SCADA and ICS for Security Experts:

How to Avoid Cyberdouchery

James Arlen, CISA

Blackhat Briefings - Las Vegas - 2010

Disclaimer

I am employed in the Infosec industry, but not authorized to speak on behalf of my employer or clients.

Everything I say can be blamed on great food, mind-control and jet lag.

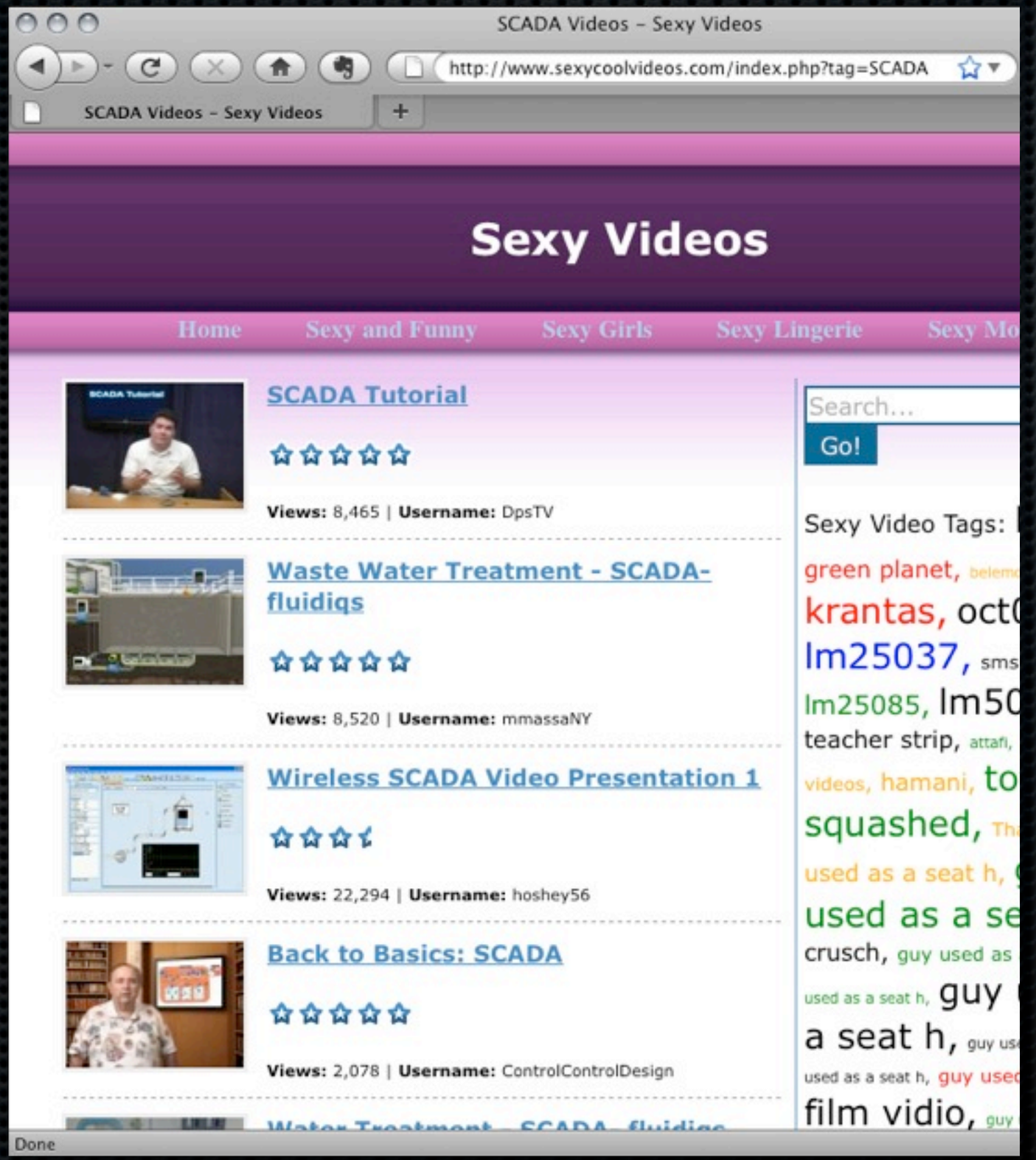
Credentials

- 15+ years information security specialist
- staff operations, consultant, auditor, researcher
- utilities vertical (grid operations, generation, distribution)
- financial vertical (banks, trust companies, trading)
- some hacker related stuff like game show host, etc.

...still not an expert at anything.

1/ Stop Sounding Stupid

Scada got sexy



Follow the money

Who's an expert now?

One time at security camp

Gotta get me a piece of that

Gotta get me a piece of that

2/ Big Things and Little Things

Not all 'scada' is SCADA

Big things: power grid

Big things: pipeline

Inter-connected sensors and controls under central management

Inter-connected sensors and controls under central management

Supervisory control and data acquisition

Little Things: chemical plant, power plant, manufacturing facility

Little Things: chemical plant, power plant, manufacturing facility

Little Things: chemical plant, power plant, manufacturing facility

Little Things: chemical plant, power plant, manufacturing facility

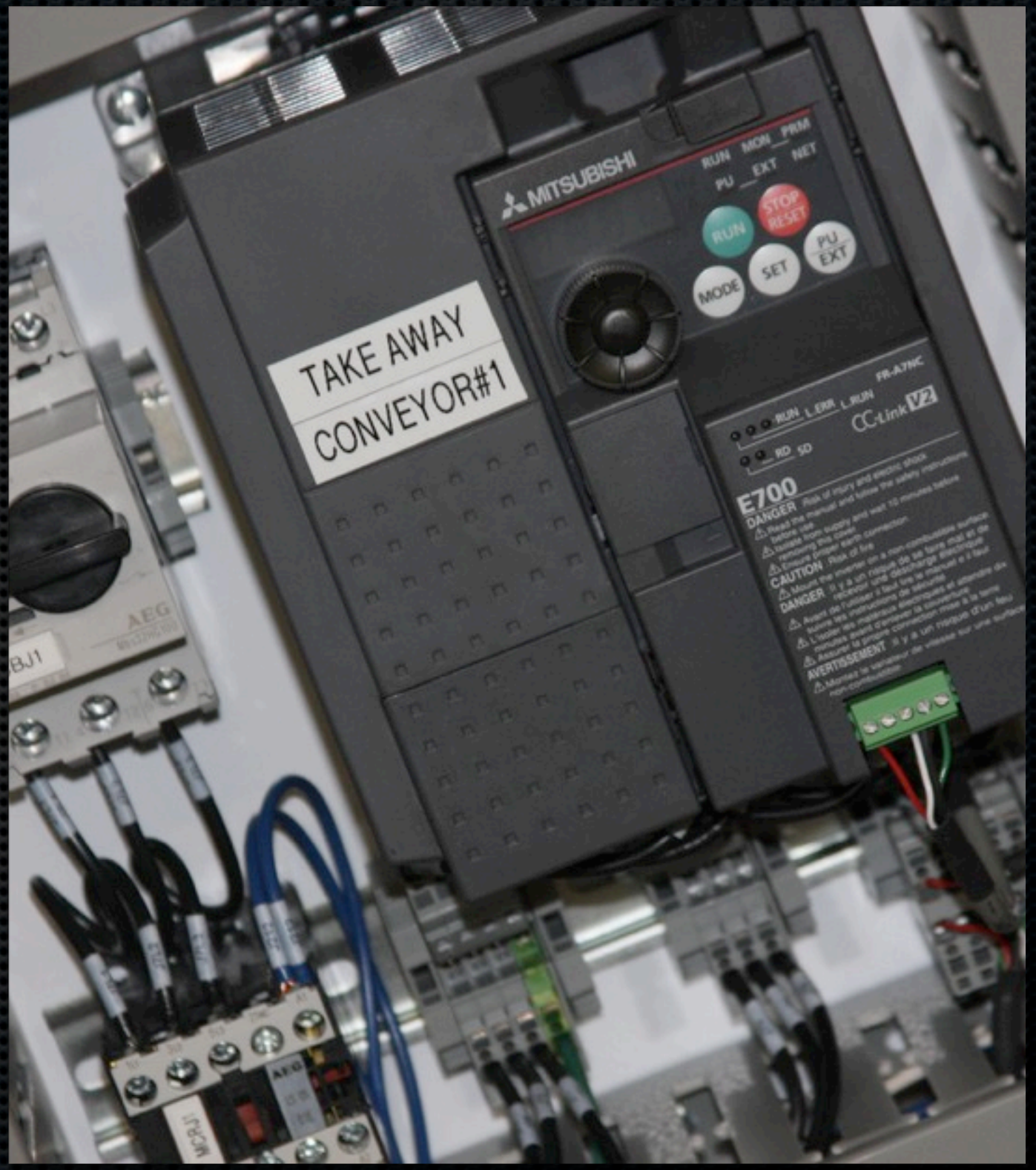
Little Things: chemical plant, power plant, manufacturing facility

Little Things: chemical plant, power plant, manufacturing facility

Lots of individual capabilities with some orchestration

Programmable logic controllers

Programmable logic controllers



Programmable logic controllers

Industrial control systems/ Distributed control systems

3/ Part of a Bigger Picture

So if you break the computer, you break everything

What happens when Edna falls into the reactant vessel

```
4 > 192.168.110.138.502: P, cksum 0xfecf (correct), 1104342266:1104342278(12) ack 3776265427 win 64193
        0x0000:  4500 0034 8caa 4000 8006 0fbb c0a8 6e83  E..4..@.......n.
        0x0010:  c0a8 6e8a 081a 01f6 41d2 ecfa e115 3cd3  ..n.....A.....<.
        0x0020:  5018 fac1 fecf 0000 0000 0000 0006 0103  P...............
        0x0030:  0000 0001                                ....
04:46:17.033314 IP (tos 0x0, ttl 128, id 16108, offset 0, flags [DF], proto TCP (6), length 51) 192.168.110.138.502
 > 192.168.110.131.2074: P, cksum 0x2fd6 (correct), 3776265427:3776265438(11) ack 1104342278 win 65391
        0x0000:  4500 0033 3eec 4000 8006 5d7a c0a8 6e8a  E..3>.@...]z..n.
        0x0010:  c0a8 6e83 01f6 081a e115 3cd3 41d2 ed06  ..n.......<.A...
        0x0020:  5018 ff6f 2fd6 0000 0001 0000 0005 0103  P..o/...........
        0x0030:  0241 c8                                  .A.
04:46:17.034105 IP (tos 0x0, ttl 128, id 36011, offset 0, flags [DF], proto TCP (6), length 52) 192.168.110.131.207
4 > 192.168.110.138.502: P, cksum 0xfec3 (correct), 1104342278:1104342290(12) ack 3776265438 win 64182
        0x0000:  4500 0034 8cab 4000 8006 0fba c0a8 6e83  E..4..@.......n.
        0x0010:  c0a8 6e8a 081a 01f6 41d2 ed06 e115 3cde  ..n.....A.....<.
        0x0020:  5018 fab6 fec3 0000 0000 0000 0006 0103  P...............
        0x0030:  0000 0001                                ....
04:46:17.035015 IP (tos 0x0, ttl 128, id 16109, offset 0, flags [DF], proto TCP (6), length 51) 192.168.110.138.502
 > 192.168.110.131.2074: P, cksum 0x2fca (correct), 3776265438:3776265449(11) ack 1104342290 win 65379
        0x0000:  4500 0033 3eed 4000 8006 5d79 c0a8 6e8a  E..3>.@...]y..n.
        0x0010:  c0a8 6e83 01f6 081a e115 3cde 41d2 ed12  ..n.......<.A...
        0x0020:  5018 ff63 2fca 0000 0002 0000 0005 0103  P..c/...........
        0x0030:  0241 c8                                  .A.
04:46:17.035426 IP (tos 0x0, ttl 128, id 36012, offset 0, flags [DF], proto TCP (6), length 52) 192.168.110.131.207
4 > 192.168.110.138.502: P, cksum 0xfeb7 (correct), 1104342290:1104342302(12) ack 3776265449 win 64171
        0x0000:  4500 0034 8cac 4000 8006 0fb9 c0a8 6e83  E..4..@.......n.
        0x0010:  c0a8 6e8a 081a 01f6 41d2 ed12 e115 3ce9  ..n.....A.....<.
        0x0020:  5018 faab feb7 0000 0000 0000 0006 0103  P...............
        0x0030:  0000 0001                                ....
```

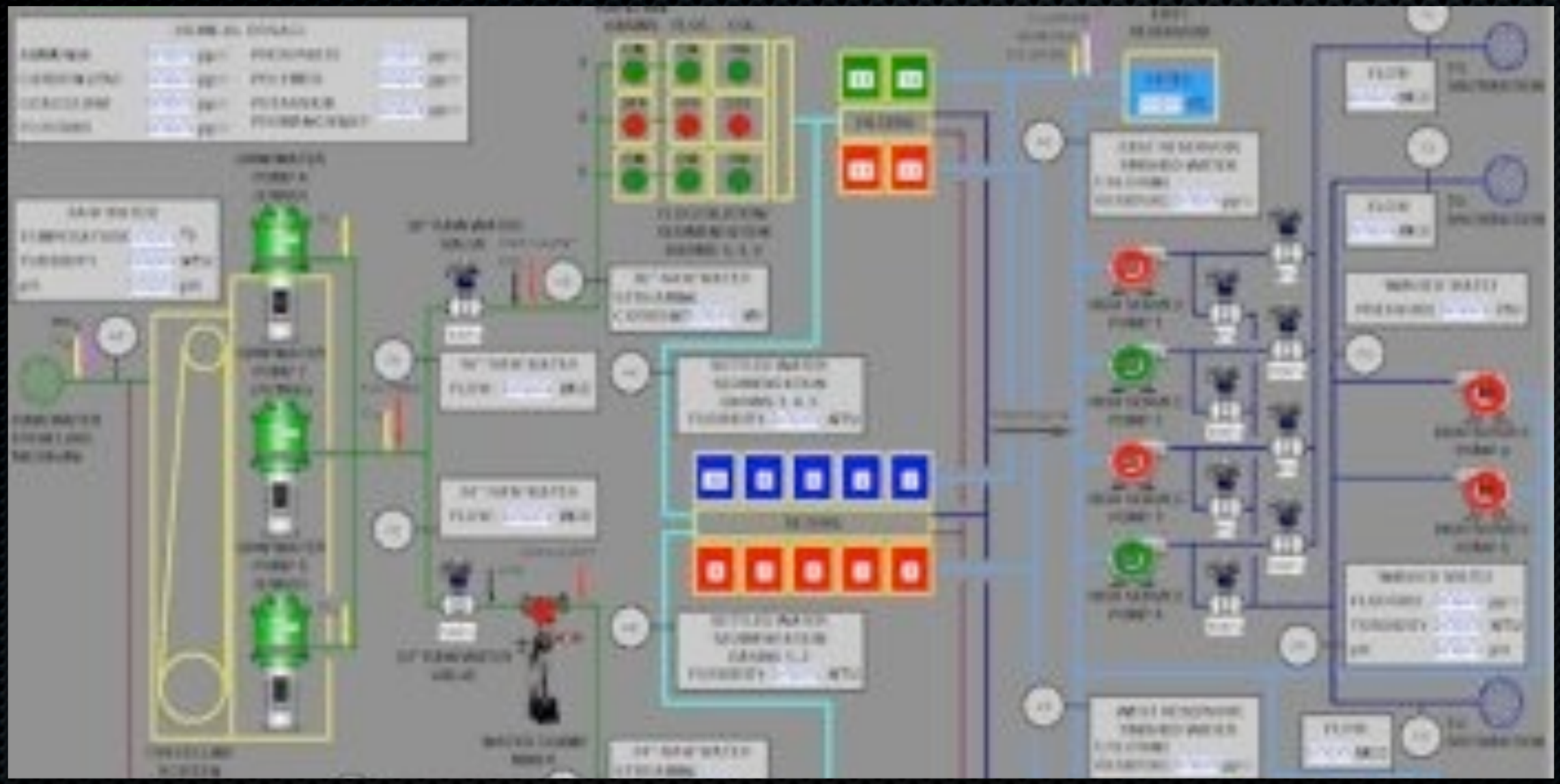
This is the data

```
        0x0030:  5377 c1c2 040c 0117 ffff 0000 0100 0301  Sw..............
        0x0040:  6400 a0d6 0000 6400 0000 0000 5b         d.....d.....[
07:37:04.828243 IP (tos 0x0, ttl 64, id 24773, offset 0, flags [DF], proto TCP (6), length 77) 192.168.0.1.
53640 > 192.168.0.2.20000: P, cksum 0xb63d (correct), 3756768673:3756768710(37) ack 2987965450 win 5840
        0x0000:  4500 004d 60c5 4000 4006 5892 c0a8 0001  E..M`.@.@.X.....
        0x0010:  c0a8 0002 d188 4e20 dfeb bda1 b218 bc0a  ......N.........
        0x0020:  5018 16d0 b63d 0000 0564 1cc4 0a00 0100  P....=...d......
        0x0030:  5377 c1c2 040c 0100 0000 ffff 0100 0301  Sw..............
        0x0040:  6400 c77b 0000 6400 0000 0000 5b         d..{..d.....[
07:37:04.910056 IP (tos 0x0, ttl 64, id 28682, offset 0, flags [DF], proto TCP (6), length 77) 192.168.0.1.
53641 > 192.168.0.2.20000: P, cksum 0x11de (correct), 3744312825:3744312862(37) ack 128424270 win 5840
        0x0000:  4500 004d 700a 4000 4006 494d c0a8 0001  E..Mp.@.@.IM....
        0x0010:  c0a8 0002 d189 4e20 df2d adf9 07a7 994e  ......N..-.....N
        0x0020:  5018 16d0 11de 0000 0564 1cc4 0a00 0100  P........d......
        0x0030:  5377 c1c2 040c 0101 0000 ffff 0100 0301  Sw..............
        0x0040:  6400 496d 0000 6400 0000 0000 5b         d.Im..d.....[
07:37:04.932977 IP (tos 0x0, ttl 64, id 52509, offset 0, flags [DF], proto TCP (6), length 77) 192.168.0.1.
53642 > 192.168.0.2.20000: P, cksum 0xe47d (correct), 3746435936:3746435973(37) ack 2533769180 win 5840
        0x0000:  4500 004d cd1d 4000 4006 ec39 c0a8 0001  E..M..@.@..9....
        0x0010:  c0a8 0002 d18a 4e20 df4e 1360 9706 3fdc  ......N..N.`..?.
        0x0020:  5018 16d0 e47d 0000 0564 1cc4 0a00 0100  P....}...d......
        0x0030:  5377 c1c2 040c 0102 0000 ffff 0100 0301  Sw..............
        0x0040:  6400 db56 0000 6400 0000 0000 5b         d..V..d.....[
07:37:04.980499 IP (tos 0x0, ttl 64, id 3763, offset 0, flags [DF], proto TCP (6), length 77) 192.168.0.1.5
3643 > 192.168.0.2.20000: P, cksum 0x3115 (correct), 3758477583:3758477620(37) ack 1033245795 win 5840
        0x0000:  4500 004d 0eb3 4000 4006 aaa4 c0a8 0001  E..M..@.@.......
        0x0010:  c0a8 0002 d18b 4e20 e005 d10f 3d96 1463  ......N.....=..c
```

This is the data

This is the process

This is the process



This is the process

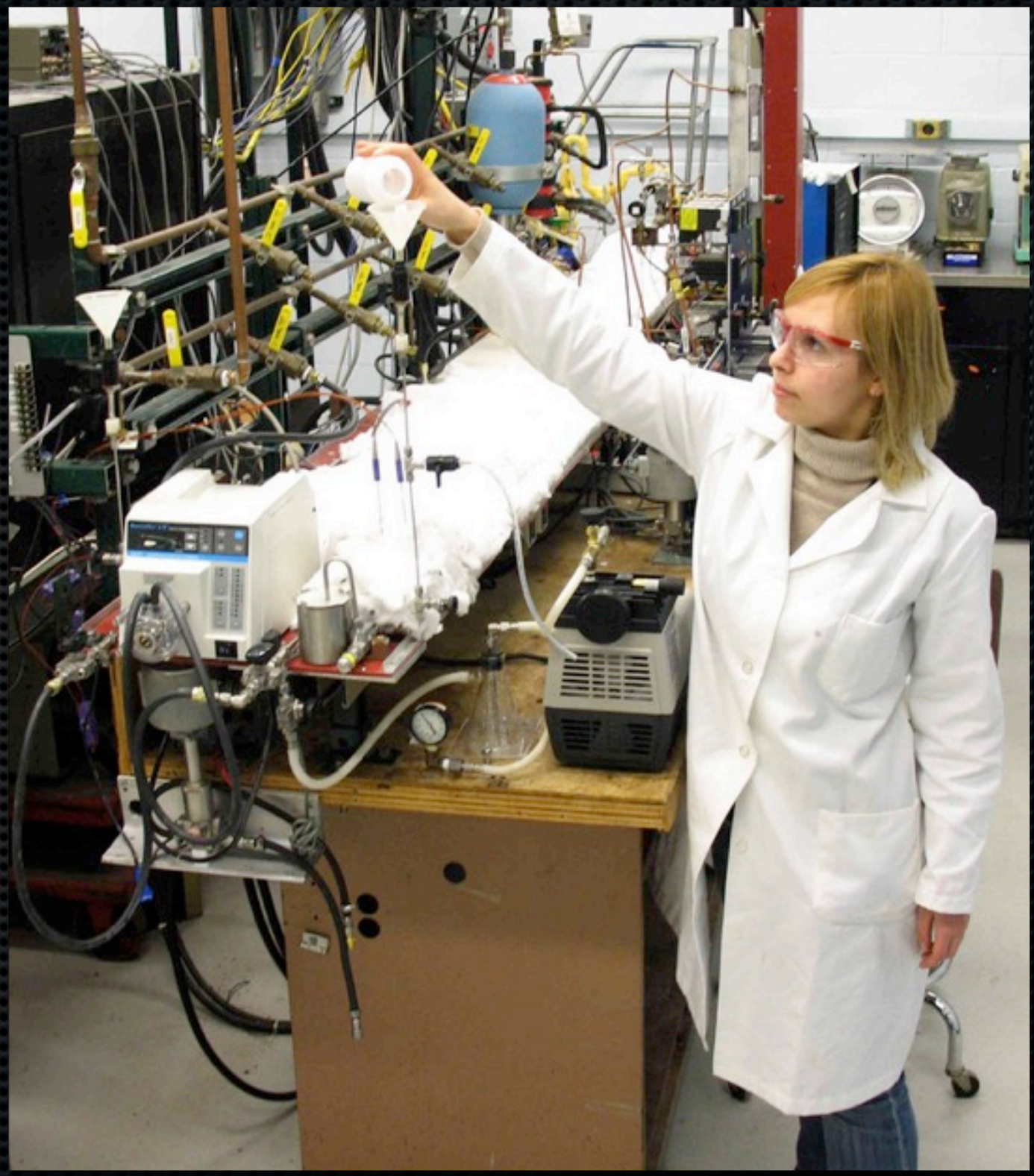
I know you can grok the protocol, can you break the controls?

I know you can grok the protocol, can you break the controls?

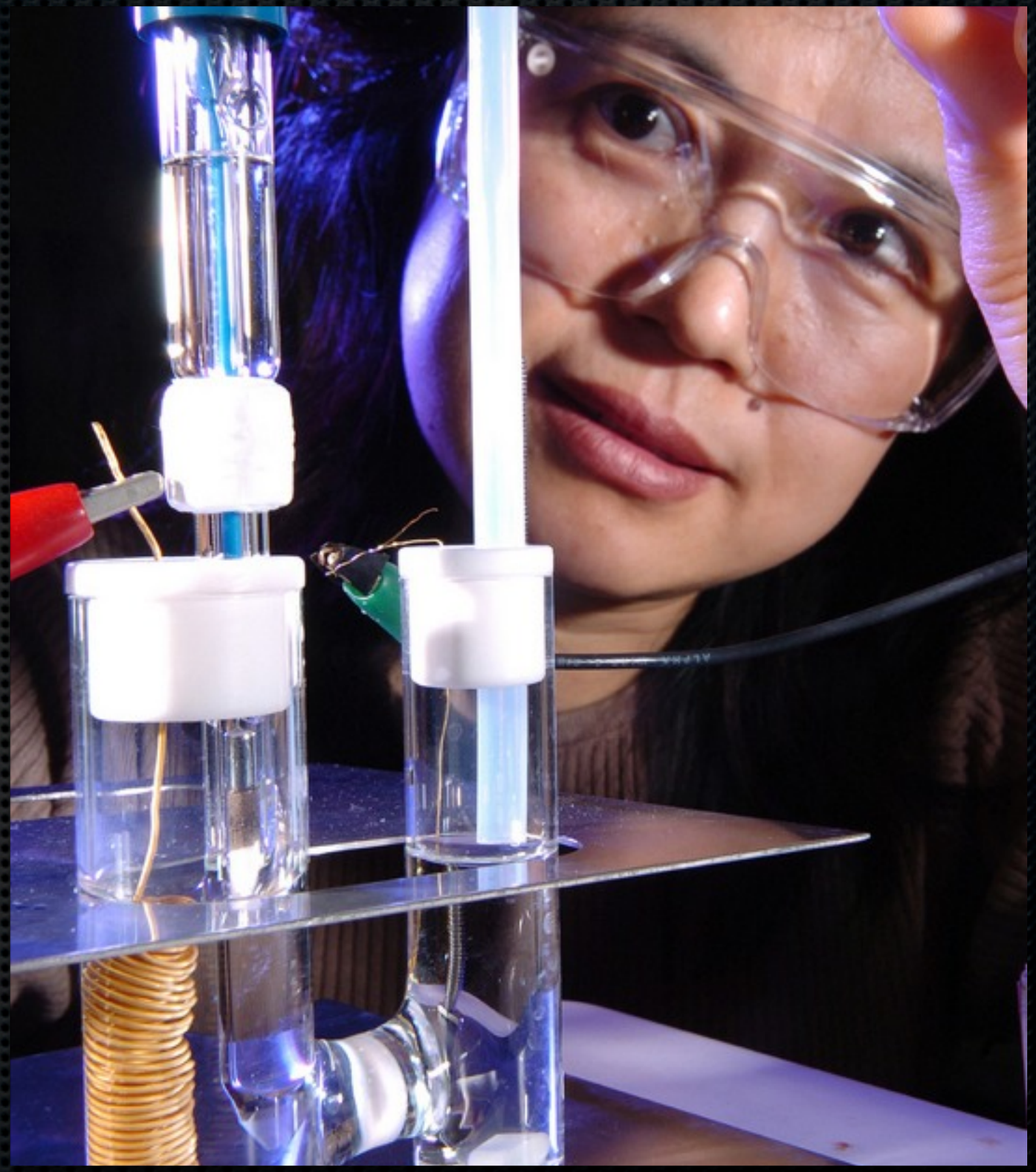
Oh, you forgot about safety

Oh, you forgot about safety

Oh, you forgot about testing

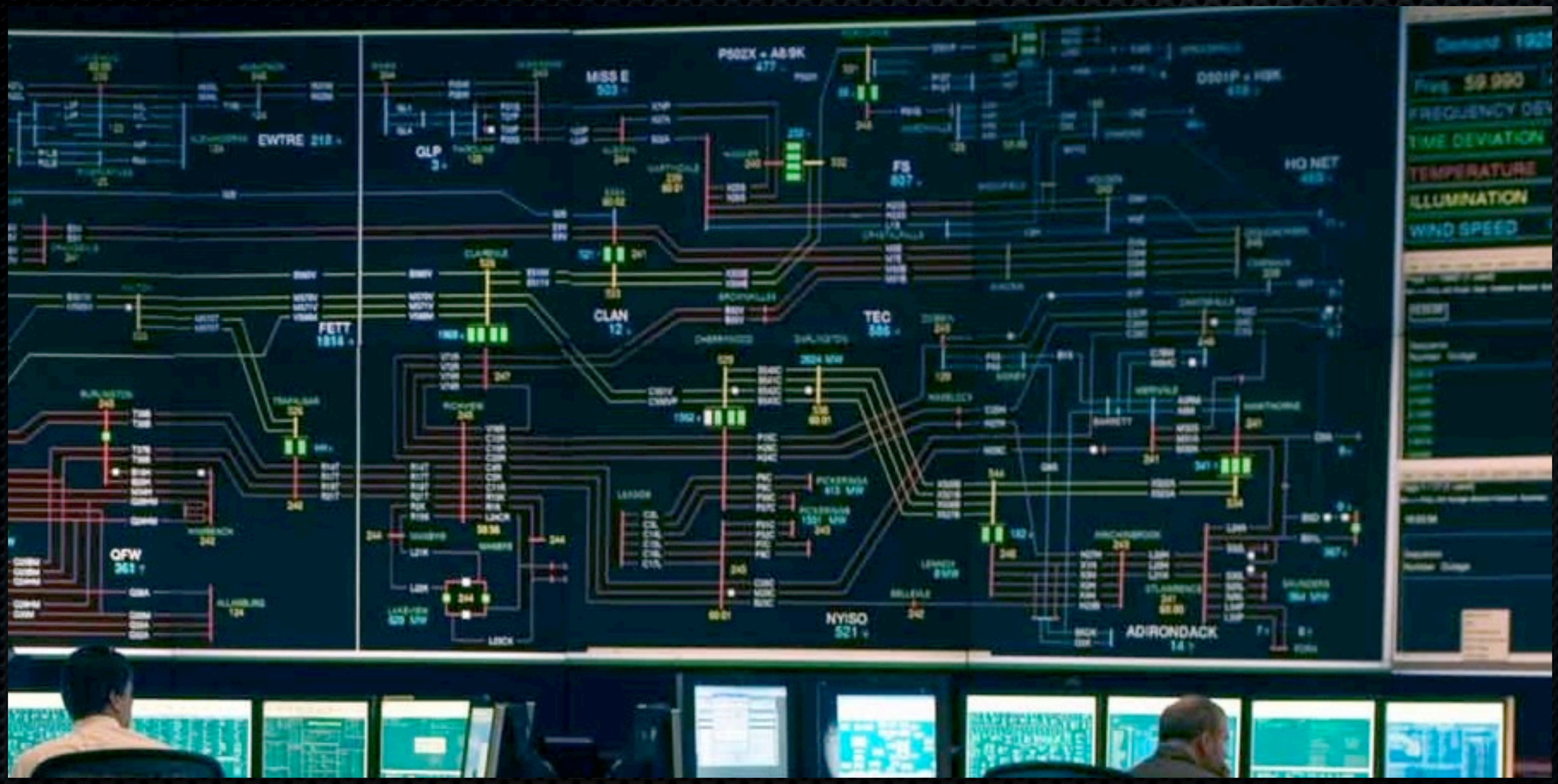


Oh, you forgot about testing



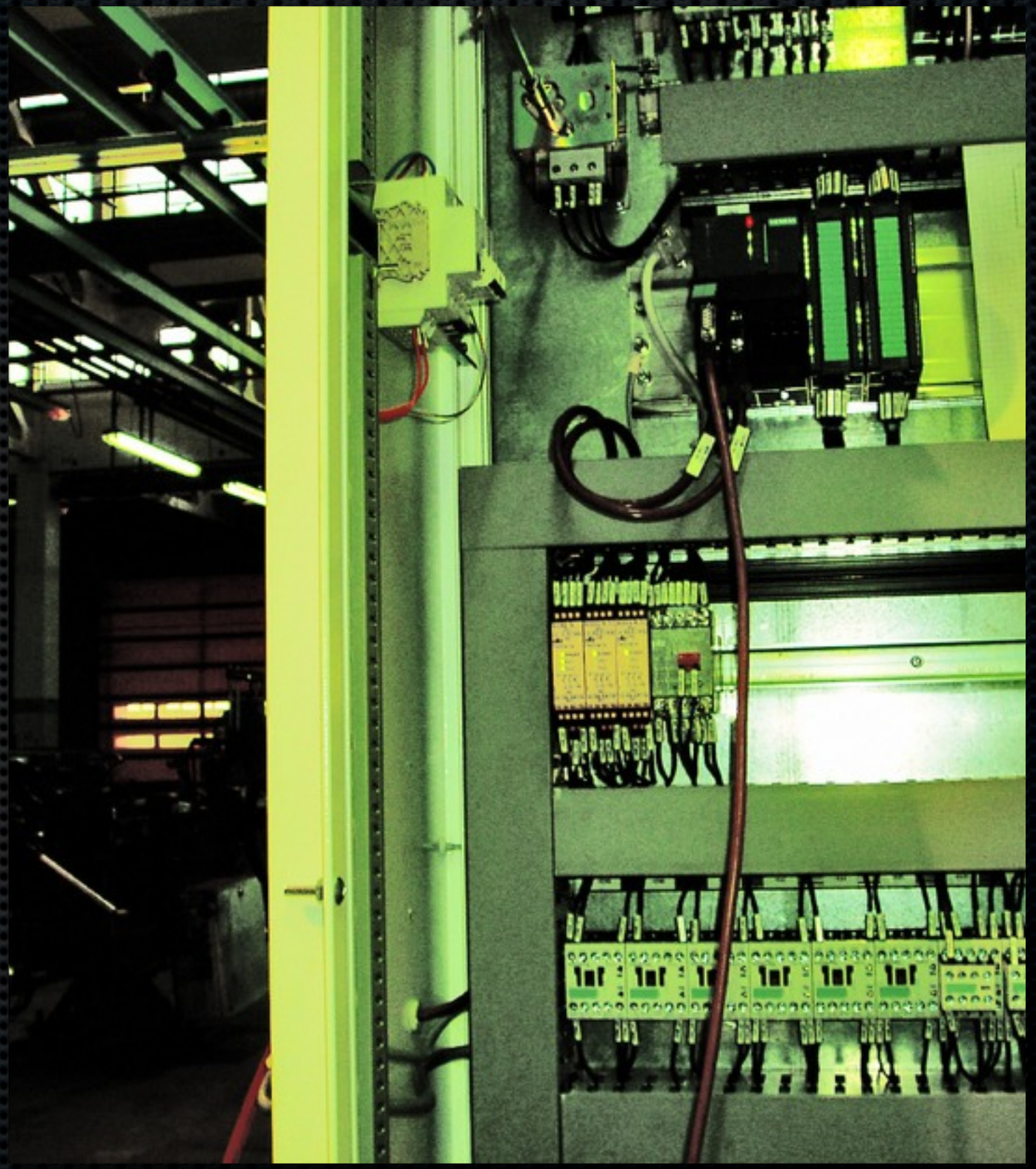
Oh, you forgot about people

Oh, you forgot about people



What if it really is SCADA?

Stuff breaks



All the &*^$ing time

And it gets fixed

And it gets fixed

And you never noticed

And you never noticed

And you never noticed

And you never noticed

But... WAIT! What about the Aurora Explosion Demo Awesome Video??????

Oh yeah, and BTW...

Smart meters aren't SCADA

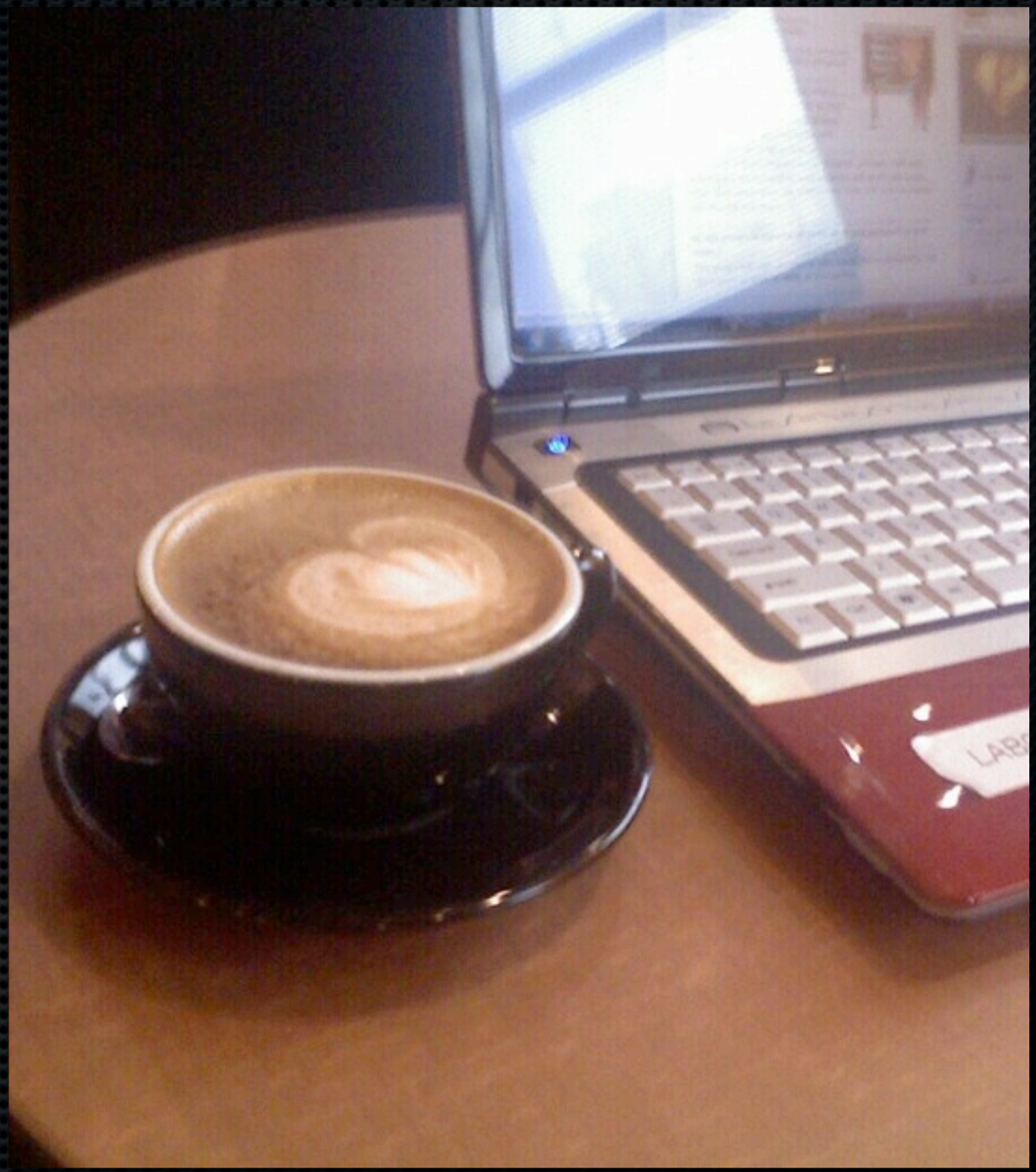
4/ Practical Positive Things

You can understand this stuff

You can help

They need you

You need to suck it up



It's time to learn before teaching

It's time to learn before teaching

5/ You Wouldn't Believe Me If I Told You

The Organization is against you

Your prima donna attitude is against you

Your age is against you

It's time to start hacking

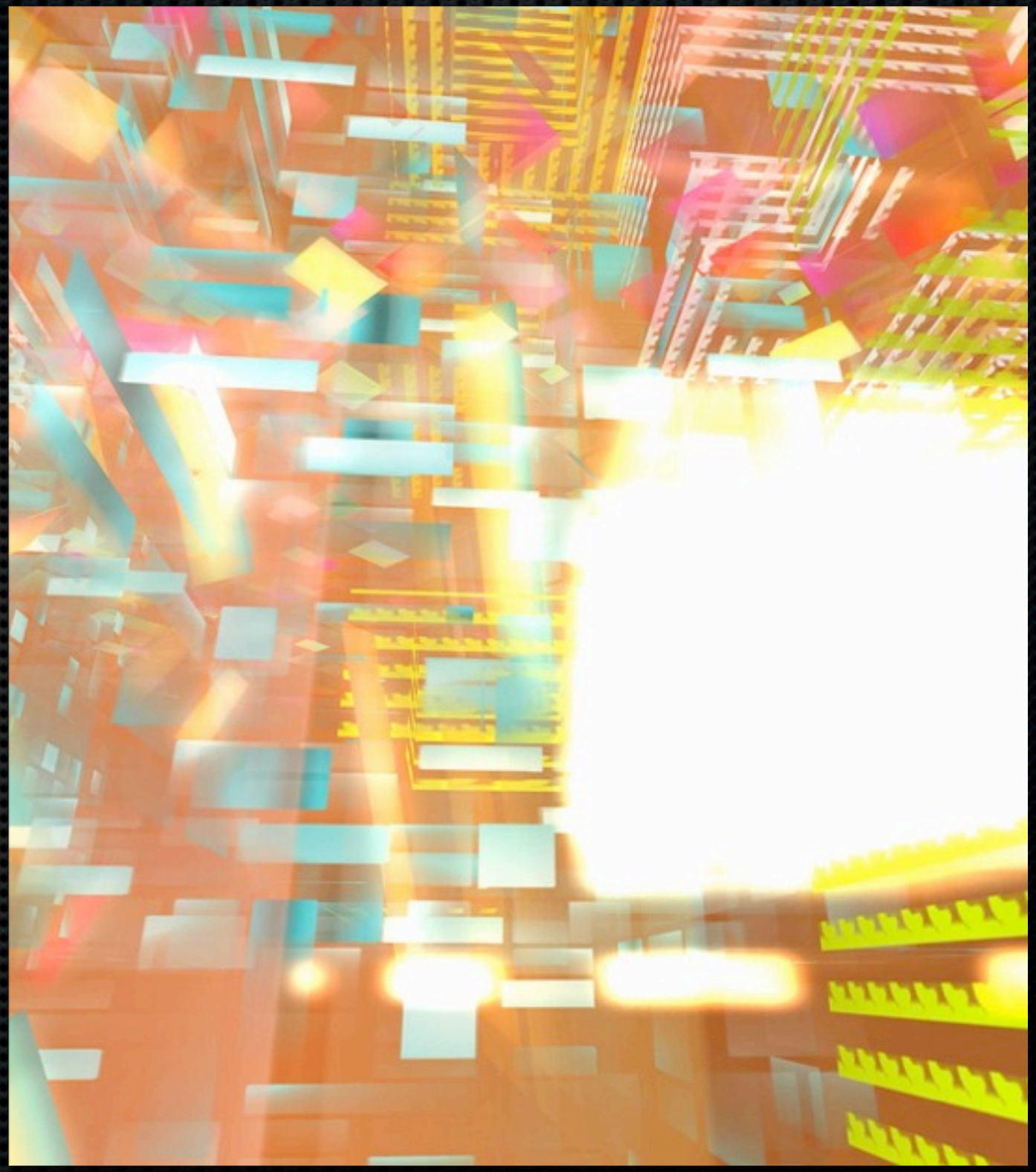
First you hack the org

Then you own their asses

Then you own their asses

6/ Movies Would Have You Believe

It's a mad mad graphical awesome world

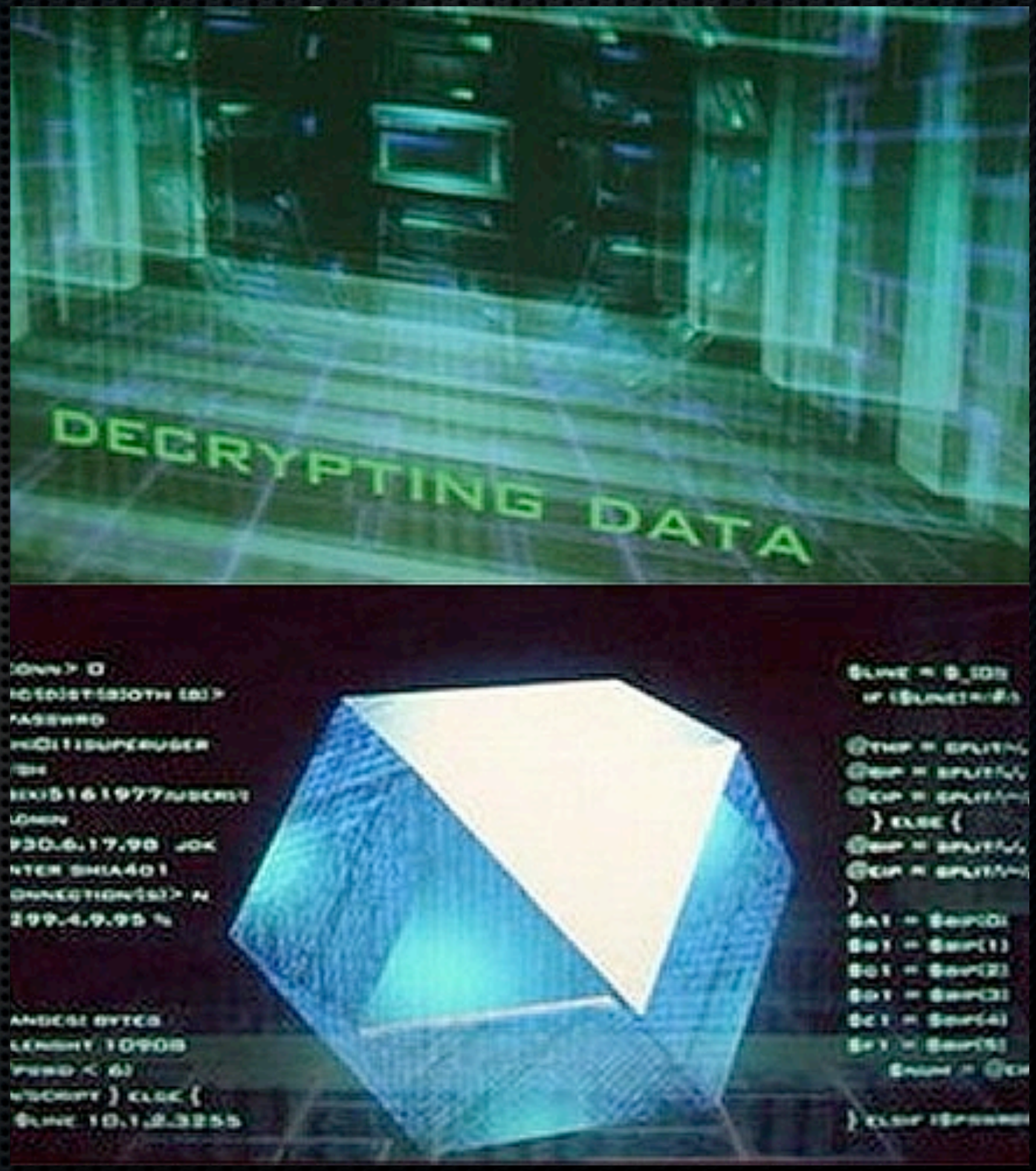


It's a mad mad graphical awesome world

It's a mad mad graphical awesome world

It's a mad mad graphical awesome world

It's a mad mad graphical awesome world



It's a mad mad graphical awesome world

It's a mad mad graphical awesome world

What an afternoon at the console really feels like

What an afternoon at the console really feels like

What an afternoon at the console really feels like

7/ The Media Hypes It As If...

CYBER CYBER CYBER CYBER

CYBER CYBER CYBER CYBER

CYBER CYBER CYBER CYBER

CYBER CYBER CYBER CYBER

CYBER CYBER CYBER APT !

There's a hacker behind the bush

Apr 8, 2010 5:11 pm US/Central

Did Hackers Cause A Meltdown?

AUSTIN (CBS 11 / TXA 21) — A lot of Texa
with the state's big appliance rebate progra
yesterday. It also ended yesterday, becaus
million allocated to the program was used u
end of the day.

We heard from dozens of people who said
unsuccessfully to access the program's wel
number to participate in the program. The
number were both overloaded when the pro

There's a hacker behind the bush

There's a hacker behind the bush

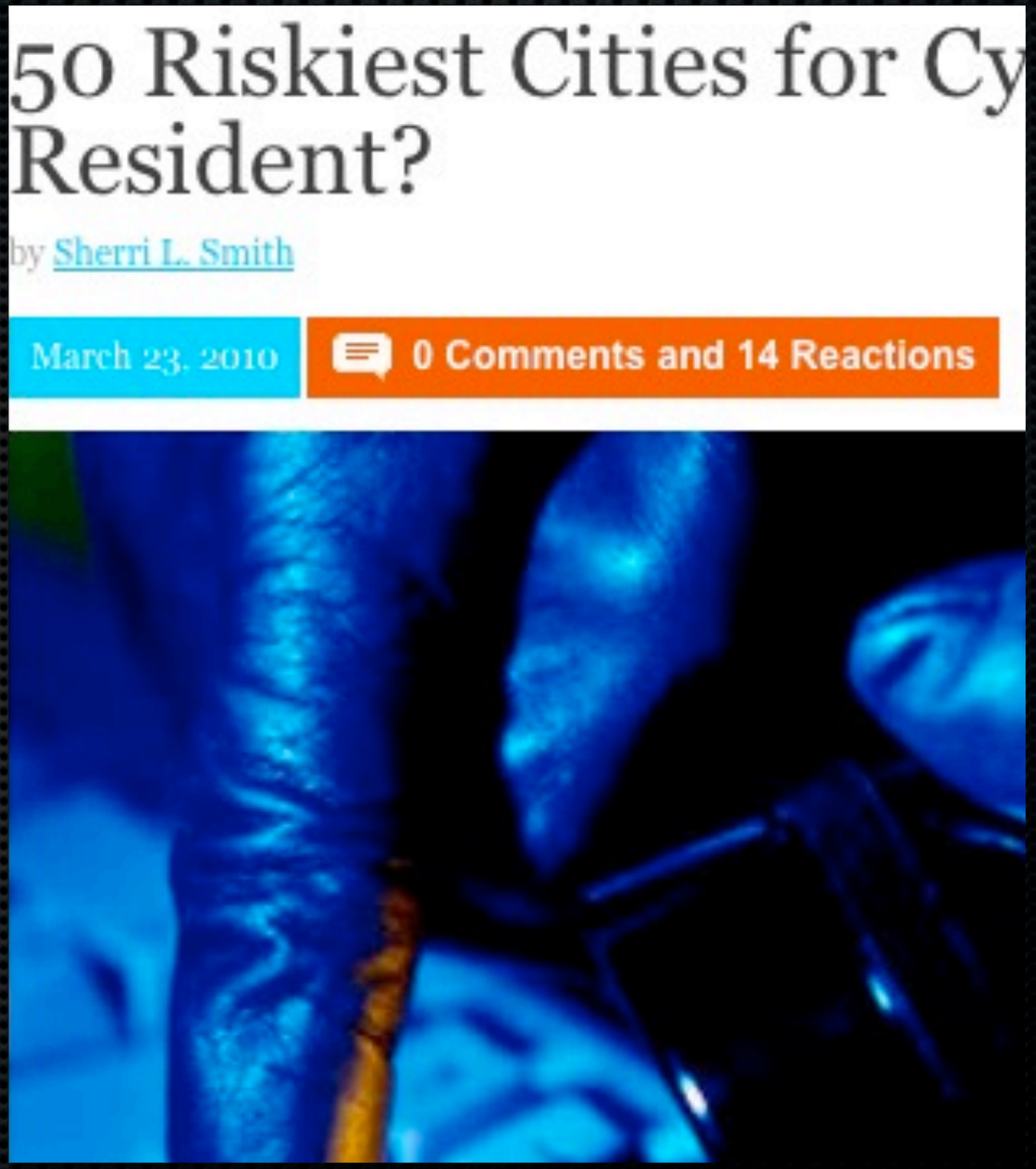
Weapons Of Mass Disruption

Andy Greenberg, 04.08.10, 10:40 AM EDT

Forbes Magazine dated April 26, 2010

The U.S. ignored Richard Clarke's warnings about al Qaeda. Will we heed his call about the looming danger of cyberwar?

There's a hacker behind the bush



There's a hacker behind the bush

FEATURES

Power surge: SCADA inc

Dan Kaplan November 04, 2008

PRINT EMAIL REPRIN

Last fall, when a Department of Hor
video depicted a turbine exploding i
hacker attack, viewers may have be
the end.

A 14yo in Mom's basement

A 14yo in Mom's basement

A 14yo in Mom's basement

L337 cadre of soldiers

L337 cadre of supersoldiers

L337 cadre of genetically engineered supersoldiers

Killer Tubes

8/ Bad Shit That Actually Happened

Not necessarily public news.

9/ What Could Have Saved It

Superheroes

Superheroes, Ninjas

Superheroes, Ninjas and Pirates

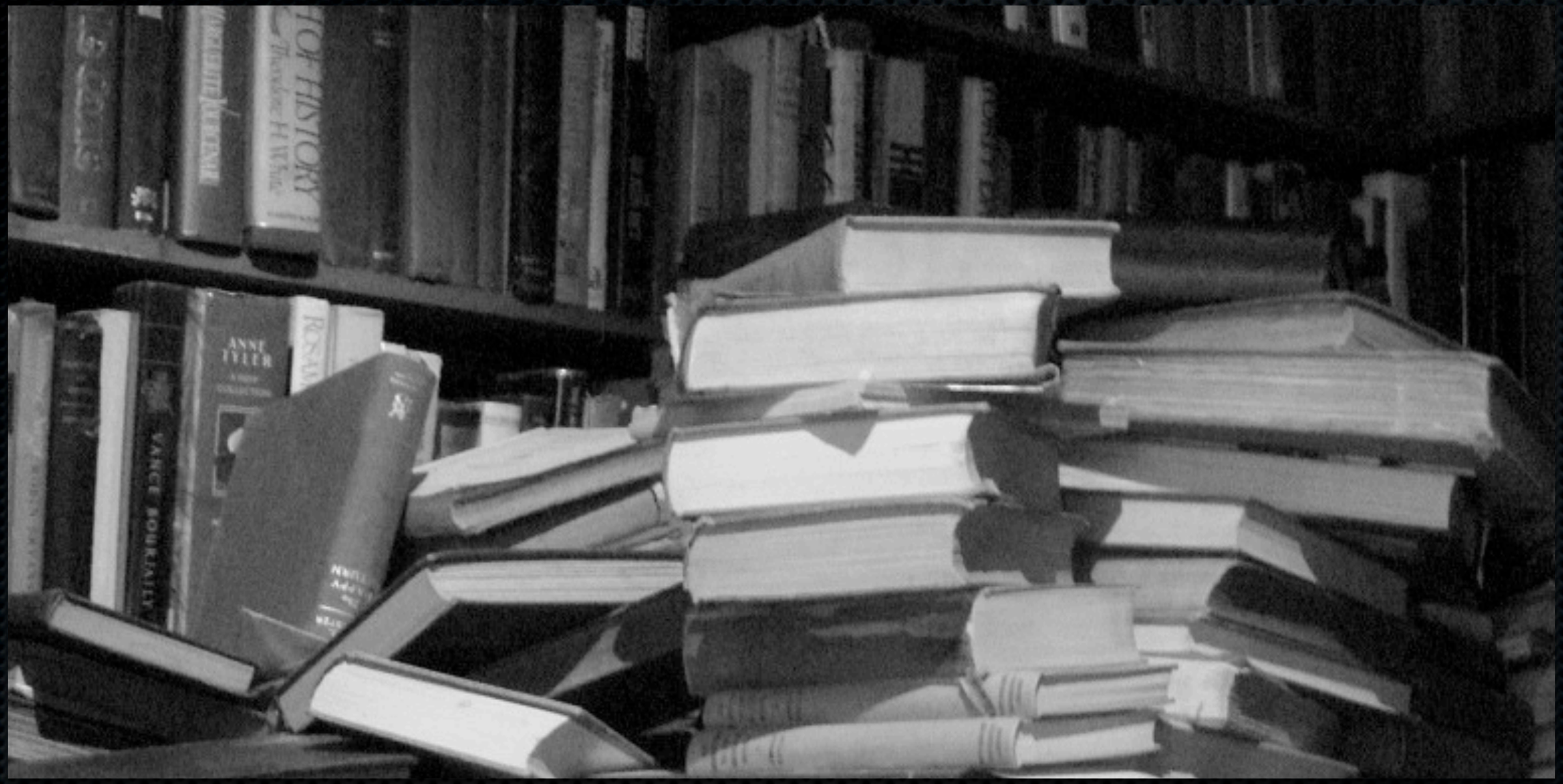
Following Instructions

Or, not sucking at implementation

Or, doing what you're told

Or, stuff that has nothing at all to do with computers

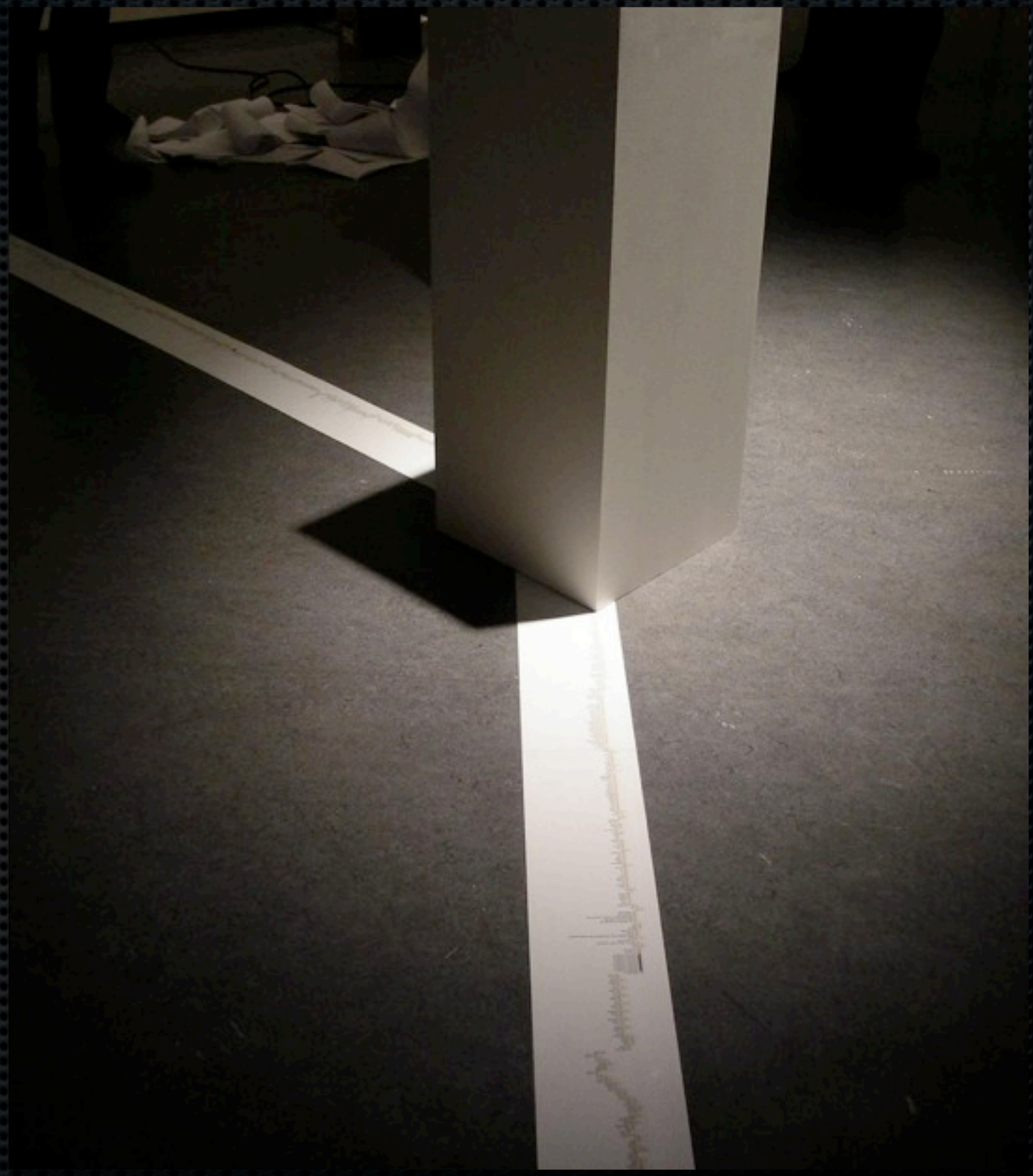
10/ What You Can Do - Little Picture



Learn

Stop listening to "experts"

Modest changes, massive results



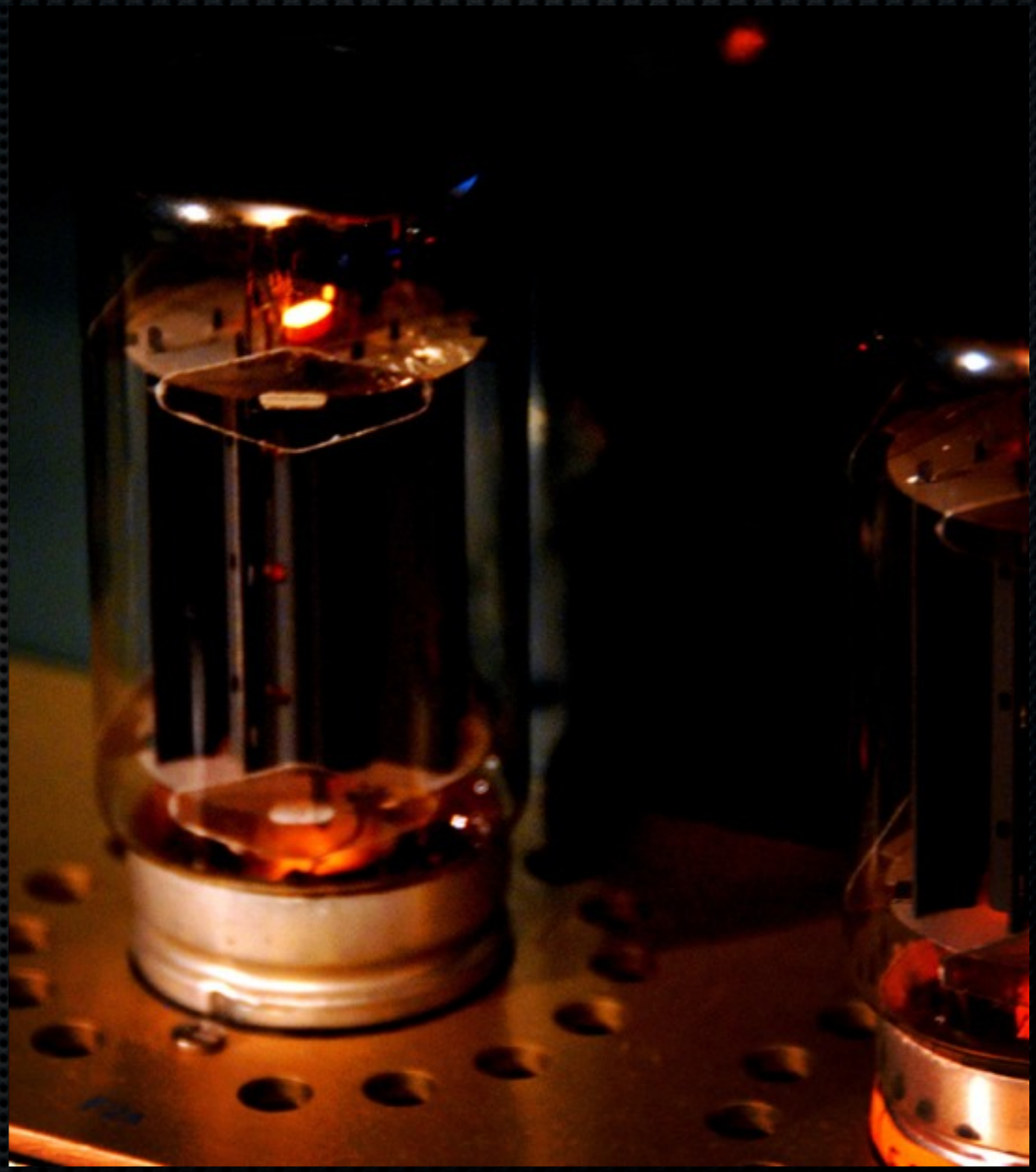
11/ What You Can Do - Big Picture

Stop feeding the trolls

Avoid being 'that person'

Press for sane acquisitions

Study past success



Study past success

Q & A

@myrcurial
myrcurial@myrcurial.com

Credits, Links and Notices

Me: http://myrcurial.com and http://cyberdouchery.com and sometimes http://liquidmatrix.org/blog

Thanks: All of you, My Family, Friends, Jeff Moss (for demanding this talk) Ping, Toni, and the rest of the Blackhat Team.

Mentors/Luminaries: D. Anderson, M. Fabro, D. Peterson, J. Brodsky, R. Southworth, M. Sachs, C. Jager, B. Radvanovsky and J. Weiss (borrowed material from all)

Inspiration: twitter, fast music, caffeine, my lovely wife and hackerish children, blinky lights, shiny things, modafinil & altruism.