical effects analysis (FMECA, FMET)
5. hazard operability studies

[?] [?] [?] [?] [?] [?] [?].

Afbakening van requirements Wet en regelgeving voor sluizen Omdat we in dit onderzoek uitgaan van het uitbreiden van bestaande sluizen is er literatuurstudie gedaan naar sluizen. In de archieven van het ministerie van verkeer en waterstaat is er het rapport Design of waterlocks[?]. Het programma van requirements kunnen we in ons model niet helemaal overnemen. Zo zijn er precondities zaols topgrafie,bestaande watersluizen,waterlevel, wind, morphologie en bodemeigenschappen.

Modellen

2.3 De Kripke structuur

2.4 Soorten modellen

2.5 Tijd

2.5.1 Een begrensde responseigenschap

Een begrensde responseigenschap stelt dat een gewenste systeemreactie op een invoer vindt plaats binnen een tijdsinterval [b, e] met ondergrens b Tijd en bovengrens e Tijd waar b e. Bijvoorbeeld wanneer een voetganger bij een stoplicht duwt op de knop om over te steken, moet het licht voor voetgangers draaien groen binnen een tijdsinterval van bijvoorbeeld [10, 15]. De behoefte aan een bovenwerk grens is duidelijk: de voetganger wil binnen korte tijd de weg oversteken tijd (en niet uiteindelijk). Er is echter ook een ondergrens nodig omdat het verkeerslicht niet ogenblikkelijk van groen naar rood mag gaan,

maar pas na een gele fase van bijvoorbeeld 10 seconden om auto's zachtjes afremmen. Waarbij P(t) het indrukken van de knop op tijdstip t en voorstelt G(t) die een groen verkeerslicht voor de voetgangers voorstelt op tijdstip t, we kunnen de gewenste eigenschap uitdrukken met de formule $\forall$ t1 $\in$ Tijd $\cdot$ (P(t1) $\rightarrow \exists$t2 $\in [t1 + 10, t1 + 15]$ G(t2)) Merk op dat deze eigenschap binnen een bepaalde tijd kan worden vervalst. Wanneer voor een bepaald tijdstip t1 met P(t1) ontdekken we dat gedurende de tijd interval [t1 + 10, t1 + 15] verscheen geen groen licht voor de voetgangers, eigendom (1.3) wordt geschonden.

2.5.2 Duration properties

Een duureigenschap is subtieler. Het vereist dat voor observatie-intervallen [b, e] die voldoen aan een bepaalde voorwaarde A(b, e) de geaccumuleerde tijd waarin het systeem zich in een bepaalde kritieke fase bevindt toestand heeft een bovengrens u(b, e). De lekstatus van bijvoorbeeld een gasbrander, waarbij gas ontsnapt zonder dat de vlam brandt, moet voorkomen maximaal 5Om de geaccumuleerde tijd t van een kritische toestand C(t) in a te meten gegeven interval [b, e] gebruiken we de integrale notie van wiskundige calculus:

$$\int_b^e C(t)\,dx$$

Vervolgens kan de duureigenschap worden uitgedrukt door een formule:

$\forall$ b,e $\in$ Tijd $\bullet$ A(b,e) $= \int_b^e C(t)\,\mathrm{d}t \leq$ u(b,e)

Andere duration properties Queries voor een time based specificatie in Uppaal worden volgens literatuur [**?**] gedefinieerd als:

- Het is te allen tijde mogelijk dat een zwakke reeks A met tijdsinterval(s) [x, y] komt voor
- Het is te allen tijde mogelijk dat een zwakke reeks A met tijdsinterval(s) [x, y] dat wel doet niet voorkomen
- Het is te allen tijde mogelijk dat een sterke reeks A met tijdsinterval(s) [x, y] komt voor
- Het is te allen tijde mogelijk dat een element uit verzameling A voorkomt binnen het interval [x, y] .
- Het is te allen tijde mogelijk dat alle elementen van verzameling A gelijktijdig voorkomen binnen de interval [x, y]
- Het is te allen tijde mogelijk dat alle elementen van verzameling A uitsluitend binnen de verzameling voorkomen interval [x, y]
- Het is te allen tijde mogelijk dat een element uit verzameling A nooit voorkomt binnen de interval [x, y .
- Het is te allen tijde mogelijk dat alle elementen van verzameling A nooit tegelijkertijd voorkomen binnen het interval [x, y]

- Het is te allen tijde mogelijk dat alle elementen van verzameling A nooit uitsluitend binnenin voorkomen het interval [x, y]
- Het is te allen tijde waar dat als er een sterke reeks A met tijdsinterval(s) [x1, y1] optreedt dan moet het binnen [x2, y2] tijdseenheid(en) gebeuren dat een element uit verzameling B voorkomt
- Het is onvermijdelijk dat als alle elementen van verzameling A gelijktijdig voorkomen binnen de interval [x1, y1] dan is het mogelijk dat er op enig moment later een zwakke reeks B ontstaat
- tijdsinterval(s) [x2, y2] treedt op
- Het is te allen tijde waar dat alle elementen van verzameling A altijd gelijktijdig voorkomen binnen het interval [x1, y1] dan moet het in precies [z] tijdseenheid(en) gebeuren dat alles elementen van verzameling B komen gelijktijdig voor binnen het interval [x2, y2]

2.6 Guards en invarianten

2.7 Deadlock

• Deadlock een bereikbare staat kan helemaal geen acties uitvoeren – Deadlock hangt af van de reeks acties die een bereikbare staat niet kan uitvoeren • Om de impasse te behouden moet A niet alleen overschatten wat P kan doen, maar ook wat P weigert

2.8 Zeno gedrag

zeno gedrag: de mogelijkheid dat in een eindige hoeveelheid tijd een oneindig antal handelingen kan worden verricht. Bijvoorbeeld tijdens het nivelleren Bij het opstellen van schepen Bij het laten wachten van schepen Bij het invaren van schepen

3 Logica

3.1 Propositielogica

In de propositielogica onderzoekt men het waarheidsgehalte van samengestelde uitspraken aan de hand van elementaire proposities en logische voegwoorden. Wij noemen de woorden 'en', 'of', 'als . . . dan . . . ', 'impliceert' logische voegwoorden. Hoewel het taalkundig geen voegwoorden zijn, noemen wij de ontkenningen 'niet' en 'geen' toch logische voegwoorden.

In de propositielogica worden proposities gemaakt van elementaire proposities en logische voegwoorden. In de symbolische propositielogica, de propositierekening, wordt een propositieformule gemaakt van variabelen (letters), logische operatoren en haakjes. Net zoals een formule in de rekenkunde, heeft het deel van een propositieformule binnen de haakjes een hogere prioriteit dan het deel buiten de haakjes. Bovendien wordt alles wat tussen haakjes staat, beschouwd als een eenheid. Om een propositieformule correct samen te stellen, moeten wij verplicht gebruik maken van de volgende grammaticale regels:

1. Een variabele is een formule;
2. Als p een formule is, dan is :p een formule;
3. Als p en q formules zijn, dan zijn (p^q), (p_q), $(p!q)en(p$q) formules.

In een propositieformule mogen haakjes worden weggelaten mits er geen verwarring ontstaat

Tijdens het logisch beschrijven van logica of bij het maken van formules over formules, is het mogelijk dat wij een paradoxale uitspraak doen. Zo'n uitspraak is vergelijkbaar met de volgende zin: Deze zin is onwaar De bovenstaande zin beschrijft zichzelf. Is deze zin nu waar of onwaar? Dit is een paradox. Wij moeten de uitspraken over de logica scheiden van de logica zelf. Daarom introduceren wij metasymbolen. Deze metasymbolen zijn geen onderdeel van de beschreven logica, maar een toevoeging aan de omgangstaal in dit dictaat.

Voor het bepalen van de waarheidswaarde van een formule f(p1; p2; : : : ; pn) moeten alle mogelijke combinaties van waardetoekenningen worden bepaald. Deze combinatie van waardetoekenningen vormen samen de waarheidstabel van deze formule.

3.2 Predicatenlogica

Hoewel de volgende redenatie in de propositielogica ongeldig is, wordt zij intu¨ıtief toch als geldig beschouwd:

1. f1 "alle republikeinen plegen geen overspel"
2. f2 "sommige overspeligen zijn president"
3. y "sommige presidenten zijn geen republikein"

De geldigheid van deze redenatie is gebaseerd op informatie, waarmee de propositielogica geen rekening mee houdt. Om deze extra informatie bij het redeneren te betrekken, moeten wij de propositielogica uitbreiden met de begrippen eigenschappen, variabelen en kwantoren. De zin "alle mensen zijn sterfelijk" geeft aan dat objecten, die de eigenschap 'menselijk zijn' hebben, blijkbaar ook de eigenschap 'sterfelijk zijn' hebben. uitspraak symbolisch:

1. sterfelijk objecten S(x)
2. menselijke objecten M(x)
3. x is een priemgetal P(x)

In de uitspraken geven wij de eigenschappen sterfelijk en priemgetal aan met de hoofdletters S en P. De variabele x stelt objecten voor. Een variabele, waarvan de waarde onbekend is, noemen wij vrije variabele. Definitie 4.1 (Predikaat) Een predikaat is een uitspraak met vrije variabelen, die een propositie wordt zodra alle vrije variabelen in dat predikaat gebonden zijn aan een waarde.

3.3 Kwantoren

Kwantificator wordt gebruikt om de variabele van predikaten te kwantificeren. Het bevat een formule, een soort verklaring waarvan de waarheidswaarde kan afhangen van de waarden van sommige variabelen. Wanneer we een vaste waarde aan een predikaat toekennen, wordt het een propositie. Op een andere manier kunnen we zeggen dat als we het predikaat kwantificeren, het predikaat een propositie wordt. Kwantificeren is dus een woordsoort dat verwijst naar kwantificeringen als 'alles' of 'sommige'.

Er zijn hoofdzakelijk twee soorten kwantoren: universele kwantoren en existentiële kwantoren. Daarnaast hebben we ook andere soorten kwantoren, zoals geneste kwantoren en kwantoren in standaard Engels gebruik. Kwantificator wordt voornamelijk gebruikt om aan te tonen dat voor hoeveel elementen een beschreven predikaat waar is. Het laat ook zien dat voor alle mogelijke waarden of voor sommige waarde(n) in het universum van het discours het predikaat waar is of niet.

3.4 Dualiteiten

Principle of Duality in Discrete Mathematics Het dualiteitsbeginsel is een soort doordringende eigenschap van de algebraïsche structuur waarbij twee concepten alleen uitwisselbaar zijn als alle resultaten in de ene formulering ook gelden in een andere. Dit concept staat bekend als dubbele formulering. We zullen unions() omwisselen in intersecties() of intersecties() in de union() en ook de universele set omwisselen voor de nulset() of nullset voor universal(U) om de dubbele verklaring te krijgen. Als we het symbool verwisselen en deze verklaring zelf krijgen, zal deze bekend staan als de zelf-duale verklaring.Het dualiteitsbeginsel is een soort doordringende eigenschap van de algebraïsche structuur waarbij twee concepten alleen uitwisselbaar zijn als alle resultaten in de ene formulering ook gelden in een andere. Dit concept staat bekend als dubbele formulering. We zullen unions() omwisselen in intersecties() of intersecties() in de union() en ook de universele set omwisselen voor de nulset() of nullset voor universal(U) om de dubbele verklaring te krijgen. Als we het symbool verwisselen en deze verklaring zelf krijgen, zal deze bekend staan als de zelf-duale verklaring. https://www.javatpoint.com/principle-of-duality-in-discrete-mathematics

https://www.brainkart.com/article/Mathematical-Logic–Duality$_4$1291/

Dualiteit, in de wiskunde, principe waarbij de ene ware uitspraak uit de andere kan worden verkregen door slechts twee woorden met elkaar te verwisselen. Het is een eigenschap die behoort tot de tak van de algebra die bekend staat als de roostertheorie en die betrokken is bij de concepten van orde en structuur die in verschillende wiskundige systemen voorkomen. Een wiskundige structuur wordt een rooster genoemd als deze op een bepaalde manier kan worden geordend (zie volgorde). Projectieve meetkunde, verzamelingenleer en symbolische logica zijn voorbeelden van systemen met onderliggende roosterstructuren, en hebben daarom ook principes van dualiteit.

https://www.britannica.com/science/duality

Duality in mathematics is not a theorem, but a "principle". It has a simple origin, it is very powerful and useful, and has a long history going back hundreds of years. Over time it has been adapted and modified and so we can still use it in novel situations. It appears in many subjects in mathematics (geometry, algebra, analysis) and in physics. Fundamentally, duality gives two different points of view of looking at the same object. There are many things that have two different points of view and in principle they are all dualities. Linear duality in the plane. Linear algebra. Fourier transform. Fourier series. Poisson summation formula Fourier theory (3) Non-compact Lie groups. Intersection pairing. Poincar´e duality Hodge theorem. https://fme.upc.edu/ca/arxius/butlleti-digital/riemann/071218$_c onferencia_a tiyah - d_a rticle.pdf$

Duality is known to be a very general as well as a broad concept, without a strict definition that captures all those uses. There usually is a precise definition when duality is applied to specific concepts, for just that context. The common idea is that there are two things that basically are just two sides of the same coin.

In mathematics, we can define duality as a principle that translates concepts, theorems, or mathematical structures into other concepts, theorems, or structures, in a one-to-one fashion, often by means of an involution operation: if the dual of let's suppose A is equal to B, then we can say that the dual of B is A.

https://www.vedantu.com/maths/duality

https://academickids.com/encyclopedia/index.php/Duality

https://math.berkeley.edu/ shiyu/s15capstone/materials/Capstone$_D uals.pdf$

4 Computation tree logic

4.1 Algemeen

Doel van de studieis het modellerern vane eng eautomatiseerde sluis in Upaal. Het testen van het model op correctheid, rechability, safety en liveness kan worden uitgewerkt aan de hand van specificates en propositie vertaald uit de requirementsanalyse. De kripke structuur is een set van locaties, transities, guards, klokken en data-variabelen waarmee een real-time model van een gautomatiseerde slus kan worden vertaald naar een wiskundig model.

4.2 Operator: AG

We moeten aantonen dat een real-time programma voldoet aan de eisen opgesteld en gespecificeerd.

Een formele verificatie van de gespecificeerde requirements ofwel modeleigenschappen wordt gerealiseerd door deze e vertalen naar de query-language van de symbolic model-checker Uppaal. [?],[?]. Het systeem is gemodelleerd als een netwerk van meerdere timed automata in de vorm van templates: controller, sluis, stoplicht, deur, pomp en schip.

Het bewijs van de modeleigenschappen kan wiskundig worden opgesteld met behulp van kwantoren, zoals:

1. E there Exists a path
2. A in All paths
3. F sometime in the Future
4. G Globally in the future
5. X neXtime

4.3 Operator: EG

EGp - p holds globally.

4.4 Operator: AF

AFp - p holds sometime in the future.

4.5 Operator: EF

EF, there exists a path,from the current state, along which some state satisfies

4.6 Operator: AX

AXp - p holds next time.

4.7 Operator: EX

EXp - p holds next time.

4.8 Operator: p U q

p holds until q holds.

4.9 Operator: p R q

R ("release") is the logical dual of the U operator. The operator requires that the second argument must hold up to and including the first state where the first argument holds. The first argument is not required to become true eventually.

Temporal Operators – AFp - p holds sometime in the future. – AGp - p holds globally. – AXp - p holds next time. – A(pUq) - p holds until q holds. – EFp - p holds sometime in the future. – EGp - p holds globally. – EXp - p holds next time. – E(pUq) - p holds until q holds. – p and q are some temporal logic formulas. – Ex.: A(req ® AF ack), AG (Øgrant1 Ú Øgrant2)

4.10 Fairness

Er wordt een fairness constraint opgelegd aan (de planner van) het systeem dat het proces eerlijk selecteert volgende worden uitgevoerd. Technisch gezien is een fairness constraint een voorwaarde voor uitvoeringen (paden) van het systeem model. Hoewel deze beperkingen geen eigenschappen zijn die moeten worden geverifieerd (het zijn eerder veronderstelde omstandigheden). worden afgedwongen door de implementatie), kunnen ze worden uitgedrukt in temporele logica.

fairness is geen te controleren eigenschap van een systeem. Denk eens aan de manier waarop asynchrone systemen zijn gemodelleerd: als een grafiek waarin elk knooppunt een mondiale systeemtoestand vertegenwoordigt, en elke opvolger van een knooppunt komt overeen met de nieuwe mondiale toestand die wordt bereikt door een bepaald van de processen die een lokale transitie maken. Zo'n model bevat doorgaans geen informatie over hoe vaak een proces wordt uitgevoerd, of hoe het volgende proces wordt uitgevoerd het uit te voeren proces wordt gekozen door de planner; in feite is het model onafhankelijk van de onderliggende besturingssysteem en dus van de planner: planning wordt niet-deterministisch behandeld. [**?**]

Data variabelen Dat variabelen zijn onder andere: water hoog en laag, en aanal schepen in de queue.

Acties Acties in het model zijn onder andere: invaren, uitvaren, deuren openen en sluiten, nivelleren

4.11 liveness properties

Veiligheidseigenschappen geven aan wat er wel of niet mag voorkomen, maar eis niet dat er ooit iets gebeurt. Levendigheidseigenschappen geven aan wat er moet gebeuren. De eenvoudigste vorm van een liveness-eigenschap garandeert dat er uiteindelijk iets goeds gebeurt. De 'goede zaak' vertegenwoordigt een wenselijke systeemtoestand, bijvoorbeeld de poorten open voor het wegverkeer. Een Booleaanse waarneembare nemen G : Tijd $\rightarrow$ 0, 1, waarbij G(t) = 1 drukt uit dat op tijdstip t de systeem in goede staat verkeert, kan deze levendigheidseigenschap tot uitdrukking worden gebracht volgens de formule: t $\in$ Tijd $\cdot$ G(t). Met andere woorden: er bestaat een tijdstip waarop het systeem zich in de goede staat. Houd er rekening mee dat deze eigenschap niet in bounded kan worden vervalst tijd. Als voor enig tijdstip t0 alleen $\neg$G(t) is waargenomen t t0, we kunnen niet klagen dat (1.2) uiteindelijk wordt

geschonden zegt niet hoe lang het zal duren voordat de goede toestand zich zal voordoen. Een dergelijke liveness-eigenschap is niet sterk genoeg in de context van realtime systemen. Hier zou men graag een tijdgebonden zien wanneer de goede toestand ontstaat. Dit brengt ons bij het volgende soort vastgoed. begrensde responseigenschappen

[?, p.23]

Een propositie kan ook worden geschreven als : $AGEF_{[x,y]} \models \Phi_1$

Of geheel als functie:

$\forall$ b,e $\in$ Time $\bullet$ A(b,e) $= \int_b^e C(t)\,\mathrm{d}t \leq$ u(b,e)

5 Conclusie

Op basis van de onderzoeksresultaten uit de literatuurstudie komt naar voren dat veilgheid een aspect is dat meot worden meegenomen bij de requirements engineering proces. Bij de therac waren er diverse problemen: communicatie, doorontwikkeling, controle en toetsing Bij de boeing 737 crashes was het probleem van controle en communicatie naar medewerkers Uit de evaluatie van de china explosion 2015 tianjin komt naar voren dat communicatie, transparantie en veiligheid niet altijd prioriteit hadden bij de lokale autoriteiten Bij de tesla autopilot crashes komen soms onvoldoende onderbouwde ontwerpkeuzes naar voren die niet goed zij afgewogen tegenover het gedrag van de bestuurder. De ramp in Tsjernobyl toont aan hoe autoriteiten een ramp in de doofpot proberen te stoppen Uit de concepten die zijn ontwikkeld en gevisualiseerd in het hoofdstuk ontwikkelgeschiedenis blijkt dat het implementeren van veiligheid in realtimesystemen niet volledig is geimplementeerd. Geprobeerd is om de afhandeling van schepen in te regelen vai procedures gebruikt door een maincontroller. Een task scheduler in het concept van 19 meiEen waterlevelsensor en en priorityqueue in templates van 12 juni, 13 juni, 23 juni en 16 juli. Of een error handling template in het concept van 22 mei, 6 juni. Dit resulteerde in de concepten van 19 en 20 september Tijdens de studie is naar voren gekomen dat de meilijkheid van modelleren in uppaal vooraal ligt bij de definitie van de propositie logca voor time-based model checking en dan met name clocks en regions. Was het makkelijk te onderzoeken? Waarom? Wat heb ik geleerd Belangrijkste leerpunt van deze studie is het belang van reqirements en specificaties. Een oede requirementsdefinitie is belangrijk voorde ontwikkeling van een model alsook het testen van de specificaties en de evaluatie hiervan.