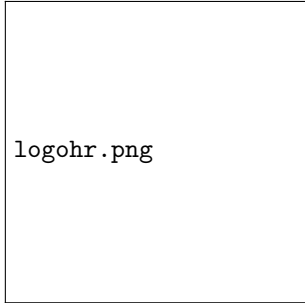


Verslag Tinlab Advanced Algorithms

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

19 mei 2023



logohr.png

Inhoudsopgave

1	Inleiding	2
2	Requirements	2
2.1	Requirements	2
2.2	Sluisdeuren	2
2.3	Stoplichten	3
2.4	Waterpomp	3
2.5	Boten	3
2.6	Specificaties	3
2.7	Notities die verwerkt moeten worden	3
2.8	Het vier variabelen model	4
2.8.1	Monitored variabelen	4
2.8.2	Controlled variabelen	4
2.8.3	Input variabelen	4
2.8.4	Output variabelen	4
2.9	Rampen	4
2.9.1	Ramp 1	4
2.9.2	Ramp 2	4
2.9.3	Ramp 3	4
2.9.4	Ramp 4	4
2.9.5	Ramp 5	4
2.9.6	Ramp 6	4
3	Research case: De digitale aanval op de Oekraïense krachtcentrale	4
3.1	Literaire analyse	5
3.1.1	Motief	5
3.1.2	Situatie Oekraïne	5
3.1.3	Situatie algemeen	5
3.1.4	Factoren	6
3.1.5	Oorzaak	6
3.1.6	Gebruikte materialen	6
3.1.7	Uitvoering van de aanval	6
3.1.8	Oplossingen	6
3.1.9	Aanbevelingen	6
3.2	Resultaten	6
3.2.1	De aanval	6
3.2.2	spearfishing	7
3.2.3	blackenergy	7
3.2.4	remote access capabilities	7
3.2.5	serial-to-ethernet communication devices	7
3.2.6	telephony denial of service attacks	7
3.3	oplossingen	7
3.4	Discussie	7
3.5	Verder lezen	7

4	Modellen	9
4.1	De Kripke structuur	9
4.2	Soorten modellen	9
4.3	Tijd	9
4.4	Guards en invarianten	9
4.5	Deadlock	9
4.6	Zeno gedrag	9
5	Logica	9
5.1	Propositie logica	9
5.2	Predicaten logica	9
5.3	Kwantoren	9
5.4	Dualiteiten	9
6	Computation tree logic	9
6.1	De computation tree	9
6.2	Operator: AG	9
6.3	Operator: EG	9
6.4	Operator: EG	9
6.5	Operator: AF	9
6.6	Operator: EF	9
6.7	Operator: AX	10
6.8	Operator: EX	10
6.9	Operator: $p \text{ U } q$	10
6.10	Operator: $p \text{ R } q$	10
6.11	Operator: EX	10
6.12	Operator: $p \text{ U } q$	10
6.13	Operator: $p \text{ R } q$	10
6.14	Operator: AF	10
6.15	Operator: EF	10
6.16	Operator: AX	10
6.17	Operator: EX	10
6.18	Operator: $p \text{ U } q$	10
6.19	Operator: $p \text{ R } q$	11
6.20	Fairness	11
6.21	Liveness	11

1 Inleiding

In deze case study wordt

2 Requirements

2.1 Requirements

Directe requirements van opdrachtgever:

Na grondige analyse van het Nederlandse sluizenpark is gebleken dat renovatie van een groot aantal sluizen noodzakelijk is. Een eerste verkenning heeft ons geleerd dat het gecombineerd renoveren en automatiseren van het Nederlandsesluizenpark een aanzienlijke verbetering kan opleveren t.a.v.:

- veiligheid
- efficiëntie
- capaciteit
- onderhoudskosten
- duurzaamheid

In het kader van het onlangs afgesloten klimaatakkoord heeft de Nederlandse overheid daarom besloten over te gaan tot een ingrijpende renovatie van diverse sluizen die ons land rijk is. Op het ministerie van infrastructuur en waterstaat is helaas onvoldoende kennis van ict en systemen aanwezig om een 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.

2.2 Sluisdeuren

De sluisdeuren.

2.3 Stoplichten

De stoplichten

2.4 Waterpomp

De waterpomp

2.5 Boten

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

Overige eisen op basis van eigen inbreng:

2.6 Specificaties

Vanuit deze requiremenst kunnen verdere specificaties opgesteld worden.

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

2.7 Notities die verwerkt moeten worden

moet de initial 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, zou 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 kunnen worden. ook bij wachtrij.

stoplichten 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

2.8 Het vier variabelen model

2.8.1 Monitored variabelen

2.8.2 Controlled variabelen

2.8.3 Input variabelen

2.8.4 Output variabelen

2.9 Rampen

2.9.1 Ramp 1

Beschrijving

Datum en plaats

Oorzaak

2.9.2 Ramp 2

Beschrijving

Datum en plaats

Oorzaak

2.9.3 Ramp 3

Beschrijving

Datum en plaats

Oorzaak

2.9.4 Ramp 4

2.9.5 Ramp 5

2.9.6 Ramp 6

3 Research case: De digitale aanval op de Oekraïense krachtcentrale

Dit verslag geeft inzicht in een analyse van de Ukraine cyber aanval, inclusief hoe de actoren zich zelf toegang gaven tot het controle systeem, welke methoden de actoren hebben gebruikt voor reconnaissance en vastleggen van het systeem, een gedetailleerde omschrijving 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 moeilijker maken. Daarnaast wordt er een

gedetailleerde omschrijving gegeven aan de beveiliging van de SCADA control systemen gebaseerd op best practices, inclusief het control network ontwerp, technieken voor whitelisting, monitoring en loggen, en opleiding van personeel.

https://na.eventscloud.com/file_uploads/aed4bc20e84d2839b83c18bcb7e2876 Owens1.pdf <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> <https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf> <https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108> <https://www.mandiant.com/resources/blog/ukraine-and-sandworm-team> https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energynfrastructures20172.pdf <https://ris.utwente.nl/ws/files/6028066/3-s20-B9780128015957000227.pdf> <https://repositorio-aberto.up.pt/bitstream/10216/119066/2/315683.pdf> <https://www.diva-portal.org/smash/get/diva2:1046339/FULLTEXT01.pdf> <https://www.vice.com/en/article/zmeyg8/ukraine-power-grid-malware-crashoverride-industroyer>

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

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

3.1 Literaire analyse

3.1.1 Motief

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

3.1.2 Situatie Oekraïne

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

3.1.3 Situatie algemeen

<https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/> https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energynfrastructures20172.pdf <https://www.cybersecurityintelligence.com/blog/attack-on-ukraines-power-grid-targeted-transmission-stations-4530.html>

3.1.4 Factoren

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

3.1.5 Oorzaak

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

3.1.6 Gebruikte materialen

https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack <https://www.cisa.gov/news-events/alerts/2017/06/12/crashoverride-malware> <https://rhebo.com/en/service/glossar/industroyer-25114/>

3.1.7 Uitvoering van de aanval

https://na.eventscloud.com/file_uploads/aed4bc20e84d2839b83c18bcba7e2876_Owens1.pdf <https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf>

3.1.8 Oplossingen

https://na.eventscloud.com/file_uploads/aed4bc20e84d2839b83c18bcba7e2876_Owens1.pdf <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>

3.1.9 Aanbevelingen

3.2 Resultaten

3.2.1 De aanval

1. An initial email spear phishing attack lures recipients into opening an attached Microsoft® document with a macro that installs Black Energy 3 (BE3) onto corporate workstations. 2. BE3 and other tools perform reconnaissance and enumeration of the network and provide an initial backdoor for the hackers into the corporate network. 3. As a result of network reconnaissance, the malicious actors discover and access the oblenenerg's 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

<https://dreamlab.net/en/blog/post/fuzzing-ics-protocols/><https://www.blackhat.com/docs/us-17/wednesday/us-17-Staggs-Adventures-In-Attacking-Wind-Farm-Control-Networks.pdf><https://blog.checkpoint.com/research/crashoverride/><https://www.blackhat.com/us-17/briefings/schedule/industroycrashoverride-zero-things-cool-about-a-threat-group-targeting-the-power-grid-6159><https://search.abb.com/library/Download.aspx?DocumentID=9AKK107045A1003&LanguageCode=en&DocumentPartId=&Action=Launch><https://iiot-world.com/ics-security/cybersecurity/five-cybersecurity-experts-about-crashoverride-malware-main-dangers-and-lessons-for-iiot/><https://www.csoononline.com/article/3200828/crash-override-malware-that-took-down-a-power-grid-may-have-been-a-test-run.html><https://www.paloaltonetworks.com/blog/2017/06/crashoverrideindustroyer-protections-palo-alto-networks-customers/><https://www.webopedia.com/definitions/crashoverride-industroyer-malware/><https://www.cyber.nj.gov/threat-center/threat-profiles/ics-malware-variants/crashoverride><https://www.nixu.com/blog/crashoverride-threat-electricity-networks><https://www.virusbulletin.com/virusbulletin/2019/03/vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/>https://en.wikipedia.org/wiki/CrashOverride_Network<https://en.wikipedia.org/wiki/Industroyer><https://www.dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/><https://www.wallix.com/blog/ics-security-russian-hacking><https://www.nixu.com/fi/node/53><https://control.com/forums/threads/comparison-between-iec60870-5-103-and-modbus-rtu.20317/>

4 Modellen

4.1 De Kripke structuur

4.2 Soorten modellen

4.3 Tijd

4.4 Guards en invarianten

4.5 Deadlock

4.6 Zeno gedrag

5 Logica

5.1 Propositielogica

5.2 Predicatenlogica

5.3 Kwantoren

5.4 Dualiteiten

6 Computation tree logic

6.1 De computation tree

6.2 Operator: AG

6.3 Operator: EG

Voor alle paden geldt dat waterlevel lager is dan niveau van de kant. Voor alle paden geldt dat een omp werkzaam is als alle sluisdeuren dicht zijn. Voor alle paden geldt dat het aantal schepen in de sluis maximaal 2 is. Voor alle paden geldt dat een schip nooit langer dan 30 seconden in een sluiskolk zit zonder dat het waterpeil is aangepast.

6.4 Operator: EG

Er bestaat op elk pad een

6.5 Operator: AF

6.6 Operator: EF

r is soms een mogelijkheid dat twee schepen in de sluis een verschillende uitvaar-richting hebben.

6.7 Operator: AX

6.8 Operator: EX

6.9 Operator: $p \cup q$

6.10 Operator: $p \mathbf{R} q$

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

6.11 Operator: EX

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

6.12 Operator: $p \cup q$

Vanaf aankomst tot uitvaren is de clocktijd lager dan 30 tijdseenheden

6.13 Operator: $p \mathbf{R} q$

Vanaf invaren tot en met uitvaren van een schip en geldig is x lager dan 15 tijdseenheden vanaf aanvaren staat een schip maximaal 40 tijdseenheden in de wachtrij.

6.14 Operator: AF

Er is altijd meerdere

6.15 Operator: EF

Er is soms een mogelijkheid dat twee schepen in de sluis een verschillende uitvaar-richting hebben.

6.16 Operator: AX

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

6.17 Operator: EX

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

6.18 Operator: $p \cup q$

Vanaf aankomst tot uitvaren is de clocktijd lager dan 30 tijdseenheden

6.19 Operator: $p \mathbf{R} q$

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

6.20 Fairness

6.21 Liveness