Build Software Safely!

17-313 Fall 2024

Foundations of Software Engineering

https://cmu-17313q.github.io

Eduardo Feo Flushing

Learning Goals

- Learn to discuss risk in a project
- Strategize about ways to mitigate risk
- Learn to get early feedback to reduce risk
- Find ways to catch our technical errors

Administrivia

Recover the points you lost in P2A. This is the procedure:

1. Check the P2A feedback
2. Fix the project plan according to the feedback provided
3. Contact your mentor on Slack to inform them you have resolved the issues. Explain the modifications you made and how they address the deficiencies.

- Midterm Next Sunday, October 6th
- Review Session: Thursday during Recitation

Smoking Section

- Last **two** full rows

Risk


Tony Webster
@webster
Follow
I appreciate the honesty.
Pick a password
Don't reuse your bank password, we didn't spend a lot on security for this app.
At least 6 characters
your password
Continue
8:20 PM - 15 Sep 2018
5,868 Retweets 15,672 Likes
58
5.9K
16K

Definition: Risk

Risk is a measure of the potential inability to achieve overall program objectives within defined cost, schedule, and technical constraints.

Conrow, E., 2003. Effective Risk Management: Some Keys to Success, 2nd ed. Reston, VA, USA: American Institute of Aeronautics and Astronautics (AIAA).

Risk is defined by two key components

The probability (or likelihood) of failing to achieve a particular outcome

The consequences (or impact) of failing to achieve that outcomes

Conrow, E., 2003. Effective Risk Management: Some Keys to Success, 2nd ed. Reston, VA, USA: American Institute of Aeronautics and Astronautics (AIAA).

Internal vs. External Risk

Risks that we can control

Risks that we cannot control

Levels of Risk Management

1. **Crisis management:** Fire fighting; address risks only after they have become major problems.
2. **Fix on failure:** Detect and react to risks quickly, but only after they have occurred.
3. **Risk mitigation:** Plan ahead of time to provide resources to cover risks if they occur, but do nothing to eliminate them in the first place.
4. **Prevention:** Implement and execute a plan as part of the software project to identify risks and prevent them from becoming problems.
5. **Elimination of root causes:** Identify and eliminate factors that make it possible for risks to exist at all.

"Rapid Development: Taming Wild Software Schedules," Steve McConnell, 1996

Levels of Risk Management

1. **Crisis management**
   - You wait until the fire is visible and then call the fire department to put it out.
2. **Fix on failure**
   - You have smoke detectors that alert you to the fire, and you react quickly once it's detected.
3. **Risk mitigation**
   - You install fire extinguishers and sprinklers to reduce the damage when a fire occurs but take no steps to prevent the fire.
4. **Prevention**
   - You install smoke detectors, inspect wiring, and remove fire hazards to reduce the chance of a fire starting.
5. **Elimination of root causes:**
   - You build the house with fireproof materials and remove all potential fire hazards to prevent the fire from ever occurring.

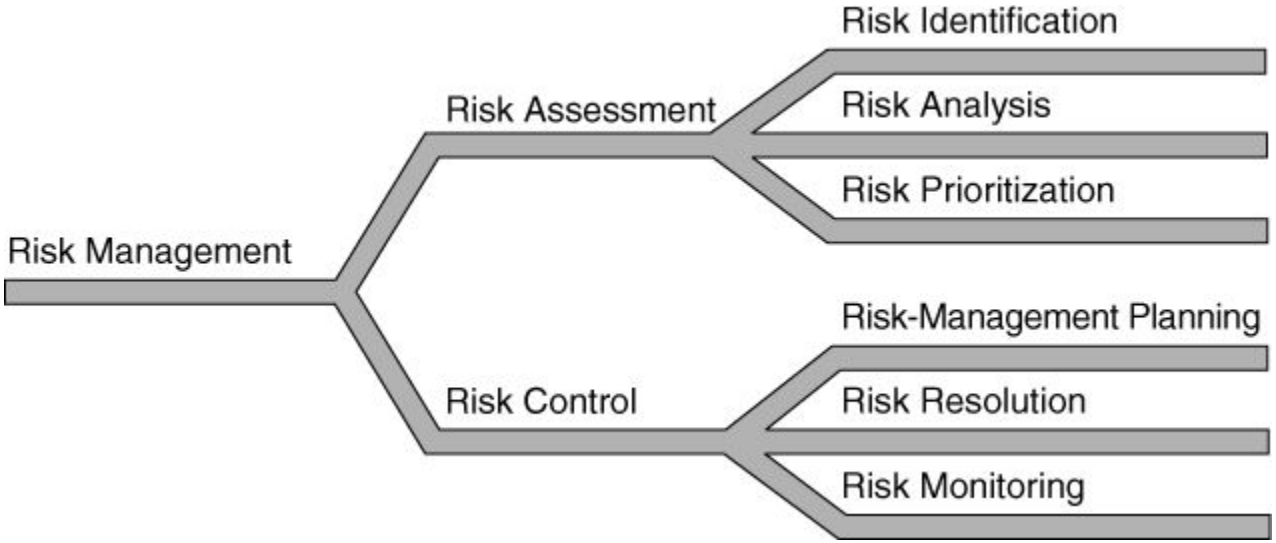
"Rapid Development: Taming Wild Software Schedules," Steve McConnell, 1996

Levels of Risk Management

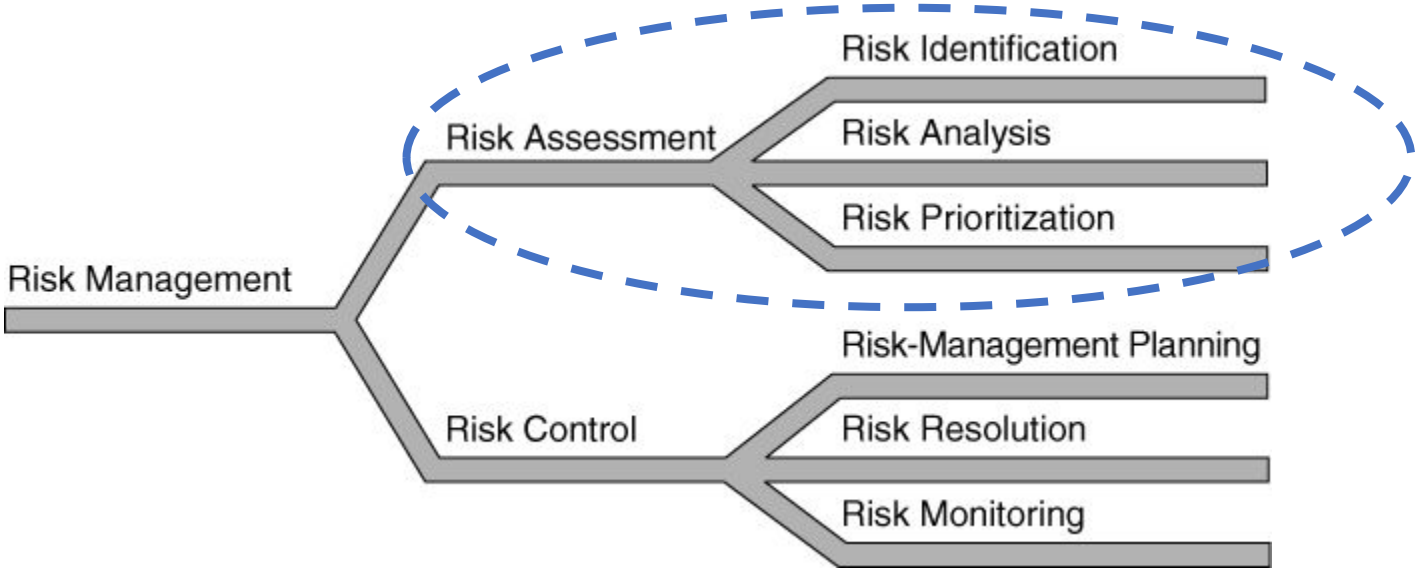
1. **Crisis management:** Fire fighting; address risks only after they have become problems.
2. **Fix on failure:** Detect and react to risks quickly, but only after they have occurred.
3. **Risk mitigation:** Plan ahead of time to provide resources to cover risks if they occur, but do nothing to eliminate them in the first place.
4. **Prevention:** Implement and execute a plan as part of the software project to identify risks and prevent them from becoming problems.
5. **Elimination of root causes:** Identify and eliminate factors that make it possible for risks to exist at all.

"Rapid Development: Taming Wild Software Schedules," Steve McConnell, 1996

Risk Management

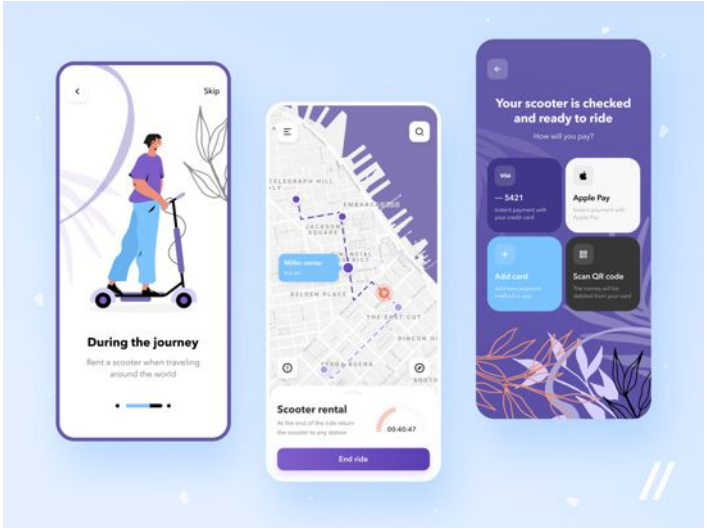


Risk Management



Team Exercise: Risk Identification

- What risks exist for the scooter app?



Risk assessment matrix

TABLE III. Risk assessment matrix

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

- MIL-STD-882E

https://www.system-safety.org/Documents/MIL-STD-882E.pdf

Aviation failure impact categories

- **No effect** – failure has no impact on safety, aircraft operation, or crew workload
- **Minor** – failure is noticeable, causing passenger inconvenience or flight plan change
- **Major** – failure is significant, causing passenger discomfort and slight workload increase
- **Hazardous** – high workload, serious or fatal injuries
- **Catastrophic** – loss of critical function to safely fly and land

DO-178b, Software Considerations in Airborne Systems and Equipment Certification, RTCA, 1992

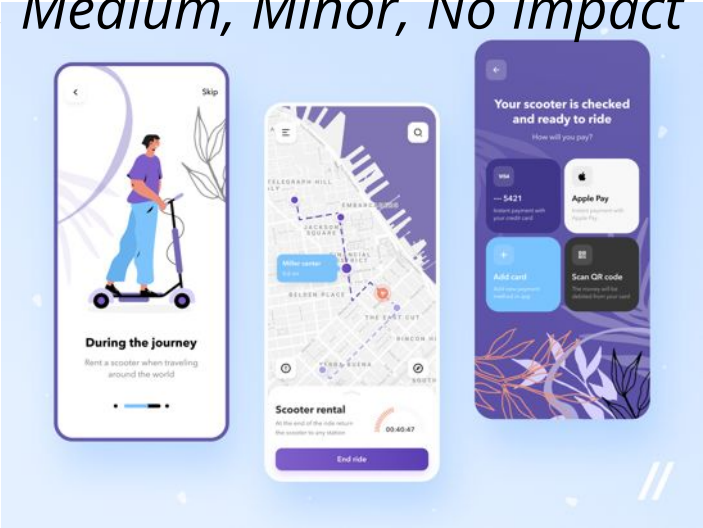
Risk Analysis

Risk	Probability (%)	Size of Loss (weeks)	Risk Exposure (weeks)
Overly optimistic schedule	50%	5	2.5
Additional features added by marketing (specific features unknown)	35%	8	2.8
Project approval takes longer than expected	25%	4	1.0
Management-level progress reporting takes more developer time than expected	10%	1	0.1
New programming tools do not produce the promised savings	30%	5	1.5
...	...	...	...
Total			12

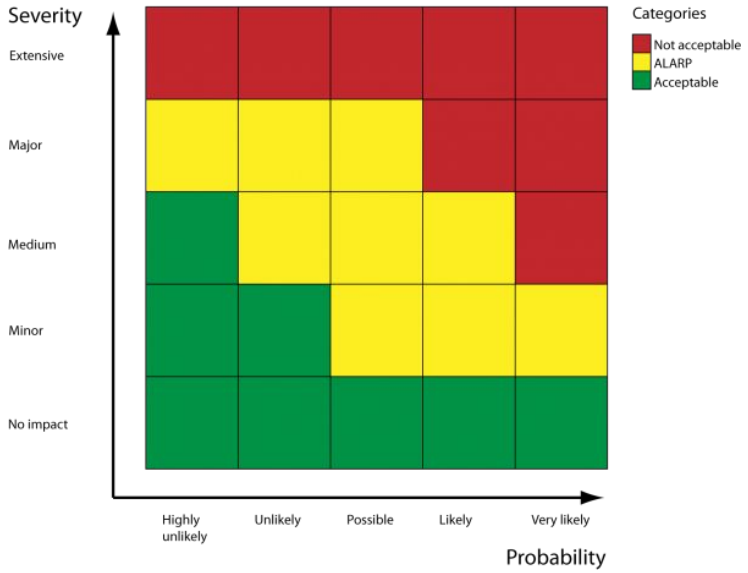
Exercise: Risk Analysis

- What is the risk probability and severity for your scooter app?

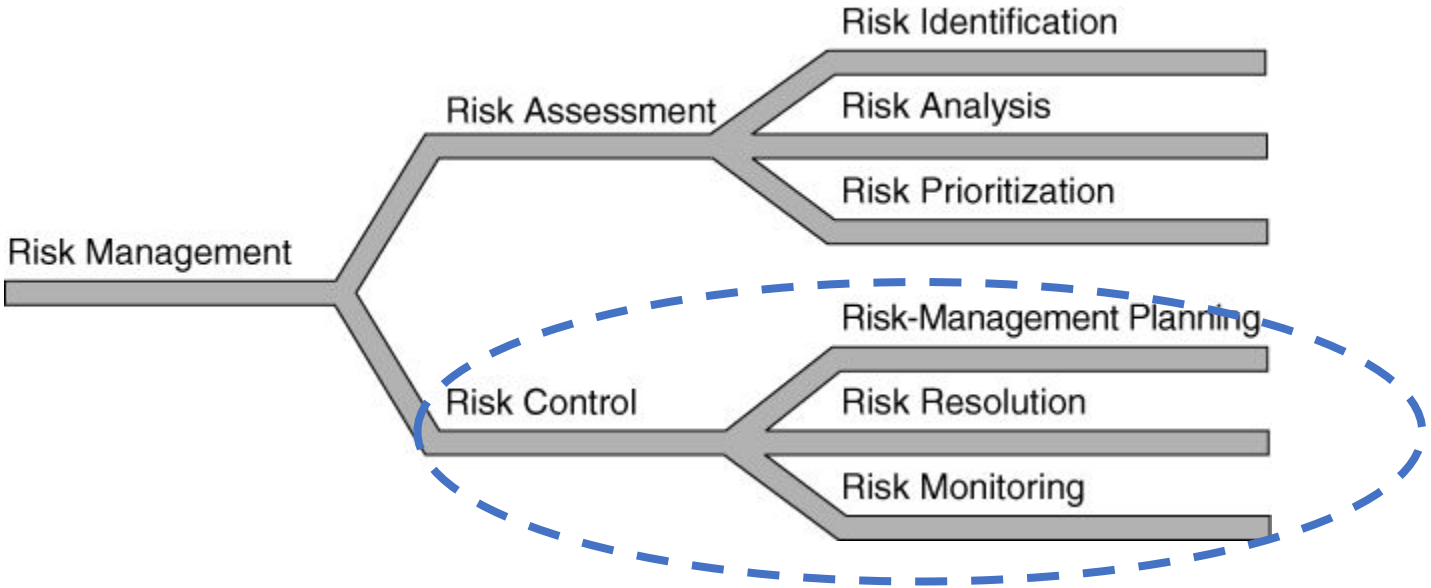
  Frequent, Probable, Not so often, almost never
  Extensive, Major, Medium, Minor, No Impact



Risk Prioritization
Focus on risks with the highest exposure



Risk Management

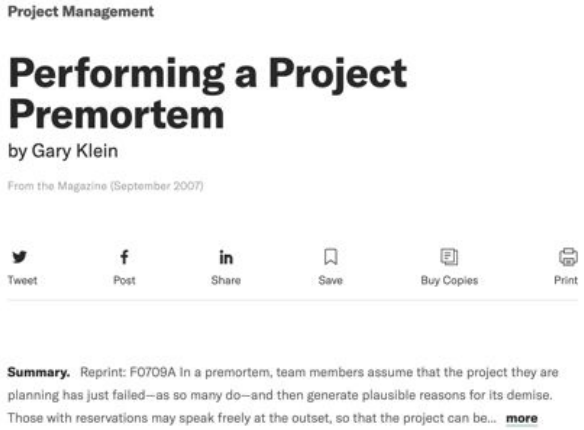


Risk Control

- What steps can be taken to avoid or mitigate the risk?
- Can you better understand and forecast the risk?
- Who will be responsible for monitoring and addressing the risk?
- Have risks evolved over time?
- Bake risks into your schedule
  - Don’t assume that nothing will go wrong between now and the end of the semester!

Pre-mortems

- "unlike a typical critiquing session, in which project team members are asked what *might* go wrong, the premortem operates on the assumption that the 'patient' has died, and so asks what *did* go wrong."



Project Management

Performing a Project Premortem

by Gary Klein

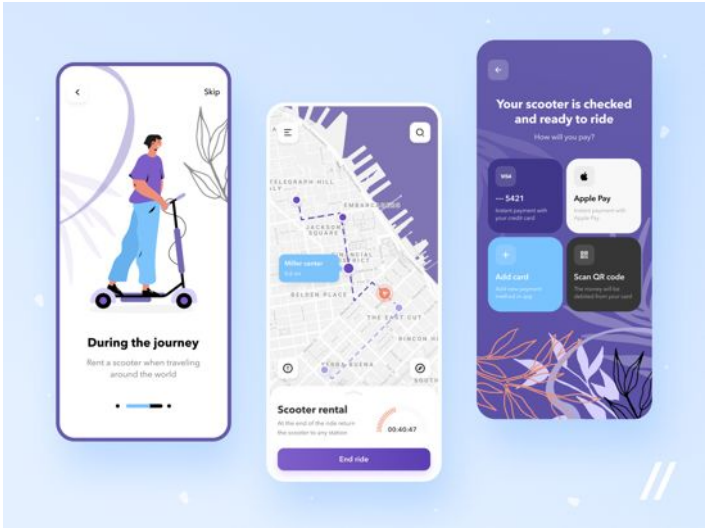
From the Magazine (September 2007)

Tweet Post Share Save Buy Copies Print

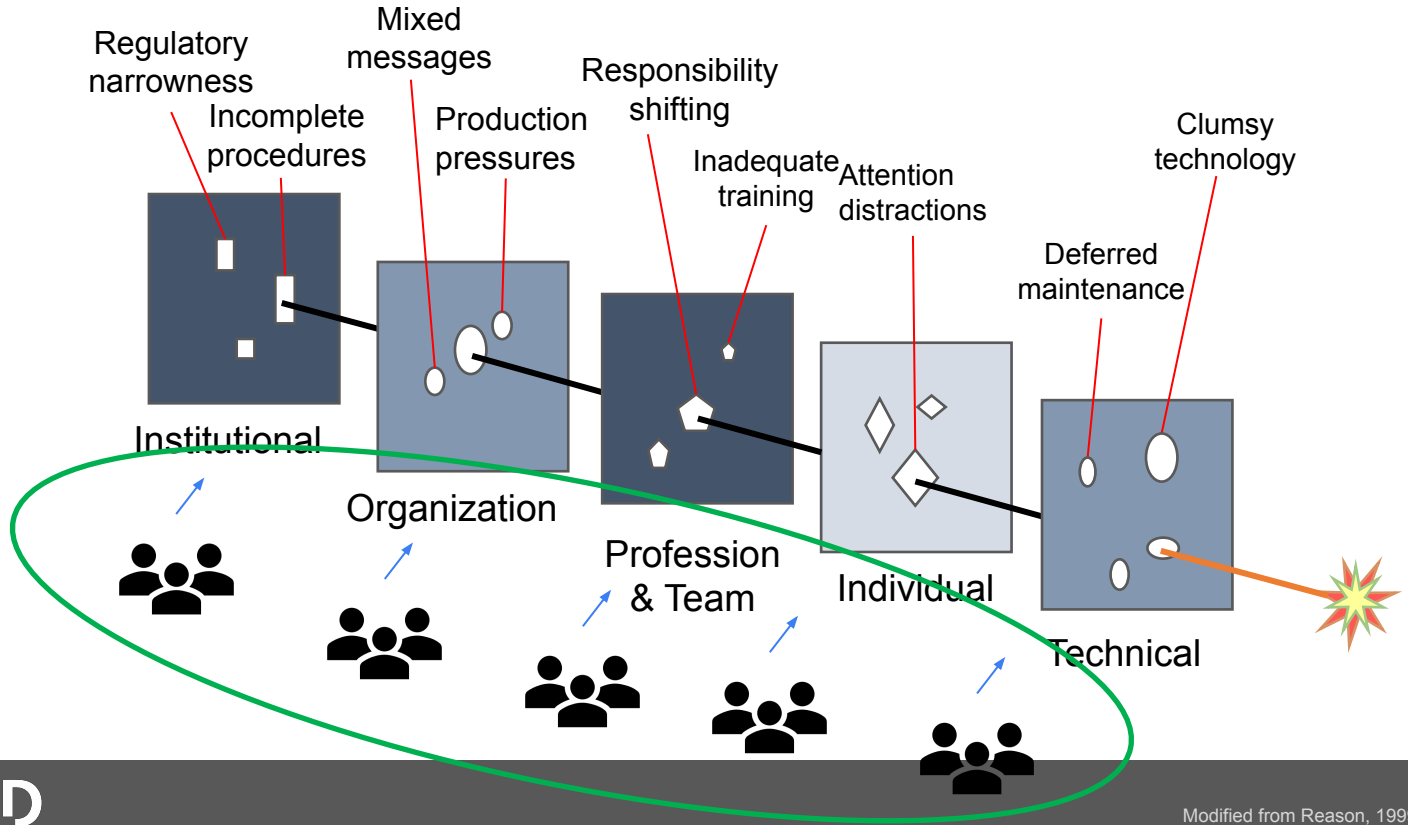
Summary. Reprint: F0709A In a premortem, team members assume that the project they are planning has just failed—as so many do—and then generate plausible reasons for its demise. Those with reservations may speak freely at the outset, so that the project can be... **more**

Discussion: Risk Elimination and Mitigation

- How can you eliminate/mitigate risk for your scooter app?

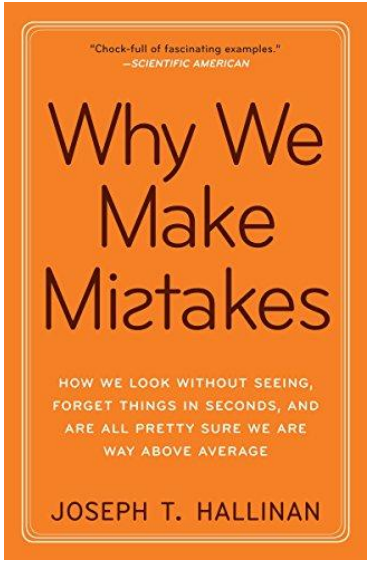


The Swiss cheese model



Can we remove human error?

Why do we make mistakes?



Generalization

- …in the words of psychologist Tom Stafford, we can't find our typos because we're engaging in a high-level task in writing. **Our brains generalize simple, component parts to focus on complex tasks**, so essentially we can't catch the small details because we're focused on a large task.

https://medium.com/swlh/why-we-miss-our-own-typos-96ab2f06afb7

Boredom can give rise to errors, adverse patient events, and decreased productivity—costly and unnecessary outcomes for consumers, employees, and organizations alike. As a function of boredom, individuals may feel over-worked or under-employed, and become distracted, stressed, or disillusioned. Staff who are bored also are less likely to engage with or focus on their work.

Original Articles

Boredom in the Workplace: Reasons, Impact, and Solutions

Michelle Cleary , PhD, RN, Jan Sayers , PhD, RN, Violeta Lopez , PhD, RN & Catherine Hungerford , PhD, RN

Pages 83-89 | Received 24 Jun 2015, Accepted 13 Aug 2015, Published online: 10 Feb 2016

Download citation https://doi.org/10.3109/01612840.2015.1084554 Check for updates

Full Article Figures & data References Citations Metrics Reprints & Permissions Get access

Abstract

Boredom in the workplace is not uncommon, and has been discussed widely in the academic literature in relation to the associated costs to individuals and organizations. Boredom can give rise to errors, adverse patient events, and decreased productivity—costly and unnecessary outcomes for consumers, employees, and organizations alike. As a function of boredom, individuals may

Related rese

People also read

Boredom at work spillover model work motivation boredom

Cognitive Load

- ..." students who switch back and forth between attending to a classroom lecture and checking e-mail, Facebook, and IMing with friends"

Computers & Education 62 (2013) 24–31

Contents lists available at SciVerse ScienceDirect

Computers & Education

journal homepage: www.elsevier.com/locate/compedu

Laptop multitasking hinders classroom learning for both users and nearby peers

Faria Sana [a], Tina Weston [b,c], Nicholas J. Cepeda [b,c,*]

[a] McMaster University, Department of Psychology, Neuroscience, & Behaviour, 1280 Main Street West, Hamilton, ON L8S 4K1, Canada
[b] York University, Department of Psychology, 4700 Keele Street, Toronto, ON M3J 1P3, Canada
[c] York University, LaMarsh Centre for Child and Youth Research, 4700 Keele Street, Toronto, ON M3J 1P3, Canada

ARTICLE INFO

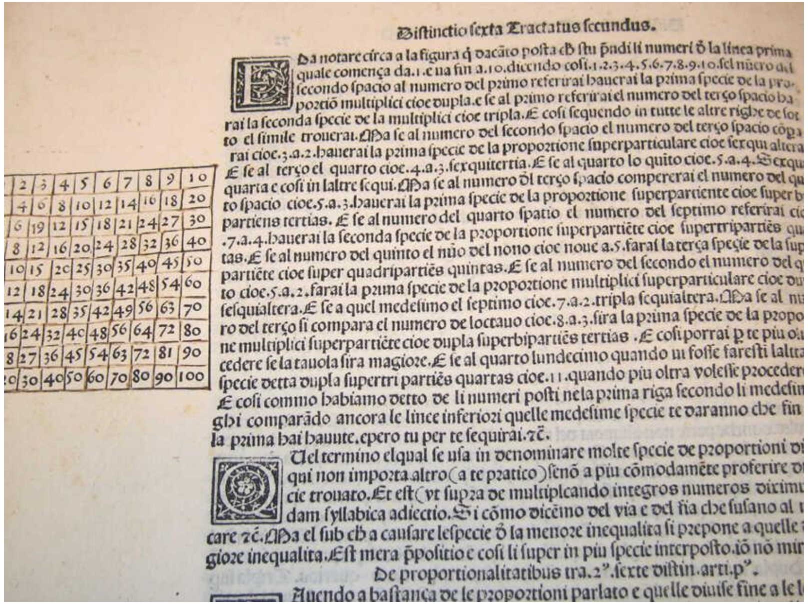
ABSTRACT

catch

Can we ~~remove~~ human error?

Can we catch human error before we ship our code?

Can we automate tasks to prevent problems?



Distinctio sexta Tractatus secundus.

Da notare circa a la figura q dacato posta ch sono pandi li numeri o la linea prima
quale comença da.1.e ua fin a.10.dicendo cosi.1.2.3.4.5.6.7.8.9.10.sel nuero del
secondo spacio al numero del primo referirai hauerai la prima specie de la pro-
portio multiplici cioe dupla.e se al primo referirai el numero del terço spacio ha
rai la seconda specie de la multiplici cioe tripla.E cosi sequendo in tutte le altre righe de sot
to el simile trouerai.Ma se al numero del secondo spacio el numero del terço spacio copa
rai cioe.3.a.2.hauerai la prima specie de la proportione superparticulare cioe serqui altera
E se al terço el quarto cioe.4.a.3.sexquitertia.E se al quarto lo quito cioe.5.a.4.Sexqu
quarta e cosi in laltre sequi.Ma se al numero dl terço spacio comperarai el numero del qu
to spacio cioe.5.a.3.hauerai la prima specie de la proportione superpartiente cioe super b
partiens tertias. E se al numero del quarto spatio el numero del septimo referirai cio
.7.a.4.hauerai la seconda specie de la proportione superpartiete cioe supertripartiēs qu
tas.E se al numero del quinto el nūo del nono cioe noue a.5.farai la terça spegie de la sup
partiete cioe super quadripartiēs quintas.E se al numero del secondo el numero del q
to cioe.5.a.2.farai la prima specie de la proportione multiplici superparticulare cioe du
sesquialtera.E se a quel medesimo el septimo cioe.7.a.2.tripla sequialtera.Ma se al nu
ro del terço si compara el numero de loctauo cioe.8.a.3.sira la prima specie de la propo
ne multiplici superpartiete cioe dupla superbipartiēs tertias .E cosi porrai p te piu o
cedere se la tauola sira magiore.E se al quarto lundecimo quando ui fosse faresti laltra
specie detta dupla supertri partiēs quartas cioe.11.quando piu oltra volesse proceder
E cosi commo habiamo detto de li numeri posti ne la prima riga secondo li medesim
ghi comparādo ancora le linee inferiori quelle medesime specie te daranno che fin
la prima hai hauute.epero tu per te sequirai.7c.

Uel termino elqual se usa in denominare molte specie de proportioni d
qui non importa altro(a te pratico)senō a piu cōmodamēte proferire d
cie trouato.Et est(vt supra de multiplcando integros numeros diximu
dam syllabica adiectio.Si cōmo dicēmo del via e del fia che susano al
care 7c.Ma el sub ch a causare lespecie o la menore inequalita si prepone a quelle
giore inequalita.Est mera ppositio e cosi li super in piu specie interposto.io no mir

De proportionalitatibus tra.2°.sexte distin.arti.p°.

Auendo a bastança de le proportioni parlato e quelle diuise fine a le l

2	3	4	5	6	7	8	9	10
4	6	8	10	12	14	16	18	20
6	19	12	15	18	21	24	27	30
8	12	16	20	24	28	32	36	40
10	15	20	25	30	35	40	45	50
12	18	24	30	36	42	48	54	60
14	21	28	35	42	49	56	63	70
16	24	32	40	48	56	64	72	80
8	27	36	45	54	63	72	81	90
20	30	40	50	60	70	80	90	100

Double entry accounting

SINGLE ENTRY

Details	Date	Income	Expenses	Balance
Building Loan	7/1		2200	26800
Utilities	7/1		950	25850

DOUBLE ENTRY

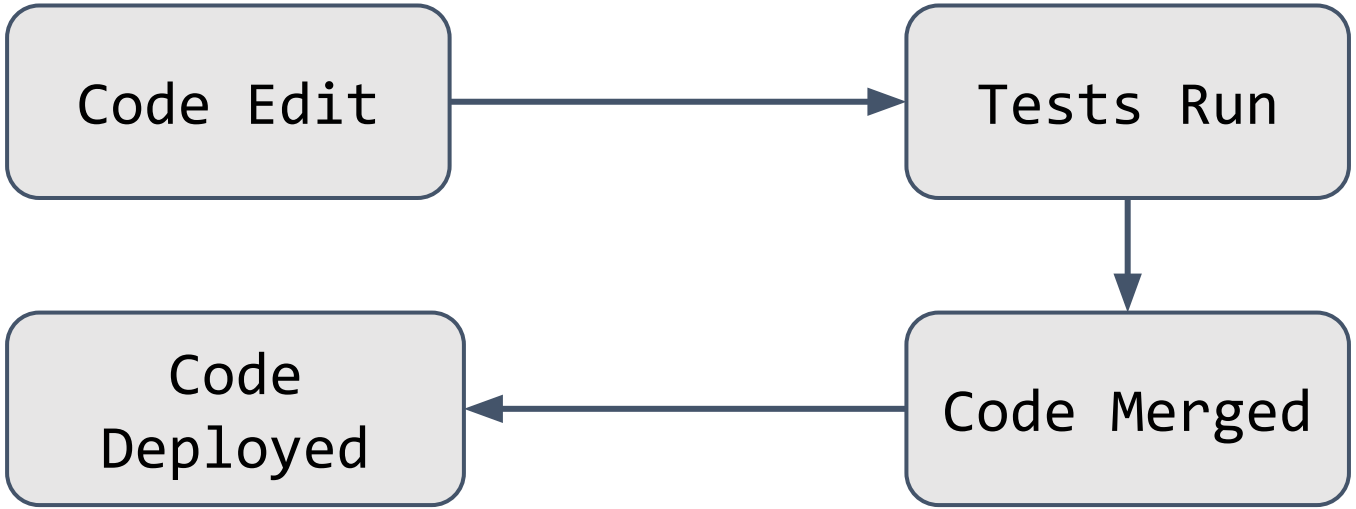
Details	Date	Fund/Account	Credit	Debit	Assets		Liabilities	Balance
					Cash	Other		
					$75,000	$9,000	$55,000	$29,000
Building Loan	7/1	Mortgage Company	$2,200				$52,800	
		Building Fund		$2,200	$47,800			$26,800
Utilities	7/1	Local Electric & Water Coop	$950					
		Building Fund		$950	$46,850			$25,850

Approach:

Automate what we can

Review what we cannot

CI/CD Pipeline overview



Continuous Integration:

Catch mistakes before you push your code!

History of CI

(1999) Extreme Programming (XP) rule: “Integrate Often”

(2000) Martin Fowler posts “Continuous Integration” blog

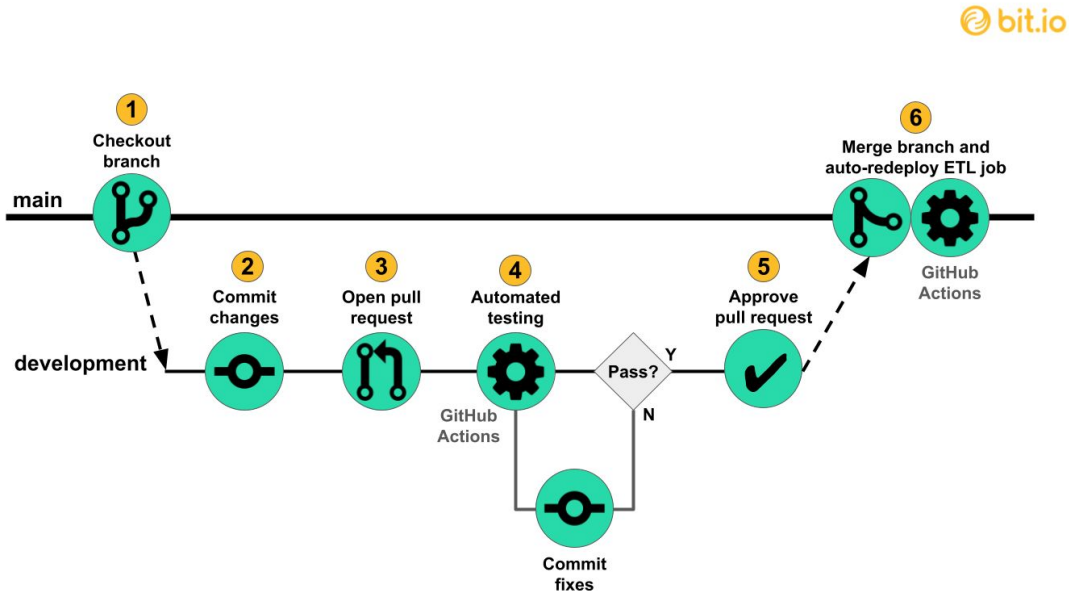
(2001) First CI tool

(2005) Hudson/Jenkins

(2011) Travis CI

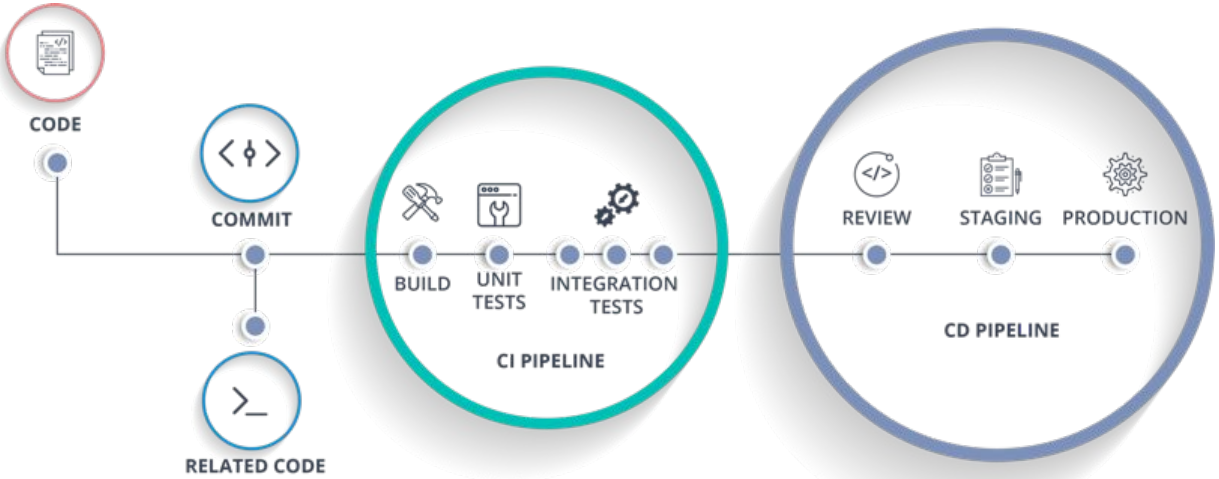
(2019) GitHub Actions

Example CI Workflow



Source: https://innerjoin.bit.io/making-a-simple-data-pipeline-part-4-ci-cd-with-github-actions-733251f211a6

Example CI/CD Workflow



CI Research

Trade-Offs in Continuous Integration: Assurance, Security, and Flexibility

Michael Hilton
Oregon State University, USA
mhilton@cmu.edu

Nicholas Nelson
Oregon State University, USA
nelsonni@oregonstate.edu

Timothy Tunnell
University of Illinois, USA
tunnell2@illinois.edu

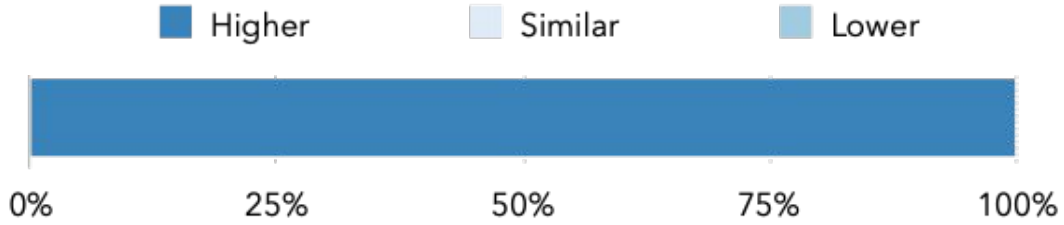
Darko Marinov
University of Illinois, USA
marinov@illinois.edu

Danny Dig
Oregon State University, USA
digd@oregonstate.edu

"523 complete responses, and a total of 691 survey responses from over 30 countries. Over 50% of our participants had over 10 years of software development experience, and over 80% had over 4 years of experience."

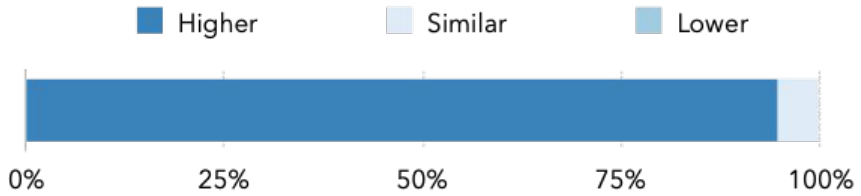
Developers report:

Do developers on projects with CI give (more/similar/less) value to automated tests?



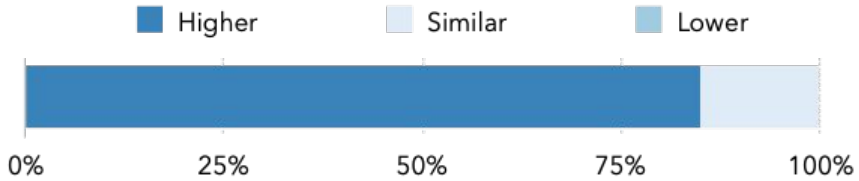
Developers report:

Do developers on projects with CI give (more/similar/less) value to automated tests?
Do projects with CI have (higher/similar/lower) test quality?



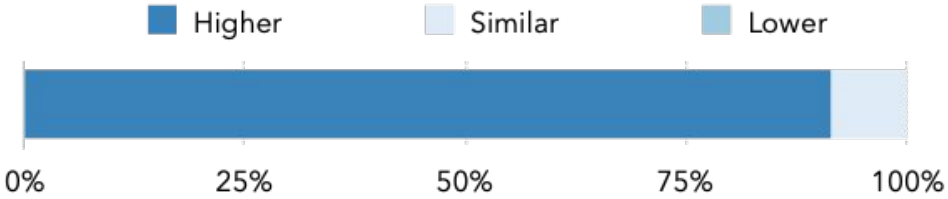
Developers report:

Do developers on projects with CI give (more/similar/less) value to automated tests?
Do projects with CI have (higher/similar/lower) test quality?
Do projects with CI have (higher/similar/lower) code quality?



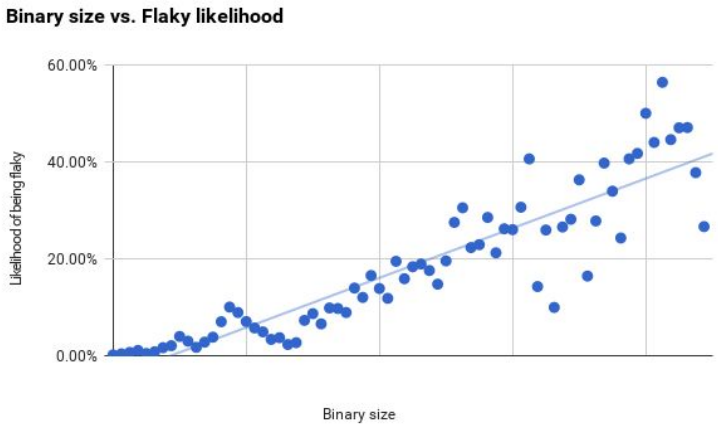
Developers report:

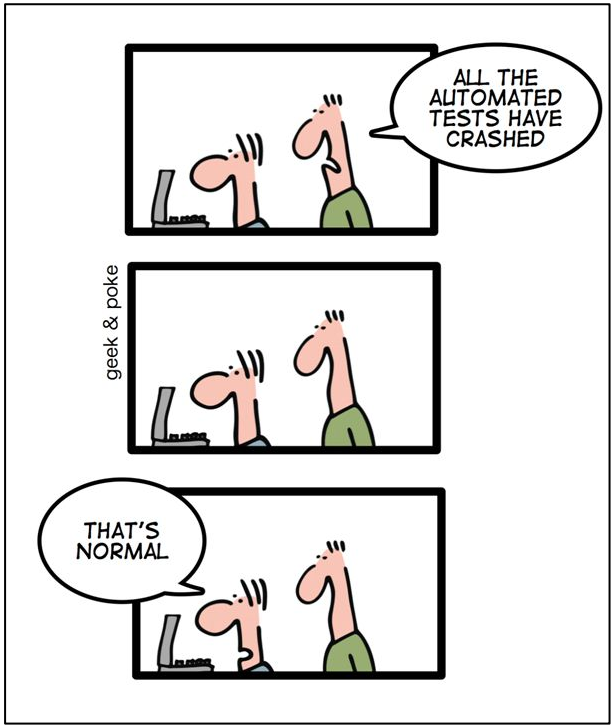
Do developers on projects with CI give (more/similar/less) value to automated tests?
Do projects with CI have (higher/similar/lower) test quality?
Do projects with CI have (higher/similar/lower) code quality?
Are developers on projects with CI (more/similar/less) productive?



Challenge: Flaky Tests

"Google has around 4.2 million tests that run on our continuous integration system. Of these, around 63 thousand have a flaky run over the course of a week"





https://testing.googleblog.com/2017/04/where-do-our-flaky-tests-come-from.html

Observation

CI helps us catch errors before others see them

For problems we can’t easily automate, we can perform code review

Risk Analysis

- **Probability** a human makes a mistake: **Very Likely**
- **Severity**: ranges, but could be extensive

Solution:

Use **CI** to catch your mistakes, make you look better, and mitigate your risks!

Use **code reviews** to teach and learn

(***next lecture***)