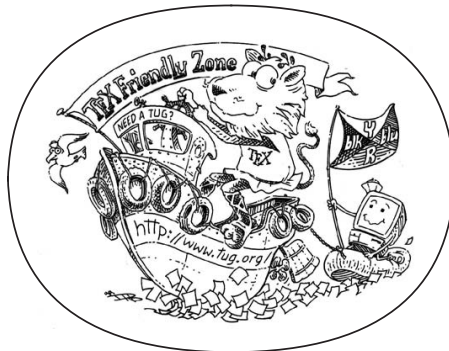


ANALYSING SOUP

BAS BRUNINK



Een weg naar veiligere software

Februari 2022 – version 0.1

SAMENVATING

Short summary of the contents... a great guide by Kent Beck how to write good abstracts can be found here:

<https://plg.uwaterloo.ca/~migod/research/beck00PSLA.html>

INHOUDSOPGAVE

1	INLEIDING	1
1.1	leeswijzer	1
I	OPDRACHT	3
2	EAGLESCIENCE	5
2.1	missie	5
2.2	visie	5
2.3	strategie	5
2.4	Relevante en actuele ontwikkelingen binnen Eaglescience	6
3	OPDRACHT	7
3.1	Opdracht vanuit Eaglescience	7
3.1.1	Eisen aan de opdracht	7
3.1.2	Deliverables	8
3.2	Opdracht fasen	8
3.3	plan van aanpak	8
3.4	Fase 1: Onderzoek	8
3.5	Fase 2: Oplevering SOUP analyse module	8
3.6	Opdracht fasen	8
II	ONDERZOEK	9
4	MATH TEST CHAPTER	11
4.1	Some Formulas	11
4.2	Various Mathematical Examples	12
5	CHAPTER TITLE	13
5.1	Section Title	13
5.1.1	Subsection Title	13
5.1.2	Subsection Title	13
5.2	Section Title	13
III	ONTWIKKELING VAN SOUP MODULE	15
IV	APPENDIX	17
A	APPENDIX TEST	19
A.1	Appendix Section Test	19
A.2	Another Appendix Section Test	19
	BIBLIOGRAFIE	21

LIJST VAN FIGUREN

LIJST VAN TABELLEN

Tabel 1	Autem usu id	20
---------	------------------------	----

LISTINGS

Listing 1	A floating example (listings manual)	20
-----------	--	--------------------

ACRONIEMEN

API Application Programming Interface

SOUP Software of unkown pedigree

UML Unified Modeling Language

INLEIDING

Het document dat voor u ligt is een resultaat van een onderzoek en product oplevering als afstudeeropdracht door Bas Brunink voor het bedrijf Eaglescience. Het zal het process beschrijven die ik gelopen heb om een module te schrijven die automatisch een SOUP analyse doet op zowel bestaande als nieuwe projecten.

1.1 LEESWIJZER

Deze scriptie neemt de lezer mee door het verloop van het project van idee tot implementatie. Met als einde een resultaat beschrijven en een prognose in de verbetering gezien de verwachting is dat er niet direct een significante verbetering te zien is.

Deel I

OPDRACHT

Het hier beschreven onderzoek en daarbij gehorende applicatie is geschreven in opdracht van Eaglescience wat gevestigd is in Amsterdam Sloterdijk. Eaglescience ontwikkeld complexe software op projectbasis voor diverse klanten vaak met een wetenschappelijke inslag. Het bedrijf telt +/- 20 medewerkers waarvan 75% ontwikkelaar/designer zijn en de resterende 25% een support rol bekleden (project managers finance manager, Quality manager) Aan het hoofd van Eaglescience staat een CEO, Marc Grootjen, CTO Bas Breier, CFO Wender van Mansvelt. Naast het ontwikkelen van nieuwe software biedt Eaglescience ook de mogelijkheid om zorg te dragen voor de eventuele hosting van het opgeleverde product. Hiermee kan Eaglescience nog beter garanderen dat de geboden kwaliteit in de software gewaarborgd blijft tijdens de levensduur van de software.

2.1 MISSIE

De missie van Eaglescience is het bedienen van onze partners door een ontwerp, ontwikkeling en service te bieden op het gebied van op maat gemaakte IT oplossingen . Om dit te kunnen bewerkstelligen heeft Eaglescience goed opgeleide IT professionals in dienst die zichzelf continue ontwikkelen op de “cutting edge” van IT technologie. De hoofd competenties van de medewerkers zijn: innovatief, intelligent, klant geïnteresseerd, flexibel en ambitieus.

2.2 VISIE

Eaglescience streeft er als innovatief IT bedrijf naar om software te ontwikkelen als een Business-to-Business dienst. Met onze technische vaardigheden bouwen we veilige en hoogwaardige software die bijdraagt aan een betere wereld. Omdat we agile werken, leveren we precies wat nodig is, niets meer en niets minder. Wij helpen onze klanten zoeken naar een langdurige betrokkenheid en samenwerking op basis van zowel vertrouwen als wederzijds respect. Omdat elke vraag uniek is, ontwikkeld Eaglescience op maat gemaakte en innovatieve software. We zijn van plan deel uit te maken van het hele proces van het formuleren van een idee tot het lanceren van het product en het waarborgen van de productie levenscyclus. Onze belangrijkste succesfactor zijn de mensen, die zich continu ontwikkelen door met de nieuwste technieken te werken op diverse projecten. Wij streven naar een optimale balans tussen werk en privé. Dit geeft onze medewerkers veel vrijheid, maar vereist zelfdiscipline en verantwoordelijkheid.

2.3 STRATEGIE

Eaglescience levert de visie via vier strategische thema's:

strategische thema's

- Maatschappelijke verantwoordelijkheid
- Persoonlijke groei
- Tevredenheid

We streven ernaar om veilige en hoogwaardige software diensten te leveren die waarde toevoegen aan onze samenleving. We streven naar een bedrijfscultuur waarin alle collega's hun talenten kunnen laten groeien. We hebben een ongecompliceerd werkhoud: we richten ons op resultaten van hoge kwaliteit, maar met een gezonde balans tussen werk en privé en voldoende tijd voor leuke en sociale evenementen. Eaglescience verwacht van alle medewerkers dat zij hun handelen baseren op vier kwaliteits principes:

- Meld situaties die niet voldoen aan onze interne procedures

- Evalueer risico's wanneer grote veranderingen worden verwacht
- Help en daag elkaar uit
- Kennis behouden over compliancy en kwaliteitsmanagement

2.4 RELEVANTE EN ACTUELE ONTWIKKELINGEN BINNEN EAGLESCIENCE

Eaglescience is aan het groeien, zowel in het aantal projecten waar aan gewerkt wordt als het aantal medewerkers. Daarnaast worden de diensten die Eaglescience aanbied ook uitgebreid. Waarbij het hosten van de ontwikkelde applicaties steeds meer wordt aangeboden. Door deze inzet ligt de verantwoordelijkheid niet alleen bij het leveren van een veilige en hoogwaardige software maar het leveren van service waarbij de applicaties in een veilige omgeving worden aangeboden. Mede door de groei van het bedrijf maar zeker ook de diensten die aangeboden wordt is het zeer relevant om taken die geautomatiseerd kunnen worden te automatiseren.

OPDRACHT

Tegenwoordig zijn software-bibliotheken niet meer weg te denken in het software ontwikkelproces van nu. Bibliotheken geven ontwikkelaars de mogelijkheid code her te gebruiken in meerdere projecten om zo efficiënter te kunnen ontwikkelen. Dit helpt weer mee om een snelle Time-To-Market te behalen. Bibliotheken kunnen door bedrijven zelf geschreven worden, in het geval van EagleScience is dit ArchES, of worden overgenomen van andere bedrijven/ instellingen. Zelfs ArchES is afhankelijk van een aantal bibliotheken die niet ontwikkeld zijn door EagleScience. Dus ontcom je er tegenwoordig niet aan om bibliotheken te gebruiken waarvan je de afkomst niet geheel kan herleiden. Deze bibliotheken wordt Software of Unknown Provenance/Pedigree (SOUP) genoemd. Door het gebruik van SOUP bibliotheken wordt er een aannemelijk risico gevormd op het gebied van veiligheid. Om deze risico's te verminderen kan er een SOUP analyse gedaan worden om op die manier inzicht te krijgen in de voor de gebruikte bibliotheken bekende kwetsbaarheden mat daarbij de mogelijke risico's en eventueel fixes om het risico te beperken of op te lossen. Binnen EagleScience wordt het belang gezien om deze analyse te doen en is daarom op zoek naar een efficiënte en mogelijk geautomatiseerde manier voor het uitvoeren van een dergelijke analyse om zo de veiligheid van de ontwikkelde applicaties te waarborgen zonder afbreuk te doen aan kwaliteit.

3.1 OPDRACHT VANUIT EAGLESCIENCE

Vanuit de CTO is de wens ontstaan om een gestructureerde methode te ontwikkelen waarbij er automatisch periodiek een SOUP analyse gedaan wordt op bestaande en nieuwe projecten. Het uiteindelijke resultaat moet zijn dat er een module wordt toegevoegd aan de reeds bestaande portal van EagleScience waarbij project verantwoordelijken inzicht kunnen verkrijgen in de kwetsbaarheden die in een project aanwezig kunnen zijn door het gebruik van externe bibliotheken.

3.1.1 *Eisen aan de opdracht*

Vanuit EagleScience zijn er een aantal eisen gesteld waaraan het eindproduct moet voldoen:

- De module dient eenvoudig te worden gebruikt in de huidige CI/CD pipeline voor bestaande en nieuwe projecten
- De module dient gebruik te maken van de bestaande ++huidige++ projectstructuur van het portal
- De module dient ondersteuning te bieden voor meerdere omgevingen(OTAP)
- De module dient met een instelbaar interval de analyse uit te voeren
- De module op project en omgeving niveau te rapporteren over bekende kwetsbaarheden
- De module dient kwetsbaarheden op minimaal drie niveau's in te schalen (kritisch, gemiddeld en laag)
- De module dient ondersteuning te bieden voor het instellen van quality gates ten aanzien van ieder niveau, per project, per omgeving
- De module voldoet aan de geldende kwaliteitsnormen binnen EagleScience, minimaal meetbaar door:
 - test coverage > 70%
 - onderdeel van de bestaande CI/CD voor het EagleScience Portal

- De module wordt ontwikkeld in Angular en Play(scala), overeenkomstig bestaande portal modules
- Geschreven code is gerevied door een Eaglescience ontwikkelaar
- In de module zijn gescheiden componenten: Frontend, Backend, API onafhankelijk en goed gedocumenteerd.
- Voor de API documentatie wordt gebruik gemaakt van swagger.

3.1.2 Deliverables

Vanuit de CTO zijn er naast de functionele eisen ook eisen gesteld aan de oplevering:

- Geïntegreerde en aantoonbaar werkende module
- De code van de module in Eaglescience GitLab
- API documentatie (middels swagger)
- Een handleiding hoe de module gebruikt dient te worden
- Eventuele aanvullende deliverables vanuit de HvA

3.2 OPDRACHT FASEN

3.3 PLAN VAN AANPAK

Content

3.4 FASE 1: ONDERZOEK

Content

3.5 FASE 2: OPLEVERING SOUP ANALYSE MODULE

Content

3.6 OPDRACHT FASEN

Content

Deel II

ONDERZOEK

Aliquam lectus. Vivamus leo. Quisque ornare tellus ullamcorper nulla. Mauris porttitor pharetra tortor. Sed fringilla justo sed mauris. Mauris tellus. Sed non leo. Nullam elementum, magna in cursus sodales, augue est scelerisque sapien, venenatis congue nulla arcu et pede. Ut suscipit enim vel sapien. Donec congue. Maecenas urna mi, suscipit in, placerat ut, vestibulum ut, massa. Fusce ultrices nulla et nisl.

4.1 SOME FORMULAS

Due to the statistical nature of ionisation energy loss, large fluctuations can occur in the amount of energy deposited by a particle traversing an absorber element¹. Continuous processes such as multiple scattering and energy loss play a relevant role in the longitudinal and lateral development of electromagnetic and hadronic showers, and in the case of sampling calorimeters the measured resolution can be significantly affected by such fluctuations in their active layers. The description of ionisation fluctuations is characterised by the significance parameter κ , which is proportional to the ratio of mean energy loss to the maximum allowed energy transfer in a single collision with an atomic electron:

$$\kappa = \frac{\xi}{E_{\max}} \quad (1)$$

E_{\max} is the maximum transferable energy in a single collision with an atomic electron.

$$E_{\max} = \frac{2m_e\beta^2\gamma^2}{1 + 2\gamma m_e/m_x + (m_e/m_x)^2} ,$$

where $\gamma = E/m_x$, E is energy and m_x the mass of the incident particle, $\beta^2 = 1 - 1/\gamma^2$ and m_e is the electron mass. ξ comes from the Rutherford scattering cross section and is defined as:

$$\xi = \frac{2\pi z^2 e^4 N_{\text{Av}} Z \rho \delta x}{m_e \beta^2 c^2 A} = 153.4 \frac{z^2 Z}{\beta^2 A} \rho \delta x \quad \text{keV},$$

where

- z charge of the incident particle
- N_{Av} Avogadro's number
- Z atomic number of the material
- A atomic weight of the material
- ρ density
- δx thickness of the material

κ measures the contribution of the collisions with energy transfer close to E_{\max} . For a given absorber, κ tends towards large values if δx is large and/or if β is small. Likewise, κ tends towards zero if δx is small and/or if β approaches 1.

The value of κ distinguishes two regimes which occur in the description of ionisation fluctuations:

1. A large number of collisions involving the loss of all or most of the incident particle energy during the traversal of an absorber.

As the total energy transfer is composed of a multitude of small energy losses, we can apply the central limit theorem and describe the fluctuations by a Gaussian distribution. This case is applicable to non-relativistic particles and is described by the inequality $\kappa > 10$ (i.e., when

You might get unexpected results using math in chapter or section heads. Consider the pdfspacing option.

¹ Examples taken from Walter Schmidt's great gallery:
<http://home.vrweb.de/~was/mathfonts.html>

the mean energy loss in the absorber is greater than the maximum energy transfer in a single collision).

2. Particles traversing thin counters and incident electrons under any conditions.

The relevant inequalities and distributions are $0.01 < \kappa < 10$, Vavilov distribution, and $\kappa < 0.01$, Landau distribution.

4.2 VARIOUS MATHEMATICAL EXAMPLES

If $n > 2$, the identity

$$t[u_1, \dots, u_n] = t[t[u_1, \dots, u_{n-1}], t[u_n, \dots, u_n]]$$

defines $t[u_1, \dots, u_n]$ recursively, and it can be shown that the alternative definition

$$t[u_1, \dots, u_n] = t[t[u_1, u_2], \dots, t[u_{n-1}, u_n]]$$

gives the same result.

CHAPTER TITLE

5.1 SECTION TITLE

Content

5.1.1 *Subsection Title*

Content

5.1.2 *Subsection Title*

Content

5.2 SECTION TITLE

Content

Deel III

ONTWIKKELING VAN SOUP MODULE

Deel IV

APPENDIX

You can put some informational part preamble text here. Illo principalmente su nos. Non message *occidental* angloromantic da. Debitas effortio simplificate sia se, auxiliar summarios da que, se avantiate publicationes via. Pan in terra summarios, capital interlingua se que. Al via multo esser specimen, campo responder que da. Le usate medical addresses pro, europa origine sanctificate nos se.

APPENDIX TEST

Aliquam lectus. Vivamus leo. Quisque ornare tellus ullamcorper nulla. Mauris porttitor pharetra tortor. Sed fringilla justo sed mauris. Mauris tellus. Sed non leo. Nullam elementum, magna in cursus sodales, augue est scelerisque sapien, venenatis congue nulla arcu et pede. Ut suscipit enim vel sapien. Donec congue. Maecenas urna mi, suscipit in, placerat ut, vestibulum ut, massa. Fusce ultrices nulla et nisl.

Etiam ac leo a risus tristique nonummy. Donec dignissim tincidunt nulla. Vestibulum rhoncus molestie odio. Sed lobortis, justo et pretium lobortis, mauris turpis condimentum augue, nec ultricies nibh arcu pretium enim. Nunc purus neque, placerat id, imperdiet sed, pellentesque nec, nisl. Vestibulum imperdiet neque non sem accumsan laoreet. In hac habitasse platea dictumst. Etiam condimentum facilisis libero. Suspendisse in elit quis nisl aliquam dapibus. Pellentesque auctor sapien. Sed egestas sapien nec lectus. Pellentesque vel dui vel neque bibendum viverra. Aliquam porttitor nisl nec pede. Proin mattis libero vel turpis. Donec rutrum mauris et libero. Proin euismod porta felis. Nam lobortis, metus quis elementum commodo, nunc lectus elementum mauris, eget vulputate ligula tellus eu neque. Vivamus eu dolor.

A.1 APPENDIX SECTION TEST

Nulla in ipsum. Praesent eros nulla, congue vitae, euismod ut, commodo a, wisi. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Aenean nonummy magna non leo. Sed felis erat, ullamcorper in, dictum non, ultricies ut, lectus. Proin vel arcu a odio lobortis euismod. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Proin ut est. Aliquam odio. Pellentesque massa turpis, cursus eu, euismod nec, tempor congue, nulla. Duis viverra gravida mauris. Cras tincidunt. Curabitur eros ligula, varius ut, pulvinar in, cursus faucibus, augue.

More dummy text

Nulla mattis luctus nulla. Duis commodo velit at leo. Aliquam vulputate magna et leo. Nam vestibulum ullamcorper leo. Vestibulum condimentum rutrum mauris. Donec id mauris. Morbi molestie justo et pede. Vivamus eget turpis sed nisl cursus tempor. Curabitur mollis sapien condimentum nunc. In wisi nisl, malesuada at, dignissim sit amet, lobortis in, odio. Aenean consequat arcu a ante. Pellentesque porta elit sit amet orci. Etiam at turpis nec elit ultricies imperdiet. Nulla facilisi. In hac habitasse platea dictumst. Suspendisse viverra aliquam risus. Nullam pede justo, molestie nonummy, scelerisque eu, facilisis vel, arcu.

A.2 ANOTHER APPENDIX SECTION TEST

Curabitur tellus magna, porttitor a, commodo a, commodo in, tortor. Donec interdum. Praesent scelerisque. Maecenas posuere sodales odio. Vivamus metus lacus, varius quis, imperdiet quis, rhoncus a, turpis. Etiam ligula arcu, elementum a, venenatis quis, sollicitudin sed, metus. Donec nunc pede, tincidunt in, venenatis vitae, faucibus vel, nibh. Pellentesque wisi. Nullam malesuada. Morbi ut tellus ut pede tincidunt porta. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam congue neque id dolor.

Donec et nisl at wisi luctus bibendum. Nam interdum tellus ac libero. Sed sem justo, laoreet vitae, fringilla at, adipiscing ut, nibh. Maecenas non sem quis tortor eleifend fermentum. Etiam id tortor ac mauris porta vulputate. Integer porta neque vitae massa. Maecenas tempus libero a libero posuere dictum. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aenean quis mauris sed elit commodo placerat. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Vivamus rhoncus tincidunt libero. Etiam elementum pretium justo. Vivamus est. Morbi a tellus eget pede tristique commodo. Nulla nisl. Vestibulum sed nisl eu sapien cursus rutrum.

There is also a useless Pascal listing below: [Listing 1](#).

LABITUR BONORUM PRI NO	QUE VISTA	HUMAN
fastidii ea ius	germano	demonstratea
suscipit instructor	titulo	personas
quaestio philosophia	facto	demonstrated

Tabel 1: Autem usu id.

Listing 1: A floating example (listings manual)

```

1 for i:=maxint downto 0 do
  begin
    { do nothing }
  end;

```

DECLARATION

Put your declaration here.

Amsterdam , Februari 2022

Bas Brunink

COLOPHON

This document was typeset using the typographical look-and-feel `classicthesis` developed by André Miede. The style was inspired by Robert Bringhurst's seminal book on typography "*The Elements of Typographic Style*". `classicthesis` is available for both \LaTeX and \LyX :

<https://bitbucket.org/amiede/classicthesis/>

Happy users of `classicthesis` usually send a real postcard to the author, a collection of postcards received so far is featured here:

<http://postcards.miede.de/>