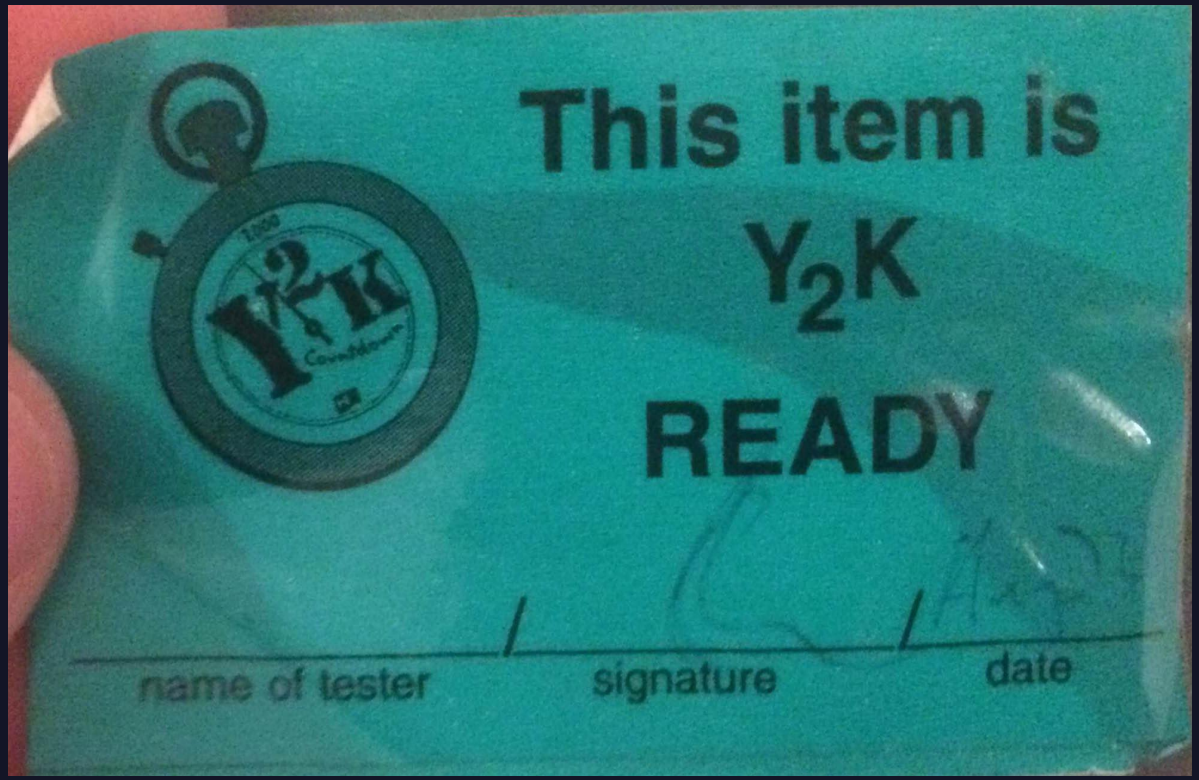

Y2K
& Other
Disappointing Disasters
Risk Reduction and Harm Mitigation
LaunchDarkly
@wiredferret


LaunchDarkly
@wiredferret



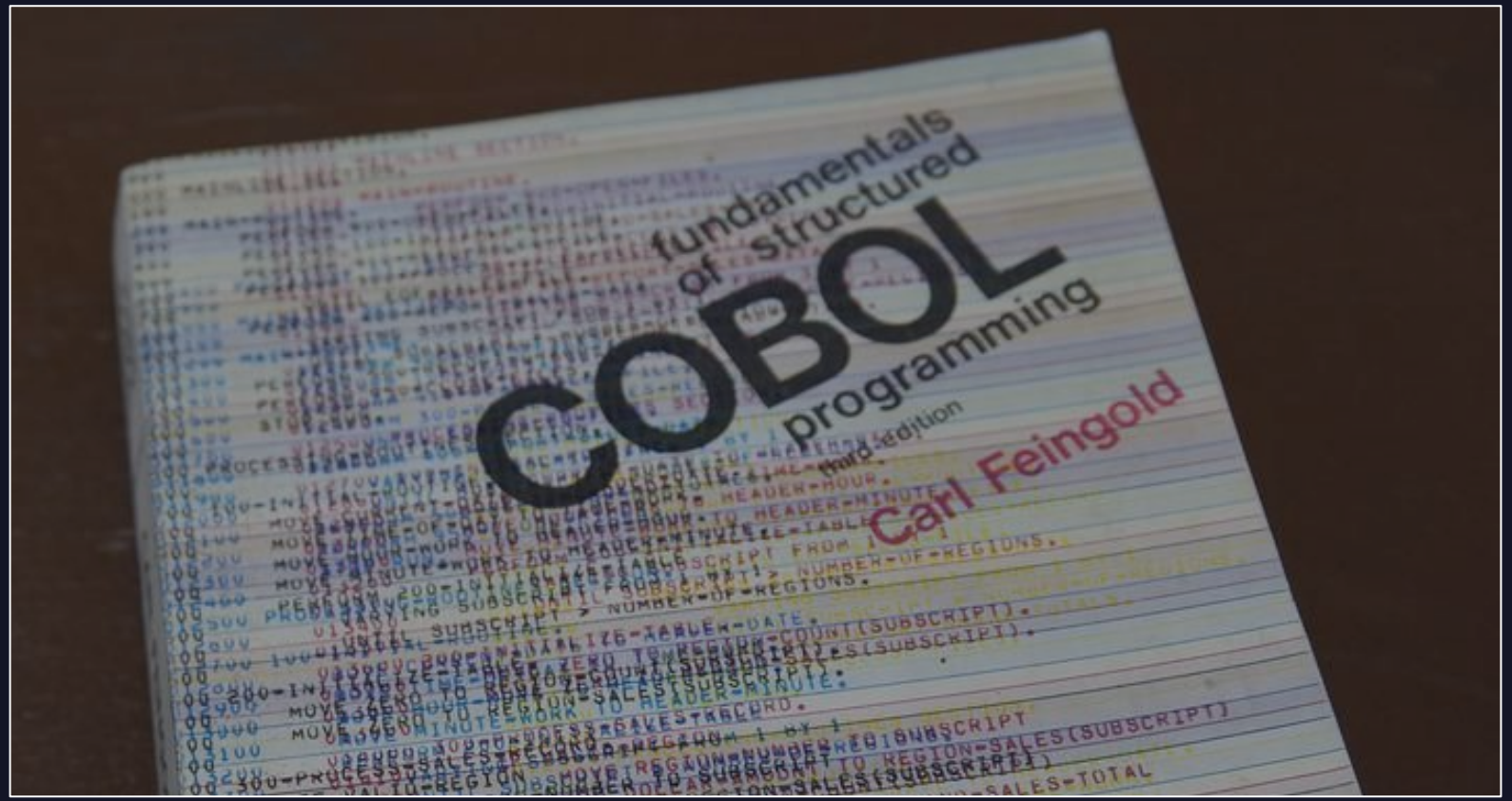
An actual pager



Ready for the big night



We actually worried



This was a vital job



No one remembers the crisis averted.

Risk Reduction



Risk Reduction

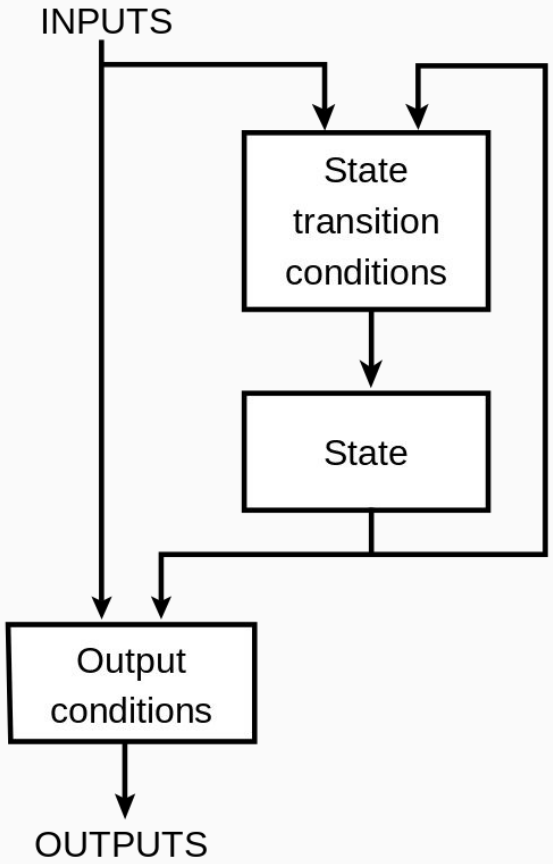
- Vaccination
- Anti-lock brakes
- Train gates

How to reduce risk

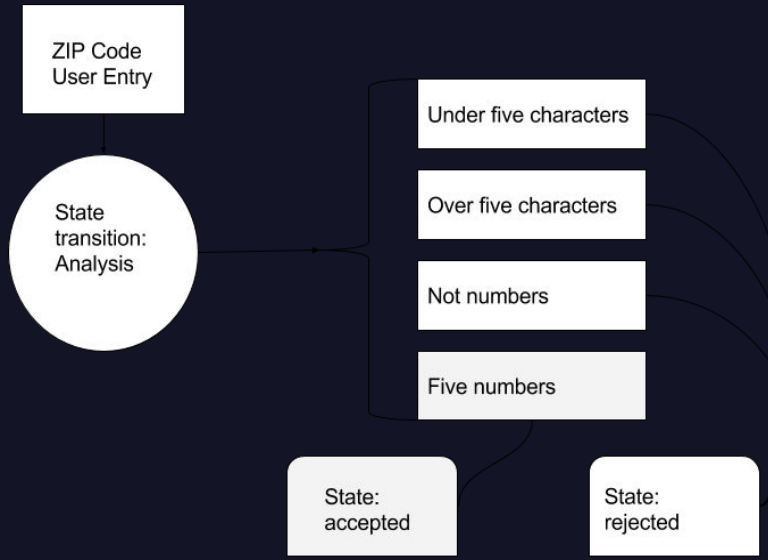


Secure your zone





Predict states



State machine

Input: ZIP code

States: <several>

Transitions: Submit or refuse

Accept Risk

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

Harm Mitigation

When Things Go Wrong






MACRONET





How to mitigate harm

Fail safe or fail secure?

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

Assume failure

- Failure is almost always an oversight
- Test with many audiences
- You can’t prevent all failures
- Make failure less catastrophic

Predict states



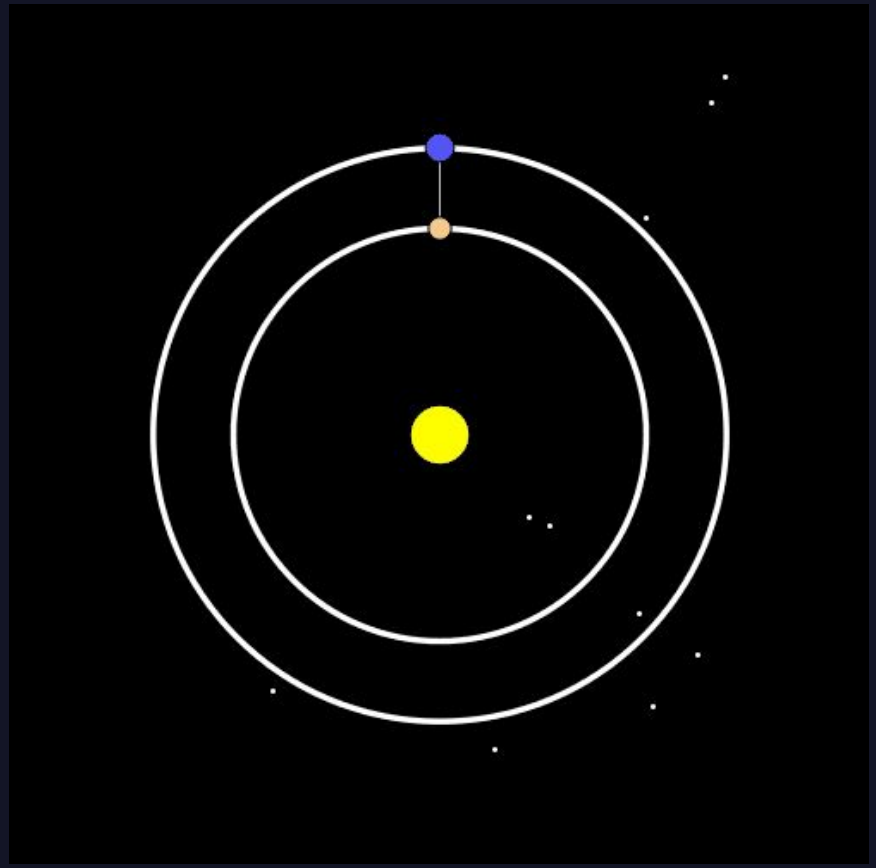
Failure is inevitable.

Disaster is not.

It’s complicated and hard

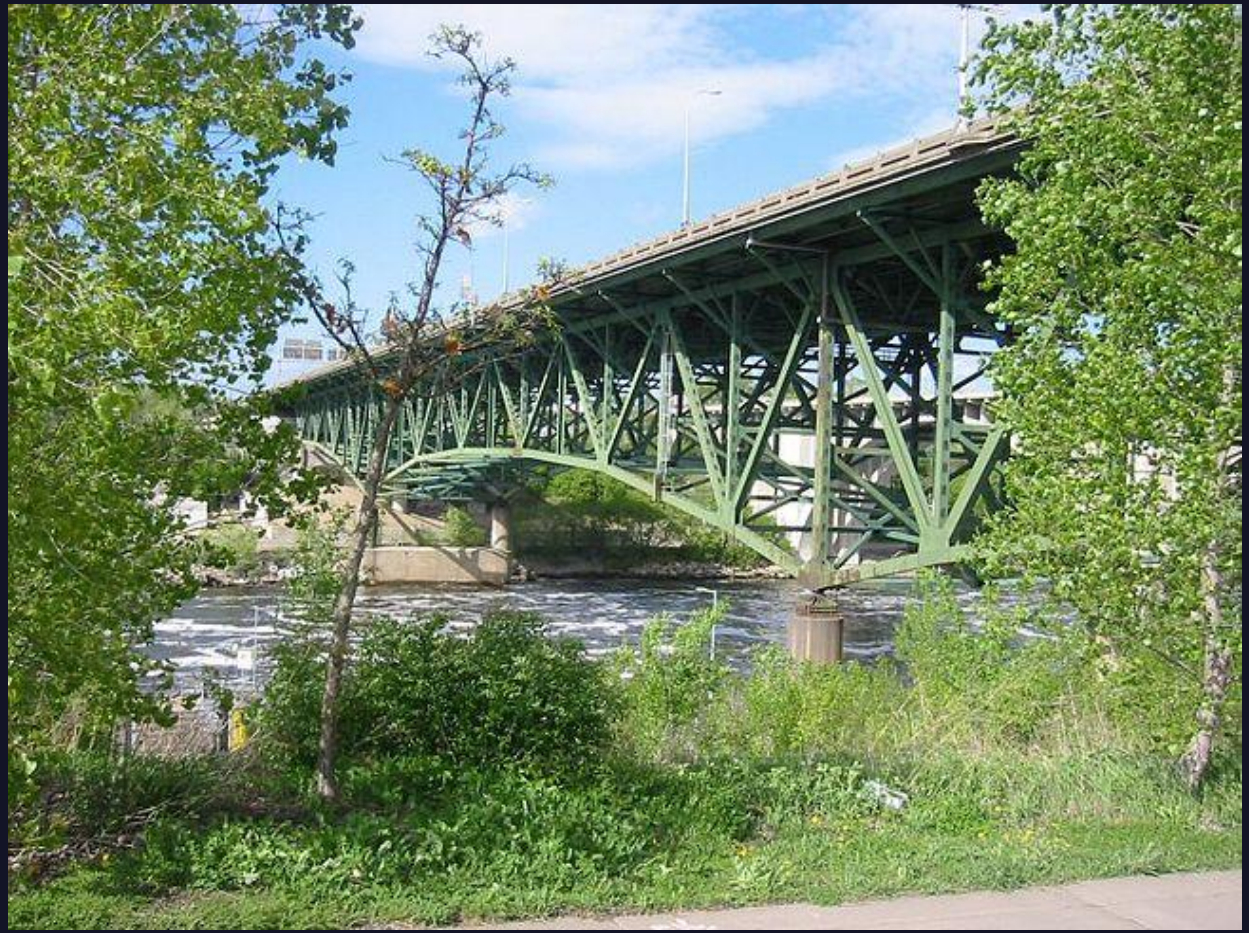

THE ORIGINAL
TINKERTOY
GIANT ENGINEER

Combinatoric Testing Complexity





What's a disaster?



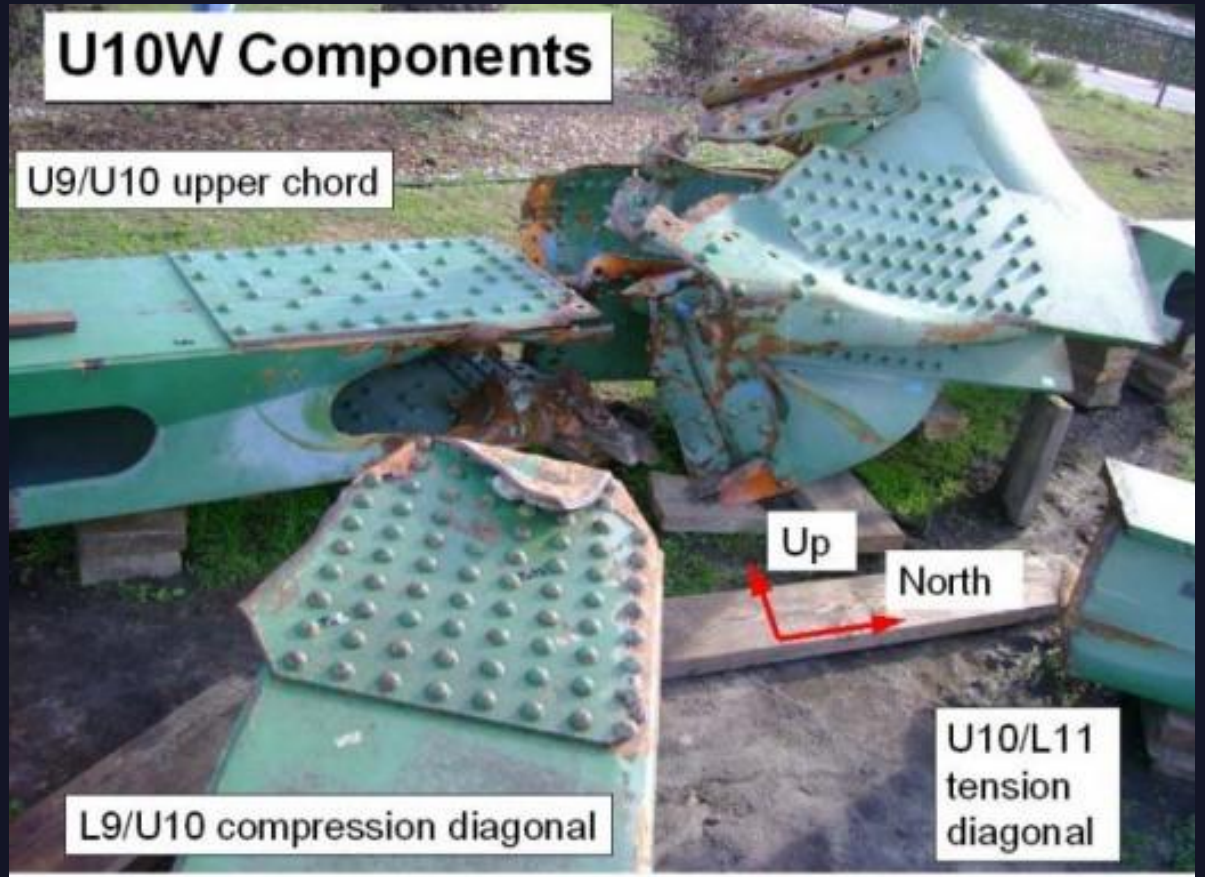
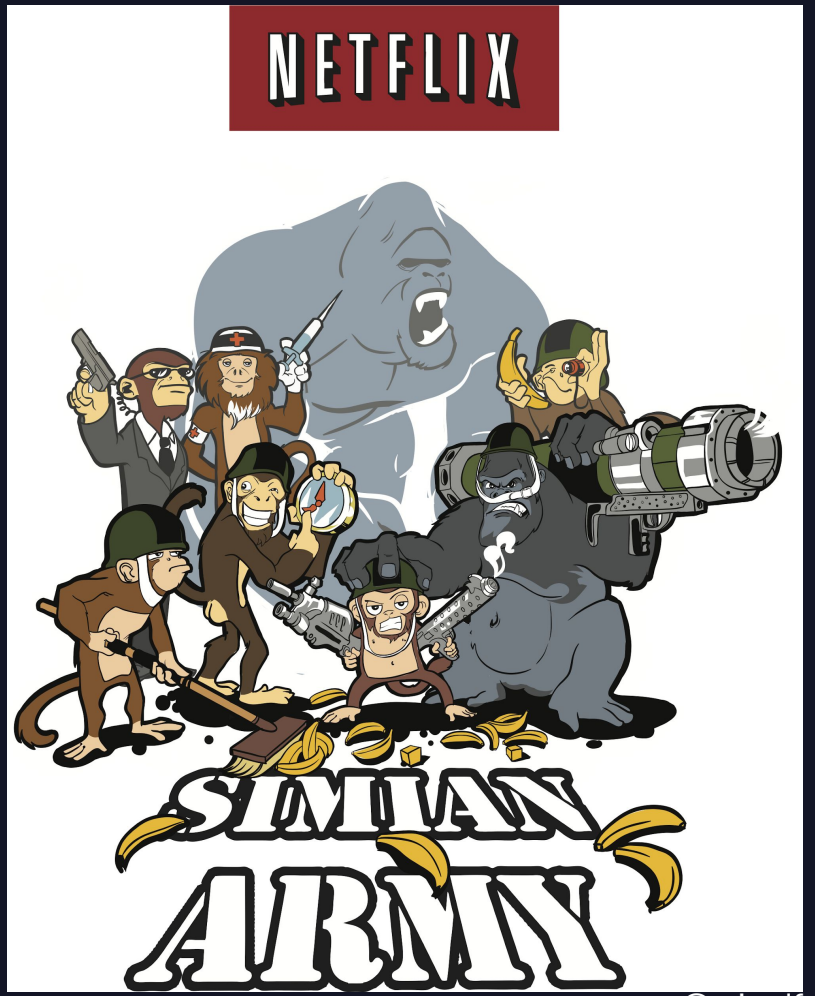


Figure 4. Reconstructed U10W components, looking at the east gusset plate.
www.engineeringcivil.com

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

Microservices and loose coupling

Fault-tolerant messaging

Data duplication

Canary launches

Kill switches and circuit breakers

Automatic recovery

Testing for load, stress and outage

tl;rt

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



launchdarkly.com/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.