

# Y2K & Other Disappointing Disasters

Risk Reduction and Harm Mitigation

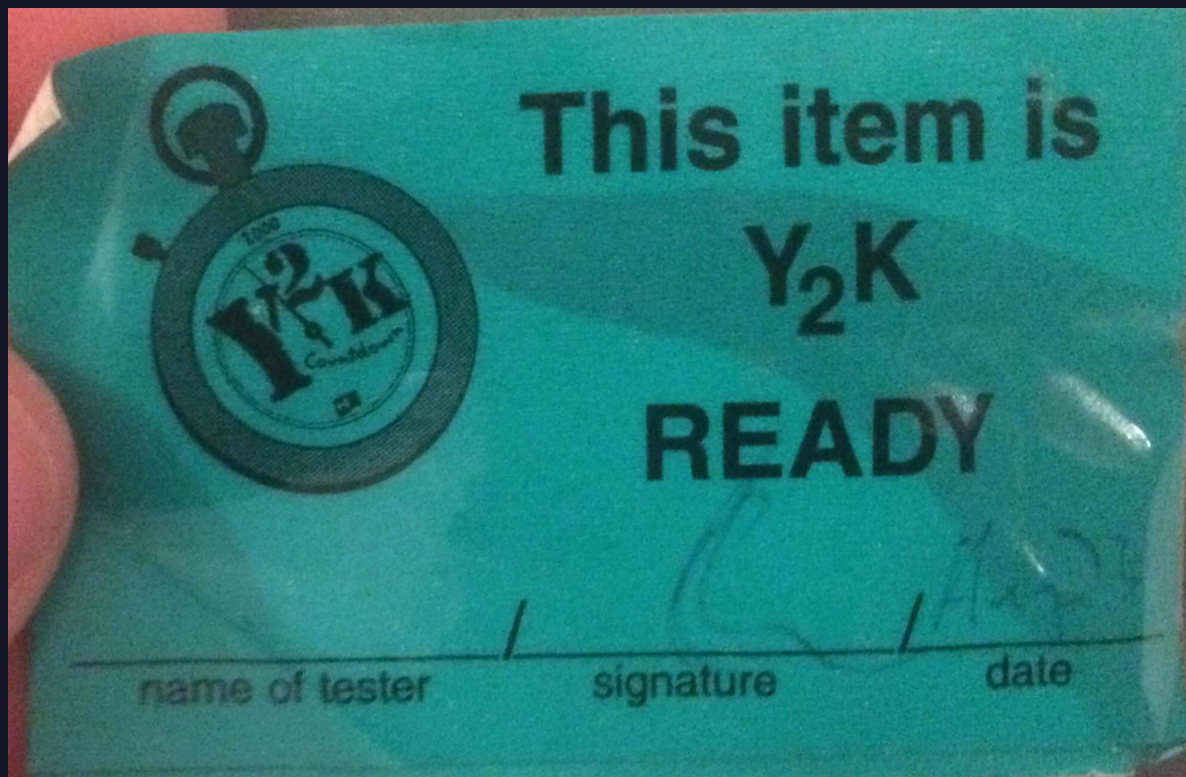






# An actual pager





Ready for the big night



**No one  
remembers the  
crisis averted.**



# Risk Reduction



# Risk Reduction

- Stay-home orders
- Vaccination
- Train gates



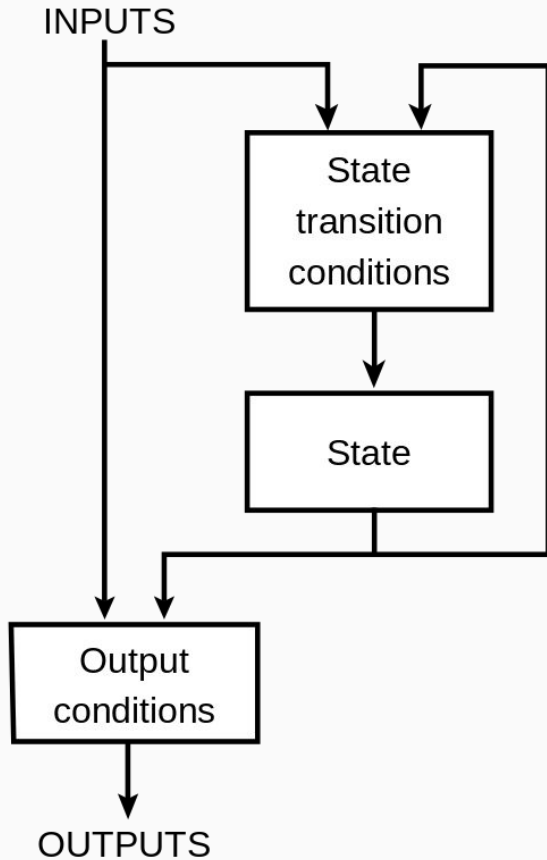
# How to reduce risk



# Secure your zone







# Predict states

---

# Accept Risk

- You can't prevent everything
- Decide what matters to save
- Make mindful tradeoffs based on data



# Harm Mitigation



# When Things Go Wrong





# How to mitigate harm



# Fail safe or fail secure?

- 
- What are you protecting?
  - What is your risk?

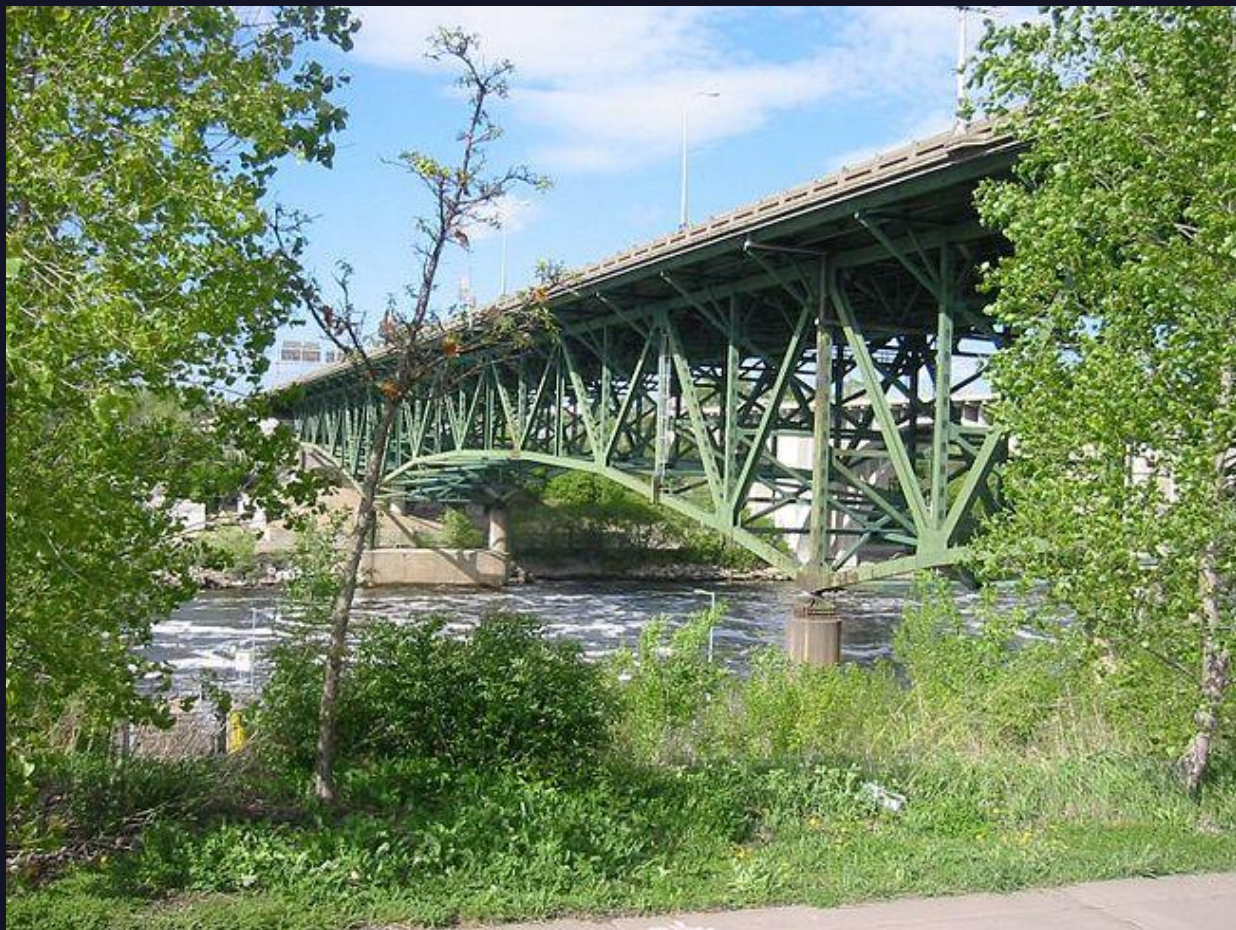
**Failure is  
inevitable.**

**Disaster is not.**



# What's a disaster?







# U10W Components

U9/U10 upper chord

Up

North

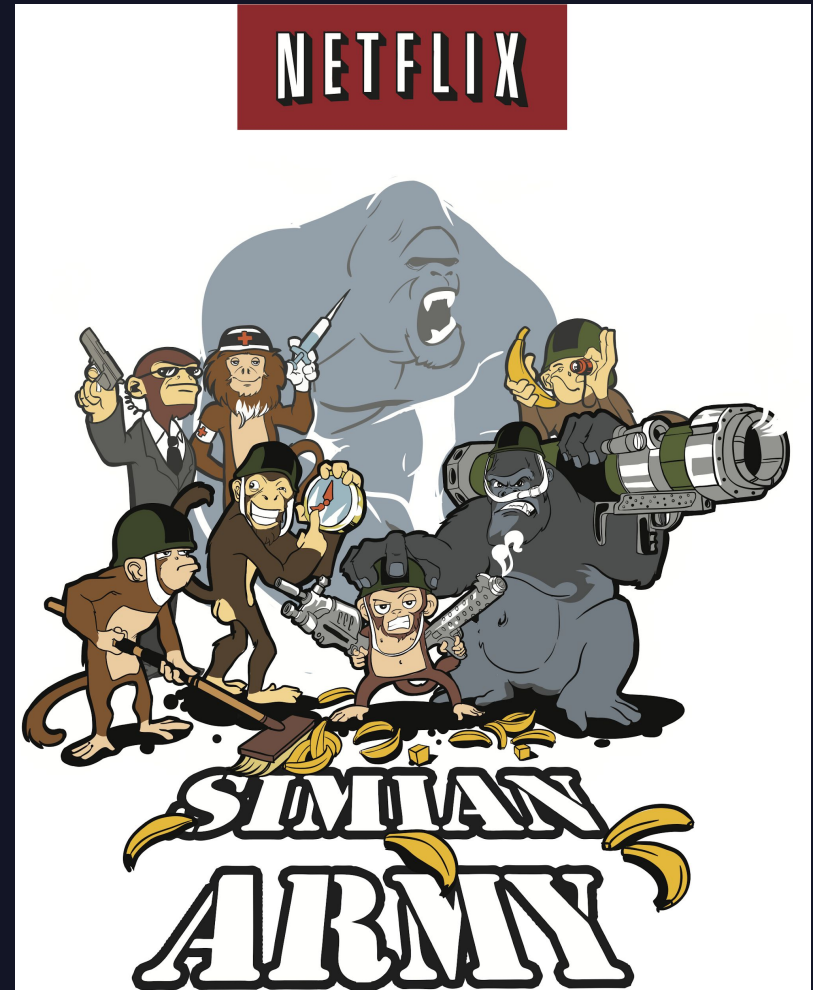
L9/U10 compression diagonal

U10/L11  
tension  
diagonal

Figure 4. Reconstructed U10W components, looking at the east gusset plate.

[www.engineeringcivil.com](http://www.engineeringcivil.com)


# Let's design for that



# Fizzle factors

- Microservices and loose coupling
- Fault-tolerant messaging
- Data duplication
- Canary launches
- Kill switches and circuit breakers
- Automatic recovery
- Testing for load, stress, and outage





Rubber bands, not rigid joints

---

# Microservices and loose coupling

# ARPA COMPUTER NETWORK

The internet routes around censorship as damage

## Fault-tolerant messaging



It's not a backup if you haven't tested restoration

---

# Data duplication



Verify

---

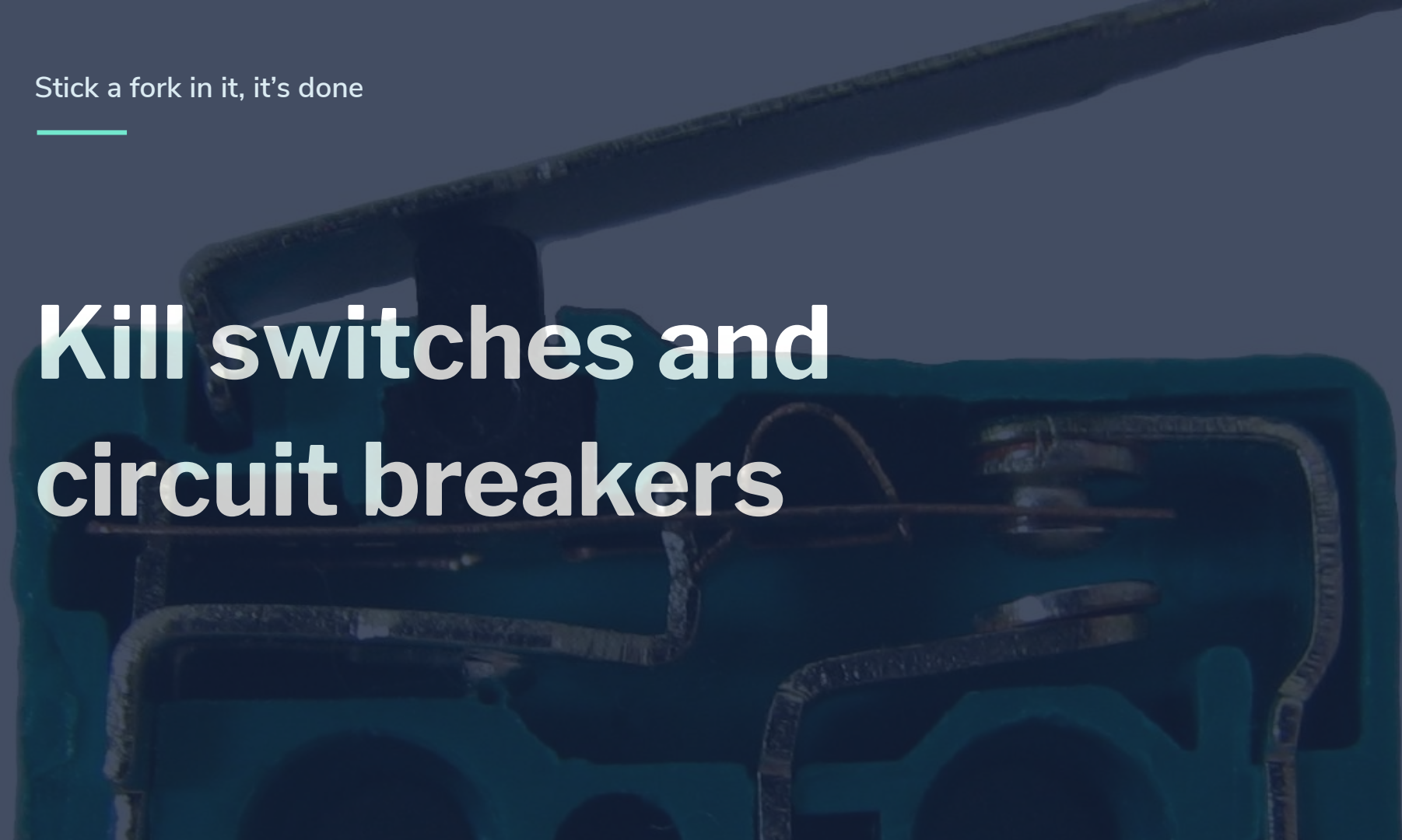
# Canary launches

Image by [Capri23auto](#) from [Pixabay](#)

Stick a fork in it, it's done

---

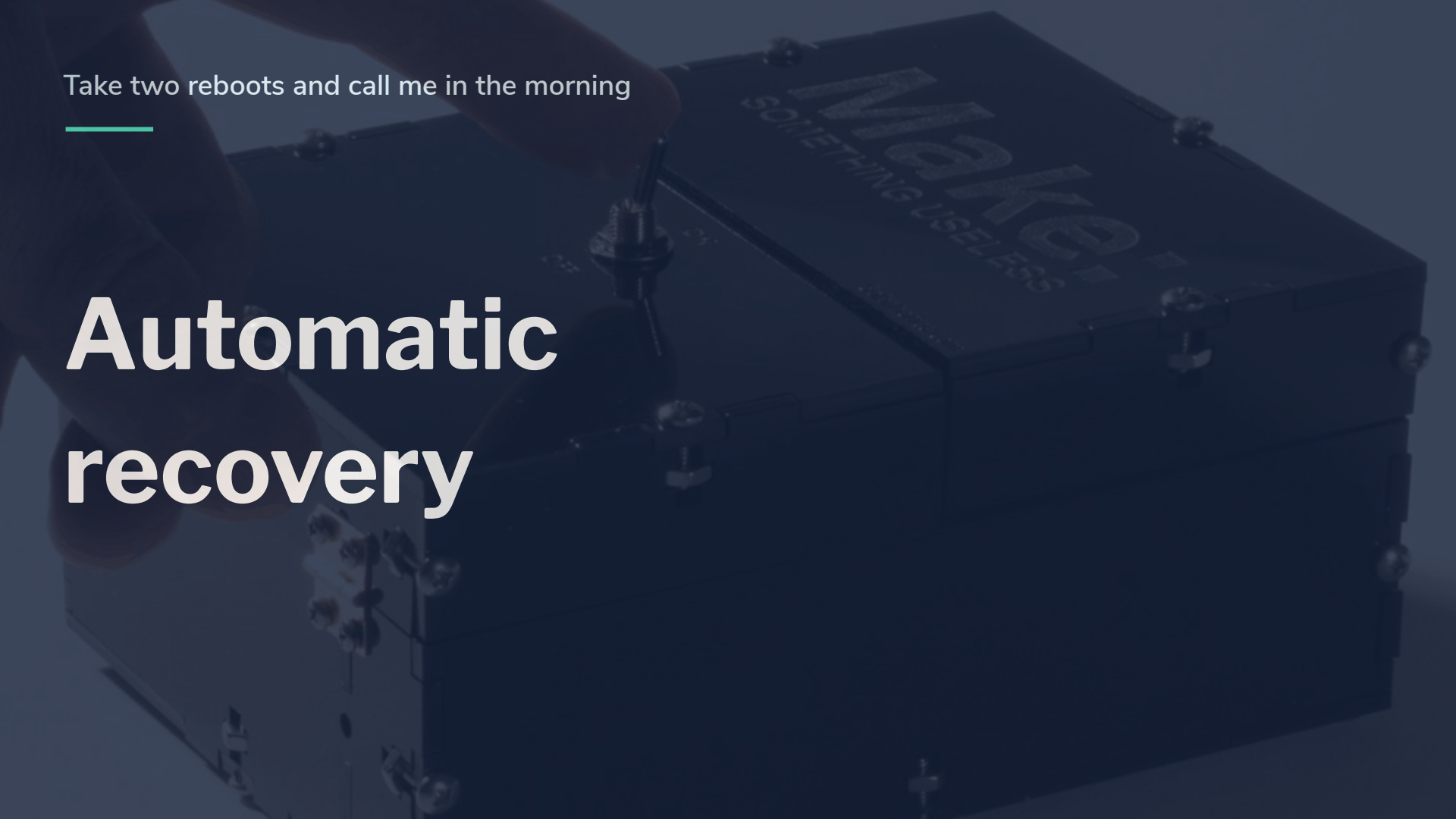
# Kill switches and circuit breakers



Take two reboots and call me in the morning

---

# Automatic recovery





Elastic scaling only gets you so far

---

# Testing for load, stress and outage



# tl;rt

- Expect failure
- Make systems less rigid
- Plan for disaster
- Degrade gracefully





LaunchDarkly

<https://tinyurl.com/failoverconf-heidi>

# The Hymn of Breaking Strain

THE careful text-books  
measure

(Let all who build beware!)

The load, the shock, the  
pressure

Material can bear.

So, when the buckled girder

Lets down the grinding span,

'The blame of loss, or murder,

Is laid upon the man.

*Not on the Stuff – the Man!*

But in our daily dealing

With stone and steel, we find

The Gods have no such feeling

Of justice toward mankind.

To no set gauge they make us–

For no laid course prepare–

And presently o'ertake us

With loads we cannot bear:

*Too merciless to bear.*

The prudent text-books give it

In tables at the end

'The stress that shears a rivet

Or makes a tie-bar bend–

'What traffic wrecks  
macadam–

What concrete should endure–

but we, poor Sons of Adam

Have no such literature,

*To warn us or make sure!*



We hold all Earth to plunder –  
All Time and Space as well –  
Too wonder-stale to wonder  
At each new miracle;  
Till, in the mid-illusion  
Of Godhead 'neath our hand,  
Falls multiple confusion  
On all we did or planned –  
*The mighty works we planned.*

We only of Creation  
*(oh, luckier bridge and rail)*  
Abide the twin damnation –  
To fail and know we fail.  
Yet we – by which sole token  
We know we once were Gods –  
Take shame in being broken  
However great the odds –  
*The burden of the Odds.*

Oh, veiled and secret Power  
Whose paths we seek in vain,  
Be with us in our hour  
Of overthrow and pain;  
That we – by which sure token  
We know Thy ways are true –  
In spite of being broken,  
*Because of being broken*  
*May rise and build anew*  
*Stand up and build anew.*