layered

trees

/tikz/,/tikz/graphs/

conversions/canvas coordinate/.code=1 , conversions/coordinate/.code=1

trees

Persoonlijk verslag

van

Galvin Bartes (0799967)

CMI-Opleiding *Technische Informatica* – Hogeschool Rotterdam

8 september 2023

Eerste docent *Dhr. W. Oele*
Tweede docent

Samenvatting

Introduction: Whilst every study published in ascientific journal contains an abstract, little researchhas been done on the exact format, content andstyle with which an abstract should be written. Thismakes it difficult for authors to adequately sum-marise their work in an abstract. Methods: In this study, the authors recruited acohort of medical students who had written at leastone scientific paper. Students were anonymouslysurveyed, on their confidence writing abstracts us-ing an online survey, maintaining confidentiality.However, this method may have been subjected toselection bias, where those who have completed ab-stracts but not written a full scientific paper may beexcluded. Use of online surveys may also contributeto selection bias, based on the fact that subject par-ticipation is voluntary and particular characteristicse.g. access to internet, whether the students viewthe site/email providing access to the questionnaire,time available for completion, etc., may differ perindividual and hence reduce the representativenessof the sample regarding the medical student popu-lation (The Writing Centre University of NorthCarolina at Chapel Hill, n.d.). Results: 73 students responded and the studyshowed that 37 Discussion: Based on the author's results, it isclear that students need more guidance on how towrite abstracts. The authors recommend that allstudents wishing to learn how to write an abstractread the National Student Association for MedicalResearch 'Anatomy of an Abstract' article. How-ever, further controlled studies should be done toeliminate biases attributed to methodology in thiscohort study to truly determine whether medicalstudents lack confidence in writing abstracts.References:1. Nulty, D. D. (2018) The adequacyof response rates to online and paper surveys: whatcan be done?Assess Eval High Educ, 33(3), 301-14.doi: 10.1080/02602930701293231

Background: The writing and publication of re-search material by medical students is an area thatoccupies the time and efforts of the students them-selves, but does not yet have a large evidence base.Purpose: Consequently, it is important to under-take research that expands this body of knowledge. Focus: This review aims to assess the confidenceof medical students in writing up abstracts for theirresearch, to gain a better overall picture of medicalstudents' feelings about undertaking and writing upresearch.Word count: 81

Informative Abstract Structured abstract includes the following heads: • Objectives: Illustrate the background and purpose of the review in one or two sentences in present tense. • Material and Methods: Write a few lines to present a general picture of the research methodology of article in past tense. • Result: Describe outcomes in few sentences.

Abstract There are two types of abstracts: one is informative abstract which describes the planned end product and result of the review manuscript or specifies the text structure. Second is descriptive abstract which describes the covered subject without specific details. Present tense will be used in the writing. Usually the length of abstract is 200 to 250 words.

Critical abstract A critical abstract is generally written about a different au-thor's work and contains all of the information mentionedabove, but also an element of evaluation or critical appraisalof the study, which may include discussion of the reliabilityand validity of the results (Labaree, 2018). For this purpose,references can be included to provide supporting evidence foryour arguments from relevant literature.The critical abstract includes information regarding thearticle e.g. author, title etc. and then briefly provides theirkey findings/conclusion. The main content of the abstractthen highlights the positives and negatives of the article.Examples of things to consider here could include: •How relevant is this research question? •Is the hypothesis clearly stated? •Type of study/trial/research? •What is the sample size? Is it large enough to providestatistically significant findings? •Were the methods used appropriate

and justified? Couldthey be improved? •Is the conclusion valid based on the evidence? •Are there any conflicts of interests?

Keywords

Dankbetuiging

Wie kan je zoal bedanken? Denk aan de begeleiders en voorbereiders van je afstudeerproject, familieleden en andere personen die je geadviseerd of gemotiveerd hebben. Het is gebruikelijk om dit voorafgaande aan het verslag te doen. Dit bedanken mag ook in de inleiding gebeuren. Bijvoorbeeld: Bij het opstellen van dit verslag heb ik dankbaar gebruik gemaakt van 'metathesis' van *Donald Craig (donald@mun.ca)*.

Inhoudsopgave

Trefwoorden

trefwoorden volgens de gebruikte thauserus. een thesaurus is een lijst vna goedgekeurde en geaccepteerde vaktermen, de 'controlled descriptors' met de verklaring en met de afgekeurde alternatieve vaktermen

Inleiding

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

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

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

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

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

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

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

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

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

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

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

Afbakening

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.

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

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

Wat is uppaal Wat is Uppaal Uppaal is an integrated tool environment for modeling, simulation and verification of real-time systems, developed jointly by Basic Research in Computer Science at Aalborg University in Denmark and the Department of Information Technology at Uppsala University in Sweden. It is appropriate for systems that can be modeled as a collection of non-deterministic processes with finite control structure and real-valued clocks, communicating through channels or shared variables [WPD94, LPW97b]. Typical application areas include real-time controllers and communication protocols in particular, those where timing aspects are critical.

model checking

Wat is statistical model checking? Dit verwijst naar verschillende technieken dfie worden gebruikt voor de monitoring van een systeem. Daarbij wordt vooral gelet op een specifieke eigenschap. Met de resultaten van de statsitieken wordt de juistheid van een ontwerp beoordeeld. Statistisch model checking wordt onder andere toegepast in systeembiologie, software engineering en industriele toepassingen. https://www-verimag.imag.fr/Statistical-Model-Checking-814.html?lang=en: :text=Statistical

[**?**] [**?**] [**?**]

Waarom gebruiken we statistisch model checking? To overcome the above difficulties we propose to work with Statistical Model Checking [KZHHJ09,You05,You06,SVA04,SVA05,SVA05b] an approach that has recently been proposed as an alternative to avoid an exhaustive exploration of the state-space of the model. The core idea of the approach is to conduct some simulations of the system, monitor them, and then use results from the statistic area (including sequential hypothesis testing or Monte Carlo simulation) in order to decide whether the system satisfies the property or not with some degree of confidence. By nature, SMC is a compromise between testing and classical model checking techniques. Simulation-based methods are known to be far less memory and time intensive than exhaustive ones, and are oftentimes the only option. https://project.inria.fr/plasma-lab/statistical-model-checking/

Alternatief Alternatieven voor Uppaal zijn Asynchronous Events,Vesta en MRMC.

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.

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

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

Controlled variabelen: door actuatoren fenomenen uit de omgeving For example, monitored variables might be the pressure and temperature inside a nuclear reactor while controlled variables might be visual and audible alarms, as well as the trip signal that initiates a reactor shutdown; whenever the temperature or pressure reach abnormal values, the alarms go off and the shutdown procedure is initiated

Input variabelen: data die de software als input gebruikt Here, IN models the input hardware interface (sensors and analog-to-digital converters) and relates values of monitored variables to values of input variables in the software. The input variables model the information about the environment that is available to the software. For example, IN might model a pressure sensor that converts temperature values to analog voltages; these voltages are then converted via an A/D converter to integer values stored in a register accesible to the software.

Output variabelen: data die de software levert als output The output hardware interface (digital-to-analog converters and actuators) is modelled by OUT, which relates values of the output variables of the software to values of controlled variables. An output variable might be, for instance, a boolean variable set by the software with the understanding that the value true indicates that a reactor shutdown should occur and the value false indicates the opposite

6 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 ondersteuning 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.

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.

Requirementsengineering Om de juiste requirements te verzamelen en selecteren hebben we meer kennis nodig van de methoden hiervoor gebruikt in het domein van requirementsengineering. Daarom is een literatuurstudie gedaan naar rapporten en artikelen die ons meer informatie over dit onderwerp verschaffen. Uitdagingen in requirementsengineering zijn incomplete requirements en specifcates, veranderende requirements en specificates en grote, complexe oftwaresystemen.

Het article the worlds a stage biedt inzicht in de requirementstechnieken voor een ambulance in london. In het artikel gaan de onderzoeks in op de volgende onderwerpen: viewpoints, sociale ascpecten,evolutie, 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

Het artikel "from inconsistencyhandling to non-conanical requirements management: a logical perspective"geeft enkele tips voor het omgaan met inconsistente requirements:

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

Het artikel "managing inconsistent specification: reasoning, analysis, action"zoekt een ontologische benadering voor het omgaan met inconsistenties in de requirements specificaties. Voor de omshrijving van een specificatie kun je gebruik maken van logica. Daarbij kun je onderschei maken in klasieke logica quasi -logica. Wat ook een rol kan spelen in domain interpretatie. De achtergrond van de gebruikers speelt ook een rol. Zo is er e=onderscheid te maken in de volgende groepen: users, customers, domain experts, designers,, manufacturers graphical textual specification

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

Hoe kan een systeem verder worden ontworpen op een manier dat non-functionele requirements worden geimplementeerd? Hoe hangt dat ontwerp samen met aanpassingen van het functionele en structurele aspect van het systeem?

block[objects, classes, methods, messages, inheritance] [goals,agents, alternative, events, actions,existence modalities,agent responsibilities]

Het artikel "representing and using nonfunctional requirements: a process-oriented approach gaat in op een het proces van requirements acquisitie. Hierbij in ogenschouw de acquisitie van prestaties, ontwerp en aanpasbaarheid. product oriented process oriented

Acquisitie Prestaties user concern -Hoe goed werkt het product -Hoe goed wordt de bron gebruikt?» Efficiency -How veilig is het product » integrity -Met hoeveel zekerheid is uit te sluiten dat het werkt »Reliability -Hoe goed werkt het product onder zware omstandigheden » sustainability -Hoe makkelijk is het product in gebruik » usability quality attribute

Acquisitie: Ontwerp user concern Hoe valide is het ontwerp -Is ht ontwerp conform de requirements -hoe makkelijk is het ontwerp te repareren -Hoe makkelijk zijn de prestaties te verifieren

quality attribute

Acquisitie: Aanpasbaarheid user concern -hoe makkelijk is het om het product aan te passen - hoe makkelijk is het om het product te updaten en/of uitbreiden» expendability - hoe makkelijk is het om een wijziging door te voeren»flexibility -hoe makkelijk is het om andere system aan te sluiten » portability - hoe makkelijk is het om het product te transporteren » interoperability -hoe makkelijk is het om te converteren tot een systeem gebruiksklaar voor communiceren met andere systemen» reaseability quality attribute

[7] [**?**] [**?**] [**?**] [**?**] [**?**] [**?**]

what is a good software specification

[558] [559] [560] [561] [562] [563] [564] [565]

Wat is een sluis

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.

Studie naar rampen aan de hand van het vier variabelen model Voor deze studie is onderzoek gedaan naar verschillende rampen aan de hand van het vier variabelen model. Elke ramp op deze manier categoriseren kan ons helpen te bepalen in hoeverre requirements een rol kunnen spelen in de veiligheid van ons model. Zo is er de bijlmerramp [**?**] , deze vond plaats op 04/10/1994. Dan nog de ramp turkisch airlines vlucht 1951 op woensdag 25 februari 2009 [**?**] [401] [403] [404] [405] [406] [407] [408] [409].

De therac-25 June 1985 and January 1987. Medical lineair accelerators accelerate electrons to createhighenergy beams that can destroy tumors with minimal impact on the surrounding healthy tissue. In the mid-1970s, AECL, developed a radical new "double-pass"concept for electron acceleration. A double passaccelerator needs much less spaceto develop comparableenergy levels because it folds the long physical mechanismrequired to accelerate the electros, and it is more economic to produce. Using this double pass concept AECL designed the Therac-25, a dual mode lineair acelerator that can deliver either photonsat 25 MeVor electrons at various energy levels. Compared with theTerac-20 The Thrac-25 is notably more compact,, more versatile, and arguably easier to use. The higejr energy takes advantage of the phenomenon "depth dose": As the energy increases, the depth in the body at which maximum dose buildup occurs alse increases, sparing the tissue above the target area. First, like the Therac-6 and the Therac-20, the Therac25 is conrolled by a PDP11. The Terac-6and Therac-20 had been designed around machines that already had histories of clinical use without computer control. The therac-20 has idependent protective circuits for monitoring electron-beam scanning, plus mechanical interlocks for policing the machine and ensuring safe operation. Finally some software for the machines was interrlatd or reused. Eleven therac-25 were installed: five in the usand six in canada. Six accidents involving massive oerdoses to patients occured between 1985 and 1987. The machine was recalled in 1987 for extensive design changes, including hardware safeguards against errors. Kennestone Regional Oncology

Center 1985 Door rechtzaken waren managegers op de hoogte van de problemen en ongelukken. Maar er werd in het vervolg niet over gerapporteerd. The treatment prescription printout failure was disabled at the time of the accident , so there was no hardcopyof the treatment data. Ontario Cancer Foundation in 1985 Since the machine did not suspendand the control display indicated no dose was delivered to the patient, the operator went ahead with a second attempt at trratment by pressing the "P"key, expecting the machine to deliver the proper dose this time. This was standard operating procedure and, described in the "The operating interfaceön p 24, Therac 25 oprators had become accustomed to freunt malfunctions that had no untowardconsequences for the patient. Again, the machine shut downin the same manner. The oeprator repeated this process four times after the original attempt- the display showing "no dose"delivered to the patient each time. After th fifth pause, the machine went into treatment suspedn, and a hospital service technician was called. The technician found nothing wrong with the machine. This was not an unusual scenario, according to the Therac-26 operator Manufactureere response Government and user response Yakima Valley Memorial Hospital in 1985 Manufactureere response Government and user response East Texas Cncer Center, March 1986 Manufactureere response Government and user response East Texas Cncer Center, April 1986 Manufactureere response Government and user response Yakima Valley Memorial Hospital Manufactureere response Government and user response [112], [114], [116], [117], [118], [119], [122], [123], [124], [125], [126], [127], [128], [129], [130], [131],[132], [133], [134], [135], [136], [137], [138], [139], [140], [**?**], [142], [143], [144], [149].

tesla autopilot features voor dataverzameling[352],[334]. De eerste tesla crash is van juni 2016 `https://impakter.com/tesla-autopilot-crashes-with-at-least-a-dozen-dead-whos-fault-man-or-machine/#:~:text=The%20first%20known%20death%20reportedly,trailer%20against%20the%20bright%20sky.`. En meerdere zouden volgen. Een ongeluk in de VS waarbij 2 inzittenden om het leven kwamen. Een persoon had plaats genomen als bijrijder en de andere persoon als passagier achter de stoel van de bestuurder. Waarschijnlijk was de autopiloot niet ingeschakeld. [**?**],[396],[395],[393],[388],[374],[369],[349],[342] De situatie en oorzaken zijn bij elke ramp verschillend. Een automobilist heeft in een rit van 37 minuten slechts 25 seconden zijn handen aan het suur gehad ondanks de melding "Hands requireed not detected". Hiermee zijn de onderzoekers van de NTSB ervan uitgegaan dat de bestuurder de autopiloot bewschouwde als een volledig autonooom rijsyssteem in plaatst van een veligheidsmechanisme [**?**]. Of in Mei 2015 als een besuurde foto's van zichzelf maakt in de testla zonder handen aan het stuur of voeten op het pedaal. [**?**] Een faatale crash in 2016 waarbij de bestuurder e veel vertrouwde op het semi-autonome rijtechnologie op het verkeerde type wegdek. [**?**] Onderzoek naar een fatale crash op 7 mei 2016 toont aan dat er beperkingen zitten aan de autopilot mode. Om specifiek te zijin is de automatische noodrem niet failsafe, blijkt uit onderzoek. [**?**] [**?**] [**?**] Op April 17 2019 een autocrash waarbij het onduidelijk is of de autopiloot aan stond. [**?**]. Een auto ongelu waarbij een tesla is betrokken. De bestuurder was waarschijnlijk afgeleid door de games op zijn apple telefoon. De NTSB gaf aan dat het crash-avoidance systeem neit otnworpen is en ook geen crash atnuaor heeft gedetecteerd. Herdoor accelereerde de autopilot het voertuig. Ook Faalde het systeem in het verschaffen van een crash aleter en werden de noodremmen niet geactiveerd. [397] Er is ook een melding van een tesla waarvan de autopilot bots tegen een stilstaande politieauto [**?**]. Ook uit dit onderzoek blijkt dat er geen gebreken waren en dat het automaische remsysteem neit kapot was. De HNTSA concludeerder dat de bestuurder zelf geen actie ondernam door bij te sturen of te remmen. In een eerder artikel kwam naar voren dat de tesla een autopilot krijgt die enkel camera's en GPS gebruikt; lidar of een radarsysteem wordt niet toegepast. [**?**] Enkele fotos van crashes met autonome rijsysstemen [384]. [386] [394], [297], [300] Tesla autopilot crashes met meer crashes en incidenten dan tot dan toe gerapporteerd [317] De meest voorkomende crashes zijn stationaire objecten bij hoge snelheden, lane incursions from stationary objects, auti=opilot confusion at forks and gores. [318] [319] [320] De veiligheidsrisicos van de tesla lopen uiteen. Zo zijn er risicos in de machinelearning technologie: veiigheidsrisico Three Small Stickers in Intersection Can Cause Tesla Autopilot to Swerve Into Wrong Lane [289], [291],de autopilot zelf [295]. Een studie door de consumntenbond in de VS toont aan dat hetautopilot systeem van de testla niet failsafe is. Zo zijn de sensoren, gebrukt voor detectie van een bestuurder negatief te beinvloeden. [348] Maar ook andere problemen met de bluetooth [292], touch screen [293], Web-based attack crashes Tesla driver interface [298]. Of zelfds de tesla batterij is veiligheidsvraagstuk geworden [302]. Maar

ook was een onderzoeker was in staat om persoonlijke details van afgedankte voertuigonderdelen te vekrijgen nadat deze waren afgekeurd vanwege upgrades en reparaties op consumentenvoertuigen. [304] Data-opslag in de cloud niet altijd bereikbaar. [351] dodelijk ongeluk [311], softwarefout maakt diestal mogelijk [314] fouten ontdekt in onderzoek [316], tesla cloud gehacked [332]. This analysis considers the potential impacts of completely self-driving vehicles on vehicular liability. [360] Dan zijn er nog maatschappelijke problemen die de aanpak moeilijker maken. Er is in de vs in verschillende staten een andere wetgeving [344] [345] [346] Toch zijn er oplossingen en tegenmaatregelen. tesla gaat advanced driver assistance systems inzetten met behulp van passive visual, ultrasonic, en radar. [359],[354] Safe system solutions door David Harkey [361] Voor elke auto uitgerust met een level 2 tot level 5 autonomy wordt nu standaard een rapport van van de crash opgvraagd door de NTSA. Dit in het kader van verder onderzoek waarbij de autoritait kijk naar ziekenhuisbehandeling, fataliteit, airbag deployment. [371].

De slmramp op 07/06/1989 [460],[463] [464],[465],[466], [467],[468], [470],[471],[472], [473],[475],[476],[477],[478],[479],[480],[481].

De schipholbrand op 27/10/2005[426],[426],[427], [428],[429],[432],[434],[438],[439], [425],[426],[427],[428],[429],[430],[431],[432], [434],[438],[439].

De explosie tanjin china 12/08/2015. Op 12 augustus 2015. Er waren twee explosies bij de Rulthai logistiek faciliteit zorgde voor de opslag vn gevaarlijke stoffen. De explosie zorgde voor de vernietiging van 12000 voertuigen, schade aan 17000 huize binnen een traal van 1 km. Er waren 173 doden inclusief brandweermensen. Een van de explosies zorgde voor een beving van 2.3 op de schaal van rigter. De volgende factoren zouden een rol hebben gepeeld: Een onjuiste afbakening van het opslagmaeriaal Er was weinig kennis bij de autoriteiten over opslagmaterialen. Zo bleek er 7000 ton aan materiaal opgeslagen, dat is ruim 70 keer te maximaal toegestande hoeveelheid. Onverenigbaar grondgebruik in de nabije omgeving. Veel woonwijken met nar schatting 6000000 bewoners en 500 lokale bedrijvenin de buurt van de opslag gevaarlijke stoffen. Opgeslagen materialen waren: calcium carbine, sodium nitraat, potassium nitraat, amminiak nitraat en cyanide. Ook is er veel kritiek geweest op de acties van de autoriteiten. Zo was er censuur vanuit de overheid op de journalistiek. Ook was er naar alle warschijnlijkheid sprake van corruptie. Zo bleek achteraf dat een van de grootste aandeelhouders Dong Shexuang de zoon te zijn van een oud-politiechef in Tanjin haven, genaamd Dong Pijun De overheid beloofde strengere toezicht en alle bedrijven moeten een risico-inventariatie maken en onderhouden[**?**], [**?**],[**?**], [215],[220],[223],[224],[225],[226], [227],[228],[229],[230], [231],[232],[235],[236], [238],[239],[240],[241],[242],[243],[245],[246], [247],[248], [249],[**?**],[**?**], [**?**],[252],[253], [255],[273],[274],[275],[276],[278],[280],[281],[282],[283], [284],[285],[287], [288].

De ethiopian airlinesop 10/03/2019[**?**],[664], [665],[666],[667], [670],[671], De oorzaak is de MCAS [672],[677], [673],[682],[683],[684],[687],[688],[699],[705], als een single point of failure [**?**] Angle-of-attack[674], Behalve de MCAS waren er nog andere failures[675], en ook deze failures [703] [676], safety record van de boeing [679], Oplossingen zijn [692].

Het mortierongeluk in Mali op 06/04/2016. Aanwezige militair brengt slachtoffer naar de fransen, vervolgens naar de Tongolezen. Maar de kwaliteit van personeel liet te wensen over. Er werd een Nederlandse arts overgevlogen. De slachtoffers werden overgevlogen naar Gao omvervolgens te worden oergevolgen naar Nederland. Het ongeluk werd veroorzaakt door een kapot afsluitplaatje in de mortier. De granaat opslag in een niet gekoelde container. Dan was er vocht in de fatale granaat. Zodoende werden er explosieve stoffen gevormd in de granaat. Tijdens de oefening werden de granaten warm in de zon. De granaat stond in veilie stand kon de explosie niet voorkomen. [**?**] [410] [411] [412] [413] [414] [415] [416] [418] [419] [420]

De ramp tjernobyl 26/04/1986. [**?**] De mislukte veiligheidscontrole op 26 apeil 1986 01.24 uurin de sovjetuni leiddte tot explosies in een van de reactoren in de kerncentrale. De reactoren hadden geen veiligheidomhulling en de reactor bevat grote hoeveelheden brandbaar grafiet. Door de explosie en de brand kwamen er radioactieve stoffen vrij.het gaat helemaal mis in de kernreactor 4. De warmteproductie nam toe met een explosie tot gevolg. 31 mensen kwamen om, waaron veel mensen dagen later door stralingsziekte. [483], [484], [485], [486], [487], [488], [489], [490], [491], [**?**], [493], [494], [496], [497], [498], [499],[500], [501],[503], [504],[505],[506],[507],[508]

Research case: De digitale aanval op de Oekrainese krachtcentrale op 23,december 2015

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. [63] [**?**] [64] [509] [511] [513] [515] [519] [520] [521] [522] 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. [63],[64],[42],[58],[59],[60],[61],[515],[62]. 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. [63] Uit onderzoek[64] 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. Oekraine wijst naar de russen [64], [**?**], [42], [56], [55], [54], [53]. Situatie Oekraiene [52], [51]. Situatie algemeen [511], [59], [49]. Factoren [48] Oorzaak [27], [47], [46], [51]. Gebruikte materialen [44], [43] Uitvoering van de aanval [63], [42]. Oplossingen [63] [63] [42] spearfishing blackenergy remote access capabilities serial-to-ethernet communication devices telephony denial of service attacks 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. [63] Discussie Verder lezen [41], [513], [39], [38], [37],[36],[35],[34],[33],[33],[32],[31],[30],[29],[28],[26],[25],[24].

Dan zijn er nog andere ongelukken met de stint, de shietpartij op militairencomplex in ossendrecht, stint-ongeluk, de enschedese vuurwerkramp en de molukse treinkaping. Meer recentelijk de coronacrisis.

Safety critical systems https://www.icheme.org/media/8976/xxiv-poster-11.pdf https://crpit.scem.westernsydney.edu.au/confpapers/CRPITV55Chambers.pdf https://users.ece.cmu.edu/ koopman/des$_s$99/$safety_critical$/$WHATARESAFETY - CRITICALSYSTEMS$?

Traditional Systems Traditional areas that have been considered the home of safetycritical systems include medical care, commercial aircraft, nuclear power, and weapons. Failure in these areas can quickly lead to human life being put in danger, loss of equipment, and so on.

Non-traditional Systems Emergency 911 service is an example of a critical infrastructure application. Other examples are transportation control, banking and financial systems, electricity generation and distribution, telecommunications, and the management of water systems

4.1 Technology

https://users.encs.concordia.ca/ ymzhang/courses/reliability/ICSE02Knight.pdf https://www.dcs.gla.ac.uk/ johnson/teaching/safety/slides/pt2.pdf https://www.dau.edu/tools/sebrainbook/Pages/Designhttps://daytonaero.com/wp-content/uploads/AC-17-01.pdf https://nebula.esa.int/content/assessment-methodology-certification-safety-gnc-critical-space-

systems https://www.cs.unc.edu/ anderson/teach/comp790/papers/safety$_{c}ritical_{a}rch.pdfhttps$: $//www.cs.uct.ac.za/mit_{n}otes/human_{c}omputer_{i}nteraction/htmls/ch02s10.html$

1. The Assembly is aware that the use of computers in safety-related applications is growing, particularly in areas such as control systems of aeroplanes, high-speed trains and nuclear power stations, medical equipment and medical records, anti-lock braking systems for vehicles and machine engineering in general, and last but not least, modern weapons and their guidance systems.

2. Many recent accidents (for example, plane crashes due to computer failure, malfunctioning robot killing a mechanic, patient dying because of malfunctioning of computer-controlled intravenous drip, rocket launch failure traced to computer error, software piracy etc.) cause public concern and raise the question of the reliability of such systems.

How has the problem of safety-critical software arisen? Essentially from an ever-increasing complexity in engineering. One may compare the steam locomotive of 1830 with the APOLLO Moon spacecraft of 1970 as an example. In 1917 WM FARREN designed, supervised the construction of and testflew an aircraft - the CE 1 and with acceptable safety! [2]. Even in 1965 a chief designer would be familiar with all the decisions taken in the design of a complex product such as an aircraft or ship. The management operation was deeply hierarchical [3] , but as systems became more complex and design teams included more and more specialists it became necessary to formalise the interfaces between the specialist groups to gain benefit and yet maintain overall design disciplines. This led to the matrix design management system in the 1970s to cope with design teams 50 times larger than before [4].

A difficulty embodied in tackling the safety related to software in engineered products arises because of software complexity and the mathematical rigour of some parts of it distorts and clouds the fundamental processes of creative engineering design.

Before discussing safety definitions and integrity a brief mention of design techniques to enhance safety. One way of increasing safety is to develop more reliable components and systems. At the outset, once the general preliminary design is defined there will be a "safety budgetällocating tolerable levels of integrity for every subsystem. Then Reliability Analysis evaluates the probability of failure and Failure Mode Effect and Criticality Analysis deals with the likely results of failure. Once the "lifeöf a part has been measured then the inspection and maintenance function will act to replace the part with a new one in good time. Another technique is to design an item to "fail-safeï.e. even if it does fail it does not create a safety risk before the fault can be rectified. This has been extensively used on structures and coping with the development of fatigue cracks. "Fail- operate", "fault tolerant designänd "graceful degradation of systemsäre other methods.

https://www.egbc.ca/getmedia/78073fda-5a83-4f0f-b12f-0a40dcbbc29d/EGBC-Safety-Critical-Software-V1-0.pdf.aspx https://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewHTML.asp?FileID=7144lang=EN https://www.dlr.de/ft/en/desktopdefault.aspx/tabid-1360/1856$_{r}ead-36215/https://ieeexplore.ieee.org/document/1007998https://coreavi.com/the-future-of-safety-critical-systems-in-the-emerging-autonomous-world/https://verticalmag.com/features/whensafetymanagementsystemsfail/$

fault stress cause consequence analysis hazops fmeca/fha/fmea fmeca = failure modes, effect and criticality anaysis step 1 functional block diagram setp 2 idendity failure modes (complete failures, partial failure, intermittant failure, gradual failure) step 3 accesss criticality step 4 repeat for potential consequences step 5 identify cause and occurence rate step 6 deteermine detection failures -type 1 the controls prevent the cause of failure mode from occuring, or reduce their rate of occurence -type 2 hes controls detect the cause of the failure mode and the lead to corrective action -type 3 these controls detect the failure mode before the product operaton, subsequent operations, or the end user step 7 calculate risk priority numbers RPN = secerity index * occurence index * detection index step 8 finalyze hazard analysis pra is aprt of hazard analysis, probaility risk analysis, the probability that product will work for T withour failure, R(T) = exp(-T/MTTF) decision theory risk = frequency * cost mttf Bellcore: reliability prediction procedure

Criticality level

36 41 58 59 62 73 84 104 Safety-critical software development Software designed by -hazard elmination -hazard reduction -hazrd controls Software implementation issues -dangerous practices -choie of safe languages 105 leveson taxonomy of design techniques -hazard elimination/avoidance: substitution, elimination, decoupling, human error removal, removal of hazardous materials -hazrd reduction: –design for control -incremental control -intermediate states -decision aids -monitoring – add barriers -hard/software lcoks –minimize single point failures -increase safety margins -exploit redundancy -allow for recovery

-hazard control: limit eposure (back to normal fast exceptions), isolate and contain (dont let things get worse, fail-safe (panic shut downs and watchdog code -hazard minimization software desigg techniques: fault taulerance -avoid common mode failures -nred for design diversity - samre requiremenrs, different programmers, different contractors, -redundant hardware mau duplicate, any faults if software is the same - N-version programming, shared requirements or diffrent implementations where voring ensures agreement -what about timing differences, comparison of continous values, wha is requirements wrong, performance of cost voting -exception handling emchanism - use run-time system to detect faults by raising exceptions or pass control to appropriate handler -propagate o outmost scope hen fail -recovery blocks: write acceptance test for modules, if it failes then eecut alternative -must be able to restore the states: take a sapshot/checkpoint, if failure then restore snapshot -control redundancy inclues: N-version programming, recovery blocks, exception handling -error detecting/correcting codes -chcksum agreements -no task scheduler but bare machine -restrict language subsets -memory jumps -overwrites -semantics -precision: interger, floating point, oeprations... -data typing issues -exception handling: is runtime recovery supported -memory monitoring: guard againt memory depletion -separate compilation by typw checking agross modules

software development -planning proces * coordinate development activities -software development processes * requirements proces * design process * coding process * integration proces -software integral processes * verification proces * configuration management * quality assurance 8 certification liaison sofwtare developmnt key issues - traceability and lifecycle focus -designed engineering reps - recommended practices -design verification -design validation

safety-critical software developemnt conclusions -software design by * hazard elimination * hazard reduction * hazard control - software implementation issues: dangerous practices and choice of safe languages Hardware Design: fault tolerant architectures -the basiscs of hardware management *preferred pars list * vendor and device selection * critical devices, techniques and vendors * device specifications * sccreening * part obsolescence *FRACAS (Failure reporting, Analysis and corrective Action Types of faults: * Design faults: erroneous requirements, erroneous software, erroneous hardware * management/ regulators * Intermittent faults -fault occurs and recurs over time -fault connections can recur * Transient faults - fault occurs but may not recurr -electromagnetif interference * Permanent faults: - fault persists -physical damage to processor - fault models -hardware redundancy

Software faults -specification errors -coding errors - tranaltion errors -runtime errors

Active redundancy Standby redundancy Triple Modular redundancy

Fault detection -runctionality checks * routine to check hardware works -signal comparisons * copare signal in same units -information redundancy * parity checking, M out of N codes -watchdog times * reset if system times out -bus monitoring * check processor is alive -power monitoring * time to respond if power is lost

Validation and verification -Verifiction is about proof and proof is about argument and an argument must be correct but not a mathematical holy grail * does it meet the requirements - show that implementation is same as functional requirements - too costly and time consuming all safety behaviour in specification verification supported by: * determinism (repeted tests) * separate safety-critical functions * well defined processes * simplucity and decoupling -Validation * are the requirements any good -during design * external review before commission * external review before commission -during implementation * additional constainrs discovered * additional requirements emmerges -during operations * were the asumptions valid * especialy environental factors Validation summary of key issues -who validates

validator * external agenets must be approved -who validates validation * clarify links to certification - what happens if validation fails * must have feedback mechanism * lnks to process improvement

222 228 mode confusion 241 individul human error - slips, lapses and mistakes - rasmussen: skill, rules, knowledge - reason,generic error modelling - risk homeostasis 242 what is error * deviation from optimal performance - very vieuw achieve the optimal * failure to achieve desired outcome -desired outcome can be unsafe * departure from intended plan -but environment may hange plan 244 types of errors - slips * correct plan but incorrect action * more readily observed -lapses * correct plan but incorrect action * failure of memory so more covert -mistakes * incorrect plan * more complex, less understood -human error modeling *analyse/distinguish error types 247 Skills, rules and knowledge: SKR -signals *sensory data from environment * continuous variables *Gibson direct perception -signs * indicate state of the environment * with conventions for action * activate stored pater into action -symbols * can be formally processed 8 related by convention to state 248 -skill-bases errors * variability if human performance -rule based errors * isclassification of situations * application fo wring rule * incorrect recoll of correct rule -knowdlegedebased errors * incomplete/incorrect knwoledge * worload and external constraints 249 - How do we account for slips ansd lapsesin SKR? can we distinguish more detailed error forms and more diverse error forms? Before an error is detected the operation is typically skill based 250 Monitoring failures -Normal monitoring * typical berore error is spotted * preoprogrammed behaviours plus * attentional checks on progress -Attentional checks * are actions acording to plan? * willl plan still achieve outcome - Failure in the checks pften leads to a slip or a lapse -Reason also identifies overattention failues 251 Problem solving failures -humans are pattern matchers * prefer to use rules * before effort of nkkowledge level -local state information * idexes stored problem hadling * schemata, frames, scripts -misapplication of good rules * incorrect situation assessment * over-generatisation of rules -application of bad rules * encoding deficiencies * action deficiencies 252 knowledge based failures -thematic vagabonding * superficial analysis/ behaviour * fit from issues to issue -encysting * myopic attention to small details * metal-level issues may be ignored -reason * individual fails to recognise failure * does not face up to consequences

254 GEMS: Error detection - dont try to elmininate errors but focus on their detection -self monitoring * correction of postural deviations * correction of motor responses * detecton of speech errors * detection of actin slips *detection of problem solving error -how do we support these activities * standard checks procedures * error hypotheses or suspicion * use simulation based training 255 256 258 GEMS: practical application -Eliminate error affoardancecs * increase visibility of task * show users constraints on action -Decision support systems * dont just present events * provide trend information * what if subjunctve displays * prostheses/ mental crushes -Memory aids for maintainance * often overlooked *aviation task cards * must maintain minatainance data -improve training * procedures or heuristics * simulator or training -error management * avoid high-risk strategies * high probability/cost of failure -ecological interface design * rasmussen and vincente 8 10 guidelines -self-awaireness * when might i make and error * contentious 261 GEMS outstanding issues -problem of intention * is an error a slip or lapse * is an error a mistake or intention -give an observations of error * afermath of accident/incident *guilt, insecurity, fear, anger -can we expect valid answers - can we make valid inferences 263 Risk Homeostasis theory 265 individual human error - slips, lapses and mistakes - rasmusses: skill, rules, knowledge - Reason: generic error modeling - Risk homeostasis 266 - workload -situation awareness -crew resource management 267 -high workload * stretches users resources -low workload * wasts user resources * can inhibit ability to respons -cannot be seen directly * is infered from behaviour 269 - various approaches * wickens on perceptual channels * kanwowiz on problem solving * hart on oer-all experience - holistic vs atomic approaches * FAA a gestalt concept * cannot measure in isolation * many xperimentalists disagree -single-user vs team approaches * workload is dynamic * shared/distributed between a team * many previous studies ignore this 270 Workload - how do we measure workload -subjective ratings * NASA TLX, task load index * consider individual differences -secondary tasks * performance on aditional task * obtrusive difficult to generalise -physiological measures * heart rate, skin temperture * lost of data but hard to interpret 271 - how to reduce workload -function allocation * staticof dynamic allocation * to crew, systems or others (ATC) -Automation * but it can increase workload * of change nature -Crew recourswe management *crew coordination * deision making * situation awareness * more revew activities isnerted into standard operating procedures [578] [579] [580] [583]

[585] [**?**] [589] [591] [**?**] [596] [600] [626] [633] [**?**] [**?**] [**?**] [**?**] [**?**]

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 [74] 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.

[**?**] Sluis Eefde kreeg niet alleen de onderhoudsbeurt, maar werd tevens uitgebreid met een tweede sluiskolk. Zo wil Rijkswaterstaat wachttijden voor de scheepvaart voorko

[77] 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.

[**?**] 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.

[**?**] 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.

[**?**] deltawerken

[**?**] 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 60%) was begin 2018 ook al uitgevoerd, maar Rijkswaterstaat ziet onvoldoende toe op de uitvoering van het resterend deel en heeft geen actueel overzicht van de overgebleven maatregelen. De 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.

[**?**] 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.

[**?**] Rittal doet onderzoek naarop afstand besdienbare sluizen

[**?**] Beveiligde VPN M2M Services levert aan inmiddels 220 gemeenten en waterschappen beveiligde connectiviteitsoplossingen voor het beheer van pompen, riolen en gemalen. Om risico's op beveiligingsincidenten te voorkomen maken wij gebruik van een VPN oplossing, waarbij de verbinding optimaal beveiligd is middels encryptie en authenticatie.

[**?**] Veiligheid op het water én op het land Gebruik van lampbewaking

[**?**]

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/10.3389/frai.2020.00007/full [**?**] 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/rug01:001235489 https://cyberpsychology.eu/article/view/12270 [**?**]

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

Analyse

Conclusie

Uppaal model

Inleiding

De computation tree

0.0.1 Semantiek

Variable Because we require that the transition relation of a kripke structuer us always total, we must extend the relation R if some state s has no successor. In this case, we modify R so that R(s,s) holds. To illustrate the notions defined in this section we consider a simple system with variables x and y that range over D=0,1. Thus, a valuation for the variables x and y is justa pair $(d_1, d_2) \in$ D x Dwhre $d_1 is the value for x and d_2 is the value for y.$

A bestaat uit een 4-tuple M = { S , S_0,$\Re$, L } met daarin:
S: de verzamelingvan alle states in het systeem
$S_0 \subseteq$ S: de verzameling van alle beginstates
$\Re \subseteq$ S x S: de transitierelatie
L= S $\rightarrow$ 2^{AP} : de labels waarmee weiedere state labelen met atomaire propositiesdie waar zijn in die state

A clock relation limits the occurrences among different clocks/events, which are defined based on run and history. A run corresponds to an execution of the system model where the clocks tick/progress. The history of a clock c represents the number of times c has ticked currently. A probabilistic relation in PrCCSL is satisfied if and only if the probability of the relation constraint being satisfied is greater than or equal to the probability threshold p 2 [0; 1]. Given k runs = fR1; : : : ;Rkg, the probabilistic relations in PrCCSL, including subclock, coincidence, exclusion, precedence and causality are defined in Table II. bron Formal Verification of Dynamic and Stochastic Behaviors for Automotive Systems

About transition A transition is composed of a unique source location a unique target location a guard, i.e. an enabling condition (g := x clg g, where <, , =, , > a label (that can be used for synchronization) a subset (potentially empty) of clocks to be reset

a clock valuation is a function v: X R^+
v[Y:=0] is the valuation obtained from v by resetting clocks from Y:

$$v[Y:=0] = \begin{cases} 1, & 0\ x \in Y. \\ 0, & \text{otherwise.} \end{cases}$$

v+d = flow of time (d units)
(v +d)(x) = v(x)+d
v $\models$ c means that valuation v satisfies the constraint c

evaluation of a clock constraint (v $\models$ g)

1. $\vee \models$ g x < k iff (x) < k

2. $\vee \models$ x k iff (x) k

3. $\vee \models$ g1 g2 iff $\models$ g1 and $\models$ g2

(s', v") and (s,v) $\xrightarrow{a}$(s', v").

Action transitions correspond to the execution of a transition from T. We write (s,v) $\xrightarrow{a}$ (s', v'), where a $\in\Sigma$, provided that there is a transition $\langle$ s,a, φ, λ, s' $\rangle$ such that v satisfies φ and v=[λ:=0].

a delay transition (s, v1) $\rightarrow$ δ(d) (s, $v_1 + d_1$)$forsome$d$_1 \geq 0$, and an action transition (s, v1 +d1) $\xrightarrow{a}$ (s', v$'_1$)$suchthat$v$_1$ + d_1 satisfies φ and v'$_1 = (v_1 + d_1)$[λ:=0].

Real-time System = Discrete System + Clock Variables by Rajeev Alur

blz 2 actions The state of a system changes over time. We refer to the state changes of a system as actions. An action is a pair (σ,σ ') of states that consists of a source state σ and a target state σ '. Intuitively, if a system is in the source state σ, then the action (σ,σ ') takes the system into the target state σ'. We say that an action is enabled in its source state and disabled in all other states. Two actions (σ,σ '1) and (σ,σ '2) are consecutive if the second action is enabled in the target state of the first action|i.e., if (σ '1=σ '2). The action (σ,σ ') is a nul l action if (σ=σ ') .

blz 6 clocks and delays

Formally, the action (σ,σ ') is a system action if for all clock variables x, either σ '(x) = σ(x) or σ '(x) = 0; the action (σ,σ ') is a time action - or delay -if there is a nonnegative real δ the duration of the delay|such that σ ' = (σ,σ '). System actions have duration 0. Every null action is, by definition, both a system action and a delay of duration 0.

blz 7 Clock constraints Let (σ, δ) be a delay, let ϕ be a state predicate, and let ψ be an action predicate. The characteristic function of ϕ maps each nonnegative real e < δ to 1 if ϕ is true for σ + e, and otherwise to 0; the characteristic function of maps e to 1 iff ψ is enabled in σ + e. A state or action predicate varies

finitely over the delay (σ, δ) if its characteristic function has

nitely many discontinuities in the interval (0,δ). Abstractly, we restrict ourselves to state predicates and action predicates that vary

nitely over all delays.

blz 8 Clock-constrained systems A clock-constrained system S = (ϕ, ψ) is a pair that consists of a timed state predicate 0|the initial condition of S|and a timed action predicate ψ |the transition condition of S. The timed behavior σ is a behavior of the clock- constrained system S if (1) the initial condition of S is initially true for σ and (2) the transition condition of S is invariantly true for σ. Every clock-constrained system S de

nes, then, the set of its divergent behaviors, which is denoted by [[S]].

The transition relation R of τ(A) is obtained by combining the delay and action transitions. We will write (s,v) R(s', v') or (s, v) $[]f(x)$ (s', v') if there exists sänd v"such that (s,v) $\xrightarrow{d}$ (s", v")$\xrightarrow{a}$ (s', v') for some d $\in \Re$.

1 For a $\in \Sigma_1 \cap \Sigma_2, if\langle$ s1,a, φ, λ_1, s$'_1\rangle \in T_1$ and $\langle$ s2,a, φ, λ_2, s'_2 $\rangle \in T_2$ then T will contain the transition $\langle$ (s1,s2), a φ , $\lambda_1 \cup \lambda_2$, (s_1',s_2') $\rangle$ 2. For a $\in \Sigma_1$ - Σ_2, if $\langle$ s, a, φ, λ, s' $\in T_1$ and t $\in S_2$ then T will contain the transition $\langle$ (s,t),a, φ, λ, (s', t) $\rangle$ 3. For a $\in \Sigma_2 - \Sigma_1, if\langle$ s, a, φ, λ, s' $\in$ T$_2 and t \in S_1$ then T will contain the transition $\langle$ (t,s),a, φ, λ, (t,s') $\rangle$

$\xi \ldots \langle \overleftarrow{\ell_0}, v_0 \rangle$,

ξ(t) = $\langle \overleftarrow{\ell_0}, v \rangle | \exists i \in \mathbb{N} \bullet (t_i \leq t \leq t_{i+1} \wedge \overleftarrow{\ell} = \overleftarrow{\ell_i} \wedge v = v_i + t - t_i)$

is a sextuplet (L, '0, C, A, E, I), where L is a set of positions '0 L is the starting position, C is a set of clocks A is a set of actions, co-actions and internal -actions, E L × A × B(C) × 2 C × L is a set of edges between positions with action, guard and a set of clocks that are reset, and I : L → B(C) assigns invariants to positions.

Timed automation clock Clock evaluation is a function of u : C → R0 from a set of clocks to non-negative real numbers. Let R C be the set of all clock evaluations. Let u0(x) = 0 for all x C. Writing u I(‘) will mean that u satisfies I(‘). It is possible to make a transition from a given state using action or delay.

Timed Automata Semantics Let (L, ‘0, C, A, E, I) be a timed automaton. Semantics . . . a transition system with label hS, s0, →i, where S L × R C is a set of states, s0 = (‘0, u0) is the initial state, → S × (R0 A) × S is a transition relation such that (‘, u) d → (‘, u + d) if d 0 : 0 d 0 d = u + d 0 I(‘)

(‘, u) a→ (‘ 0 , u0) if e = (‘, a, g, r, ‘0) E e g, u0 = [r 7→ 0]u, u0 I(‘0),

u + d maps each clock x C every hour to the value u(x) + d, for d R0,

r 7→ 0]u indicates clock evaluation, which maps every clock in r to 0 and agrees with u over C r

Voor het modelleren van een systeemhebben we nodig:
alle states van het systeem.
We stoppen deze in een verzameling
S: de verzamleing van alle states van een systeem
Elke individuele state noemen we s_0, s_1,...s_n.

Ons model is een tupel met daarin de verzameling states: M(S)

De transities tussen states vormen een relatie R ⊆S xS

De systemen die wij modelleren zijn reactief:Systemenkunnen eindeloos rondjes lopen door een aantal toestanden.

Belangrijk gevolg: Voor elke state s geldt dat er een state s’ bestaat zodanig dat geldt R(s,s’)

Elke state heeft een uitgaande transities.
Een transitierelatie, waarin elke stateeen uitgaande transitie heeft noemt men totaal.
Alle transitierelatiesin de systemen die wij modelleren zijn totaal.

Om uitspraken te kunnen doen over ons systeem gebruiken we:
Een verzamelingatomaire poposities (AP):
proposities die niet verder op te delen zijnin kleinere/kortere proposities.

Een labeling functie: L De labeling L= S → 2^{AP} functie is een functie dieelke state "labeled"met een verrzameling atomaire propostities die waar zijn in die state.
bron Formal Verification of Dynamic and Stochastic Behaviors for Automotive Systems

De safety en reachability requirements die formeel zijn gespecificeerd worden in Uppaal geverifieerd met de A en E state formule. Andrerere opreratoren zijn

0.0.2 Formele specificaties: Queries

Reachability Query: Een veelvoorkomend type query is het controleren van de bereikbaarheid van een bepaalde toestand of toestandscombinatie in het systeem. Bijvoorbeeld, "Is het mogelijk om vanuit toestand A toestand B te bereiken?"

Is het mogelijk om vanuit toestand idle weer in toestand idle te komen? Is het mogelijk om vanuit toestand deurDownOpen in toestand deurUpOpen te komen?

Invariant Query: Een invariant is een eigenschap die altijd waar moet zijn tijdens de uitvoering van het systeem. Een query kan worden gebruikt om te controleren of een bepaalde toestand altijd aan een bepaalde voorwaarde voldoet. Bijvoorbeeld, "Is het zo dat altijd wanneer we in toestand C zijn, eigenschap X waar is?"

Is het zo dat altijd wanneer we in toestand deurDownClosed of deurUpClosed zijn, alle stoplichten op rood staan? Is het zo dat altijd wanneer er een stoplicht op groen is, het waterniveau gelijk is aan de minimum of maximum?

Liveness Query: Liveness verwijst naar de eigenschap dat bepaalde gebeurtenissen uiteindelijk zullen plaatsvinden. Een query kan worden gebruikt om te controleren of bepaalde gebeurtenissen in het systeem altijd zullen plaatsvinden, ongeacht de invoer. Bijvoorbeeld, "Zal gebeurtenis Y uiteindelijk altijd plaatsvinden?"

Reachability Specification: Een reachability-specificatie controleert of het mogelijk is om een bepaalde toestand of toestandscombinatie in het systeem te bereiken. Het kan worden uitgedrukt als "Er bestaat een pad vanuit toestand A naar toestand B."

Invariant Specification: Een invariant-specificatie controleert of een bepaalde eigenschap altijd waar moet zijn gedurende de uitvoering van het systeem. Bijvoorbeeld, "In toestand C moet eigenschap X altijd waar zijn."

Safety Specification: Een safety-specificatie controleert of een bepaalde eigenschap nooit wordt overtreden tijdens de uitvoering van het systeem. Het kan worden uitgedrukt als "Op elk pad door het systeem moet eigenschap Y nooit waar zijn."

Liveness Specification: Een liveness-specificatie controleert of bepaalde gebeurtenissen uiteindelijk altijd plaatsvinden. Het kan worden uitgedrukt als "Uiteindelijk zal gebeurtenis Z altijd optreden."

Fairness Specification: Een fairness-specificatie beschrijft de eerlijkheidsvereisten van het systeem en kan bepalen hoe bepaalde gebeurtenissen worden behandeld, zodat ze niet voor onbepaalde tijd kunnen worden vermeden.

Controleerbaarheidspecificatie: Een controleerbaarheidspecificatie geeft aan welke eigenschappen in het systeem kunnen worden gecontroleerd of welke aspecten van het systeem kunnen worden gestuurd.

Safety Safety Properties are used to verify that something bad will never happen. Dit kan worden gespecificeerd met de volgende vergelijking

Scope	CCTL proposities
It is true ...	
It is possible ...	E $\triangle$
it is inevitable ...	A $\triangle$
it is at all time true ...	AG
It is at all times possible	AG E$\triangle$
it is at all time inevitable	AG A$\triangle$
-	$\square(a_0 \implies ((\neg a_2 \wedge \neg a_3)\,\mathcal{U} a_1) \vee (\neg a_2 \wedge \neg a_3))$
AG(p)	M, s $\models AG(p) \Leftrightarrow \forall \pi \in \sqcap(M,s) \cdot \forall i \cdot M, \pi[i] \models p$
EG(p)	M, s $\models EG(p) \Leftrightarrow \exists \pi \in \sqcap(M,s) \cdot \forall i \cdot M, \pi[i] \models p$
AF(p)	M, s $\models AF(p) \Leftrightarrow \forall \pi \in \sqcap(M,s) \cdot \exists i \cdot M, \pi[i] \models p$
EF(p)	M, s $\models EG(p) \Leftrightarrow \exists \pi \in \sqcap(M,s) \cdot \forall i \cdot M, \pi[i] \models p$
AX(p)	M, s $\models AX(p) \Leftrightarrow \forall \pi \in \sqcap(M,s) \cdot M, \pi[1] \models p$
EX(p)	M, s $\models EX(p) \Leftrightarrow \forall \pi \in \sqcap(M,s) \cdot M, \pi[1] \models p$
A(p $\cup q$)	M, s $\models A(p \cup q) \Leftrightarrow \forall \pi \in \sqcap(M,s) \cdot \exists k \cdot M, \pi[k] \models q \wedge (\forall i \leq k \cdot M, \pi[i] \models p)$
E(p $\cup q$)	M, s $\models E(p \cup q) \Leftrightarrow \exists \pi \in \sqcap(M,s) \cdot \exists k \cdot M, \pi[k] \models q \wedge (\forall i \leq k \cdot M, \pi[i] \models p)$
A(p $\Re q$)	M, s $\models A(p \Re q) \Leftrightarrow \forall \pi \in \sqcap(M,s) \cdot \forall k \cdot \wedge(\forall i \leq k \cdot M, \pi[i] \models \neg p) = (M, \pi[k]] \models q$
E(p $\Re q$)	M, s $\models E(p \Re q) \Leftrightarrow \forall \pi \in \sqcap(M,s) \cdot \forall k \cdot \wedge(\forall i \leq k \cdot M, \pi[i] \models \neg p) = (M, \pi[k]] \models q$
-	

-	M, s $\models p \Leftrightarrow$ p $\in L(s)$
-	M, s $\models \not f 1 \Leftrightarrow$ M, s f1
-	M, s $\models f1 \vee f2 \Leftrightarrow$ M,s $\models f1 or M, sf2$
-	M, s $\models f1 \wedge f2 \Leftrightarrow$ M,s $\models f1 and M, sf2$
-	M, s $\models$ E$g_1 \Leftrightarrow$ there is a path $\pi from\ s\ such\ that\ M, \pi \models g1$
-	M, s $\models p \Leftrightarrow$ for every path $\pi\ starting from\ s, M, \pi \models g1$
-	M, s $\models p \Leftrightarrow$ s is the first state of M, s $\models f1$
-	M, s $\models \not g_1 \Leftrightarrow$ M, $\pi g1$
-	M, s $\models p \Leftrightarrow$ M, $\pi \models g1 or M, \pi M, \pi \models g2$
-	M, s $\models p \Leftrightarrow$ M, $\pi \models g1 and M, \pi M, \pi \models g2$
-	M, s $\models p \Leftrightarrow$ M, $\pi^1 \models g1$
-	M, s $\models p \Leftrightarrow$ there exists a k $\geq 0, such that\ M, \pi^k \models g1$
-	M, s $\models p \Leftrightarrow$ for all i $\geq 0, M, \pi^i \models g1$
-	M, s $\models g1g2 \Leftrightarrow$ there exists ak ≥ 0 *such that M*, $\pi^k \models g2$
-	and for all $0 \leq j < k, M, \pi^j \models g1$
-	M, s $\models p \Leftrightarrow$ for all j $\geq 0, iff\ for\ every\ i < j, M, \pi^i$ g1 then M,π^j $\models g2$

Tabel 1: Resolution suffixes

Main scope	CCTL Operations
-	
-	
-	
-	

Tabel 2: Resolution suffixes

AG $EF_{[x,y]} \vee$

A (every path") E (exists a path") X (

time") G (ör ") F (ör nally") U (") R (")

Requirement	queries
It is true ...	A[] not maincontroller.rd1 imply
It is possible ...	A[] maincontroller.rd1 imply
it is inevitable ...	A[] not deadlock imply
it is at all time true ...	E<> maincontroller.rd1 imply
It is at all times possible	E<> maincontroller.s7
it is at all time inevitable	E<> maincontroller.s7d

De computation tree

0.0.3 Evaluatie

$\forall x (P(x) \rightarrow Q(x)) premise$
$\forall x P(x) premise$

P(x_0)$\forall x$e 2
Q(x_0)$\rightarrow$ e 3, 4

$\forall x Q(x) \forall x$ i 3–5

{a,b} or †a,b
$\langle a, b \rangle or a, b$

f : $A \to B$

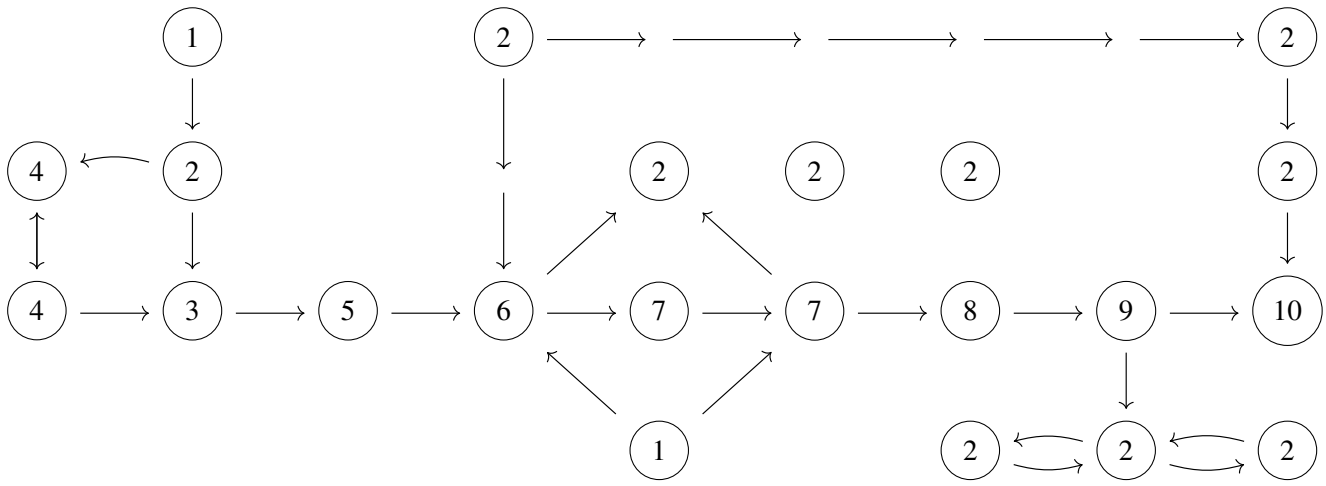
f $\circ g$
$x \mapsto f(x)$

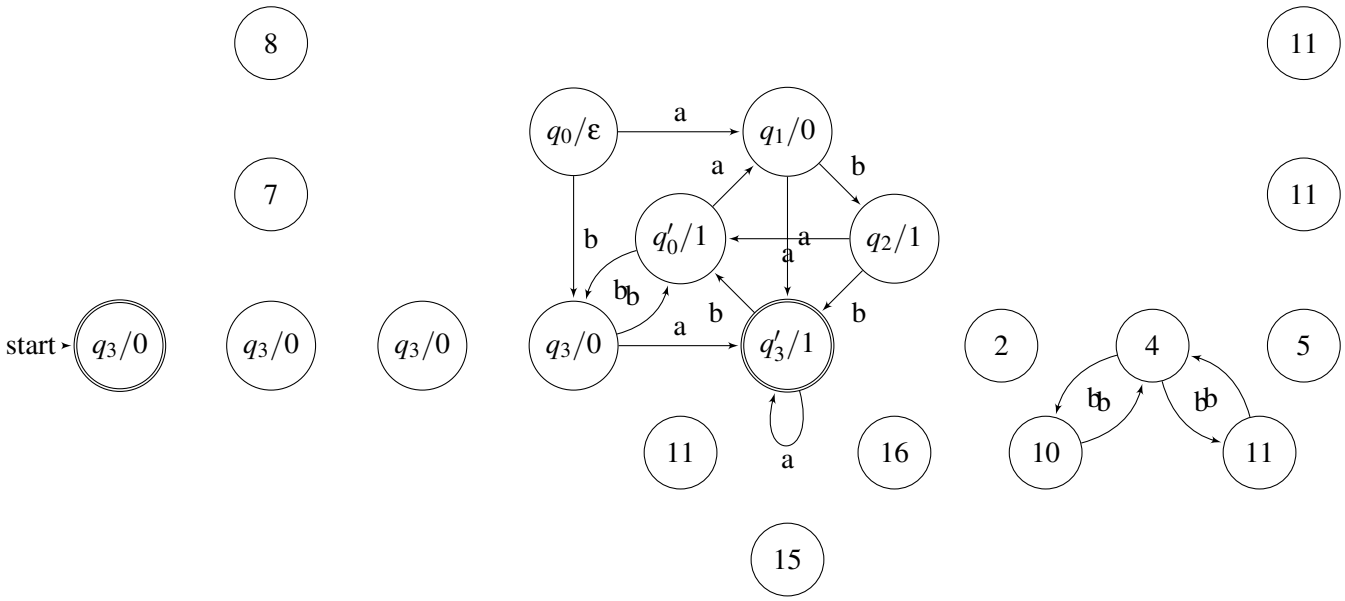
$$f \colon \mathbb{R} \to \mathbb{R}$$
$$x \mapsto x^2$$

$$\begin{array}{ccccccc}
ABCDE & \longleftrightarrow & F & \longrightarrow & G & \longrightarrow & H \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
ABCDEFGH & \longleftrightarrow & II & \longrightarrow & JJ & \longrightarrow & KK \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
ABCD & \longrightarrow & EEE & \longrightarrow & FFF & \longrightarrow & GGG
\end{array}$$

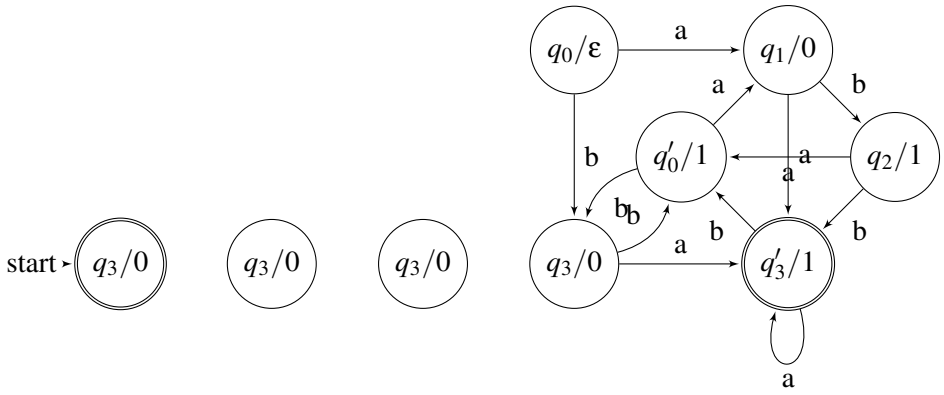
Models

Maincontroller

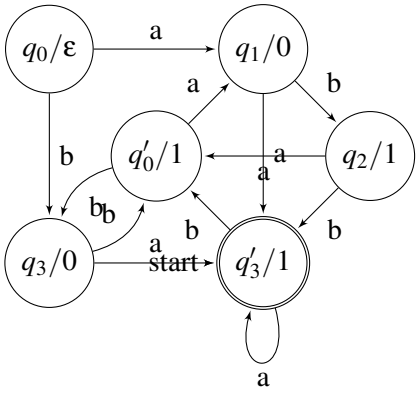




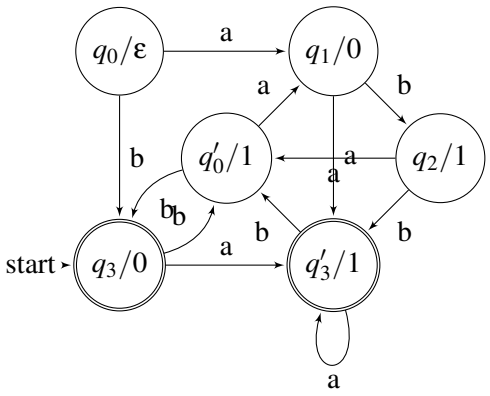
Labeling functions



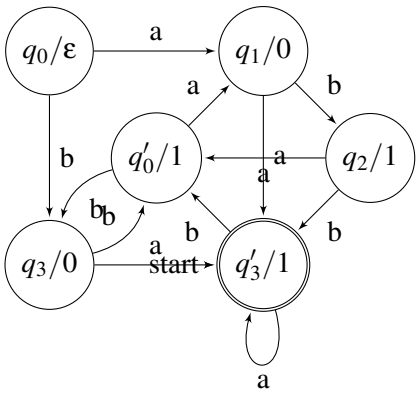
Schip



Deur



Stoplicht



pomp

Verificatie

We moeten aantonen dat een real-time programma voldoet aan de eisen opgesteld en gespecificeerd. De meest gebruikte methode voor het bewij

zen van de correctheid van untimed programma’s zijn aangepast voor timed programs. We hebben nog geen aanpask gevonden voor het gebruik en bewijzen van correct gebruik van clocks. Een bewijs voor het gebruik van real-time programmas met clocks is gegeven in T.A. Henzinger and P.W. Kopke. Verification methods for the di- vergent runs of clock systems

In dit hoofdstuk formaliseren we de requirements ogegeven in de requiremenstlis tin hoofdstuk .. en bewijzen we de correcte toepassing met gebruik van de symbolic model-checker van Uppaal. Het systeem is gemodelleerd als een netwerk van meerdere timed automata: controller, sluis, stoplicht, deur, pomp en schip.

Het bewijs vn corret gebruik kan ook worden aangetoond met help van bewijs voor inorrectgebruik

Verificatie resultaten

Het door ons uitgetippelde testpath of scenario

Timed automata

Data variabelen

Acties

Clock regions [?]

CTL logica Alle veiligheid en reachability requirements formeel gespecificeerd in hoofdstuk ... zijn geverifieerd in uppaal met gebruik an A en E state formulae. Deze zijn als volgt:

$M, s \models p \Leftrightarrow p \in L(s)$
$M, s \models \not f1 \Leftrightarrow M, s \;\; f1$
$M, s \models f1 \vee f2 \Leftrightarrow M,s \models f1$ or $M,s \;\; f2$
$M, s \models f1 \wedge f2 \Leftrightarrow M,s \models f1$ and $M,s \;\; f2$
$M, s \models E\, g_1 \Leftrightarrow$ there is a path π from s such that $M, \pi \models g1$
$M, s \models p \Leftrightarrow$ for every path π starting from s, $M, \pi \models g1$
$M, s \models p \Leftrightarrow$ s is the first state of $M, s \models f1$
$M, s \models \not g_1 \Leftrightarrow M, \pi \;\; g1$
$M, s \models p \Leftrightarrow M, \pi \models g1$ or $M, \pi\; M, \pi \models g2$
$M, s \models p \Leftrightarrow M, \pi \models g1$ and $M, \pi\; M, \pi \models g2$
$M, s \models p \Leftrightarrow M, \pi^1 \models g1$

M, s $\models$ p $\Leftrightarrow$ there exists a k $\geq$ 0, such that M, $\pi^k \models$ g1
M, s $\models$ p $\Leftrightarrow$ for all i $\geq$ 0,M,$\pi^i \models$ g1
M, s $\models$ g1 g2 $\Leftrightarrow$ there exists ak $\geq$ 0 such that M, $\pi^k \models$ g2
and for all 0 $\leq$ j < k, M,$\pi^j \models$ g1 M, s $\models$ p $\Leftrightarrow$ for all j $\geq$ 0, if for every i < j,M,π^i g1 then M,$\pi^j \models$ g2

Conclusie

Wat hebben alle bovenstaande rampen/ongelukken gemeen? Veiligheid. Bij de therac waren er diverse problemen: communicatie, doorontwikkeling, controle en toetsing Was het makkelijk te onderzoeken? Waarom? Bij de boeing 737 crashes was het probleem van controle en communicatie naar medewerkers Was het makkelijk te onderzoeken? Waarom?

Uit de evaluatie van de china explosion 2015 tianjin komt naar voren dat communicatie, transparantie en veiligheid niet altijd prioriteit hadden bij de lokale autoriteiten Was het makkelijk te onderzoeken? Waarom?

Bij de tesla autopilot crashes komen soms onvoldoende onderbouwde ontwerpkeuzes naar voren die niet goed zij afgewogen tegenover het gedrag van de bestuurder vlucht 1951 Was het makkelijk te onderzoeken? Waarom?

De ramp in Tsjernobyl toont aan hoe autoriteiten een ramp in de doofpot proberen te stoppen Was het makkelijk te onderzoeken? Waarom?

Wat heb ik geleerd Ik heb erg veel geleerd van het veilig opzetten van VPN's. Een VPN opzettenhad ik namelijk nog nooit gedaan. Het opzetten van SSH en het aanmaken vanVM's was al bekend. Ook had ik nog nooit met UDP sockets geprogrammeerd.Verder heb ik geleerd hoe ik in de praktijk een VM in een VLAN kan zetten enhoe VLAN's netwerken van elkaar kunnen scheiden.Het leukste onderdeel van het project, was dat wonderbaarlijk mijn gekozenoplossing elegant werkte. UDP Servers en clients zijn gerealiseerd met minderdan enkele regels logisch scipt. Ik had aan genomen dat het werken met socketsin shell absoluut rampzalig zou uitpakken. Ik ben blij dat het opdracht zo vrijwas, zodat ik experimenteel kon zijn met mijn implementatie.

Discussie

discussie geldigheidsgrenzen van de waarnemingen betrouwbaarheid van de waarnemingen waaarde van de waarnemingen vergelijking van het oude en het nieuwe product/methode/apparaat volgens de genoende criteria. De gewijzigde factor maakt het product/methode/apparaat geheel/half/niet beter

Preconditions Topography By means of maps (land, water, river, sea, ownership, regional and zoning plans) a detailed description of the environment should be provided, including any planned changes to existing situations, in so far as this is of importance to the lock and adjoining lock approaches. Special attention should be paid to historical, natural and scientific values. The maps should also show sewerage, cables and mains as well as drainage facilities in the area concerned. Existing lock (locks) Water levels (approx.) Wind Morphology Soil characteristics Functional requirements Functional requirements regarding navigation General Lock approaches Primarily as part of the traffic management in locking Stop over harbour Harbour of refuge Compulsory harbour Hazardous substances Leading jetties Chamber and heads The principal dimensions The design The facilities and equipment Functional requirements regarding the water retaining (structure)

Dan zijn er nog de functionele eigenschappen. Functional requirements regarding water management General Limiting water loss Separation of salt and fresh water or clean and polluted water Water intake and discharge

Functional requirements regarding the crossing, dry infrastructure Roads Cables and mains

User requirements

Levels Locking levels Situating the lock Accessibility Smoothness and safety of dealing with traffic Design levels Normative High Water (NHW) Locking level high water gate

Mogelijke voorkeur voor het scheiden van verschillende soorten vaten Separation in using line-up area, waiting area and chamber Separating vessels during locking Separation of vessels during over night stop Separation for use of the leading jetty (leidende steiger) Leading jetty for seagoing vessels Leading jetty for inland navigation Leading jetty for recreational navigation

Mooring facilities in chamber and lock approach Chamber Lock approaches Leading jetty

Operating times

Levelling times

Operational management Process descriptions Normal locking process Obstructions High water retaining structure Intake/discharge Salt /freshwater or clean/polluted water Information for operational management Procedures and facilities for negative operational situations Power supply LevellingCollisions Too low/too high water levels and inspections Problems with ice

Operating Situating the control building Local control facilities Means of communication Choice (partly) automated and self-service Remote control of locks

Verlichting, signalering en boarding Verlichting (for details, see Lit. [2.1]) Ship crews and operating personnel must take into account that comfort is decreased during locking that takes place through the night. Given the decreased visibility and orientation, extra effort is required. This effort has to be kept as low as possible in order to prevent decreased safety. For this purpose, suitable and economically sound illumination of the lock complex is essential. The lighting has to be geared to the ever-increasing use of central control at locks and has to be aimed at places where activities (manoeuvres, tying and untying, going on land) are executed. The locations drawing the attention of the individual captain for instance, are the free area, the line-up and waiting area, the chamber entrance, the chamber, lock grounds, chamber exit and the outlet area to the unlit waterway. The attention of operating personnel will particularly focus on the vessels in the line-up and waiting areas, inbound vessels, the chamber, the gates, the lock grounds

and the sailing of outbound vessels. Given the necessity of illuminating the lock and lock approaches, a number of general minimum conditions are set. This illumination is compulsory and could be included in the design plan: • a clear view of the lock complex has to be provided for the benefit of orientation from the water; • the illumination has to be sufficiently even; • during arrival and departure dazzling, which is often caused by excessive glare of lock parts because of cameras etc., should be prevented; • in the control building the illumination should be adjusted to the outside environment and images recorded as TV pictures should have such contrast and definition that the operating personnel is given sufficient information; • uniformity in the illumination plan for the setup of light towers, height of points of light and light colour is desired. In Lit. [2.1], as extension of these conditions, a number of specific recommendations are made that are of importance to the design.

Scheepsbemanningen en bedienend personeel moeten er rekening mee houden dat het comfort tijdens het schutten afneemt vindt de hele nacht plaats. Gezien de verminderde zichtbaarheid en oriëntatie is extra inspanning vereist. Dit inspanning moet zo laag mogelijk worden gehouden om verminderde veiligheid te voorkomen. Voor dit doel geschikt en economisch verantwoorde verlichting van het sluizencomplex is essentieel. De verlichting moet zijn afgestemd op het steeds toenemende gebruik van centrale bediening bij sluizen en moet gericht zijn op plaatsen waar werkzaamheden (manoeuvres, vast- en losmaken, aan land gaan) worden uitgevoerd. De locaties die bijvoorbeeld de aandacht trekken van de individuele kapitein zijn de vrije ruimte, de opstelling en wachtruimte, de kolkingang, de kolk, het sluisterrein, de kolkuitgang en het uitloopgebied naar de onverlichte waterweg. De aandacht van het bedienend personeel zal met name gericht zijn op de schepen in de opstel- en wachtruimtes, inkomende schepen, de kolk, de deuren, het sluisterrein en het uitvaren uitgaande schepen. Gezien de noodzaak van verlichting van de sluis en sluistoegangen gelden een aantal algemene minimumvoorwaarden spelen zich af. Deze verlichting is verplicht en kan in het inrichtingsplan worden opgenomen: • er moet vrij zicht zijn op het sluizencomplex ten behoeve van de oriëntatie vanaf het water; • de verlichting moet voldoende egaal zijn; • bij aankomst en vertrek verblinding, wat vaak wordt veroorzaakt door overmatige verblinding van sluisdelen doordat van camera's e.d. moet worden voorkomen; • in het controlegebouw dient de verlichting afgestemd te zijn op de buitenomgeving en beelden opgenomen als tv-beelden moeten zo'n contrast en definitie hebben dat het bedienend personeel wordt gegeven voldoende informatie; • uniformiteit in het verlichtingsplan voor de opstelling van lichtmasten, hoogte van lichtpunten en lichtpunten kleur is gewenst. In Lit. [2.1] In het verlengde van deze voorwaarden worden een aantal specifieke aanbevelingen gedaan die dat wel zijn belangrijk voor het ontwerp. Vereist verlichtingsniveau For the average value of illumination intensity on horizontal surfaces of the above-mentioned lock parts, 10 lux is adhered to. On vertical surfaces that are more often more striking due to the perpendicular directional view, a lower value of 3.5 lux can be used. At a number of critical parts of the lock (both for the captain and the lock master) a larger contrast is desired and can be achieved by stronger illumination of areas that should be in the light or providing these with white markings. The latter is preferable. At critical lock parts such as gates and leading jetties, the vertical illumination strength should be higher: 7 lux. On the chamber and mooring area where accurate visibility is required, the previously stated values of 10 lux for horizontal and 3.5 lux for vertical apply. The waiting area and the free area, where illumination is mostly for orientation, require an illumination level of 5 lux horizontal respectively 3.5 lux vertical.

Voor de gemiddelde waarde van de verlichtingsintensiteit op horizontale oppervlakken van het bovengenoemde slot onderdelen wordt 10 lux aangehouden. Op verticale vlakken die door de loodlijn vaker opvallender zijn gericht zicht kan een lagere waarde van 3,5 lux worden gebruikt. Op een aantal kritische onderdelen van de sluis (zowel voor de gezagvoerder als de sluismeester) is een groter contrast gewenst en kan worden bereikt door sterkere verlichting van gebieden die in het licht moeten staan of moeten worden voorzien deze met witte aftekeningen. Dit laatste heeft de voorkeur. Bij kritische sluisdelen zoals poorten en voorloop aanlegsteigers dient de verticale verlichtingssterkte hoger te zijn: 7 lux. Op de kamer en het ligplaatsgebied waar nauwkeurig zicht vereist is, de eerder genoemde waarden van 10 lux voor horizontaal en 3,5 lux voor verticale toepassing. De wachtruimte en de vrije ruimte, waar de verlichting vooral ter oriëntatie is, vereisen een verlichtingsniveau van 5 lux horizontaal respectievelijk 3,5 lux verticaal. Omgevingsverlichting en begeleiding Misleading illumination in the surrounding area can give the captain a wrong picture of the course of the waterway that provides access to the lock chamber. This can be prevented if the waterway or the lock complex is illuminated over a sufficient length or

by adapting the surrounding illumination to the illumination of the complex. For visual guidance, differences in illumination strength at crossings should not exceed a factor 2. Uniformiteit For the uniformity (E) of the illumination, a minimum value of Emin/Emax = 0.3 should be adhered to for both vertical and horizontal areas. Glare Unsafe situations due to dazzling should be avoided. The correct combination of armature, lamp and positioning is of importance. Kleurherkenning en soort lamp The colour of the light is one of the factors in the recognition of boards and signalling. Both white and yellow light can be used. In the lamp choice of illumination, both high-pressure and low-pressure lamps as well as energy saving lamps qualify. In the application of low-pressure (monochromatic) sodium (vapour) light, colour recognition is impossible. If this is the case, separate illumination of traffic signs is recommended.

De kleur van het licht is een van de factoren bij de herkenning van borden en signalering. Beide wit en geel licht kan worden gebruikt. Bij de lampkeuze van verlichting, zowel hogedruk- en lagedruklampen als energie spaarlampen komen in aanmerking. Bij de toepassing van lagedruk (monochromatisch) natrium (damp) licht, kleurherkenning is onmogelijk. In dat geval is het aan te raden om verkeersborden apart te verlichten. Marking White markings are a good and inexpensive tool for obtaining sufficient contrast in the dark while using little light. Marking vertical surfaces, such as guiding structures and guard walls, to support the visual guidance of navigation is very effective.

Witte aftekeningen zijn een goed en goedkoop hulpmiddel om tijdens het gebruik voldoende contrast in het donker te krijgen klein licht. Markering van verticale oppervlakken, zoals geleideconstructies en veiligheidsmuren, ter ondersteuning van het visuele begeleiding van navigatie is zeer effectief. Signalling Signalling should be executed according to the stipulations of the Police Regulations on Inland Navigation ('Binnenvaart Politie Reglement' (BPR))and the Rhine Navigation Police Regulations ('Rijnvaart Politie Reglement' (RPR)), (Lit. [2.4]).Signal indication and lock illumination choices should be adjusted to terrain illumination of the lock for the benefit of colour recognition; it should have sufficient attention value.

De seingeving dient te worden uitgevoerd volgens de bepalingen van het Politiereglement Binnenvaart Scheepvaart (Binnenvaart Politie Reglement (BPR)) en het Rijnvaartpolitiereglement ('Rijnvaart Politie Reglement' (RPR)), (Lit. [2.4]). Keuzes voor signaalindicatie en slotverlichting moeten aangepast aan terreinverlichting van de sluis ten behoeve van kleurherkenning; het zou voldoende moeten hebben attentie waarde. Boarding Boards should be executed in accordance with the stipulations of the BPR and RPR, (Lit. [2.4]).The colour recognition could be (substantially) reduced due to the terrain illumination. Sufficient attention should be paid to adjusting the illumination or to separate board illumination. Verlichtingsplan The user requirements for illumination should be incorporated in an illumination design plan. The chamber depth (distance between low normative water level and the lock coping) and the chamber width are of great importance. In Lit. [2.1] examples are provided for a number of chamber width categories (5-13 m, 13-20 m, 20-24 m, larger than 24 m; chamber depth about. 5 m) of the resulting illumination characteristics (such as illumination strength and uniformity), departing from the relationship between lock design and the given characteristics of illumination installation (such as positioning and illumination facilities).

Stroomvoorziening Emergency power supply is required for vital parts of the installation so that, in case of malfunction, it can automatically take over the energy supply within minutes. A no-break facility is required for installation parts that lose data in case of power loss. In addition, emergency lights should be present.

In essence, power is obtained from the public network. In consultation with the local power company, assessments have to be made about where this is possible and whether the connection contains sufficient capacity or whether this will have to be adjusted. Of importance is the total capacity required, voltage variations and frequency of the energy to be supplied. In addition to capacity for lock operation, the capacity for construction (civil and steel) will have to be determined. It could be taken into consideration whether the cables for construction could later become part of the supply for the lock. The lock complex should contain the necessary facilities for high tension, transformers and low-tension equipment. In addition, room is reserved and facilities provided for cable location lines from the low-tension area to the various lock parts (cable racks, cable channels, cable shafts, lead-through pipes etc.) Take into account the other cables and mains required for lock operation as well as those for third parties (Par. 2.3.4.2). For

emergency power supply generators and no-break installations, see Par. 2.4.6.3.

Noodvoorzieningen voor stroomtoevoer i vereist voor bepaalde delen van de installatie, in geval van een storing kan deze binne enkele minuten leveren.

Een no-break facicilieit is vereist voor de ondeerdelen die data verliezen in gevala van sstroomuitval. Het sluizencomplex moet gaciliteiten hebben voor hoogspanning, transformatoren en laagspanningsapparatuur.

Beschikbaarheid Introduction Causes of non-availability Water levels above and below locking levels Guidelines on the boundaries of locking levels are provided in Par. 2.4.1.1 (maximum and minimum locking levels). Overall, this results in non-availability smaller than 2The specific boundaries should be set on economic grounds. Too much wind, bad visibility

De beschikbaarheid van een sluis kan beinvloed worden door een te hoog waterlevel boven de sluis. Dan is er nog de mogelijkheid op te veel wind en slecht zicht. Storingen aan installaties, bedieningsmechanismen en werking. Er moeten oplossingen komen zodat ern signalen worden gegeven wanneer een storing zich voordoet, een betre reactie op signalen en reserveonderdelen. Based on the previously mentioned economic considerations, requirements will have to be drafted for the design of the lock or the series of locks for the acceptable risk of failure of these facilities. As an example, the values applied for the renovation of the 'Zuider- en de Kleine sluisin IJmuiden' are stated (Lit. [2.13]). Not available due to: • malfunction installations : 0,5• malfunction operating mechanisms : 0,5• malfunction operation : 0,25The number of times that malfunction occurs could also be a determining factor. Not every malfunction results in complete obstruction. The objective is to limit the duration of the malfunction as much as possible (alerting, responding, spare parts). For emergency power supply and no-break installations, please see Par. 2.4.6.3.

Botsingen For non-availability due to collisions, at best a forecast can be made, based on the information available for similar locks with a corresponding navigation volume. As an example, the 'Zuidersluis bij IJmuiden' (Lit. [2.13]) is mentioned, where the non-availability due to significant damage due to collisions amounted to 17 hours per annum (about 0.2Within economically acceptable boundaries, the objective will be to limit the collisions and consequences thereof. The accent is placed on gates (and operating mechanisms), moveable bridges and – to a lesser degree – on berthing jetties and guide structures. Measures to decrease risk of collision are, among others: • good design of approach jetties (Par. 2.3.1.3 and 2.4.2.2); • positioning of the flooring of moveable bridges – in opened condition – outside the outer walls of the lock (Par. 2.3.4.1); • anti-collision structures in front of the gates (Par. 2.4.11.1). This is an expensive facility that will only be applied in special cases; • protection of operating mechanism on gates. Preventing collisions with the operating mechanism can be effected by fitting a tail end to the gate and connecting this to the operating mechanism (Renovation Oranjesluizen). An extended operating mechanism chamber could also be used so that the vulnerable cylinder rod cannot be hit in the lock (Middensluis IJmuiden). Measures to limit the duration of the repairs (obstruction) are, among others, having the spare gates and spare parts available (Par. 2.5.2 en 2.5.3). Maatregelen om het aantal botsingen te voorkomen zijn: Good ontwerp voor aanvaarstijgers. positionering van de vloer van beweegbare poorten anti-bots structuren aan de voorkant van de sluisdeuren bescherming van werkende meschanismen van de slusdeuren

Maintenance

Constructies beschermen tegen schade Aanrijdbeveiliging voor poorten Mitre gates and pivot (leaf) gates must be fitted with wood fender on the outside surfaces of the opened gates to protect the construction from damage caused by inbound and outbound vessels. Wood fender can also be fitted to other gates in places where they might be hit by vessels. In special circumstances (for instance Wijk bij Duurstede, Tiel, Belfeld, Panheel, Twenthe-kanaal) trap constructions are positioned in front of the closed gates. The energy of vessels that do not stop in time is absorbed here and the construction prevents the gates from being hit (see par. 17.3.3). For this purpose, cables (cable nets) and friction drums can be used. For the circumstances and setup of these constructions, we refer to Lit. [2.15]. It does concern expensive constructions for which the investments will have to be weighed against the risk of failure of the water retaining structure, the navigation interests etc. Anti-collision devices protecting lock gates could be economically sound at high-lift locks.

Verstekpoorten en draaipunt. In bijzondere reegvallen staan er valconstructies bij de gesloten poorten voor vaartuigen die niet op tijd stoppen. zodoende wordt de klap opgevangen. Anti-bots apparaten die de sluisdeuren beschermen zijn economisch verantwoor bij hoge liftsluizen. Aanrijdbeveiliging voor beton- en damwandconstructies Construction surfaces against which vessels moor or along which they shave, have to be as smooth as possible in order to guide well and limit potential damage (construction and vessel). For inland navigation, a concrete structure meets the requirements. In the case of other construction materials such as sheet pile, the flat surface should be made of wooden or synthetic posts and rails wherever possible. This system can be limited to the day surfaces that vessels meet. Constructievlakken waar schepen aanmeren of waarlangs ze scheren, moeten zo glad mogelijk zijn mogelijk om goed te begeleiden en mogelijke schade (constructie en vaartuig) te beperken. Voor de binnenvaart, een betonconstructie voldoet aan de eisen. In het geval van andere bouwmaterialen zoals damwand, het vlakke oppervlak dient zoveel mogelijk te bestaan uit houten of kunststof palen en rails. Dit systeem kan worden beperkt tot de dagoppervlakken die schepen ontmoeten.

Additional facilities are necessary in places where concrete surfaces are interrupted or come to an end because of expansion joints, gate and ladder recesses. In the case of expansion joints, it will be sufficient to use (sizeable) bevelled edges, steel corner protection profiles should be applied in recesses. Corner guards made of tropical hardwood can also be fitted, especially where it concerns rugged navigation such as tug-pushed dumb barges and sea-going vessels. As protection from hawsers etc, the top of the wall should be fitted with steel capstone profiles. In locks for large ocean going vessels, floating wooden frames (the Netherlands) or rubber wheel fenders (Belgium) are used. Op plaatsen waar betonvlakken worden onderbroken of ophouden, zijn aanvullende voorzieningen nodig vanwege dilatatievoegen, poort- en ladderuitsparingen. In het geval van dilatatievoegen is dit voldoende om (flinke) afgeschuinde randen te gebruiken dienen stalen hoekbeschermingsprofielen in uitsparingen te worden aangebracht. Hoek ook beschermkappen van tropisch hardhout kunnen worden aangebracht, zeker als het om ruige navigatie gaat zoals sleepboten en zeeschepen. Als bescherming tegen trossen enz., de bovenkant van de wand dient voorzien te zijn van stalen deksteenprofielen. In sluizen voor grote zeeschepen, drijvend van hout frames (Nederland) of rubberen wielspatborden (België) worden gebruikt.

The facilities are intended to minimize damage to vessels and constructions, but also to prevent backing up and friction effects during mooring and unmooring of vessels with large side surfaces, thereby decreasing the pass through time.

Voorzieningen tegen vandalisme Lightning protection Safety Voorzieningen voor drenkelingen For rescuing people who accidentally end up in the water, ladders should be fitted to the chamber wall and to (high) smooth walls in the lock approach. At the upper end, these ladders are equipped with handgrips. For offering help from the quayside, life-saving devices (life buoy, hooks) should be present on the lock coping in a clearly visible place. Ladders in the chamber and the lock approach also have an accessibility function. For locations and distances, also see par. 2.4.13.2 and 2.4.13.3. Voor het redden van drenkelingen moetn er ladders zijn. Veiligheidsvoorzieningen Design and management of safety facilities of personnel will be executed in accordance with Health and Safety Regulations, construction regulations, labour regulations and safety regulations (CE directives). A number of facilities are mentioned below. Railings are attached to the top of gates. If the lock coping is more than 2.5 m above minimum locking level, fencing is placed behind the bollards. This fencing is always desirable where it concerns recreational navigation and where tourists are allowed on the lock coping. In the technical areas, workshops, bridges, control portals, rolling gate casings and the like, where work is executed and people walk around where there are differences in height in the surrounding area, railings are provided. From a height difference of 0.60 m or more with the surrounding area, a railing has to be provided at 1 – 1.10 m. Height differences of more than 12 m require the railing to be placed at a height of 1.20. Often, additional protection against falling is provided from height differences of more than 2.5 m such as safety lines, lifelines, harness belts and the like.

Steel ladders should not be in regular use. Straight stairs, a spiral staircase or step ladders should be installed. Ladders can be used between vertical (90o) and 75o and be equipped with simple round rungs. The ladder width is between 0.38 and 0.46 m and the step distance is between 0.25 – 0.20 m. If the ladder connects with the (landing) coping, the distance between the styles of the ladder should be

enlarged to 0.60 and it has to be connected to the railing. If the ladders are higher than 3.60 m, they have to be provided with a safety cage. This cage has an inside measurement of 0.76 m and starts from 2.40 m above the ground. At ladder heights above 6 m, an intermediate landing is required.

Basement chambers that could possibly flood (for instance those of operating mechanisms of mitre gates) have to be provided with an exit that can be opened from the inside. In addition, sufficient natural ventilation will be required as well as plunger pumps. The area in which the operating mechanisms are working need to be shielded from the environment to ensure that nobody gets stuck between machine parts. The lock complex should have sufficient and visible First Aid provisions.

Ontwerp en beheer van veiligheidsfaciliteiten voor personel worden uitgevoerd in overeenstemming met de gezondheids-veiligheidsregelgeving, constructieregelgeing,arbeidsregelgeving en veilgieheidsregeveving. Enkele voorbeelden zijn traliewerk, hekwerk, stalen ladders, kelder kamers en eerste hulp kits Brand blussen Toegankelijkheid van sluis en sluistoegangen Lock Infrastructure Accessibility of vessels in the lock Accessibility of vessels in the lock approache Accessibility of vessels with dangerous goods in the lock approaches

Supplemental client wishes

Eisen aan de levensduur Ontwerp levensduur sluizencomplex Steel parts Electrical installations Hardware and software Damwand constructies Leidende structuren Maintenance requirements Maintenance strategy The maintenance strategy will mainly be based on the requirements regarding the safety of the retaining structure (par. 2.3.2), the availability for lock operation (par 2.4.10) and the life span (2.4.15). The external appearance of the structure will also play a role in the strategy (building inspection). With the exception of the safety requirements, which are fixed, it concerns an assessment between the aggregate costs of investments and capitalized maintenance, and the interest of obstructions for navigation. An example is to consider applying 2 horizontal roller-bearing gates per head for a maritime navigation lock (par. 2.5.2). The optimization of the materials, maintenance choices etc. within the given design life span of a lock is discussed in par 2.4.15. Environmental requirements necessitate certain maintenance activities to be executed in closed areas. Providing these facilities on site could be costly and it could be attractive to have these activities executed by third parties. Overall, the objective is to incur a minimum of aggregate costs as well as provide the largest service provision to navigation. The latter includes a limitation of the number and duration of obstructions for maintenance (par. 2.4.10) and attention for limited passage during maintenance. Please refer to the modules of ‘Raamwerk Onderhoud van Natte Kunstwerken’ (Lit. [2.20]), which is drafted by the Civil Engineering Division of the Ministry of Transport and Public Works. At present, the following modules are available: "Keuze van onderhoud voor een puntdeur", "Damwandenänd "Ducdalven en remmingwerken". Based on this strategy, maintenance plans, books and schedules will have to be drafted for the various parts. Supplemental to this, measures and procedures for navigation during maintenance will have to be drafted.

De onderhoudstrategie wordt bepaald of basis van de vasthoudende structuur, de mogelijkheden voor sluisbediening en de levenscyclus. het uiterlijk van de structuur speelt een belangrijke rol bij de strategie, namelijk gebouw inspectie. Bahalve veiligheidseisen gaat dit over de toetsing van de totale investeringskosten en noodzakelijk onderhoud, en de behoefte aan belemmering voor nativatie. Het optimaliseren van materialen, onderhoudskeuzen binnen de levenscyclus van de sluis. Omgevingseisen maken het nodg onderhoudsactiviteten uit te voeren in afgesloten ruimten. 2.5.2 Spare Reserve poorten Onderdelen en materialen Slot openleggen (of niet) Nowadays, it is no longer usual to lay open the complete lock for maintenance. The reasons are that it is often too costly (measures required against floating up) and that the main construction of chamber and heads are maintenance free, the probable exception being wood fenders for sheet pile constructions and floating frames at sea locks. The latter parts should be easy to replace. Incidental repairs to head constructions could be executed by divers or in diving bells. Inspection and maintenance focus on gate supports (sill and side seals), fulcrums, and gate conduction, in other words, parts that are located in the head. There are two possibilities: 1. Lying open a head, for which stop log weirs or dewatering weirs and rabbets are necessary. 2. Removable pivot-inspection chambers and other local steel dewatering means for the fulcrums, support and gate condition. This also includes the dewatering stop logs for the gate recesses for lift and roller-bearing gates. Gate supports and rabbets are also required for the drainage. These means for water removal are stored in the near

vicinity in a highly accessible place and could possibly be used for several locks. The choice between two possibilities depends on the inspection and maintenance frequency, the costs and the duration of the obstruction for navigation. Option 1, in which too much space is laid open is, in essence, usually only applied at smaller locks.

Tegenwoordig is het niet meer nodig om een complete sluis open te leggen voor onderhoud. De reden is dat dit duur is en dat de hoofd constructie van de kamer en hoofden vrij zijn van onderhoud afgezien van houden spatborden voor damwandbouwers en zwevende kozijnen.

Poortsteuningen en ponningen zijn nodig voor de drainage Toegankelijkheid voor het personeel Monitoring(Toezicht houden) Monitoring is a permanent measuring and registration system for normative parameters for the condition of structures, the loads and stresses that they are submitted to and the degree in which corrosion processes have progressed. Even though the application in construction is still limited, it is necessary to keep up with the rapid developments. Monitoring is useful, certainly for places of lock structures that are difficult to inspect (for instance at soil facing side) and for erosion processes that are hardly visible on the surface (such as chloride penetration). Monioren betekent het permanent meten en registeratie systeemvoor normatieve parameters voor de conditie van de structuren,ladingen. Het iis belangrijk alle ontwikkelingen in de gaten te houden. Monitoren is nuttig, zeker voor onderdelen van de sluis die moeilijk te inspectiren zijn zoals de bodem en voor erosie processen die moelijk zichtbaar zijn vanaf het oppervlak. Cathodic protection can be used as a monitoring system at the same time. Electrical installation, hard- en software Storage areas and workshops Environmental requirements in the use phase Aesthetics

In ons model houden we geen rekening met omgevingseisen zoals de materialen gebruiket voor de bouw, recreatie, bodemvervuiling, grondwaterverlies. Oo is er geen rekening gehouden met verkeer, communicatiekabels onderwater en netspanningskabels.

Environmental requirements with regard to building materials Recreation Environmental requirements in the construction phase Required building site and final grounds Polluted soil Groundwater withdrawal Upkeep/maintenance of road and navigation traffic, cables and mains Upkeep/maintenance of the water retaining structure

Permits and procedures at the construction of a lock Construction permits and zoning plan amendments Demolition permit Flood Defence Act Environmental Management Act (M.E.R.) Act on Earth Removal Pollution of Surface Waters Act Groundwater Act permit Water management Act Soil Protection Act Nature Conservation Act Management of Waterways and Public Works Act (Wet beheer RWS-werken) Noise Abatement Act Provincial Road Ordinance Building Materials (Soil and Surface Waters Protection) Decree Other permits and exemptions Standards and guidelines Standards Guidelines

Checklist

Bronnen

[1] Lamport L.: *LaTeX: A Document Preparation System*, Addison-Wesley, 1994

[2] Oostrum van P.: *Handleiding LaTeX*, Vakgroep Informatica, Universiteit Utrecht, 1998, http://people.cs.uu.nl/piet/latexhnd.pdf

[3] Wikibooks LaTeX: http://nl.wikibooks.org/wiki/LaTeX

[4] Wikibooks LaTeX: https://www.waterkant.net/suriname/2023/05/29/milieuactivist-sleur-zeer-grote-onwaarheden-

challenges in requirements engineering

[5] ... LaTeX: https://www.researchgate.net/publication/2462377_Challenges_in_Requirements_Engineering why goals-oriented for requirements engineering

[6] ... LaTeX: https://www.researchgate.net/publication/249901480_Goal-Oriented_Requirements_Engineering_An_Overview_of_the_Current_Research design and build of collaborative information agents

[7] ... LaTeX: https://www.researchgate.net/publication/221622575_Design_of_Collaborative_Information_Agents treating nfiras first gradefor its testability

[8] ... LaTeX: software requirements negotiation a theory ui based spiral approach

[9] ... LaTeX: https://www.cs.rug.nl/search/uploads/Teaching/RE2009Fall/paper/1995_Boehm_ICSE_Software%20Requirements%20Negotiation%20and%20Renegotiation%20Aids%20A%20Theory-W%20Based%20Spiral%20Approach.pdf the worlds a stage: a survey on requirementsengineering using a real life case study

[10] ... LaTeX: https://www.researchgate.net/publication/2548016_The_world's_a_stage_a_survey_on_requirements_engineering_using_a_real-life_case_study_Karin_Koogan_Breitman_Julio_Cesar_S_do_Prado_Leite from inconsistencyhandling to non-conanical requirements management: a logical perspective

[11] ... LaTeX: https://www.researchgate.net/publication/257272175_From_inconsistency_handling_to_non-canonical_requirements_management_A_logical_perspective managing inconsistent specification: reasoning, analysis, action

[12] ... LaTeX:
https://www.researchgate.net/publication/2635497_Managing_Inconsistent_Specifications_Reasoning_Analysis_and_Action representingand using nonfunctional requirements: a process-oriented approach

[13] ... LaTeX:
https://www.researchgate.net/publication/3187474_Representing_and_Using_Non-Functional_Requirements_A_Process-Oriented_Approach Four dark corners of requirements engineering

[14] ... LaTeX:
http://www.cse.msu.edu/~chengb/RE-491/Papers/dark-corners-re-zave-jackson.pdf classification of research methods in requirements engineering

[15] ... LaTeX:
https://www.researchgate.net/publication/220565934_Classification_of_Research_Efforts_in_Requirements_Engineering agent-basedtactocs for goal-oriented requirements elaboration

[16] ... LaTeX:
https://www.researchgate.net/publication/3952082_Agent-based_tactics_for_goal-oriented_requirements_elaboration challenges in requirements engineering

[17] ... LaTeX:
why goals-oriented for requirements engineering

[18] ... LaTeX:
scann 0087 design and build ofcollaborative information agents

[19] ... LaTeX:
treating nfiras first gradefor its testability

[20] ... LaTeX:
scan 0089 software requirements negotiation a theory ui based spiral approach

[21] ... LaTeX:
the worlds a stage: a survey on requirementsengineering using a real life case study

[22] ... LaTeX:

[23] ... LaTeX:
https://www.nerc.com/_layouts/15/Nerc.404/CustomFileNotFound.aspx?requestUrl=https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[24] ... LaTeX:
https://www.nixu.com/fi/node/53

[25] ... LaTeX:
https://www.wallix.com/blog/ics-security-russian-hacking

[26] ... LaTeX:
https://en.wikipedia.org/wiki/Industroyer

[27] ... LaTeX:
https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-gri

[28] ... LaTeX:
https://en.wikipedia.org/wiki/Crash_Override_Network

[29] ... LaTeX:
https://www.virusbulletin.com/virusbulletin/2019/03/
vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/

[30] ... LaTeX:
https://www.cyber.nj.gov/threat-center/threat-profiles/ics-malware-variants/
crashoverride

[31] ... LaTeX:
https://iiot-world.com/ics-security/cybersecurity/five-cybersecurity-experts-about-crashov

[32] ... LaTeX:
https://search.abb.com/library/Download.aspx?DocumentID=9AKK107045A1003&
LanguageCode=en&DocumentPartId=&Action=Launch

[33] ... LaTeX:
https://www.blackhat.com/us-17/briefings/schedule/#industroyercrashoverride-zero-things-co

[34] ... LaTeX:
https://dreamlab.net/en/blog/post/fuzzing-ics-protocols/

[35] ... LaTeX:
http://www.connectivity4ir.co.uk/article/175490/IEC-62351--Secure-communication-in-the-ene
aspx

[36] ... LaTeX:
https://www.win.tue.nl/~setalle/2017_fauri_encryption.pdf

[37] ... LaTeX:
https://dl.acm.org/doi/fullHtml/10.1145/3381038

[38] ... LaTeX:
https://arxiv.org/pdf/2001.02925.pdf

[39] ... LaTeX:
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.
pdf

[40] ... LaTeX:
"https://www.researchgate.net/publication/333671061_Attacking_
IEC-60870-5-104_SCADA_Systems"

[41] ... LaTeX:
https://scialert.net/fulltext/?doi=tasr.2014.396.405

[42] ... LaTeX:
"https://www.boozallen.com/content/dam/boozallen/documents/2016/09/
ukraine-report-when-the-lights-went-out.pdf"

[43] ... LaTeX:
https://rhebo.com/en/service/glossar/industroyer-25114/

[44] ... LaTeX:
https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack

[45] ... LaTeX:
https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

[46] ... LaTeX:
https://www.darkreading.com/threat-intelligence/first-malware-designed-solely-for-electric
d/d-id/1329114

[47] ... LaTeX:
https://arstechnica.com/information-technology/2017/06/
crash-override-malware-may-sabotage-electric-grids-but-its-no-stuxnet/

[48] ... LaTeX:
http://web.mit.edu/smadnick/www/wp/2016-22.pdf

[49] ... LaTeX:
https://www.cybersecurityintelligence.com/blog/attack-on-ukraines-power-grid-targeted-tran
html

[50] ... LaTeX:
https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_
energy_infrastructures_2017_2.pdf

[51] ... LaTeX:
https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

[52] ... LaTeX:
https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

[53] ... LaTeX:
https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-powe

[54] ... LaTeX:
https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-w

[55] ... LaTeX:
https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN

[56] ... LaTeX:
https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm/
u-s-firm-blames-russian-sandworm-hackers-for-ukraine-outage-idUSKBN0UM00N20160108

[57] ... LaTeX:
https://www.wired.com/story/russian-hackers-attack-ukraine/

[58] ... LaTeX:
https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108

[59] ... LaTeX:
https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_
energy_infrastructures_2017_2.pdf

[60] ... LaTeX:
https://ris.utwente.nl/ws/files/6028066/3-s2_0-B9780128015957000227.pdf

[61] ... LaTeX:
https://repositorio-aberto.up.pt/bitstream/10216/119066/2/315683.pdf

[62] ... LaTeX:
https://www.vice.com/en/article/zmeyg8/ukraine-power-grid-malware-crashoverride-industroye

[63] ... LaTeX:
https://na.eventscloud.com/file_uploads/aed4bc20e84d2839b83c18bcba7e2876_
Owens1.pdf

[64] ... LaTeX:
https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[65] ... LaTeX:
https://na.eventscloud.com/file_uploads/aed4bc20e84d2839b83c18bcba7e2876_
Owens1.pdf

[66] ... LaTeX:
https://www.tweedekamer.nl/downloads/document?id=80443e97-f17e-499c-b3f2-ad608f32e1aa&
title=Rapportage%20Staat%20van%20de%20infra%20RWS%20%28definitief%29.pdf

[67] ... LaTeX:
https://www.nu.nl/internet/5814282/rekenkamer-waterwerken-niet-goed-beveiligd-tegen-cybera
html

[68] ... LaTeX:
https://www.deltalimburg.nl/article/9824/Onderhoudswerkzaamheden+aan+Sluis+
Linne+afgerond

[69] ... LaTeX:
https://nieuwesluisterneuzen.eu/veiligheid

[70] ... LaTeX:
https://www.mrdmarinesupport.nl/nl/maritieme-dienstverlening/
ondersteuning-veiligheid/

[71] ... LaTeX:
https://www.infrasite.nl/bouwen/2021/05/27/veiligheid-voorop-begin-project-sluis-of-brug-a

[72] ... LaTeX:
https://www.wdodelta.nl/bediening-schutsluizen-vechterweerd-en-vilsteren

[73] ... LaTeX:
https://www.infrasite.nl/waterbouw-deltas/2021/05/21/
sluis-heel-onder-handen-genomen/

[74] ... LaTeX:
https://www.hdsr.nl/actueel/nieuws/@154100/lichtprojecties-zetten-waterliniesluizen/

[75] ... LaTeX:
https://nos.nl/artikel/2277937-rekenkamer-hack-aanval-op-waterwerk-niet-altijd-opgemerkt

[76] ... LaTeX:
https://varendoejesamen.nl/kenniscentrum/artikel/onderhoud-sluis-linne-afgerond

[77] ... LaTeX:
https://www.gww-bouw.nl/artikel/de-eerste-sluis-met-kantelende-sluisdeur/

[78] ... LaTeX:
https://tkhsecurity.com/nl/waterwerken/

[79] ... LaTeX:
https://www.h2owaternetwerk.nl/h2o-actueel/rekenkamer-vitale-waterwerken-nog-onvoldoende-b

[80] ... LaTeX:
https://www.magazinesrijkswaterstaat.nl/bereikbaarzeeland/2021/01/
krammersluizencomplex-verleden-heden-en-toekomst

[81] ... LaTeX:
https://www.hdsr.nl/publish/pages/86927/sluizen_in_of_bij_een_waterkering_-_uitvoeringsregels.pdf

[82] ... LaTeX:
https://api1.ibabs.eu/publicdownload.aspx?site=sluis&id=100100292

[83] ... LaTeX:
https://services.pilz.nl/wp-content/uploads/2021/12/brochure_bruggen_2018.pdf

[84] ... LaTeX:
https://lokaleregelgeving.overheid.nl/CVDR375606/6

[85] ... LaTeX:
https://zoek.officielebekendmakingen.nl/stb-2019-27.html

[86] ... LaTeX:
https://a-quin.nl/nieuws/veiligheid-van-bruggen-sluizen-waarborgen-wie-wat-hoe/

[87] ... LaTeX:
https://www.gemeentesluis.nl/Bestuur_en_Organisatie/Wetten_Regels_Bekendmakingen

[88] ... LaTeX:
https://www.overijssel.nl/onderwerpen/verkeer-en-vervoer/varen-in-overijssel/informatie-bedieningstijden-sluizen-en-bruggen-noordwest-overijssel/

[89] ... LaTeX:
https://www.rijkswaterstaat.nl/water/wetten-regels-en-vergunningen

[90] ... LaTeX:
https://www.schuttevaer.nl/nieuws/actueel/2022/11/23/binnenvaart-zit-klem-tussen-regels-en-realiteit-kapotte-steigers-en-gesperde-sluizen-dwin

[91] ... LaTeX:
https://repository.officiele-overheidspublicaties.nl/CVDR/CVDR271406/1/html/CVDR271406_1.html

[92] ... LaTeX:
https://www.zeeland.nl/actueel/bedieningstijden-sluizen-en-bruggen

[93] ... LaTeX:
https://www.amsterdam.nl/verkeer-vervoer/varen-amsterdam/regels-varen/

[94] ... LaTeX:
https://www.schielandendekrimpenerwaard.nl/wat-doen-we/regels-en-afspraken-over-beheer-keur-en-leggers/

[95] ... LaTeX:
http://www.wetboek-online.nl/wet/Wet%20tot%20samenvoeging%20van%20de%20gemeenten%20Aardenburg%20en%20Sluis.html

[96] ... LaTeX:
https://www.rijnland.net/regels-op-een-rij/richtlijnen-en-akkoorden/alle-regelgeving-van-rijnland/

[97] ... LaTeX:
https://www.itbb.nl/diensten/advies-ce-markering-europese-richtlijnen/

[98] ... LaTeX:
https://www.portofamsterdam.com/nl/scheepvaart/zeevaart/regelgeving

[99] ... LaTeX:
https://www.watersportverbond.nl/nieuws/achterstallig-onderhoud-wachtplaatsen-bruggen-en-s

[100] ... LaTeX:
https://varendoejesamen.nl/nieuws

[101] ... LaTeX:
https://www.flevoland.nl/wat-doen-we/flevowegen-vlot-en-veilig-door-flevoland/water/varen-in-flevoland/bediening-bruggen-en-sluizen

[102] ... LaTeX:
https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32020L0012&from=DE

[103] ... LaTeX:
https://www.werkenvoornederland.nl/organisatie/rijkswaterstaat/ict-middelen-maken-om-bruggen-sluizen-en-tunnels-te-besturen

[104] ... LaTeX:
https://www.lobocom.nl/infra-bruggen-sluizen

[105] ... LaTeX:
https://waterrecreatienederland.nl/content/uploads/2018/04/richtlijnen-vaarwegen-2017.pdf

[106] ... LaTeX:
https://www.wetterskipfryslan.nl/melden-en-regelen/vergunningen-wetten-en-regels

[107] ... LaTeX:
https://www.onlinezeilschool.nl/sluizen/

[108] ... LaTeX:
https://www.provincie.drenthe.nl/onderwerpen/verkeer-vervoer/vaarwegen/rondje-drenthe/bedieningstijden/

Bronnen:

[109] ... LaTeX:
https://www.sciencedirect.com/science/article/pii/S0167642315001033

[110] ... LaTeX:
https://www.cas.mcmaster.ca/~lawford/papers/AVoCS2013.pdf

[111] ... LaTeX:
https://core.ac.uk/download/pdf/38891842.pdf

Therac

sheets

[112] ... LaTeX:
https://web.cs.ucdavis.edu/~rogaway/classes/188/winter04/therac-25.pdf

[113] ... LaTeX:
https://people.physics.carleton.ca/~drogers/egs_windows_collection/tsld008.htm [?]

[114] ... LaTeX:
https://en.wikipedia.org/wiki/Therac-25

[115] ... LaTeX:
https://www.youtube.com/watch?v=-7gVqBY52MY [?] reproduceren van de error. IN dit stuk wordt uitgelgd hoe het product werkt en waarom bepaalde beslssingen zijn genomen in de ontwerp/productiefase

[116] ... LaTeX:
https://www.bugsnag.com/blog/bug-day-race-condition-therac-25 kort artikel met daarin een opsomming van alle fouten in het systeem en een korte uitleg

[117] ... LaTeX:
https://www.bowdoin.edu/~allen/courses/cs260/readings/therac.pdf uitgebreid artikel over hoe de fout werd gereproduceerd en de resultaten daaruit voortkwamen. Alsnog werden er na de reproductie fase nog meer fouten gevonden.

[118] ... LaTeX:
https://hackaday.com/2015/10/26/killed-by-a-machine-the-therac-25/ artikel

[119] ... LaTeX:
https://ethicsunwrapped.utexas.edu/case-study/therac-25 onderzoeksartikel waarin de bug wordt uitgelgd: de racecondities, de bytepositie en het testen worden berkitiseerd envenals andere onderdelen van het softwareproces

[120] ... LaTeX:
https://thedailywtf.com/articles/the-therac-25-incident [?] onrealistisch testplan. In dit artikel egt de auteur het belang nog eens uit van goede requirements en implementatie, niet de software is waar het probleem ligt

[121] ... LaTeX:
https://www.computer.org/csdl/magazine/co/2017/11/mco2017110008/13rRUxAStVR [?] geschiedenis

[122] ... LaTeX:
http://computingcases.org/case_materials/therac/case_history/Case%20History.html

artikel

[123] ... LaTeX:
https://medium.com/swlh/software-architecture-therac-25-the-killer-radiation-machine-8a05e computer error. De ongeval en de malfunction nog een keer uitgelegd

[124] ... LaTeX:
http://www.ccnr.org/fatal_dose.html rapport

[125] ... LaTeX:
http://sunnyday.mit.edu/papers/therac.pdf

[126] ... LaTeX:
https://pubmed.ncbi.nlm.nih.gov/101762/

onderzoeksartkel

[127] ... LaTeX:
http://www1.cs.columbia.edu/~junfeng/08fa-e6998/sched/readings/therac25.pdf

[128] ... LaTeX:
https://ieeexplore.ieee.org/document/274940 uitgebreid artikel gaat hier ook wat meer over de hardware

[129] ... LaTeX:
https://www.linkedin.com/pulse/therac-25-industrial-design-engineering-systems-wang-ph-d- artikel waarin in 3 delen de problemaiekwordt blootgesteld

[130] ... LaTeX:
http://www.cse.msu.edu/~cse470/Public/Handouts/Therac/Therac_2.html case study sheets artikel waarin vooral de fabriikant ervan langs krijgt

[131] ... LaTeX:
http://users.csc.calpoly.edu/~jdalbey/SWE/Papers/THERAC25.html lessons learned. Vooral de begrippen betrouwbaarheid, welgevalligheid, veilgheid en gebruiksvriendelijkheid

[132] ... LaTeX:
https://bohr.wlu.ca/cp164/therac/therac25.htm root-cause analysis case study

[133] ... LaTeX:
https://dusk.geo.orst.edu/ethics/papers/Therac.Huff.pdf case study

[134] ... LaTeX:
https://www.sebokwiki.org/wiki/Medical_Radiation opzetten van systematische acceptaatie test met therac als voorbeeld

[135] ... LaTeX:
https://www.sciencedirect.com/science/article/pii/S1474667017448245 artikel waarin een diagnose plaatvindt voor het bedrijf en de ingenieur/ontwerper

[136] ... LaTeX:
https://magsilva.pro.br/apps/wiki/testing/Therac_25 rapport oorzaken aangegeven in artikel

[137] ... LaTeX:
https://www.chemeurope.com/en/encyclopedia/Therac-25.html het onderzoek en enkele ontwerptekeningen en oplossingen

[138] ... LaTeX:
https://pvs-studio.com/en/blog/posts/0438/

[139] ... LaTeX:
https://www.coursera.org/lecture/software-design-threats-mitigations/therac-25-case-study-VmQPa

[140] ... LaTeX:
https://www.semanticscholar.org/paper/The-story-of-the-Therac-25-in-LOTOS-Thomas/6c9c6024cf95aadae8b7edf1160e0e4500410eb9

[141] ... LaTeX:
https://news.ycombinator.com/item?id=21679287 wiki

[142] ... LaTeX:
https://en.wikibooks.org/wiki/Professionalism/Therac-25 analyse

[143] ... LaTeX:
https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.96.369&rep=rep1&type=pdf samenvatting

[144] ... LaTeX:
https://onlineethics.org/cases/resources-engineering-and-science-ethics/investigation-therac-25-accidents-abstract

rapport over de fouten die de verschillende partijen hebben gemaakt(overheid, ingenieurs, bedrijf, operators) en de verbeterpunten

[145] ... LaTeX:
https://www.cs.colostate.edu/~bieman/CS314/Notes/therac25.pdf [?] onderzoeksrapport

[146] ... LaTeX:
https://www.cs.ucf.edu/~dcm/Teaching/COP4600-Fall2010/Literature/Therac25-Leveson.pdf [?] slides online over het technisch mankement Wat is er gebeurd, nou het volgende: Normal radiation treatments: 6,000 rads over a 3 week period, under certain conditions Therac-25 was delivering 60,000 rads during one session. En wat ging er mis? Paradigm Shift

Therac-25 replaced expensive hardware safety interlocks with software controls Real-time software Design Race condition caused focusing element to be incorrectly set No indication of actual hardware settings Error messages appeared the same regardless of how important Error messages were difficult to understand All errors messages could be manually overridden

[147] ... LaTeX:
https://hci.cs.siue.edu/NSF/Files/Semester/Week13-2/PPT-Text/Slide13.html [?] oorzaak-gevolg diagram

[148] ... LaTeX:
https://www.thinkreliability.com/InstructorBlogs/Blog-Therac-25.pdf [?] veiligheidsanalyse naar de rapportage van foutmeldingen, de beslissingsmatrix waarmee het programma wordt uitgevoerd en de software-analyse door een consultat

[149] ... LaTeX:
https://sqa.stackexchange.com/questions/9798/asking-for-help-with-this-therac-25-bugged-c

Krakend zorgssteem door covid-19 in suriname

vaccinatieterkort communicatie met bevolking communicatie met binnenland testen van vaccinaties besmetting vanuit eht buitenland isolatie na vakantie en voor toeristen tekort aan ic-personeel tekort aan ic-bedden tekort aan zuurtstof tekort aan middelen

Wat blijkt hieruit: de impact van de crisis wereldwijd de afhnakelijkheid van landen op goede samenwerking Nut en noodzaak van regelgeving Naveling van maatregels Communicatie over beleid vanuit de overheid naar de burgers Belang van een verzorgingstaat Een wetenschappelijke ontwikkeling die kan inspelen op gevoelige 'trends De impact van een lockdown op de economie Afschaling van andere noodzakelijke no-covid zorg De bereikbaarheid van een ziekenhuis Waar heeft het toe geleid?

[150] ... LaTeX:
https://www.waterkant.net/suriname/2007/02/06/school-in-suriname-gesloten-om-zenuwgasvoorr

[151] ... LaTeX:
https://nl.wikipedia.org/wiki/Nationaal_Co%C3%B6rdinatiecentrum_voor_Rampenbeheersing

[152] ... LaTeX:
https://www.examenkamer.nl/index.php/27-vca-examens-in-suriname

Waterramp suriname met cyanice

boeing 737 crashes

algemene vragen oorzaken

[153] ... LaTeX:
https://www.seattletimes.com/business/boeing-aerospace/what-led-to-boeings-737-max-crisis-a-qa/

[154] ... LaTeX:
https://www.schneier.com/blog/archives/2019/04/excellent_analy.html fout in de software

[155] ... LaTeX:
https://www.forbes.com/sites/georgeavetisov/2019/03/19/malware-at-30000-feet-what-the-737-max-says-about-the-state-of-airplane-software-security?sh=4d26f7052a9e het nationaal veiligheidsbelang

[156] ... LaTeX:
https://www.forbes.com/sites/lorenthompson/2020/11/23/five-reasons-return-of-boeings-737-max-to-service-is-important-to-national-security/?sh=2128ea552018 falend toezicht

[157] ... LaTeX:
https://www.seattletimes.com/business/boeing-aerospace/failed-certification-faa-missed-safety-issues-in-the-737-max-system-implicated-in-the-lio onderzoeksrapport

[158] ... LaTeX:
https://www.faa.gov/foia/electronic_reading_room/boeing_reading_room/media/737_RTS_Summary.pdf

[159] ... LaTeX:
https://en.wikipedia.org/wiki/Boeing_737_MAX_groundings veiligheidsrisico's menselijke fouten

[160] ... LaTeX:
https://www.theverge.com/2019/5/2/18518176/boeing-737-max-crash-problems-human-error-mcas- overzicht van crashes

[161] ... LaTeX:
https://www.theverge.com/2019/3/22/18275736/boeing-737-max-plane-crashes-grounded-problems veiligheidsopmerking

[162] ... LaTeX:
https://www.airlineratings.com/news/boeings-737-max-will-one-safest-aircraft-history/ aanpassingen

[163] ... LaTeX:
https://www.boeing.com/commercial/737max/737-max-software-updates.page waarschuwingen//output signalen

[164] ... LaTeX:
https://leehamnews.com/2020/11/24/boeing-737-max-changes-beyond-mcas/ software gerelateerde fouten

[165] ... LaTeX:
https://spectrum.ieee.org/aerospace/aviation/how-the-boeing-737-max-disaster-looks-to-a-s onderzoeksrapport de rol van de publieke opinie

[166] ... LaTeX:
https://pubsonline.informs.org/do/10.1287/orms.2019.05.05/full/ onderzoek van europese luchtvaart agentschap

[167] ... LaTeX:
https://www.easa.europa.eu/newsroom-and-events/news/easa-declares-boeing-737-max-safe-return-service-europe veiligheidsvraagstuk

[168] ... LaTeX:
https://phys.org/news/2019-03-boeing-max-safety-tragedies.html artikel over sensoren

[169] ... LaTeX:
https://www.flightglobal.com/airframers/boeing-delays-737-max-10-deliveries-two-years-to-
142245.article goedkeuring van europese luchtvaart autoriteiten advies aan de faa

[170] ... LaTeX:
https://www.hstoday.us/subject-matter-areas/airport-aviation-security/
oig-tells-faa-to-improve-safety-oversight-following-boeing-737-max-review/

[171] ... LaTeX:
https://www.geekwire.com/2020/faas-go-ahead-737-maxs-return-flight-kicks-off-massive-soft

[172] ... LaTeX:
https://www.researchgate.net/publication/338420944_A_Promise_Theoretic_
Account_of_the_Boeing_737_Max_MCAS_Algorithm_Affair achtergrond informatie

[173] ... LaTeX:
http://www.b737.org.uk/mcas.htm algemeen vertrouwen

[174] ... LaTeX:
https://www.cnbc.com/2019/05/16/what-you-need-to-know-about-boeings-737-max-crisis.
html toestemming europese autoriteiten problemen

[175] ... LaTeX:
https://arstechnica.com/information-technology/2020/01/
737-max-fix-slips-to-summer-and-thats-just-one-of-boeings-problems/ uitgebreid artikel over de onderzoeken en het vliegverbod

[176] ... LaTeX:
https://www.cnet.com/news/boeing-737-max-8-all-about-the-aircraft-flight-ban-and-investig
computers als oorzaak lessons learned

[177] ... LaTeX:
https://www.designnews.com/electronics-test/5-lessons-learn-boeing-737-max-fiasco

[178] ... LaTeX:
https://www.eurocontrol.int/publication/effects-network-extra-standby-aircraft-and-boeing-
single point of failure

[179] ... LaTeX:
https://dmd.solutions/blog/2019/04/05/how-a-single-point-of-failure-spof-in-the-mcas-soft

[180] ... LaTeX:
https://asiatimes.com/2021/01/boeings-737-max-and-the-fear-of-flying/ lijst van tehnische aanpassingen

[181] ... LaTeX:
https://www.caa.co.uk/Consumers/Guide-to-aviation/Boeing-737-MAX/

[182] ... LaTeX:
https://dsm.forecastinternational.com/wordpress/2020/12/14/
airbus-and-boeing-report-november-2020-commercial-aircraft-orders-and-deliveries/
code lek

[183] ... LaTeX:
https://www.wired.com/story/boeing-787-code-leak-security-flaws/

[184] ... LaTeX:
https://www.fitchratings.com/research/corporate-finance/boeing-737-max-return-backlog-risks-remain-16-09-2020 Cultuurverandering, deregulatie, systeemwijziging of gewoon een kwestie van competentie

[185] ... LaTeX:
https://www.aerospacetestinginternational.com/features/what-broke-the-737-max.html extra aanpassingen

[186] ... LaTeX:
https://theaircurrent.com/aviation-safety/boeings-737-max-software-done-but-regulators-pl
wat ging er mis een analyse van een ex-iloot De utoriteiten waren op de hoogte

[187] ... LaTeX:
https://www.extremetech.com/extreme/303373-the-faa-knew-the-737-max-was-dangerous-and-kep
kwaliteiten van het alarmsysteem niet goed bekend

[188] ... LaTeX:
https://time.com/5687473/boeing-737-alarm-system/

[189] ... LaTeX:
https://www.nasdaq.com/articles/boeing-gets-dealt-another-737-max-cancellation-blow.-what-it-means-for-boeing-stock-2020

[190] ... LaTeX:
https://www.eetimes.com/boeing-crashes-highlight-a-worsening-reliability-crisis/
veiligheidsvraagstuk

[191] ... LaTeX:
https://www.latimes.com/business/story/2019-12-11/faa-boeing-737-max-crashes
probleemanalyse, veiligheidsvraagstuk

[192] ... LaTeX:
https://www.politico.com/story/2019/03/15/boeing-737-max-grounding-1223072 falend toezicht

[193] ... LaTeX:
https://www.pogo.org/analysis/2019/10/corrupted-oversight-the-faa-boeing-and-the-737-max/

[194] ... LaTeX:
https://www.afacwa.org/the_inside_story_of_mcas_seattle_times doelstellingen en veiligheidsvraagstukken

[195] ... LaTeX:
https://www.marxist.com/737-max-scandal-boeing-putting-profits-before-safety.htm

[196] ... LaTeX:
https://finance.yahoo.com/news/australia-lifts-ban-boeing-737-035817682.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAHZCJYy_0A5VS2WiPoCvH4xdrRNkmkdsv5EWJ2RLIz_AS-rxsTty6AF1_HlmJiRyWYqCXDi4p0Xs4isYkNkCq2Pfo-pQ60Xz_IfTNjm4FgoZiBMC4zpZlB6F0fwecrjE_ujAXZzG4xPJnWCd8-G3VLlPTY8h3H31eQ1i8hY9AIyy autoriteiten krijgen tik op de vingers

[197] ... LaTeX:
https://medium.com/@jpaulreed/the-737max-and-why-software-engineers-should-pay-attention-

[198] ... LaTeX:
https://news.ycombinator.com/item?id=19414775

[199] ... LaTeX:
https://www.bbc.com/news/55366320

[200] ... LaTeX:
https://www.marketscreener.com/news/latest/China-studies-Boeing-737-MAX-recertification-wa
motor in brand

[201] ... LaTeX:
https://www.euractiv.com/section/aviation/news/boeing-grounds-777s-after-engine-fire/

[202] ... LaTeX:
https://gulfnews.com/business/aviation/uae-airspace-to-see-return-of-boeing-737-max-1.
1613627548923 motor in brand gevlogen

[203] ... LaTeX:
https://techxplore.com/news/2021-02-boeing-urges-grounding-777s.html

[204] ... LaTeX:
https://www.politico.eu/article/uk-temporarily-bans-some-boeing-aircraft-after-pratt-whitn

[205] ... LaTeX:
https://www.timeslive.co.za/news/world/2021-02-23-damage-to-united-boeing-777-engine-cons
faa was niet kritisch genoeg

[206] ... LaTeX:
https://federalnewsnetwork.com/government-news/2021/02/
federal-watchdog-blasts-faa-over-certification-of-boeing-jet/

china explosion 2015 tianjin verhaal van brandweermannen

artikel

invloed van social media

[207] ... LaTeX:
https://www.economist.com/asia/2015/08/18/a-blast-in-tianjin-sets-off-an-explosion-online

[208] ... LaTeX:
https://america.cgtn.com/2015/08/12/explosion-reported-in-tianjin-china

[209] ... LaTeX:
https://factcheck.afp.com/no-photo-was-taken-chinese-city-tianjin-august-2015

vergelijking van twee rampen

[210] ... LaTeX:
https://airshare.air-inc.com/how-does-the-beirut-explosion-compare-to-tianjin

overheid en media

[211] ... LaTeX:
https://newbloommag.net/2015/08/17/tianjin-explosion/

chemische industrie ondeer de loep

[212] ... LaTeX:
https://www.voanews.com/east-asia-pacific/tianjin-blast-puts-spotlight-chemical-industry

[213] ... LaTeX:
https://abcnews.go.com/International/apocalyptic-aftermath-devastating-images-tianjin-chir
story?id=33057017

[214] ... LaTeX:
https://www.reachingoutacrossdurham.co.uk/osk/tianjin-explosion-2021

[215] ... LaTeX:
https://aiche.onlinelibrary.wiley.com/doi/abs/10.1002/prs.11789

[216] ... LaTeX:
https://www.automotivelogistics.media/thousands-of-cars-destroyed-in-tianjin-port-explosio
13570.article

[217] ... LaTeX:
https://www.joc.com/port-news/asian-ports/port-tianjin/
tianjin-port-explosions-could-be-most-expensive-maritime-disaster_20150826.
html

[218] ... LaTeX:
https://www.bloomberg.com/news/articles/2015-08-12/explosion-in-northern-china-shatters-wi

[219] ... LaTeX:
https://unece.org/fileadmin/DAM/env/documents/2016/TEIA/OECD_WGCA_24-27_OCT_
2016/Session_3_Zhao_-__Introduction_of_Tianjin_Accident_-_Jinsong_Zhao.pdf
gemaakte fouten

[220] ... LaTeX:
https://porteconomicsmanagement.org/pemp/contents/part6/port-resilience/
site-2015-tianjin-port-explosions/

[221] ... LaTeX:
https://www.alamy.com/stock-image-tianjin-china-17th-aug-2015-tianjin-explosion-aftermath
html

[222] ... LaTeX:
https://www.popularmechanics.com/technology/news/a16871/
massive-explosions-china-city-of-tianjin/

[223] ... LaTeX:
https://www.imago-images.com/st/0080815934

[224] ... LaTeX:
https://www.chemistryworld.com/news/deadly-chemical-blast-at-chinese-port/
8857.article

[225] ... LaTeX:
https://www.process-worldwide.com/tianjin-explosion-from-chemical-perspective-insights-and
vergelijking met andere explosies

[226] ... LaTeX:
https://apnews.com/article/lebanon-fires-us-news-explosions-middle-east-53f4206a7f1db0812
invloed van de ramp op de industrie

[227] ... LaTeX:
https://fortune.com/2015/08/14/tianjin-port-explosion-shipping-delays/ is er
sprake van een doofpot

[228] ... LaTeX:
https://www.washingtontimes.com/news/2015/aug/20/inside-china-tianjin-explosions-cover-up-
eigendomsverzekering

[229] ... LaTeX:
https://www.artemis.bm/news/tianjin-explosions-property-insurance-loss-could-reach-3-5bn-

[230] ... LaTeX:
https://www.thechinastory.org/yearbooks/yearbook-2015/forum-the-abyss-%E5%9D%8E/tianjin-explosions/ effecten op de lange termijn

[231] ... LaTeX:
https://www.flexport.com/blog/tianjin-explosion-effect-on-supply-chains/

[232] ... LaTeX:
https://www.cicm.org.my/images/articles/CICM-Article-on-Tianjin-Blast-Oct2015.pdf lessons learned

[233] ... LaTeX:
https://www.genre.com/knowledge/blog/lessons-from-the-tianjin-explosion-en.html

[234] ... LaTeX:
https://www.ft.com/content/ad62904c-44ce-11e5-b3b2-1672f710807b

[235] ... LaTeX:
https://www.huffingtonpost.co.uk/2015/08/13/tianjin-explosion-china-shocking-footage-caugh
n_7980888.html

[236] ... LaTeX:
https://www.thatsmags.com/china/post/19189/massive-fire-rocks-tianjin-port gevolgen voor de industrie

[237] ... LaTeX:
https://www.everstream.ai/risk-center/special-reports/the-jiangsu-yancheng-explosion/

[238] ... LaTeX:
https://www.newyorker.com/news/news-desk/after-tianjin-an-outbreak-of-mistrust-in-china framing vanuit de chinese media

[239] ... LaTeX:
https://www.neliti.com/publications/101997/the-chinese-media-framing-of-the-2015s-tianjin-

[240] ... LaTeX:
https://www.reinsurancene.ws/chinese-insurers-settle-1-5-billion-tianjin-blast-claims/ niewsartikel

[241] ... LaTeX:
https://www.thechemicalengineer.com/news/update-78-confirmed-dead-after-chinese-chemicals-

[242] ... LaTeX:
https://www.caixinglobal.com/2016-11-10/chinese-executive-receives-suspended-death-senten
html toegang tot de ramplplek vanuit de okale journalistiek

[243] ... LaTeX:
https://chinadigitaltimes.net/2015/08/he-xiaoxin-how-far-can-i-go-and-how-much-can-i-do/ artikel

[244] ... LaTeX:
https://www.wnpr.org/post/china-examines-aftermath-immense-twin-explosions-killed-dozens

[245] ... LaTeX:
https://theconversation.com/what-is-ammonium-nitrate-the-chemical-that-exploded-in-beirut-

[246] ... LaTeX:
https://chemicalwatch.com/36730/nationwide-inspections-in-china-follow-tianjin-explosion

[247] ... LaTeX:
https://www.thehindu.com/news/international/investigation-begun-into-china-gas-explosion-a
article34818324.ece

[248] ... LaTeX:
https://santiagotimes.cl/2019/03/24/64-killed-600-injured-in-china-chemical-plant-blast/
oorzaken

[249] ... LaTeX:
https://klingecorp.com/blog/what-caused-the-tianjin-explosions/ case study

mismanagement als oorzaak

[250] ... LaTeX:
https://www.nytimes.com/2016/02/06/world/asia/tianjin-explosions-were-result-of-mismanagem
html

[251] ... LaTeX:
https://cen.acs.org/articles/94/web/2016/02/Chinese-Investigators-Identify-Cause-Tianjin.
html autoriteiten publiceren onderoeksrapport

[252] ... LaTeX:
https://cen.acs.org/articles/94/i7/Chinese-Investigators-Identify-Cause-Tianjin.
html fotos van de rampplek

[253] ... LaTeX:
https://www.theatlantic.com/photo/2015/08/photos-of-the-aftermath-of-the-massive-explosion
401228/

[254] ... LaTeX:
https://edition.cnn.com/2015/08/13/asia/china-tianjin-explosions/index.html
niuwesartiekel

[255] ... LaTeX:
https://www.cbc.ca/news/world/china-explosion-tianjin-1.3189455 verantwoorde-
lijke

[256] ... LaTeX:
https://www.thestar.com/news/world/2016/11/09/chinese-executive-gets-death-sentence-over-t
html

risicobeperking/controle

[257] ... LaTeX:
https://www.swissre.com/en/china/news-insights/articles/
analysis-of-tianjin-port-explosion-china.html

censuur

[258] ... LaTeX:
https://foreignpolicy.com/2015/09/10/censored-china-young-survivor-tianjin-explosion-viral

censuur

[259] ... LaTeX:
https://qz.com/756872/a-year-after-the-tianjin-blast-public-mourning-and-discussion-about

verschillende artikelen

[260] ... LaTeX:
https://www.scmp.com/topics/tianjin-warehouse-explosion-2015

[261] ... LaTeX:
https://www.wsj.com/articles/BL-CJB-27664

[262] ... LaTeX:
https://www.nbcnews.com/news/world/tianjin-explosions-californian-witness-filmed-dramatic-

[263] ... LaTeX:
https://ui.adsabs.harvard.edu/abs/2016AGUFM.S13D..06P/abstract afwikkeling van de ramp

[264] ... LaTeX:
https://chinadialogue.net/en/pollution/9188-back-to-the-blast-zone-one-year-after-the-tia

[265] ... LaTeX:
https://www.wired.com/2015/08/chinas-huge-tianjin-explosion-looked-like-space/

[266] ... LaTeX:
https://www.abc.net.au/news/2015-08-13/explosion-rocks-north-chinese-city-of-tianjin/6693336?nw=0

ambtenaren onderzocht

risico-inschatting

[267] ... LaTeX:
https://www.mdpi.com/2071-1050/12/3/1169/htm

[268] ... LaTeX:
https://www.mdpi.com/2071-1050/12/3/1169/htm

[269] ... LaTeX:
https://www.cbsnews.com/news/tianjin-port-china-massive-explosion-hundreds-injured/

[270] ... LaTeX:
https://www.hkjcdpri.org.hk/download/casestudies/Tianjin_CASE.pdf

[271] ... LaTeX:
https://time.com/3996168/tianjin-explosion-china-pictures/

onderzoeksrapport

[272] ... LaTeX:
https://www.hfw.com/Tianjin-Port-explosion-August-2015

[273] ... LaTeX:
https://news.un.org/en/story/2015/08/506912-following-tianjin-explosion-un-expert-calls-ch

[274] ... LaTeX:
https://www.france24.com/en/20150812-huge-explosions-rock-chinese-city-tianjin

[275] ... LaTeX:
https://choice.npr.org/index.html?origin=https://www.npr.org/2015/08/14/432280627/what-caused-the-warehouse-explosions-in-tianjin-china 123 verantwoordelijken

[276] ... LaTeX:
https://www.bbc.com/news/world-asia-china-35506311

[277] ... LaTeX:
https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%
2fwww.washingtonpost.com%2fnews%2fworldviews%2fwp%2f2015%2f08%2f12%
2fvideos-show-chinese-city-of-tianjin-rocked-by-enormous-explosion%2f

lang artiekel

[278] ... LaTeX:
https://www.businessinsider.com/the-chemical-explosion-in-china-killed-more-than-100-peop
international=true&r=US&IR=T

[279] ... LaTeX:
https://pubmed.ncbi.nlm.nih.gov/27311537/

[280] ... LaTeX:
https://www.reuters.com/article/us-china-blast-insurance-idUSKCN0QM0N220150817

[281] ... LaTeX:
https://www.sciencedirect.com/science/article/abs/pii/S0305417916300079

[282] ... LaTeX:
https://en.wikipedia.org/wiki/2015_Tianjin_explosions

[283] ... LaTeX:
https://www.bbc.com/news/world-asia-china-33844084

[284] ... LaTeX:
https://www.independent.co.uk/news/world/asia/tianjin-explosion-photos-china-chemical-fact
html veiligheidshandhaving

[285] ... LaTeX:
https://www.ilo.org/legacy/english/protection/safework/ctrl_banding/toolkit/
main_guide.pdf

[286] ... LaTeX:
https://echa.europa.eu/documents/10162/21332507/guide_chemical_safety_sme_en.
pdf

[287] ... LaTeX:
https://ec.europa.eu/taxation_customs/dds2/SAMANCTA/EN/Safety/AppendixD_EN.
htm

[288] ... LaTeX:
https://www.ilo.org/safework/info/publications/WCMS_113134/lang--en/index.htm

tesla autopilot crashes

veiligheidsrisico

[289] ... LaTeX:
https://spectrum.ieee.org/cars-that-think/transportation/self-driving/
three-small-stickers-on-road-can-steer-tesla-autopilot-into-oncoming-lane

[290] ... LaTeX:
https://www.tesla.com/VehicleSafetyReport veiligheidsrapport mbt autopilot

[291] ... LaTeX:
https://electrek.co/2020/07/31/tesla-q2-2020-safety-report-strong-improvement-autopilot-a
consumentenrapport bluetooth veiligheidsvraagstuk

[292] ... LaTeX:
https://www.wired.com/story/tesla-model-x-hack-bluetooth/ veiigheidsvraagstuk vanwege touch screen

[293] ... LaTeX:
https://www.consumerreports.org/car-recalls-defects/nhtsa-asks-tesla-to-recall-model-s-model-x-touch-screen-safety-issues/ veiligheidsvraagstuk

[294] ... LaTeX:
https://cio.economictimes.indiatimes.com/news/digital-security/security-researchers-hack-steal-tesla-model-x-within-minutes/79406553 veiligheidsvraagstuk rapport over autopilot

[295] ... LaTeX:
https://www.forbes.com/sites/bradtempleton/2019/09/06/ntsb-report-on-tesla-autopilot-accident-shows-whats-inside-and-its-not-pretty-for-fsd/?sh=6905e7d4dc55 de invloed van de bestuurder bij tesla ongeluk

[296] ... LaTeX:
https://techcrunch.com/2021/01/08/nhtsa-tesla-sudden-unintended-acceleration-driver-error/ veiligheidsvraagstuk

[297] ... LaTeX:
https://www.darkreading.com/threat-intelligence/security-risks-discovered-in-tesla-backup-d/d-id/1339462 veiligheidsvraagstuk

[298] ... LaTeX:
https://portswigger.net/daily-swig/web-based-attack-crashes-tesla-driver-interface veiigheidsvraagstuk

[299] ... LaTeX:
https://www.cnbc.com/2019/04/03/chinese-hackers-tricked-teslas-autopilot-into-switching-la html veiligheidsvraagstuk veiligheidsvraagstuk

[300] ... LaTeX:
https://www.vox.com/recode/2020/2/26/21154502/tesla-autopilot-fatal-crashes rapport over ongeluk veiligheidsvraagstuk veiligheidsvraagstuk

[301] ... LaTeX:
https://www.caranddriver.com/news/a29369387/nhtsa-tesla-safety/ veiligheidsvraagstuk ransomware aanval op tesla tesla batterij is veiligheidsvraagstuk geworden

[302] ... LaTeX:
https://www.latimes.com/business/story/2020-07-01/federal-safety-officials-probe-tesla-bat ongeluk

[303] ... LaTeX:
https://www.bbc.com/news/technology-51645566 veiligheidsvraagstuk veiligheidsvraagstuk

[304] ... LaTeX:
https://www.thedrive.com/news/33272/tesla-discarded-old-car-parts-with-customers-personal- dodelijk ongeluk

[305] ... LaTeX:
https://www.theguardian.com/technology/2018/jun/07/tesla-fatal-crash-silicon-valley-autopi veiligheidsvraagstuk: ransomware veiligheidsvraagstuk: medewerker in de fout

[306] ... LaTeX:
https://digitalguardian.com/blog/tesla-data-theft-case-illustrates-danger-insider-threat

[307] ... LaTeX:
https://jalopnik.com/tesla-is-stopping-some-model-3-production-report-1846353323
veiligheidsvraagstuk: hackers je systeem laten testen verdedigen tegenover ransomware veiligheidsrisico prijzen omlaag autopilot

[308] ... LaTeX:
https://www.bloomberg.com/graphics/2019-tesla-model-3-survey/autopilot.html
malware door een medewerker

[309] ... LaTeX:
https://www.teslarati.com/tesla-employee-fbi-thwarts-russian-cybersecurity-attack/
dodelijk ongeluk

[310] ... LaTeX:
https://www.marketwatch.com/story/apple-engineer-killed-in-tesla-suv-crash-on-silicon-val

[311] ... LaTeX:
https://www.marketwatch.com/story/nearly-100-of-teslas-stolen-in-the-us-since-2011-have-b
waarom een tesla stelen bijna onmogelijk is

[312] ... LaTeX:
https://www.welivesecurity.com/2019/03/25/white-hats-hack-tesla-keep/ veiligheidsonderzoek

[313] ... LaTeX:
https://www.tripwire.com/state-of-security/security-data-protection/
tesla-encouraging-good-faith-security-research-in-bug-bounty-program/ softwarefout maakt diestal mogelijk

[314] ... LaTeX:
https://www.bankinfosecurity.com/tesla-model-x-stolen-in-minutes-using-software-flaws-a-1
fouten ontdekt in onderzoek

[315] ... LaTeX:
https://www.cnet.com/roadshow/news/tesla-ev-appeal-loyalty-study/

[316] ... LaTeX:
https://www.bbc.com/news/technology-56156801

[317] ... LaTeX:
https://www.washingtonpost.com/technology/2023/06/10/
tesla-autopilot-crashes-elon-musk/

[318] ... LaTeX:
https://www.autopilotreview.com/tesla-autopilot-accidents-causes/

[319] ... LaTeX:
https://www.skynettoday.com/briefs/tesla-investigations

[320] ... LaTeX:
https://www.tesladeaths.com/

tesla cloud gehacked

[321] ... LaTeX:
https://arstechnica.com/information-technology/2018/02/
tesla-cloud-resources-are-hacked-to-run-cryptocurrency-mining-malware/

[322] ... LaTeX:
https://www.motortrend.com/news/tesla-model-y-ev-safety-quality-issues-problems/

[323] ... LaTeX:
https://securityledger.com/2019/04/hackers-remotely-steer-tesla-model-s-using-autopilot-sy

[324] ... LaTeX:
https://www.pcmag.com/news/report-tesla-suspends-model-3-production-in-california-until-ma

[325] ... LaTeX:
https://www.scmp.com/business/money/article/3121173/
tesla-conduct-complete-self-inspection-after-chinese-regulators

[326] ... LaTeX:
https://www.businesswire.com/news/home/20180220005222/en/
RedLock-Releases-Cloud-Security-Report-Highlighting-Focus-on-Shared-Responsibilities-Unco

[327] ... LaTeX:
https://www.epa.gov/automotive-trends/highlights-automotive-trends-report

[328] ... LaTeX:
https://www.livemint.com/Companies/o2QLbtJc9EQ7ZcpxqgFbBP/
Teslas-reward-for-finding-security-bugs-Model-3.html

[329] ... LaTeX:
https://revealnews.org/blog/tesla-fired-safety-official-for-reporting-unsafe-conditions-la

[330] ... LaTeX:
https://heimdalsecurity.com/blog/security-alert-teslacrypt-4-0-unbreakable-encryption-wors

[331] ... LaTeX:
https://www.eweek.com/cloud/tesla-cloud-account-data-breach-revealed-in-redlock-security-

[332] ... LaTeX:
https://www.theverge.com/2020/10/21/21527577/tesla-full-self-driving-autopilot-beta-softwa

[333] ... LaTeX:
file:///C:/Users/gally/Downloads/applsci-10-02749-v2.pdf

[334] ... LaTeX:
https://www.braincreators.com/brainpower/insights/teslas-data-engine-and-what-we-should-al

[335] ... LaTeX:
https://bernardmarr.com/default.asp?contentID=1251

[336] ... LaTeX:
https://arstechnica.com/cars/2019/10/how-teslas-latest-acquisition-could-accelerate-autopi

[337] ... LaTeX:
https://towardsdatascience.com/teslas-deep-learning-at-scale-7eed85b235d3

[338] ... LaTeX:
file:///C:/Users/gally/Downloads/applsci-10-02749-v2.pdf

[339] ... LaTeX:
https://www.techiexpert.com/how-tesla-is-using-artificial-intelligence-and-big-data/

[340] ... LaTeX:
https://www.analyticssteps.com/blogs/how-tesla-making-use-artificial-intelligence-its-oper

[341] ... LaTeX:
https://www.forbes.com/sites/bernardmarr/2018/01/08/
the-amazing-ways-tesla-is-using-artificial-intelligence-and-big-data/?sh=
5e396aa24270

[342] ... LaTeX:
https://www.cnn.com/2021/04/21/tech/tesla-full-self-driving-launch/index.
html

[343] ... LaTeX:
https://www.theverge.com/2021/3/18/22338427/tesla-autopilot-crash-michigan-nhtsa-investiga

[344] ... LaTeX:
https://www.wionews.com/technology/doctor-among-victims-of-lethal-tesla-car-crash-in-texa

[345] ... LaTeX:
https://www.bloomberg.com/news/newsletters/2021-06-23/
hyperdrive-daily-after-30-tesla-crashes-what-s-a-regulator-to-do

[346] ... LaTeX:
https://en.wikipedia.org/wiki/Tesla_Autopilot

[347] ... LaTeX:
https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety

[348] ... LaTeX:
https://www.caradvice.com.au/947080/elon-musk-responds-to-deadly-texas-tesla-crash-as-con

[349] ... LaTeX:
https://usa.streetsblog.org/2021/04/19/regulators-could-have-prevented-fatal-tesla-crash/

[350] ... LaTeX:
https://www.brookings.edu/research/autonomous-vehicles-as-a-killer-app-for-ai/

[351] ... LaTeX:
https://www.latimes.com/business/story/2020-02-24/autopilot-data-secrecy

[352] ... LaTeX:
https://www.jdsupra.com/post/contentViewerEmbed.aspx?fid=
9844cae0-aa5a-45a5-988f-7f02fa5709c1

[353] ... LaTeX:
https://www.washingtonpost.com/technology/2020/10/21/tesla-self-driving/

[354] ... LaTeX:
https://spectrum.ieee.org/cars-that-think/transportation/self-driving/
fatal-tesla-autopilot-crash-reminds-us-that-robots-arent-perfect

[355] ... LaTeX:
https://thenextweb.com/news/another-tesla-owner-is-dead-because-of-autopilot

[356] ... LaTeX:
https://towardsdatascience.com/another-self-driving-car-accident-another-ai-development-le

[357] ... LaTeX:
https://www.theautochannel.com/news/2021/07/21/1024631-is-it-still-wrongful-death-if-car-
html

[358] ... LaTeX:
https://ai.stackexchange.com/questions/1488/why-did-a-tesla-car-mistake-a-truck-with-a-br

[359] ... LaTeX:
https://resources.tasking.com/p/benefits-tesla-autopilot-and-how-adas-will-save-lives

[360] ... LaTeX:
https://www.jipitec.eu/issues/jipitec-9-3-2018/4806

[361] ... LaTeX:
https://static.tti.tamu.edu/conferences/traffic-safety19/presentations/lunch/harkey.pdf

[362] ... LaTeX:
https://thepressfree.com/have-google-and-amazon-backed-the-wrong-technology/

[363] ... LaTeX:
https://www.irishtimes.com/business/innovation/robotaxis-have-google-and-amazon-backed-the-4626749

[364] ... LaTeX:
https://www.afr.com/technology/how-teslas-autopilot-got-it-wrong-in-fatal-crash-20160704-

[365] ... LaTeX:
https://economictimes.indiatimes.com/markets/stocks/news/what-me-worry-fed-chiefs-emotional-tone-can-drive-markets-study-suggests/articleshow/84618073.cms

[366] ... LaTeX:
https://www.ehstoday.com/safety/article/21919260/ntsb-fatal-crash-involving-tesla-autopilo

[367] ... LaTeX:
https://www.vanityfair.com/news/2016/07/how-the-media-screwed-up-the-fatal-tesla-accident

tesla crash report

[368] ... LaTeX:
https://www.reuters.com/business/autos-transportation/us-safety-agency-says-it-has-opened-probes-into-10-tesla-crash-deaths-since-2016-2021-06-

[369] ... LaTeX:
https://www.politico.com/news/2021/05/18/ntsb-tesla-owner-was-in-drivers-seat-before-apri

[370] ... LaTeX:
https://www.theverge.com/2021/5/10/22429198/tesla-ntsb-texas-crash-driverless-preliminary-

[371] ... LaTeX:
https://www.cnet.com/roadshow/news/tesla-autopilot-nhtsa-crash-report-self-driving-car-dri

[372] ... LaTeX:
https://abc11.com/tesla-crash-battery-fire-national-transportation-safety-board-driverless-10619772/

[373] ... LaTeX:
https://www.businessinsider.com/tesla-autopilot-crashes-regulators-open-probes-into-30-rep international=true&r=US&IR=T

[374] ... LaTeX:
https://driving.ca/column/lorraine/lorraine-explains-what-the-nhtsas-self-driving-car-cras

[375] ... LaTeX:
https://www.teslarati.com/tesla-model-s-crash-texas-ntsb-preliminary-report/

[376] ... LaTeX:
https://insideevs.com/news/506498/ntsb-report-tesla-texas-crash/

[377] ... LaTeX:
https://electrek.co/2021/06/03/tesla-tsla-crashes-report-new-orders-in-china-free-falling

[378] ... LaTeX:
https://www.newsy.com/stories/ntsb-releases-report-on-fatal-tesla-crash/

[379] ... LaTeX:
https://www.ndtv.com/world-news/autopilot-not-used-in-april-tesla-crash-says-us-report-24

[380] ... LaTeX:
https://www.autocar.co.nz/autocar-news-app/fatal-driverless-tesla-crash-report-shows-autop

[381] ... LaTeX:
https://teleperformance-waha.sabacloud.com/Saba/Web_spf/EU2PRD0152/app/
dashboard

[382] ... LaTeX:
https://www.independent.co.uk/news/world/americas/tesla-texas-crash-model-s-autopilot-b184
html

[383] ... LaTeX:
https://www.wired.com/2017/01/probing-teslas-deadly-crash-feds-say-yay-self-driving/

[384] ... LaTeX:
https://saferoads.org/wp-content/uploads/2020/03/AV-Crash-List-with-Photos-February-2020.
pdf

[385] ... LaTeX:
https://mashable.com/article/nthsa-tesla-autopilot-model-x-crash-investigation

[386] ... LaTeX:
https://www.usnews.com/news/top-news/articles/2021-03-18/
us-safety-agency-reviewing-23-tesla-crashes-three-from-recent-weeks

[387] ... LaTeX:
https://chicago.suntimes.com/consumer-affairs/2021/6/30/22557122/
nhtsa-automated-driving-crash-reports-tesla-national-highway-traffic-safety-administratio

[388] ... LaTeX:
https://arstechnica.com/cars/2021/05/ntsb-finds-no-reason-to-suspect-autopilot-in-fatal-te

[389] ... LaTeX:
https://jalopnik.com/the-ntsb-to-partially-blame-teslas-autopilot-in-fatal-c-1803136365

[390] ... LaTeX:
https://www.latimes.com/business/autos/la-fi-hy-tesla-autopilot-20170119-story.
html

[391] ... LaTeX:
https://www.vice.com/en/article/z3xxaw/ntsb-releases-preliminary-report-on-tesla-crash-tha

[392] ... LaTeX:
https://choice.npr.org/index.html?origin=https://www.npr.org/2018/06/07/
618081406/no-driver-input-detected-in-seconds-before-deadly-tesla-crash-ntsb-finds

[393] ... LaTeX:
https://www.click2houston.com/news/local/2021/04/18/
2-men-dead-after-fiery-tesla-crash-in-spring-officials-say/

[394] ... LaTeX:
https://static.nhtsa.gov/odi/inv/2016/INCLA-PE16007-7876.pdf

[395] ... LaTeX:
https://www.firstpost.com/tech/news-analysis/tesla-model-s-involved-in-fatal-crash-in-the
html

[396] ... LaTeX:
https://www.autoweek.com/news/green-cars/a36173804/both-local-police-and-nhtsa-probe-tesla

[397] ... LaTeX:
https://www.zdnet.com/article/apple-and-tesla-under-fire-over-software-engineers-fatal-au

[398] ... LaTeX:
https://www.google.com/search?q=tesla+crash+report&rlz=1C1AVUC_
enNL953NL953&ei=p3kNYa6sLI_UsAeSoZrwDw&start=100&sa=N&ved=2ahUKEwjum77s_
ZzyAhUPKuwKHZKQBv44WhDw0wN6BAgBEEg&biw=1920&bih=933

vlucht 1951

[399] ... LaTeX:
https://nl.wikipedia.org/wiki/Turkish_Airlines-vlucht_1951 technisch rapport

[400] ... LaTeX:
file:///C:/Users/gally/Downloads/rapport_ta_nl_aangepast.pdf beschrijving terugblik met overlevenden tijdlijn

[401] ... LaTeX:
https://www.noordhollandsdagblad.nl/cnt/dmf20190221_65390940 artikel terugblik met overlevenden advies raad voor de veiligheid de overlevende, de oorzaak, regeling, herdenking, smartengeld verhaal van een overlevende herdenking herdenking bemanning deed niets met foutmelding parlementaire besluitenlijst kamervragen over de onafhankelijkheid van de raad voor veiligheid verhaal van een overlevende beschrijvend artikel van letsel en gewonden

[402] ... LaTeX:
https://www.ntvg.nl/artikelen/vliegtuigongeval-schiphol-25-02-2009-letsels-en-verdeling-va
technische fout als oorzaak

[403] ... LaTeX:
https://nl.wikinews.org/wiki/Technische_fout_oorzaak_vliegtuigcrash_Turkish_
Airlines-vlucht_1951 gesprek met pieter van vollenhove voorzitter van de onderzoeksraad voor veiligheid onderzoeksraad voor veiligheid is onderdruk gezet

[404] ... LaTeX:
https://www.luchtvaartnieuws.nl/nieuws/categorie/72/algemeen/
conclusies-crash-tk1951-na-amerikaanse-druk-afgezwakt niuwesartikel feitenverloop

[405] ... LaTeX:
https://www.adformatie.nl/contentmarketing/communicatie-na-vliegramp-vertoonde-gebreken
zwarte doos

[406] ... LaTeX:
https://flightlevel.be/244/onderzoek-polderbaan-crash-turkish-airlines-1951/

[407] ... LaTeX:
http://wikimapia.org/11633002/nl/Crash-Turkish-Airlines-vlucht-1951

[408] ... LaTeX:
https://www.flightradar24.com/data/flights/tk1951

[409] ... LaTeX:
https://www.flightstats.com/v2/flight-tracker/TK/1951

de mali missie

[410] ... LaTeX:
https://joop.bnnvara.nl/nieuws/rapport-haalbaarheid-en-houdbaarheid-van-mali-missie-twijfe

[411] ... LaTeX:
https://www.consilium.europa.eu/nl/press/press-releases/2021/01/11/
eucap-sahel-mali-mission-extended-until-31-january-2023-and-mandate-adjusted/

[412] ... LaTeX:
https://nos.nl/artikel/650637-kamer-bezorgd-over-mali-missie

[413] ... LaTeX:
https://www.bnr.nl/nieuws/10015679/koenders-positief-tegenover-verlening-mali-missie

[414] ... LaTeX:
https://www.bnr.nl/nieuws/politiek/10345553/kabinet-wil-mali-missie-stoppen-verrassend-bes

[415] ... LaTeX:
https://www.ad.nl/nieuws/clash-om-mali-missie-dreigt-binnen-coalitie~a4151d4f/

[416] ... LaTeX:
https://www.nd.nl/cultuur/boeken/536861/boek-kijkje-bij-de-mali-missie

[417] ... LaTeX:
https://www.youtube.com/watch?v=jmZ6uSbpCvg

[418] ... LaTeX:
https://www.ewmagazine.nl/nederland/achtergrond/2016/07/
twee-nederlanse-militairen-dood-bij-oefening-mali-missie-325226/

[419] ... LaTeX:
https://www.nporadio1.nl/nieuws/cultuur-media/9e3b076e-5401-4630-bf39-f925213c5b6b/
onverwachte-openhartigheid-over-missie-in-mali

[420] ... LaTeX:
https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vjfm5p0nujzw?
ctx=vj2mc67lofnr

sollicitatie de bureaucratie aankomst interview van de burgerbevolking steun van de bevolking minuut 15:00 de organisatie minuut 23:00 De militaire briefing minuut 34:00 prioriteit minuut 39:00 briefing minuut 40:00 de communicatie met ministerie over inlichten minuut 44:00

[421] ... LaTeX:
https://www.2doc.nl/documentaires/series/2doc/2016/juli/de-missie.html

militair overleden door schietoefening in ossendrecht

[422] ... LaTeX:
https://amp.nos.nl/artikel/2094524-militair-omgekomen-bij-schietoefening-ossendrecht.
html

[423] ... LaTeX:
https://www.onderzoeksraad.nl/nl/page/4293/lessen-uit-schietongeval-ossendrecht

[424] ... LaTeX:
https://www.bndestem.nl/bergen-op-zoom/dood-van-militair-sander-klap-35-in-ossendrecht-wa

Wat is de rol van defensie? Wat is er gedaan om de veligheid van de medewerkers te waarborgen? Waarom zijn deze regels niet nageleefd? Wat zijn de gevolgen? Zijn de acties die naderhand zijn ondernomen wel redelijk naar de slachtoffers, het nationale veiligheisbeeld en de medewerkers?

schipholbrand

Wat is er gebeurd?

[425] ... LaTeX:
https://nl.wikipedia.org/wiki/Schipholbrand artikel

[426] ... LaTeX:
https://www.youtube.com/watch?v=1i-hfEzxFfk psychologische gevolgen rapport

[427] ... LaTeX:
https://www.onderzoeksraad.nl/nl/page/392/brand-cellencomplex-schiphol-oost-nacht-van-26-
artikel met video herdenking impact op de persoon herdenking

[428] ... LaTeX:
https://www.vpro.nl/argos/speel~POMS_VPRO_461907~schadevergoeding-voor-ex-verdachte-schiph
html chronologie

[429] ... LaTeX:
https://www.nu.nl/binnenland/3355935/feitenoverzicht-schipholbrand-en-rechtszaken.
html tijdlijn

[430] ... LaTeX:
https://www.singeluitgeverijen.nl/isbn/de-schipholbrand/ vervolgens van ministers beeldanalyse en reconstructie

[431] ... LaTeX:
https://eenvandaag.avrotros.nl/item/schipholbrand-niet-ontstaan-in-cel-11/
herdenking korte samenvatting rapport artikel verwijzing naar het rapport vanuit de politieke oppositie beeld vanuit de gevangenisbewaarder nationaliteit slachtoffers schipholbrand verblijfsvergunning voor de slachtoffers gen schadevergoeding voor de verdachte verdachte voor de rechter geen schadevergoeding voor verdachte artikel wat ging er mis bji de schipholbrand brand veroorzaakt door een peuk smaadschrift bewakers worden niet vervolgd proces schipholbrand moet over en de brandveilgheid moet worden verbeterd de rol van het parlement in de evaluatie

[432] ... LaTeX:
https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vi3aof7awcxg onderzoeksmemo herdenking

[433] ... LaTeX:
https://archief.ntr.nl/nova/page/detail/uitzendingen/3847/Den%20Haag%
20Vandaag_%20herdenking%20Schipholbrand.html herdenking invloed van de ramp op samenleving

[434] ... LaTeX:
https://www.npostart.nl/heropen-onderzoek-schipholbrand/13-11-2008/POMS_NTR_
103332 opmerkelijk rapport gestolen in de nasleep

[435] ... LaTeX:
https://www.nd.nl/nieuws/nederland/600395/schipholbrand-blijft-schrijnen

[436] ... LaTeX:
https://www.ed.nl/economie/om-geen-schadevergoeding-voor-verdachte-schipholbrand~a6c7c51d/
63042600/?referrer=https%3A%2F%2Fwww.google.com%2F

[437] ... LaTeX:
https://www.groene.nl/artikel/schipholbrand-vereist-debat

[438] ... LaTeX:
https://www.rizoomes.nl/brandweer/brand-cellencomplex-schiphol/

publicaties

[439] ... LaTeX:
http://www.msnp.nl/downloads/Onderzoeksmemo%20beeldanalyse%20Schipholbrand%
20prot.pdf

Wat waren de regels destijds? Waren de autoriteiten in staat om op tijd in te grijpen of om erger te voorkomen? Wat is er gedaan om de veiligheid van illegalen en gevangenissbewaarders te verbeteren

vuurwerkramp enschede

[440] ... LaTeX:
https://www.youtube.com/watch?v=OMkIsj8FsHw

[441] ... LaTeX:
https://depot03.archiefweb.eu/archives/archiefweb/20210703085353/http:
//www.vuurwerkramp.enschede.nl/publicaties/00005/#.YOAlp-gzaUk

Wat waren de afspraken omtrent vuurwerkopslag? Waarom werden de voorschriften neit nageleefd?

explosie in beirut

[442] ... LaTeX:
https://bmchealthservres.biomedcentral.com/articles/10.1186/
s12913-020-05906-y

[443] ... LaTeX:
https://news.sky.com/story/beirut-blast-cctv-captures-moment-huge-explosion-devastated-hos

[444] ... LaTeX:
https://www.unodc.org/unodc/en/frontpage/2020/September/
unodc-assists-lebanon-in-reestablishing-container-shipments-in-the-aftermath-of-the-port-
html

[445] ... LaTeX:
https://reliefweb.int/sites/reliefweb.int/files/resources/
LEB201-Lebanon-Emergency-Response.pdf

[446] ... LaTeX:
https://www.downtoearth.org.in/news/governance/beirut-blast-lessons-time-for-india-to-stre

[447] ... LaTeX:
https://www.justsecurity.org/72122/the-cost-of-resilience-the-roots-and-impacts-of-the-be

[448] ... LaTeX:
https://www.fire-magazine.com/the-port-of-beirut-explosion-a-timely-reminder

[449] ... LaTeX:
https://www.ctvnews.ca/sci-tech/mapping-the-beirut-explosion-what-the-impact-would-look-l
5053932

secyrity:

[450] ... LaTeX:
https://permanent.fdlp.gov/gpo45474/AN_advisory.pdf

secyrity:

[451] ... LaTeX:
https://permanent.fdlp.gov/gpo45474/AN_advisory.pdf

bijlmerramp

slmramp Wat is er gebeurd?

[452] ... LaTeX:
https://www.srnieuws.com/suriname/290721/slm-ramp-herdacht/

[453] ... LaTeX:
https://werkgroepcaraibischeletteren.nl/documentaire-waarom-nou-jij-over-de-slm-ramp-in-8

[454] ... LaTeX:
https://www.vpro.nl/speel~WO_NTR_15390142~andere-tijden-17-apr-2019-3-09-min-fouten-en-mi
html

[455] ... LaTeX:
https://www.canonvannederland.nl/nl/kalender/06/1989-06-07

[456] ... LaTeX:
https://vijfeeuwenmigratie.nl/archief-herdenkingen-slm-ramp

[457] ... LaTeX:
https://www.hulpverleningsforum.nl/index.php?topic=84702.0

[458] ... LaTeX:
https://www.nporadio1.nl/fragmenten/focus/f792e720-bd85-4c18-8a71-b334d9d5de7e/
2019-04-17-slm-ramp-een-paar-cowboys-hebben-achter-de-stuurknuppel-gezeten

[459] ... LaTeX:
https://www.waterkant.net/suriname/2017/06/07/herdenking-slm-ramp-28-jaar-geleden-surinam

[460] ... LaTeX:
https://www.espn.nl/video/clip?id=8744942

[461] ... LaTeX:
http://www.themediabrothers.nl/tag/slm-ramp/

[462] ... LaTeX:
https://www.rijnmond.nl/nieuws/182546/30-jaar-na-de-SLM-ramp-Ik-mis-mijn-broer-nog-elke-d

[463] ... LaTeX:
https://www.voetbalkrant.com/nieuws/2020-05-01/het-vergeten-verhaal-van-de-slm-ramp

[464] ... LaTeX:
https://www.bd.nl/sport/de-slm-ramp-en-het-hartverscheurende-verhaal-van-jerry-en-winnie-
?referrer=https%3A%2F%2Fwww.google.com%2F

[465] ... LaTeX:
https://www.amsterdam.nl/stadsarchief/nieuws/slm-ramp/

[466] ... LaTeX:
https://www.rtvoost.nl/nieuws/313496/Nabestaande-SLM-ramp-Heb-ik-wel-mijn-broer-en-moeder

[467] ... LaTeX:
https://www.bredavandaag.nl/nieuws/algemeen/337919/nac-herdenkt-andro-knel-slm-ramp-precie

[468] ... LaTeX:
https://www.anderetijden.nl/aflevering/792/Een-aangekondigde-vliegramp

[469] ... LaTeX:
https://nl.wikipedia.org/wiki/SLM-ramp database

[470] ... LaTeX:
https://aviation-safety.net/database/record.php?id=19890607-2 rapport

[471] ... LaTeX:
https://reports.aviation-safety.net/1989/19890607-2_DC86_N1809E.pdf

[472] ... LaTeX:
https://aviation-safety.net/investigation/cvr/transcripts/cvr_py764.php

[473] ... LaTeX:
https://en.wikipedia.org/wiki/Surinam_Airways_Flight_764

[474] ... LaTeX:
https://web.archive.org/web/20050113010822/https://www.ntsb.gov/ntsb/brief.asp?ev_id=34510&key=0

[475] ... LaTeX:
https://nos.nl/artikel/2287986-slm-vliegramp-van-precies-30-jaar-geleden-trof-ook-nederla

[476] ... LaTeX:
https://www.dagvantoen.nl/vliegtuigcrash-slm-bij-zanderij-meer-dan-170-doden/

[477] ... LaTeX:
https://www.waterkant.net/suriname/2006/06/07/vliegramp-suriname-op-7-juni-1989-2/
uitgebreid engels artikel

[478] ... LaTeX:
http://www.edufd.nl/planecrash/ ntsb investigtion

[479] ... LaTeX:
http://www.oldjets.net/slm-dc-8-crash.html uitgebreid engels artikel

[480] ... LaTeX:
https://admiralcloudberg.medium.com/contract-to-kill-the-crash-of-surinam-airways-flight-
persbericht

[481] ... LaTeX:
https://apnews.com/article/5b240d758ee4c5422381cc7cdc98566b Wat is de rol van de autoriteiten? Welke andere betrokkeen? Enw at is hun verantwoordelijkheid Hadden de negatieve gevolgen voorkomen kunnen worden? Hoe werd er over veiligheid gedacht?

Tsjernobyl

[482] ... LaTeX:
https://www.youtube.com/watch?v=Xw3SFOfbR84

[483] ... LaTeX:
https://nl.wikipedia.org/wiki/Kernramp_van_Tsjernobyl

[484] ... LaTeX:
https://www.rivm.nl/straling-en-radioactiviteit/stralingsincidenten-en-kernongevallen/tsjernobyl

[485] ... LaTeX:
https://www.anderetijden.nl/aflevering/599/Tsjernobyl-als-Nederlandse-ramp
wat er is gebeurd en hoe het leven verdergaat

[486] ... LaTeX:
https://www.nationalgeographic.nl/het-leven-in-tsjernobyl-gaat-door pernsioenfondsen en de tjernobyl ramp In 2021 worden mensen nog steeds blootgesteld blijkt ut een gezamelijk onderzoek van greenpeace en oekraiense wetenschappers stijging van de nucliaire activiteit gemeten in tjernobyl Het toerisme aspect De chronologie

[487] ... LaTeX:
https://historianet.nl/maatschappij/rampen/tsjernobyl-atoomhel-bij-reactor-4

[488] ... LaTeX:
https://nos.nl/artikel/2101523-de-spookstad-van-tsjernobyl-30-jaar-later Dieren in de omgeving van tjernobyl De chronologie Echtreme droogte zorgd voor gevaar

[489] ... LaTeX:
https://www.knmi.nl/over-het-knmi/nieuws/35-jaar-na-tsjernobyl-liggen-branden-op-de-loer

[490] ... LaTeX:
https://www.kivi.nl/afdelingen/risicobeheer-en-techniek/columns/
kernramp-tsjernobyl-het-dilemma-van-scherbitsky Joernalistiek, entertainment en de waarheid

[491] ... LaTeX:
https://www.vrt.be/vrtnws/nl/2020/04/06/in-de-ban-van-tsjernobyl-vooruitblik/
Een onderzoek

Huidige gevolgen van de explosie van toen

[492] ... LaTeX:
https://www.newscientist.nl/nieuws/steeds-meer-kernreacties-in-ontoegankelijke-ruimte-in-t
De ramp, hoe de mensen ermee omgingen en hoe er nu geleef wordt

evaluatieonderzoek en amatregeen

[493] ... LaTeX:
https://www.kernenergieinnederland.nl/node/308

[494] ... LaTeX:
https://www.google.com/maps/d/u/0/viewer?ie=UTF8&hl=nl&t=h&msa=0&ll=51.
388923%2C30.099792&spn=0.685583%2C1.645203&z=9&source=embed&mid=1MLcOcMK_
WrIJYMuTf0VVuYnMqQI Invloed van de mens op de omgeving

[495] ... LaTeX:
https://www.animalstoday.nl/mens-schadelijker-natuur-tsjernobyl/ Heroplevende splijtingsreacties docu van schooltv Radioactiviteit bereikt nederland documentaire en maatregelen

[496] ... LaTeX:
https://historiek.net/kernramp-van-tsjernobyl-1986/8769/ Het verhaal van een overledende Toerisme toerisme toerisme Dieren in de omgevong Toevluchtsoord voor vluchtelingen van de oorlog met russische seperatisten Ouderen die terugkeerden naar hun woonplaats na de gedwongen verhuizing door de autoriteiten De straling neemt weer toe Lessen geleerd van tjernobyl

[497] ... LaTeX:
https://www.nucleairforum.be/thema/veiligheid-als-prioriteit/
tsjernobyl-de-feiten Toerisme Bosbrand in tjernobyl invloed van de ramp op belgie

[498] ... LaTeX:
https://fanc.fgov.be/nl/noodsituaties/zware-ongevallen-het-buitenland/1986-kernongeval-tsjernobyl Boek recensie Fotos en berekeningen ontmanteling en toerisme Belangrijke lessen en overeenkomsten De journalistieke waarheid van de koude oorlog De lessen van

[499] ... LaTeX:
https://magazines.autoriteitnvs.nl/nieuwsbrief-anvs/2019/02/de-lessen-van-tsjernobyl Een toristenattractie maken van tjernobyl De radioactieve straling toen en nu de 30km zone door de ogen van toeristen artikel stedentrip rapport

[500] ... LaTeX:
https://wisenederland.nl/wp-content/uploads/2020/06/TSJERNOBYL.pdf slapend monster docu krantenartikel hbo serie docuserie de nieuwe sacrofaag hulp aan slachtoffers slapende reactor krantenartikel

[501] ... LaTeX:
https://onh.nl/verhaal/besmette-melk-en-radioactieve-spinazie-tsjernobyl-in-holland hbo serie internationale gevolgen toerisme nieuwe koepel media communicatie docu dieren

[502] ... LaTeX:
https://www.amboanthos.nl/boek/nacht-in-tsjernobyl/ koepel koepel

[503] ... LaTeX:
https://www.deingenieur.nl/artikel/nieuwe-antistralingskoepel-tsjernobyl-bijna-af toerisme toeristisch reiperspectief toerisme niwe koepel overschakelen naar duurzaamheid docu tjernobyl wekt nu duurazme energie toerisme overeenkomsten tjernobyl en fukushima drank en sla uit tjernobyl geen efficiente opslag is mogelijk

[504] ... LaTeX:
http://essay.utwente.nl/63353/1/Verschuur,_W._-_s0123617_(verslag).pdf

[505] ... LaTeX:
https://www.paperlessarchives.com/chernobyl_nuclear_accident_doc.html

[506] ... LaTeX:
https://www.pnnl.gov/main/publications/external/technical_reports/pnnl-13294.pdf

[507] ... LaTeX:
http://www.geocities.ws/scannapuerci/demauroinnovation.pdf

[508] ... LaTeX:
https://www-pub.iaea.org/MTCD/publications/PDF/Pub1312_web.pdf
MH17

[509] ... LaTeX:
https://na.eventscloud.com/file_uploads/aed4bc20e84d2839b83c18bcba7e2876_Owens1.pdf

[510] ... LaTeX:
https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01

[511] ... LaTeX:
https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/

[512] ... LaTeX:
https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack

[513] ... LaTeX:
https://www.researchgate.net/publication/333671061_Attacking_IEC-60870-5-104_SCADA_Systems

[514] ... LaTeX:
https://ris.utwente.nl/ws/files/6028066/3-s2_0-B9780128015957000227.pdf

[515] ... LaTeX:
https://www.diva-portal.org/smash/get/diva2:1046339/FULLTEXT01.pdf

[516] ... LaTeX:
https://www.semanticscholar.org/paper/Cybersecurity-analysis-of-a-SCADA-system-under-and-I
dfa7c12551ebe7b24da8d806e87e946051a57cb9

[517] ... LaTeX:
https://tutcris.tut.fi/portal/files/16294332/jafary_1534.pdf

[518] ... LaTeX:
http://blog.nettedautomation.com/2017/

[519] ... LaTeX:
https://www.us-cert.gov/ncas/alerts/TA17-163A

[520] ... LaTeX:
https://www.vice.com/en_us/article/zmeyg8/ukraine-power-grid-malware-crashoverride-industr

[521] ... LaTeX:
http://blog.wallix.com/ics-security-russian-hacking

[522] ... LaTeX:
https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0

[523] ... LaTeX:
https://www.varendoejesamen.nl/storage/app/media/downloads/vlot-en-veilig-door-brug-en-sluis-.pdf

[524] ... LaTeX:
http://www.scarphout.be/assets/bedieningstijden2014.pdf

[525] ... LaTeX:
https://www.theobakker.net/pdf/sluizen.pdf

[526] ... LaTeX:
http://www.watersportalmanak.nl/files/File/Brugbediengstijden_watersport.pdf

[527] ... LaTeX:
https://www.crow.nl/downloads/pdf/verkeer-en-vervoer/verkeersmanagement/verkeersregelinstallaties/stappenplan-machinerichtlijnen_web.aspx

[528] ... LaTeX:
https://puc.overheid.nl/rijkswaterstaat/doc/PUC_95170_31/

[529] ... LaTeX:
http://wsv.wsvdegors.nl/wp-content/uploads/2017/05/Bedieningstijden_201701.pdf

[530] ... LaTeX:
https://www.commissiemer.nl/projectdocumenten/00004717.pdf

[531] ... LaTeX:
https://tasmanroutes.nl/wp-content/uploads/docs/1900-bedieningstijden-groningen-drenthe.pdf

[532] ... LaTeX:
http://www.vliz.be/docs/groterede/GR21_Zeesluis.pdf

[533] ... LaTeX:
https://www.bhic.nl/media/document/file/rien-biemans-sluis-en-stuw-bij-lith.pdf

[534] ... LaTeX:
https://www.nattekunstwerkenvandetoekomst.nl/upload/documents/tinymce/KpNK-2017-SKW-01c001-v1-Zoutindringing-door-schutsluizen-overzicht-projecten-en-aanzet-fo
pdf

[535] ... LaTeX:
https://www.arnhemspeil.nl/nap/dok/2011-12-00-rijkswaterstaat-richtlijnen-vaarwegen.pdf

[536] ... LaTeX:
https://rijkewaddenzee.nl/wp-content/uploads/2016/08/Inventarisatie-toestand-vispasseerbaarheid-zoet-zout-overgangen-Waddenzee-2-6-2016-PRW-ra
pdf

[537] ... LaTeX:
http://www.nevepaling.nl/files/Image//nederlands/informatiecentrum/2014-definitieve-voorkeursvariantennotitie-visvriendelijk-sluisbeheer-afsluitdijk-en-houtr
/2014_definitieve_voorkeursvariantennotitie_visvriendelijk_sluisbeheer_afsluitdijk_en_houtribdijk.pdf

[538] ... LaTeX:
https://www.ifv.nl/kennisplein/Documents/20120614-BwNL-Handboek-brandbeveiligingsinstallat
pdf

[539] ... LaTeX:
https://ienc-kennisportaal.nl/wp-content/uploads/2017/01/Objectbeschrijving-Heumen.pdf

[540] ... LaTeX:
https://library.wur.nl/edepot/websites/stolwijkersluis/presentatie-data/data/pdf/TUDelft-bouwhistorisch-onderzoek.pdf

[541] ... LaTeX:
https://www.icentrale.nl/wp-content/uploads/bsk-pdf-manager/2019/01/20170929_Project-2.02-Deliverable-Gehele-werkpakket-2.02.pdf

[542] ... LaTeX:
https://www.stowa.nl/sites/default/files/assets/PUBLICATIES/Publicaties%202000-2010/Publicaties%202000-2004/STOWA%202004-XX%20boekenreeks%2020.pdf

[543] ... LaTeX:
https://www.nm-magazine.nl/pdf/NM_Magazine_2017-3.pdf

[544] ... LaTeX:
https://www.varendoejesamen.nl/storage/app/media/knooppunten/knooppuntenboekje_03_Friesland_Groningen_Drenthe.pdf

[545] ... LaTeX:
https://deafsluitdijk.nl/wp-content/uploads/2014/05/Plan-project-MER-Afsluitdijk.pdf

[546] ... LaTeX:
https://www.uni-saarland.de/fileadmin/user_upload/Professoren/FreyG/DS_KT_GF_INCOM_May_2012.pdf vanaf 2.1 tot en met 5

[547] ... LaTeX:
http://www.lasid.ufba.br/publicacoes/artigos/Integrating+UML+and+UPPAAL+for+Designing,+Specifying+and+Verifying+Component-Based+Real-Time+Systems.pdf

hf7 Reachability: i.e. some condition an posssibly be satisfied Safety: i.e. some condition will never occur Liveness: i.e. some condition wille eventually become true [] eventually or leadsto hf 8 Het systeem is deadlockvrij De wachttijd is altijd gelijk aan de invaarttijd $_2xdenivlleertijdendeinvaartijdvandeoverkant$

[548] ... LaTeX:
https://www.diva-portal.org/smash/get/diva2:495691/FULLTEXT01.pdf

blz 6 tot en met 10

[549] ... LaTeX:
https://www.cister-labs.pt/docs/formal_verification_of_aadl_models_using_uppaal/1331/view.pdf

hf 3 geeft een voorbeeld van een template met guard en acies De volgende automata worden gebruikt met hun lokale variabelen

De volgende globale variabelen

Een lijst met relevante einschappen van een schutsluis:

[550] ... LaTeX:
https://iopscience.iop.org/article/10.1088/1742-6596/1821/1/012031/pdf

hf 5 deadlock

[551] ... LaTeX:
http://www.es.mdh.se/pdf_publications/2934.pdf

hf 3 tool support Modelling in UML Code generation Domain Model Behaviour model State Hierarchy Transitions Trigger methods Time events Effects Requirements Environment model

hf 4

[552] ... LaTeX:
https://files.ifi.uzh.ch/stiller/CLOSER%202014/WEBIST/WEBIST/Internet%20Technology/Full%20Papers/WEBIST_2014_130_CR.pdf

[553] ... LaTeX:
https://files.ifi.uzh.ch/stiller/CLOSER%202014/WEBIST/WEBIST/Internet%20Technology/Full%20Papers/WEBIST_2014_130_CR.pdf

Bijlage A performance

[554] ... LaTeX:
https://home.hvl.no/ansatte/aaks/articles/2015IKT617.pdf

test specification

[555] ... LaTeX:
https://d-nb.info/987511998/34

sheet 24 tot 65

[556] ... LaTeX:
http://ppedreiras.av.it.pt/resources/empse0809/slides/TheUppaalModelChecker-Julian.pdf

2.3.4.2 4.7

coffie apparaat

[557] ... LaTeX:
https://www.comp.nus.edu.sg/~cs5270/Notes/chapt6a.pdf

what is a good software specification

[558] ... LaTeX:
http://www.cs.ru.nl/~fvaan/PV/what_is_a_good_model.html#:~:text=A%20good%20model%20has%20a%20clearly%20specified%20purpose%20and%20(ideally,code%20generation%2C%20and%20test%20generation.

[559] ... LaTeX:
https://onix-systems.com/blog/7-basic-software-development-models-which-one-to-choose

[560] ... LaTeX:
https://www.educative.io/blog/software-process-model-types

[561] ... LaTeX:
https://medium.com/globalluxsoft/5-popular-software-development-models-with-their-pros-and-cor

[562] ... LaTeX:
https://www.jamasoftware.com/blog/characteristics-of-excellent-requirements/

[563] ... LaTeX:
https://www.gaudisite.nl/ValidationOfRequirementsSlides.pdf

[564] ... LaTeX:
https://www.informit.com/articles/article.aspx?p=1152528&seqNum=4

[565] ... LaTeX:
https://www.altexsoft.com/blog/software-requirements-specification/

[566] ... LaTeX:
E:MijnDocumentenvakkenadvncedalgorithms_advanced_algorithsresearch sheet 28 transitorische relaties vertalen van ctl naar ltl

Urgent locations Is hetzelfde als het toevoegen van een clock x, met een invariant x<=o op de locatie. Zolang een systeem in een urgente locatie zit mag er geen tijd verstrijken Bjivoorbeeld als een sluis klaar is engeen schpeen in de sluis. Dan moet er een urgentie zijn dat alle schepen waar mogelijk worden opgesteld voor invaren. Als er geen schepen in de wachtrij en er staan geenschepen klaar om in te varen dn is er misschien urgentie om aan de andere kant schepen op te halen. Commited locations Als een of meerdere locaties ingesteld zijn als committed. Een committed state kan niet vertragen en de volgende transitie moet een transitie zijn waarin de uitgaande edge komt van een committed edge

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

[567] ... LaTeX:
https://repository.tno.nl/islandora/object/uuid%3Acdef48df-da49-46b6-8678-5c62a88a0090

[568] ... LaTeX:
https://wayback.archive-it.org/9650/20200409062940/http:/p3-raw.greenpeace.org/international/Global/international/publications/nuclear/2016/Nuclear_Scars.pdf

[569] ... LaTeX:
https://bdtechtalks.com/2020/07/29/self-driving-tesla-car-deep-learning/

critical safety systems chemicals

[570] ... LaTeX:
https://esc.uk.net/safety-critical-systems

[571] ... LaTeX:
https://www.oecd.org/chemicalsafety/chemical-accidents/41269710.pdf

[572] ... LaTeX:
https://safety-work.org/fileadmin/safety-work/articles/Verwechslung_von_Chemikalien/Stoffverwechslung_e.pdf

[573] ... LaTeX:
https://ifs.host.cs.st-andrews.ac.uk/Books/SE9/Web/Dependability/CritSys.html

[574] ... LaTeX:
https://www.acs.org/content/dam/acsorg/about/governance/committees/chemicalsafety/publications/identifying-and-evaluating-hazards-in-research-laboratories.pdf

[575] ... LaTeX:
https://www.computer.org/csdl/magazine/so/2017/04/mso2017040049/13rRUxCitHw

[576] ... LaTeX:
https://msquair.files.wordpress.com/2012/06/assca-guiding-philosophic-principles-on-the-design
pdf

[577] ... LaTeX:
https://epsc.be/Documents/PS+Fundamentals/_/EPSC_Process%20Safety%20Fundamentals%20-%20Booklet_March2021.pdf

[578] ... LaTeX:
https://www.icheme.org/media/8976/xxiv-poster-11.pdf

[579] ... LaTeX:
https://crpit.scem.westernsydney.edu.au/confpapers/CRPITV55Chambers.pdf

[580] ... LaTeX:
https://users.ece.cmu.edu/~koopman/des_s99/safety_critical/

critical safety systems airplanes

[581] ... LaTeX:
file:///C:/Users/gally/Downloads/AGARDAG300.pdf

[582] ... LaTeX:
https://arxiv.org/abs/1502.02605

[583] ... LaTeX:
https://users.encs.concordia.ca/~ymzhang/courses/reliability/ICSE02Knight.pdf

[584] ... LaTeX:
https://www.jstor.org/stable/44682826

[585] ... LaTeX:
http://www.dcs.gla.ac.uk/~johnson/teaching/safety/slides/pt2.pdf

[586] ... LaTeX:
https://sites.google.com/site/cis115textbook/safety-critical-systems

[587] ... LaTeX:
https://www.dau.edu/tools/se-brainbook/Pages/Design%20Considerations/
Critical-Safety-Item.aspx

[588] ... LaTeX:
https://mcdpinc.com/safety-critical-systems

[589] ... LaTeX:
https://faculty.up.edu/lulay/MEStudentPage/failsafe.pdf

[590] ... LaTeX:
https://www.enidine.com/CorporateSite/media/itt/Resources/Distributors/
EndUserDocuments/Suppliers_Documents/QAM03_Rev_E.pdf

[591] ... LaTeX:
https://daytonaero.com/wp-content/uploads/AC-17-01.pdf

[592] ... LaTeX:
https://rmas.fad.harvard.edu/pages/chartered-private-aircraft-0

[593] ... LaTeX:
https://pubmed.ncbi.nlm.nih.gov/7966484/

[594] ... LaTeX:
https://nebula.esa.int/content/assessment-methodology-certification-safety-gnc-critical-space-

[595] ... LaTeX:
https://www.aopa.org/training-and-safety/online-learning/safety-spotlights/
aircraft-systems

[596] ... LaTeX:
https://www.cs.unc.edu/~anderson/teach/comp790/papers/safety_critical_arch.pdf

[597] ... LaTeX:
https://queue.acm.org/detail.cfm?id=2024356

[598] ... LaTeX:
https://www.law.cornell.edu/cfr/text/14/1.1

[599] ... LaTeX:
http://libraryonline.erau.edu/online-full-text/ntsb/safety-reports/SR06-02.pdf

[600] ... LaTeX:
https://www.cs.uct.ac.za/mit_notes/human_computer_interaction/htmls/ch02s10.html

[601] ... LaTeX:
https://flightsafety.org/

[602] ... LaTeX:
https://engineering.stanford.edu/magazine/article/mykel-kochenderfer-ai-and-safety-critical-sy

[603] ... LaTeX:
https://www.faasafety.gov/files/gslac/courses/content/258/1097/AMT_Handbook_
Addendum_Human_Factors.pdf

[604] ... LaTeX:
https://www.eurocontrol.int/sites/default/files/2019-06/src-doc-1-e1.0.pdf

[605] ... LaTeX:
http://aerossurance.com/safety-management/critical-maintenance-tasks/

[606] ... LaTeX:
https://www.gao.gov/assets/gao-21-86.pdf

[607] ... LaTeX:
https://criticalsoftware.com/en/news/coding-the-skies

[608] ... LaTeX:
https://aviation.stackexchange.com/questions/46677/what-are-the-design-parameters-for-airliner

[609] ... LaTeX:
https://www.cantwell.senate.gov/news/press-releases/cantwells-comprehensive-bipartisan-bicamer

[610] ... LaTeX:
https://www.forbes.com/advisor/travel-rewards/737-max-what-is-safety-anyway/

[611] ... LaTeX:
https://www.tandfonline.com/doi/full/10.1080/00140130903521587

[612] ... LaTeX:
https://www.doi.gov/aviation/safety

[613] ... LaTeX:
https://dspace.mit.edu/bitstream/handle/1721.1/118438/ICAT_2018_07_Christoper%
20Courtin_Report.pdf?sequence=1&isAllowed=y

[614] ... LaTeX:
https://www.defence.gov.au/dasp/Docs/Manuals/7001053/eTAMMweb/1049.htm

[615] ... LaTeX:
https://www.aviationpros.com/aircraft/commercial-airline/article/10239806/
staying-legal-another-failed-faa-safety-program

[616] ... LaTeX:
https://www.iata.org/en/services/consulting/safety-operations/

[617] ... LaTeX:
https://hbr.org/2017/09/the-tragic-crash-of-flight-af447-shows-the-unlikely-but-catastrophic-

[618] ... LaTeX:
https://www.infosys.com/industries/communication-services/documents/
landing-gear-design-and-development.pdf

[619] ... LaTeX:
https://www.acqnotes.com/Attachments/AF_System-Safety-HNDBK.pdf

[620] ... LaTeX:
https://www.transportation.gov/testimony/state-airline-safety-federal-oversight-commercial-avi

[621] ... LaTeX:
https://www.federalregister.gov/documents/2019/02/13/2019-00758/
safe-and-secure-operations-of-small-unmanned-aircraft-systems

[622] ... LaTeX:
https://archive.etsc.eu/documents/safety%20in%20airports.pdf

[623] ... LaTeX:
https://journals.sagepub.com/doi/pdf/10.1177/002029400403700202

[624] ... LaTeX:
https://www.unmannedsystems.ca/wp-content/uploads/2019/01/
DRAFT-AC-922-001-RPAS-SAFETY-ASSURANCE.pdf

[625] ... LaTeX:
https://www.ccsdualsnap.com/pressure-switches-in-aerospace-applications/

[626] ... LaTeX:
https://www.egbc.ca/getmedia/78073fda-5a83-4f0f-b12f-0a40dcbbc29d/
EGBC-Safety-Critical-Software-V1-0.pdf.aspx

[627] ... LaTeX:
https://readwrite.com/2018/12/21/air-travel-is-far-safer-than-you-think-heres-why/

[628] ... LaTeX:
https://fas.org/sgp/crs/misc/R45939.pdf

[629] ... LaTeX:
https://cdn.ymaws.com/www.astna.org/resource/collection/
4392B20B-D0DB-4E76-959C-6989214920E9/ASTNA_Safety_Position_Paper_2018_FINAL.pdf

[630] ... LaTeX:
https://transportation.house.gov/imo/media/doc/2020.09.15%20FINAL%20737%20MAX%
20Report%20for%20Public%20Release.pdf

[631] ... LaTeX:
https://www.transportstyrelsen.se/globalassets/global/luftfart/seminarier_
och_information/seminarier-2016/luftvardighet-camo-och-145-verkstader/
11b-critical-task-fpl.pdf

[632] ... LaTeX:
https://www.h-a-c.ca/IHSS_Helicopter_Safety_History_05.pdf

[633] ... LaTeX:
https://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewHTML.asp?FileID=7144&lang=EN

[634] ... LaTeX:
https://www.skybrary.aero/index.php/Cockpit_Automation_-_Advantages_and_Safety_
Challenges

[635] ... LaTeX:
https://ntrs.nasa.gov/citations/20120014507

[636] ... LaTeX:
https://www.sciencedirect.com/science/article/abs/pii/S092575351730601X

[637] ... LaTeX:
https://www.semanticscholar.org/paper/Safety-critical-avionics-for-the-777-primary-flight-Yeh/
8facf90f4a9051c3ab8ce11e39d0893118268d90

[638] ... LaTeX:
https://www.easa.europa.eu/faq/19013

[639] ... LaTeX:
https://ntrs.nasa.gov/api/citations/20120014507/downloads/20120014507.pdf

[640] ... LaTeX:
https://www.hsdl.org/c/firework-safety/

[641] ... LaTeX:
https://www.cpsc.gov/Safety-Education/Safety-Education-Centers/Fireworks

[642] ... LaTeX:
https://www.seattletimes.com/subscribe/signup-offers/?pw=redirect&
subsource=paywall&return=https://www.seattletimes.com/opinion/editorials/
firework-safety-even-more-critical-after-heat-wave/

[643] ... LaTeX:
https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/mineralsmetals/pdf/mms-smm/
expl-expl/20170828-G05-09E_ACC.pdf

[644] ... LaTeX:
https://www.prnewswire.com/news-releases/fireworks-related-injuries-and-deaths-spiked-during-t
html

[645] ... LaTeX:
https://www.osha.gov/sites/default/files/publications/OSHA3912.pdf

[646] ... LaTeX:
https://www.firelinx.com/wp-content/uploads/2021/02/FLX-Issues-in-Firing-System-Safety.
pdf

[647] ... LaTeX:
http://www.eig2.org.uk/wp-content/uploads/WTOFD-Blue-Guide.pdf

[648] ... LaTeX:
https://www.hse.gov.uk/explosives/er2014-fireworks-retail-prem.pdf

[649] ... LaTeX:
https://www.firerescue1.com/firefighter-safety/articles/
11-fireworks-safety-videos-from-the-serious-to-the-humorous-fHy0M4pT2gjcQ8jA/

[650] ... LaTeX:
https://www.aidic.it/cet/16/53/044.pdf

[651] ... LaTeX:
http://www.alarmascasas.com.mx/sites/default/files/85006-0061%20--%20FireWorks%
20Brochure.pdf

[652] ... LaTeX:
https://www.ehs.ufl.edu/programs/fire/fireworks/

[653] ... LaTeX:
https://www.interlogix.com.au/documents/FireWorks%20Features%20and%20Operation%
20(fire%20only).pdf

[654] ... LaTeX:
https://townhall.virginia.gov/l/GetFile.cfm?File=C:%5CTownHall%5Cdocroot%
5CGuidanceDocs%5C960%5CGDoc_DFP_4448_v1.pdf

[655] ... LaTeX:
https://ec.europa.eu/growth/sectors/chemicals/specific-chemicals_en

[656] ... LaTeX:
http://www.iiakm.org/ojakm/articles/2015/volume3_3/OJAKM_Volume3_3pp27-36.pdf

[657] ... LaTeX:
https://www.bristol.gov.uk/documents/20182/1175006/Fireworks+in+retail+premises/
6aa6ee24-5b74-43b4-a1d9-747689b1dbc9

[658] ... LaTeX:
https://www.eversys.com.br/imagens/uploads/arqs/bra_arquivos/
04-software-gerenciador-fireworks-brochura.pdf

[659] ... LaTeX:
http://www.doiserbia.nb.rs/img/doi/0354-9836/2016/0354-98361500050G.pdf

[660] ... LaTeX:
http://s3.eurecom.fr/docs/wisec14_Costin.pdf

[661] ... LaTeX:
https://www.firetechsystems.com/assets/uploads/2018/09/FireWorks-Brochure.pdf

[662] ... LaTeX:
https://blog.ritzsafety.com/fireworks-safety-tips

[663] ... LaTeX:
https://www.engineerlive.com/content/fire-detection-and-protection-through-safety-critical-sys
algemene vragen
algemene vragen oorzaken

[664] ... LaTeX:
https://www.seattletimes.com/business/boeing-aerospace/what-led-to-boeings-737-max-crisis-a-qa

[665] ... LaTeX:
https://www.schneier.com/blog/archives/2019/04/excellent_analy.html
fout in de software

[666] ... LaTeX:
https://www.forbes.com/sites/georgeavetisov/2019/03/19/malware-at-30000-feet-what-the-737-max-
?sh=4d26f7052a9e
het nationaal veiligheidsbelang

[667] ... LaTeX:
https://www.forbes.com/sites/lorenthompson/2020/11/23/five-reasons-return-of-boeings-737-max-t
?sh=2128ea552018
falend toezicht

[668] ... LaTeX:
https://www.seattletimes.com/business/boeing-aerospace/failed-certification-faa-missed-safety-
onderzoeksrapport

[669] ... LaTeX:
https://www.faa.gov/foia/electronic_reading_room/boeing_reading_room/media/737_
RTS_Summary.pdf

[670] ... LaTeX:
https://en.wikipedia.org/wiki/Boeing_737_MAX_groundings
veiligheidsrisico's menselijke fouten

[671] ... LaTeX:
https://www.theverge.com/2019/5/2/18518176/boeing-737-max-crash-problems-human-error-mcas-faa
overzicht van crashes

[672] ... LaTeX:
https://www.theverge.com/2019/3/22/18275736/boeing-737-max-plane-crashes-grounded-problems-inf
veiligheidsopmerking

[673] ... LaTeX:
https://www.airlineratings.com/news/boeings-737-max-will-one-safest-aircraft-history/
aanpassingen

[674] ... LaTeX:
https://www.boeing.com/commercial/737max/737-max-software-updates.page
waarschuwingen//output signalen

[675] ... LaTeX:
https://leehamnews.com/2020/11/24/boeing-737-max-changes-beyond-mcas/
software gerelateerde fouten

[676] ... LaTeX:
https://spectrum.ieee.org/aerospace/aviation/how-the-boeing-737-max-disaster-looks-to-a-softwa
onderzoeksrapport de rol van de publieke opinie

[677] ... LaTeX:
https://pubsonline.informs.org/do/10.1287/orms.2019.05.05/full/
onderzoek van europese luchtvaart agentschap

[678] ... LaTeX:
https://www.easa.europa.eu/newsroom-and-events/news/easa-declares-boeing-737-max-safe-return-s

[679] ... LaTeX:
https://phys.org/news/2019-03-boeing-max-safety-tragedies.html
artikel over sensoren

[680] ... LaTeX:
https://www.flightglobal.com/airframers/boeing-delays-737-max-10-deliveries-two-years-to-2023/
142245.article
goedkeuring van europese luchtvaart autoriteiten advies aan de faa

[681] ... LaTeX:
https://www.hstoday.us/subject-matter-areas/airport-aviation-security/
oig-tells-faa-to-improve-safety-oversight-following-boeing-737-max-review/

[682] ... LaTeX:
https://www.geekwire.com/2020/faas-go-ahead-737-maxs-return-flight-kicks-off-massive-software-

[683] ... LaTeX:
https://www.researchgate.net/publication/338420944_A_Promise_Theoretic_Account_
of_the_Boeing_737_Max_MCAS_Algorithm_Affair
achtergrond informatie

[684] ... LaTeX:
http://www.b737.org.uk/mcas.htm
algemeen vertrouwen

[685] ... LaTeX:
https://www.cnbc.com/2019/05/16/what-you-need-to-know-about-boeings-737-max-crisis.
html
toestemming europese autoriteiten problemen

[686] ... LaTeX:
https://arstechnica.com/information-technology/2020/01/737-max-fix-slips-to-summer-and-thats-
uitgebreid artikel over de onderzoeken en het vliegverbod

[687] ... LaTeX:
https://www.cnet.com/news/boeing-737-max-8-all-about-the-aircraft-flight-ban-and-investigatio
computers als oorzaak lessons learned

[688] ... LaTeX:
https://www.designnews.com/electronics-test/5-lessons-learn-boeing-737-max-fiasco

[689] ... LaTeX:
https://www.eurocontrol.int/publication/effects-network-extra-standby-aircraft-and-boeing-737-
single point of failure

[690] ... LaTeX:
https://dmd.solutions/blog/2019/04/05/how-a-single-point-of-failure-spof-in-the-mcas-software-

[691] ... LaTeX:
https://asiatimes.com/2021/01/boeings-737-max-and-the-fear-of-flying/
lijst van tehnische aanpassingen

[692] ... LaTeX:
https://www.caa.co.uk/Consumers/Guide-to-aviation/Boeing-737-MAX/

[693] ... LaTeX:
https://dsm.forecastinternational.com/wordpress/2020/12/14/
airbus-and-boeing-report-november-2020-commercial-aircraft-orders-and-deliveries/
code lek

[694] ... LaTeX:
https://www.wired.com/story/boeing-787-code-leak-security-flaws/

[695] ... LaTeX:
https://www.fitchratings.com/research/corporate-finance/
boeing-737-max-return-backlog-risks-remain-16-09-2020
Cultuurverandering, deregulatie, systeemwijziging of gewoon een kwestie van competentie

[696] ... LaTeX:
https://www.aerospacetestinginternational.com/features/what-broke-the-737-max.
html
extra aanpassingen

[697] ... LaTeX:
https://theaircurrent.com/aviation-safety/boeings-737-max-software-done-but-regulators-plot-mo
wat ging er mis een analyse van een ex-iloot De utoriteiten waren op de hoogte

[698] ... LaTeX:
https://www.extremetech.com/extreme/303373-the-faa-knew-the-737-max-was-dangerous-and-kept-it-
kwaliteiten van het alarmsysteem niet goed bekend

[699] ... LaTeX:
https://time.com/5687473/boeing-737-alarm-system/

[700] ... LaTeX:
https://www.nasdaq.com/articles/boeing-gets-dealt-another-737-max-cancellation-blow.
-what-it-means-for-boeing-stock-2020

[701] ... LaTeX:
https://www.eetimes.com/boeing-crashes-highlight-a-worsening-reliability-crisis/
veiligheidsvraagstuk

[702] ... LaTeX:
https://www.latimes.com/business/story/2019-12-11/faa-boeing-737-max-crashes

probleemanalyse, veiligheidsvraagstuk

[703] ... LaTeX:
https://www.politico.com/story/2019/03/15/boeing-737-max-grounding-1223072

falend toezicht

[704] ... LaTeX:
https://www.pogo.org/analysis/2019/10/corrupted-oversight-the-faa-boeing-and-the-737-max/

[705] ... LaTeX:
https://www.afacwa.org/the_inside_story_of_mcas_seattle_times

doelstellingen en veiligheidsvraagstukken

[706] ... LaTeX:
https://www.marxist.com/737-max-scandal-boeing-putting-profits-before-safety.htm

[707] ... LaTeX:
https://finance.yahoo.com/news/australia-lifts-ban-boeing-737-035817682.
html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_
referrer_sig=AQAAAHZCJYy_0A5VS2WiPoCvH4xdrRNkmkdsv5EWJ2RLIz_AS-rxsTty6AF1_
HlmJiRyWYqCXDi4p0Xs4isYkNkCq2Pfo-pQ60Xz_IfTNjm4FgoZiBMC4zpZlB6F0fwecrjE_
ujAXZzG4xPJnWCd8-G3VLlPTY8h3H31eQ1i8hY9AIyy

autoriteiten krijgen tik op de vingers

[708] ... LaTeX:
https://medium.com/@jpaulreed/the-737max-and-why-software-engineers-should-pay-attention-a041

[709] ... LaTeX:
https://news.ycombinator.com/item?id=19414775

[710] ... LaTeX:
https://www.bbc.com/news/55366320

[711] ... LaTeX:
https://www.marketscreener.com/news/latest/China-studies-Boeing-737-MAX-recertification-wants-

motor in brand

[712] ... LaTeX:
https://www.euractiv.com/section/aviation/news/boeing-grounds-777s-after-engine-fire/

[713] ... LaTeX:
https://gulfnews.com/business/aviation/uae-airspace-to-see-return-of-boeing-737-max-1.
1613627548923

motor in brand gevlogen

[714] ... LaTeX:
https://techxplore.com/news/2021-02-boeing-urges-grounding-777s.html

[715] ... LaTeX:
https://www.politico.eu/article/uk-temporarily-bans-some-boeing-aircraft-after-pratt-whitney-e

[716] ... LaTeX:
https://www.timeslive.co.za/news/world/2021-02-23-damage-to-united-boeing-777-engine-consister
[716] faa was niet kritisch genoeg

Evaluatie

In de evaluatie reflecteer je over je eigen afstudeerproces. Daarbij moet je vooral letten op de leereffecten. Welke competenties had je nodig? Welke competenties kwam je tekort en moest je zelf verwerven? Waren dit algemene of specifieke competenties? Voldeden de beroepscompetenties aan de standaard van het *HBO-I* (analyseren, adviseren, ontwerpen, realiseren en beheren)? Vielen de algemene competenties in de vijf categorieën van de *Dublin Descriptoren*[1] zoals het verkrijgen van kennis en inzicht, het toepassen van kennis en inzicht, het maken van onderbouwde keuzen (oordeelsvorming), het communiceren (schriftelijk en mondeling) en het verkrijgen van leervaardigheden?

[1] Dublin Descriptoren zijn eisen aan de competenties voor de bachelor en master studies aan universiteiten en hogescholen in Europa.

Requirement tracability matrix

Tabel 3: Caption

Requirements	**Accuracy**	**Coverage**	**Scalability**	**Infrastructure**
Inertial Navigation	✓	✓	✓	
RFID	✓	✓	✓	
Bluetooth		✓		✓
WLAN	✓	✓		✓
Infrared	✓	✓		✓

swot analyse

	Helpful	Harmful
Internal origin	Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.	Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.
Internal origin	Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.	Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

	Helpful	Harmful
Internal origin	Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.	Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

	Helpful	Harmful
Internal origin	Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.	Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

.1 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.

[63],[64],[42],[58],[59],[60],[61],[515],[62].

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. [63]

Uit onderzoek[64] 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.

.1.1 Literaire analyse

Motief

Oekraine wijst naar de russen [64], [**?**],[42],[56],[55],[54],[53].

Situatie Oekraiene

[52],[51].

Situatie algemeen

[511],[59],[49].

Factoren

[48]

Oorzaak

[27],[47],[46],[51].

Gebruikte materialen

[44], [43]

Uitvoering van de aanval

[63],[42].

Oplossingen

[63]

Aanbevelingen

.1.2 Resultaten

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.

[63]

[42]

spearfishing

blackenergy

remote access capabilities

serial-to-ethernet communication devices

telephony denial of service attacks

.1.3 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. [63]

.1.4 Discussie

.1.5 Verder lezen

[**?**],[513],[39],[38],[37],[36],[35],[34],[33],[33],[32],[31],[30],[29],[28],[26],[25],[24].

	Helpful	Harmful
Internal origin	Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.	Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

	Helpful	Harmful
Internal origin	Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.	Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Werken met LaTeX

Het is niet verplicht om met LaTeX te werken. Men mag ook gebruik maken van andere tekstverwerkers zoals *MS-Word*, Wel is het verplicht het afstudeerverslag LaTeX-geformateerd in te leveren en van de LaTeX-template `modelverslag.sty` gebruik te maken.

De LaTeX-template bevat enkele macro's voor het opstellen van een hoofdstuk (`\hoofdstuk`), een paragraaf (`\paragraaf`), een afbeelding (`\figuur`). De overige LaTeX macro's en omgevingen blijven bruikbaar. Bijvoorbeeld de `tabular`-omgeving om tabellen te maken:

```
\begin{tabular}{formaat}
        ...
\end{tabular}
```

Afmetingen (1 pt = 0,351 mm)	
paper width	597.50787pt
text width	455.24411pt
column width	455.24411pt
column seperate	10.0pt
oddside margin	-1.1381pt
evenside margin	-1.1381pt
paper height	845.04684pt
text height	729.6886pt
top margin	-15.36449pt

Een nadeel van tabellen dat ze vaak te groot zijn voor de twocolumn-mode. Het zou mooi zijn als ze ingedrukt kunnen worden. Bovendien is deze tabel niet-zwevend, hij wordt geplaatst tussen de tekstdelen waar hij is ingevoerd. Dit kan bezwaarlijk zijn bij pagina-overgangen. In dat geval kan je beter gebruikmaken van zwevende tabellen (en figuren) die door LaTeX zelf op een geschikte plaats worden gezet. Wel moet aan een zwevende tabel een label en een onderschrift gekoppeld worden om er naar te kunnen verwijzen. Voor een zwevende horizontale tabel met label en onderschrift wordt in de 'template' de `tabel`-omgeving aangeboden:

```
\begin{tabel}[afm]{formaat}{label}{onderschrift}
...
\end{tabel}
```

De `tabel`-omgeving plaatst 'zwevende' tabellen in verslag- en publicatie-mode. Het eerste argument is een optioneel `[afm]` argument met de defaultwaarde `\normalsize` voor de afmeting van de karakters. De mogelijke waarden voor de afmeting zijn – van groot tot klein – de volgende macro's: (`\huge`, `\LARGE`, `\Large`, `\large`, `\small`, `\footnotesize`, `\scriptsize` en `\tiny`).

Bovendien zijn de standaard `tabular` kolomformaten `r,l,c,|,||,p{lengte}` uit de tabelomgeving uitgebreid met kolomformaten `\R, \C, \L` voor variabele celinhoud zoals het plaatsen van meerdere regels per cel.

Een verticale tabel is mogelijk met de omgeving (`TABEL`) met dezelfde kolomformaten mogelijkheden. In LaTeX zijn de tabellen, vooral in de `twocolumn`-mode erg lastig. Bijvoorbeeld in de tabellen 2 en 3 zijn twee verschillende uitwerkingen van de tabelomgevingen:

Plaats afbeeldingen alleen in het hoofdverslag als ze de tekst ondersteunen en de leesbaarheid niet verlagen. In de tekst kan naar afbeeldingen worden verwezen met de macro `\ref{fig:label}`.

In LaTeX[1] geschreven verslagen zijn op diverse manieren afbeeldingen[2] te plaatsen. Een van die manieren is gebruik te maken van de macro `\figuur` in de `modelverslag`-package'.

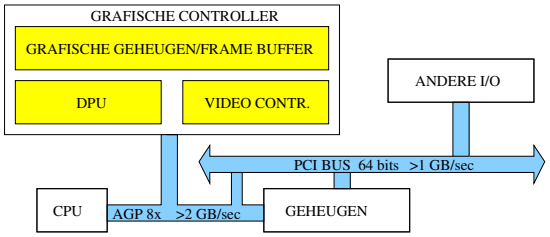
7C0	hexadecimal
3700	octal
11111000000	binary
1984	decimal

Tabel 4: Vaste cellen, variabele breedte

OpenGL core library	OpenGL32 voor MS-Windows en GL voor de meeste X-Window systemen
OpenGL Utility Library	GLU
Koppeling met het platform	GLX voor X-Window en WGL voor MS-Windows
OpenGL Library Utility Toolkit	GLUT, bibliotheek voor het openen van windows, invoer van muis en toetsenbord, menus, event-driven in- en uitvoer

Tabel 5: Variabele cellen, variabele breedte

'Vector graphics' figuren van het 'pdf-', 'eps-' en 'svg-' formaat[2] met een ingewikkelde 'bounding box' zijn moeilijk op de juiste schaal te brengen. Vaak moet dat met uitproberen bepaald worden. Het plaatsen van figuren met absolute afmetingen of een vaste 'scale' factor, kan leiden tot minder soepele oplossingen zoals figuur 1. Deze figuur heeft naast een rotatie (`angle=270`) een vaste scale-factor (`scale=0.45`) die alleen geschikt is voor de 'twocolumn-mode'.

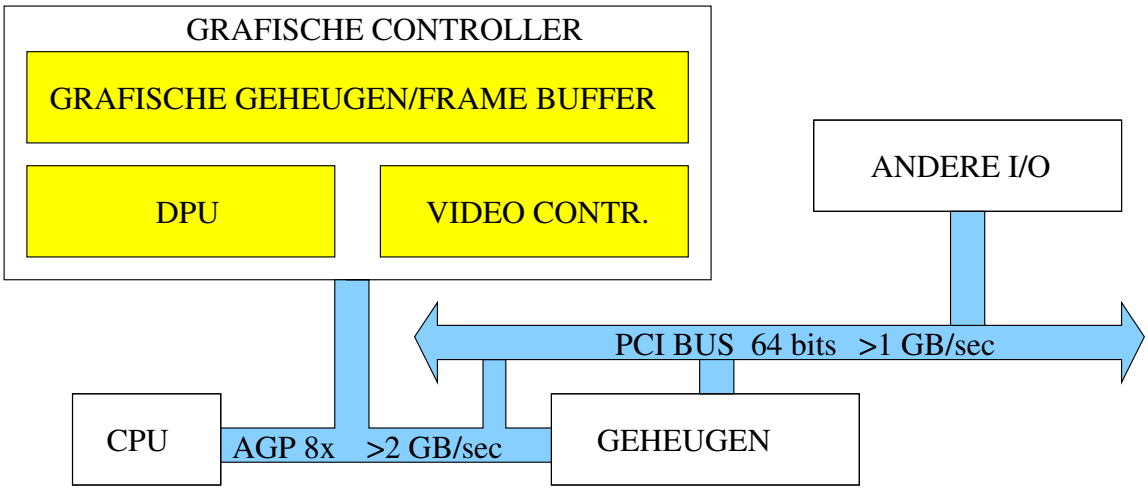


Figuur 1: Vaste breedte (pdf)

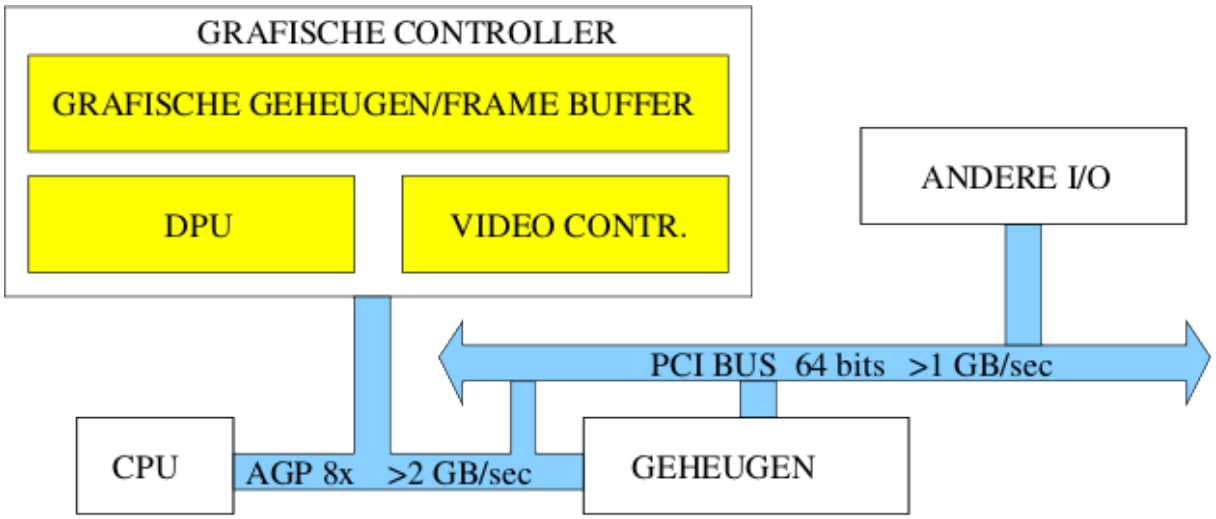
In plaats van `scale=x` kan je beter de relatieve afmeting `width=\Procent{y}` gebruiken. De waarde *y* wordt in de verslag-mode met uitproberen gevonden, zie figuur 2.

Het afmetingsprobleem is iets gemakkelijker op te lossen met 'bitmap graphics' van het 'jpg-', 'gif-' en 'png-' formaat omdat de figuren al van te voren geschaald kunnen worden als de 'bounding box' bij het inlezen bekend is. De breedte (`width`) kan als percentage van de kolombreedte (`width=\Procent{0 ... 99}`) worden opgegeven zoals dat bij figuur 3 gedaan is. Voor een 100% waarde neemt men `width=\columnwidth` De afmeting wordt automatisch aangepast aan de nieuwe kolombreedte.

[2]Een pdf-bestand kan zowel vector-graphics als bitmap-graphics bevatten.

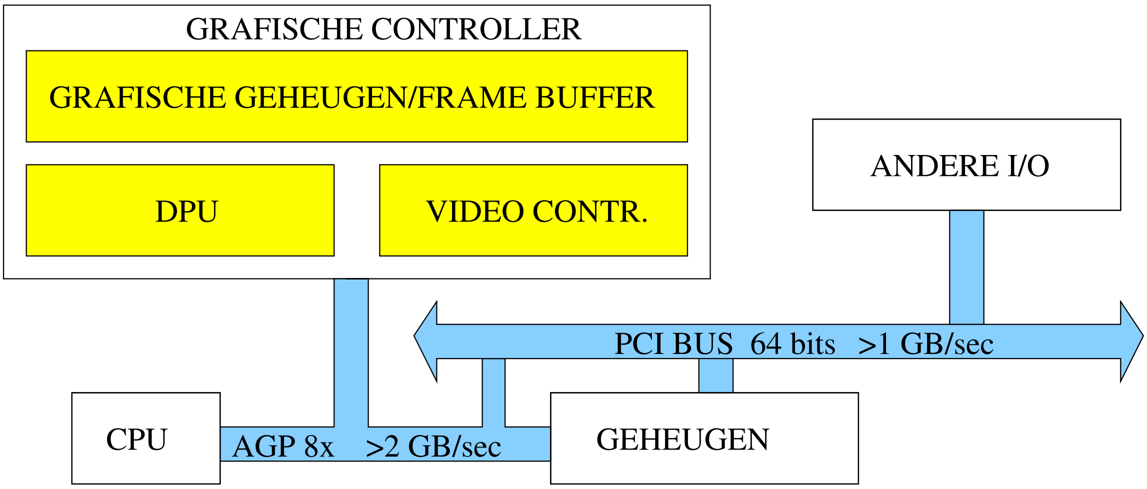


Figuur 2: Variabele breedte (pdf)



Figuur 3: Variabele breedte (png)

De macro `\PROCENT{0...99}` is nodig voor de macro's `Tabel` en `Figuur`. Deze laatste twee macro's maken het mogelijk dat tabellen en afbeeldingen in de twocolumn-mode passen met behoud van hun originele afmeting en detaillering (zie figuur 4). De parameters van deze macro's komen overeen met de parameters van de macro's `tabel` en `figuur`.



Figuur 4: Vaste breedte ook in twocolumn-mode (pdf)

In het algemeen heeft vector-graphics een betere kwaliteit van de weergave dan bitmap-graphics.

Bijzondere tekens en afbreekproblemen

Bijzondere tekens zoals de á, à, ä, é, è, ë, ï, ü, ç . . . worden probleemloos door LaTeX geaccepteerd als normale utf8 karakters. Voor de uitzonderingen bestaan macro's zoals het euro-symbool € waarvoor de macro `\euro` nodig is. In wiskundige formules kan je gebruik maken van de macro `\eurom`.

In de two-columnmode zijn regels soms te lang als er gebruik gemaakt is van `verb` of `verbatim` of woorden die niet goed worden afgebroken. In dat laatste geval kan je in zo'n woord een afbreekpunt introduceren met de twee tekens `\-`. Een regel kan gecontroleerd afgebroken door van te voren onzichtbare knikpunten te plaatsen met de `\Knak` macro. De volgende regel moet in in tegenstelling met de twocolumnmode in de verslagmode ongeknakt worden weergegeven:

```
... aaaaaaa\Knak{}aaaaaaa ...
```

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

Voor regels waarbij de structuur niet gebroken mag worden, is de `\Knak`-methode ongeschikt, bijvoorbeeld bij scripts en broncode. Daarentegen zorgt de `Aanpassen`-omgeving ervoor dat in de twocolumn-mode de regels met behoud van de originele structuur worden weergegeven. Daarvoor wordt een kleinere letterafmeting gebruikt (default de `\scriptsize`). Deze omgeving werkt alleen met niet al te lange regels. Bij zeer lange regels moet de letterafmeting zeer klein worden waardoor de leesbaarheid in het gedrang komt. In dat geval moet naar een andere oplossing gezocht worden zoals het opnemen van de probleemregels (broncode en scripts) in de bijlagen.

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

Hoewel het gebruik van opsommingen (`\item`), letterlijke citaten `quotation` en kaders (`\fbox`) in de twocolumn-mode tot problemen kunnen leiden, zijn ze beperkt toegestaan. Bijvoorbeeld voor de kaders rond de teksten kan je beter gebruik maken van de `tabular`-omgeving (of de `tabel`-omgeving als je geen last wil hebben van pagina-overgangen), dan voor de standaard `\fbox`-methode. De kolom van deze omkaderde tabel moeten dan wel een relatieve afmetingsverhouding de `\columnwidth` krijgen.

```
\begin{center}
\begin{tabular}{|>\C p{\Procent{80}}|}
\hline
Afbreekproblemen ...
\hline
\end{tabular}
\end{center}
```

Afbreek- en andere opmaakproblemen pak je als laatste aan, dus bij je definitieve verslag! Tabellen, figuren en listingen in het hoofdverslag tot het noodzakelijke beperken.

Algoritmen en broncode[3]

Als je algoritmen met een mooie layout wilt hebben, dan zou je het `algorithmic`-pakket kunnen gebruiken. Met dit pakket kan je het algoritme op een logische manier opbouwen met pseudotaal. Het bestand 'verslag.tex' bevat al de pakketten `algorithmic` en `listings` die voor dit verslag nodig zijn. Als je zelf packages wil toevoegen of verwijderen (afblijven van `\usepackage{moduleverslag}`) dan moet dat in de preambule 'verslag.tex'.

```
\usepackage{algorithmic}
```

Een algoritme moet je maken binnen een algorithmic-omgeving, een voorbeeld:

if $i \geq maxval$ **then**
  $i \leftarrow 0$
else
  if $i + k \leq maxval$ **then**
    $i \leftarrow i + k$
  end if
end if

Broncode kan je in een `verbatim`-omgeving opnemen. De broncoderegels zien er net zo uit zoals je ze ingetypt hebt. Het `listings`-pakket is geavanceerder dan de `verbatim`-omgeving.

```
\usepackage{listings}
```

Merk even op dat alle commando's van het `listings`-pakket beginnen met `lst`, dit conform de lppl-licentie.

De broncode zelf zet je in een `listings`-omgeving, net zoals bij de `verbatim`-omgeving, om broncode te zetten gebruik je het `\lstinline`-commando op dezelfde manier als het `\verb`-commando. Je kunt ook broncode van een extern document laden met het commando:

```
\lstinputlisting{pathname}
```

Het argument 'pathname' is de relatieve of absolute locatie van het bronbestand, de map(pen) gecombineerd met de bestandsnaam. Als je broncode van een bronbestand laadt, ben je zeker dat de broncode in je LaTeX-document altijd actueel is en hou je het LaTeX-document overzichtelijk. Als de broncode niet in dezelfde map of een submap van het LaTeX-document staat of je gebruikt absolute 'pathnames', dan is

het mogelijk dat het verslag niet op andere computers gecompileerd kan worden. Bij het inleveren van je afstudeerverslag in LaTeX-formaat zal je hiermee rekening moeten houden.

Alle opties in het `listings`-pakket hebben eenzelfde structuur `sleutel=waarde`. Als je alleen 'Java' gebruikt hebt, dan kan je deze taal voor je volledig document na de regel `\usepackage{listings}` in preambule 'verslag.tex' definiëren met `\lstset{language=java}`

```
public class HelloWorld {
        public static void main(String[] args) {
                System.out.println("Hello, world!");
        }
}
```

De sleutel is hier dus `language` en de waarde die je aan de sleutel geeft is `java`. Alles wat je als opties binnen de `\lstset`-macro zet kan je per `listings`-omgeving apart definiëren. Bijvoorbeeld html-broncode met `\begin{lstlisting}[language=html]`:

```
<html>
<head>
<title>Hello</title>
</head>
<body>Hello</body>
</html>
```

rampen extra

bijlmerramp

Beschrijving

Datum en plaats

Oorzaak

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.

[?]

ramp turkisch airlines vlucht 1951

Beschrijving

Datum en plaats

Oorzaak

Inadequaat handelen van de piloten ondanks een defecte hoogtemeter en onvolledige instructies van de luchtverkeersleiding/

[**?**]

[401] [403] [404] [405] [406] [407] [408] [409]

tjernobyl

Beschrijving

Datum en plaats

Oorzaak

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.

[**?**] Tsjernobyl [483] [484] [485] wat er is gebeurd en hoe het leven verdergaat [486] pernsioenfondsen en de tjernobyl ramp In 2021 worden mensen nog steeds blootgesteld blijkt ut een gezamelijk onderzoek van greenpeace en oekraiense wetenschappers stijging van de nucliaire activiteit gemeten in tjernobyl Het toerisme aspect De chronologie [487] [488] Dieren in de omgeving van tjernobyl De chronologie Echtreme droogte zorgd voor gevaar [489] [490] Joernalistiek, entertainment en de waarheid [491] Een onderzoek Huidige gevolgen van de explosie van toen [**?**] De ramp, hoe de mensen ermee omgingen en hoe er nu geleef wordt evaluatieonderzoek en amatregeen [493] [494] Invloed van de mens op de omgeving Heroplevende splijtingsreacties docu van schooltv Radioactiviteit bereikt nederland documentaire en maatregelen [496] Het verhaal van een overledende Toerisme toerisme toerisme Dieren in de omgevong Toevluchtsoord voor vluchtelingen van de oorlog met russische seperatisten Ouderen die terugkeerden naar hun woonplaats na de gedwongen verhuizing door de autoriteiten De straling neemt weer toe Lessen geleerd van tjernobyl [497] Toerisme Bosbrand in tjernobyl invloed van de ramp op belgie [498] Boek recensie Fotos en berekeningen ontmanteling en toerisme Belangrijke lessen en overeenkomsten De journalistieke waarheid van de koude oorlog De lessen van [499] Een toristenattractie maken van tjernobyl De radioactieve straling toen en nu de 30km zone door de ogen van toeristen artikel stedentrip rapport [500] slapend monster docu krantenartikel hbo serie docuserie de nieuwe sacrofaag hulp aan slachtoffers slapende reactor krantenartikel [501] hbo serie internationale gevolgen toerisme nieuwe koepel media communicatie docu dieren koepel koepel [503] toerisme toeristisch reiperspectief toerisme niwe koepel overschakelen naar duurzaamheid docu tjernobyl wekt nu duurazme energie toerisme overeenkomsten tjernobyl en fukushima drank en sla uit tjernobyl geen efficiente opslag is mogelijk wetenschappelijke artikelen zaterdag 26 april 1986. Er vind routineonderhoud plaats bij reactor 4, De controle wordt uitegevoerd door de dagploeg. Vnwege een test wordt jhet koelsysteem uitgeschakeld. Door omstandigheden wordt de test uitgesteld en wordt de verantwoordelijkheid overgedragen aan de avondploeg. De operator maakt bedieningsfouten waardoot de reactor bijna stil komt te liggen. En vervolgens probeert hij de reactor weer op gang te brengen. ondanks de snelle temperatuurstijging wordt het experiment doorgezet. Dan wordt ook het veiligheidssysteem stilgelgd. Terwijl het koelwater langzaam opwarmt, sluit hij de klep waarlangs de stoom naar de generator stroomt.

De temperatuur van de reactorstaven neemt daarna snel toe. Terwijl er een oncontroleerbare kettingreactie op gang komt, laat het personeel in paniek de regelstaven zakken om de warmteontwikkeling af te

remmen. Het is dan echter al te laat. Door een ontwerpfout loopt het vermogen razendsnel op tot 33.000 megawatt, ruim tien keer hoger dan normaal.

In een oogwenk verandert al het koelwater in stoom. De ontploffing die daarop volgt, blaast het 2000 ton zware deksel van de reactor af.

In de ravage vat het gloeiend hete grafiet in de reactor spontaan vlam. De uitslaande brand en een tweede explosie voeren een radioactieve rookwolk tot 8 kilometer hoogte. In een poging het vuur in reactor 4 te doven, storten helikopters vanuit de lucht zand, lood en boorzuur in de reactorkern. Het mag echter niet baten.

Intussen is de nucleaire brandstof zo heet geworden dat die door de bodem van het reactorvat dreigt te smelten. Als dat gebeurt, kan het bluswater onder het vat in één klap verdampen en dreigt een derde explosie die een groot deel van Europa onbewoonbaar zal maken. Om dit te voorkomen moet het water hoe dan ook worden weggepompt.

Drie brandweermannen wagen zich daarvoor in de ruimte onder de reactor, blootgesteld aan 300 sievert per uur, 300.000 keer de dosis die een Nederlander jaarlijks maximaal mag oplopen. Ze slagen daarin, maar twee van hen overlijden enkele dagen later aan acute stralingsziekte.

Hoewel geigertellers de dag na de ramp onrustbarende waarden aangeven, slaat het plaatselijk bestuur geen alarm. De bevolking is het niet gewend om vragen te stellen.

De volgende dag blijkt er wel degelijk iets ernstigs aan de hand te zijn. In een lange rij bussen worden de 135.000 inwoners op 27 april uit het besmette gebied geëvacueerd, om er nooit meer terug te keren.

De ramp is dan nog steeds geen wereldnieuws. De Sovjetautoriteiten blijken er niet eens van op de hoogte te zijn – president Gorbatsjov klaagt later dat hij via Zweden aan zijn informatie moest komen. [504] [505] [506] [507] [508]

therac-25

Beschrijving

Datum en plaats

Oorzaak

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 probleemclassicificatie 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 sheets [112] [114] reproduceren van de error. IN dit stuk wordt uitgelgd hoe het product werkt en waarom bepaalde beslssingen zijn genomen in de ontwerp/productiefase [116] kort artikel met daarin een opsomming van alle fouten in het systeem en een korte uitleg [117] uitgebreid artikel over hoe de fout werd gereproduceerd en de resultaten daaruit voortkwamen. Alsnog werden er na de reproductie fase nog meer fouten gevonden. [118] artikel [119] onderzoeksartikel waarin de bug wordt uitgelgd: de racecondities, de bytepositie en het testen worden berkitiseerd envenals andere onderdelen van het softwareproces onrealistisch testplan. In dit artikel egt de auteur het belang nog eens uit van goede requirements en implementatie, niet de software is waar het probleem ligt geschiedenis [122] artikel [123] computer error. De ongeval en de malfunction nog een keer uitgelegd [124] rapport [125] [126] onderzoeksartkel [127] [128] uitgebreid artikel gaat hier ook wat meer over de hardware [129] artikel waarin in 3 delen de problemaiekwordt blootgesteld [130] case study sheets artikel waarin vooral de fabriikant ervan langs krijgt [131] lessons learned. Vooral de begrippen betrouwbaarheid, welgevalligheid, veilgheid en gebruiksvriendelijkheid [132] root-cause analysis case study [133] case study [134] opzetten van systematische acceptaatie test met therac als voorbeeld [135] artikel waarin een diagnose plaatvindt voor het bedrijf en de ingenieur/ontwerper [136] rapport oorzaken aangegeven in artikel [137] het onderzoek en enkele ontwerptekeningen en oplossingen [138] [139] [140], [**?**] wiki [142] analyse [143] samenvatting [144] rapport over de fouten die de verschillende partijen hebben gemaakt(overheid, ingenieurs, bedrijf, operators) en de verbeterpunten onderzoeksrapport slides online over het technisch mankement Wat is er gebeurd, nou het volgende: Normal radiation treatments: 6,000 rads over a 3 week period, under certain conditions Therac-25 was delivering 60,000 rads during one session. En wat ging er mis? Paradigm Shift Therac-25 replaced expensive hardware safety interlocks with software controls Real-time software Design Race condition caused focusing element to be incorrectly set No indication of actual hardware settings Error messages appeared the same regardless of how important Error messages were difficult to understand All errors messages could be manually overridden oorzaak-gevolg diagram veiligheidsanalyse naar de rapportage van foutmeldingen, de beslissingsmatrix waarmee het programma wordt uitgevoerd en de software-analyse door een consultat [149]

tesla crash report

Beschrijving

Datum en plaats

Oorzaak

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.

tesla autopilot crashes

[317] [318] [319] [320] veiigheidsrisico

[289] [290] veiligheidsrapport mbt autopilot [291] consumentenrapport bluetooth veiligheidsvraagstuk [292] veiigheidsvraagstuk vanwege touch screen [293] veiligheidsvraagstuk [294] veiligheidsvraagstuk rapport over autopilot [295] de invloed van de bestuurder bij tesla ongeluk veiligheidsvraagstuk [297] veiligheidsvraagstuk [298] veiigheidsvraagstuk [299] veiligheidsvraagstuk veiligheidsvraagstuk [300] rapport over ongeluk veiligheidsvraagstuk veiligheidsvraagstuk [301] veiligheidsvraagstuk ransomware aanval op tesla tesla batterij is veiligheidsvraagstuk geworden [302] ongeluk [303] veiligheidsvraagstuk veiligheidsvraagstuk [304] dodelijk ongeluk [305] veiligheidsvraagstuk: ransomware veiligheidsvraagstuk: medewerker in de fout [306] [307] veiligheidsvraagstuk: hackers je systeem laten testen verdedigen tegenover ransomware veiligheidsrisico prijzen omlaag autopilot [308] malware door een medewerker dodelijk ongeluk [311] waarom een tesla stelen bijna onmogelijk is

veiligheidsonderzoek

softwarefout maakt diestal mogelijk

[314] fouten ontdekt in onderzoek [316] tesla cloud gehacked [332] [334] [337] [339] [340] [341] [**?**] [**?**] [342] [343] [344] [345] [346] [347] [348] [349] [350] [351] [352] [353] [354] [355] [356] [357] [358] [359] [360] [361]

tesla crash report

[368] [369] [370] [371] [372] [373] [374] [384] [386] [387] [388] [390] [391] [392] [393] [394] [395] [396] [397] [**?**] [**?**] [**?**] [**?**] [**?**] [**?**] [**?**] [**?**] [**?**] [**?**] [**?**]

tesla crash publications overview

slmramp

Beschrijving

Datum en plaats

Oorzaak

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.

[460] [463] [464] [465] [466] [467] [468] database [470] rapport [471] [472] [473] [475] [476] [477] uitgebreid engels artikel [478] ntsb investigtion [479] uitgebreid engels artikel [480] persbericht [481] Wat is de rol van de autoriteiten? Welke andere betrokkeen? Enw at is hun verantwoordelijkheid Hadden de negatieve gevolgen voorkomen kunnen worden? Hoe werd er over veiligheid gedacht?

schipholbrand

Beschrijving

Datum en plaats

Oorzaak

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 Wat is er gebeurd? [426] artikel [426] psychologische gevolgen rapport [427] artikel met video herdenking impact op de persoon herdenking [428] chronologie [429] tijdlijn vervolgens van ministers beeldanalyse en reconstructie [**?**] herdenking korte samenvatting rapport artikel verwijzing naar het rapport vanuit de politieke oppositie beeld vanuit de gevangenisbewaarder nationaliteit slachtoffers schipholbrand verblijfsvergunning voor de slachtoffers gen schadevergoeding voor de verdachte verdachte voor de rechter geen schadevergoeding voor verdachte artikel wat ging er mis bji

de schipholbrand brand veroorzaakt door een peuk smaadschrift bewakers worden niet vervolgd proces schipholbrand moet over en de brandveilgheid moet worden verbeterd de rol van het parlement in de evaluatie [432] onderzoeksmemo herdenking herdenking invloed van de ramp op samenleving [434] opmerkelijk rapport gestolen in de nasleep [438] publicaties [439] Wat waren de regels destijds? Waren de autoriteiten in staat om op tijd in te grijpen of om erger te voorkomen? Wat is er gedaan om de veiligheid van illegalen en gevangenissbewaarders te verbeteren Wat is er gebeurd? [425],[426] psychologische gevolgen rapport [427] artikel met video herdenking impact op de persoon herdenking [428] chronologie [429] tijdlijn [430] vervolgens van ministers beeldanalyse en reconstructie [431] herdenking korte samenvatting rapport artikel verwijzing naar het rapport vanuit de politieke oppositie beeld vanuit de gevangenisbewaarder nationaliteit slachtoffers schipholbrand verblijfsvergunning voor de slachtoffers gen schadevergoeding voor de verdachte verdachte voor de rechter geen schadevergoeding voor verdachte artikel wat ging er mis bji de schipholbrand brand veroorzaakt door een peuk smaadschrift bewakers worden niet vervolgd proces schipholbrand moet over en de brandveilgheid moet worden verbeterd de rol van het parlement in de evaluatie [432] onderzoeksmemo herdenking herdenking invloed van de ramp op samenleving [434] opmerkelijk rapport gestolen in de nasleep [438] publicaties [439] Wat waren de regels destijds? Waren de autoriteiten in staat om op tijd in te grijpen of om erger te voorkomen? Wat is er gedaan om de veiligheid van illegalen en gevangenissbewaarders te verbeteren

explosie tanjin china

Beschrijving

Datum en plaats

Oorzaak

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/ [**?**] verhaal van brandweermannen [**?**] artikel [**?**] invloed van social media [215] gemaakte fouten [220] [223] [224] [225] vergelijking met andere explosies [226] invloed van de ramp op de industrie [227] is er sprake van een doofpot [228] eigendomsverzekering [229] [230] effecten op de lange termijn [231] [232] lessons learned [235] [236] gevolgen voor de industrie [238] framing vanuit de chinese media [239] [240] niewsartikel [241] [242] toegang tot de ramplplek vanuit de okale journalistiek [243] artikel [245] [246] [247] [248] oorzaken [249] case study [**?**] niewsartikel [**?**] chronologische uiteenzetting [**?**] corruptie mismanagement als oorzaak autoriteiten publiceren onderoeksrapport [252] fotos van de rampplek [253] niuwesartiekel [255] [273] [274] [275] 123 verantwoordelijken [276] lang artiekel [278] [280] [281] [282] [283] [284] veiigheidshandhaving [285] [287] [288]

ethiopian airlines

Beschrijving

Datum en plaats

Oorzaak

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.

[**?**] [664] [665] [666] [667] [668] [669] [670] [671] [672] [673] [674] [675] [676] [677] [678] [679] [680] [681] [682] [683] [684] [685] [686] [687] [688] [689] [691] [692] [693] [694] [695] [696] [697] [698] [699] [700] [701] [702] [703] [704] [705] [706] [707] [708] [709] [710] [711] [712] [713] [714] [716]

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/10.3389/frai.2020.00007/full [**?**] 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/rug01:001235489 https://cyberpsychology.eu/article/view/12270 [**?**]

Research case: De digitale aanval op de Oekrainese krachtcentrale

Beschrijving

Datum en plaats

Oorzaak

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. [63] [**?**] [64] [509] [511] [513] [515] [519] [520] [521] [522] 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. [63],[64],[42],[58],[59],[60],[61],[515],[62]. 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. [63] Uit onderzoek[64] 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.

Literaire analyse

Motief Oekraine wijst naar de russen [64], [**?**], [42], [56], [55], [54], [53].

Situatie Oekraiene [52], [51].

Situatie algemeen [511], [59], [49].

Factoren [48]

Oorzaak [27], [47], [46], [51].

Gebruikte materialen [44], [43]

Uitvoering van de aanval [63], [42].

Oplossingen [63]

Aanbevelingen

Resultaten

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. [63] [42]

spearfishing

blackenergy

remote access capabilities

serial-to-ethernet communication devices

telephony denial of service attacks

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. [63]

Discussie

Verder lezen [41], [513], [39], [38], [37],[36],[35],[34],[33],[33],[32],[31],[30],[29],[28],[26],[25],[24].

Mali

Beschrijving

Datum en plaats

Oorzaak

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.

[**?**] [410] [411] [412] [413] [414] [415] [416]

[418] [419] [420] sollicitatie de bureaucratie aankomst interview van de burgerbevolking steun van de bevolking minuut 15:00 de organisatie minuut 23:00 De militaire briefing minuut 34:00 prioriteit minuut 39:00 briefing minuut 40:00 de communicatie met ministerie over inlichten minuut 44:00 [**?**]

Analyse

Conclusie

Deelonderzoeken

AlgemeenDeelonerzoek naar veiligheidsrisico's voor sluizen

Wet en regelgeving voor sluizen

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 [74] 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.

[**?**] Sluis Eefde kreeg niet alleen de onderhoudsbeurt, maar werd tevens uitgebreid met een tweede sluiskolk. Zo wil Rijkswaterstaat wachttijden voor de scheepvaart voorko

[77] 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.

[**?**] 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.

[**?**] 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.

[**?**] deltawerken

[**?**] 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 60%) was begin 2018 ook al uitgevoerd, maar Rijkswaterstaat ziet onvoldoende toe op de uitvoering van het resterend deel en heeft geen actueel overzicht van de overgebleven maatregelen. De 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.

[**?**] 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.

[**?**] Rittal doet onderzoek naarop afstand besdienbare sluizen

[**?**] Beveiligde VPN M2M Services levert aan inmiddels 220 gemeenten en waterschappen beveiligde connectiviteitsoplossingen voor het beheer van pompen, riolen en gemalen. Om risico's op beveiligings-

incidenten te voorkomen maken wij gebruik van een VPN oplossing, waarbij de verbinding optimaal beveiligd is middels encryptie en authenticatie.

[**?**] Veiligheid op het water én op het land Gebruik van lampbewaking

[**?**]

explosie in libabon, beirut

Beschrijving

Datum en plaats

Oorzaak

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.

[**?**]

[**?**]

[**?**]

stint ongeluk

Beschrijving

Datum en plaats

Oorzaak

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

[567]

vuurwerkramp in enschede

[**?**]

Wat waren de afspraken omtrent vuurwerkopslag? Waarom werden de voorschriften neit nageleefd?

ecourt in nederlandse rechtspraak

Beschrijving

Datum en plaats

Oorzaak

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-$2017_20180201.pdf$[**?**]

molukse treinkaping

Beschrijving

Datum en plaats

Oorzaak

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

Ramp schietpartij militair ossendrecht

Beschrijving

Datum en plaats

Oorzaak

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 [**?**] [422] [423] [424]

Wat is de rol van defensie? Wat is er gedaan om de veligheid van de medewerkers te waarborgen? Waarom zijn deze regels niet nageleefd? Wat zijn de gevolgen? Zijn de acties die naderhand zijn ondernomen wel redelijk naar de slachtoffers, het nationale veiligheisbeeld en de medewerkers?

Model

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

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).

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.

- Vooraanmelding
- informatie inwinnen
- operationele melding
- aankomst volgorde
- aanwijzen wachtplaats
- verstrekken informatie
- aanwijzen opstelplaats
- opstellen schutproces
- verstrekken informatie
- invaarvolgorde en ligplaats in sluis
- uitvaren
- operationele afmmelding
- utvaren verboden
- aanwijzing invaren nieuwe schepen
- invaren verboden
- deuren gesloten
- 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

Requirements definitie 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.

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?

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.

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

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)

Aandachtspunten

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

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.

Functionele en niet-functionele eisen

specificaties

Het vier variabelen model van de sluis Systemen (met daarin software) en de bijbehorende vier variabelen:

Monitored variabelen : door sensoren gekwanti

ceerdefenomenen uit de omgeving

Controlled variabelen door actuatoren bestuurde fenomenen uit de omgeving

Input variabelen

Output variabelen 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

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.

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.

4.2 5 en 6 Het Sluisbeheeerder model wordt getoond in fuguur[]. Het model is een uitbreiding van een schutsluis met alle condities en effecten. De kleuren in de automation verwijizen naar de kleuren in de staat van de automata . De template begint met een initiele lokatie start. De sluisbeheerder initieert het proces door een aangekomen schip te registreren metbehulp van een sychronizate met het channel... over de edge richtng de lokatie äanmelden."Dit symboliseert een opstartprocedure, ook wordt een functie enqueeu$_a$*anmeldLijst*()*gebruiktomdejuistewaardentegevenaanlokaleenglobaleavariabelen.Delokatieaanmeldenregiss*
/*uitvaartvandeverschillendeschepenwordenlijstenbijgehouden* : *list*$_w$*achtrij*$_b$*eneden*, *list*$_p$*os*$_i$*nvaren*$_b$*eneden*, *list*$_s$*chepe*

Het model voltooit de volgende transitie op basis van de waarde van de boolean *sluis*$_b$*ove* en *sluis*$_b$*eneden*. en de lokale klok variabele x. Vanaf de locatie invaarverbod$_g$*econtroleerdwordtgecontroleerdofernoginvarendeschepenzijndieindesluiskolkpassen.Opdelokatiesluis*

De lokatie start$_n$*ivellerenkiestopbasisvandevariabelensluis*$_b$*ovenendevariabelensluis*$_b$*enedenhetnivellereingsprogra*

De lokatie klaarmaken$_v$*oor*$_o$*penenwordtbereiktalsdehoogtevandesluisdoorhetnivellereingsprogrammaisbereikt.De*

De lokatie uitvaren$_t$*oegestaanheefteenverbinding*(*edge*)*metdelokatiesluis*$_a$*fsluiten.Eriseenselectstatement*, *e* :
id$_t$*gebruiktalsonderdeelvanhetprotocolomalleuitvarendeschepenuitdequeuevandesluiskolktehalen*, *enwordtdanookg*

Vanuit de positie van de sluis worden de schepen gesignaleerd op een invaarverbod en worden de deuren van de sluis gesloten. De lokatie sluiskolk$_a$*fgeslotenisbereikt*.

Ship [guards, invariants, assignents, synchronizations, properties,aannames] De template Schip begint bij de Init lokatie. De lokatie is verbonden met de lokatie aangekomen met een edge waarbij een synchronizatie wordt aangeroepen met de template sluisbeheerder. De clock wordt op nul gezet. De lokatie aangekomen is verbonden met de lokatie aangemeld. De edge bevat een synchronizatie waarmee de edge een synchronizatie uitvoert met de template Sluisbheheerder. De volgende

lokatie is controleren. De edge waarmee de lokatie aangemeld in verbinding staat met de lokatie cnotroleren heeft een synchronisatie voor de template Sluisbeheerder. De lokatie controleren heeft ook een edge met de lokatie wachten. Een schip max maximaal 30 seconden wachten op de lokatie wachten voordat er een mogelijkheid is om opniew in aanmerking te komen voor een controle. Als een schip langer dan 30 tijdseenheden moet wachten de is er een mogelijkheid voor het schip te vertrekken. Hierbij eindigt het schip het invaarproces. Een schip kan dus na aanvaren maximaal 20 seconden wachten om toestemming te krijgen voor een positie invaren anders wordt deze verwezen naar een wachtrij. Hierna volgdde lokate invarene. De lokatie invarene implieert dat een schip in een invaarproces is dat eindigt in de lokatie gestopt. Hierop volgd de lokatie nivelleer$_{s}tart.Hieropwordteennivelleer_{p}rocesgestart.Daarbijiseesynchronisatiemetdetemplate Sluisbeheerder.Delokat$
$3tijdseenhedenmageenschipvertrekken.$

Deur De deur bevat de volgende lokaties: dicht, openend, open en sluitende. Een deur sluit niet in een enkele actie. Het proces die een deur dooploopt zijn de processen openend en sluitende. De finale lokaties zijn open en dicht.

Nivelleermachine De nivelleermachine begint bij de lokatie uit. Met een synchronisatie wordt een nivelleermachine aangezet. De automatie kiest een programma en werkt deze uit in de lokatie bezig. Als ht programma is afgerond volgt de lokatie klaar. Na elk nivelleerproces wordt de machine uitgezet

Stoplicht Een stoplicht heeft twee lokaties: rood en groen.

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.

Verificaie extra

De safety en reachability requirements die formeel zijn gespecificeerd worden in Uppaal geverifieerd met de A en E state formule. Andrerere opreratoren zijn

inleiding 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.

ctl CTL formulas are based on the following operators: A (every path") E (exists a path") X ($time$")$G(or)F(or)$ U () R ()

Deze zijn als volgt:

A[] not maincontroller.rd1 imply

A[] maincontroller.rd1 imply

A[] not deadlock imply

E<> maincontroller.rd1 imply

E<> maincontroller.s7

E<> maincontroller.s7d

Formele specificaties

Timed automata Before we consider a reachability problem, we show how real-time systems can be modoeled as parralel compositions of timed automata [3,5]. We assume an interleavingor asynchroneous semantics for this operation. Let A1 = ($\sum$, S1, $\S_0^1$, X_1, I_1, T_1) and A_2 = ($\sum_2$, $S1_2$, $\S_0^1$, X_2, I_2, T_2) be two timed automata. Assume that the two automata have disjoint sets of clocks, that is $X_1 \cap X_2 = \emptyset$. Then, the parralel composition of A_1, and A_2 is the timed automation:

A_1 || A2 = ($\Sigma \cup \Sigma_2$, S_1 x S2, $\S_0^1$ x $\S_0^2$, $X_1 \cup X_2$, I, T), where I(s_1,s_2)=$I_1(s_1) \wedge I_2(s_2)$ and the edge relation T is given by the following rules:

1 For a $\in \Sigma_1 \cap \Sigma_2$, if $\langle$ s1,a, φ, λ_1, s_1' $\rangle \in T_1$ and $\langle$ s2,a, φ, λ_2, s_2' $\rangle \in T_2$
then T will contain the transition $\langle$ (s1,s2), a φ , $\lambda_1 \cup \lambda_2$, (s_1',s_2') $\rangle$
2. For a $\in \Sigma_1$ - Σ_2, if $\langle$ s, a, φ, λ, s' $\in T_1$ and t $\in S_2$ then T will contain the transition $\langle$ (s,t),a, φ, λ, (s', t) $\rangle$

3. For a $\in \Sigma_2$ - Σ_1, if $\langle$ s, a, φ, λ, s' $\in T_2$ and t $\in S_1$ then T will contain the transition $\langle$ (t,s),a, φ, λ, (t,s') $\rangle$

Thus the locations of the parralel composition are pairs of locations from the component automata, and the invariant of such a location is the conjunction of the invariants of the component locations. There will be a transition in the parralel compoition for ach pair of transitions from the individual timed automata with the same action The source location of the transition will be the composite location obtained from the source locations of the individual transitions. Te target location will be the compositelocation obtained from the target locations of the individual transitions. The guard will be the conjunction of the guards for the individual transitions, and the set of clocks that are reset will be the union of sets that are reset by the individual transitions. If the action of a transition is only an action of one of the two processes, then there will be a transition in the parralel composition for each location of the othertimed automation. The source and target locations of the original transition and the location fromthe other automation. All of the other components of the transition will remain the same.

Timed automata A timed automation[8,99] is a finite augmented with a finite set of real-valued clocks. We assume that transitions are instantaneous. However, time can elapse when the automation is in a state or location. When a transition occurs, some of the clocks ma be reset to zero. At any instant, the reading clock is equal to the time that has elapsed since the lat time the clock was reset. We assume that time passes at the same rate for all clocks. In order to prevent pathological behaviours, we only consider automata that are non-zeno, that is, only a finite number of transitions can happen within a finite amout of time.

A clock constraint, called a guard, is associated with each transition. The transition can be taken only if the current values of the clocks satisfy the clock constraint. A clock cnstraint is also associated with each location of the automation. This constraint i called the invariant of the location. Time can elapse in the location only as long as the invariant of the location is true. An example of a timed automation is shown in Figure 17.1 The automation consists of two locations s0 and s1, two clocks x and y, and ä"transition from s0 to s1, and a "b"transition from s1 to s0. The automation starts in location s0. It can remain in that location as long as the clock y is less than or equal to 5. As soon as the value of y is greater than or equal to 3, the automation can make an ä"transition to location s1 and reset the clock y to 0. the automation can remain in location s1 as long as y is less than or equal to 10 and x is less than or equal to 8. When y is at least 4 and x is at least 6, it can make a "b"transition back to location s0 and reset x.

The remainder of this section contains a formal semantics for timed automata in terms of infinite state transition graphs[3,8]. We begin with a precise definition of clock constraints. Let X be a set of clock variables, ranging over the nonneative real numbers $\Re^+$. Define the set of clock constraints C(X) as follows: All inequalities of the form x $\prec$ c or c $\prec$ x are in C(X) where $\prec$ is either < or and c is a nonnegative rational number. If φ_1 ad φ_1 are in C(X), then $\varphi_1 \wedge \varphi$ is in C(X).

Note that if X contains k clocks; then each clock constraints is a convex subset of k-dimensional Eucledian space.Thus, if two points satisfy a clock constraint, then all of the points on the line sement connecting these points satisfy the clock constraint. A timed automation is a 6-tuple A = (Σ, S, S_0, X, I, T) such that:
Σ is a finite alphabet
S is a finite set of locations
S0 $\subseteq$ S is a set of starting locations
X is a set of clocks
I : S $\rightarrow$ C(X) is a mapping from locations to clock constraints called the location invariant.
T $\subseteq$ S x Σ x C(X) x 2^x x S is a set of transitions. The 5-tuple $\langle$ s,a,φ, λ, s' $\rangle$ corresponds to a transition from location s to location s' labeled with a, a constraint φ that specifies when the transition is enabled, and a set of clocks $\lambda \subseteq$ X that are reset when the transition is executed.

We will require that time be allowed to progress to infinity, that is, at each location the upper bound imposed on the clocks be either infinity, or smaller than the maximum bound imposed by the invariant and by the transitions outgoing from the location. In other words, it is possible either to stay at a location forever, or the invariant will force the automation to leave the location, and at that point at least one transition will be enabled. For timed automata, these constraints can be imposed syntactically.

A model for a timed automation A is an infinite state transition graph τ(A) = (Σ, Q, Q^0, R). Each state in Q is a pair (s, v) where s $\in$ S is a location and v : X $\rightarrow R^+$ is a clock assignement, mapping each clock to a nonnegative real value. The set of initial states Q_0 is given by (s,v)| s $\in S_0 \wedge \forall$ x $\in$ X[v(x) =0].

In order to define the state transtion relation for τ(A), we must first introduce some notation. For $\lambda \subseteq$ X, define v[λ := 0] to be the clock assignment that is the same as v for clocks in X - λ and maps the clocks in λ to 0. For d $\in \Re$, define v +d as the clock assignment that maps each clock x $\in$ X to v(x) +d. The clock assignment v -d is defined in the same manner. From the brief discussion in the introduction, we know that a timed automation has two basic types of transitions:

Delay transitions correspond to the elapsing of time while staying at some location.

We write (s, v) $\xrightarrow{d}$ (s, v+d), where d $\in R^+$, provided that for every 0 $\leq$ e $\leq$ d, the invariant l(s) holds for v +e.

Action transitions correspond to the execution of a transition from T. We write (s,v) $\xrightarrow{a}$ (s', v'), where a $\in \Sigma$, provided that there is a transition $\langle$ s,a, φ, λ, s' $\rangle$ such that v satisfies φ and v=[λ:=0].

The transition relation R of τ(A) is obtained by combining the delay and action transitions. We will write (s,v) R(s', v') or (s, v) $[]f(x)$ (s', v') if there exists sänd v"such that (s,v) $\xrightarrow{d}$ (s", v")$\xrightarrow{a}$ (s', v') for some d $\in \Re$. In this chapter we will describe an algorithm for solving the reachability problem for τ(A): Given a set of initial states Q_n, we show how to compute the set of all states q $\in$ Q that are reachable from Q_0 by transitions in R. This problem is nontrivial because τ (A) has an infinite number of states. In order to accomplish this goal, it is necessary to use a finite representation for the infinite state space of τ(A). Developing such representations is the main topic of te following sections.

clock regions In the definition of timed automata, we allowed the clock constraints that serve as the invariants of locations and the guards of transitions to contain arbitrary rational constants. We can multiply the constants in each clock constraint by the least common multiple m of the denominators of all the constants to integers. The value of a clock can still be an arbitrary nonnegative real number. Note that applying this transformation can change the clock assignments in the set of reachable states of T(A). Fortunately, this does not cause a mjor problem. Ther reachale states of the original auomation can be obtained from the locations of te transformed automation by applying the inverse transformation, that is, dividing each clock value by m.

Th largest constant in the tranformed in the transformed automation is the product of m and the largest constant in the original automation. Thus, the transformation at worst results in quadratic blowup in the length of the encodings of th lock constraints[3]. This increase in complexity is acceptable, since the transformation simplifies certain operations on clock constraints that will be needed later in the chapter. We will apply this tranformation uniformly to all of th clock constraints that appear in the timed automata the we study. Consequently, in the future we can assume without loss of generality that all constants in clock constraints that we encounter are integers.

In order to obtain a finite representation for the infinite state space of a timed automation, we define clock regions[7,8], which represents sets of clock assignments. If two states, which correspond to the same location of the timed automation A, agree on the integral parts of all clock constraint in the invariant of a location or in the guard of a transition is satisfied or not. The ordering of the fractional parts of the

clock values determines which clock will change its integral part first. This is because clock constraints cn involve only integers, and all clocks increase at the same rate.

For example, let A be a timed automation with two clocks x1 and x2. Let s be a location in A with an outgoing transition e to some other location. Consider two states (s,v) and (s,v') in T(A) that correspond to location s. Suppose that v(x1) = 5.3, v(x2)=7.5, v'(x1)=5.5 and v'(x2) = 7.9. Assume that the guard φ associated with e is $x1 \geq 8 \wedge x2 \geq 10$. It is easy to see that if (s,v) eventually satisfies the guard, then so will (s, v').

The value of a clock cn get arbitrarily large; however, if the clock is never compared to a constant greater than c, then the value of the clock will have no effect on the computation of A once it exceeds c. Suppose, for instance, that the block x is never compared to a constant greater than 100 in the invariant associated wit a location or in the guard of a transition.

Then, based on the behaviour of A, it is impossible to distinguish between x having the value 101 and x having the value 1001. Alur,Courcoubetis, and Dill[7,8] show how to formalize this reasoning. For each clock $x \in X$, let cx, be the largest constant that x is compared with in the invariant of any location or in the guard of any transition. For $t \in \Re^+$, let ft(t) be the fractional part of t, and let [t] be the integral part of t. Thus, t = [t] + fr(t). We define an equivalence relation $\cong$ on the set of possible clock assignments as follows: Let v and v' be two clock assignments. Then $v \cong v'$ if and only if three conditions are satisfied:

For all $x \in X$ either $v(x) \geq cx$, and $v'(x) \geq gx$ or [v(x)] =[v'(x)]. For all x,y $\in X$ such that $v(x) \leq cx$ and $v(y) \leq cy$, $fr(v(x)) \leq fr(v(y))$ if and only if $fr(v'(x)) \leq fr(v'(y))$ For all $x \in X$ either $v(x) \leq cx$, fr(v(x)) =0 if and only if fr(v'(x)) =0. it is easy to see that $\cong$ does indeed define anequivalence relation. The equivalence classes of $\cong$ are called regions[7,8]. We will write [v] to denote the region which containsthe clock assignment v.Each region can be represented by specifying

1. for every clock $x \in X$, once clock constraint from the set x=c | c=0...., cx $\cup$c -1 < x < c | c=1,.....cx $\cup$ x > cx 2. for every pairof clocks x, y $\in X$ such that c-1 < x< cand d-1<y< d are clock constraints in the first condition, whether fr(x) is less than, equal to, or greater than fr(y).

Figure 17.7 which is taken from [8], shows the clockregions for a timed automationwith two clocks x and y where cx = 2 and cy =1. In this example, there are a total of 28 regions: 6 corner points, 14 open line segments and 8 open regions.

We will use this observation to show that $\cong$ has finite index and, consequently, that the number of regions is finite. Our proofof this fact is based on the proof given in [8].

Lemma 43 The number of equivalence classes that $\cong$ induces on C(X) is bounded by $|X|! \cdot 2^{|X|} \cdot \prod$ (2xc +2) proof An equivalence class [v] of $\cong$ can be described by a tripple of arrays i the following manner. For each block $x \in X$, the array α tells which of the intervals [],[] contains the value v(x). Thus, the array α represents the cloc assignment v if and only if for each clock $x \in X$, $v(x) \in \alpha(x)$. The number of ways to choose α is $\prod$.

Let X_a be th set of clocks with nonzero fractional part. The array β: $x_a \rightarrow 1,....|A_a|$ is a permutation of X_a, which gives the ordering of the fractional parts of the clocks in Xa with respect to $\leq$. Thusm the array represents a clock assignment c if and if for each pair $x,y \in X_a$, if $\beta(x) < \beta(y)$ then $fr(v(x)) \leq fr(v(y))$. For a given α, the number of ways to choose β is bounded by $|X_\alpha|!$ which is bounded by |X|!.

The third component γ is a boolean array indeed by X_a that is used to specify which clocks in X_a have the same fractional part. For each clock c, γ(x) tells whether or not the fractional part of v(x) equals the fractional part of its predecessor in the array β. Thus the array γ represents a clock assignment v if and only if for each x X, γ(x) equals 0 exactly when there is a clock $\gamma \in X_a lpha$ such that β(y) = β(x) +1 and fr(v(x)) equals fr(v(y)). The number of ways of choosing γ is bounded by the number of boolean arrays over X_α, which is bounded by $2^{|X|}$. Hence, α encoded the integral parts of he clock assignments, and β with γ encodes the ordering of their fractioal aprts. It is easy to see that the sets represented bytriples are equivalence of ≅ and that every equivalence class is represented by some triple. The bound given in the statement of the lemma is the product of the bounds associated with α, β, and γ. This completes the proof of the lemma.

The following properties of the equivalence relation ≅ are used in later in this chapter. Lemma 44 Let v1 and v2 be twoclock assignments1, let φ be a clock constraint, and let λ ⊆ X be a set of clocks. 1. if v1 ≅ v2 and t is a nonnegative integer, then v1 + t ≅ v2 +t. 2. if v1 ≅ v2, then ∀ t1 ∈ $R^{|+|}{}_2 \in R^{|+|}$[v1 +t1 ≅ v2 + t2] 3. if v1 ≅ v2, then v1 satisfies φ if and only if v2 satisfies φ 4. If v1 ≅ v2, then v1[λ:=0] ≅ v2 [λ:=0]

Note that the first property may not hold if t is not an integer. For example, (2.8) ≅ (.1, .2), but (.2, .8) +.3 is not equivalent to (.1,.2) + .3. All of the properties except the second are straightforward to prove and will be left to the reader. A proof if the scond property is sketched below. The proof is not diificultm but it is somewhat tedious. It can be safely skipped when this chapter is read for the first time.

Proof Assume that v1 ≅ v2. We can assume that t1 > 0 because, otherwise, we can simply choose t2=0. Let Xx1,x2,.....,xn. We can threat v1 as a vector v1 = ⟨ a1, ..., an ⟩, where a_i is the alue of clock x_i in v_1. Similarly, we let v2 = ⟨ b1, ..., b_n ⟩. Since corresponding clocks have the same integer part, we can assume without loss of generality that $0 \leq a_i < 1$ and $0 \leq b_i < 1$. Also , assume that the clock values are sorrted into increasing order so that $a_1 \leq a_2 \leq ... \leq a_n$ and b1 ≤ $b_2 \leq .... \leq b_n$.

case 1 Assume that the largest element in v1 + t1 is less than or equal to 1. This case is trivial. We can easilty choose t2 so that v + t1 ≅ v2 + t2

case 2 Assume that 0 ≤ t1 < 1. Let the first element of v1 +t1. That is greater than or equal to 1 be a_k+t1. Chhoose ∈ so that ∈ =0 if $a_k + t_1$ =1 and so that 0< ∋<b$_k$-$b_k - 1$ if a_k+t_1 > 1. Note that b_k-1 < b_k = b_k-1, then a_k=a_k-1 and a+t_1 is not the first elment of v1+t1 that is greater than o equal to 1. We will show that v1+t1 ≅ v2+(1+ ∈ - b_k). In order to show this we will split the vectors into two parts. Let

L1= ⟨ a_1 + t1, ..., a_k-1 + t1 ⟩, and L2= ⟨ b_1 + (1 + ∈ - b_k), ..., b_k-1 + (1+ ∈ - b_k) ⟩ In each case it is straightforward to show that

1. all of the elements are positive 2. the elements are sorted in increaing order, and 3. all of the elements are less than 1 Because of these conditios it is easy to see that $L_1 \cong L_2$. Similarly, let

R_1= ⟨ a_k + t1, ..., a_n + t1 ⟩, and R_2= ⟨ b_k + (1 + ∈ - b_k), ..., b_k-1 + (1+ ∈ - b_k) ⟩

All of the elements in R_1 and R_2 are greater than or equal to 1. The fractional parts are given by R_1 - 1 and R_2 -1, respectively. For these vectors it is straightforward to show that

1. all of the elements are nonnegative 2. the elements are sorted in increasing order, and 3. all of the elements are less than 1

Moreover, an element in one vector is 0 if and only if the corresponding element in the order vector is 0. Thus R_1 -1 ≅ R_2 -1. It follows immediately that $R_1 \cong R_2$. It is not difficult to see that the fractioal parts of R_2 precede the fractional parts of L_2. Let i ≥ k and j < k. Then b_i + (1 + ∈ - b_k) -1 ≤ b_j + (1+ ∈ - b_k). is equivlent to b_i - $b_j \leq 1$, which is obviously true. The same relationship holds for the fractioal parts of R_1 and L_1, that is. $a_i + t_1$ -1 ≤ $a_j + t_1$.

hence , we obtain $R_1 \cdot L_1 \cong R_2 \cdot L_2$, where "·ïs concatenation of vectors. This shows that for all t_1 with 0 ≤ t1 < 1, there exits a t2 such that $v_1 + t_1 \cong$ v2 + t_2 and completes the proof of

case 3 Finally, supppose that $t_1 \geq 1$. Let t1'= t_1 - [t_1], so that $0 \leq t_1 < 1$. Find t_2 such that $v_1 + t_1 \cong$ v2 + t2. Then: v1 + t1 + [t1] $\cong$ v2 + t2 + [t1].

If we choose t2 = [t1], then we have v1 + t1 $\cong$ v2 + t2 as required. This completes the proof of the second property.

The equivalence relation $\cong$ over clock assignments an be extended to an equvalence relation over the state space of T(A) by requiring that equivalent states have identical locations and equivalent clock assignments: (s,v) $\cong$ (s', v') if and only if s = s' and v $\cong$ v'. The key property of he equivalence reltion $\cong$ is given by the following lemma [5]:

Lemma 45 If v1 $\cong$ v2 and (s, v_1) $\xrightarrow{a}$ (s', v'). The transition $\langle$ s, a, φ, λ, s' $\rangle$ that takes state (s, v1) to state (s', v1') corresponds to two transiions of the timed automation.

Proof Assume that v1 $\cong$ v2 and (s, v1) $\xrightarrow{a}$ (s', v'1). The transition $\langle$ s, a, φ, λ, s' $\rangle$ that takes state (s, v1) to state (s', v'1) corresponds to two transitions of the timed automation:

a delay transition (s, v1) $\xrightarrow{d1}$ (s, $v_1 + d_1$) for some $d_1 \geq 0$, and an action transition (s, v1 +d1) $\xrightarrow{a}$ (s', v_1') such that $v_1 + d_1$ satisfies φ and $v'_1 = (v_1 + d_1)[\lambda := 0]$.

Since v1 $\cong$ v2 and v1 satisfies I(s), v2 also satisfies I(s). Furthermore, there exists d2 ≥ 0 such that v1 + d1 $\cong$ v2 + d2. Since v1 + d1 satisfies I(s), v2 +d2 also satisfies I(s). Because the clock constraint I(s) is convex and is satisfied by both v2 and v2 + d2, I(s) must be satisfied by v2 + e for all e such that 0 $\leq$ e $\leq$ d2. Consequently, the delay transition (s, v2) $\xrightarrow{d2}$ (s, v2 +d2) is legal.

Since v1 + d1 $\cong$ v2 +d2, both v1+ d1 and v2+ d2 must satisfy the clock constraint for the guard φ. Thus, the transition $\langle$ s, a, φ, λ , s' $\rangle$ myst also be enabled in the state *s, $v_2 + d_2$. Let $v'_2 = (v_2 + d_2)[\lambda := 0]$. Then v'$_2$ is equivalent to v'_1. Hence, there is an action transition (s, $v_2 + d_2$) $\xrightarrow{a}$ (s', v'_2). Combining the delay transition with the action transition, we get (s, v_2) $\xrightarrow{a}$ (s', v'_2) as required.

As a result of the lemme, we can conostruct a finite state transition raph that is bisimilaion equivalnt to the infinite state transition graph T(A). The finite state transition graph is called the region graph of A[7,8] and is denoted by R(A). A region is a pair (s, [v]). Since $\cong$ has a finite index, there are only a finite nuber of regions. The states of the region graph are the regions of A. The construction of R(A) will have the property that whenever (s,v) is a state of T(A), the region (s, [v]) where s_0 is an initial state of A and v_0 is a clock assignment that assigns 0 to every clock. The transition relation of R(A) is defined so that bisimulation equivalence is guaranteed. There will be a transition labeled with a from the region (s,[v]) to the region (s', [v']) if and only there are assignments $\omega \in$ [v] and ω' $\in$ [v'] such that (s, ω) can make a transition to (s', ω')

We summarize the construction of the region graph R(A) below. Let A = (σ, S, S_0, X, I, T) be a timed automation. Then, The states of R(A) have the form (s, [v]) where s $\in$ S and [v] i a clock region The initial states have the form (s_0, [v]) where $s_0 \in s_0$ and v(x)=0 for all x $\in$ X. R(A) has a transition ((s,[v]),a, (s',[v'])) if and only if (s, ω) $\xrightarrow{a}$ (s', ω') for some $\omega \in$ [v] and some ω' $\in$ [v']. We can use Lemma 45 to prove bisimulation equivalene.

Theorem 31 We will show that T(A) and R(A) are bisimilar. Define the bisimulation relation B by (s,v)B(s,[v]). It is easy to see that the initial state (s_0, v_0) corresponds o the state (s_0, [v_0]). Next, we show that for each transtition of T(A), there is a corrresponding transition of R(A), and vice versa. Suppose first that (s,v)B(s,[v]). Suppose on the other hand that (s,v)B(s,[v]) and that (s,v)$\xrightarrow{a}$(s',[v']). Then there exit $\omega \cong$ v and ω' $\cong$ v' such that (s', v") and (s,v) $\xrightarrow{a}$(s', v"). Hence v"$\cong \omega \cong$ v', so [v"] = [v']. By the definition of B, (s', v") B (s', [v"]), it follows that (s', v")B(s', [v']).

Safety Safety Properties are used to verify that something bad will never happen. Dit kan worden gespecificeerd met de volgende vergelijking

$$\Box(a_0 \implies ((\neg a_2 \wedge \neg a_3)\,\mathcal{U} a_1) \vee (\neg a_2 \wedge \neg a_3))$$

AG(p) M, s $\models AG(p) \Leftrightarrow \forall \pi \in \sqcap(M,s) \cdot \forall i \cdot M, \pi[i] \models p$

EG(p) M, s $\models EG(p) \Leftrightarrow \exists \pi \in \sqcap(M,s) \cdot \forall i \cdot M, \pi[i] \models p$

AF(p)

EF(p)

AX(p)

EX(p)

A(p $\cup q) M,s \models A(p \cup q) \Leftrightarrow \forall \pi \in \sqcap(M,s) \cdot \exists k \cdot M, \pi[k] \models q \wedge (\forall i \leq k \cdot M, \pi[i] \models p)$
$E(p \cup q)$

A(p $\Re q$)

E(p $\Re q$)

$\forall x (P(x) \rightarrow Q(x)) premise$
$\forall x P(x) premise$

$P(x_0) \forall x$e 2
$Q(x_0) \rightarrow$ e 3, 4

$\forall x Q(x) \forall x$i 3–5

{a,b} or †a,b
$\langle a,b \rangle or a,b$

f : $A \rightarrow B$

f $\circ g$
$x \mapsto f(x)$

$$f : \mathbb{R} \rightarrow \mathbb{R}$$
$$x \mapsto x^2$$

M, s $\models$ p $\Leftrightarrow$ p $\in$ L(s)
M, s $\models \not$f1 $\Leftrightarrow$ M, s $\not\models$ f1
M, s $\models$ f1 $\vee$ f2 $\Leftrightarrow$ M,s $\models$ f1 or M,s $\models$ f2
M, s $\models$ f1 $\wedge$ f2 $\Leftrightarrow$ M,s $\models$ f1 and M,s $\models$ f2
M, s $\models$ E $g_1 \Leftrightarrow$ there is a path π from s such that M, $\pi \models$ g1
M, s $\models$ p $\Leftrightarrow$ for every path π starting from s, M, $\pi \models$ g1
M, s $\models$ p $\Leftrightarrow$ s is the first state of M, s $\models$ f1
M, s $\models \not g_1 \Leftrightarrow$ M, $\pi \not\models$ g1
M, s $\models$ p $\Leftrightarrow$ M, $\pi \models$ g1 or M, π M, $\pi \models$ g2
M, s $\models$ p $\Leftrightarrow$ M, $\pi \models$ g1 and M, π M, $\pi \models$ g2
M, s $\models$ p $\Leftrightarrow$ M, $\pi^1 \models$ g1
M, s $\models$ p $\Leftrightarrow$ there exists a k $\geq$ 0, such that M, $\pi^k \models$ g1
M, s $\models$ p $\Leftrightarrow$ for all i $\geq$ 0,M,$\pi^i \models$ g1
M, s $\models$ g1 g2 $\Leftrightarrow$ there exists ak $\geq$ 0 such that M, $\pi^k \models$ g2
and for all 0 $\leq$ j < k, M,$\pi^j \models$ g1 M, s $\models$ p $\Leftrightarrow$ for all j $\geq$ 0, if for every i < j,M,π^i g1 then M,$\pi^j \models$ g2

Reachability Reachability properties are used to check whether a given state formula can be satisfied by some reachable state.

Liveliness Liveness properties are used to verify that something eventually will hold

Security

Performance About transition A transition is composed of a unique source location a unique target location a guard, i.e. an enabling condition (g := x c|g g, where <, , =, , > a label (that can be used for synchronization) a subset (potentially empty) of clocks to be reset

a clock valuation is a function v: X R^+ v[Y:=0] is the valuation obtained from v by resetting clocks from Y:

v[Y:=0]= $\begin{cases} 1, & 0 \text{ x} \in \text{Y}. \\ 0, & \text{otherwise}. \end{cases}$

v+d = flow of time (d units) (v +d)(x) = v(x)+d v $\implies$ c meansthat valuationv satisfies the constraint c

evaluation of a clock constraint (v $\implies$ g) v $\implies$ g x < k iff (x) < k |= x k iff (x) k |= g1 g2 iff |= g1 and |= g2

(s', v") and (s,v) $\xrightarrow{a}$(s', v").

Action transitions correspond to the execution of a transition from T. We write (s,v) $\xrightarrow{a}$ (s', v'), where a $\in\Sigma$, provided that there is a transition $\langle$ s,a, φ, λ, s' $\rangle$ such that v satisfies φ and v=[λ:=0].

a delay transition (s, v1) $\rightarrow$ δ(d) (s, $v_1 + d_1$)$forsome$d$_1 \geq 0$, and an action transition (s, v1 +d1) $\xrightarrow{a}$ (s', v'_1)$suchthat$v$_1$ + d_1 satisfies φ and v'$_1 = (v_1 + d_1)$[λ:=0].

We think of thevariables innV as the present sate variables and the variables in V'as next state variables. Each variable v i V has a corresponding next state variable in V', which we denote y v'. A valuation for the variables in V and V' can be vieuwed as designating an ordered pair of states or a transition, and we can represent setsof these valuations using formulas as above. We refer to a set of pairs of states as a transition relation. If R is a transition relation, then we write R(V,V') to denote a formula that represents it. In order to write specifications that describe properties of concurrent systems we need to define a set of atomic propositions AP. Atomic propositionswill typically have the form v=d where v $\in$ V and d $\in$ D. A proposition v =d will be truein a state s if s(v)=d. Whenv is a variable over the boolean domain-True,False, it is not necessarly to include both v = True and v = False in AP.We will write v to indicate that s(v)=True and $\neq$ v to indicate that s(v)=False. We now show how to derive

blz 16

We now show how to derive Kripke M=(S,S_0,R,L) from the first order formulas S_0 and R that represent the concurrent system. The set of states is hthe set of all variations for V the set of initial states S_0 is the set of all valuations s_0 for V that satisfy the formula S_0 let s and s' be the two states, then R(s,s') holds if R evaluates to True when each v $\in$ V is assigned the value s(v) and each v' $\in$ V' is assigned the value s'(v). The labeling function L: S $\rightarrow$ $frm{-}e^{AP}$ is defined so that L(s) is the subsetof all atomic propositions true in s. If v is a variable over the boolean domain, then v $\in$ L(s) indicates that s(v)=True, and v $\notin$ L(s) indicates that s(v)=False. L: S $o$frm-e^{AP} is a function that labels each state with the set of atomic propositions true in that state

Because we require that the transition relation of a kripke structuer us always total, we must extend the relation R if some state s has no successor. In this case, we modify R so that R(s,s) holds. To illustrate the notions defined in this section we consider a simple system with variables x and y that range over D=0,1. Thus, a valuation for the variables x and y is justa pair (d_1, d_2) $\in$ D x Dwhre d_1 is the value for x and d_2 is the value for y.

blz 33 Fairness A fairness constraint an be an arbitraty set of states, usually described by the formula of the logic. if fairness constraints are interpreted as sets of states, then a fair path must contain an element of each fairness constraint infinetely often. If fairness constrants are interpreted as CTL formula, then a path is fair if each constraint is true infnetely often along the path. The path quantifiers in the logic are then restricted fair paths. Formally, a fairkripke structure is a 4-tuple M = (S,R,L,F), where S, L and R are defined as before and F $\subseteq frm-e^S$ is a set of fairness constraints (often called Buchi acceptance conditions) Let $\pi = s_0, s_1$ be a path in M. Define inf(π) = s| s=s_i for infinitely many i.

We say that π is fair if and only if for every P $\in$ F, inf() $\cap$ P $\neq \emptyset$. The semantics of CTL* wth respect to a fair kripke structure is very similar to the semantics of CTL* with respect to ordinary kripke structure. We will write M,s $\models_F$ f to indicate that the state formula f is true in state s of the fair Kripke structure M. Similarly, we write M, $\pi \models_f$ g to indicate that the path formula g is true along path π in M. Only clauses 1, 5 and 6 in the origial semanticss change. 1. M, s $\models_f$ p $\Leftrightarrow$ there exists a fair path from s and p $\in$ L(s) 5. M, s $\models_f$ p $\Leftrightarrow$ there exists a fair path π starting from s such that $\pi \models_f$ g1 6. M, s $\models_f$ p $\Leftrightarrow$ for all fair paths π starting from s, $\pi \models_f$ g1

To illustrate the use of fairness, conider again the communication protocol for reliable channels. There is one fairness constraint for each channelthat expresses the reliability of that channel. A possible choice for the fairness constraint associated with channel i is the set of states that satisfy the formula $\neq$ send $\vee$ $receive_i$. Thus, a computation path is fair if and only if for every channel, infinitly often either a message is received. Other notions of fairness are dealt with in[116]. blz 36 ctl model checking

The model checkingproblem is easy to describe. given a kripke structure M =(S,R,L) that represents a finite-state concurrent system and a termporal logic formula f expressing some desired specification, find the set of all states n S that satisfy f: s $\in$ S | M, s $\models$ f
Let M = (S,R, L) be a kripke structur. Assume that we want to determine which states in S satisfy the CTL formula f. The algorithm will operate by labeling each state s with the set label(s) of subformulas of f which are true in s. Initially, label(s) is just L(s). The algorithm then goes through a series of stages.During the ith stage, subformulas with i-1 nested CTL operators are processed. When a subformula is processed, it is added to the labelig of each state in which it is true. Onze the algorithm terminates, we will have that M, s *models* f iff f $\in$ label(s) blz 40 Fairness constraints In this subsection we show how to extendthe CTL model checking algorithmto handle fairness constraints. Let M = (S,R,L,F) be a fair kripke structure. Let F = P1, ..., P_k be the setof fairness constraints. We will say that a strongly connnected component C of the graph of M is fair wth respect to F if and only if for each $P_i \in$ F, there is a state $t_i \in$ (C $\cap$ P_i). We first give an algorithmfor checking EG f_1 with respect to a fair structure. In order to establish the correctness of this algorith, we need a lemma that is analogous to Lemma 1.As before, let M' be obtained from M by deleting from S all of those states at which f_1 does not fairly hold. Thus, M'=(S',R',L',F') where §$^{'}$ = s $\in$ S | M,s $\models$ F f1, R' = R|$_S$'xS', L' = L|$_s$;, and F' = $P_i \cap$ S' | $P_i \in$ F.

Lemma 2 M,s $\models$ F EG f1 iff the followingtow conditions are satisfied: 1. s $\in$ S' 2. There exists a path S' that leads from s to somenode t in a nontrivial fair strongly connected component of thr graph (S',R')

In order to determine if M, s $\models$ f p for some p $\in$ AP, we check M,s $\models$ p $\wedge$ fair using the ordinary model-checking procedure. blz 68 Fairness in model checking with fixpoint

blz 69

blz 70

blz 71 Counterexamples and whitnesses

blz 72

blz 73

blz 74

blz 121 automata theory blz 141

blz 171 Equivalence and preorders between systems blz 172

blz 173

blz 174

blz 175

blz 176

blz 177 simulation relations blz 178

blz 179

blz 180

blz 232 INvariants blz 233

blz 234

blz 265

blz 266

blz 267

blz 268 parralel compositioon Before we consider a reachability problem, we show how real-time systems can be modoeled as parralel compositions of timed automata [3,5]. We assume an interleavingor asynchroneous semantics for this operation. Let A1 = ($\sum$, S1, $\S_0^1$, X_1, I_1, T_1) and A_2 = ($\sum_2$, $S1_2$, $\S_0^1$, X_2, I_2, T_2) be two timed automata. Assume that the two automata have disjoint sets of clocks, that is $X_1 \cap X_2 = \emptyset$. Then, the parralel composition of A_1, and A_2 is the timed automation:

$A_1 \parallel$ A2 = ($\Sigma \cup \Sigma_2$, S_1 x S2, $\S_0^1$ x $\S_0^2$, $X_1 \cup X_2$, I, T), where I(s_1,s_2)=$I_1(s_1) \wedge I_2(s_2)$ and the edge relation T is given by the following rules:

1 For a $\in \Sigma_1 \cap \Sigma_2$, if $\langle$ s1,a, φ, λ_1, s_1' $\rangle \in T_1$ and $\langle$ s2,a, φ, λ_2, s_2' $\rangle$ T_2 then T will contain the transition $\langle$ (s1,s2), a φ , $\lambda_1 \cup \lambda_2$, (s_1',s_2') $\rangle$ 2. For a $\in \Sigma_1$ - Σ_2, if $\langle$ s, a, φ, λ, s' $\in T_1$ and t $\in S_2$ then T will contain the transition $\langle$ (s,t),a, φ, λ, (s', t) $\rangle$ 3. For a $\in \Sigma_2$ - Σ_1, if $\langle$ s, a, φ, λ, s' $\in T_2$ and t $\in S_1$ then T will contain the transition $\langle$ (t,s),a, φ, λ, (t,s') $\rangle$

Thus the locations of the parralel composition are pairs of locations from the component automata, and the invariant of such a location is the conjunction of the invariants of the component locations. There will be a transition in the parralel compoition for ach pair of transitions from the individual timed automata with the same action The source location of the transition will be the composite location obtained from the source locations of the individual transitions. Te target location will be the compositelocation obtained from the target locations of the individual transitions. The guard will be the conjunction of the guards for the individual transitions, and the set of clocks that are reset will be the union of sets that are reset by the individual transitions. If the action of a transition is only an action of one of the two processes, then there will be a transition in the parralel composition for each location of the othertimed automation. The source and target locations of the original transition and the location fromthe other automation. All of the other components of the transition will remain the same.

blz 269 modelling with timed automata

blz 274 clock regions

blz 280 clock zones

blz 281

Timed automata Timed automata A timed automation[8,99] is a finite augmented with a finite set of real-valued clocks. We assume that transitions are instantaneous. However, time can elapse when the automation is in a state or location. When a transition occurs, some of the clocks ma be reset to zero. At any instant, the reading clock is equal to the time that has elapsed since the lat time the clock was reset. We assume that time passes at the same rate for all clocks. In order to prevent pathological behaviours, we only consider automata that are non-zeno, that is, only a finite number of transitions can happen within a finite amout of time.

A clock constraint, called a guard, is associated with each transition. The transition can be taken only if the current values of the clocks satisfy the clock constraint. A clock cnstraint is also associated with

each location of the automation. This constraint i called the invariant of the location. Time can elapse in the location only as long as the invariant of the location is true. An example of a timed automation is shown in Figure 17.1 The automation consists of two locations s0 and s1, two clocks x and y, and ä"transition from s0 to s1, and a "b"transition from s1 to s0. The automation starts in location s0. It can remain in that location as long as the clock y is less than or equal to 5. As soon as the value of y is greater than or equal to 3, the automation can make an ä"transition to location s1 and reset the clock y to 0. the automation can remain in location s1 as long as y is less than or equal to 10 and x is less than or equal to 8. When y is at least 4 and x is at least 6, it can make a "b"transition back to location s0 and reset x.

The remainder of this section contains a formal semantics for timed automata in terms of infinite state transition graphs[3,8]. We begin with a precise definition of clock constraints. Let X be a set of clock variables, ranging over the nonneative real numbers $\Re^+$. Define the set of clock constraints C(X) as follows: All inequalities of the form x $\prec$ c or c $\prec$ x are in C(X) where $\prec$ is either < or $\leq$ and c is a nonnegative rational number. If φ_1 ad φ_1 are in C(X), then $\varphi_1 \wedge \varphi$ is in C(X).

Note that if X contains k clocks; then each clock constraints is a convex subset of k-dimensional Eucledian space.Thus, if two points satisfy a clock constraint, then all of the points on the line sement connecting these points satisfy the clock constraint. A timed automation is a 6-tuple A = (Σ, S, S_0, X, I, T) such that Σ is a finite alphabet S is a finite set of locations S0 $\subseteq$ S is a set of starting locations X is a set of clocks I : S $\rightarrow$ C(X) is a mapping from locations to clock constraints called the location invariant. T $\subseteq$ S x Σ x C(X) x 2^x x S is a set of transitions. The 5-tuple $\langle$ s,a,φ, λ, s' $\rangle$ corresponds to a transition from location s to location s' labeled with a, a constraint φ that specifies when the transition is enabled, and a set of clocks $\lambda \subseteq$ X that are reset when the transition is executed.

We will require that time be allowed to progress to infinity, that is, at each location the upper bound imposed on the clocks be either infinity, or smaller than the maximum bound imposed by the invariant and by the transitions outgoing from the location. In other words, it is possible either to stay at a location forever, or the invariant will force the automation to leave the location, and at that point at least one transition will be enabled. For timed automata, these constraints can be imposed syntactically.

A model for a timed automation A is an infinite state transition graph τ(A) = (Σ, Q, Q^0, R). Each state in Q is a pair (s, v) where s $\in$ S is a location and v : X $\rightarrow R^+$ is a clock assignement, mapping each clock to a nonnegative real value. The set of initial states Q_0 is given by (s,v)| s $\in S_0 \wedge \forall$ x $\in$ X[v(x) =0]. In order to define the state transtion relation for τ(A), we musr first introduce some notation. For $\lambda \subseteq$ X, define v[λ := 0] to be the clock assignment that is the same as v for clocks in X - λ and maps the clocks in λ to 0. For d $\in \Re$, define v +d as the clock assignment that maps each clock x $\in$ X to v(x) +d. The clock assignment v -> d is defined in the same manner.
From the brief discussion in the introduction, we know that a timed automation has two basic types of transitions: Delay transitions correspond to the elapsing of time while staying at some location. We write (s, v) $\xrightarrow{d}$ (s, v+d), where d $\in R^+$, provided that for every 0 $\leq$ e $\leq$ d, the invariant l(s) holds for v +e.
Action transitions correspond to the execution of a transition from T. We write (s,v) $\xrightarrow{a}$ (s', v'), where a $\in \Sigma$, provided that there is a transition $\langle$ s,a, φ, λ, s' $\rangle$ such that v satisfies φ and v=[λ:=0].

The transition relation R of τ(A) is obtained by combining the delay and action transitions. We will write (s,v) R(s', v') or (s, v) $[]f(x)$ (s', v') if there exists sänd v"such that (s,v) $\xrightarrow{d}$ (s", v")$\xrightarrow{a}$ (s', v') for some d $\in \Re$. In this chapter we will describe an algorithm for solving the reachability problem for τ(A): Given a set of initial states Q_n, we show how to copute the set of all states q $\in$ Q that are reachable from Q_0 by transitions in R. This problem is nontrivial because τ (A) has an infinite number of states. In order to accomplish this goal, it is necessary to use a finite representation for the infinite state space of τ(A). Developing such representations is the main topic of te following sections.

blz 268 parralel composition

blz 274 clock regions

clock regions In the definition of timed automata, we allowed the clock constraints that serve as the invariants of locations and the guards of transitions to contain arbitrary rational constants. We can multiply the constants in each clock constraint by the least common multiple m of the denominators of all

the constants to integers. The value of a clock can still be an arbitrary nonnegative real number. Note that applying this transformation can change the clock assignments in the set of reachable states of T(A). Fortunately, this does not cause a mjor problem. Ther reachale states of the original auomation can be obtained from the locations of te transformed automation by applying the inverse transformation, that is, dividing each clock value by m.

Th largest constant in the tranformed in the transformed automation is the product of m and the largest constant in the original automation. Thus, the transformation at worst results in quadratic blowup in the length of the encodings of th lock constraints[3]. This increase in complexity is acceptable, since the transformation simplifies certain operations on clock constraints that will be needed later in the chapter. We will apply this tranformation uniformly to all of th clock constraints that appear in the timed automata the we study. Consequently, in the future we can assume without loss of generality that all constants in clock constraints that we encounter are integers.

In order to obtain a finite representation for the infinite state space of a timed automation, we define clock regions[7,8], which represents sets of clock assignments. If two states, which correspond to the same location of the timed automation A, agree on the integral parts of all clock constraint in the invariant of a location or in the guard of a transition is satisfied or not. The ordering of the fractional parts of the clock values determines which clock will change its integral part first. This is because clock constraints cn involve only integers, and all clocks increase at the same rate.

For example, let A be a timed automation with two clocks x1 and x2. Let s be a location in A with an outgoing transition e to some other location. Consider two states (s,v) and (s,v') in T(A) that correspond to location s. Suppose that v(x1) = 5.3, v(x2)=7.5, v'(x1)=5.5 and v'(x2) = 7.9. Assume that the guard φ associated with e is $x1 \geq 8 \wedge x2 \geq 10$. It is easy to see that if (s,v) eventually satisfies the guard, then so will (s, v').

The value of a clock cn get arbitrarily large; however, if the clock is never compared to a constant greater than c, then the value of the clock will have no effect on the computation of A once it exceeds c. Suppose, for instance, that the block x is never compared to a constant greater than 100 in the invariant associated wit a location or in the guard of a transition.

Then, based on the behaviour of A, it is impossible to distinguish between x having the value 101 and x having the value 1001. Alur,Courcoubetis, and Dill[7,8] show how to formalize this reasoning. For each clock $x \in X$, let cx, be the largest constant that x is compared with in the invariant of any location or in the guard of any transition. For $t \in \Re^+$, let ft(t) be the fractional part of t, and let [t] be the integral part of t. Thus, t = [t] + fr(t). We define an equivalence relation $\cong$ on the set of possible clock assignments as follows: Let v and v' be two clock assignments. Then $v \cong v'$ if and only if three conditions are satisfied:

For all $x \in X$ either $v(x) \geq cx$, and $v'(x) \geq gx$ or [v(x)] =[v'(x)]. For all x,y $\in X$ such that $v(x) \leq cx$ and $v(y) \leq cy$, $fr(v(x)) \leq fr(v(y))$ if and only if $fr(v'(x)) \leq fr(v'(y))$ For all $x \in X$ either $v(x) \leq cx$, fr(v(x)) =0 if and only if fr(v'(x)) =0. it is easy to see that $\cong$ does indeed define anequivalence relation. The equivalence classes of $\cong$ are called regions[7,8]. We will write [v] to denote the region which containsthe clock assignment v.Each region can be represented by specifying

1. for every clock $x \in X$, once clock constraint from the set x=c | c=0...., cx $\cup$c -1 < x < c | c=1,.....cx $\cup$ x > cx 2. for every pairof clocks x, $y \in X$ such that c-1 < x< cand d-1<y< d are clock constraints in the first condition, whether fr(x) is less than, equal to, or greater than fr(y).

Figure 17.7 which is taken from [8], shows the clockregions for a timed automationwith two clocks x and y where cx = 2 and cy =1. In this example, there are a total of 28 regions: 6 corner points, 14 open line segments and 8 open regions.

We will use this observation to show that $\cong$ has finite index and, consequently, that the number of regions is finite. Our proofof this fact is based on the proof given in [8].

Lemma 43 The number of equivalence classes that $\cong$ induces on C(X) is bounded by $|X|! \cdot 2^{|X|} \cdot \prod$ (2xc +2) proof An equivalence class [v] of $\cong$ can be described by a tripple of arrays i the following manner. For each block $x \in X$, the array α tells which of the intervals [],[] contains the value v(x). Thus,

the array α represents the cloc assignment v if and only if for each clock x $\in$ X, v(x)$\in$ α(x). The number of ways to choose α is $\prod$.

Let X_a be th set of clocks with nonzero fractional part. The array β: $x_a \rightarrow$ 1,....$|A_a|$ is a permutation of X_a, which gives the ordering of the fractional parts of the clocks in Xa with respect to $\leq$. Thusm the array β represents a clock assignment c if and if for each pair x,y $\in X_a$, if β(x) < β(y) then fr(v(x)) $\leq$ fr(v(y)). For a given α, the number of ways to choose β is bounded by $|X_\alpha|!$ which is bounded by |X|!.

The third component γ is a boolean array indeed by X_a that is used to specify which clocks in X_a have the same fractional part. For each clock c, γ(x) tells whether or not the fractional part of v(x) equals the fractional part of its predecessor in the array β. Thus the array γ represents a clock assignment v if and only if for each x X, γ(x) equals 0 exactly when there is a clock $\gamma \in X_alpha$ such that β(y) = β(x) +1 and fr(v(x)) equals fr(v(y)). The number of ways of choosing γ is bounded by the number of boolean arrays over X_α, which is bounded by $2^{|X|}$. Hence, α encoded the integral parts of he clock assignments, and β with γ encodes the ordering of their fractioal aprts. It is easy to see that the sets represented bytriples are equivalence of $\cong$ and that every equivalence class is represented by some triple. The bound given in the statement of the lemma is the product of the bounds associated with α, β, and γ. This completes the proof of the lemma.

The following properties of the equivalence relation $\cong$ are used in later in this chapter. Lemma 44 Let v1 and v2 be twoclock assignments1, let φ be a clock constraint, and let $\lambda \subseteq$ X be a set of clocks. 1. if v1 $\cong$ v2 and t is a nonnegative integer, then v1 + t $\cong$ v2 +t.

2. if v1 $\cong$ v2, then $\forall$ t1 $\in R^{|+|}{}_2 \in R^{|+|}$[v1 +t1 $\cong$ v2 + t2]

3. if v1 $\cong$ v2, then v1 satisfies φ if and only if v2 satisfies φ

4. If v1 $\cong$ v2, then v1[λ:=0] $\cong$ v2 [λ:=0]

Note that the first property may not hold if t is not an integer. For example, (2.8) $\cong$ (.1, .2), but (.2, .8) +.3 is not equivalent to (.1,.2) + .3. All of the properties except the second are straightforward to prove and will be left to the reader. A proof if the scond property is sketched below. The proof is not diificultm but it is somewhat tedious. It can be safely skipped when this chapter is read for the first time.

Proof Assume that v1 $\cong$ v2. We can assume that t1 > 0 because, otherwise, we can simply choose t2=0. Let Xx1,x2,.....,xn. We can threat v1 as a vector v1 = $\langle$ a1, ..., an $\rangle$, where a_i is the alue of clock x_i in v_1. Similarly, we let v2 = $\langle$ b1, ..., b_n $\rangle$. Since corresponding clocks have the same integer part, we can assume without loss of generality that $0 \leq a_i < 1$ and $0 \leq b_i < 1$. Also , assume that the clock values are sorrted into increasing order so that $a_1 \leq a_2 \leq ... \leq a_n$ and b1 $\leq b_2 \leq .... \leq b_n$.

case 1 Assume that the largest element in v1 + t1 is less than or equal to 1. This case is trivial. We can easilty choose t2 so that v + t1 $\cong$ v2 + t2

case 2 Assume that $0 \leq$ t1 < 1. Let the first element of v1 +t1. That is greater than or equal to 1 be a_k+t1. Chhoose $\in$ so that $\in$ =0 if a_k+t_1 =1 and so that 0< $\ni$<b$_k$-b_k-1 if $a_k+t_1 > 1$. Note that b_k-1 < b_k = b_k-1, then a_k=a_k-1 and $a+t_1$ is not the first elment of v1+t1 that is greater than o equal to 1. We will show that v1+t1 $\cong$ v2+(1+ $\in$ - b_k). In order to show this we will split the vectors into two parts. Let

L1= $\langle$ a_1 + t1, ..., a_k-1 + t1 $\rangle$, and L2= $\langle$ b_1 + (1 + $\in$ - b_k), ..., b_k-1 + (1+ $\in$ - b_k) $\rangle$ In each case it is straightforward to show that

1. all of the elements are positive 2. the elements are sorted in increaing order, and 3. all of the elements are less than 1 Because of these conditios it is easy to see that $L_1 \cong L_2$. Similarly, let

R_1= $\langle$ a_k + t1, ..., a_n + t1 $\rangle$, and R_2= $\langle$ b_k + (1 + $\in$ - b_k), ..., b_k-1 + (1+ $\in$ - b_k) $\rangle$

All of the elements in R_1 and R_2 are greater than or equal to 1. The fractional parts are given by R_1 - 1 and R_2 -1, respectively. For these vectors it is straightforward to show that

1. all of the elements are nonnegative 2. the elements are sorted in increasing order, and 3. all of the elements are less than 1

Moreover, an element in one vector is 0 if and only if the corresponding element in the order vector is 0. Thus R_1 -1 $\cong$ R_2 -1. It follows immediately that R_1 $\cong$ R_2. It is not difficult to see that the fractioal parts of R_2 precede the fractional parts of L_2. Let i $\geq$ k and j < k. Then b_i + (1 + $\in$ - b_k) -1 $\leq$ b_j + (1+ $\in$ - b_k). is equivlent to b_i - b_j $\leq$ 1, which is obviously true. The same relationship holds for the fractioal parts of R_1 and L_1, that is. a_i + t_1 -1 $\leq$ a_j + t_1.

hence , we obtain $R_1 \cdot L_1 \cong R_2 \cdot L_2$, where "·ïs concatenation of vectors. This shows that for all t_1 with 0 $\leq$ t1 < 1, there exits a t2 such that v_1 + vt_1 $\cong$ v2 + t_2 and completes the proof of

case 3 Finally, supppose that $t_1 \geq 1$. Let t1'= t_1 - [t_1], so that 0 $\leq$ t_1 < 1. Find t_2 such that v_1 + t_1 $\cong$ v2 + t2. Then: v1 + t1 + [t1] $\cong$ v2 + t2 + [t1].

If we choose t2 = [t1], then we have v1 + t1 $\cong$ v2 + t2 as required. This completes the proof of the second property.

The equivalence relation $\cong$ over clock assignments an be extended to an equvalence relation over the state space of T(A) by requiring that equivalent states have identical locations and equivalent clock assignments: (s,v) $\cong$ (s', v') if and only if s = s' and v $\cong$ v'. The key property of he equivalence reltion $\cong$ is given by the following lemma [5]:

Lemma 45 If v1 $\cong$ v2 and (s, v_1) $\xrightarrow{a}$ (s', v'). The transition $\langle$ s, a, φ, λ, s' $\rangle$ that takes state (s, v1) to state (s', v1') corresponds to two transiions of the timed automation.

Proof Assume that v1 $\cong$ v2 and (s, v1) $\xrightarrow{a}$ (s', v'1). The transition $\langle$ s, a, φ, λ, s' $\rangle$ that takes state (s, v1) to state (s', v'1) corresponds to two transitions of the timed automation:

a delay transition (s, v1) $\xrightarrow{d1}$ (s, v_1 + d_1) for some $d_1 \geq 0$, and an action transition (s, v1 +d1) $\xrightarrow{a}$ (s', v_1') such that v_1 + d_1 satisfies φ and v'_1 = (v_1v + d_1)[λ :=0].

Since v1 $\cong$ v2 and v1 satisfies I(s), v2 also satisfies I(s). Furthermore, there exists d2 $\geq$ 0 such that v1 + d1 $\cong$ v2 + d2. Since v1 + d1 satisfies I(s), v2 +d2 also satisfies I(s). Because the clock constraint I(s) is convex and is satisfied by both v2 and v2 + d2, I(s) must be satisfied by v2 + e for all e such that 0 $\leq$ e $\leq$ d2. Consequently, the delay transition (s, v2) $\xrightarrow{d2}$ (s, v2 +d2) is legal.

Since v1 + d1 $\cong$ v2 +d2, both v1+ d1 and v2+ d2 must satisfy the clock constraint for the guard φ. Thus, the transition $\langle$ s, a, φ, λ , s' $\rangle$ myst also be enabled in the state *s, v_2 + d_2 . Let v'_2 = (v_2 +d_2)[λ :=0]. Then v'_2 is equivalent to v'_1. Hence, there is an action transition (s, v_2 + d_2) $\xrightarrow{a}$ (s', v'_2). Combining the delay transition with the action transition, we get (s, v_2) $\xrightarrow{a}$ (s', v'_2) as required.

As a result of the lemme, we can conostruct a finite state transition raph that is bisimilaion equivalnt to the infinite state transition graph T(A). The finite state transition graph is called the region graph of A[7,8] and is denoted by R(A). A region is a pair (s, [v]). Since $\cong$ has a finite index, there are only a finite nuber of regions. The states of the region graph are the regions of A. The construction of R(A) will have the property that whenever (s,v) is a state of T(A), the region (s, [v]) where s_0 is an initial state of A and v_0 is a clock assignment that assigns 0 to every clock. The transition relation of R(A) is defined so that bisimulation equivalence is guaranteed. There will be a transition labeled with a from the region (s,[v]) to the region (s', [v']) if and only there are assignments ω $\in$ [v] and ω' $\in$ [v'] such that (s, ω) can make a transition to (s', ω')

We summarize the construction of the region graph R(A) below. Let A = (σ, S, S_0, X, I, T) be a timed automation. Then, The states of R(A) have the form (s, [v]) where s $\in$ S and [v] i a clock region The initial states have the form (s_0, [v]) where s_0 $\in$ s_0 and v(x)=0 for all x $\in$ X. R(A) has a transition ((s,[v]),a, (s',[v'])) if and only if (s, ω) $\xrightarrow{a}$ (s', ω') for some ω $\in$ [v] and some ω' $\in$ [v']. We can use Lemma 45 to prove bisimulation equivalene.

Theorem 31 We will show that T(A) and R(A) are bisimilar. Define the bisimulation relation B by (s,v)B(s,[v]). It is easy to see that the initial state (s_0, v_0) corresponds o the state (s_0, [v_0]). Next, we show that for each transtition of T(A), there is a corrresponding transition of R(A), and vice versa. Suppose first that (s,v)B(s,[v]). Suppose on the other hand that (s,v)B(s,[v]) and that (s,v)$\xrightarrow{a}$(s',[v']). Then there exit $\omega \cong$ v and ω' $\cong$ v' such that (s', v") and (s,v) $\xrightarrow{a}$(s', v"). Hence v"$\cong \omega \cong$ v', so [v"] = [v']. By the definition of B, (s', v") B (s', [v"]), it follows that (s', v")B(s', [v']).

blz 280 clock zones blz 281 Intersection

blz 281 Clock reset

blz 281 elapsing of time In principle, the three oeraions on clock zones described above can be used to construct a finite representationof the transition graph T(A) corresponding to a timed automation.

Real-time System = Discrete System + Clock Variables by Rajeev Alur

blz 2 actions The state of a system changes over time. We refer to the state changes of a system as actions. An action is a pair (σ,σ ') of states that consists of a source state σ and a target state σ '. Intuitively, if a system is in the source state σ, then the action (σ,σ ') takes the system into the target state σ'. We say that an action is enabled in its source state and disabled in all other states. Two actions (σ,σ '1) and (σ,σ '2) are consecutive if the second action is enabled in the target state of the

rst action|i.e., if (σ '1=σ '2). The action (σ,σ ') is a nul l action if (σ=σ ') .

blz 6 clocks and delays

Formally, the action (σ,σ ') is a system action if for all clock variables x, either σ '(x) = σ(x) or σ '(x) = 0; the action (σ,σ ') is a time action - or delay -if there is a nonnegative real δ the duration of the delay|such that σ ' = (σ,σ '). System actions have duration 0. Every null action is, by de

nition, both a system action and a delay of duration 0.

blz 7 Clock constraints Let (σ, δ) be a delay, let ϕ be a state predicate, and let ψ be an action predicate. The characteristic function of ϕ maps each nonnegative real e < δ to 1 if ϕ is true for σ + e, and otherwise to 0; the characteristic function of maps e to 1 iff ψ is enabled in σ + e. A state or action predicate varies

finitely over the delay (σ, δ) if its characteristic function has

nitely many discontinuities in the interval (0,δ). Abstractly, we restrict ourselves to state predicates and action predicates that vary

nitely over all delays.

blz 8 Clock-constrained systems A clock-constrained system S = (ϕ, ψ) is a pair that consists of a timed state predicate 0|the initial condition of S|and a timed action predicate ψ |the transition condition of S. The timed behavior σ is a behavior of the clock- constrained system S if (1) the initial condition of S is initially true for σ and (2) the transition condition of S is invariantly true for σ. Every clock-constrained system S de

nes, then, the set of its divergent behaviors, which is denoted by [[S]].

blz 9 Clock-constrained programs

blz 10 Delay predicates

blz 11 Real-time systems A real-time system S = (ϕ, ψ, χ) is a triple that consists of a clock-constrained system (ϕ, ψ) and a delay predicate χ the environment condition of S. The timed behavior σ is a behavior of the real-time system S if (1) σ is a behavior of the clock-constrained system that underlies S and (2) the environ- ment condition of S is invariantly true for σ. Every real-time system S defines, then, the set of its divergent behaviors, which is denoted by [[S]].

For example, the following real-time system S2 = (ϕ, ψ, χ) changes the value of m from 0 to 1 at time 3 at the earliest and at time 5 at the latest: ϕ = (m =0 $\wedge$ x =0) ψ = (m $\geq$ 3 $\wedge$ m1' =1) χ = (m =0 $\wedge$ x < 5) $\vee$ (m=1)

blz 12 Real-time executability

blz 13 Real-time programs

blz 15 Sequential real-time processes

blz 17 Concurrent real-time processes

blz 19 Embedded real-time processes

blz 30 Verification of Safety Properties

A safety property is simply a closed set of behaviors.

$$\frac{\begin{array}{r} x = 1 \\ y = 2 \end{array}}{x + y = 3}$$

World a machine samenvating

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 en het Montaingnes's principe. Het Von Neumand principe uitgelegd 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