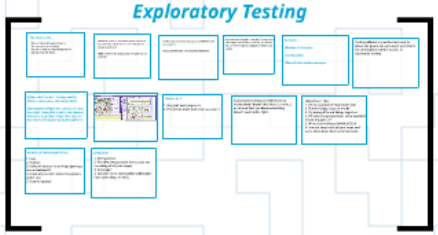
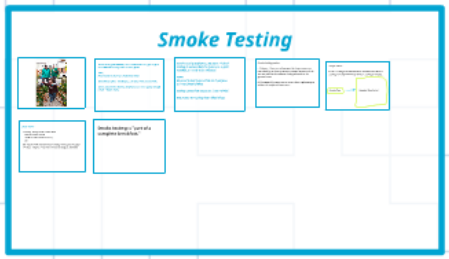
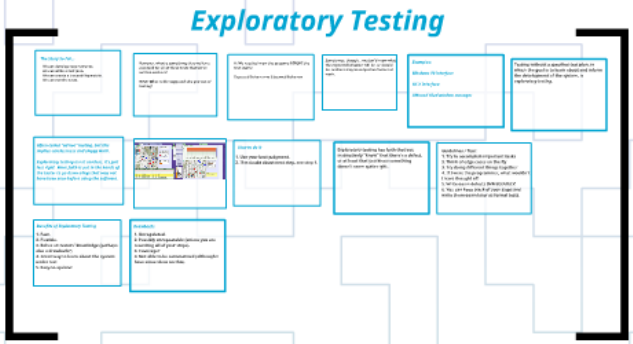
Let's Get Informal: Exploratory, Smoke and Stochastic Testing



Let's Get Informal: Exploratory, Smoke and Stochastic Testing





Exploratory Testing

The Story So Far...

We can develop requirements.
We can write a test plan.
We can create a traceability matrix.
We can run the tests.

However, what is something that we have assumed for all of these tests that we've written and run?

HINT: What is the supposed *sine qua non* of testing?

A: We need to know the outcome BEFORE the test starts!

Expected Behavior vs Observed Behavior

Sometimes, though... we don't know what the expected behavior will be, or should be, or there may be subjective factors at work.

Examples:

Windows 10 interface

OS X interface

XMonad tiled window manager

Testing without a specified test plan, in which the goal is to learn about and inform the development of the system, is *exploratory testing*.

Often called "ad hoc" testing, but this implies carelessness and sloppy work.

Exploratory testing is not careless, it's just less rigid. More faith is put in the hands of the tester to go down alleys that may not have been seen before using the software.

How to do it

1. Use your best judgment.
2. If in doubt about next step, see step 1.

Exploratory testing has faith that you instinctively "know" that there's a defect, or at least that you know something doesn't seem quite right.

Guidelines / Tips:
1. Try to accomplish important tasks
2. Think of edge cases on the fly
3. Try doing different things together
4. If I were the programmer, what wouldn't I have thought of?
5. Write down defects IMMEDIATELY!
6. You can keep track of your steps and write them down later as formal tests.

Benefits of Exploratory Testing

1. Fast.
2. Flexible.
3. Relies on testers' knowledge (perhaps also a drawback?)
4. Great way to learn about the system under test
5. Easy-to-update!

Drawbacks

1. Unregulated.
2. Possibly unrepeatable (unless you are recording all of your steps).
3. Coverage?
4. Not able to be automatized (although I have some ideas on this).

The Story So Far...

We can develop requirements.
We can write a test plan.
We can create a traceability matrix.
We can run the tests.

However, what is something that we have assumed for all of these tests that we've written and run?

HINT: What is the supposed *sine qua non* of testing?

A: We need to know the outcome BEFORE the test starts!

Expected Behavior vs Observed Behavior

Sometimes, though... we don't know what the expected behavior will be, or should be, or there may be subjective factors at work.

Examples:

Windows 10 interface

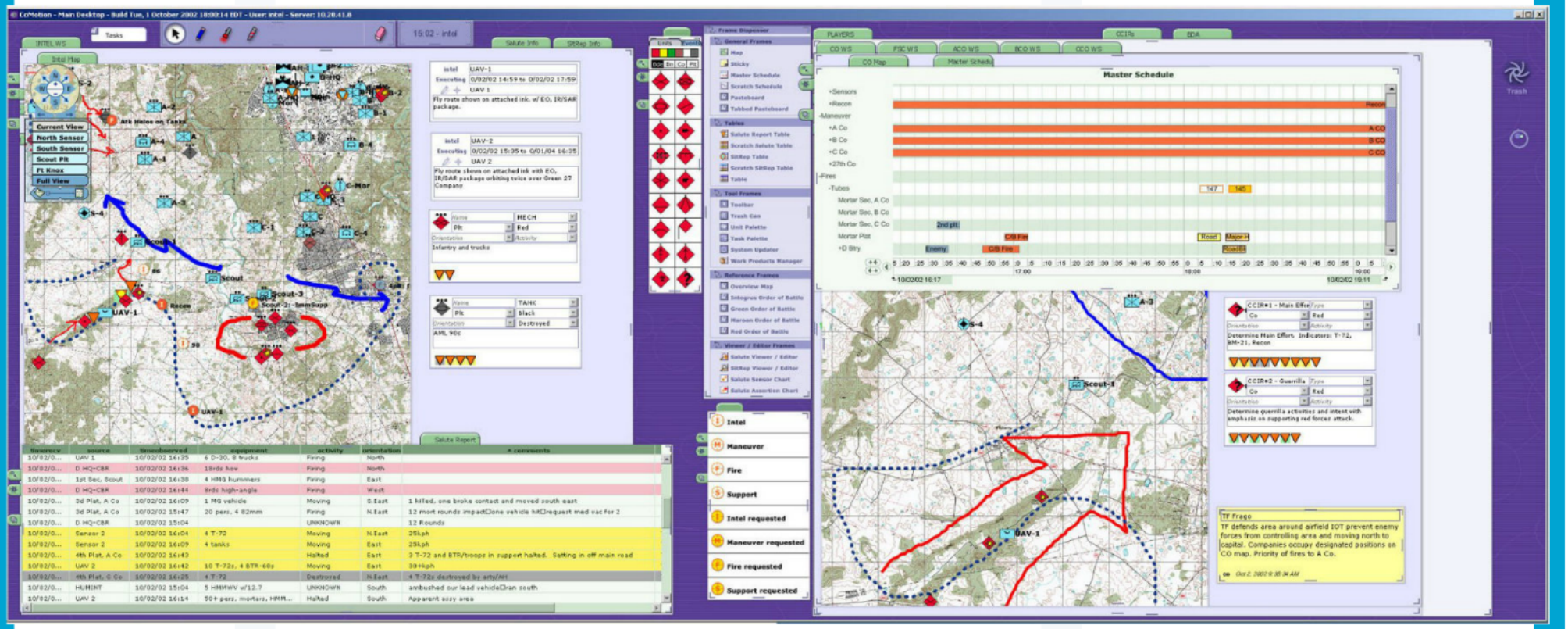
OS X interface

XMonad tiled window manager

Testing without a specified test plan, in which the goal is to learn about and inform the development of the system, is *exploratory testing*.

Often called "ad hoc" testing, but this implies carelessness and sloppy work.

Exploratory testing is not careless, it's just less rigid. More faith is put in the hands of the tester to go down alleys that may not have been seen before using the software.


CoMotion - Main Desktop - Build Tue, 1 October 2002 18:00:14 EDT - User: intel - Server: 10.20.41.8
Master Schedule
+Sensors
+Recon
-Maneuver
+A Co
+B Co
+C Co
+27th Co
-Fires
-Tubes
Mortar Sec, A Co
Mortar Sec, B Co
Mortar Sec, C Co
Mortar Plat
+D Btry
Intel
Maneuver
Fire
Support
Intel requested
Maneuver requested
Fire requested
Support requested
TF Frago
TF defends area around airfield IOT prevent enemy forces from controlling area and moving north to capital. Companies occupy designated positions on CO map. Priority of fires to A Co.

How to do it

1. Use your best judgment.
2. If in doubt about next step, see step 1.

Exploratory testing has faith that you instinctively "know" that there's a defect, or at least that you know something doesn't seem quite right.

Guidelines / Tips:

1. Try to accomplish important tasks
2. Think of edge cases on the fly
3. Try doing different things together
4. If I were the programmer, what wouldn't I have thought of?
5. Write down defects IMMEDIATELY!
6. You can keep track of your steps and write them down later as formal tests.

Benefits of Exploratory Testing

1. Fast.
2. Flexible.
3. Relies on testers' knowledge (perhaps also a drawback?)
4. Great way to learn about the system under test
5. Easy-to-update!

Drawbacks

1. Unregulated.
2. Possibly unrepeatable (unless you are recording all of your steps).
3. Coverage?
4. Not able to be automatized (although I have some ideas on this).

Smoke Testing

Smoke testing (PLUMBING): send smoke down the pipes to find leaks BEFORE sending water or other fluids.

WHY?
Much easier to clean up smoke than water.

Won't waste effort - hooking up to a water main is non-trivial.

Won't cause further damage (high-pressure water going through a hole -> bigger hole).

Smoke testing (software): Do some minimal testing to ensure that the system is, in fact, testable, or ready to be released.

WHY?
No need to test system that can't perform minimal functionality.

Setting up test harnesses etc. is non-trivial.

May waste time going down blind alleys.

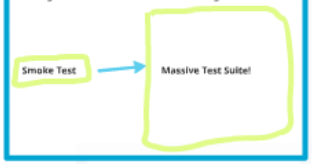
Smoke testing can be:

1. Scripted : There are a few small but important test cases (taking an hour or two to execute, at most) which are run prior to the software being released to the greater team.

2. Unscripted: An experienced tester does exploratory or ad hoc testing for an hour or so.

Keep in mind:

Smoke testing is an ADDITION to traditional software testing. It is a GATEWAY to further testing or release.



Media Check

A really, really basic smoke test:
Can the CD be read?
Do files exist on the server?
etc.

NB: Some texts use the term "sanity" testing for "smoke testing". I try to avoid this term as it may be offensive.

Smoke testing is "*part* of a complete breakfast."

Smoke testing (PLUMBING): send smoke down the pipes to find leaks BEFORE sending water or other fluids.

WHY?
Much easier to clean up smoke than water.

Won't waste effort - hooking up to a water main is non-trivial.

Won't cause further damage (high-pressure water going through a hole -> bigger hole).

Smoke testing (software): Do some minimal testing to ensure that the system is, in fact, testable, or ready to be released.

WHY?
No need to test system that can't perform minimal functionality.

Setting up test harnesses etc. is non-trivial.

May waste time going down blind alleys.

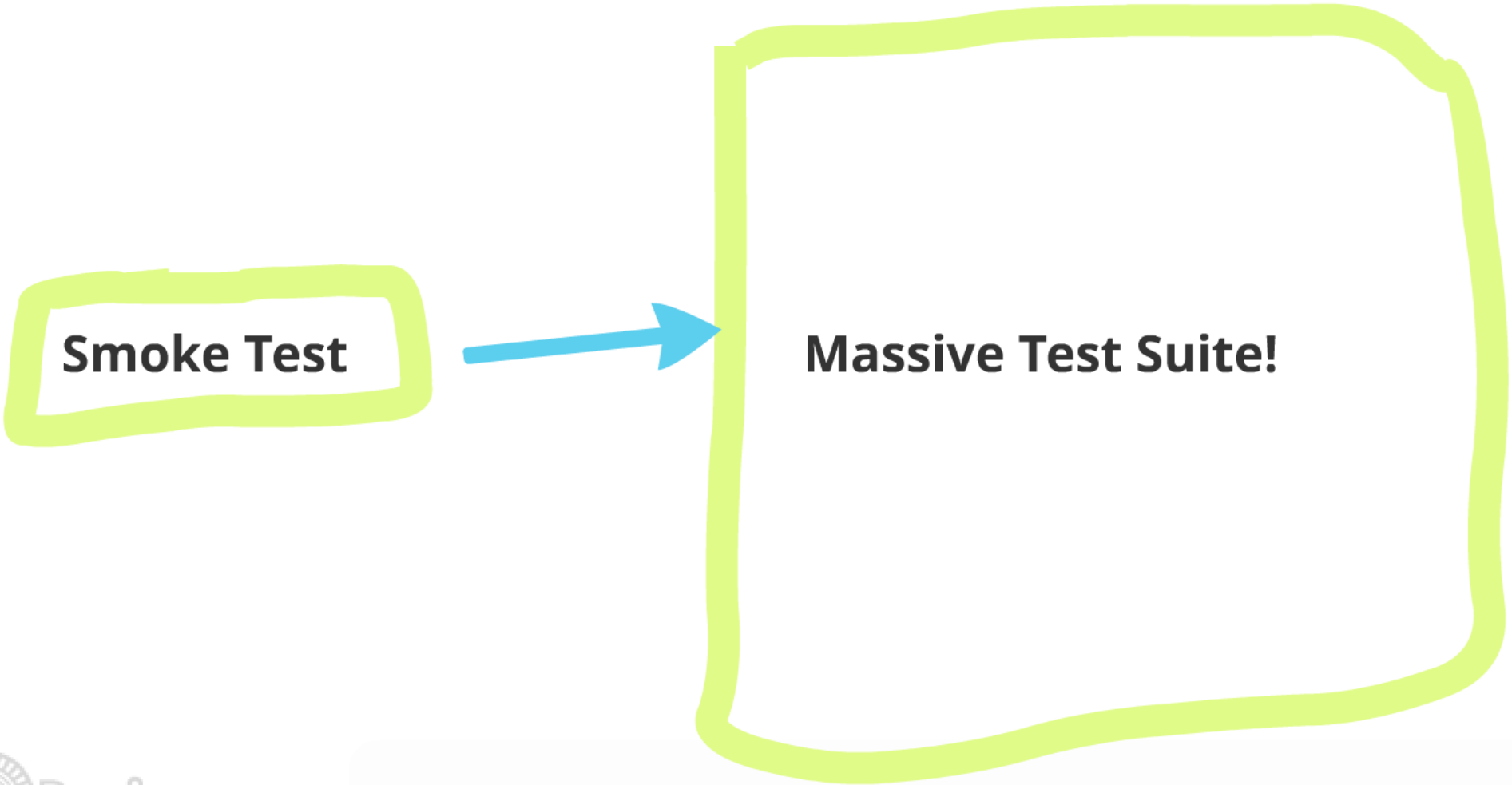
Smoke testing can be:

1. Scripted : There are a few small but important test cases (taking an hour or two to execute, at most) which are run prior to the software being released to the greater team.

2. Unscripted: An experienced tester does exploratory or ad hoc testing for an hour or so.

Keep in mind:

Smoke testing is an ADDITION to traditional software testing. It is a GATEWAY to further testing or release.



Media Check

A really, really basic smoke test:

- **Can the CD be read?**
- **Do files exist on the server?**
- **etc.**

NB: Some texts use the term "sanity" testing for "smoke testing". I try to avoid this term as it may be offensive.

Smoke testing is "*part* of a complete breakfast."

Stochastic Testing

stochastic, *adj.*

randomly determined; having a random probability distribution or pattern that may be analyzed statistically but may not be predicted precisely.

mid 17th cent.: from Greek stokhastikos, from stokhazesthai 'aim at, guess,' from stokhos 'aim.'

Also called "monkey testing".

PROTIP: Using words with Greek roots sounds more impressive than words named after primates.

Infinite monkey + Infinite typewriters

=

the works of Shakespeare

Think of stochastic testing as property based testing, with few or no limits on input, and often the only invariant is "the system keeps running!"

```
2 + 2 = 4
DOWAGER
(praying hands emoji)
fewjwe8r3
> 9000
{ "attr" : "value" }
(){#U(d)))(((()
fehioe
0x98AB654
int main () { printf ("meow"); }
ALL LIVING CREATURES DIE ALONE
e=++)@$
N{}#HIFHEUE
```

→ *SYSTEM* =)

Variants:

Smart Monkey - does what you expect a user to do
Evil Monkey - Goes out of its way to provide bad input (executable code, strange numbers, binary data, etc)
Chaos Monkey (from Netflix) - Randomly kill servers/processes

Chaos Monkey

Randomly terminates AWS instances

Run regularly on Netflix servers

Related Tools

Cut network connectivity
Reduce bandwidth
Modify permissions
Remove user
Change network topology
Induce latency

We live in a distributed world. These kinds of things happen.

Better to find out now and know how to deal with than get a call at 3 AM.

"The Fallacies of Distributed Computing"
-by Peter Deutsch

1. The network is reliable.
2. Latency is zero.
3. Bandwidth is infinite.
4. The network is secure.
5. Topology doesn't change.
6. There is one administrator.
7. Transport cost is zero.
8. The network is homogeneous.

Graceful Degradation

"The best way to avoid failure is to fail constantly." - Jeff Atwood

"If you want to make a difficult task easier, do it all the time." -Bill Laboon

The more you deal with a problem:

1. The more you know HOW to deal with it
2. The easier it is to automate it away

Example: Generators

Computers have moved from being *pets* to *cattle*.

Testing large, distributed systems means treating your systems as fungible "units of computation".

Example: Google

http://googletesting.blogspot.com/

"How Google Tests Software" by Whittaker, Arbon, and Carollo

stochastic, *adj.*

randomly determined; having a random probability distribution or pattern that may be analyzed statistically but may not be predicted precisely.

mid 17th cent.: from Greek stokhastikos, from stokhazesthai 'aim at, guess,' from stokhos 'aim.'

Also called "monkey testing".

PROTIP: Using words with Greek roots sounds more impressive than words named after primates.

Infinite monkey + Infinite typewriters

=

the works of Shakespeare

Think of stochastic testing as property based testing, with few or no limits on input, and often the only invariant is "the system keeps running!"

```
2 + 2 = 4
DOWAGER
(praying hands emoji)
fewjwe8r3
> 9000
{ "attr" : "value" }
{}{#U(d)))))))))
fehioe
0x98AB654
int main () { printf ("meow"); }
ALL LIVING CREATURES DIE ALONE
e=++)@$
N((#HIFHEUIE
```

Variants:

Smart Monkey **- does what you expect a user to do**

Evil Monkey **- Goes out of its way to provide bad input (executable code, strange numbers, binary data, etc)**

Chaos Monkey (from Netflix) **- Randomly kill servers/processes**

Chaos Monkey

Randomly terminates AWS instances

Run regularly on Netflix servers

Related Tools

Cut network connectivity

Reduce bandwidth

Modify permissions

Remove user

Change network topology

Induce latency

We live in a distributed world.
These kinds of things happen.

Better to find out now and know how to deal with than get a call at 3 AM.

"The Fallacies of Distributed Computing"

-by Peter Deutsch

1. The network is reliable.
2. Latency is zero.
3. Bandwidth is infinite.
4. The network is secure.
5. Topology doesn't change.
6. There is one administrator.
7. Transport cost is zero.
8. The network is homogeneous.

Graceful Degradation

"The best way to avoid failure is to fail constantly." - Jeff Atwood

"If you want to make a difficult task easier, do it all the time." -Bill Laboon

The more you deal with a problem:

1. The more you know HOW to deal with it
2. The easier it is to automate it away

Example: Generators

Computers have moved from being *pets* to *cattle*.

Testing large, distributed systems means treating your systems as fungible "units of computation".

Example: Google

http://googletesting.blogspot.com/

"How Google Tests Software" by Whittaker, Arbon, and Carollo

Let's Get Informal: Exploratory, Smoke and Stochastic Testing