(Thanks Jinx!)

Tractor Jacking II

Special appearance by CAT, FORD, MF Etc…

brought to you by

Chris/Jesse

Overview

- **Setting the scene….**
  - What do we need to survive…and how will we loose it
  - Breaking it down

- **Tractors….Seriously?**
  - What started it, and why…
  - Methods for accomplishing the "evil genius plan"
  - Lynch mob time from the men in overalls….

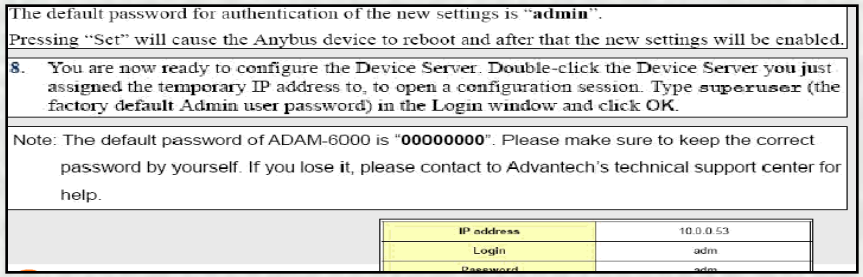
- **All things with engines:**
  - Mass transit, boats and other benign things.
  - B1's and Tanks
  - Boeing again, this time Dreamliners ☺

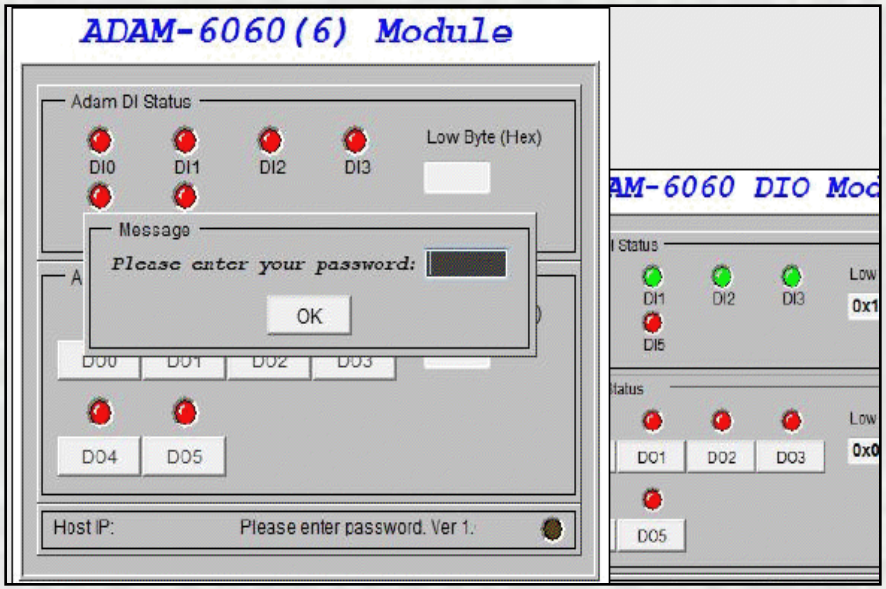
- **Q&A: Ask questions throughout….**

Survival Requirements

- **Heat** – Covered with SCADA Hacks (or we'll leave it up to the Stux variants ☺)
- **Light** – See above, traditional SCADA, or more updated SmartGrid hacks….pick your poison.
- **Water** –Web enabled pump monitors…open pump stations, SCADA and other vulnerabilities.
- **Communication** – All yours, we need to leave something
- **Transportation** – Got that covered here…
- **Food** – Got that covered at the source (See tractors) or we'll hit the supply chain.

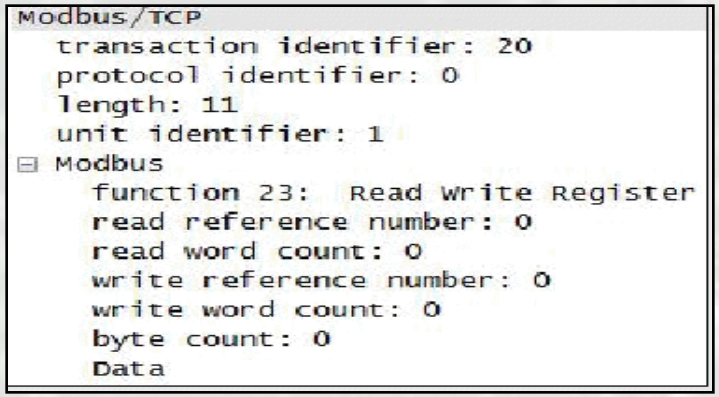
Heat-Check/Owned



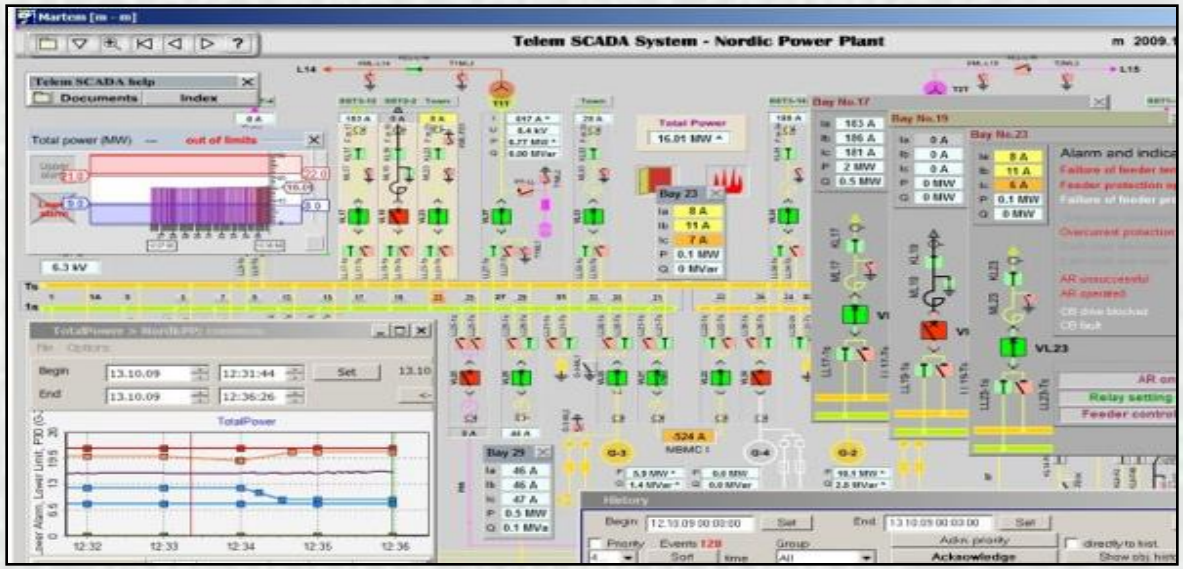


Top Left, Initiation string for cooling plant shutdown…attached to a reactor. Got to love lazy days at the coffee shop…(pwd=00000000)

Right, reconfiguring a digital relay to blackout a city, or take down a transport system?



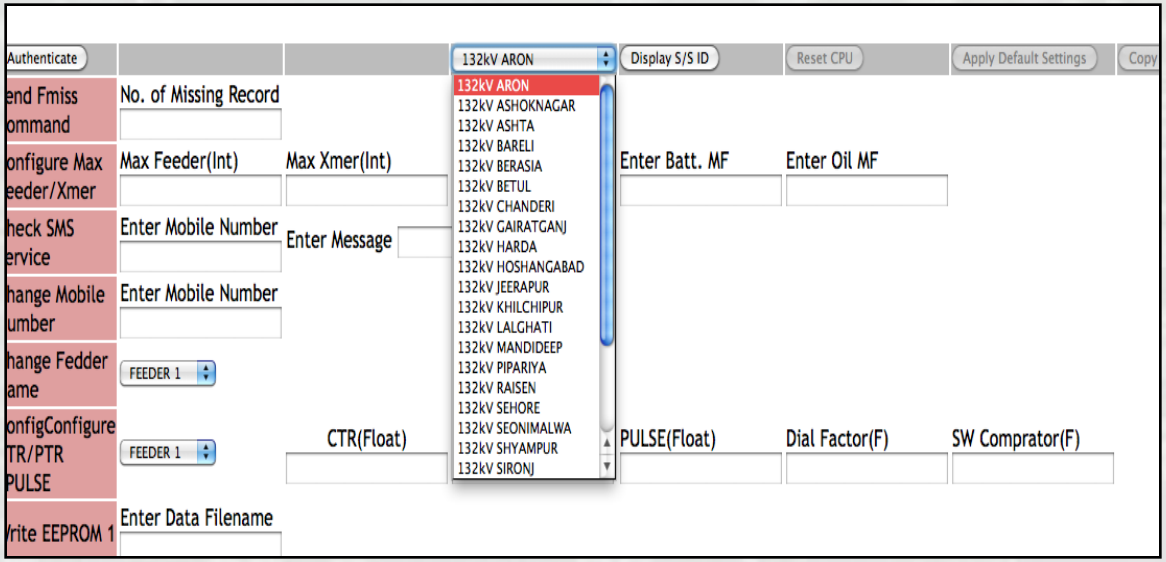
Light – Let there be Dark….



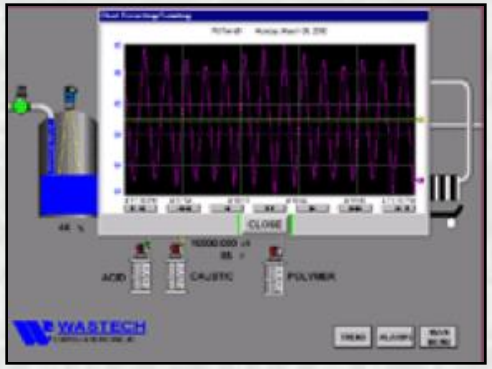
Nordic Power, Terminal access to entire SCADA system, open thanks to a well described network configuration, identified IP and our RDP friend running as Admin.

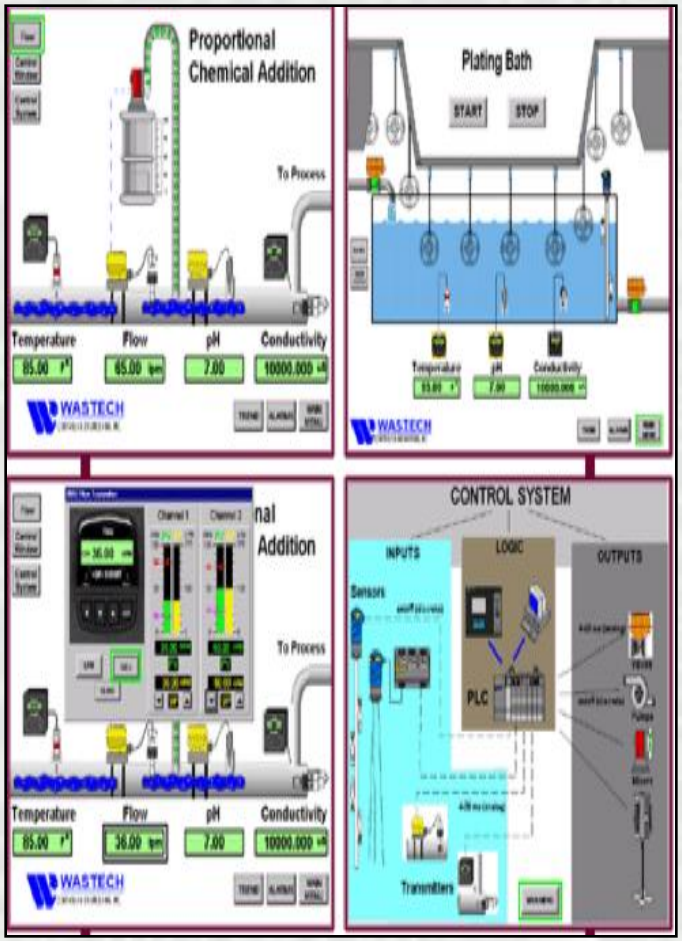
Just don't ask, I needed another screenshot for SCADA/Electrical systems, searched on the net, found a wide open "web interface" to all these systems…

FTP open too, load away…

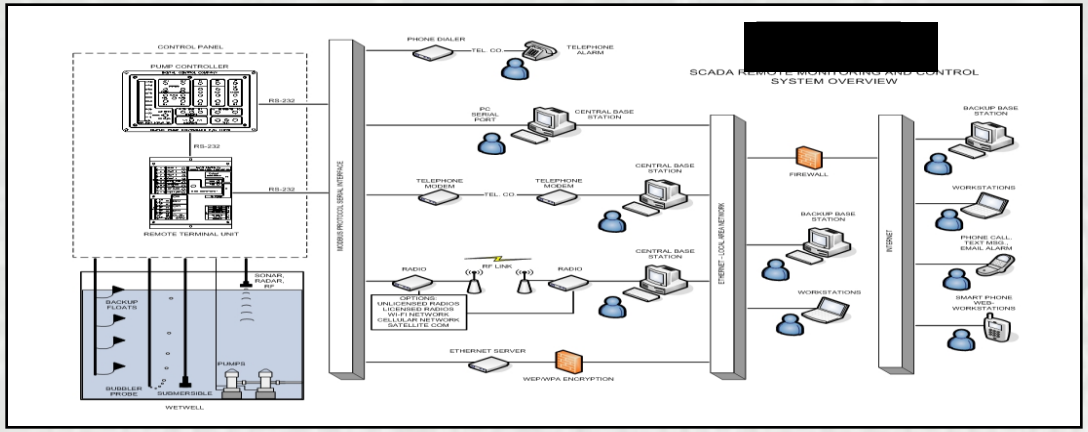


Water? - Yea, got that too…

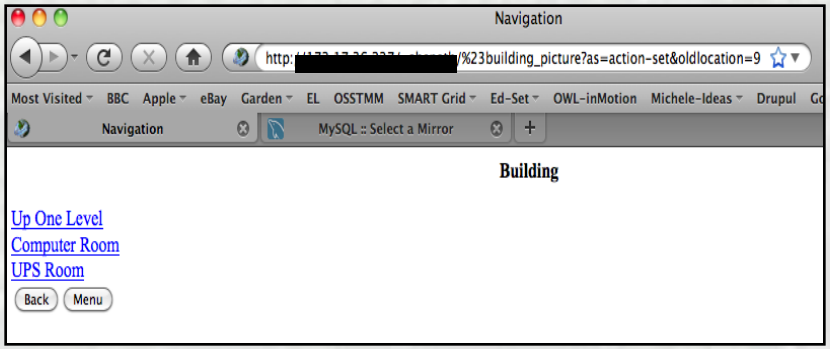




SCADA and water treatment above and to the side, and someone kindly posting the entire internal configuration of their water distribution plant below, including remote WiFi AP ID/PWD



Communication - Done

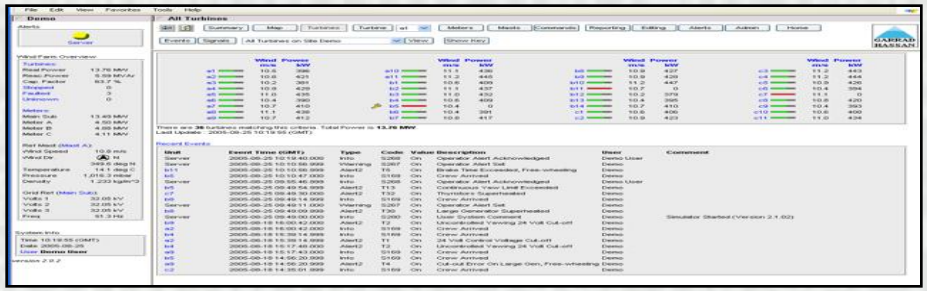


Environmental controls for buildings, including Datacenter and UPS Suite. Mostly web enabled…..and 3rd party accessible

First you are cooked……

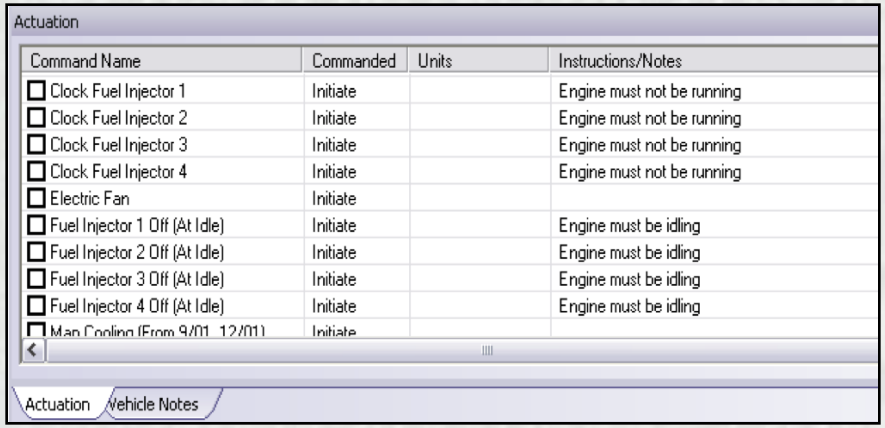
Then, using the devices to the right, it's possible to duplicated your RFID tags, and lock you out of the Datacenter……

So now you get to watch from afar…

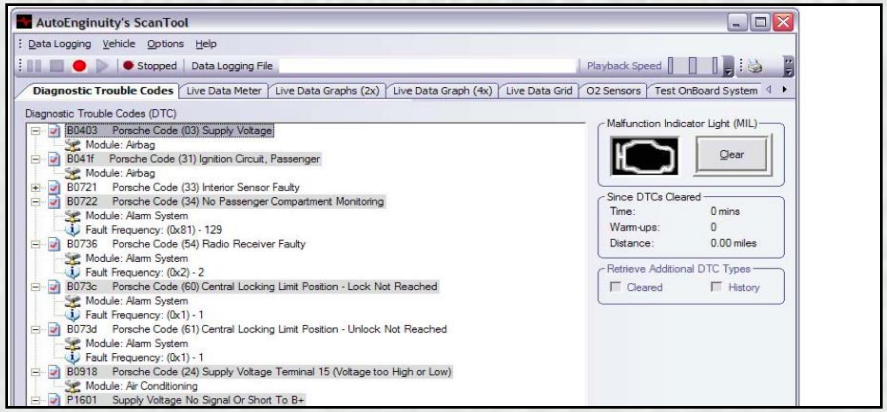


As a SCADA vulnerability is used to traverse the power grid and turn off your electricity ☺ …Would Sir/Madam Like their server rare, medium or well done?

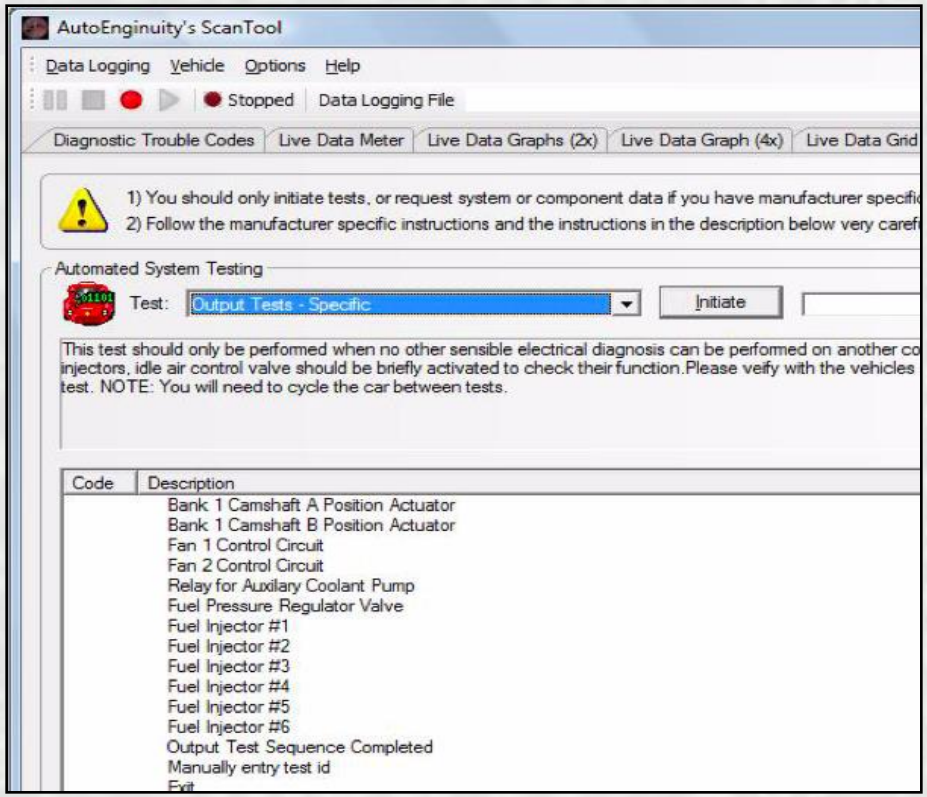
Transportation-Owned



Mercedes S600 interface



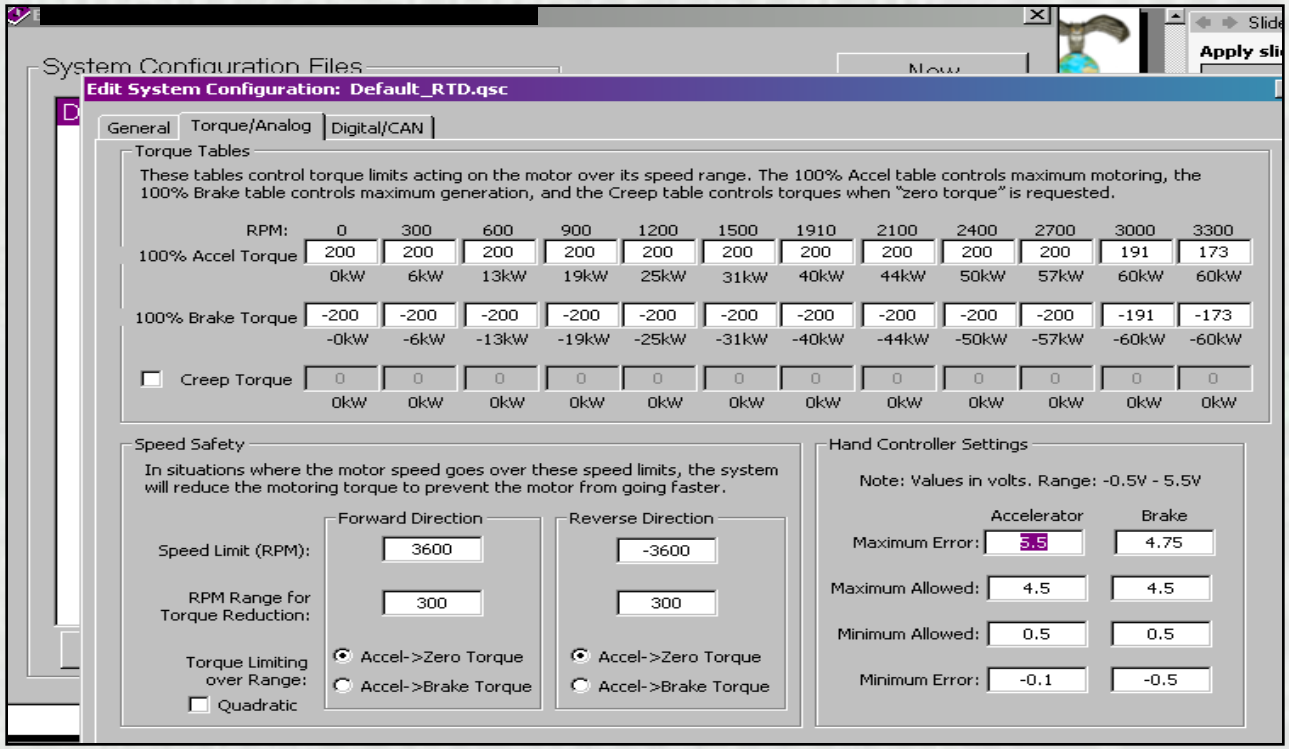
Porsche Interface



Main Audi/VW group interface, this was done on an A8L

Think of all the fun you could have bringing the Presidential motorcade to a standstill in the middle of DC one day…(Kidding, honest)

Mass Transit - Check



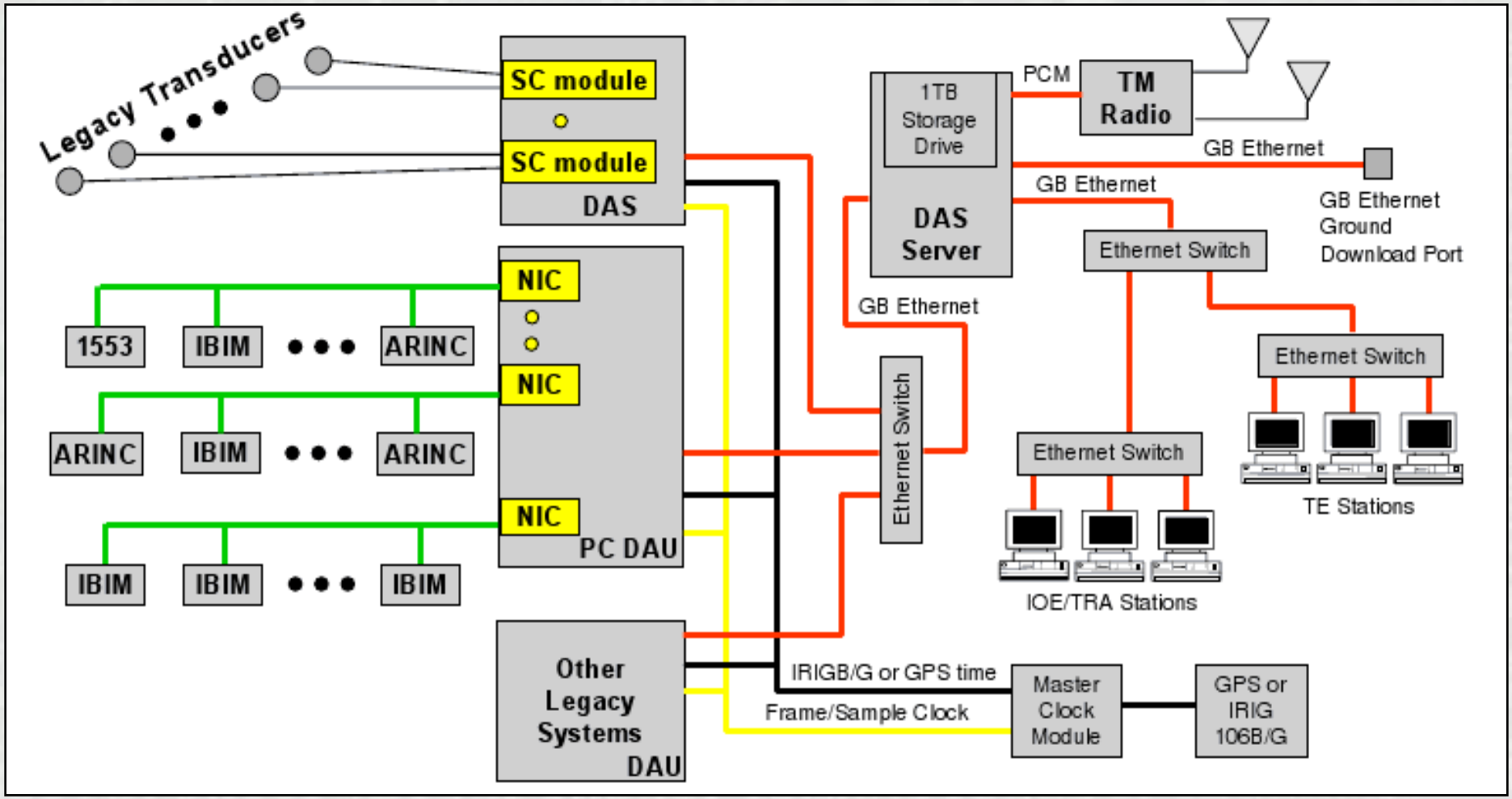
Management software for the hybrid engines, this also works for the mall type busses (tried and tested)

Concept is still the same, the AP needs to be configured for the bus to recognize and associate.

Next, simple 4 digit pin, either crack or social engineer it, and then fire up the UQM Motor S/W

There's two options on these types of assessments, either a rapid re-flash of the configuration files (UQM configuration package) or the "Reader" which can be configured to run either wireless or Bluetooth over the Com1/3 port (serial re-mapped or just use O/S built in options)

Intellibus…and TTP (Tomorrow)



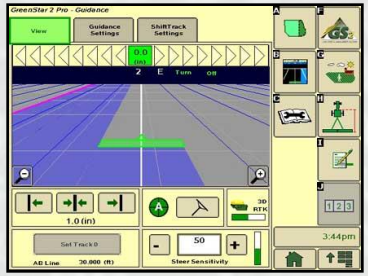
Thanks chaps for the graphics…..We'll demo some intriguing entry points!

Tractors…(Food)

- Why
  - Blame Jesse, and a late evening over pancakes
- Why again?
  - Because cars are single/one-time hits
  - Because nobody else has done it
  - 2 Billion metric tons of food (more on that later)
- Seriously?
  - Yes, seriously, bear with us on this…we are not going to give away the code, but we'll at least point you in the right direction.

How to Tractor Jack…

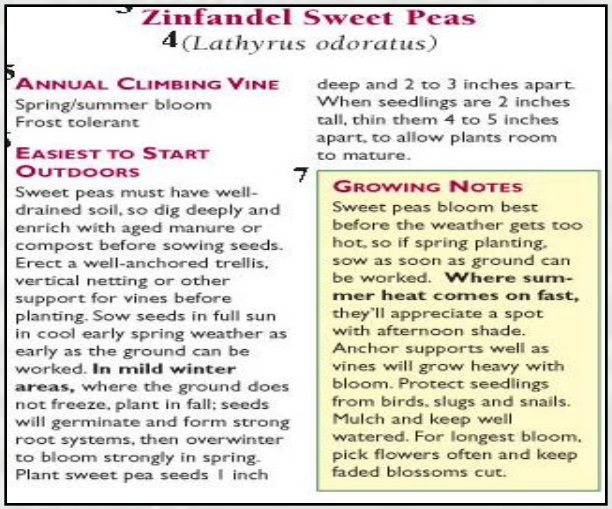
- Several components to the art of tractor configurations
- Main target needs to remain obliviously the distribution
- Same process as virus/trojan propagation, you need a host and a carrier
- Distributed architecture (We love FTP Servers)
- Simple code insertion and/or manipulation



Seeds 101

Vegetable	Catalog # range	avg. sds/oz	sds/100'	Pkt plants	distance apart	thin to	row spacing	seed depth	m s te
Amaranth	3000-12	25000	1/16 oz	100'	3"	6"	18"	1/8"	6
Artichoke	3608	180	T	10 pl	3'	No	2'	1/2"	6
Arugula	3020-29	13000	3g	60'	1"	4"	18"	1/4"	5
Asian Greens, assorted	3200-23	5000-10000	varies					1/4"	5
Basil	4414-4470	18000	5g	10-80'	1/2"	4"	18"	1/4"	6
Bean, Bush, Dry	200-79,326-90	90	8 oz	25'	3-4"	No	2-3'	1"	6
Bean, Fava	299	17	1#	12'	4-6"	No	2-3'	1"	5
Bean, Lima	323-325	65	1#	40-60'	4-6"	No	3'	1"	6
Bean, Pole	280-97,318,325,354	65	6 oz	10 pl/oz	6/pole	3/pole	3-4'	1"	6
Bean, Soy	480-99	85	5 oz	10'	3"	No	3'	1"	6
Beet	2100-99	2200	5/8 oz	20'	1"	2-4"	12-18"	1/2"	4
Broccoli	3300-29	7000	5g	.5g=10'	1"	24-30"	30"	1/4"	5
Brussels Sprouts	3330-49	5000	5g	.5g=10'	1"	24-30"	24-30"	1/4"	5
Cabbage	3350-99	7500	5g	.5g=10'	1"	24-30"	24-30"	1/4"	4
Carrot	2000-99	18000	10g	1/8oz=35'	1/4"-1/2"	1"	16-24"	1/2"	4
Cauliflower	3400-40	8000	4g	.5g=12'	1"	30"	30-36"	1/4"	4
Celery/Celeriac	3610-49	75000	T	500	8"	No	2-3'	1/8"	4
Chard	3030-42	800-2000	1-1/2 oz	5-13'	1"	3-6"	18-24"	1/2"	4
Chicory	3046-48	18000	T	300 pl	1'	No	2'	1/8"	5
Chinese Cabbage	3224-3225	9500	1/4 oz	25'	1/2"	12-18"	24-30"	1/4"	5
Corn, OP	500-699	100	4 oz	50'	3"	1'	3'	1"	5
Corn, hybrid	500-699	155	4 oz	50'	3"	1'	3'	1"	5

Too deep, as our Cannabis friends point out, and the see runs out of energy before it breaks to the surface



Zinfandel Sweet Peas

4 (Lathyrus odoratus)

ANNUAL CLIMBING VINE

Spring/summer bloom
Frost tolerant

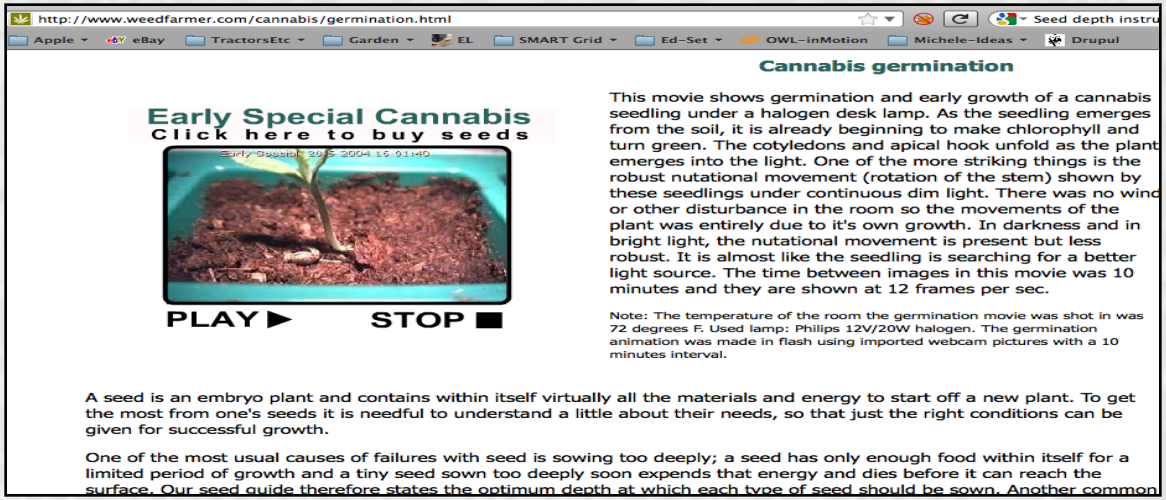
EASIEST TO START OUTDOORS

Sweet peas must have well-drained soil, so dig deeply and enrich with aged manure or compost before sowing seeds. Erect a well-anchored trellis, vertical netting or other support for vines before planting. Sow seeds in full sun in cool early spring weather as early as the ground can be worked. **In mild winter areas,** where the ground does not freeze, plant in fall; seeds will germinate and form strong root systems, then overwinter to bloom strongly in spring. Plant sweet pea seeds 1 inch deep and 2 to 3 inches apart. When seedlings are 2 inches tall, thin them 4 to 5 inches apart, to allow plants room to mature.

GROWING NOTES

Sweet peas bloom best before the weather gets too hot, so if spring planting, sow as soon as ground can be worked. **Where summer heat comes on fast,** they'll appreciate a spot with afternoon shade. Anchor supports well as vines will grow heavy with bloom. Protect seedlings from birds, slugs and snails. Mulch and keep well watered. For longest bloom, pick flowers often and keep faded blossoms cut.

Seeds need to be planted at a certain depth. Self contained "energy" only lasts for so long….too shallow and they are susceptible to the elements too early



http://www.weedfarmer.com/cannabis/germination.html

Cannabis germination

Early Special Cannabis
Click here to buy seeds

PLAY ▶ STOP ■

This movie shows germination and early growth of a cannabis seedling under a halogen desk lamp. As the seedling emerges from the soil, it is already beginning to make chlorophyll and turn green. The cotyledons and apical hook unfold as the plant emerges into the light. One of the more striking things is the robust nutational movement (rotation of the stem) shown by these seedlings under continuous dim light. There was no wind or other disturbance in the room so the movements of the plant was entirely due to it's own growth. In darkness and in bright light, the nutational movement is present but less robust. It is almost like the seedling is searching for a better light source. The time between images in this movie was 10 minutes and they are shown at 12 frames per sec.

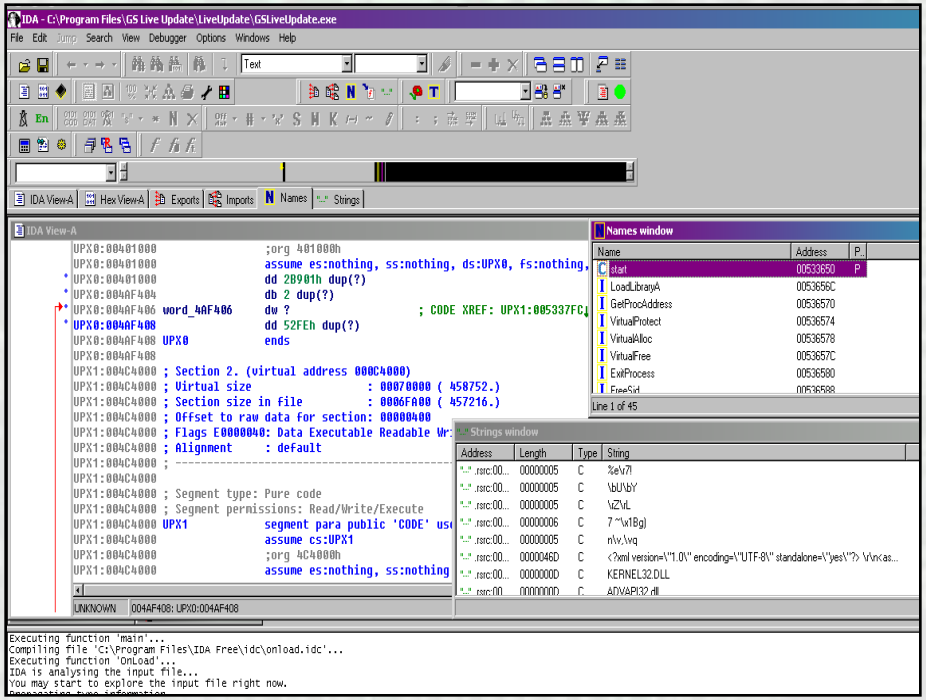
Note: The temperature of the room the germination movie was shot in was 72 degrees F. Used lamp: Philips 12V/20W halogen. The germination animation was made in flash using imported webcam pictures with a 10 minutes interval.

A seed is an embryo plant and contains within itself virtually all the materials and energy to start off a new plant. To get the most from one's seeds it is needful to understand a little about their needs, so that just the right conditions can be given for successful growth.

One of the most usual causes of failures with seed is sowing too deeply; a seed has only enough food within itself for a limited period of growth and a tiny seed sown too deeply soon expends that energy and dies before it can reach the surface. Our seed guide therefore states the optimum depth at which each type of seed should be sown. Another common

Method 1 - Variables

- Easier of the two methods, still involves a re-write of the configuration file, however the depth variable JUST needs to be fooled.
- Ensure within the code you at least attempt to "hide" the variables.
- GUI Depth has to remain "constant" whereas code depth variable can be adjusted for a different unit of measurement WYSIWYG (Not!).
- Within two of the consoles the variables are standard library input/outputs, so the knowledgebase necessary is minimal. (cin/cout) for one of them.
- In ALL cases a detailed understanding of ISOBUS will be necessary (Deere's ISOBUS Data Dictionary is 159 etc.)



IDA Pro Software…

Method 2 – 1+1=3 Code

- Some of the systems do not use simple depth variables, for these we need to do some math adjustment

- Code dependant upon manufacturer…

- Simply put we need to influence the libraries that are in place by adding in “our” own adjustments

- Specify (declare) the integer and then ensure the correct library variables are found, and then just simply cout/cin!

Deployment

- Coding done, deployment method is by utilizing the existing infrastructure (and programs deployed by manufacturers)

- Two options here
  - Upload to manufacturer's server (use your imagination!)
  - Direct influence of the endpoint devices (PC's that "manage" the in-tractor consoles) This can be done by identifying networks and then the correct open ports…hint (use a bloody sniffer & proxy on your code!)
  - Don't forget the language variants for the config files!

- Certify/Sign the code, a couple of the sneakier manufacturers have some level of security. Circumventing this is simply taking the original code, decompiling (IDA Etc) and then reverse engineering into the authentication methodology.

Now What?

- Code deployed, now it’s a matter of waiting for the updates to be picked up by the endpoint PC’s
- From PC’s (which automatically pick up updates) the consoles on-board are updated via USB cable/card/stick.
- As long as you’ve done your work correctly new configuration will be accepted by the terminal and adjusted/rates are now offset to your specifications.
- Our test subjects Yellow/Green tractors accepted the modified code on the second try...(the ☺ test)

Now We Wait…

- **Given all that's past the following happens:**
  - Crop sown March/April
  - Sprouting 2-4 weeks later (IF it were normal)
  - Configuration file 1 should have a shallow setting thus increasing frost and/or wind damage (roots etc) (1+1=1.5)

- **At this point crop producer realizes they have an issue, and re-seeding would occur, then we have two options.**
  - Same configuration file 1 would have the shallow setting thus increasing wind damage (roots etc) (1+1=1.5)
  - OR secondary configuration file is available that now has a depth variable of 1+1=4 (or more..) so crops would "eventually" come up…but too late for harvest
  - OR given we have access to planter, and it's possible that depth would be suspected, modify the spacing variable and decrease yield (seed weight variable in some Mnf.)

Target Audience

- **USA** – Corn, Wheat and Soy
- **Brazil** – Soybean, wheat and corn
- **Europe** – Wheat, barley and oilseed
- **China** – Wheat, barley, oilseed and rice
- **Russia** – Wheat, barley, corn and sunflower

Rough estimates we could affect approximately 1.5-2Billion metric ton of food production…not bad for some minor edits and coding to configuration files

Target Audience - Revised!

Due to the threat of lynch mob behavior from the Thotcon crew in Chicago we have **REMOVED** Barley from the target list (and hops)…thereby **preserving the BEER….** and still destroying food!

- **USA** – Corn, Wheat and Soy
- **Brazil** – Soybean, wheat and corn
- **Europe** – Wheat, and oilseed
- **China** – Wheat,, oilseed and rice
- **Russia** – Wheat, corn and sunflower

Rough estimates we could affect approximately **1.5-2Billion metric ton of food** production…not bad for some minor edits and coding to configuration files

Tractor Walkies….

Communication architectures:

- Distance (GSM/GPRS/EDGE)
- Near field, "follow the tractor"
- Field to Internet communications

My Data, Your Combine

Vector:

Not all farmers have their own major utilities (combines, trucks etc), utilizing a 3rd party service instead to harvest their crops at the optimum time:

How?

1. Measure the field (SCADA/WiFi)
2. Organized farming:
3. Shared architecture:
4. Trusted resources:
5. Future? (Seeds/Fertilizer)
6. Maintenance etc: