UNIVERSITAT POLITÈCNICA DE CATALUNYA (UPC)
FACULTAT D'INFORMÀTICA DE BARCELONA (FIB)

Resiliència a nivell d'aplicació

Grau en Enginyeria Informàtica – Enginyeria del Software

Autor: Mihai Lucut

Director: Dimas Cabré Chacon, Everis

Ponent: Xavier Burgués, ESSI

Gener 2017

Índex

1 Gestió del projecte 4
1.1 Context 4
1.2 Estat de l'art 6
1.3 Formulació del problema 8
1.4 Abast 9
1.5 Metodologia i rigor 10
2 Pla de projecte 11
2.1 Objectius 11
2.2 Tasques 12
2.2.1 Documentar 12
2.2.2 Resumir i criticar 13
2.2.3 Proposar 13
2.2.4 Requisits 13
2.2.5 Disseny 13
2.2.6 Implementació i verificació 13
2.3 Implementació dels principis de resiliència 14
2.4 Riscos 15
2.5 Identificació dels costos 16
2.5.1 Costos directes 16
2.5.2 Costos indirectes 18
2.6 Viabilitat econòmica 19
2.7 Control de gestió 20
2.8 Sostenibilitat 21
2.8.1 Econòmic 21
2.8.2 Social 22
2.8.3 Ambiental 22
3 Execució del projecte 23

3.1 Primera part: Principis teòrics de resiliència 23
3.1.1 Release it 26
3.1.2 Patterns of resilience 38
3.1.3 Resilience reloaded 40
3.1.4 A Framework for Self-Healing Software Systems 41
3.1.5 Principis proposats 42
3.1.6 Comentaris finals 44
3.2 Segona part: Implementació dels principis 45
3.2.1 Aplicació 45
3.2.2 Mode offline 49
3.2.3 NullPointerException 53
4 Conclusions 55
4.1 Objectius 55
4.2 Planificació temporal i pressupost 56
4.3 Treballs futurs 57
4.4 Valoració personal 58
4.5 Valoració Everis 59
5 Annex 61
5.1 Diagrames de Gantt 61
6 Bibliografia 62

1 Gestió del projecte

1.1 Context

Poc després d'haver construït el que es considera la primera computadora[1] de la història, van començar els intents per fer que aquesta adoptés el mètode de *pensament* humà o racional. Ens referim a la Intel·ligència Artificial[2] que no va ser reconeguda com a àrea de la ciència fins a una dècada després. Entre els principals problemes que aquesta tracta hi trobem: el raonament, el coneixement, la planificació, el processament de textos naturals i la percepció. Inclús l'arquitectura del PC ha anat evolucionant perquè s'assemblés a la del nostre propi cervell.

La resiliència és un altre exemple de qualitat pròpia de l'ésser humà que volem que caracteritzin els sistemes. Hollnagel[1] la defineix com l'habilitat intrínseca d'un sistema d'adaptar el seu funcionament abans, durant o després de canvis i disturbis de tal manera que mantingui disponibles les funcions requerides en condicions esperades o no.

En primer lloc es va començar a estudiar la resiliència en els sistemes informàtics en l'àmbit del hardware. Des de la redundància a nivell de bits o a nivell de fitxers pel que fa l'emmagatzematge de dades, fins als mecanismes d'encaminament d'internet. El hardware pateix errors de tota mena per això es fan còpies de seguretat, s'utilitzen tecnologies de virtualització de l'emmagatzematge com els RAID, etc.

---

[1] L'Eniac, presentat al 1946 en Pennsylvania
[2] Fundada com a tal en1956 en una conferència a Dartmouth College, per John McCarthy, Marvin Minsky, Allen Newell, Arthur Samuel i Herbert Simon.

L'ús del terme resiliència en l'àmbit dels sistemes informàtics podria donar a entendre que implícitament ens referim a aspectes hardware. Però el software també pateix errors. No només degut al fet que s'està executant sobre el hardware. El software conté errors, com més complex és un sistema més errors pot tenir. Tal com sosté Richard Cook, en *How Complex Systems Fail*[2], en un sistema complex sempre hi ha alguna part que esta fallant.

L'objectiu d'aquest treball és estudiar i proposar principis que es podrien seguir, des de la fase de disseny, per aconseguir aplicacions resilient. El projecte suggereix que el concepte és transversal tant a nivell de fase del desenvolupament com a nivell de rol. Mitjançant una aplicació mòbil s'implementarà i s'analitzarà el funcionament del subconjunt de principis proposats.

El projecte ha estat impulsat pel departament d'Innovació d'Everis que és el principal *stakeholder*, promotor i beneficiari directe del projecte. El valor que el projecte aporta no resideix en ell mateix, sinó en la seva aplicació en futurs projectes.

1.2 Estat de l'art

El pioner en utilitzar i explicar el concepte de resiliència software és Michael T. Nygard. El seu llibre *Release It!*[3] encara que hagi sortit fa una dècada es considera com la bíblia de les aplicacions resilient. L'autor estudia diversos principis que es poden implementar mitjançant patrons a fi d'aconseguir software resilient i preparat per l'entorn de producció. En aquest sentit, a diferència de Nygard, nosaltres pensem que el software avui en dia està massa enfocat a l'entorn de producció. Considerem que l'esforç d'aconseguir resiliència es recompensa en tots els entorns i no només en producció.

Al llarg del llibre es proposen patrons de disseny per a la construcció de software resilient. També s'analitzen les situacions on aplicar-los, mitjançant casos reals de l'experiència de l'autor. En posteriors treballs i conferències sobre el tema es tornen a explicar els principis proposats per Nygard i també es recomana i referència el seu llibre. Com és el cas de la presentació *Patterns of resilience*[4] d'Uwe Friedrichsen. Aquest fa un recull d'alguns patrons explicant-los però tenint el mateix enfocament: l'entorn de producció. Els patrons estudiats per ell, amb exemples més a prop de la tecnologia actual, estan sota el paraigües dels grans patrons del disseny de l'enginyeria software com ara: baix acoblament, aïllament, etc.

Alguns autors no parlen en aquests termes per aconseguir resiliència. Com és el cas de Nicolò Perino[5] que proposa crear un *framework* que doti sistemes de caràcter general amb capacitats d'auto recuperabilitat. L'ambició d'aquest *framework* és

esquivar errors funcionals en temps d'execució. El seu enfocament es basa en la redundància intrínseca de les llibreries, és a dir, trobar mètodes independents que proporcionin la mateixa resposta.

El framework de Perino no és l'únic dissenyat per a proporcionar resiliència i cada cop se'n creen més. Alguns ja estan consolidats com per exemple akka[3], o hystrix[4]. Altres, com els projectes Simian Army proven el nivell de resiliència i ajuden a millorar-la. Partint de la idea de deixar un mico armat en un *datawarehouse*, s'han implementat diversos projectes que ataquen o inspeccionen instàncies o clústers de forma aleatòria en els sistemes de Netflix. Tenint en compte el principi que menciona Michael Nygard; els cucs de llarga durada no es poden detectar en la fase dels tests. Netflix amb The Simian Army[5] prova les seves aplicacions en l'entorn de producció.

[3] Akka és un conjunt d'eines (toolkit) i runtime per a la construcció d'aplicacions distribuïdes amb alta concurrència, resilient i orientades als missatges en JVM.
[4] Hystrix és una llibreria de Netflix que ajuda a incrementar la resiliència de les aplicacions en entorns distribuïts.
[5] Igual que Akka i Hystrix, Simian Army també està publicada sota llicència Apache-2.0.

1.3 Formulació del problema

Conscienciar-nos que els errors poden passar desapercebuts en les fases de *debug* o de testeig va donar fruit a termes com *fault-tolerance, resilience, self-healing o anti-fragility*. Tots aquests conceptes parteixen d'una hipòtesi contraria a la clàssica en quant a maximitzar la disponibilitat d'un software. Mentre la manera clàssica consisteix a minimitzar el número d'errors, la resiliència dóna per suposat que els errors apareixeran i tracta de minimitzar el seu impacte. El canvi és en l'òptica de la coneguda fórmula de la disponibilitat :

$$\text{Availability} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$$

Formula 1. La disponibilitat d'un software.

Mean Time To Failure és el temps mitjà entre errors, com més gran sigui vol dir que hi ha menys errors, el que significa més disponibilitat. Però la segona variable és el *Mean Time To Repair* que és el temps mitjà que dura la reparació.

Segons el nostre punt de vista la disponibilitat d'una aplicació no va lligada a l'entorn de producció. Aquesta qualitat és desitjable i es pot aconseguir mitjançant la resiliència. En termes d'éssers humans que interaccionen amb l'aplicació podríem dir que la resiliència és pot aconseguir per mitja de l'empatia de l'aplicació amb l'usuari. En el cas de l'entorn de desenvolupament l'usuari és el desenvolupador, i en el cas de l'entorn de producció n'és l'usuari final.

Tenir empatia cap al desenvolupador, pot facilitar molt la construcció del software. Per exemple, el framework Spring què en iniciar una aplicació s'han de carregar 400 *beans*, comporta un temps d'espera totalment innecessari en un entorn de desenvolupament. Pensar que l'usuari d'aquest framework només necessitarà 5-10 beans per provar la funcionalitat que està provant és ser empàtic. Això podria resultar en un mode d'execució d'aquest framework amb una política de carrega *on-demand* dels beans. Encara que aquest no és un exemple de resiliència, utilitzar l'empatia podria arribar a trencar la dita: <<*En casa de herrero, cuchillo de palo* >>.

1.4 Abast

Des de l'àmbit teòric volem estudiar l'origen i l'evolució del concepte de resiliència en el software, els principis proposats per diversos experts del tema i els avantatges d'aplicar-los. Aquests principis poden aparèixer com a patrons de disseny o principis d'implementació.

Dins l'abast del projecte també està implementar i analitzar el comportament de principis de resiliència. Començarem tractant els errors que poden sortir de les dependències. Concretament s'implementaran el mode *offline* d'execució de l'aplicació. Finalment ens centrarem en els errors que podrien produir els cucs amagats dins del codi. Concretament el codi de la part servidor. S'implementarà un mecanisme per eliminar les excepcions del tipus NullPointerException, a fi d'aconseguir-ho necessitarem un repositori de classes del backend.

Queda fora de l'abast del projecte la metodologia d'aplicar aquests principis. Aquest projecte suggereix principis per aconseguir resiliència, no té l'ambició de proporcionar ni ser una guia sistemàtica d'on ni com aplicar-los. Per manca de temps i altres recursos, no s'implementaran tots els principis estudiats i analitzats en la part teòrica d'aquest projecte.

1.5 Metodologia i rigor

En primer lloc s'ha de fer una tasca de documentació, consultant diverses fonts d'autoritat reconeguda en el tema de la resiliència software. A part d'utilitzar fonts confiables sempre es contrastarà la informació extreta amb el director del projecte. Sempre mantindrem una actitud critica davant dels principis de resiliència trobats sigui quina sigui la seva procedència. Les anàlisis dels principis tant com els principis proposats es validaran amb el director en reunions de manera periòdica.

2 Pla de projecte

2.1 Objectius

Amb la realització del projecte pretenem arribar al compliment de quatre objectius, tal com es pot veure a la Taula 2: els primers dos estan en l'àmbit teòric i els dos últims en l'àmbit pràctic. Com ja hem dit, la resiliència software ja es porta tractant des d'una dècada. Hi ha una gama amplia de principis ja proposats, sobretot en els últims anys. El projecte pretén resumir, explicar i, quan creguem necessari, criticar els principis que ja s'han proposat en aquest tema. Finalment, es proposa aportar alguns principis propis, implementar i estudiar els beneficis d'aplicar aquests principis al software.

Id	Objectiu
Obj1	Estudiar l'estat de la resiliència en l'àmbit del software.
Obj2	Resumir i analitzar principis de resiliència.
Obj3	Proposar nous principis de resiliència des d'un enfocament diferent.
Obj4	Implementar i analitzar els avantatges d'aplicar els principis proposats.

Taula 2. Objectius teòrics i pràctics del projecte.

2.2 Tasques

El projecte té una duració total estimada de vuit mesos i mig. Iniciat el 15 d'Abril 2016 i amb data final 31 de Desembre 2016, inclou un marge de quinze dies per desviacions que poguessin sorgir. La càrrega total aproximada és de 735 hores, que es divideixen en dues parts iguals. La primera és teòrica i consisteix a estudiar, analitzar i proposar principis de resiliència per a aplicacions. La segona part és pràctica i consisteix a implementar un subconjunt dels principis analitzats en la part teòrica.

En l'Annex s'adjunten els diagrames de Gantt amb l'estimació temporal i les relacions de precedència. Ja que només hi ha un autor, les dues fases i les tasques que les componen seran dutes a terme de manera seqüencial. Per aquesta raó no s'inclou el diagrama de Pert. El camí crític conté totes les tasques.

2.2.1 Documentar

En la primera part d'aquesta tasca farem la recerca de materials de suport pel tema de la resiliència software. Ens hem proposat cercar informació en diverses bases de dades especialitzades com ara Goolgle Scholar, ACM, IEEE Xplore. En la segona part farem l'estudi i l'anàlisi del material trobat. És la primera tasca, per tant no té cap dependència. Té una duració estimada de gairebé set setmanes. En el diagrama de Gantt estan representades les dues parts d'aquesta tasca: fer recerca i lectura i estudi.

2.2.2 Resumir i criticar

Tal com ja ens hem proposat, en la primera part del projecte farem un recull de principis de resiliència software. En aquesta fase escollirem algunes fonts i resumirem els principis que proposen. Contrastarem el que sosté la teoria amb l'experiència del director del projecte.

2.2.3 Proposar

Encara dins de la part teòrica del projecte volem proposar algun principi de resiliència. Degut a l'enfocament i experiència del director pensem aportar al tema de la resiliència software.

2.2.4 Requisits

En la part pràctica del projecte necessitem prendre els requisits dels principis de resiliència a implementar.

2.2.5 Disseny

Aquesta tasca té com a propòsit establir el disseny dels principis que implementem. Encara que no pretenem donar principis de disseny de la resiliència, suggerim una solució desacoblada.

2.2.6 Implementació i verificació

En primer lloc buscarem una aplicació Java per dotar-la de resiliència. Implementarem i li afegirem els principis que hem proposat. Finalment provarem el funcionament dels principis de resiliència amb tests.

2.3 Implementació dels principis de resiliència

Hi ha diverses raons per implementar una aplicació i aplicar els principis teòrics. Per tant hem decidit utilitzar els artefactes produïts en una assignatura[6] anterior. Consta d'una aplicació Android que disposa d'un servei al qual accedeix mitjançant una API rest. El servei s'encarrega principalment de la persistència. L'aplicació consisteix a proveir informació del nivell d'adaptabilitat dels llocs o locals públics per persones amb discapacitats motrius.

Per raons no rellevants s'ha hagut d'incloure la implementació de part de l'aplicació en el que és el projecte. Tot i que implementar una aplicació Android no és l'objectiu d'aquest projecte és una tasca necessària per acabar provant la viabilitat i el funcionament d'aquests principis. El programador està assabentat dels requeriments i coneix el disseny a seguir. Per tant, pel que fa a l'aplicació, la part més costosa en temps serà la implementació, ja que serà la segona aplicació Android executada pel programador. Contant amb el coneixement de l'aplicació i amb gran part dels artefactes generats durant l'assignatura pensem que és viable escollir-la.

[6] PES 2015 tardor

2.4 Riscos

Comentem breument les tasques que presenten riscos de provocar desviacions del pla temporal que hem fet:

En la tasca de desenvolupament de l'aplicació, concretament en la fase d'implementació preveiem un risc potencial. Un canvi de tecnologia suposaria una desviació, però el considerem poc probable.

Per les possibles desviacions s'han deixat dues setmanes de marge per cada part, tal com es pot apreciar en els diagrames de Gantt. A més d'això durant el període de l'1 d'Agost al 16 de Setembre s'ha decidit fer un curs d'Android de 30 hores, justament per la falta d'experiència del programador. Encara i no tenir prou amb les dues setmanes de marge es reduiria l'abast deixant fora de la implementació alguns principis.

2.5 Identificació dels costos

2.5.1 Costos directes

El cost total del projecte vindrà donat per la suma dels costos dels recursos consumits per cada fase, tenint en compte els riscos associats a cada fase i la contingència. En primer lloc considerem els costs dels recursos humans tal com es pot apreciar a la Taula 3.

Rol	Cost per hora [€]
Cap de projecte	30,00 €
Analista	30,00 €
Dissenyador	30,00 €
Tècnic programador	25,00 €
Tester	25,00 €
Documentador	30,00 €
Tècnic de sistemes	25,00 €

Taula 3. Preu per hora del rol.

Afegint el nombre d'hores de cada rol i els percentatges de participació de cada rol en cada fase obtenim el cost per rol dels recursos humans. El cost per cada rol en el projecte i el cost total dels recursos humans es troben a la Taula 4.

Tasca	Hores	Rols	Cost
Fer recerca	67,5	Documnentador 90%, Cap de projecte 10%	2.025,00 €
Llegir i estudiar	67,5	Documentador	2.025,00 €
Resumir i criticar	67,5	Documentador	2.025,00 €
Proposar	90	Cap de projecte	2.700,00 €
Requisits	90	Cap de projecte	2.700,00 €
Disseny	67,5	Dissenyador 90%, Analista 90%	2.025,00 €
Implementació	157,5	Tècnic programador	3.937,50 €
Verificació	67,5	Analista 5%, Tècnic programador 5%, Tester 90%	1.704,38 €
TOTAL	675		19.141,88 €

Taula 4. Cost dels rols en cada fase.

Tal com s'ha previst s'ha deixat un marge de dues setmanes per a cada una de les parts, que donen la diferència d'hores entre el projecte total de 735 i les hores totals de cada rol per fase de 675.

En quant al risc, el canvi de tecnologies en la fase d'implementació és poc probable. En aquest cas, ens costaria una setmana més. Per aquesta setmana hem de sumar 100,00 € que seria el 10% del cost del Tècnic Programador.

2.5.2 Costos indirectes

Com a costos indirectes tenim l'amortització dels recursos hardware i l'energia elèctrica. És a dir, un portàtil: Dell i5-5300U a 2,3GHz i 8GB RAM i un terminal Android: Oneplus X Snapdragon 801 i 3GB de RAM. El cost total dels dispositius hardware és de 1570,00 €. La duració total de 32 setmanes equival a 224 dies de feina. Això dóna un cost d'amortització (1570 * 0,25 *224*4,5)/(8*365) = 135,49 €.

A més a més hem de considerar els 8 mesos de corrent i connexió a internet, recursos també necessaris per dur a terme el projecte. Segons el model del portàtil tenim un consum d'energia de 0,92[7] kWh, donant un total de 676,2 kWh pel total del projecte. Per tant, el consum total d'energia suposa un cost de 87,91 €[8]. El cost associat a la connexió a internet suposa un total de 8*50 = 400 €.

Al total de 19.141,88 + 56,20 + 135,49 + 87,91 + 400 = 19,821,48 € li hem d'afegir la contingència, en aquest cas d'un 12%. Per tant, el cost total del projecte arriba a **23,785.78 €.**

[7] El consum inclou l'energia del portàtil, el terminal Android i la pantalla que s'ha emprat.
[8] Preu del kWh contractada amb Gas Natural Fenosa http://tarifasgasluz.com/faq/precio-kwh

2.6 Viabilitat econòmica

El valor econòmic que aporta el projecte és directament proporcional al nombre de projectes al que s'apliquin els principis recollits aquí. En conseqüència, el projecte en si no segueix cap model econòmic i no pretén ser viable econòmicament parlant. El fet d'implementar les aplicacions amb principis de resiliència, suposa per una banda un *overhead* pels equips de desenvolupadors però, per l'altre banda implica un manteniment més barat. El cost afegit per la formació dels equips més el cost de produir una aplicació resilient surt en benefici de l'empresa.

2.7 Control de gestió

Al final de setmana es recolliran les dades preses cada dia, de la dedicació de cada rol per dia i tasca. Segons aquestes dades es comprovarà no només la quantitat d'hores dedicades sinó també el rendiment. D'aquesta manera es podrà estimar si el temps restant amb la productivitat actual portarà a acabar la tasca en el temps previst. Per una altra banda també, s'estimarà el cost d'aquestes hores i recursos utilitzats, tal com es pot observar en la secció de la Taula 5. Les possibles desviacions dels costos indirectes s'avaluaran al final de cada mes.

Tasques \ Desviacions		Tarifa		Consum		Total	
		Mà d'obra	Recursos	Mà d'obra	Recursos	Mà d'obra	Recursos
Fer recerca	Estimat						
	Real						

Taula 5. Control de gestió del desviament per tasca.

2.8 Sostenibilitat

Per resumir l'anàlisi de la sostenibilitat s'ha generat la matriu de sostenibilitat, que és on hem analitzat els beneficis i possibles riscos del projecte en tres aspectes: econòmic, social i ambiental. Tal com podem observar a la Taula 6 i com expliquem en cada apartat els riscos són petits.

	Ambiental	Econòmic	Social	Total
Projecte en producció	Anàlisi de recursos	Viabilitat econòmica	Impacte personal	
Rang de puntuació:	**8** [0:10]	**6** [0:10]	**8** [0:10]	**22** [0:30]
Vida útil i resultats	Petjada ecològica	Cost final	Impacte social	
Rang de puntuació:	**6** [0:20]	**6** [0:20]	**12** [0:20]	**24** [0:60]
Riscs	Perjudicis ambientals	Riscs econòmics	Perjudicis socials	
Rang de puntuació:	**-3** [-20:0]	**-4** [-20:0]	**-2** [-20:0]	**-9** [-60:90] **46**

Taula 6. Matriu de sostenibilitat.

2.8.1 Econòmic

Com s'ha pogut veure, s'ha fet una avaluació dels costos, tant dels recursos humans com dels recursos materials. El projecte és el resultat d'una iniciativa d'innovació d'Everis. Es preveu tant l'ampliació del treball com la reutilització en futurs projectes. L'aplicació de principis de resiliència varia de projecte a projecte. Per manca de temps no s'ha realitzat un anàlisi sobre el nombre mínim de projectes als que s'ha d'aplicar la resiliència per cobrir el cost del projecte.

2.8.2 Social

El projecte aporta un valor afegit en l'aspecte social dels desenvolupadors que seguiran els principis resilient. Aquest valor, s'aconsegueix a curt termini amb beneficis per l'equip: millora l'ambient de l'equip a causa de l'empatia mútua que facilita el desenvolupament del software. D'altra banda, l'impacte social d'aplicar principis de resiliència a les aplicacions també cobreix una necessitat de l'usuari final. Aquest té una millor experiència d'usuari, ja que l'aplicació en gran part s'encarrega de resoldre els problemes que podrien sorgir.

2.8.3 Ambiental

El principal recurs material utilitzat és el portàtil. Aquest té un fort impacte ambiental. Encara que és poc probable que arribi a ser o reciclat al final de la seva vida útil, encara servirà per la realització d'altres projectes. El portàtil, doncs, comporta un impacte ambiental negatiu encara que durant la realització del projecte no es produeixi un considerable volum de CO_2. L'energia elèctrica és la principal font i és la causa de la producció de 2.32[9] tones de CO_2 durant la realització del projecte. Per una altra banda es preveu un ús reduït del paper que tindrà una generació de CO_2 menyspreable.

---

9 http://www.idae.es/uploads/documentos/documentos_11406_guia_practica_energia_3ed_a2010_509f8287.pdf pg.41

3 Execució del projecte

3.1 Primera part: Principis teòrics de resiliència

La idea inicial del projecte partia del projecte anomenat Chaos Monkey, el codi del qual Netflix havia alliberat el 2015. Aquest forma part d'un conjunt de projectes anomenats The Simian Army[10], tal com es pot veure a la Taula 7. Serveixen per provar la resiliència dels seus sistemes. D'aquí ha sorgit la idea de baixar un esglaó més, dins del que és la resiliència software, es volien estudiar els principis que podrien regir una aplicació resilient.

Mico	Descripció
Chaos Monkey	Apaga instancies de manera aleatoria.
Latency Monkey	Introdueix demores artificials en la comunicació entre client i servidor.
Conformity Monkey	Apaga instancies que no segueixen les bones practiques.
Doctor Monkey	Notifica els serveis si troben instancies malaltes, per exemple massa CPU, i les apaga.
Janitor Monkey	Ordena i neteja l'entorn. Busca i esborra recursos no utilitzats.
Security Monkey	Busca violacions de seguretat o vulnerabilitats. Verifica la vigència dels certificats SSL i DRM.
10-18 Monkey	Detecta errors de configuració o d'execució de les instancies que serveixen clients en diferents zones geogràfiques.
Chaos Gorilla	Semblant al Chaos Monkey però simula un desbortament d'una zona de cobertura sencera (Amazon).

Taula 7. Projectes que composen The Simian Army.

La principal font de resiliència n'és, sense dubte, l'experiència. Aquesta és inherent i varia en funció de cada persona implicada en el desenvolupament del

[10] Disponible en github: https://github.com/Netflix/SimianArmy

software. Un dels beneficis que dona l'experiència és la resiliència. Com ja hem mencionat, entenem per resiliència la capacitat del software a respondre en circumstàncies adverses i/o sortir d'elles de manera autònoma.

De la resiliència en l'àmbit del software no fa tant que se'n parla, gairebé una dècada[11]. En el seu llibre, *Release it*, Michael T. Nygard tracta el tema de la resiliència software des de la seva experiència.

Cal dir que el terme de resiliència ha anat evolucionant en aquest àmbit. Hi ha tres termes que estan molt relacionats, veure Figura 8. El primer és el concepte de *Fault Tolerance*, que consisteix en construir software robust. Es a dir, la fallida d'un o més components no comporta la caiguda de tot el sistema. El tercer és el concepte d'*Anti Fragility* que és la capacitat d'un sistema no només de tornar a l'estat normal sinó avançar cap a un estat millor. La resiliència està entre ells, o els inclou?

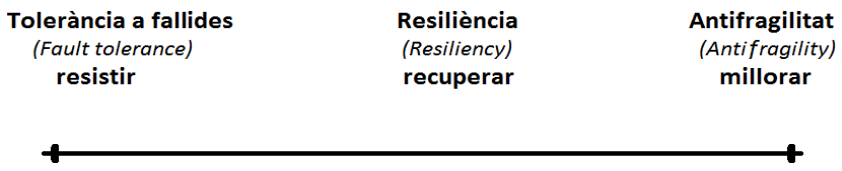


Figura 8. Conceptes relacionats amb la resiliència.

En el llibre Release It, la resiliència esta més a prop de la tolerància a fallides. En general, els principis que proposa doten al software de resistència que ell considera com a resiliència.

[11] Considerem el llibre Release it! (2007) com el primer en el que no només es parla sino que es tracta la resiliència software àmpliament i en detall.

Jonas Bonér, creador del framework akka, en la seva presentació[6], utilitza els termes de la Figura 8 per definir la resiliència. Per ell, la resiliència esta en algun punt entremig, és més que la Tolerància a fallides i menys que l'antifragilitat. Els principis de resiliència han de recuperar l'estat òptim. En quant a la resiliència purament software repeteix els patrons que apareixen en Release It. En temes de resiliència a nivell de sistema distribuït es centra en la resiliència que aporta akka, donant exemples d'ús.

Uwe Friedrichsen, també tracta el tema en algunes presentacions. En la primera[4], està d'acord amb Jonas Bonér afirmant que la resiliència va més enllà del fet de simplement resistir als errors, és tornar a l'estat òptim.

En canvi en la segona[7], hi ha una evolució en el concepte de resiliència. Aquí, proposa una arquitectura conceptual de la resiliència que comença a incloure el concepte d'antifragilitat.

Per nosaltres la resiliència engloba la tolerància a fallides, la recuperació i l'anti fragilitat. Anomenem, doncs, principi de resiliència qualsevol principi que doti el software amb capacitat de resistència, recuperació o inclús millora. Es a dir, una aplicació resilient és aquella que segueix donant servei a un determinat nivell de qualitat després d'haver patit errors i és capaç de tornar a l'estat òptim o incús a un estat millor. En el cas ideal aquesta recuperació és transparent de cara a l'usuari. En els altres casos s'informa l'usuari que la funcionalitat no esta disponible temporalment i es torna a informar quan s'hagi efectuat la recuperació.

3.1.1 Release it

Ara analitzarem els patrons que Michael T. Nygard proposa en el seu llibre, *Release it*[3], per aconseguir aplicacions resilient o més resilient. Alguns d'aquests patrons ja s'han anat incorporant als *bons costums* i/o a *frameworks* corresponents. Des del principi deixa clar que la principal motivació en construir software resilient és econòmica. El subtítol de la portada ho indica: "*Design and Deploy Production-Ready Doftware.* Segons sosté Nygard, una decisió de disseny és una decisió econòmica; i qualsevol *estalvi* que es vulgui fer en aquesta fase tindrà repercussions *cares* en producció. Per tant, la programació ha de ser pragmàtica, orientada a l'entorn de producció, no a l'entorn de proves o QA.

Encara que és difícil trobar-se dues vegades amb el mateix problema, tard o d'hora surten els anti patrons. Són aquelles situacions sistemàtiques que porten a errors, i per tant es poden aplicar solucions generals. El llibre s'estructura en quatre grans parts: Estabilitat, Capacitat, Reptes Generals de Disseny i Operacions. En els primers dos temes s'estudia en profunditat els anti patrons i els patrons corresponents.

En els darrers dos temes més que principis de resiliència són consells. Aspectes importants a tenir en compte a l'hora de dissenyar, com ara, la xarxa, la seguretat o la disponibilitat. Finalment, en el tema d'operacions tracta els aspectes de transparència i d'adaptació. Encara que està molt enfocat en l'entorn de producció, l'autor aconsegueix donar una visió prou completa del patrons que es podrien aplicar per aconseguir software resilient.

3.1.1.1 Estabilitat

Com ja havíem comentat, el primer tema que tracta és l'estabilitat. El software resilient ha de ser estable. Un error d'una certa funcionalitat no pot ser que faci caure tot el sistema, sent necessari un reinici de l'aplicació o del servidor. L'autor identifica una gran varietat d'elements com a anti patrons en aquest tema. Aquests són: els punts d'integració, les reaccions en cadena, cascades d'errors, els usuaris, *threads* bloquejats, atacs d'auto denegació de servei, efectes d'escalat, capacitats no balancejades, respostes lents, SLA, respostes no determinades.

3.1.1.1.1 Anti patrons

Els punts d'integració es van multiplicant conforme el sistema d'informació d'una organització va creixent. Cada cop hi ha més fonts i consumidors d'informació que es necessiten integrar, necessiten interaccionar. Per exemple, CRM, ERP, MRP, BPO entre d'altres. Per tant cada socket, procés, pipe o crida remota pot i arribarà a penjar-se.

Les reaccions en cadena tenen que veure amb temes d'escalabilitat a nivell horitzontal. La Figura 9 mostra una granja amb vuit servidors darrere un balancejador de carrega. El problema apareix en cas de caiguda d'un servidor, els que queden s'han de repartir entre tots la seva feina. Depenent del tipus, l'error podria provocar la caiguda d'una altre servidor, fins arribar a caure tot el sistema.

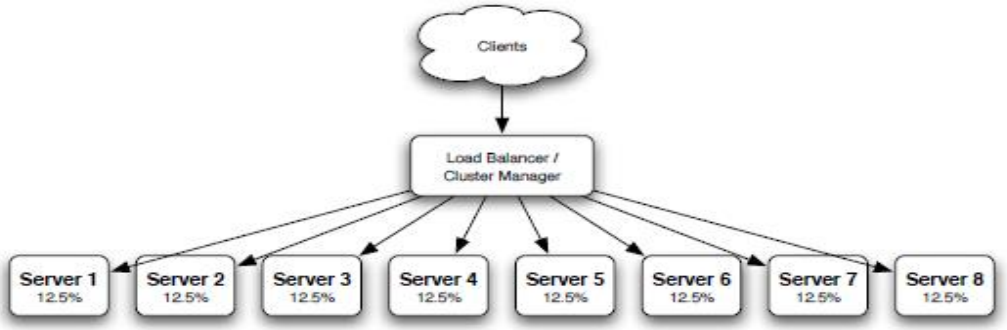


Figura 9. Exemple d'escalabilitat horitzontal.

Les cascades d'errors són semblants a les reaccions en cadena però a nivell de capes. Si els errors d'una capa provoquen erros en la capa que els crida parlem de cascades d'errors. Per exemple si el clúster de bases de dades es cau, i les aplicacions que servia no maneguen bé aquests errors aquestes començaran a fallar. Solen aparèixer quan s'esgota alguna pool amb recursos.

El comportament dels usuaris, tant de manera individual com general és prou demandant per no dir totalment imprevisible. A més el sistema escala en funció del hardware contractat i no en funció de la quantitat d'usuaris[12]. Per tant la pregunta és com reacciona el sistema quan la demanda supera la seva capacitat per respondre?

Els threads bloquejats apareixen a l'hora d'explotar el paral·lelisme de les CPU's. El multithreading és complex i normalment no és factible provar l'aplicació amb un nombre suficientment alt de peticions. Per tant son problemes que difícilment surten abans d'entrar en producció.

[12] Aquest és un exemple d'argument antiquat ja que des del segon trimestre del 2008 han començat a aparèixer serveis de host que proporcionen un escalat en funció del nombre d'usuaris.

Els atacs d'auto denegació de servei: *self-denial attack* apareix quan el sistema com un tot, inclús els humans "conspiren" en contra d'aquest. Per exemple una campanya de màrqueting que atreu molts més clients dels que el sistema esta preparat per rebre.

Les capacitats no balancejades tenen a veure amb el gestor d'escalat i les diferències entre recursos frontend versus backend.

Les respostes lents apareixen normalment quan el sistema ja esta en un nivell de demanda excessiu, per culpa del *garbage collector* o *memory leaks*.

El service-level agreement és el contracte que regula les condicions de servei. També conté les clàusules de penalitzacions econòmiques en cas que el servei no compleix les condicions. El problema és que un sistema no pot tenir un SLA millor que el de la pitjor de les seves dependències.

S'ha de dissenyar amb escepticisme. En molts casos una aplicació tracta la seva base de dades amb massa confiança. Qualsevol dependència pot en un moment donat retornar una resposta no esperada. Per exemple la base de dades podria respondre amb un resultat considerablement més gran que normalment. Si l'aplicació no limita la quantitat d'informació que esta disposada a processar poden passar coses no desitjades, el temps que triga és massa i l'usuari perd l'interès, desbordaments de memòria, etc.

3.1.1.1.2 Patrons

Per prevenir els escenaris problemàtics, en quant a l'estabilitat del sistema, enumerats més a dalt, Nygard proposa vuit patrons. Com ja hem mencionats alguns ja estan implementats per les llibreries que és veuen actuant en dites circumstàncies. Per exemple, el primer patró és el timeout. Però el programador ha de ser conscient i configurar-ho pròpiament.

El següent patro s'anumena circuit breaker. Consisteix en monitorar el timeout i obrir el circuit si aquest salta molt sovint. Per tant, si el circuit està obert, ja sabem que no aconseguirem resposta, podem respondre que molt ràpidament. Un procés addicional és necessari en aquest cas per anar preguntant pel servei. De manera automàtica, l'aplicació pot detectar que el servei torna a estar disponible i tancar el circuit tornant a l'estat normal.

Els *bulkheads* o mampares, veure Figura 10, separen l'espai d'una embarcació en compartiments. En cas de produir-se forats, el compartiment afectat es pot tancar i contenir l'aigua i evitar la propagació d'aquesta a la resta del vaixell. Seguint aquest exemple l'aplicació hauria d'estar dividida en particions que no deixin propagar els errors a traves de les mampares.

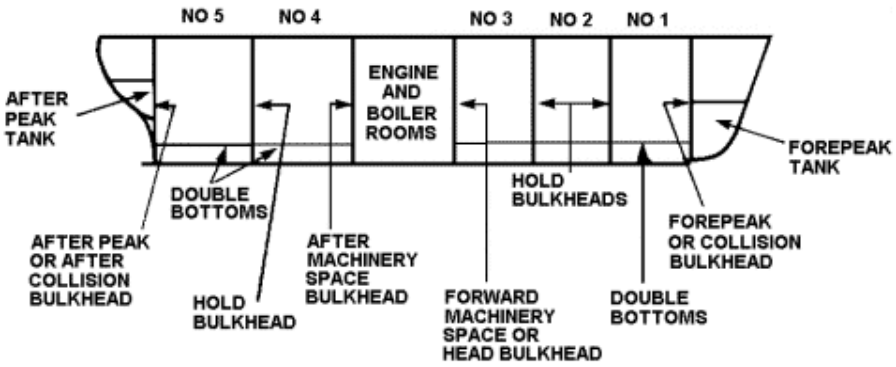


Figura 10. Mampares d'una embarcació.

Com a exemple, a la Figura 11, tenim a Baz com a dependència de Foo i de Bar. Per exemple, un manteniment Baz podria ser impossible de realitzar degut a la impossibilitat de respectar els SLA de Foo i SLA de Bar a l'hora. En aquest cas, Baz hauria d'estar compartimentat protegint els clients. Evidentment s'ha d'estudiar bé la la mida dels compartiments, des les thread pools fins als servidors en un claster.

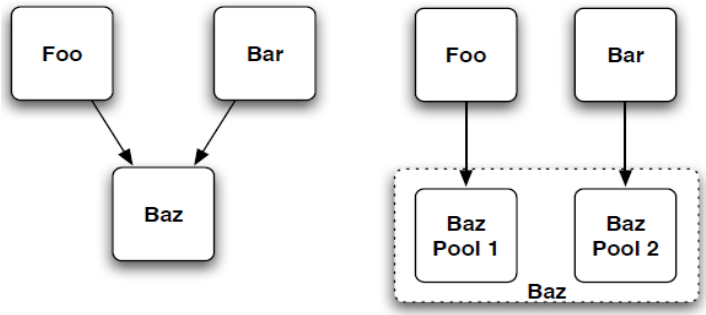


Figura 11. Aplicació del principi de mampares

El Steady-state és l'estat normal de l'aplicació. Aquest s'hauria de mantenir per si mateix sense necessitat d'intervenció humana diària. Pels problemes d'espai dels logs o neteja de la base de dades s'haurien de fer scripts que s'executin automàticament. Un altre aspecte a considerar per garantir un estat òptim de

l'aplicació consisteix en controlar la memòria que la cache pot ocupar. Per últim els logs. Aquests, si s'han de conservar per llei és recomana no mantenir-los en servidors de l'entorn de producció.

Si una resposta lenta és pitjor que no donar cap resposta, llavors una resposta lenta i errònia és encara pitjor. Aquest patró proposa vigilar les fonts probables d'errors i avançar-se amb la resposta en cas que és pugui determinar que fallarà. Això no sempre es pot determinar, però si és el cas, no només estalvia temps de l'usuari sino recursos del sistema. Per tant abans de fer qualsevol crida, s'hauria de comprovar tot el que es pugui abans de fer-la. En primer lloc validar l'input i en segon comprovar, si el circuit breaker corresponent està tancat, etc.

Les comunicacions són potencials fonts d'errors que s'han de tractar i protegir. La manera que proposa Michael Nygard és mitjançant el protocol de *handshaking*. Quan això no és possible, s'haurien de fer comprovacions d'estat: *Health-checks*, en cas que fer la comprovació sigui menys costosa que una crida que falla. També és recomanable utilitzar el handshaking per qualsevol protocol propi de baix nivell, per exemple a nivell de socket.

Test Harness representa un enfocament de desconfiança total amb respecte qualsevol dependència. Temps, format, contingut, mida de la resposta, o inclús el protocol de comunicació poden sortir del que s'havia especificat. Com tard o d'hora algun d'aquests problemes passaran, s'ha d'estar preparat. Les proves del software ha d'incloure escenaris com els mencionats i més.

Finalment un ben conegut patró de disseny: el baix acoblament, en aquest cas aplicat al *middleware.* Aquell espai amb un desordre singular que permet la comunicació de sistemes que no s'havien dissenyat per treballar en conjunt. La Figura 12 mostra l'espectre d'acoblament pel middleware.

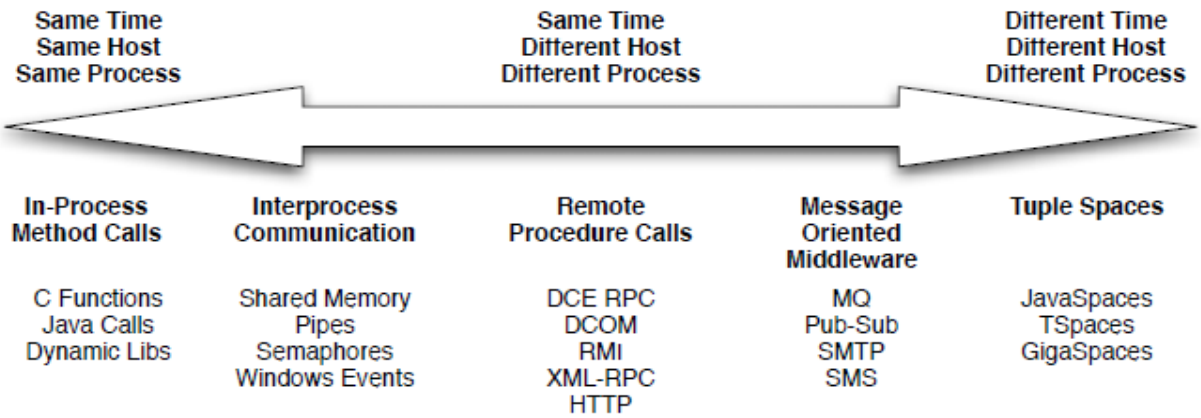


Figura 12. Els nivells d'acoblament i implementacions.

3.1.1.2 Capacitat

La capacitat d'un sistema és el rendiment(*troughput*) màxim sostenible pel sistema amb un temps acceptable de resposta per cada petició. La capacitat d'un sistema es defineix en funció de tres conceptes: velocitat per petició, rendiment en quant a numero de peticions processades per unitat de temps i l'escalabilitat. En aquest cas s'entén per escalabilitat incrementar la capacitat. Un greu problema que apareix en la anàlisis de la capacitat és la falta de linearitat. Per exemple, si un sistema

pot donar suport a 10.000 usuaris utilitzant un 50% de la CPU, és fals deduir que el sistema hauria de suportar 20.000 en total.

Segons l'autor hi ha una sèrie de problemes o circumstancies que amenacen la capacitat d'un sistema. Aquestes són: Resource Pool Contention, AJAX Overkill, Overstaying Sessions, Wasted Space in HTML, el botó de recarrega, Handcrafted SQL, Integration Point Latency.

3.1.1.2.1 Anti patrons

Quan el *pool* de threads actius que demanen accés a la base de dades supera el numero de connexions disponibles apareix el problema de Resource Pool Contention. El coll d'ampolla del sistema és la limitació del numero de recursos disponibles, ja que normalment les pool de connexions bloquegen indefinidament els threads en cas que no es puguin servir. Aquest és clarament un problema que amenaça la capacitat.

L'ús en excés de l'AJAX es pot convertir en un problema. Podria fer veure que el navegador esta penjat, l'increment de comunicació per la xarxa podria disparar-se i suposar una carrega massa gran i innecessària tan pel servidor com per l'aplicació.

La gestió del temps de caducitat de les sessions d'usuari és un altre factor important en qüestió de capacitat. Un fet curiós és que els usuaris que més recursos necessiten són els usuaris més desitjats pel negoci. Però la memòria del servidor és bé escàs.

Sempre que no és te cura de la mida del HTML, aquest acaba sent una mica més gran. El problema apareix per dos raons. Primer l'increment innecessari de la

memòria dels servidors web, i segon l'ús de l'ample de banda addicional inútilment. Un altre efecte que això provoca té com a actors els navegadors. Aquests, en funció de la mida del HTML mantenen una connexió durant més o menys temps.

El botó de recarrega del navegador està en mans de l'usuari, i això no són bones noticies. Cada cop que és prem el navegador abandona la petició anterior, obre un socket i fa una petició nova. El problema es que ningú mata la petició anterior, el servidor no sap que la pot descartar.

Combinar el servei d'ORMs amb consultes fetes a ma, encara que prometen eficiència són molt impredictibles. Tota la configuració de la base de dades esta preparada per les consultes dels ORM. No s'haurien de permetre les consultes fetes a mà o minimitzar el seu ús.

Qualsevol comunicació remota comporta una certa latència, que normalment és 1000 vegades més gran que una crida local. Encara que aquest és un problema d'eficiència per l'usuari, pel sistema acabarà sent un problema de capacitat.

3.1.1.2.2 Patrons

Per evitar problemes de Resource Pool Contention s'han de configurar adequadament les Pool Connections. Aquestes poden a més d'evitar alentir tot el sistema, millorar la capacitat. A part, s'han de protegir tots els threads que demanin connexió a la base de dades.

Una bona implementació de cache pot reduir problemes de rendiment. Redueix la carrega del servidor de la base de dades. Però s'ha de verificar que aquest és el cas, s'ha de mesurar la tassa d'encerts i la freqüència d'ús dels contingut. En la configuració de la cache s'ha de tenir en compte el límit d'espai que pot ocupar la cache i implementar un bon mecanisme de flush.

En el món web cada cop es requereix contingut dinàmic i específic. Portat a l'extrem arribem a trobar parts molt estàtiques a dins. Les parts estàtiques es poden pre-calcular.

Per últim, dins del tema de la capacitat, està el *Garbage Collector*. És la manera més rapida i fàcil per millorar la capacitat en aplicacions Java. Cal doncs, analitzar el comportament del Garbage Collector, l'ús del *heap* i el temps que es triga per treure la brossa, i ajustar la mida del heap. Configurar-lo bé porta avantatges de capacitat a més, té la capacitat de descobrir *memory leaks.*

Com a resum esquemàtic dels principis de resiliència que proposa el llibre tenim la Figura 13. Aquesta mostra les interaccions de patrons i anti patrons. Els quadrats representen els patrons i els ovals els anti patrons.

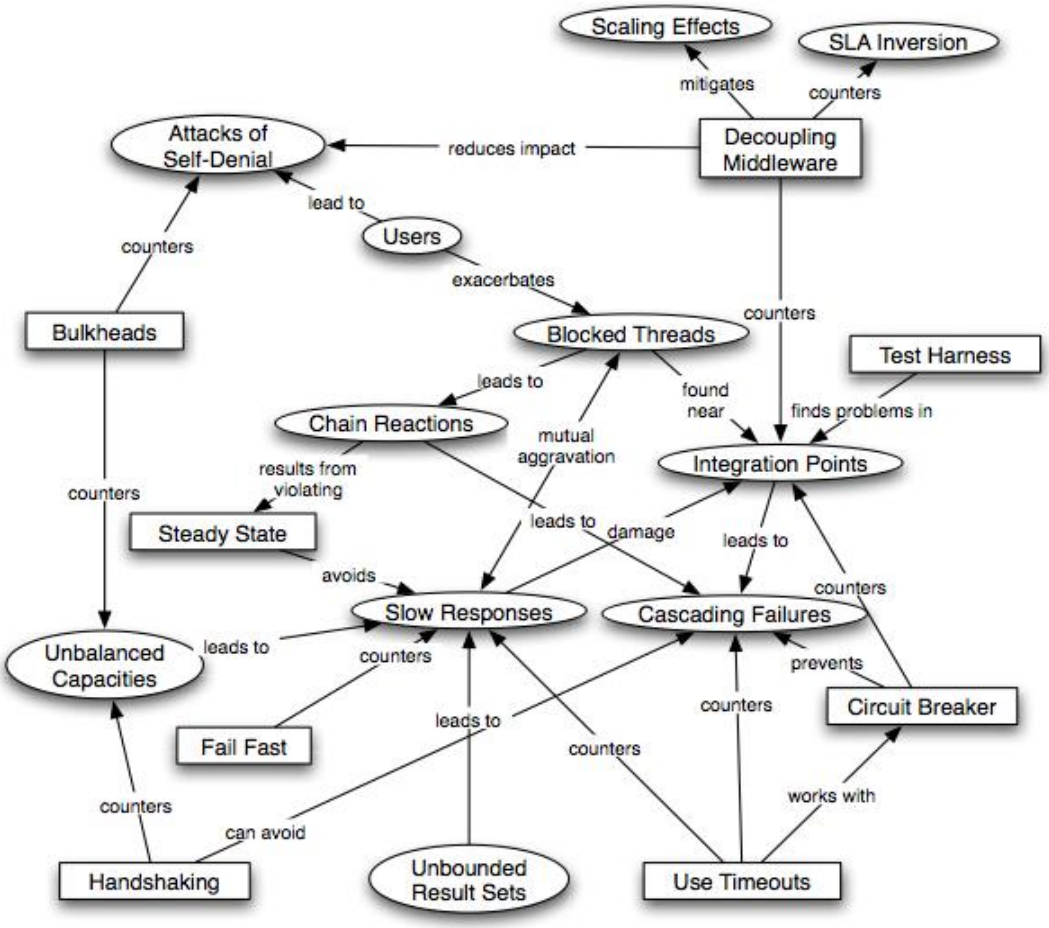


Figura 13. Interacció entre patrons i antipatrons

3.1.2 Patterns of resilience

Uwe Friedrichsen té una sèrie de presentacions sobre la resiliència que són més recents[4][7]. En la primera, Patterns of resilience recupera molts dels principis que proposa Michael Nygard. També menciona i recomana el seu llibre, *Release it*. En quant als errors en sistemes complexos, parteix de tres hipòtesis. Els errors no són una excepció, no es poden predir i no es poden evitar. Per tant, recomana acceptar-los[13][4].

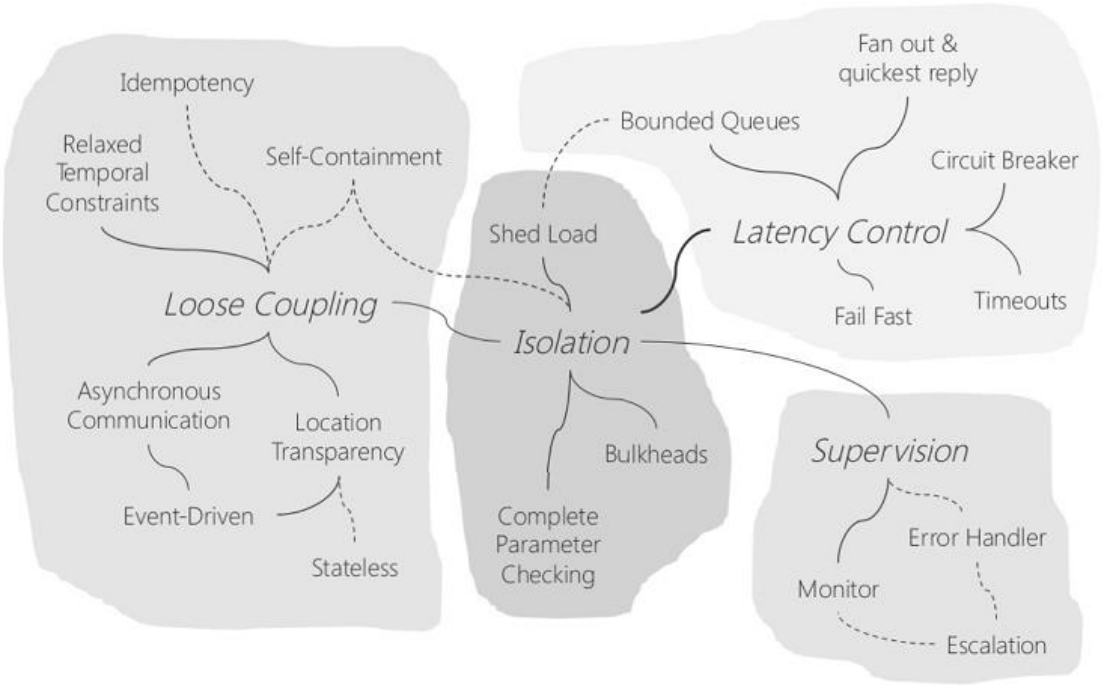


Figura 14. Patrons de resiliència i relacions.

A continuació dona la seva definició de resiliència com la capacitat d'un sistema per manegar una situació inesperada. En el millor dels casos sense que l'usuari se

[13] "Do not try to avoid failures. Embrace them".

n'adoni i en el pitjor cas amb una degradació del servei. Segueix el mateix enfocament a producció que trobem en el llibre, considerant la resiliència com una nova manera d'incrementar la disponibilitat del software. Després explica com els patrons de disseny influeixen sobre el sistema. Aquests s'expliquen fins a arribar a mostrar el codi. El resum visual dels patrons proposats per l'autor es pot veure a la Figura 14.

Comentarem aquí un parell dels principis de resiliència que proposa en Uwe Friedrichsen. Dins del tema de l'aïllament, els Bulkheads ja els trobem en el llibre de Nygard. Per tant els dos que queden són: Complete Parameter Checking i Shed Load.

3.1.2.1 Complete Parameter Checking

Per argumentar la comprovació dels paràmetres de tots els mètodes, invoca la llei de Postel[8]. Aquesta llei sosté que en el disseny de software un ha de ser liberal en el que accepta però conservador en el que envia. Es recomana doncs que cada paràmetre tingui un tipus de dades específic. Així és protegeix el mètode de crides malicioses.

3.1.2.2 Shed Load

Aquest principi és preocupa de guardar els recursos. Per evitar una sobrecarrega de peticions, s'ha de posar un *porter*[14] davant dels recursos. Per tant és limita la quantitat de peticions en funció de la carrega que el sistema ja en té.

[14] Gatekeeper

3.1.3 Resilience reloaded

En la segona presentació[7] a més de proposar encara més principis de resiliència, ja es proposa una arquitectura per les aplicacions resilient. Es fa, doncs, distinció entre els principis de resiliència que caracteritzen el software (Core), i els que han de ser externs (Detecció, Tractament i Prevenció). El terme de resiliència ha evolucionat per incloure la prevenció, Figura 15. Per tant, no inclou només tolerància a fallides, sinó també antifragilitat, veure Figura 8.

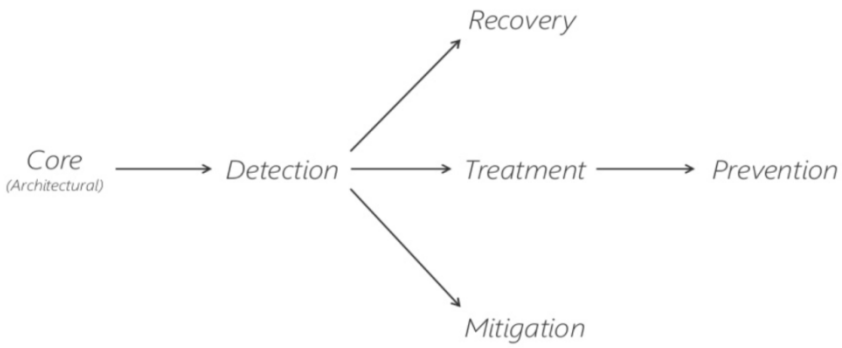


Figura 15. Arquitectura per a software resilient.

3.1.4 A Framework for Self-Healing Software Systems

En aquest article, resultat del seu doctorat, Nicolò Perino proposa un framework per aconseguir resiliència software. La idea consisteix a aprofitar la redundància a nivell de mètode de les llibreries. Segons el seu anàlisis hi ha una redundància explotable en les llibreries Java.

El framework introdueix un overhead entre un 9% i un 140%. Aquest és degut al fet que cada mètode que té un equivalent ha d'anar envoltat per un bloc *try-catch*. Els resultats de les proves amb algunes aplicacions mostra un percentatge d'auto recuperació entre el 20% i el 50%.

3.1.5 Principis proposats

En el cas ideal d'aplicació resilient, s'ha d'analitzar des de la fase de disseny quins principis de resiliència aplicables són aplicables. La implementació d'aquests principis ha d'estar totalment desacoblada de l'aplicació. Els diferents principis de resiliència també han d'estar desacoblats entre ells. De tal manera el nivell de resiliència es pugui incrementar o disminuir amb facilitat. Entenem però que hi ha principis de resiliència que no arriben a complir aquest ideal. Inclús entre els principis, que proposem i hem implementat nosaltres.

Hem començat tractant el tema de la connectivitat. Cada cop hi ha més velocitat a les xarxes de comunicació i cada cop es fan més aplicacions que utilitzin les dades. Però qualsevol xarxa encara esta lluny de ser infal·lible. Per tant, pensem que s'ha d'explorar al màxim les funcionalitats que podria donar una aplicació a l'usuari encara que temporalment l'usuari es trobi sense connexió.

El primer principi de resiliència que hem proposat l'anomenem mode offline. Consisteix en utilitzar el concepte de cache persistent en el dispositiu de l'usuari. D'aquesta manera les dades que utilitza l'usuari estan més a prop. Tant si es tracta de dades que consumeix, com si es tracta de dades que produeix.

El segon principi de resiliència tracta els errors interns d'una aplicació. Aquests s'amaguen en el codi de qualsevol projecte de software. Passem, doncs, de les dependències d'una aplicació als errors inesperats que pot produir la mateixa

aplicació. Degut a que alguns errors no s'arriben a trobar en la fase de test es solen capturar tots els errors i crear vistes personalitzades d'una varietat d'errors. Hi ha varies raons per actuar així, com ara la seguretat o inclús la confiança de l'usuari.

En aquest cas no volem que l'aplicació simplement informi de l'error sino que provi d'arreglar-lo. Per fer-ho farem *conscient* al mòdul de resiliència d'un repositori de classes. Si alguna classe dona problemes aquest pot provar de substituir-la amb una versió més nova.

3.1.6 Comentaris finals

Moltes de les propostes que s'han fet, començant pel llibre, estan enfocats a una resiliència que s'aconsegueix en la fase del disseny. Estem d'acord que la resiliència comença en aquesta fase, però no s'acaba allà. També insistim en una solució desacoblada i incremental. Considerem que el pensament empàtic cap a l'usuari en qualsevol fase és la forma més adequada de generar principis de resiliència. Amb usuari, no ens referim simplement a l'usuari final, el mateix desenvolupador és un usuari de l'aplicació.

En el cas del treball d'en Nicolò Perino trobem alguns problemes en el plantejament. Per una banda, l'anàlisi de les llibreries, en cerca de la redundància és fa de manera manual. Per una altra banda, la investigació s'ha fet segons al *Javadoc*. Trobem insuficient raó per considerar dos mètodes redundants només perquè el Javadoc ho afirmi.

Tal com havíem explicat, la nostra visió sobre aplicacions resilient és d'una o més capes que es poden afegir. No tots els principis de resiliència requereixen el mateix nivell d'intrusisme, per tant, és possible afegir resiliència a posteriori al software.

3.2 Segona part: Implementació dels principis

3.2.1 Aplicació

Per la implementació dels principis de resiliència hem escollit aprofitar una aplicació que és el resultat de l'assignatura de PES anomenada Hangaround. L'aplicació té coma objectiu facilitar l'accés a vida social de les persones amb discapacitats motrius. El cas emblemàtic d'aquest públic objectiu són les persones que utilitzen cadires de rodes. Amb l'ajuda de la comunitat d'usuaris que la fan servir, l'aplicació proporciona informació sobre el nivell d'adaptació d'espais o locals d'accés públic. A la Figura 16 es pot veure que l'aplicació segueix el paradigma de client-servidor i les seves dependències, tant la part client com de la part servidor.

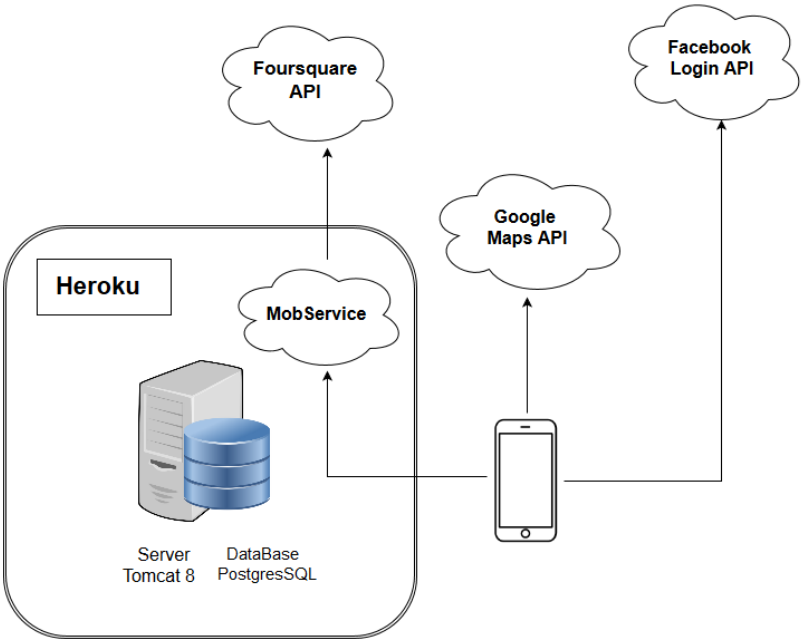


Figura 16. Infraestructura i dependències.

3.2.1.1 Servidor: MobService

La part servidor és un servei web amb arquitectura API REST, implementada en Java, corre sobre un Tomcat i esta allotjada en Heroku. S'encarrega principalment de la persistència de les dades. Té com a dependència principal l'API de Foursquare que utilitza per a proveir llocs al voltant de la ubicació o direcció cercada. En els casos d'ús només farem servir cerques de ciutats. Foursquare proporciona els llocs: locals, bars, museus, etc. Aquests llocs es guarden en una base de dades relacional en el servidor.

La cerca de llocs es fa en Foursquare però des del la nostra API. Els paràmetres que utilitzarem per fer la cerca són: *near* i *limit*. Amb el primer especifiquem una ciutat i amb el segon limitem en numero de resultats que desitgem mostrar. En els casos d'ús variarem el seu valor entre 1 i 25 segons convingui. Per a cada lloc que no és troba ja en el backend és guarda, amb un thread en background, amb un nivell d'adaptabilitat desconegut: UNKNOWN.

Els usuaris poden fer valoracions en relació amb el nivell d'adaptabilitat dels llocs. Hi ha quatre nivells: UNKNOWN – desconegut, UNADAPTED – sense adaptar, PARTIAL – parcial, i TOTAL. La part servidor determina el nivell d'adaptabilitat d'un lloc en funció de les valoracions que han fet els usuaris sobre aquell lloc. Una valoració requereix tres paràmetres: accés, serveis(wc) i ascensor. Un lloc té com a nivell d'adaptabilitat la que correspon a la ultima valoració que li han fet.

El primer es refereix a l'accés i mobilitat dins del perímetre del lloc, principalment rampa a l'entrada i amplitud dels passadissos. El segon comprova

l'existència de serveis adaptats. Tant el primer com el segon tenen una codificació binaria de cert o fals. Finalment la presència o absència de l'ascensor és el tercer paràmetre. Aquest només tindria sentit avaluar-lo en el cas en què el local té més d'una planta. La codificació d'aquest paràmetre consisteix en un enumerable amb els següents valors: HAS – el lloc disposa d'ascensor destinat a l'ús públic, NO_NEED – el lloc només té una planta, finalment HAS_NOT – el lloc té més d'una planta però no disposa d'ascensor.

3.2.1.2 Client: Hangaround

En la part client disposem d'una aplicació mòbil per a dispositius android. Esta implementada en Java, aplicació nativa. Com a principals dependències té l'API de Facebook per facilitar l'accés dels usuaris sense la necessitat de crear un compte nou. Els llocs que proporciona Foursquare es representen en un mapa. Per mostrar els llocs s'utilitza l'API de Google Maps.

Després de fer la cerca de llocs com s'explica anteriorment, per a cada lloc recuperat de Foursquare es busca el nivell d'adaptabilitat que té en el backend. Actualitzant un per un els llocs mostrats, amb marcadors de l'API de Google Maps, en el mapa. Aquests marcadors mostren el nivell d'adaptabilitat dels llocs que representen segons la llegenda de colors que es pot veure a la Taula 17.

Color	Descripció
GREEN	Totalment adaptat
YELLOW	Parcialment adaptat
RED	Cap adaptació
CYAN	Desconegut (per defecte)

Taula 17. Codi de colors dels marcadors en el mapa.

Clicant els marcadors es pot fer una valoració sobre aquell lloc mitjançant el formulari que apareix mitjançant un pop-up, com es pot veure a la Figura 18.

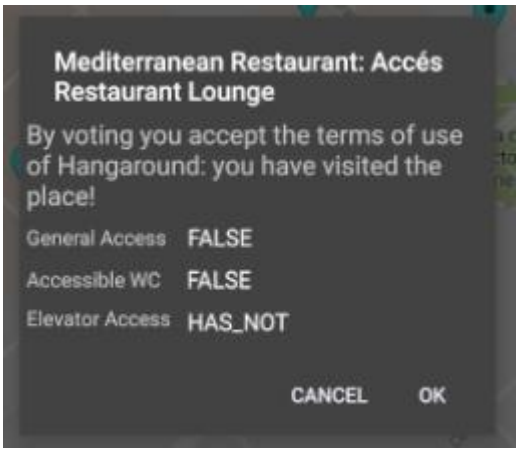


Figura 18. Pop-up amb formulari per fer una votació.

3.2.2 Mode offline

Com ja hem mencionat, la motivació d'aquest principi és donar el màxim de funcionalitats en cas de desconnexió. Per una banda, prova de mitigar els efectes de perdre la connexió al backend. Per l'altre banda, la pèrdua de connexió del mòbil a internet. La capa de resiliència s'encarregarà d'abordar els dos problemes.

3.2.2.1 Pèrdua de connexió al backend

La xarxa pot fallar o l'aplicació que s'executa en el backend pot fallar. Per un error propi o per culpa d'una dependència. Siguin quines siguin les causes o els causants d'aquests errors, el backend pot arribar a no ser disponible[15]. En tal cas, l'aplicació no seria capaç d'oferir cap funcionalitat. Qualsevol intent de connexió al backend retornaria un missatge d'error. En termes de disponibilitat, la indisponiblitat del backend provoca la indisponiblitat de totes les funcionalitats de l'aplicació.

Com ja havíem dit, vam implementar una cache per a cada una de les dues funcionalitats bàsiques: consultar llocs i el seu nivell d'adaptabilitat i valorar llocs. La cache, en els dos casos, és persistent i es troba en el dispositiu; no depenem de la xarxa i per tant és prou ràpida. Les cache són persistents, en una base de dades NoSQL (key-value) proporcionada per l'Android SDK, SharedPreferences.

[15] El backend perd la disponibilitat si dona una resposta errònia o dona una resposta massa tard.

En primer lloc hem implementat una cache per a les cerques; cerca-resultat. On la cerca és el text cercat en format String i el resultat és el conjunt de llocs que torna el backend per aquella cerca en format JSONArray. La lectura de la cache no es fa indefinidament. L'usuari esta informat que s'ha perdut la connexió amb el servidor de l'aplicació, però no només això, sino que en background s'inicia un thread que cada deu segons va comprovant si s'ha restablert la connexió amb el servidor. En tornar a estar disponible el servidor, l'usuari torna a estar notificat i la funcionalitat torna a estar al cent per cent disponible. El mòdul de resiliència ha provocat que l'aplicació toleri la fallida del backend i que torni a l'estat òptim tan aviat com sigui possible.

En segon lloc hem implementat una cache per a les valoracions. Encara que el backend no estigui disponible, l'usuari pot interaccionar amb l'aplicació valorant llocs. La cache guardarà totes les valoracions efectuades per part de l'usuari mentre està sense connexió amb el servidor. Quan es detecti que el servidor torna a estar disponible, entrada per entrada s'envien les valoracions de la cache per guardar-les en el backend.

3.2.2.2 Pèrdua de connexió a internet

El segon problema que havíem mencionant i que te a veure amb la connexió és el fet que el dispositiu es trobi en una zona de cobertura insuficient. Tot i ser semblant al primer hi ha una problemàtica afegida ja que l'aplicació té més dependències no nomes amb el backend. Per una banda el login mitjançant l'API de Facebook i el mapa per ubicar els llocs proporcionada per l'API de Google Maps. Degut als termes d'ús

d'aquesta darrera API, veure Captura 19, hem hagut de canviar la representació dels llocs quan el dispositiu no esta connectat. Només està autoritzat fer ús de cache dins del servei que Google proporciona.

Per no canviar tota la implementació de l'aplicació original s'ha decidit fer una vista en format llista amb els llocs, nova disponible a la Captura 20. Utilitzant l'API d'OpenStreetMap no s'hagués hagut de canviar la representació; menys d'intrusió.

10.5 Intellectual Property Restrictions.

a. No distribution or sale except as permitted under the Terms. You will not distribute, sell, or otherwise make any part of the Service available to third parties except as permitted by these Terms.

b. No derivative works. You will not modify or create a derivative work based on any Content unless expressly permitted to do so under these Terms. For example, the following are prohibited: (i) creating server-side modification of map tiles; (ii) stitching multiple static map images together to display a map that is larger than permitted in the Maps APIs Documentation; or (iii) tracing or copying the copyrightable elements of Google's maps or building outlines and creating a new work, such as a new mapping or navigation dataset.

c. No use of Content outside the Service. You will not use any Content outside of the Service except as expressly permitted to do so in Subsection (d). For example, you will not export or save the Content to a third party's platform or service.

d. No caching or storage. You will not pre-fetch, cache, index, or store any Content to be used outside the Service, except that you may store limited amounts of Content solely for the purpose of improving the performance of your Maps API Implementation due to network latency (and not for the purpose of preventing Google from accurately tracking usage), and only if such storage:

i. is temporary (and in no event more than 30 calendar days);

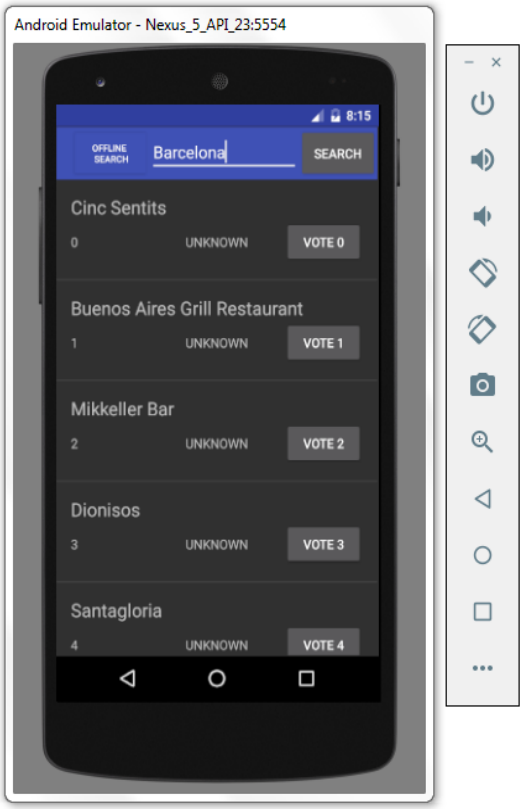
ii. is secure;

iii. does not manipulate or aggregate any part of the Content or Service; and

iv. does not modify attribution in any way.

e. No mass downloading. You will not use the Service in a manner that gives you or a third party access to mass downloads or bulk feeds of any Content. For example, you are not permitted to offer a batch geocoding service that uses Content contained in the Maps API(s).

Captura 19. Extret dels termes d'ús de Google Maps API



Captura 20. Nova vista per mostrar els llocs en mode offline.

Hi ha una limitació del model escollit deguda a no fer pre-fetch i per tant els llocs disponibles per a consultar sense cap impediment són només els llocs prèviament cercats. L'usuari pot trobar-se utilitzant les dades i encara sent potents l'autonomia dels dispositius mòbils està condicionada per la capacitat de la bateria. Tenint en compte aquests dos factors hem considerat que el millor enfocament seria no consumir ni dades ni espai en el dispositiu per fer pre-fetch.

3.2.3 NullPointerException

Suposant que l'ús que li dona un usuari encara i sent correcte provoca una excepció, com per exemple: NullPointerException. El comportament que desitgem que l'aplicació tingui en aquest cas és de provar de recuperar-se d'aquest error i acabar servint l'usuari amb la resposta desitjada. Les limitacions temporals han impedit la construcció d'un agent Java que faci la substitució de classes en calent. En conseqüència hem emprat un plugin ja existent, jRebel.

jRebel és capaç fer la substitució en calent, sense que calgui reiniciar el servidor, sense haver d'interrompre[16] la interacció de l'usuari amb l'aplicació. El seu funcionament consisteix en vigilar per una banda l'aplicació desplegada i per l'altre el directori target. En detectar que el timestamp és diferent executa la substitució. Això ens porta al segon ingredient necessari per que aquest principi es pugui aplicar. El mòdul de resiliència se li ha d'especificar la ruta al repositori de classes (l'equivalent al directori target en l'ús convencional del plugin). Aquest repositori de classes compilades podria estar estructurat de manera que proveeixi diverses versions.

En aquest exemple, de caire didàctic, no hem tingut en compte aquesta possibilitat. Per simplicitat també, per l'execució de la demostració el plugin s'ha configurat per un Tomcat que s'executa en local. L'error s'ha introduït en la primera versió de la classe FourSquareController i sense afectar altres classes[17]. Però en un cas real s'hauria de buscar la classe i les seves classes dependents, ja que s'haurien de

[16] En aquest cas l'usuari només pateix una demora de 2 segons en rebre la resposta.
[17] L'error introduït afecta una única classe per tant desapareix en fer una simple substitució de la classe.

substituir totes en conjunt. Aquestes podrien estar agrupades en *minijars* per facilitar l'aplicació d'aquest principi. Per tant, recomanem aplicar aquest principi en arquitectures de microserveis.

Un aspecte important aquí seria la política de substitució. Cal decidir si s'aplica la substitució en temps real, però amb el risc que la solució torni a donar algun altre error, o executar algunes proves abans de fer la substitució i incorporar el canvi de versió en crides posteriors.

En un entorn real aquest principi podria suposar problemes d'escalabilitat. Una aplicació podria tenir versions diferents de codi en clústers diferents.

Considerem com a cas ideal d'aplicar resiliència a una aplicació mitjançant un disseny extensible, es a dir, una arquitectura de plugins. Perseguim un nivell mínim d'intrusisme, de tal manera que els principis de resiliència que es considerin es vagin afegint a l'aplicació sense estar acoblats. En aquest sentit hem implementat els primers dos principis de resiliència amb el paradigma de programació orientada als aspectes (AOP). En Android els aspectes només poden capturar mètodes que s'executin en el UI thread. calgut implementar de manera acoblada els mètodes que permeten comprovar en background si s'ha establert la connexió amb el servidor o si el dispositiu torna a tenir connexió a internet.

4 Conclusions

4.1 Objectius

Considerem que els objectius del projecte s'han assolit satisfactòriament. A la Taula 21 trobem la Taula 2 ampliada per avaluar el compliment dels objectius inicials.

Id	Objectiu	Avaluacio (sobre 10)
Obj1	Estudiar l'estat de la resiliència en l'àmbit del software.	8
Obj2	Resumir i analitzar principis de resiliència.	7
Obj3	Proposar nous principis de resiliència des d'un enfocament diferent.	8
Obj4	Implementar i analitzar els avantatges d'aplicar els principis proposats.	7

Taula 21. Avaluació dels objectius.

Hi ha una amplia gama de principis per aconseguir resiliència software. Puntuem amb un vuit l'assoliment del primer objectiu perquè les fonts que més en parlen sobre el tema no són a nivell acadèmic sinó pràctic. Encara i així, aquestes fonts no deixen de ser fiables ja que conten amb desenvolupadors experimentats. Ni en el cas del llibre, ni el de les presentacions no hem pogut resumir i analitzar tots els principis que els seus autors suggereixen, per això hem puntuat amb un set el segon objectiu.

El mode offline ja l'implementen algunes aplicacions però el considerem un bon principi de resiliència que és el resultat de tenir empatia amb l'usuari. Finalment la implementació dels principis no ha estat totalment desacoblada, com en el cas ideal. Només hem mencionat alguns dels problemes d'escalabilitat del segon principi.

4.2 Planificació temporal i pressupost

S'ha seguit la planificació temporal amb petites desviacions. El risc de canvi de tecnologia no s'ha donat. Però hi ha hagut petits errors en l'estimació d'algunes tasques. La tasca de la recerca ha patit una desviació de dos setmanes degut a l'ambigüitat del concepte de la resiliència. Aquest concepte s'entén i s'ha aplicat abans en el món de l'enginyeria. S'utilitza en arquitectura en plans de contingència en casos de desastres naturals. En l'àmbit informàtic, la resiliència hi apareix en temes de xarxes i a nivell hardware. Degut a l'escassa informació sobre el tema en les bases de dades especialitzades ha fet que la tasca de recollida d'informació requereixi un esforç més gran i d'un estudi més detallat de paraules i conceptes claus relacionats.

Després de considerar altres fonts[18] la quantitat de material ens ha fet exhaurir els períodes de marge que havíem deixat. Hi ha hagut, doncs, un increment de 1.650€[19], que representa 6.94% del pressupost total inicial. El cost total del projecte arriba a **25.435,75€**

[18] Presentacions de les conferencies Devoxx i Goto; que són més de caire pràctic que acadèmic.
[19] El marge era d'un total de 60h, per programar: 30h*25€ = 750€ i per documentar: 30h*30€ = 900€

4.3 Treballs futurs

La tendència del software d'incrementar el nivell de complexitat i distribució fa cada cop més necessari un enfocament resilient. Encara queda camí per recórrer, ja que principis teòrics existeixen. Només entre el llibre[3] i la presentació[4] hi ha més de quaranta patrons o principis per aconseguir resiliència.

Veiem que el Machine Learning seria l'enfocament més adequat per dotar el software de resiliència. Com a possible projecte de futur seria cercar o aplicar principis de resiliència mitjançant xarxes neuronals. Aquestes tenen la capacitat no només de detectar els errors. Per exemple, si es determina que un mètode ja no retorna el que hauria, podrien prendre el control, i proporcionar la sortida en base a l'entrada.

Una altre concepte explotable en aquest sentit s'inspira en el funcionament del nostre cervell. En el seu llibre, I el cervell va crear l'home[9], Antonio R. Damasio sosté que el cervell disposa d'una representació del cos humà. Un mòdul de resiliència que tingués la representació dels components facilitaria la supervisió de l'estat o el funcionament de l'aplicació. En el segon principi, el mòdul de resiliència només *coneix* l'existència del repositori de classes, però aquest coneixement podria anar incrementant.

4.4 Valoració personal

Començant pel tema, la resiliència, el projecte es veia molt interessant i ha sigut així des del principi fins al final. La resiliència per a mi ha donat molt més sentit als patrons i principis de disseny estudiats a la carrera.

L'enfocament teòric i pràctic crec que també ha estat un bon plantejament. Començant per la part teòrica, el llibre[3], encara que és relativament antic ha aportat molt coneixement. Amb exemples orientats al mon Java, en general he pogut seguir i entendre les directrius que Michael T. Nygard donava. El director, Dimas Cabré Chacón amb la seva experiència, ha estat clau en contrastar les dos cares d'aquest projecte; la teoria i la pràctica.

En la segona part he tingut la oportunitat de implementar alguns principis que he trobat molt interessants. Com per exemple el tractament dels errors NullPointerException. He hagut de implementar una part d'una aplicació android. També he hagut d'aprendre a fer servir l'AOP. Estic content amb la feina feta i amb el coneixement adquirit durant la realització d'aquest projecte.

4.5 Valoració Everis

A continuació presentem la valoració del cap del projecte, i en representació de l'empresa Everis, el senyor Dimas Cabré Chacón.

Actualment existeix una demanda creixent en el món professional de la consultoria IT de productes de software que incorporin elements de resiliència. Aquesta demanda es justifica per la necessitat de que els sistemes puguin gestionar-se de forma autònoma, no assistida o independent a mesura que es fan més grans i complexos. Aquesta necessitat també aplica a components modulars de software (llibreries) de petita mida que solen ser integrats en sistemes majors. La recuperació de sistemes governada per persones pot ser molt costosa en aquesta mena de sistemes, ja que la detecció de esdeveniments no desitjats, el seu diagnòstic i la seva correcció acostuma a significar una inversió de temps que impedeix respondre a la cada cop més exigent necessitat de disposar de sistemes 7x24.

En l'àmbit professional, la resiliència s'estudia des de dues òptiques significatives. La primera és el nivell d'integració, on es distingeixen sistemes de monitorització (absolutament desacoblats), sistemes de sensors (parcialment acoblats), i sistemes conscients (totalment acoblats). La segona és el model de diagnòstic i correcció, que pot ser determinista (basat en algorismes més o ments complexos de resolució), o cognitiu (basat en un aprenentatge continu de les característiques i el comportament del sistema).

En aquest estudi s'han explorat exitosament alguns dels elements clau del disseny i desenvolupament de sistemes amb resiliència. S'han tractat tan en l'àmbit teòric com pràctic diversos aspectes dels mencionats anteriorment, i entenem que ha servit per a que el seu autor disposi d'un coneixement i d'uns fonaments sòlids que li permetrien emprar-los beneficiosament en l'àmbit professional. Aquest coneixement seria vital per a poder afrontar el desenvolupament de software amb resiliència que podríem anomenar conscient i cognitiu. Això significaria l'aplicació de les modernes tècniques d'intel·ligència artificial (especialment *Deep Learning*) per a poder modelar la nova generació de mecanismes d'auto-diagnosi i auto-recuperació dels sistemes de software.

Com a director del projecte, comparteixo la idea del treball que un sistema que incorpori consciència per a poder disposar de mecanismes d'auto-recuperació autònoms necessàriament ha disposar d'una representació interna d'ell mateix i dels seus estats i "vivències". Aquestes serien les properes línies d'investigació i aprofundiment que es proposaria escometre si l'autor s'incorporés al món professional IT.

5 Annex

5.1 Diagrames de Gantt

	Name	Duration	Start	Finish
1	Part I	14.9w	04/15/2016	07/28/2016
2	Fer recerca	3w	04/15/2016	05/05/2016
3	Llegir i estudiar	3w	05/05/2016	05/25/2016
4	Resumir i criticar	3w	05/25/2016	06/14/2016
5	Proposar	4w	06/14/2016	07/11/2016
6	Part II	15w	09/16/2016	12/29/2016
7	Requisits	2w	09/16/2016	09/29/2016
8	Disseny	2w	09/29/2016	10/12/2016
9	Implementació	7w	10/12/2016	11/29/2016
10	Verificació	3w	11/29/2016	12/19/2016

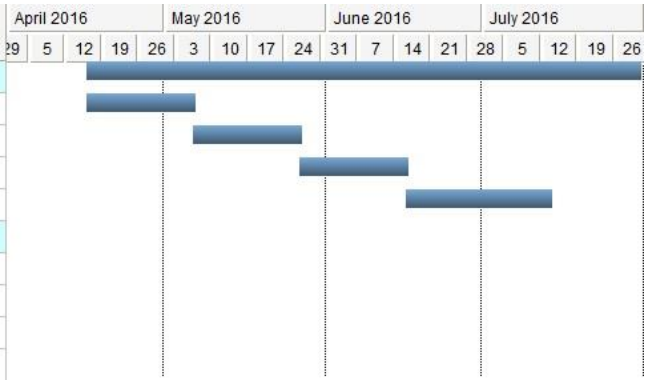


Diagrama 22. Tasques de la primera part en diagrama de Gantt.

	Name	Duration	Start	Finish
1	Part I	14.9w	04/15/2016	07/28/2016
2	Fer recerca	3w	04/15/2016	05/05/2016
3	Llegir i estudiar	3w	05/05/2016	05/25/2016
4	Resumir i criticar	3w	05/25/2016	06/14/2016
5	Proposar	4w	06/14/2016	07/11/2016
6	Part II	15w	09/16/2016	12/29/2016
7	Requisits	2w	09/16/2016	09/29/2016
8	Disseny	2w	09/29/2016	10/12/2016
9	Implementació	7w	10/12/2016	11/29/2016
10	Verificació	3w	11/29/2016	12/19/2016

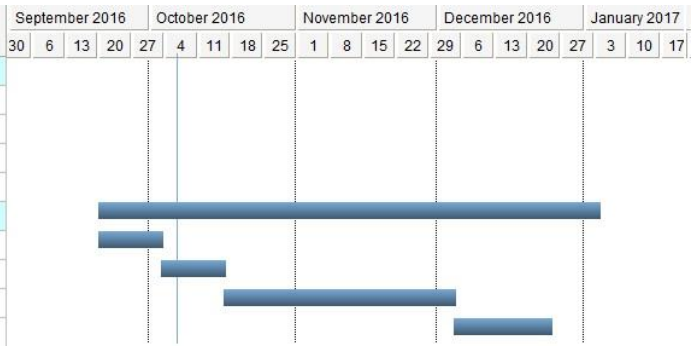


Diagrama 23. Tasques de la segona part en diagrama de Gantt

6 Bibliografia

[1] E. . Hollnagel, D. D. . Woods, and N. . Leveson, *Resilience engineering: Concepts and precepts*. 2006.

[2] R. I. Cook, “How Complex Systems Fail,” *Cogn. Technol. Lab. Univ. Chicago*, pp. 1–5, 2000.

[3] M. T. Nygard, *Release It! Design and Deploy Production-Ready Software*. 2007.

[4] Friedrichsen Uwe, “Patterns of resilience,” 2015. [Online]. Available: http://www.slideshare.net/ufried/patterns-of-resilience.

[5] N. Perino, “A Framework for Self-healing Software Systems,” pp. 1397–1400, 2013.

[6] B. Jonas, “Without Resilience Nothing Els Matters,” 2015, p. 193.

[7] Friedrichsen Uwe, “Resilience reloaded - more resilience patterns,” 2016, p. 102.

[8] P. Jon, “RFC 761,” p. 83, 1980.

[9] A. R. Damasio, *I el cervell va crear l’home*. 2010.