Verslag Tinlab Advanced Algorithms

T. Ravensbergen
G. Bartes
K. G. Razmjou
69

27 mei 2023

Inhoudsopgave

Inleiding

1 Inleiding

In deze case study wordt

1.0.1 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.

1.0.2 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.

1.0.3 Wat is een sluis

1.0.4 Wat worrdt er omschreven en wat is er geleerd

1.0.5 Wat is uppaal

1.0.6 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

1.0.7 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.

1.0.8 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.

1.0.9 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.

1.0.10 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?

1.0.11 Design goals

Het systeem moet minimaal aan de volgende prestatie eisen voldoen

1. (a) Requirements gebaseerd op rampenanalyse
2. Data
    (a) Model testbaar in upaal

1.0.12 Welke aanpak is gekozen en welke studies liggen hieraan ten grondslag?

https://link.springer.com/article/10.1007/s10626-020-00314-0

1.0.13 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.

Methodologie

1.0.14 Literatuuronderzoek

Literature Review

S.no	Author	Title	Findings	Gap in literature
S.no	Author	wanrooy _vab1991a.pdf	Findings	Gap in literature
S.no	Author	wa3300-bezuien2000(1).pdf	Findings	Gap in literature
S.no	Author	Title	Findings	Gap in literature
S.no	Author	Title	Findings	Gap in literature
S.no	Author	rapport-veiligheid-van-op-afstand-bediende-burggen.pd	Findings	Gap in literature
S.no	Author	pronk.pdf	Findings	Gap in literature
S.no	Author	Olieman1987a.pdf	Findings	Gap in literature
S.no	Author	richtlijnen-vaarwegen-2020.pdf	Findings	Gap in literature
S.no	Author	richtlijnen-vaarwegen-2017 _tcm21-127359(1).pdf	Findings	Gap in literature
S.no	Author	Olieman1987a.pdf	Findings	Gap in literature
S.no	Author	Meijer1980b.pdf	Findings	Gap in literature
S.no	Author	Meijer1980c.pdf	Findings	Gap in literature
S.no	Author	kst-31200-A-80-b2.pdf	Findings	Gap in literature
S.no	Author	duurzaamheid _bij _de _ontwikkeling _van _reevesluis.pdf	Findings	Gap in literature
S.no	Author	De _deltawerken _Cultuurhistorie _ontwerpgeschiedenis _web-A.pdf	Findings	Gap in literature
S.no	Author	wa3300-Bezuijen2000.pdf	Findings	Gap in literature
S.no	Author	Sander van Alphen Haalbaarheidsstudie naar grote sluisdeuren uitgevoerd in hogesterktebeton.pdf	Findings	Gap in literature
S.no	Author	Dalmeijer1994a.pdf	Findings	Gap in literature
S.no	Author	Dalmeijer1994b.pdf	Findings	Gap in literature
S.no	Author	Dalmeijer1994c.pdf	Findings	Gap in literature
S.no	Author	ceg _pruijssers _1982.pdf	Findings	Gap in literature
S.no	Author	Capaciteitsanalyse _van _de _prinses_margrietsluis _in _lemmer _- _Marc _Lamboo.pdf	Findings	Gap in literature
S.no	Author	Boer1979a.pdf	Findings	Gap in literature
S.no	Author	bijlagerapport _c _- _analyse _geavanceerd-definitief _v1 _0.pdf	Findings	Gap in literature
S.no	Author	Bijl1988a.pdf	Findings	Gap in literature
S.no	Author	Bentum1978a.pdf	Findings	Gap in literature
S.no	Author	Alphen.pdf	Findings	Gap in literature
S.no	Author	Abbenhuis1975a.pdf	Findings	Gap in literature
S.no	Author	Abbenhuis1974a.pdf	Findings	Gap in literature
S.no	Author	https://wiki.woudagemaal.nl/w/index.php/Sluizen	Findings	Gap in literature
S.no	Author	Title	Findings	Gap in literature

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.('https://link.springer.com/article/10.1007/s10626-020-00314-0', 2020). Of dit ook het geval is bij het modellereren van sluizen is nu de vraag. De verschillende factoren en achtergronden die hiermee samenhangen met het modelleren van een sluiszullen in dit hoofdstuk toegelicht worden. Bovendien worden er hypotheses gevormd die de basis vormen voor de beantwoording van de onderzoeksvraag.

2.1 Beperking uppaal ten overstaan van ons model

Welke versie van Uppaal gebruiken wij en welke beperkingen heeft deze software voor het bereiken van onze doelstelling

2.2 MODE CONFUSION

Mode confusion tredd op als gepbserveerd gedrag van een technisch systeem niet past in het gedragspatroon dat de gebruiker in zijn beeldvorming heeft en ook niet met voorstellingsvermogen kan bevatten.

2.3 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.

https://www.dalton.nl/literatuur/item/252-de-automatiseringsparadox https://www.debicker.eu/de-automatiseringsparadox/ https://vse.nl/de-paradox-van-de-industriele-automatisering/ https://automatie-pma.com/nieuws/industriele-automatiseringsparadox https://blog.xot.nl/2016/11/21/slimme-apparaten-maken-ons-dom-en-kwetsbaar/index.html

2.4 Wat is een model

2.4.1 Conceptueel model

Om duding te geven aan het grote plaatsje

2.4.2 in vivo model

Levende organismendie in de werkelijkheid of in een laboriatrum vergelijkbare eigenschappen bezitten als bestaande fenomenen in de werkeljkheid. Deze objecten zijn vergelijkbaar met werkelijkobjecten en geven vergelijkbare resultaten

2.4.3 in vitro model

Een model dat dezelfde condities biedt buiten het onderzoeksobject om, maar is voldoende vergelijkbaar om vergelijkbare processen te simuleren. Zowel invivo als in vitro modellen zijn beperkt door de materialen die beschikbaar ijn voor onderzoek en de arbeidsomstandigheden waaronder ze worden gebruikt. Desondanks zijn het geen werkelijke natuurlijke modellen dus vvoor een onderzoek kan boedt het geen volledige uitsluitsel.

2.4.4 In silicio model

Ee veelzijdig object. Het verwijst naar simulaties die gebruik maken van wiskundige modellen in computer,een zijn dus afhankelijk van silicone chips. In silico model analyseert wiskundige vergelijkingen om resultaten te geven onder bepaalde omstandigheden. Deze vergelijkingen vertellen iets over de correlatie van verschillende objecten van een wetenschappelijk onderzoek. OM deze modellen te kunnen gebruiken is het noodzakelijk te omschrijven waat de fenomenen in kwestie van onderzoek zijn door middel van getallen. Kwanttitatieve relaties kunnen worden geintegreerd in het model en waar deze relaties complex zijn is een computer noodzakelijk deze op telossen. Vaak worden hierbij verschillende mechanismen gebruikt. Als je bijvoorbeeld de prijsontwikkeling van een marsreep in kaart wilt brengen.

2.4.5 in simulacra model

2.5 World and machine samenvatting

Waarom zijn wij engineers? Omdat we bruikbare apparaten willen laten functioneren in de wereld waarin we leven. Dat doen we door de machine te beschrijven en deze beschrijving van instructies bieden we aan onze computer opdat deze als de attribuut en gedragingen uitleest zoals wij die hebben omschreven. Dit alles op basis van theoretische funderingen en praktisch inzicht.

Het doel van een machine is om te worden geinstalleerd en te worden gebruikt. De eisen die we stellen zitten in de omgeving en in de wereld en de machine is slechts de oplossing die we bedenken om aan een eis te voldoen.

De relatie machine-wereld world gecategoriseerd in:

Het modelleer aspect: waar een machine de wereld simuleert

Het interface aspect: waar er fysieke interactie is tussen de machine en de wereld

Het engineering aspect: waar de machine zich gedraagt als een controlemotor gebruikmakend van de gedragingen van de omgeving in de wereld

Het probleem aspect: waar de omgeving in de wereld en de omvang van het probleem invloed heeft op de machine en de oplossing

Het modelleer of simulatie aspect over een deel van de wereld. Er zijn data,object en proces modellen. Het doel van een model is toegang te geven tot informatie over die wereld. Door het opvangen van statische weergaven en gebeurtenissen kunnen wij deze gebruiken van opgeslagen informatie die we kunnen hergebruiken. Een model kan bruikbare informatie bevatten omdat zowel het model als de wereld warin het model zich bevind gemeenschappelijke omschrijvingen hebben die waar

zijn voor zwel het model als voor de wereld. Daarbij moet gesteld worden dat de interpretatie van een model verschilt met een interpretatie van de wereld.

Omdat zowel de wereld als de machine fysieke realiteiten zijn an niet slechts abstracties, zijn de gemeenschappelijke beschrijvingen slechts een deel van de werkelijheid van beide objecten. For elk object zijn er meerdere beschrijvingen. Toch maken niet alle omschrijvingen deel uit van het getoonde reportoire. Zoals niet alle eigenschappen van een boek; meer dan een auteur, pseudoniemen, een onderdeel van een reeks, een gerevisiteerde versie, worden gereflecteerd in een database.

Het interface aspect. Een machine kan een probleem in de wereld oplossen als de wereld en de machine phenomena kunnen uitwisselen. Maar de participatie is niet symmetrisch: een status kan als phenomena worden uitgewisseld maar slechts een partij kan er invloed op uitoefenen maar beiden kunnen dezelfde status signaleren.

Het engineering aspect gaat over requirements, specificaties, en programma's. Requirements hebben betrekking op phenomena in de wereld. Een programma heeft alleen betrekking tot de machinale phenomena. Het doel van programma's is om eigenschappen en gedragingen te omschrijven van de machine ten behoeve van de gebruiker. Tussen de requirements en de programma's zitten de specificaties. Omdat programma's dan wel beschrijvingen zijn van een gewenste machine, maar dat moeten beschrijvingen zijn van de machines die de computers kunnen uitvoeren zodanig dat de computer deze beschrijvingen ook zo kan interpreteren. De engineer moet de eigenschappen van de wereld kennen en begrijpen en deze eigenschappen manipuleren en laten werken met als doel het dienen van het systeem.

Het probleem aspect. Het onderscheid tussen specificatie en implementatie. Het probleem zit in de relatie van de machine en de wereld. De machine brengt de oplossing maar het probleem zit in de wereld. Een vertoog over een probleem moet dus gaan over de wereld en over de opvatting die de gebruiker heeft in de wereld. Omdat de wereld veelzijdig is moeten we ervan uit gaan dat er verschillende soorten problemen zijn. Een realistisch probleem wordt dus niet opgelost met een simpele hiërarchische structurele aanpak en een homogene decompositie maar met een paralleele structurele oplossing waar beide kanten van het probleem worden opgelost.

Ontkenningen

We hebben als engineers de taak om een machine te bouwen aan de hand van de specificaties opgeleverd door de opdrachtgever. Een engineer heeft niet als taak de fitheid voor een doeleind te onderzoeken, maar wel de haalbaarheid naar een doeleind aan de hand van kennis, tijd, resources, budget en ontwikkelmethodiek. Daaruit komt naar voren dat een engineer zich richt op: elicitation (schetsen van een requirement), description (omschrijving) en analyse van de requirements waaraan het systeem moet voldoen. Vertaalt naar de volgende vragen: Wat is precies de klantwens? Wat is de precieze omschrijving van het probleem? Voor welke doelen wordt het systeem gebouwd? Welke functies moet het systeem hebben?

Denial by hacking: obsessief bezig zijn met een systeem omdat het de gebruiker veel macht geeft. Een uitgebreidheid van een systeem zorgt er soms voor dat mensen niet meer geprikkeld zijn na te denken over probleemstellingen, domein beschrijvingen en analyse.

Denial by a abstraction. Wiskundige benaderingen van werkelijke problemen is

een belangrijke intellectuele strategie om problemen te formuleren. Een software ontwikkelaar moet een probleem kunnen omschrijven in zo min mogelijk woorden, maar de complexiteit ligt in de oplossing.

Denial by vagueness. De vaagheid van een omschrijving is terug te vinden in:

Von Neumann's principe

Principe van reductionisme

Shanley principe

Montaingnes's principe

Von Neumand principe

Voor een vocabulair moet een grondslag zijn ontwikkeld waarmee gesproken kan worden over de wereld en de machine. Belangrijke phenomenen moeten geindtifieerd worden, door middel van een grondregel of 'herkenningsregel' moet een fenomeen worden herkend, en vervolgens het fenomeen een formele term geven die gebruikt wordt als duiding van een bepaalde omschrijving. Dan moet voor de formele term een symbool gevonden worden. Samen vormen de grondregel en het symbool een designatie.

Principe van reductionisme

Simpelweg het openbreken van termen met een weerlegbare definitie totdat alle begrippen die worden gebruikt om iets te duiden niet meer te herconstrueren zijn in hun definitie.

Shanley principe

Er bestaan volgens dit principe geen scherpe verdelingen in de wereld zoals wetenschappers soms denken. Een strenge opvatting over de wereld waarin een individu geclassificeerd kan worden als een onsamenhangend geheel. Maar dat is slechts een opname van een beeld. De werkelijkheid staat soms toe dat een elementair individueel object in verschillende classificaties verschillende getypeerd kan worden in een andere setting of view.

Montaignes principe

De incative mood; gaat over wat we beweren waar te zijn.

De optitative mood; gaat over wat we willen dat waar is

2.6 SIX Variable 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 natreven vande 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.

Het verschil tussen essentie en incarnatie van een systeem. Een essentie bevestigd de mogelijkheden dat een systeem moet hebben om te voldoen aan de eise, ongeacht hoe het systeem is geimlementeerd. De incarnatie bevestigd of omvat de mogelijjkheden die te maken hebben met details omtrent implementatie. Een heuristiek voor het identificeren van de essentie van een systeem is de aanname van perfecte technologie, ofwel de aanname dat de technologie binnen een systeem perfect is. Om essentie te indentificeren nemen we aan dat technologie buiten de machine om perfect is. Zouden we incarnatie overwegen dan wordt de aanname van perfecte machin-externe technologie opgeheven.

Voor de documentatie van contextuele beslissingen en opties/alternatieven wordt de OVM (Orthogonale variability Model) gebruikt. Oorspronkelik was deze methode bedoeld om de variatiepunten en de variant van een productlijn samen met hun variabele afhankelijkheden(mandatory, optional, alternative) en beperkende afhankelijkheden(requires en excludes)te omvatten. De variant kan worden gerelateerd aan een ontwikkelartefact zoals een requirement of een diagram als een zogenoemde artefact dependency. Een artefact is dan gedefinieerd als variabele. Voor de documentatie van de keuzen die we maken is een selectie model gemaakt. We gebruiken het OVM voor de documentatie van contextuele beslissingen die moeten worden genomen, opties en alternatieven die selecteerbaar zijn, en de afhankelijkheden tussen hen. met behulp van de artefact dependency relateren we de alternatieven aan variabele elementen van de AND/OR graaf. Voor documentatie van de keuzes gebruiken we ook een selectiemodel. De kracht van het OVM model en de voornaamste reden deze methode te gebruiken is dat deze is in staat is om een variant te relateren aan een geheel model, een model element, of een selectie van een model.

AND/OR graaf wordt gebruikt voor de documentatie van refinement/decompositie of requirements. De AND/OR graaf is een directe, asyclische graaf met nodes knopen die requirements voorstellen en lijnen die AND-decomposities voorstellen en OR-decompositiestussen de requirements. Een decompositie van een requirement in een set van subrequirements R1,....Rn is een OR-decompositie iff die dusdanig aan een subrequirement voldoet en daarmee voldoet aan requirement R. Wat moet worden gedocumenteerd met betrekkig tot de AND/OR graaf is de abeargumentering waarom elkeAND/OR-decomopositie voldoende is.

2.6.1 Conceptueel model

System requirement: uitspraak over wereld fenomenen (gedeeld of niet) of doelen die bereikt moeten worden. met enige regelmaat informeel, niet precies geformuleerd. Software requirement/speci

catie: uitspraak over gedeelde fenomenen of doelen die de machine moet bereiken middels de onderdelen waar die machine uit bestaat of middels de fenomenen

waar de machine controle over heeft. doorgaans preciezer, meetbaar, exact 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.) Software: Kan niet direct communiceren met de buitenwereld. Snapt derhalve niets van de buitenwereld. Kan alleen maar bestaan in en communiceren met het systeem.

2.7 Requirementsengineering

scannen64-75

challenges in requirements engineering why goals-oriented for requirements engineering design and build of collaborative information agents treating nfiras first gradefor its testability software requirements negotiation a theory ui based spiral approach the worlds a stage: a survey on requirementsengineering using a real life case study from inconsistencyhandling to non-conanical requirements management: a logical perspective managing inconsistent specification: reasoning, analysis, action representingand using nonfunctional requirements: a process-oriented approach Four dark corners of requirements engineering classification of research methods in requirements engineering agent-basedtactocs for goal-oriented requirements elaboration

challenges in requirements engineering deceding exactly what to buildand documenting the results misidentofication of requirements as a problem Biggest software problem: -incomplete requirement and specification -cganging requirements and specification -large complex sofwtare systems Analyzing change inbussiness/operational environment and managing fluctuaing and conflicting equirements. cycle: need identification and problem analysis requirement determination requirement specification requirement fulfilllment More problems: why goals-oriented for requirements engineering

scann 0087 design and build ofcollaborative information agents A laguage to specify functional requirements and scenatio's for sysems of informations agents A language to specify design descriptions treating nfiras first gradefor its testability

scan 0089 software requirements negotiation a theory ui based spiral approach problem of detailed concers ofusers, non-users and interfaces n evolutionaru development ceoncept of operational 1) win-conditions-capturing the desired objective of the individual 2) conflict/risk/uncertainty specs capturing the conflicts between win conditions and their associated rest and uncertainties 3) points of agreement capturing the agreed upon set of condictions which satisfy stakeholders win conditions and also define the system objectives WinWin0 concept of operation in initial fase WinWin1 -) decommitment frm previously relevant POA -) exploring options, such as reusing components reducing negationed software functionaliry on deferring lower priority capabilities -) understanding notifications of options, choices and filtering options that are noncompatible with stakeholder critical conditions -) handling the ripple effects of changes introduced to resolve the conflict -) bounding and focussing the domain of discourse with respect to negotiated sys-

tems 3.2 confrontational win-conditions-capturing incomplete set of options weak association between new CRU and new conflict resolving win-conditions-capturing uncontrolled search for alternatives 4.3 potential conflicts 1) interactions due to node mismatch 2) complexity of interactions 4.4 renegotioation support tradeoff by COCOMO-tool node-based re-negotianions support for cost/schedule/functionality, performance tradeoff analysis

use cases decribe the possible system interactions that eexternal agenets may have with a system

identification of goals to be acheved by the envisioned system. The operational character of such goals are services and constraints assignment of responsibilities of resulting requirements to agenets as humans, devices and software 1) elicitation 2) goal modeling 3) goal generalization 4) mapping goals into sotware objects, events and operations the worlds a stage: a survey on requirementsengineering using a real life case study viuwepoints, social aspects,evolution, non-functional requirements, conflict resolution, traceability

Goal of this paper is requirement engineering on London aulance service Method of opinions: crew, staff, management, computational, transport, services Evolutioon: changes, specification and technology trade Environment: company policies, regulation, impact solution on organizational Non-functional aspect: communicatio problem, malfunctions, less critical isues: cost, tradeoff beween performance user interfaces vieuwpoint: is a subset of all system requirements expressible in a given requirements notation regardless of the stakeholders involved

log change basic model vieuw hypertext vieuw data transmission problems continued difficulties installation problems problems caused by mistake tracebility requirements[selecting reliable information] PRE requirement specification traceability, repository baed approach 1) compromise specification 2) representatives 3) agreement dimensions Domain: part of the worl in which the computer system effects will be felt, inclusing its peoples, organizational structure, related legislation, physical location and met only the compyter systems

Functional vs quality requiements How to determine quality characteristiec in specific situation What different stakeholders are involved in different ways in particular bussiness processes strategies: testing, comparing, analysis, trial and error uncertainties: bussiness processes, information technology used, knowledge of various types of usrs, knowledge of various types of developers invoved

Communication between stakeholders p[geographic and temporal distance] goals describe the macro-level o requremens scenarios are used to describe the medium level of requirements vieuwpoints describe the microlelvel of requirements functional concerns: primary bussiness goal non-functional concern: security, performance, compatibility refers to gravity of functional concern cognition mappings used for: simulation organisational strategies modeling support for strategic problems formulation and decisio analysis modeling of social psychologycal processes knowledge based construction manageral problem construction failure nodes effect analysis modeling virtual worlds and analysis of their behaviour requirements analysis system requirement specification

from inconsistencyhandling to non-conanical requirements management: a logical perspective

1) identifying non-canonicalrequirements 2) measuring them 3) generate caandidate proposals for handling them 4) choosing acccptable probosals 5) revising them acccording to the proposals model phases using: paraconsistent reasoning, non-monotnic reasoning

Requirement U scenarion -¿ Scenarion E

managing inconsistent specification: reasoning, analysis, action classic logic quasi-classical logic ¿¿ inconsistency implies action

specification information ¿¿ natural language deduction rules method information ¿¿ reduction ad absurdum domain interpretation

background: users, customers, domain experts, designers,, manufacturers graphical textual specification

Basic constraint, legal constraint, cooperation constraint 1) scenatio definition 2) scenario analysis 3) scenario consolidation

How can a system be further designed so that ne non-functional requirements mentioned will met? How does that design relate to further refinements of the functionaland structural aspectsof the system

block[objects, classes, methods, messages, inheritance] [goals,agents, alternative, events, actions,existence modalities,agent responsibilities] primitice terms structuring mechanism primitive operations genral intergrity rules

Softgoals are satisfied when there is a suffucienr positive and little negative eludence for this claim, and that they are usatisfiable when there issufficient negative evidence and little positive support for their satisfiability.

service computing 1)role 2) goal 3) process 4)service How to constrainand extendthe semantic interoperability n the process of self-organizationand action emergence for the distributing service resource? How to categorise the structure of nteroperability? Howto satisfy stakeholders requirements?

Connecting ontologies: 1) semantic distance 2) semantic interoperability masurement 3) semantic interoperability capability

1) event 2) entity 3) attribute 4) value 5)quantity 6) value 7) secondary feature 8)syntax 9) eventrole 10)eventfeatures

representingand using nonfunctional requirements: a process-oriented approach product oriented process oriented

Acquisition Performance user concern -How well does it function -hwo well does it utilize a source ¿¿ Efficiency -How secure is it ¿¿ integrity -What confidence can be placedand what it does ¿¿Reliability -How well does it perform underadverse conditions ¿¿ sustainability -How easy is it to use it ¿¿ usability quality attribute

Acquisition: Design user concern How valid is the design -how well does it conform to requirements -how easy is it to repair -ow easy is it to verify its performance quality attribute

Acquisition: Adaption user concern -how adaptable is it - how easy is it to exportand uprade its capability ¿¿ expendability - how easy is it to change ¿¿flexibility -how easy is it to infer with other system ¿¿ portability - how easy is it to transport ¿¿ interoperability how easy is it to convert for use with other application¿¿ reaseability quality attribute

3 Onderzoeksresultaten naar rampen

3.1 Inleiding

3.2 Systeemrampen

3.2.1 bijlmerramp

Motor 3 (de binnenste motor aan de rechtervleugel van het vliegtuig) brak af, beschadigde de vleugelkleppen en botste tegen motor 4 die vervolgens ook afbrak. De ernst van de situatie werd op Schiphol niet goed ingezien. Dit kwam onder meer doordat lost in de luchtvaart de gebruikelijke term is om het verlies van motorvermogen te melden. Op Schiphol werd er dan ook van uitgegaan dat er twee motoren waren uitgevallen. Dat ze letterlijk verloren waren wist men niet. Gezien het grote aantal handelingen dat de bemanning in een paar minuten moest uitvoeren en de keuzes die de piloot maakte, veronderstelde de parlementaire enquêtecommissie die de ramp later zou onderzoeken dat ook de bemanning waarschijnlijk niet heeft geweten dat beide motoren van de rechtervleugel waren afgebroken. De buitenste motor van een 747 is vanuit de cockpit slechts met moeite zichtbaar en de binnenste motor helemaal niet.

Op de avond van de 4e oktober 1992 was landingsbaan 06 (de Kaagbaan) in gebruik. De piloot verzocht de luchtverkeersleiding op Schiphol echter een noodlanding te mogen maken op de Buitenveldertbaan (baan 27). Waarom hij juist deze baan koos, is nooit duidelijk geworden. Een keuze voor deze baan lag niet voor de hand; omdat de wind uit het noordoosten kwam, zou het toestel met flinke staartwind moeten landen. Langs de landingsbaan waren enkele grote brandweerwagens van Schiphol geplaatst. Deze zogeheten crashtenders moesten een brand tijdens de landing meteen blussen. Na de crash werd één zwarte doos teruggevonden. De bijbehorende band was in vier stukken gebroken, waardoor de laatste 2 minuten en 45 seconden ervan niet meer te gebruiken waren. De doos werd voor onderzoek naar Washington gestuurd en leverde uiteindelijk onderstaande informatie op. Om goed uit te komen voor de landingsbaan vloog het beschadigde toestel eerst nog een rondje boven Amsterdam. Tijdens dit rondje gaf de gezagvoerder de copiloot opdracht de vleugelkleppen (flaps) uit te schuiven. Links schoven de kleppen uit, maar doordat de afgebroken motor 3 de rechtervleugel had beschadigd schoven de kleppen op die vleugel niet uit. Als gevolg hiervan kreeg het toestel links meer draagvermogen dan rechts. De piloot meldde aan de verkeersleiding dat er ook problemen met de flaps waren. Aanvankelijk ging het aanvliegen van de Buitenveldertbaan goed. Op het moment dat het vliegtuig daalde tot onder de 1500 voet en snelheid minderde, raakte het echter compleet onbestuurbaar en maakte het een ongecontroleerde, scherpe bocht naar rechts. Over de radio was te horen dat de gezagvoerder zijn copiloot in het Hebreeuws opdracht gaf om alle kleppen in te trekken en het landingsgestel uit te klappen. Vervolgens meldde de copiloot in het Engels aan de luchtverkeersleider dat het toestel zou gaan neerstorten. Uit later onderzoek bleek dat het vliegtuig eerder enkel recht bleef vanwege de hoge snelheid (280 knopen, zijnde 519 km/u). 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.

https://aviation-safety.net/database/record.php?id=19921004-2lang=nl

3.2.2 vuurwerkramp in enschede

https://www.enschede.nl/inhoud/commissie-oosting https://www.politie.nl/binaries/content/assets/politie/wob/00
landelijk/vuurwerkramp-enschede/bijlagen-rapport-vuurwerkramp-enschede.pdf https://www.researchgate.net/publi

3.2.3 ramp turkisch airlines

Inadequaat handelen van de piloten ondanks een defecte hoogtemeter en onvolledige instructies van de luchtverkeersleiding/ https://catsr.vse.gmu.edu/SYST460/TA1951$_{A}ccidentReport.pdf$

Wat ging er allemaal mis bij de bovengenoemde rampen en ongelukken.....

Wat hebben deze rampten te maken met de requirements en specificaties van deze odpracht?

3.2.4 tjernobyl

Een ramp bij een kernreacor in de sovjetunie. Door een bedieningsfout in een testprocedure werd het vermogen van de koelinstallaties negatief beinvloed. 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 eksplosie tot gevolg. https://www-pub.iaea.org/MTCD/publications/PDF/Pub913e$_{w}eb.pdf$

3.2.5 therac-25

Softwarefout uit zich als hardwarefout de klachtafhandeling geen onderzoek geen second opinion is prioriteit wel gechecked na onderzoek bellen en geen prioriteit aanwezig te zijn alleen importeurs en fabriken mogen fouten in frabrieksinstellingen rapporteren Therac25 Systeem ligt plat veel voorkomende eror stdaardafhandeling om de error te verwerpen resultaat: de patient kreeg overdosis patient overleden onderzoek opgestart, stuatie niet reproduceerbar foutmarkering: gezien als uitzonderlijk, software aanpassing van groote magnitude 5; de oorzaak was waarschijlijk mechanisch maar neit vastgesteld; conceptueel odel niet aangepast probleemclassificatie door autorititen het probleem en de impact daarvan anar beneden bijgesteld AEFL doe gedeeltelijke aanpassing om hardware na berisping Canadese autoriteit Derde patient overleden door eythema AECL wijst alle doodsoorzaken af AECL beweert dat geen vergeli- jkbare voorvalle bij andere machines of patienten zijn voorgekomen geen vervolgonderzoek vanwege garanties bedrijf gaat uit van geen mogelijke functionele fout vierde patient overleden aan overdodis ontstaan door bug in software onjuiste aanduiding bij de foutmelding verkeerde reactie/invoer ddoor operator communicatie tussen patient en operator werd onvoldoende gemon- itorred (apparatuur niet aangesloten, en audio monitor kapot) engineer van AECL stelt geen fouten vast Engineer AECl kan fout niet reproduceren Geen communicate

tussen bedrijf en uitgezonden technisci over vergelijkbare probleemgevallen vijfde geval malfunction 54 leidt tot overdosis en de dood fout gereproduceerd door operator bedrijf fout was daa entryspeed herpublicatie van de ongevallen en de eerdere ongevallen in de meia apparaat wel nog in gebruik genomen niet handig, waarschuwingsberichten en aanwijzingen voor een bugfix naar de gebruikers door druk van fda is bedrijf op zoek gegaan naar permanente oplossing zesde geval software fout door softwarefout otntstaat lightstruct .. op de patient na onderzoek door AECL blijkt niet alleen hardware de oorzak gebruikers direct geinformeerd oplossing gevonden, media ingeschakeld om

transparantie af te dwingen door de gebruikersgroep en de FDA AECL gedwongen functionaliteit aan te passen Engineers hebben meer studie moeten maken van gebruikte technologie en onderhoudbaarheid daarvan

3.2.6 tesla crash report

Door een softwarefout zijn er situaties ontstaan waarin het systeem informatie een onvoldoende informatie positie had om de juiste beslissingen te maken. Of dat de informatieverwerking niet juist was.

3.2.7 stint ongeluk

Vier kinderen, een bestuurder kwamen om en een vijfde persoon , een kind raakte zwaargewond. Uit odnerzoek van bleek : Foute torsieveer voor de gashendel werd geleverd Geen van de drie onderzochte voertuigen haalden de wettelijk vereiste remvertraging De automatische parkeerrem kan leiden tot gevaarlijke situaties wanneer deze ongewenst geactiveerd wordt tijdens het rijden. Het losraken van de nuldraad naar de gashendel leidt volgens TNO tot ongewenst versnellen van het voertuig en een oncontroleerbare situatie voor de bestuurder. Voor alle drie onderzochte voertuigen geldt dat het ontbreken van een zitplaats leidt tot veiligheidsrisico's voor remmen en sturen door de grotere kans dat de bestuurder van het voertuig valt. Als de bestuurder van een Stint valt, leidt dit in alle rijsituaties tot een onbeheersbare situatie

https://repository.tno.nl/islandora/object/uuid

3.2.8 slmramp

Toen 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.

Uit onderzoek bleek dat de papieren van de bemanning niet in orde waren. 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.

https://aviation-safety.net/investigation/cvr/transcripts/cvr$_{p}y764.phphttps://aviation-safety.net/database/record.php?id = 19890607 - 2$

3.2.9 schipholbrand

Om een goed verhaal op te stellen, moet vooraf aan enkele voorwaarden worden voldaan. De eerste voorwaarde is de geschiktheid van het afstudeerproject. Als een afstudeerproject niet tot keuzes leidt, kan men zich afvragen of dat wel een echte afstudeeropdracht is. Een afstudeerproject zonder onderzoeksaspecten is ook verdacht. Daarnaast moet een afstudeerproject passen in het profiel van een opleiding om beoordeelbaar te zijn. De andere voorwaarde voor goed een verhaal is de registratie van werkzaamheden tijdens het a

3.2.10 Ramp schietpartij militair ossendrecht

Een militaire overleid op een schietbaan in ossendracht door onvoldoende begeleiding van cursisten, geen toezicht op de lokatie. Eẘas een instructuur in opleiding die niet volledig was mmeegenomen in het poroces en ook was er geen baancommandant aanwezig. Geen van de aanwezig instructeurts had de juiste papieren om de cursisten te begeleiden. De aanwezig instructeur had geen zich op de instructeur in opleiding, evenmin de andere militairen. In de instructiehandleiding ontbreken richtlijnen voor bijzondere schietbanen. Ook was er geen keuring. Door personelstekort is er geen andacht besteed aan documentastie(een slyllabus) hoe en met welke risico's oefeningnen moeten worden ingericht. Ok werd er vooraf geen veiliheidsanaklyse gedaan. Het gebrek aan lesmateriaal en deskundigen is gemeld binnen de defensieorganisatie maar dit heeft niet geleid tot enige verandering in de situatie. Op een afgekeurde scheitbaan Tezicht door een instructeur in opleiding die zelf geen persoonlijke begeleiding heeft gehad tijdens de uitvoering Belangrijk is dat defensie haar taken kan uitvoeren met personeel dat is getraind in situaties die de risicos van de werkomgeving aan de cursisten kunnen laten zien. Conclusie Zonder gekwalificeerde instructuers. Zonder toezicht Zonder lesmateriaal Zonder adequate veiligheidsanalyse https://www.youtube.com/watch?v=6jmkDClGDHo

3.2.11 molukse treinkaping

https://www.youtube.com/watch?v=h99Fe9XzzHI

3.2.12 explosie tanjin china

Later bleek uit een onderzoek van de Chinese autoriteiten dat de explosie overeenkwam met de ontploffing van 450 ton TNT.[6] De oorzaak van de explosie lag in de spontane zelfontbranding van 207 ton cellulosenitraat dat in containers was opgeslagen op het terminalterrein.[6] Verder lag op een tweede locatie nog eens 26 ton van dit explosieve materiaal opgeslagen. De tweede ontploffing werd versterkt door de

opslag van 800 ton kunstmest in de vorm van ammoniumnitraat in de nabijheid.[6] De opslag van cellulosenitraat is aan strenge regels gebonden. Het moet koel en droog worden opgeslagen. De containers stonden buiten opgesteld in de brandende zon. De temperatuur liep op tot 36 °C en bereikte binnen de containers waarschijnlijk de 65 °C.[6] De verpakking van de cellulosenitraat droogde uit waardoor de ontploffing kon ontstaan. Op het terrein lagen meer gevaarlijke stoffen opgeslagen dan waarvoor vergunningen waren verstrekt.[6] Dit leidde tot een kettingreactie met grote schade tot gevolg. Door de brand en bluswater is in de directe omgeving veel milieuschade opgetreden.

https://www.hindawi.com/journals/joph/2019/1360805/

3.2.13 explosie in libabon, beirut

Op 23 september 2013 voer het vrachtschip de Rhosus onder Moldavische vlag[7] van Batoemi in Georgië naar Beira in Mozambique met 2.750 ton ammoniumnitraat

Gezien het ernstige gevaar van het bewaren van deze goederen in de hangar onder ongeschikte klimatologische omstandigheden, herhalen we ons verzoek aan de marine-instantie om deze goederen onmiddellijk weer te exporteren om de veiligheid van de haven en de mensen die er werken te verzekeren, of om akkoord te gaan om ze te verkopen. Voorafgaand aan de explosie was er een brand in een opslagplaats.

https://www.hrw.org/report/2021/08/03/they-killed-us-inside/investigation-august-4-beirut-blast https://www.researchgate.net/publication/348325979$_{B}eirut_{E}xplosion_{t}he_{f}ull_{s}toryhttps$: $//reliefweb.int/sites/reliefweb.int/files/resources/CaseStudy_{B}eirutExplosion_{T}echBioHazardsweb.pdf$

3.2.14 ethiopian airlines

Ethiopian Airlines Flight 302 Door problemen met de flight control One minute into the flight, the first officer, acting on the instructions of the captain, reported a "flight control"problem to the control tower. Two minutes into the flight, the plane's MCAS system activated, pitching the plane into a dive toward the ground. The pilots struggled to control it and managed to prevent the nose from diving further, but the plane continued to lose altitude. The MCAS then activated again, dropping the nose even further down. The pilots then flipped a pair of switches to disable the electrical trim tab system, which also disabled the MCAS software. However, in shutting off the electrical trim system, they also shut off their ability to trim the stabilizer into a neutral position with the electrical switch located on their yokes. The only other possible way to move the stabilizer would be by cranking the wheel by hand, but because the stabilizer was located opposite to the elevator, strong aerodynamic forces were pushing on it. As the pilots had inadvertently left the engines on full takeoff power, which caused the plane to accelerate at high speed, there was further pressure on the stabilizer. The pilots' attempts to manually crank the stabilizer back into position failed. Three minutes into the flight, with the aircraft continuing to lose altitude and accelerating beyond its safety limits, the captain instructed the first officer to request permission from air traffic control to return to the airport. Permission was granted, and the air traffic controllers diverted other approaching flights. Following instructions from air traffic control, they turned

the aircraft to the east, and it rolled to the right. The right wing came to point down as the turn steepened. At 8:43, having struggled to keep the plane's nose from diving further by manually pulling the yoke, the captain asked the first officer to help him, and turned the electrical trim tab system back on in the hope that it would allow him to put the stabilizer back into neutral trim. However, in turning the trim system back on, he also reactivated the MCAS system, which pushed the nose further down. The captain and first officer attempted to raise the nose by manually pulling their yokes, but the aircraft continued to plunge toward the ground.

https://www.hindawi.com/journals/ijae/2014/472395/

3.2.15 ethiek

Ethiek

persuasive technology https://www.humanetech.com/youth/persuasive-technology https://www.minddistrict.com/blog/persuasive-technology-new-insights-in-behavioural-change https://www.sciencedirect.com/book/9781558606432/persuasive-technology https://spectrum.ieee.org/how-persuasive-technology-can-change-your-habits https://www.frontiersin.org/articles/1 https://psmag.com/environment/captology-fogg-invisible-manipulative-power-persuasive-technology-81301 https://www.makeuseof.com/what-is-persuasive-technology/ https://lib.ugent.be/catalog/rug01: https://cyberpsychology.eu/article/view/12270

3.2.16 ecourt in nederlandse rechtspraak

niet odnerzocht https://www.njb.nl/blogs/a-court-with-no-face-and-no-place/ http://www.e-court.nl/wp-content/uploads/2018/03/Procesreglement-e-Court-2017$_2$0180201.pdf

3.2.17 cyber aanval op Oekraïene

Om een goed verhaal op te stellen, moet vooraf aan enkele voorwaarden worden voldaan. De eerste voorwaarde is de geschiktheid van het afstudeerproject. Als een afstudeerproject niet tot keuzes leidt, kan men zich afvragen of dat wel een echte afstudeeropdracht is. Een afstudeerproject zonder onderzoeksaspecten is ook verdacht. Daarnaast moet een afstudeerproject passen in het profiel van een opleiding om beoordeelbaar te zijn. De andere voorwaarde voor goed een verhaal is de registratie van werkzaamheden tijdens het a op 23,december 2015 vind er een cyber aanval plaats op het elektriciteitsnet van de Oekraine. Dit was de eerste bekende aanval op een elektrisch contole system. Dit verslag geeft inzage in een analyse van de Ukraine cyber aanval, inclusief hoe de actoren zich zelf toegang gavan tot het controle systeem, welke methoden de acoren hebben gebruikt voor reconnaissance en vastleggen van het systeem, een gedetailleerde omshrijving van de aanval op 15 December 2015, en de methoden die gebruikt zijn door de aanvallers om hun sporen uit te wissen en daarmee het het stoppen van schade toebrengen nog moeilker maken. Daarnaast wordter een gedetailleerde omschrijving gevevenv an de beveiliging van de SCADA ccontrol systemen gebaeerd op bst practices, inclusief het control network ontwerp, technieken voor whtelisting, monitoring en loggen, en opleiding van personeel. [2]

[?] [1]

3.2.18 Mali

Een granaat explodeerd in een mortier De medische zorg na het ongeval was neit voldoende

De algemeen militair verpleegkundige gaf aan het slachtoffer nar het vn-hospitaal in kidal te brengen De chaauffeur van de bushmaster kende de locatie niet en bracht het slachtoffer naar een door frane militairren bemand hospitaal mmet minder mediswche faciliteiten Hierna alsnog overgebracht naar het vn-hospitaal. Dit verlieop neit door nederlandse maatstaven. pas toen een nederlandse arts arrivveerde werd door de Tongolese artsen een buikoperatie uitgevoerd. Dit gebrurde zonder adequate anesthesie. Na de operatie werde de gewonde militair overgelogen naar nederland. En later naar nederland.

granaat stond niet op scherp en in afgegaan in veilige stand Granaat werd opgeslagen in neit gekoelde containers waardoor deze aan te hoge temeperaturen zijn blootgesteld. Door de comvinatie van vocht en warmte in de granaat zeer gevoelige explosieve stoffen werden gevormd. Tijdens de oefening was de fatale granaat in de zon. Het afsluitplaatje in de granaat bleek niet in staat om doorslag in veilige stand te voorkomen waarna de granaat explodeerde. De moritren zijn aangeschaft bij de amerikanen. gredurende de aanschafperiode zijn procedures en controles op kwaliteit en veiligheid deels nagelaten. Dit veiligheidsgarantie werd vermeld in het koopcontract. Conclusie Koopcontract werd niet goed doorgelezen Geen controle op kwaliteit en veiligheid Geen controle op kwaliteit en veiligheid Zwakke plekken in het ontwerp Geen controle op kwaliteit en veiligheid 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 Ok 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.

https://www.youtube.com/watch?v=PC2ekl4SaNA

3.3 Analyse

3.4 Conclusie

4 Deelonderzoeken

4.0.1 Research case Oekraiene

4.0.2 Deelonerzoek naar veiligheidsrisico's voor sluizen

4.0.3 Wet en regelgeving voor sluizen

4.0.4 Ondeerzoeksresultaten naar sluisbeveiliging

Verouderde computersystemen zijn door de jaren heen gekoppeld aan netwerken, zodat ze op afstand te besturen zijn. Dit zorgt ervoor dat systemen kwetsbaar zijn voor aanvallen van buitenaf. De beveiliging is in de loop der jaren niet voldoende ontwikkeld om de infrastructuur goed te beveiligen.

Volgens het onderzoek is er de afgelopen jaren wel het nodige geïnvesteerd om de beveiliging op te schroeven, maar deze maatregelen zijn nog onvoldoende doorgevoerd. https://www.nu.nl/internet/5814282/rekenkamer-waterwerken-niet-goed-beveiligd-tegen-cyberaanvallen.html rapport Digitale dijkverzwaring: cybersecurity en vitale waterwerken Crisisdocumentatie is verouderd en er worden geen volwaardige pentesten uitgevoerd. Uit het onderzoek blijkt dat nog niet alle vitale waterwerken rechtstreeks zijn aangesloten op het Security Operations Center (SOC) van Rijkswaterstaat. Hierdoor bestaat het risico dat RWS een cyberaanval niet of te laat detecteert. De minister van Infrastructuur en Waterstaat moet nog stappen zetten om aan de eigen doelstellingen voor cybersecurity te voldoen De Algemene Rekenkamer beveelt de minister van Infrastructuur en Waterstaat ook aan om het actuele dreigingsniveau te onderzoeken en te besluiten of extra mensen en middelen nodig zijn. Ook is het voor een snelle en adequate reactie op een crisissituatie van essentieel belang dat informatie up-to-date is. Pentesten zouden integraal onderdeel uit moeten maken van de cybersecuritymaatregelen bij vitale waterwerken. Verder zou moeten worden bezien of medewerkers van het SOC beter moeten worden gescreend. https://www.rekenkamer.nl/publicaties/rapporten/2019/03/28/digitale-dijkverzwaring-cybersecurity-en-vitale-waterwerken Sluis Eefde kreeg niet alleen de onderhoudsbeurt, maar werd tevens uitgebreid met een tweede sluiskolk. Zo wil Rijkswaterstaat wachttijden voor de scheepvaart voorko https://www.gww-bouw.nl/artikel/de-eerste-sluis-met-kantelende-sluisdeur/

Om de lokale bemanning, die de oren en ogen waren van de sluizen, te vervangen waren camera's, communicatielijnen en software nodig. Hoge kwaliteit videobeelden, met echte kleuren en zonder enige vertraging zijn belangrijk voor de operators en zij moeten hierop kunnen vertrouwen. Er zijn verschillende testen gedaan met diverse camera's en cameraposities om kleurechtheid te kunnen bieden onder alle omstandigheden. Het resultaat was een perfecte kleur op alle 70+ camera's op iedere locatie.

Vertraging van videobeelden was een cruciale factor in dit project. Het is uiterst belangrijk dat de operator op zijn beeld ziet wat er daadwerkelijk op locatie gebeurt, zonder enige vertraging. Om te laten zien of er eventuele vertraging is, is er een speciale functie gecreëerd. Deze functie laat een rood kruis zien op het scherm wanneer de vertraging meer is dan 500 miliseconden. Zo ziet de operator direct of

het beeld wat hij ziet actueel is.

Een andere functie die voor dit project is gecreëerd, is bij de videobeelden aan te geven van welke kant van de sluis het camerabeeld is. Voor de operators is het belangrijk dat ze weten vanaf welke kant het vaartuig komt en waar deze naartoe vaart. Een simpele oplossing was om een blauw kader te maken om het videobeeld van de ene kant van de sluis en geen kader om het videobeeld van de andere kant.

https://tkhsecurity.com/nl/waterwerken/

Het crisismodel kan beter, is de derde deelconclusie van de Algemene Rekenkamer. Er is geen specifiek scenario voor een crisis die wordt veroorzaakt door een cyberaanval. Ook ontbreekt inzicht in de effecten van een cybercrisis op andere sectoren, de zogeheten cascade-effecten. Tevens is de crisisdocumentatie op onderdelen verouderd. https://www.h2owaternetwerk.nl/h2o-actueel/rekenkamer-vitale-waterwerken-nog-onvoldoende-beschermd-tegen-cyberaanvallen

Ook maakt cyberveiligheid nog geen volwaardig onderdeel uit van reguliere inspecties.' De Rekenkamer hamert erop dat alle vitale waterinfrastructuur zo snel mogelijk op het SOC wordt aangesloten. Ook zouden werknemers van Rijkswaterstaat die belangrijke waterkeringen bedienen beter gescreend moeten worden op hun antecedenten. Sollicitanten hoeven nu slechts een Verklaring Omtrent Gedrag te overleggen, maar dat is een heel lichte toets. https://www.volkskrant.nl/nieuws-achtergrond/hacker-dringt-door-in-controlekamer-waterwerk-cyberterrorist-kan-ons-land-onder-water-zetten b6fcbc3c/?referrer=https

deltawerken https://www.magazinesrijkswaterstaat.nl/bereikbaarzeeland/2021/01/krammersluizencomplex-verleden-heden-en-toekomst

Volgens Rijkswaterstaat is het kostbaar en technisch uitdagend om klassieke automatiseringssystemen te moderniseren en wordt er daarom vooral ingezet op detectie van aanvallen en een adequate reactie daarop. Uit het onderzoek blijkt dat Rijkswaterstaat de afgelopen jaren zelf van alle tunnels, bruggen, sluizen et cetera heeft vastgesteld welke cyberveiligheidsmaatregelen moeten worden genomen. Een groot deel van die maatregelen (ongeveer 60De minister heeft een aantal waterwerken die Rijkswaterstaat beheert als vitaal aangewezen. . Uit het onderzoek blijkt dat nog niet alle vitale waterwerken rechtstreeks zijn aangesloten op het Security Operations Center (SOC) van Rijkswaterstaat. De ambitie om eind 2017 bij alle vitale waterwerken cyberaanvallen direct te kunnen detecteren was in het najaar van 2018 daarmee nog niet gerealiseerd. Hierdoor bestaat het risico dat RWS een cyberaanval niet of te laat detecteert. https://www.watersport-tv.nl/nw-31400-7-3715235/nieuws/cybersecurity$_vitale_waterwerken_niet_waterdicht.html$

Over de cyberbeveiliging van gemeenten en waterschappen wordt al langer geklaagd. Zo meldde EenVandaag al in 2012 dat rioolgemalen en sluizen gemakkelijk van afstand te bedienen waren, onder meer door bijzonder slechte wachtwoorden. https://www.rtlnieuws.nl/nieuws/nederland/artikel/3758966/cyberbeveiliging-waterschappen-hapert-sluizen-kunnen-worden

Rittal doet onderzoek naarop afstand besdienbare sluizen https://expert.rittal.nl/wp-content/uploads/2017/05/Referentieverhaal-Provincie-Zuid-Holland.pdf

Beveiligde VPN

M2M Services levert aan inmiddels 220 gemeenten en waterschappen beveiligde connectiviteitsoplossingen voor het beheer van pompen, riolen en gemalen. Om ri-

sico's op beveiligingsincidenten te voorkomen maken wij gebruik van een VPN oplossing, waarbij de verbinding optimaal beveiligd is middels encryptie en authenticatie. https://www.vtmgroep.nl/blog/waterwerken-in-nederland-onvoldoende-beveiligd-tegen-cyberaanvallen

Veiligheid op het water én op het land Gebruik van lampbewaking http://www.wesemann.nl/nl/nieuws-en-pers/274-veiligheid-op-het-water-en-op-het-land.html

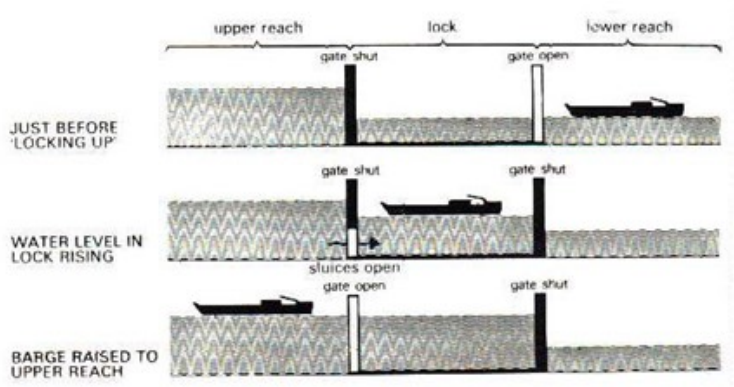
5 Modelontwikkeling en keuzen in Uppaal

Uppaal source

6 Requirements

6.1 Inleiding

Om voor mezelf een beeld te krijgen van wat een sluis is en hoe deze moet werken is er een aantal foto's verzameld van sluizen.



Uit deze afbeelding blijkt het volgende: Hoogteverschip t.o.v NAP 2 sluisdeuren stoplichten Uit een onderzoek naar de werking van de verschillende sluizen in nederland wordt rekening gehouden met de aanmelding van sluizen en de gebruiktstijd van sluizen.

Met de aanmelding van schepen wordt omschreven welke acties er door de schipper de sluismeeter moet worden gedaan om de positie, tijdstip en lengte van een invarendship te communiveren.

Met de gebruikstijd wordt de daadwerkelijke tijd aangeduid waarin het scheepsverkeer/waterverkeer gebruik kan maken van de sluis en onder welke voorwaarden zoals wachttijd, gewicht, terugvaarmogelijkheden etc).

6.2 Requirements

Directe requirements van opdrachtgever:
Na grondige analyse van het Nederlandse sluizenpark is gebleken dat renova-tie van een groot aantal sluizen noodzakelijk is. Een eerste verkenning heeft onsgeleerd dat het gecombineerd renoveren en automatiseren van het Nederlandsesluizenpark een aanzienlijke verbetering kan opleveren t.a.v.:
- veiligheid
- efficientie
- capaciteit
- onderhoudskosten
- duurzaamheid

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. Op het ministerie van infrastructuur en waterstaat is helaas onvoldoende kennis van ict en systemen aanwezig om eenen ander uit te voeren. Wij vragen u een model (of een onderling samenhangend aantal modellen)aan te leveren, opdat ontwerpen van verschillende, volledig geautomatiseerde sluizen in de toekomst gerealiseerd kunnen worden.

Eigen inbreng van deze requirements:
Wij gaan er van uit dat het volgende van ons verwacht wordt:
Maak een model dat als template dient gebruikt te worden voor het automatiseren van verschillende soorten sluizen. Verder moeten overwegingen gemaakt worden die goed onderbouwd zijn.

Aangezien er van ons alleen een model verwacht wordt, zullen wij ons geheel focussen op de fundamentele werking van de sluis en hierbij zullen wij ons dus niet bezig houden met fysieke eisen zoals veiligheidshekjes en borden. Onze focus ligt geheel op de werking van de sluis; elke state waar de sluis zich in mag bevinden en welke beslissingen de sluis moet maken op basis van bestaande protocols en benoemde eisen.

Deze requirements zullen hieronder uitgewerkt worden, per sluisonderdeel, deze bestaande uit de sluisdeuren, de sloplichten, de waterpomp en de boten.

6.3 Sluisdeuren en stoplichten

De sluisdeuren aan weerszijde van de sluis worden gebruikt om de toegang tot de sluiskolk mogelijk te maken en te bewaken in combinatie met de stoplicht.

6.4 Waterpomp

De waterpomp pompt water in de sluis of pompt water weg naar gelang de richting van het ingevaren schip.

6.5 Boten

De meeste sluizen die zich in Nederland bevinden zijn schutsluizen; deze sluizen zijn bedoeld om boten, zowel vrachtschepen als pleziervaart afhangend van de locatie van de sluis, te verwerken. Om deze reden gaan wij deze dus ook verwerken in ons model. Mocht een sluis niet bedoeld zijn om boten te verwerken, dan zou dit model alsnog toegepast kunnen worden opp desbetreffende sluis. Boten worden toegevoed aan de queue. Hoe dit gebeurt, dat ligt aan de specifieke sluis. Sinds wij een template maken, hoeven wij geen rekening te hounden met hoe de schepen in de queue komen. Het enige wat wij hoeven te doen, is de data verwerken.

6.6 Specificaties

Vanuit deze requiremenst kunnen verdere specificaties opgesteld worden.

Even ter duidelijkheid: een requirement beschrijft wat een programma moet doen, en een specificatie beschrijft hoe men van plan is om deze requirements te realiseren.// Voorbeeld:// Requirement is dat de sluis meerdere boten moet kunnen verwerken; de specificatie zou hier zijn fdat de sluis minstens twee keer zo groot moet zijn dan de grootste boot die door de sluis kan.

6.7 Requirements voor Het sluismodel

6.8 Requirements

Requirements zijn alleen die eisen die gesteld worden aan het gedrag of de kwaliteit van het systeem om te voorzien in de behoeften van een belanghebbende uit de business.

Initially the clutch is closed To open the clutch, it takes at least 100 ms and at most 150 ms To close the cluch, it takes at least 100 ms and at most 150 ms Initially the gearbox is neutral To release the gear, it takes at least 100 ms and at most 200 ms. To set a gear it takes at leasst 100 ms and at mose 300 ms. The engine is always in a predefined state called initial when no gear is set. To find zero torque in the engine, it takes at least 1150 ms and at most 400 ms. ut at 400 ms, the engine may enter an error state or find synchronous speed. The engine may regulate on synchronous speed in at most 500 ms. When in an error state, the engine will regulate on synchrobous speed in at least 50 ms.

A gear change should ne performed within 1 seond (P6-p*,P3) When an error arises, the system will reach a predefined error state marking the error (p9-p11) The system should be able to use all gears (p2-p3) There will be no deadlocked stat in the system(p17) When the system indicates gear neutral, the engine should be in initial state (p12) The gearbox controller will never indicate open or closed clutch when the clutch is closed or open respctively(p14) The gearbox controller will never indicate gear set or geur neutral wen the gear is nog set or idle respectively (p15) When the engine is regulating on torque, the clutch is closed (p16)

6.9 Veiligheidsoverwegingen

- Performance
  - A gear change should be completed within 1.5 seconds unless an unrecoverable error ocurs.
  - A gear change, under normal operation conditions should ne performced within 1 second
  - When a gear is set, he engine shoud be regulating torque.
  -
  -

–

- Predeictability The predictability requirements are to ensire strict synhronization and control betwee components.
  - There should be no deadlocks in the system
  - When the engine is regulating torque, the clutch should be closed.
  - It is able to use all gears.
  - It uses the engine to enhance zero torque and synchronous speed over the transition.
  - It uses the gearbox to set and release gears.
  - It is allowed to use the clutch in difficult conditions.
  - It does not request zero torque when changing from neutral gear.
  - The gear controller does not request synchronous speed when changing to neutral gear.
  –
- Functionality The followin requirements are to ensure the desired functionality of the gear controller.
  –
  –
  –
  –
  –
  –
- Error detection: Th gear controller detects and indicates error only when:
  - a) the clutch is not openend in time;
  - b) the clutch is not closed in time;
  - c) the gearbox is not able to set a gear in time,
  - the gearbox is not able to release a gear in time.
  –
  –
- Safety
  –
  –
  –
  –

  -
  -
  - Ik wil zeker zijn dat mijn schip niet tegen de sluisdeuren aanvaart als een stoplicht op groen is
  - Ik wil er zeker van zjn dat mijn schip niet tegen de tweede deur vaaart als het eerste stoplcht op groen is
  - Ik wil er zeker van zijn dat als mijn schip de sluis op hoog binnentreerd dat het waterniveu in de sluis gelijk si aan hoog.
  - Ik wil er zeker van zjn dat als mijnship de sluis op een laag waterpeil binnenvaart dat het waternivel in de sluis gelijk i aan hoog.
  - Ik wil er zeker van zijn dat als mijn schoip de sluis op laag binnenvaart dat het waterniveu in de sluis gelijk is s aanlaag.
  - Ik wil een signaal wanneer er een schip in de slis zit als sluisbediening
  - Ik wil als sluiscontrollller een signaal als de dueren openstaan en een schip komt aanvaren en er is tegelijk een schip inn de sluis.
  - Ik wil max 2 schepen in de sluis
  - Ik wil dat een schip de sluis pas na 5 seconden in de atarrival state kan binnentreden
  - Ik wil dat mijn stoplicht lleen bedient kan worden door de sluis
  - Ik wil dat de deuren alleen bedient kunnen worden door de sluis
  - Ik wil dat sensoren alleen bedient kunnen worrden door de sluis
  - Een schip moet een route kunnen aflaggen

- Liveness
  -
- Fairness
  -

6.9.1 Uppaal kripke structuren

6.9.2 Functionele en niet-functionele eisen

6.9.3 specificaties

6.9.4 Het vier variabelen model

Systemen (met daarin software) en de bijbehorende vier variabelen:

6.9.5 Monitored variabelen

: door sensoren gekwanti
ceerdefenomenen uit de omgeving

6.9.6 Controlled variabelen

door actuatoren bestuurde fenomenen uit de omgeving

6.9.7 Input variabelen

6.9.8 Output variabelen

6.9.9 Aankomst, uitvoering, vrijgave

6.9.10 ontwerp

6.9.11 Onderdelen

Op basis van de schets kunnen we vaststellen dat een sluismodel uit de volgende onderdelen bestaat.

1. Een tweetal sluisdeuren.
2. Een sluiskolk waarin de schepen in- enuitvaren
3. een stoplicht om een signaal af te geven voor invaren en uitvaren.
4. Een nivelleermachine zorgt ervoor dat het water in de sluis op het gewenste niveau wordt gebracht
5. Een control-system dat ervoor zorgt dat de opdrachten van de sluisbeheerder (geautomatiseerd) worden uitgevoerd

6.9.12 Werking

Een schip komt aanvaren en meld zich aan bij de sluismeester. De sluismeester geeft een signaal aan het controlsystem voor het openen van de sluisdeuren, nadat geccontroleerd is of de nivelleermachine al klaar is. Als er ruimte is voor een invarend schip mag het schip dat zoich heeft aangemeld en toestemming heeft in de sluis varen. Op het moment dat de sluis vol is gaan de sluisdeuren dicht. Eenmaal afgesloten kan de nivelleermachine beginnen om het water in de sluiskolk op het gewenste waterpeil te brengen. Als dit nivelleerprces is afgerond geeft het controlsystem daan da de sleusdeuren open kunnen. Als de sleusdeuren open zijn en het uitvaarsignaal is op groen dan moet het schip in de sluis de sluis uitvaren.

extra cases Uit het zojuist genoemnde scenario valt het volgende op te maken.

1. Een schip geeft een signaal aan een sluismeester.
2. Er wordt gekeken of er wel plek is in de sluis .
3. Er wordt gekeken of de nivelleermachine is afgerond.
4. Er wordt gekeken wat het niveo van de waterpeil in de sluiskolk is.
5. Er wordt gekeken of de sluisdeuren gereed zijn voor invarende schepen.

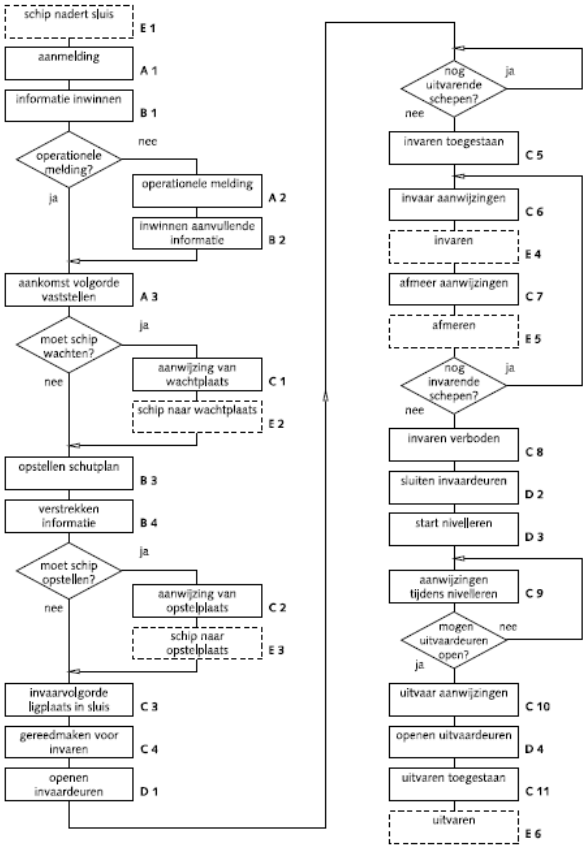
Aandachtspunten

1. Voorrang tussen schepen onderling in de sluis?
2. Hoe lang mag een schip zich in de sluis bevinden?

6.10 Afbakening

- Wat doet de sluis niet.
- De sluiss houdt geen rekening met links of rechtsrijdend verkeer vanuit de zeevaart
- De sluis heeft geen queue met daarin een id gekoppeld aan de sluis.
- De waterpomp wordt alleen aan en uitgezet
- De waterpomp houdt geen rekening met waterstand
- Houdt geen rekening met een schip in de sluis dat is blijven hangen.

Formal description of the system



Figuur 50: Stroomschema sluispassage

- Vooraanmelding
- informatie inwinnen
- operationele melding
- aankomst volgorde
- aanwijzen wachtplaats
- verstrekken informatie
- aanwijzen opstelplaats
- opstellen schutproces
- verstrekken informatie
- invaarvolgorde en ligplaats in sluis
-

- gereedmaken voor invaren
- openen invaardeuren
- invaren toegestaan
- aanwijzingen voor invaren
- aanwijzingen tijdens afmeren
- invaren verboden
- sluiten invaardeuren
- start nivelleren
- stop nivelleren
- aanzwijzingen voor uitvaren
- openen uitvaardewuren
- uitvaren toegestaan

- uitvaren
- operationele afmmelding
- utvaren verboden
- aanwijzing invaren nieuwe schepen verboden gesloten

6.11 Notities die verwerkt moeten worden

moet de intitial state altijd in een loop zitten in uppaal? wat zijn urgent channels? rampen? er staat wel iets in de planning maar kan geen lessen of verdere documentatie of requirements terug vinden?

gesprek wessel: main controller slim dat direction een bool is. pomp is te slim, zoiu alleen maar aan of uit moeten gaan, of nog weg en in pompen maar meer niet. niets met waterlevel en aantal schepen. schip: niet doen. als een schip zich aanmeld, dan gebeuren er dingen, maar gaat hij naar binnen? je weet niet wat dat schip gaat doen want menselijk gedrag. beter niet het schip uitgebreid maken, maar eerder de sluis. te veel aannames.

wessel model: alleen als wachtrij vol zit, doet de sluis iets. deur heeft een parameter zodat er meerdere deuren in de simulator neergezet kunnnen worden. ook bij wachtrij.

stoplichen kunnen er wel in maar als je simpeler wilt, gaan die als eerste weg. zes variabelen model is voorgesteld maar niet goed op gereageerd. alleen er van af weten is genoeg. rampen alleen voor persoonlijk verslag

Liveness Liveness properties are of the formn: something will eventually happen, e.g. when pressing the on button of the remote control of the television, then eventually the television should turn on. Or in a model of a communication protocol, any message that has been sent should eventually be received.

Fairness

Security Safety propertires are of the form: "something bad will never happen". For instance, in a model of a nuclear power plant, a safety propertymight be, that the operating temperature is always (invariantly) under a certain threshold, or that a

meltdown never occurs. A variation of this property is that "something will possibly never happen". For instance when playing a game, a safe state is one in which we can still win he game, hence we will possible not loose. The system cannot reach states or enable events that are fornidden by the requirements

Performance There requirements limit the maximum time to perform when no recoverable errors occur.

brainstorm 22-5-2022

invaardeuren en uitvaardeuren Gaan we uit van binnendeuren en buitendeuren? Er ontstaat dan een extra ruimte in de sluis. Hoeveel schepen kunnen in deze ruimte? Wat is de maximale wachtreij in deze ruimte en wat zijn de verkeersregels in deze nruimte?

invaarstoplicht en uitvaarstoplicht Als invaren is toegestaan hoe wordt dit dan doorgegeven aan de schepen in de sluis? moeten zij dan uit zichzelf wachten of krijgen zij een signaal dat zij wewl/niet mogen uitvaren? En moeten zij dan kiezen voor links, midden of rechts? Of maakt dat allemaal niets uit?

invaarwachtrij en uitvaarwachtrij Als er meerder schepen in een sluiskolk zitten moet het systeem dan rekeneing houden met het schip dat als eerste is ingevaren en/of het langst in de sluis zit?

Formal validation and verification aan de hand van Kripke model

Parallele compositie Om een sluispark te kunnen modelleren meerdere templates die de verschillende abstracties van het systeem aantonen.

Synchronisatgie Zorgt ervoor dat een transitie die genomen worden in de ene kripke tructuur op hetzelfde moment wordt opgenomen in een andere kripke structuur.

Modelling with timed automata

Clock regions

Clock zones

Difference bound matrices

Complexity considerations

6.11.1 templates

Schip

Sluis

Aanvoer

Afvoer

Pomp

Pompbediening

Stoplicht

Deur

6.12 Formele logica

0004 0031 Modelcheckig boek blz 14 E = main=, deur=, stoplicht=, sensor=, pomp=, wachtrij=, queue=, sluiskolk= Q0 = F C Q = sluiskolk$_a fgeslotenQ = E0, ...En00640077$

X: volgende keer F: in de toekomst G: altijd geldig A: voor alle paden E: voor enkele paden U: waar zolang de volgende inclusief geldt R: waar zolang geldt inclusief de startpositie

M, s-¿ f betekent f is geldig in state s in kripke structuur M M, ph -¿ f is geldig op een pad in kripke structuur M M. s -¿ FP ¡-¿ er bestat een fair pad dat begint bij s en p € L(s) M, s-¿E(g) er bestaat een fair pad M dat begint van s zodanig dat phi -¿ F(g) M, s-¿ F A(g) voor alle fair pads phi beginnend vanad s, phi -¿ F(g)

7 Conclusies

8 Eindvverantwoording

Ik heb erg veel geleerd van het analyseren van de vershillende requirements en specificaties en het opzetten van een model in Uppaal. Een dergelijk model opzetten had ik namelijk nog nooit gedaan. Het uitvoeren van onderzoek heb ik eerder gedaan. Ook de toetsing van het model met behulp van propositie heb ik nog nooit gedaan. Verder heb ik de kennis die had van programmeren/ design pattersn gebruikt om de verschillende templates in mijn Uppaal model van elkaar te onderscheiden. Het leukste onderdeel van het project vond ik hoe mijn templatemodel deadlockvrij werkte. Voor de verificatie van het model heb ik veel achtergrondinformatie opgezet, en het is mooi om te zien dat je met enkele duidelijke zinnen kan aantonen of een propositie geldig is of niet. Verder had ik moeite met het opstellen van de juiste veiligheidseisen bij het model. Ik had aangenomen dat ik het project niet zou halen omdat ik de opdracht niet in teamverband heb uitgevoerd. Ik ben toch blij dat ik een concept heb opgeleverd dat ik kan toetsen aan de doormijzef opgestelde eisen en dat ik met mijn huidige kennis de proposities uit de requirements kan toetsen.

Important: In the list of references at the end of thesis, abbreviated journal and conference titles aren't allowed. Either you must put the full title in each item, or create a List of Abbreviations at the beginning of the references, with the abbreviations in one column on the left (arranged in alphabetical order), and the corresponding full title in a second column on the right. Some abbreviations, such as IEEE, SIGMOD, ACM, have become standardized and accepted by librarians, so those should not be spelled out in full.

9 Discussie

9.1 Future work

9.1.1 Hoogte waterniveau

9.1.2 type deuren naar waterniveau

De sluis kan ook rekening houden met waterniveau van hoog naar laag. Als een schip naar binnen vaart moet de sluis weten welk schip ook werer naar buiten vaart en aan welke kant.

9.1.3 voorrang uitvarend op invarend

Als een schip uitvaart komt er een moment dat een sluis ruimte vrij heeft. Voordat de sluisdeur sluit nadat eenschip is vertrokken kan er nog een polling worden gedaan naar alle schepen in de buurt om te zien of deze willen en kunnen invaren.

9.1.4 stoplicht invarend en stoplicht uitvarend

Een handige functionaliteit is dat voor invarende schepen er een stoplicht is en voor uitvarende schepen. Anders ontstaat er een probleem van collission.

9.1.5 Volgorde

Kunnen aantonen dat schepen kunnen worden behandeld met voorkeur, wie het eerst komt die het eerste in behandeling wordt genomen.

10 Research case: De digitale aanval op de Oekrainese krachtcentrale

Dit verslag geeft inzage in een analyse van de Ukraine cyber aanval, inclusief hoe de actoren zich zelf toegang gavan tot het controle systeem, welke methoden de acoren hebben gebruikt voor reconnaissance en vastleggen van het systeem, een gedetailleerde omshrijving van de aanval op 15 December 2015, en de methoden die gebruikt zijn door de aanvallers om hun sporen uit te wissen en daarmee het het stoppen van schade toebrengen nog moeilker maken. Daarnaast wordter een gedetailleerde omschrijving gevevenv an de beveiliging van de SCADA ccontrol systemen gebaeerd op bst practices, inclusief het control network ontwerp, technieken voor whtelisting, monitoring en loggen, en opleiding van personeel.

https://na.eventscloud.com/file$_uploads/aed4bc20e84d2839b83c18bcba7e2876_Owens1.pdfhttps$: $//www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/https$: $//www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdfhttps$: $//www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108https$: $//www.mandiant.com/resources/blog/ukraine-and-sandworm-teamhttps$: $//www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdfht$ $//ris.utwente.nl/ws/files/6028066/3-s2_0-B9780128015957000227.pdfhttps$: $//repositorio-aberto.up.pt/bitstream/10216/119066/2/315683.pdfhttps$: $//www.diva-portal.org/smash/get/diva2$: $1046339/FULLTEXT01.pdfhttps$: $//www.vice.com/en/article/zmeyg8/ukra$ $power-grid-malware-crashoverride-industroyer$

Oop 23,december 2015 vind er een cyber aanval plaats op het elektriciteitsnet van de Oekraine. Dit was de eerste bekende aanval op een elektrisch controle system met corrupte firmware. Daarnaas wordt er een telecom-based denial of service attack met geautomatieerde systemen om het telefoonverkeer uit te schakelen. [2]

Uit onderzoek[1] naar de aanval, uitgevoerd door Oekraiene sen Amerikaanse militairenblijkt bleek onder meer dat de power grids in sommige gevallen beter waren beveiligd dan de Amerikaanse. Desondanks was de viligheid niet optimaal door onder andere de hetgegeven dat werknemers op afstand konden inloggen en geen gebruik van 2-stapsverificatie.

10.1 Literaire analyse

10.1.1 Motief

Oekraine wijst naar de russen [1] https://www.wired.com/story/russian-hackers-attack-ukraine/ https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm/u-s-firm-blames-russian-sandworm-hackers-for-ukraine-outage-idUSKBN0UM00N20160108 https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN https://theconversation.com/cyberattac on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802 https://jsis.washington.edu/news/cyberat critical-infrastructure-russia-ukrainian-power-grid-attacks/

10.1.2 Situatie Oekraiene

https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

10.1.3 Situatie algemeen

https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/ https://www.ifri.org/sites/default/files/atoms/files/desarnaud$_{c}yber_{a}ttacks_{e}nergy_{i}nfrastructures_{2}017_{2}.pdfhttps$ $//www.cybersecurityintelligence.com/blog/attack-on-ukraines-power-grid-targeted-transmission-stations-4530.html$

10.1.4 Factoren

http://web.mit.edu/smadnick/www/wp/2016-22.pdf

10.1.5 Oorzaak

https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/ https://arstechnica.com/information-technology/2017/06/crash-override-malware-may-sabotage-electric-grids-but-its-no-stuxnet/ https://www.darkreading.com/threat-intelligence/first-malware-designed-solely-for-electric-grids-caused-2016-ukraine-outage https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

10.1.6 Gebruikte materialen

https://en.wikipedia.org/wiki/2015$_{U}kraine_{p}ower_{g}rid_{h}ackhttps://www.cisa.gov/news-events/alerts/2017/06/12/crashoverride-malwarehttps://rhebo.com/en/service/glossar/industroyer-25114/$

10.1.7 Uitvoering van de aanval

https://na.eventscloud.com/file$_{u}ploads/aed4bc20e84d2839b83c18bcba7e2876_{O}wens1.pdfhttps://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf$

10.1.8 Oplossingen

https://na.eventscloud.com/file$_{u}ploads/aed4bc20e84d2839b83c18bcba7e2876_{O}wens1.pdfhttps://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01$

10.1.9 Aanbevelingen

10.2 Resultaten

10.2.1 De aanval

1. An initial email spear phishing attack lures recipients into opening an attached Microsoft® document with a macro that installs Black Energy 3 (BE3) onto

corporate workstations. 2. BE3 and other tools perform reconnaissance and enumeration of the network and provide an initial backdoor for the hackers into the corporate network. 3. As a result of network reconnaissance, the malicious actors discover and access the oblenergos' Microsoft Active Directory® servers that contain corporate user accounts and credentials. 4. With the harvested credentials, the malicious actors use an encrypted tunnel from an external network to get inside the oblenergo network, establishing a presence on the oblenergo control system networks. 5. Malicious actors discover and access the control center supervisory control and data acquisition (SCADA) human-machine interface (HMI) servers and substations. While a router separates corporate and SCADA networks, the firewall rules are improperly configured. 6. On December 23, 2015, at 3:30 p.m., the malicious actors begin their power outage attacks by entering operations and SCADA networks through backdoors on the compromised SCADA workstations. The malicious actors take control away from HMI operators and then open breakers. 7. The malicious actors perform several other actions with the intent of complicating the responses of control operators and increasing the effort required to return the system to normal operating conditions. These actions include: a. Launching a coordinated Telephony Denial of Service (TDoS) attack that floods call centers to prevent legitimate calls from getting through. b. Disabling the UPSs for the control centers. c. Corrupting the firmware on a remote terminal unit (RTU) HMI module and serial-to-Ethernet port servers. 8. Malicious actors execute KillDisk malware in an attempt to wipe out the control center HMIs and pivotpoint workstations. https://na.eventscloud.com/file$_uploads/aed4bc20e84d2839b83c18bcba7e2876_Owens1.pdfhttps$: $//www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf$

10.2.2 spearfishing

10.2.3 blackenergy

10.2.4 remote access capabilities

10.2.5 serial-to-ethernet communication devices

10.2.6 telephony denial of service attacks

10.3 oplossingen

Identificeer alle risicos en schrijf een plan foor het managen van de risico's. Implementeer effecteve controle om het riico te managen. Creeer een diepgaand model dat ervoor zor dat er efectieve en efficiente security controls worden uitgevoerd. Aangaande de gebeurtenissen in de oekraiene kunnen de volgende security controls worden opgenomen in het securitymodel: Initial access to enterprise network, pivot in interprise network, elevate priviliges, maintainance access, gain access to control system, attack, attack complication, destroy hard drives. [2]

10.4 Discussie

10.5 Verder lezen

https://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=0513EED48102FDAD1BD940260EF12B11?doi=10.1.1.
https://scialert.net/fulltext/?doi=tasr.2014.396.405 https://www.researchgate.net/publication/333671061$_{A}ttacki$
$60870-5-104_{S}CADA_{S}ystemshttps://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_{I}ndu$
$//blog.nettedautomation.com/2017/https://arxiv.org/pdf/2001.02925.pdfhttps:$
$//dl.acm.org/doi/fullHtml/10.1145/3381038https://www.win.tue.nl/\ setalle/2017_{f}auri_{e}ncryption.pdfhtt$
$//www.connectivity4ir.co.uk/article/175490/IEC-62351--Secure-communication-$
$in-the-energy-industry.aspxhttps://www.virsec.com/resources/blog/virsec-$
$hack-analysis-deep-dive-into-industroyer-aka-crash-overridehttps:$
$//dreamlab.net/en/blog/post/fuzzing-ics-protocols/https://www.blackhat.com/docs/us-$
$17/wednesday/us-17-Staggs-Adventures-In-Attacking-Wind-Farm-$
$Control-Networks.pdfhttps://blog.checkpoint.com/research/crashoverride/https:$
$//www.blackhat.com/us-17/briefings/schedule/industroyercrashoverride-$
$zero-things-cool-about-a-threat-group-targeting-the-power-$
$grid-6159https://search.abb.com/library/Download.aspx?DocumentID=$
$9AKK107045A1003amp;LanguageCode=enamp;DocumentPartId=amp;Action=$
$Launchhttps://iiot-world.com/ics-security/cybersecurity/five-cybersecurity-$
$experts-about-crashoverride-malware-main-dangers-and-lessons-$
$for-iiot/https://www.csoonline.com/article/3200828/crash-override-$
$malware-that-took-down-a-power-grid-may-have-been-a-test-$
$run.htmlhttps://www.paloaltonetworks.com/blog/2017/06/crashoverrideindustroyer-$
$protections-palo-alto-networks-customers/https://www.webopedia.com/definitions/crashoverride-$
$industroyer-malware/https://www.cyber.nj.gov/threat-center/threat-$
$profiles/ics-malware-variants/crashoverridehttps://www.nixu.com/blog/crashoverride-$
$threat-electricity-networkshttps://www.virusbulletin.com/virusbulletin/2019/03/vb2018-$
$paper-anatomy-attack-detecting-and-defeating-crashoverride/https:$
$//en.wikipedia.org/wiki/Crash_{O}verride_{N}etworkhttps://en.wikipedia.org/wiki/Industroyerhttps:$
$//www.dragos.com/resource/crashoverride-analyzing-the-malware-$
$that-attacks-power-grids/https://www.wallix.com/blog/ics-security-$
$russian-hackinghttps://www.nixu.com/fi/node/53https://control.com/forums/threads/comparison-$
$between-iec60870-5-103-and-modbus-rtu.20317/$

pgf
field1 = G. Wales, field2 = Mathematics

Betrokken partij	Verantwoordelijk	datetimestamp here
Korte notitie		

test

Foto incident

11 Bijlage: Testcases en resultaten

11.1 Wat wordt getest en hoe

11.2 Requirement specification in queries

```
Sluis.Draining-->Deuren.laag_open
Deuren.laag_open-->Stoplicht.Green
E<> (Ship.ship_can_move&&Stoplicht.Green)
A[] not (Stoplicht.Green && not (Deuren.hoog_open||Deuren.laag_open||Deuren.stopgaplow1||De
A[] not ((Deuren.hoog_open||Deuren.laag_open||Deuren.Opening_laag||Deuren.Opening_hoog||Deu
Sensor.Wait-->Sensor.Wait
Stoplicht.Green-->Stoplicht.Green
(Deuren.hoog_open||Deuren.laag_open)-->(Deuren.laag_open||Deuren.hoog_open)
Deuren.laag_open-->Deuren.Closed
Deuren.hoog_open-->Deuren.Closed
Deuren.Closed-->Stoplicht.Red
Ship.ship_can_move-->Deuren.Closed
Deuren.hoog_open-->Stoplicht.Green
Ship.ship_can_move-->Stoplicht.Green
A[] not (Deuren.laag_open && Deuren.hoog_open)
Ship.ship_can_move-->Ship.ship_can_move
A[] not (Deuren.laag_open && Sluis.water != Sluis.water_laag)
A[] not (Deuren.hoog_open && Sluis.water != Sluis.water_hoog)
A[]not deadlock
```

- P1 Het is mogelijk dat de sluis van richting verandert. E¡¿ !Main.Direction
- P2 Het is mogelijk dat de sluispomp in een cyclus teveeel water heeft gepompt en dat er daardoor water weggepompt dan wel bijgekompt dient te worden E¡¿ main.waterlevel
- P3 Het is al binnen 100 ms mogelijk omte achterhalen aan welke kant de sluisdeuren open moeten.
- P4 Als de richting van een schip gelijk is aan N, dan is het waterlevel niet gelijk aan 1-5 of R
- P5 De sluispomp is nooit in positie AAN, wanneer de sluisdeuren open zijn.
- P6 In het geval dat er geen errors zijn (in de stoplichten, sluisdeuren) and ideal (wachtrij) scenario,
- a) dan is een cyclus gegarandeerd binnen 100 ms (including 100 ms) (undefined)
- a') dan is een cyclus niet gegarandeerd binnen 100 ms

- b) dan is het onmogelijk om van beneden naar boven te varen, of andersom binnen 150 ms
- b') dan is het mogelijk om van beneden naar boven te varen, of andersom binnen 150 ms
- c) het is onmogelijk om van richting te veranderen in minder dan 400 ms als de pomp al op niveau x is
- c') het is mogelijk om van richting te veranderen in minder dan 400 ms als de pomp al op niveau x is
- P7 Als zich geen errors voordoen bij stoplicht en deur,maar de waterpomp uitvalt:
- a) a gear switch is gearanteerd after 1055 ms (not including 1055) (deleted)
- a') it is impossible to switch gear in 1055 ms (deleted)
- b) it is impossible to switch gear in less than 550 ms (deleted)
- b') it is possible to switch gear at 550 ms (deleted)
- c) it is impossible to switch gear in less than 700 ms if the switch is not from/to gear N (deleted)
- c') it is posible to switch gear at 700 ms if the switch is not from/to gear N (deleted)
- p8 When no error occurs, but engine fails to find synchronous speed
- a) a gear switch is guaranteerd in 1205 ms (incuding 1205)
- a') a gear switch is not gearanteerd at less than 1205 ms
- b) it is imposible to switch gear in less than 450 ms
- b') is is possible to switch gear at 450 ms
- c) it is impossible to switch gear in less than 750 ms if the switch is not from/to gear N
- c') it is not possible to switch gear at 750 ms if the switch is not from/to gear N
- p9 Clutch errors
- a)If the clutch is not closed properly (i.e. a timeout occurs) the gearbox controller will enter the locationCCCloseError with 200 ms (undefined)
- b) When the gearbox controller enters location CCloseError, there is always a problem in the clutch with closing the clutch. (undefined)

- a) If th clutch is not closed properly (ie. a timeout occurs) the gearbox controller will enter the location CCloseError within 200 ms (undefined)
- b) When the gearbox controller enters location CCloseError, there is always a problem in the clutch with closing the clutch. (undefined)
- p10 Gearbox errors
- a) If the gearbox can not enter a requested gear (i.e. a tieout occurs) the gearbox controller will enter the location GsetError within 350 ms (undefined)
- b) When the gearbox controller enters location GSetError, there is always a problem in the gearbox with setting the gear. (undefined)
- p11 IF no error occurs in the engine, it is guaranteed to find synchronous speed (undefined)
- p12 Wanneer beide sluisdeuren in state gesloten zijn, dan is de pomp in zijn initiale state of 100 ms verwijderd van zijn initiele state
- A[]
- p13 When the gear controller has a greater set, torque regulaton is always indicated in the engine (undefined)
- A[]
- p14
- a) Als de deur open is(ongeacht boven of beneden, dan bevind de sluispomp zich in een predefined state (undefined) A[] (gate(0).open——gate(1).open) -¿ (main.pomp$_i dle||main.pomp2_i dle)b)Alsdedeurisgeslotendanbevinddemaincontrollerzichineenpredefi$
$main.idle$

- p15
- p16 If engine regulation is on torque, then the clutch is closed (undefined) A[](Engine.Torque imply Clutch.closed
- p17Voor invaren geldt altijd: waterlevel, pomp uit, sluisdeuren open en stoplicht op groen A[] main.s5 -¿ main.waterlevel$_l aagidle_p omp1gate(0).opengate(1).open(stoplight(0).greenstoplight(1).gree$
$forall(i : id_d)forall(j : id_s)gate(i).closedstoplight.roodmain.rd_1p19uitvarendenhebbenvoorangopinvarenden$
- p20 Voor invarenden geldt pomp uit, sleusdeur open en stoplicht op groen A[] main.s6 -¿ gate(0).open gate(1).open stoplight(0).groen stoplight(1).groen
- p21 voor nivelleren geldt pomp is aan, sluisduren zijn doicht en het stoplicht is op rood A[] (main.rn1 —— main.rn2) -¿ forall (i:id$_d)forall(j : id_s)gate(i).closedstoplight(j).roodp22Alseenschipver$
- p23 urgent locations; het is niet mogelijk om hier te wachten

- p24 urgent syn; een synchronisatie moet direct worden uitgevoerd als de guards geldig zijn
- p25 als een schip binnen is, en er zijn wachtende schepen, dan moet het stoplicht via oranje naar rood A[]
- p26 committed; als deze staat actief is dan wordt de eerst volgende transitie uitaande van deze state
- p27 als een schjip binnen vaart mnoiet hij ook eft binnen zijn en niet binnenvaren, dit geldt ook voor p28 sluisdeuren en pompen dus deze zijn committed. A[]
- p28 Een schip komt aanvaren en geeft een signaal aan de sluis. A[]
- p29 Indien er meer dan twee schepen in de sluis zitten dan wordt het ship geplaats in de wachrij. A[] Queue.list[N-1] == 2 -¿ (Sluiskolk.list[N]==1 ——Sluiskolk.list[N]==2)
- p30 Een schip kan pas naar binnenrijden als de sluisdeuren open zijn, het stoplicht is op groen er er zijn minder dan 2 schepen in de sluis. A[] main.s6 schip.varen -¿ Queue.list[N-1] ¡2
- p32 Eenmaal in de sluis zal het schip moeten wachten op de sluis en de pomp. A[] Queue.list[N-1] == 2
- p33 Een schip mag alleen uitvaren als de pomp klaar is, de sleusdeuren open. A[] schip.varen main.s12 —— main.s13 -¿ (!main.rn1 !main.rn2)
- p34 Een sluis ontvang een aankomst signaal van een schip en bestuurt de sluisdeuren en de pomp. A[]
- p35 De sensor is een onderdeel van de sluis en ontvangt signalen van naderende schepen. A[]
- p36 De sleusdeur voor boven en beneden kunnen beiden open en dicht. De sluisdeur wordt aangestuurd door de sluis. A[]
- p37 Een pomp begint met pompen bij een signaal van de sluis. Een sluis op zijn beurt geeft alleen een signaal aan de pomp als de sleudeuren dichtzijn A[] pomp.pomp$_a ctive -> main.s6 forall(i : id_d) gate(i).closed p38 Geen deadlock$
- p39 Voor geen enkel pad geldt dat als de deuren gesloten zijn volgens de kluis dat er een deur openstaat om een schip naar buiten te laten. A[] not forall(i:id$_d$)$gate.closed -> (main.s12||main.s13) p40 Voor alle pad en gelddat alseen sluisaanhetvoorbereidenis, danzijnalledeurendcht.A[]n forall(gate(0).closed$
- p41 Voor alle paden geld dat als een deur dicht is het aantal schepen in de kade gelijk is aan nul A[] p42 Voor geen enkel pad geld dat als het binnenstoplicht op groen staat dat het niet toegestaan in naar binnen te varen E¡¿ stoplight(2).groen —— stoploght(3).groen -¿ main.s6

- p43 Voor alle paden geldt dat de globale tijd langer is dan 30 tijdseenheden A[] main.s13-¿ main.processtime¿30
- p44 Er is een pad waarvoor geld dat als een schip wilt stoppen dat er meer dan 5 schepen in de sluis zitten. E¡¿
- p45 Voor alle paden geldt als schip vrtrekt is sluisdeur dicht A[]
- p46 Voor alle paden geldt als stoplicht op rood sluisdeuren dicht en schip vertrokken dan is de nivelleermachine uit A[]
- p47 Er is geen pad waarop een schip vertrekt vanuit de rechtersluisdeur en de linkersluisdeur is open en linkeruitaartstoplicht en linkeruitvaartsoplicht opgroen en nibelleermachine is aan E¡¿
- p48 Er is een pad waarvoor geldt dat linkerslsuisdeuren dicht zijn, rechtersluisdeuren dicht zijn rechteruitvaartstoplicht is rood en rechteruitvaartstoplicht is rood terwijl eer geen schip in de sluis licht E¡¿
- p49 EEn stoplich staat altijd op groen als de deuren open staan en de pomp niet bezig is. A[] forall(i:id$_s$)$stoplight.groen -> gate(0).opengate(1).open(main.pomp1_idle||main.pomp2_idle)p50Ingee$
- p51 Voor alle paden in een pomp geldt dat als water level lager is dan waterlaag pompwaterweg is altijd false A[] (main.waterlevel¡waterlaag) -¿ (!pompwaterweg——pompwaterweg==false)
- p52 Voor alle paden gelft dat als water level hoger is dan waterhoog dan is pompwater altjd false A[]
- p53 Het zal nooit gebeuren dat een pomp water toevoegt als deuren open zjn, geen schip in sluis en stoplicht op groen A[] not main.rn1 —— main.rn2 -¿ gate(0).open gate(1).open Queue.list[N-1] == 0 ((stoplight(0).groen——stoplight(1).groen) ——(stoplight(3).groen stoplight(4).groen))
- p54 Het kan gebeuren dat bij pompr het stoplicht op rood staat, het schip in de sluis en deur is dicht, en waterstand gelijk aan waterlaag E¡¿ (main.blocked1 —— main.blocked2) -¿ Queue.list[N-1] ¿0 gate(0).closed gate(1).closed main.waterlevel==main.waterlevel$_laagp55Eris$ $main.rn1||main.rn2-> gate(0).closedmain.waterlevel == waterlaag$
- p56 Het kan voorkomen dat bij state pompaan het waterniveau gelijk is aan waterlaag E¡¿ main.rn1——main.rn2 -¿ main.waterlevel== main.waterlaag
- p57 Voor alle paden gelt dat er een mogelijkheid is dat deur is open/dicht en sluis nivelleert omhoog/omlaag A[] gate(0).open ()main.direction ==0——main.direction==1)
- p58 A[](1¿0)
-
-

-
-
-

11.3 Operator: AG

Voor alle paden

11.4 Operator: EG

Uiteindelijk geldt er een pad waarvoor geldt

11.5 Operator: AF

Voor alle paden/richtingen vroeg of laat

11.6 Operator: EF

Er is een pad

11.7 Operator: AX

Alle opvolgende toestanden
[?]

11.8 Operator: EX

Er bestaat vanaf de volgende minstens 1 state waarvoor geldt

11.9 Operator: p U q

Er geldt p tot q [?]

11.10 Operator: p R q

q moet waar zijn totdat en inclusief de situatie dat p voor het eerst waar is, als p niet geldig is, dan moet q vooraltjd geldig zijn

11.11 De computation tree

11.12 Operator: AG

11.13 Operator: EG

Voor alle paden geldt dat waterlevel lager is dan niveau van de kant. Voor alle paden geldt dat een omp werkzaam is als alle sluisdeuren dicht zijn. Vpoor alle

paden geldt dat het aantal schepen in de sluis maximaal 2 is. Voor alle padedn geldt dat een schip nooit langer dan 30 seconden in een sluiskolk zit zonder dat het waterpeil is aangepast.

11.14 Operator: EG

Er bestaat op elk pad een

11.15 Operator: AF

11.16 Operator: EF

r is soms een mogelijkheid dat twee schepen in de sluis een verschillende uitvaarrichting hebben.

11.17 Operator: AX

11.18 Operator: EX

11.19 Operator: p U q

11.20 Operator: p R q

Voor alle paden geldt dat een schip alleen kan invaren als de sluisdeur aan de andere zijde is gesloten.

11.21 Operator: EX

Er bestaat geen situatie dat een pomp actief is terwijl er een sluisdeur open staat

11.22 Operator: p U q

Vanaf aankomst tot uitvaren is de clocktijd lager dan 30 tijdseenheden

11.23 Operator: p R q

Vanaf invaren tot en met uitvarenvan een schip en geldig is x lager dan 15 tijdseenheden vanaf aanvaren staat een schip maximaal 40 tijdseenheden in de wahtrij,.

11.24 Operator: AF

Er is altijd meerdere

11.25 Operator: EF

r is soms een mogelijkheid dat twee schepen in de sluis een verschillende uitvaarrichting hebben.

11.26 Operator: AX

Voor alle paden geldt dat een schip alleen kan invaren als de sluisdeur aan de andere zijde is gesloten.

11.27 Operator: EX

Er bestaat geen situatie dat een pomp actief is terwijl er een sluisdeur open staat

11.28 Operator: p U q

Vanaf aankomst tot uitvaren is de clocktijd lager dan 30 tijdseenheden

11.29 Operator: p R q

Vanaf invaren tot en met uitvarenvan een schip en geldig is x lager dan 15 tijdseenheden vanaf aanvaren staat een schip maximaal 40 tijdseenheden in de wahtrij,.

11.30 Fairness

11.31 Liveness

Testresultaten CTL logica

$$\mathsf{D{=}x{\in}}\ 1 \leq x \leq 100$$
$$\mathsf{D{=}[]x{\in}}\ 1 \leq x \leq 100$$
$$\mathsf{D{=}[]x{\in}}\ 1 \leq x \leq 100$$
$$\mathsf{D{=}[]x{\in}}\ 1 \leq x \leq 100$$
$$\mathsf{D{=}[]x{\in}}\ 1 \leq x \leq 100$$
$$\mathsf{D{=}*x{\in}}\ 1 \leq x \leq \tfrac{200}{2}$$

$Sisasetof finitestates$
$S0 \subseteq Sisdesetvaninitielestatess$
$S0 \subseteq SxSiseentransitierelatiedietotaalmoetzij, datbetekent, datvoorelkestates \in Sereenstatsiss' \in SzodatR(s, s')\ La$
$\forall x\, \exists y$
$x\, y \cap \subset \in \vee \diamondsuit\ \dashv \ni\ \pm$

1	A[] !deadlock	TRUE
2	A[] not (Sluis.Tussenstop5 && Deur.Klaar_voor_uitvaart)	Disconnected
3	A[] (Sluis.Voorbereiden imply Deur.Dicht)	TRUE
4	A[] (Deur.Dicht imply Counter==0)	TRUE
5	A[] (Buitenstoplicht.Groen imply invaren_allowed==true)	TRUE
6	A[] ! (Binnenstoplicht.Groen imply invaren_allowed==false)	FALSE
7	A[] (globale_tijd¿30)	FALSE
8	E¡¿ (Schip.Stoppen and (Counter ¿5))	Ship not a structure
9	A[] (Schip.Vertrekken imply Sluisdeur.Dicht)	-

Time bound derivation

Verification results

verklareing

11.32 Fairness

AG(AF(p))

```
In welke staat de automaat zich ook bevindt, in alle richtingen kom je vroeg of laat een s
```

11.33 Liveness

```
Altijd en overal geldt: Als p geldt dan geldt vroeg of laat q
Ookal treedt p nooit p volgens de logica klopt het dan dat q volgt uit p.
In een situatie, waarin p nooit optreedt, spreekt men van een
vacuous truth.
```

mydata.csv

11.34 safety

11.35 zeno vrij

Geen enkele state kan oneindig een transitie uitvoeren. Elke state heeft een uitgaande transitie.

11.36 deadlocks

Actielijst			
Onderwerp	Besluit	Wie	Gereed
Orange	Fruit	Vitamin C	It is fruit, which is full of nutrients and low in calories. They can promote clear, healthy skin and also lowers the risk for many diseases. It reduces cholesterol and also helps in building a healthy immune system.
Cauliflower	vegetable	B-Vitamins	It is the vegetable, which is high in fiber and B-Vitamins. It also provides antioxidants, which help in fighting or protect against cancer. It enhances digestion and has many other nutrients.

project name						
Test case ID				Test designed by		
test priority (low/medium/high)				Test design date		
Module name				Test executed by		
Test title				Test execution date		
Description						
Pre condition						
Dependencies						
Step	Test steps	Test data	expected result	Acual result	(pass or fail)	notes

12 Appendix B: Model eerste deelname aan cursus 2020

12.1 Queries

```
Sluis.Draining-->Deuren.laag_open
Deuren.laag_open-->Stoplicht.Green
E<> (Ship.ship_can_move&&Stoplicht.Green)
A[] not (Stoplicht.Green && not (Deuren.hoog_open||Deuren.laag_open||Deuren.stopgaplow1||I
A[] not ((Deuren.hoog_open||Deuren.laag_open||Deuren.Opening_laag||Deuren.Opening_hoog||De
Sensor.Wait-->Sensor.Wait
Stoplicht.Green-->Stoplicht.Green
(Deuren.hoog_open||Deuren.laag_open)-->(Deuren.laag_open||Deuren.hoog_open)
Deuren.laag_open-->Deuren.Closed
Deuren.hoog_open-->Deuren.Closed
Deuren.Closed-->Stoplicht.Red
Ship.ship_can_move-->Deuren.Closed
Deuren.hoog_open-->Stoplicht.Green
Ship.ship_can_move-->Stoplicht.Green
A[] not (Deuren.laag_open && Deuren.hoog_open)
Ship.ship_can_move-->Ship.ship_can_move
A[] not (Deuren.laag_open && Sluis.water != Sluis.water_laag)
A[] not (Deuren.hoog_open && Sluis.water != Sluis.water_hoog)
A[]not deadlock
```

13 Appendix B: Model herkansing tweede deelname aan cursus 2020

13.1 Template source

```
// Place global declarations here.
/*
Project working

AtArrival
StoplightRed
DoorOpen
StoplightGreen
Startmove
Sensor
SchipEntered
Doorclosed
StoplightRed
---------
Nivelleer started
NIvelleer stopped
Waterlevel equilibrium
-----------
AtLeaving
Stoplightred
Dooropened
Stoplightgreen
StartMove
Sensor
SchipHasLeft
Doorclosed
StoplightRed


Uitleg
Als het schip boven is, dan is waterlvel gelijk aan hoog, filling valve is dicht, lower ga
Schip is in waterlock, waterlevel is hoog, filling valve is dicht, lower gates gesloten, u
Schip is dan laag, waterlevel gelijk aan laag, filling valve is dicht, lowergates zijn ope
AtArrivalHigh

AtArrivalLow
Als schip beneden is dan is waterlevel gelijk aan laag, filling valve is dicht, lower gate
Schip is in water lock, waterlevel is laag, flilling valve is open, lower gates zijn geslo
Schip is dan hoog, waterlevel is gelijk aan hoog, filling valve is dicht, uppergates zijn
```

```
*/

const int N = 2;         // # trains
typedef int[0,N-1] id_t;

chan        appr[N], stop[N], leave[N];
urgent chan go[N];

// waterniveau in in meter van 0 tot 10
typedef int[3,10] waterniveau;

waterniveau level;


//doors
chan lower_gate;
chan upper_gate;
//filling
chan emptying_valve;
chan filling_valve;
bool nivelleer_sessie_bezig;
// water level
chan high_water_level;
chan low_water_level;
//sluices
chan signal_sluis_low[N];
chan signal_sluis_high[N];
//
chan move[N];
//
chan groen;
chan rood;

clock central;

\\geef de schip parameter const id_t id
// Place local declarations here.
clock schip_clock;

\\sensor declaraties
clock x;
```

```
\\sluis declaraties

const int water_laag=3;
const int water_hoog=10;
const int water_median=(water_hoog+water_laag)/2;
int[water_laag,water_hoog] water=water_median;
// level wordt gelijk gezet met temp
// temp is gelijk aan waterniveau
clock sluis_clock;
id_t list[N+1];
int[0,N] len;
bool contentHigh, contentLow;
// Put an element at the end of the queue
void enqueue(id_t element)
{
list[len++] = element;
}

// Remove the front element of the queue
void dequeue()
{
int i = 0;
len -= 1;
while (i < len)
{
list[i] = list[i + 1];
i++;
}
list[i] = 0;
}

// Returns the front element of the queue
id_t front()
{
return list[0];
}

// Returns the last element of the queue
id_t tail()
{
return list[len - 1];
}



\\stoplicht declaraties
```

```
clock stoplicht_clock;



\\pomp declaraties

const int water_laag=3;
const int water_hoog=10;
const int water_median=(water_hoog+water_laag)/2;
int[water_laag,water_hoog] water=water_median;
clock pomp_clock;
// waterniveau van de sensor voor de sluis is gelijk aan level
waterniveau depth;



// een constraint op een bepaalde variabele
bool isForLow()
{
// return false;

if( level>=3) return true;
else return false;

}

bool isForHigh()
{
// return false;

if( level>=6) return true;
//else if(level>=6) return true;

else return false;

}



//verschillende tijdseenheden voor even en oneven lampnummers
```

13.2 Queries

```
Project declaraties
//Declarations

chan boot_hoog;
chan boot_laag;
chan changedoor_low;
chan changedoor_high;
chan ship_moves;
chan ship_abletomove;
chan changelight;

\\Sluis declaraties
const int water_laag=0;
const int water_hoog=10;
const int water_median=(water_hoog+water_laag)/2;
int[water_laag,water_hoog] water=water_median;
clock x;
\\Stoplicht declaraties

\\Ship declaraties
clock x;
\\Sensor declaraties

\\Deuren declaraties
bool stoplicht_hoog=false;
bool stoplicht_laag=false;
clock x;


\\System declaraties
system Deuren,Sensor,Sluis,Ship,Stoplicht;


Uitleg
Als het schip boven is, dan is waterlvel gelijk aan hoog, filling valve is dicht, lower ga
Schip is in waterlock, waterlevel is hoog, filling valve is dicht, lower gates gesloten, u
Schip is dan laag, waterlevel gelijk aan laag, filling valve is dicht, lowergates zijn ope
AtArrivalHigh

AtArrivalLow
Als schip beneden is dan is waterlevel gelijk aan laag, filling valve is dicht, lower gate
```

```
Schip is in water lock, waterlevel is laag, flilling valve is open, lower gates zijn gesl
Schip is dan hoog, waterlevel is gelijk aan hoog, filling valve is dicht, uppergates zijn
```

14 Deelonderzoek naar veiligheidsrisico's en eisen voor sluizen

15 Deelonderzoek wet en regelgeving voor sluizen

Gevonden weblinks in google op 07-04-2023 met zoekopdracht: "wet en regelgeving voor sluizen"

pgf /form field1/.store in=, field2/.store in=,

Referenties

[1] Inside the cunning, unprecedented hack of ukraine's power grid.

[2] title.