Requirements and Specifications (Part 1/2)

Martin Kellogg

Requirements and Specifications (Part 1)

Today's agenda:

- **Reading Quiz**
- Post-mortem on Gradescope outage this weekend
- What are specifications, and why do we care?
- In-class exercise

[with thanks to Michael D. Ernst for the GroupThink Specification Exercise]

Reading Quiz: Reqs and Specs (1)

Reading Quiz: Reqs and Specs (1)

Q1: When the author of “How to be a Program Manager” was an Excel PM, his job mostly involved:

A. talking to people
B. programming
C. both of these in about equal amounts

Q2: Google’s design docs typically list “non-goals”. A “non-goal” is:

A. something the system definitely must not do
B. something undesirable, that the designers would prefer that the system not do (but if it’s needed to achieve other goals, that’s ok)
C. something desirable, but not a priority

Reading Quiz: Reqs and Specs (1)

Q1: When the author of “How to be a Program Manager” was an Excel PM, his job mostly involved:

A. talking to people
B. programming
C. both of these in about equal amounts

Q2: Google’s design docs typically list “non-goals”. A “non-goal” is:

A. something the system definitely must not do
B. something undesirable, that the designers would prefer that the system not do (but if it’s needed to achieve other goals, that’s ok)
C. something desirable, but not a priority

Reading Quiz: Reqs and Specs (1)

Q1: When the author of “How to be a Program Manager” was an Excel PM, his job mostly involved:

A. talking to people
B. programming
C. both of these in about equal amounts

Q2: Google’s design docs typically list “non-goals”. A “non-goal” is:

A. something the system definitely must not do
B. something undesirable, that the designers would prefer that the system not do (but if it’s needed to achieve other goals, that’s ok)
C. something desirable, but not a priority

Requirements and Specifications (Part 1)

Today's agenda:

- Reading Quiz
- **Post-mortem on Gradescope outage this weekend**
- What are specifications, and why do we care?
- In-class exercise

[with thanks to Michael D. Ernst for the GroupThink Specification Exercise]

Gradescope outage post-mortem

- First: what's a **post-mortem**?

Post-mortems

Definition: a ***postmortem*** or ***post-mortem*** (from Latin for “after death”) is a written record of an incident, its impact, the actions taken to mitigate or resolve it, the root cause(s), and the follow-up actions to prevent the incident from recurring

Post-mortems

Definition: a ***postmortem*** or ***post-mortem*** (from Latin for “after death”) is a written record of an incident, its impact, the actions taken to mitigate or resolve it, the root cause(s), and the follow-up actions to prevent the incident from recurring

- **writing** the postmortem is a good way to **fully understand** what caused an emergency (cf., “writing clarifies your thinking”)

Post-mortems

Definition: a ***postmortem*** or ***post-mortem*** (from Latin for “after death”) is a written record of an incident, its impact, the actions taken to mitigate or resolve it, the root cause(s), and the follow-up actions to prevent the incident from recurring

- **writing** the postmortem is a good way to **fully understand** what caused an emergency (cf., “writing clarifies your thinking”)
- good postmortems are **blameless** and **actionable**:

Post-mortems

Definition: a ***postmortem*** or ***post-mortem*** (from Latin for “after death”) is a written record of an incident, its impact, the actions taken to mitigate or resolve it, the root cause(s), and the follow-up actions to prevent the incident from recurring

- **writing** the postmortem is a good way to **fully understand** what caused an emergency (cf., “writing clarifies your thinking”)
- good postmortems are **blameless** and **actionable**:
  - “**blameless**” = find the faults in the process, not the people

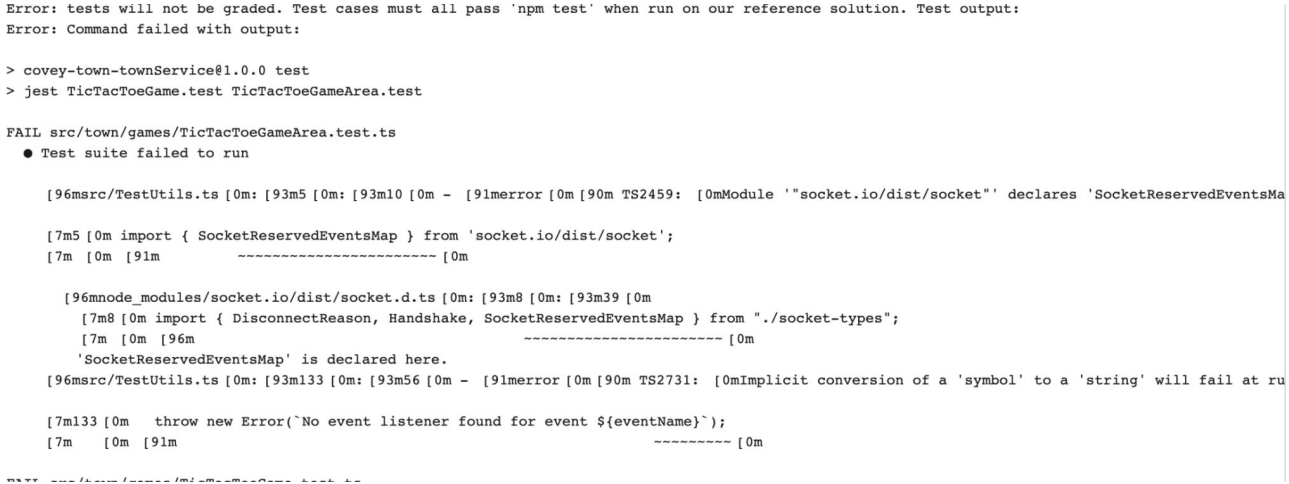
Post-mortems

Definition: a ***postmortem*** or ***post-mortem*** (from Latin for “after death”) is a written record of an incident, its impact, the actions taken to mitigate or resolve it, the root cause(s), and the follow-up actions to prevent the incident from recurring

- **writing** the postmortem is a good way to **fully understand** what caused an emergency (cf., “writing clarifies your thinking”)
- good postmortems are **blameless** and **actionable**:
  - “**blameless**” = find the faults in the process, not the people
  - “**actionable**” = give specific guidance for how to avoid the problem in the future (these become tickets)

Gradescope outage post-mortem

- First: what's a **post-mortem**?
- **Outage description:** starting Saturday morning at ~5:00am eastern time, Gradescope refused to run IP1 tests with the following error:



```
Error: tests will not be graded. Test cases must all pass 'npm test' when run on our reference solution. Test output:
Error: Command failed with output:

> covey-town-townService@1.0.0 test
> jest TicTacToeGame.test TicTacToeGameArea.test

FAIL src/town/games/TicTacToeGameArea.test.ts
  ● Test suite failed to run

    [96msrc/TestUtils.ts[0m:[93m5[0m:[93m10[0m - [91merror[0m[90m TS2459: [0mModule '"socket.io/dist/socket"' declares 'SocketReservedEventsMa

    [7m5[0m import { SocketReservedEventsMap } from 'socket.io/dist/socket';
    [7m [0m [91m         ~~~~~~~~~~~~~~~~~~~~~~~[0m

      [96mnode_modules/socket.io/dist/socket.d.ts[0m:[93m8[0m:[93m39[0m
        [7m8[0m import { DisconnectReason, Handshake, SocketReservedEventsMap } from "./socket-types";
        [7m [0m [96m                                      ~~~~~~~~~~~~~~~~~~~~~~~[0m
        'SocketReservedEventsMap' is declared here.
    [96msrc/TestUtils.ts[0m:[93m133[0m:[93m56[0m - [91merror[0m[90m TS2731: [0mImplicit conversion of a 'symbol' to a 'string' will fail at ru

    [7m133[0m    throw new Error(`No event listener found for event ${eventName}`);
    [7m    [0m [91m                                                       ~~~~~~~~~[0m
```

Gradescope outage post-mortem

- First: what's a **post-mortem**?
- **Outage description**
- **Root cause**: covey.town's dependency socket.io released a new version (4.8.0) at ~4:00am eastern on Saturday. This version contained unexpected breaking changes in the typescript definitions.
    - the autograder automatically picked up the change, causing the test utilities not to compile

Gradescope outage post-mortem

- First: what's a **post-mortem**?
- **Outage description**
- **Root cause**
- **Resolution**: I became aware of the incident on Monday afternoon and deployed a new autograder that uses the old version

Gradescope outage post-mortem

- First: what's a **post-mortem**?
- **Outage description**
- **Root cause**
- **Resolution**
- **What went wrong**
  - I wasn't reachable by anyone with visibility into the incident
  - There wasn't automated monitoring that alerted me, either

Gradescope outage post-mortem

- First: what's a **post-mortem**?
- **Outage description**
- **Root cause**
- **Resolution**
- **What went wrong**
  - I wasn't reacha
  - There wasn't a

These are process/monitoring problems:

- the TAs should've had a way to page me, even if I was offline (I was sick)
- Gradescope should be set up to automatically notify the course staff when everyone's getting zeroes

Gradescope outage post-mortem

- First: what's a **post-mortem**?
- **Outage description**
- **Root cause**
- **Resolution**
- **What went wrong**
- **Action items**:
  - I'll give the TAs a direct way to reach me
    - I'll also add this to the course setup manual so that next semester I remember to do it!
  - I'll look into automatic monitoring for Gradescope

Other reminders

- IP1 submissions are still open: you can use late days until Thursday AoE
  - We'll use your latest submission and count late days automatically. Individual and project late days are separate.

Other reminders

- IP1 submissions are still open: you can use late days until Thursday AoE
  - We'll use your latest submission and count late days automatically. Individual and project late days are separate.
- IP2 isn't due until October 14. However, you should start now:
  - The project plan first draft is due October 7. If you wait until October 8 to start IP2, you probably won't finish in time.

Other reminders

- IP1 submissions are still open: you can use late days until Thursday AoE
  - We'll use your latest submission and count late days automatically. Individual and project late days are separate.
- IP2 isn't due until October 14. However, you should start now:
  - The project plan first draft is due October 7. If you wait until October 8 to start IP2, you probably won't finish in time.
- Fill out the project team formation survey by AoE today to get a free reading quiz credit
  - teams formed tomorrow

Requirements and Specifications (Part 1)

Today's agenda:

- Reading Quiz
- Post-mortem on Gradescope outage this weekend
- **What are specifications, and why do we care?**
- In-class exercise

[with thanks to Michael D. Ernst for the GroupThink Specification Exercise]

Specifications tell you what to do (but not how to do it)

- **A perfect implementation is no good if it solves the wrong problem**
- **It's difficult to create a specification that is**
  - complete
  - consistent
  - precise
  - concise

[with thanks to Michael D. Ernst for the GroupThink Specification Exercise]

Bundestag Sound System, 1992

- **No sound from speakers in new building**
  - system requirement: no feedback
  - new all-glass room

- **"This glass does not absorb the sound. The computers, detecting feedback, turn down the volume. A steady state is only achieved when the microphones are turned off."**

  Dr. Debora Weber-Wulff

[with thanks to Michael D. Ernst for the GroupThink Specification Exercise]

Ariane 5 launch vehicle, 1996

- **Went off course during launch**
  - Ariane 4 guidance software reused in Ariane 5
  - Ariane 5 accelerated much faster
  - velocity variable overflowed, computer crashed

- **"The failure of the Ariane 501 was caused by the complete loss of guidance and attitude information... due to specification and design errors in the software."**

  ESA Inquiry Board

Mars Polar Lander, 1999

- **Crashed while landing on Mars**
  - sensor transient when legs deployed
  - software thought vehicle had landed
  - engine shut down during descent

- **"There was no software requirement to clear spurious signals prior to using the sensor information to determine that landing had occurred."**

  Mars program independent assessment team

Specifications matter

- **A specification:**
  - connects customer and engineer
  - ensures parts of implementation work together
  - defines correctness of implementation
- **Therefore everyone must understand specs**
  - Designers, implementers, testers, managers, marketing, technical support, … users!
- **Good specifications are essential**

[with thanks to Michael D. Ernst for the GroupThink Specification Exercise]

Requirements and Specifications (Part 1)

Today's agenda:

- Reading Quiz
- Post-mortem on Gradescope outage this weekend
- What are specifications, and why do we care?
- **In-class exercise**

[with thanks to Michael D. Ernst for the GroupThink Specification Exercise]

Groupthink Specification Exercise

[with thanks to Michael D. Ernst for the GroupThink Specification Exercise]

Groupthink game

As a group, specify behavior of a desktop telephone

Individually, answer questions about its behavior

Goal: all group members give same answer

- No defaults based on the game (e.g., "always A")

The winning group receives a prize

[with thanks to Michael D. Ernst for the GroupThink Specification Exercise]

Desktop telephone

Handset (speaker and microphone)

Keypad

- `talk`
- `redial`
- `ansmachine`
- `end`

24-character display

Answering machine

Phone jack

[with thanks to Michael D. Ernst for the GroupThink Specification Exercise]

Requirements

Display indicates current functionality

- caller ID
- number being called
- "Answering machine"
- "Ready"

Answering machine picks up after 2 rings

You decide other aspects of system behavior

[with thanks to Michael D. Ernst for the GroupThink Specification Exercise]

Definitions

Lineidle: phone is on-hook (“hung up”)

- sent from phone to phoneline

Lineactive: phone is off-hook (“picked up”)

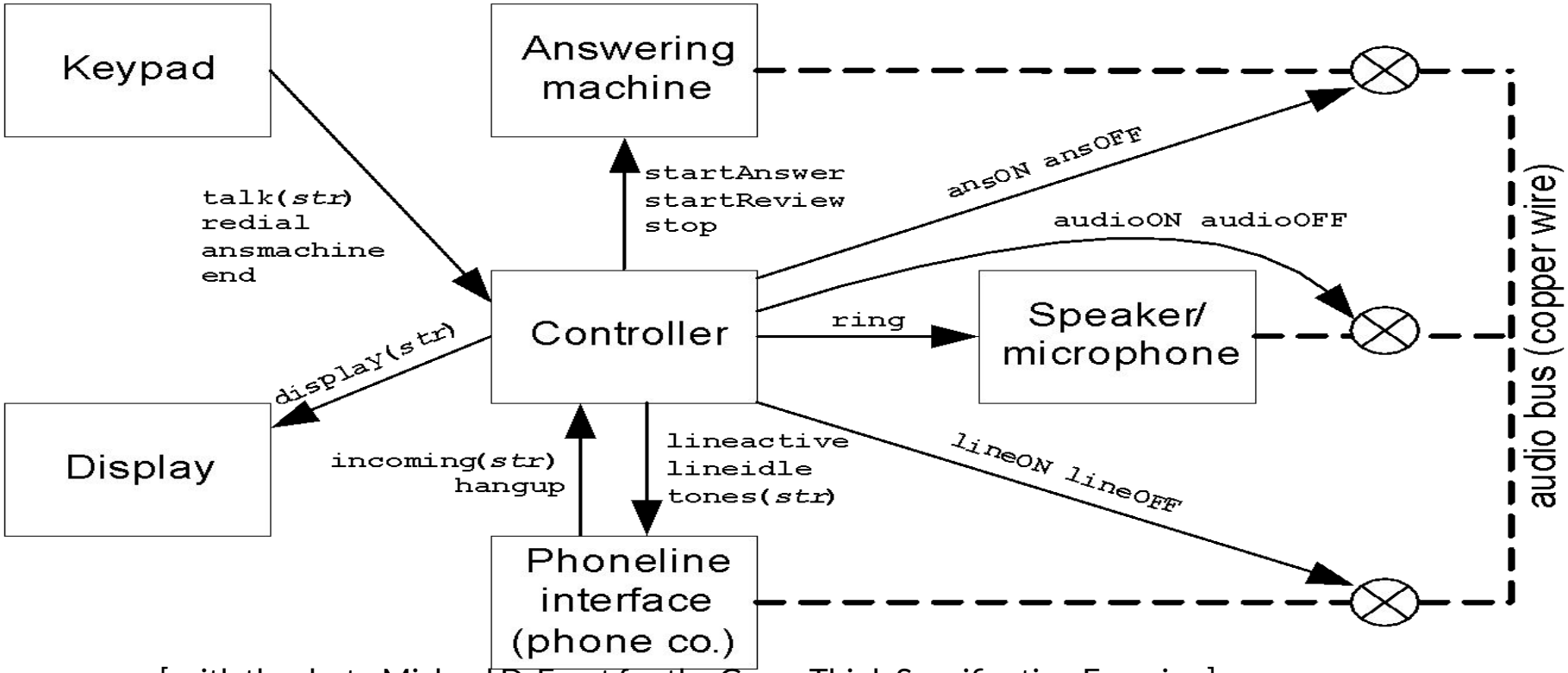
- sent from phone to phoneline

Ring signal: causes phone to ring once

- sent from phoneline to phone

[with thanks to Michael D. Ernst for the GroupThink Specification Exercise]

System architecture



[with thanks to Michael D. Ernst for the GroupThink Specification Exercise]

Sample question

The user is connected to an outside party. The outside party hangs up. What state is the phoneline in?

A. Lineactive (the user hears dialtone)

B. Lineidle (the user does not hear dialtone)

[with thanks to Michael D. Ernst for the GroupThink Specification Exercise]

Question 0