(Thanks Jinx!)

Planes, Trains and Automobiles

Special appearance by John Deere…

brought to you by

One World Labs (OWL) Research
Chris/Jesse

Overview

- **Setting the scene….**
  - What do we need to survive…and how will we loose it
  - Cars (updated from B-Sides…..with guest appearance from Boeing)
  - 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….

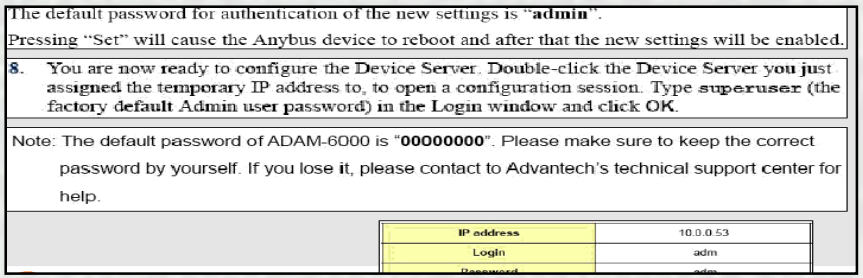
- **All things with engines:**
  - Mass transit, boats and other benign things.
  - B1's and Tanks
  - Boeing again, this time Dreamliners ☺

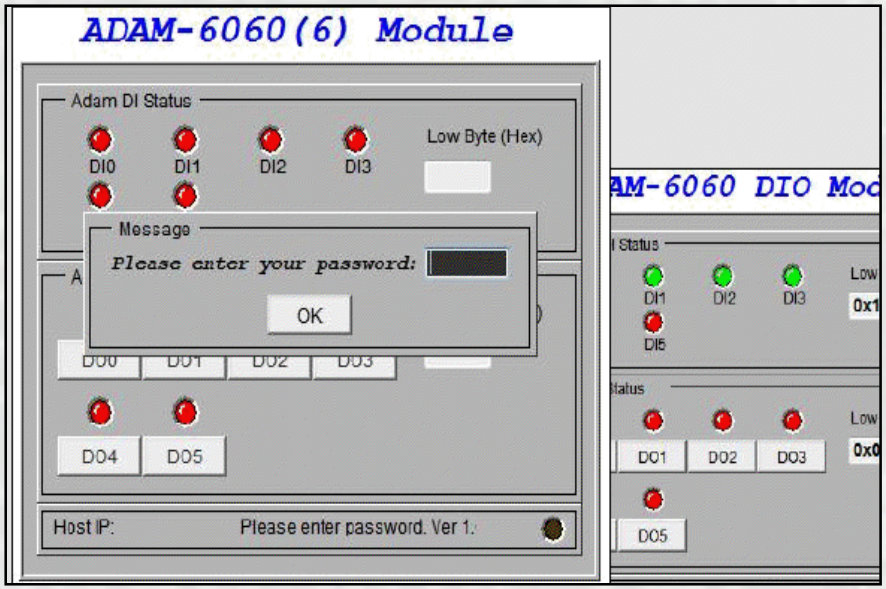
- **Q&A: Ask questions throughout….**

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.
- **Food** – Got that covered at the source (See tractors) or we'll hit the supply chain.
- **Communication** – All yours, we need to leave something
- **Transportation** – Got that covered here…

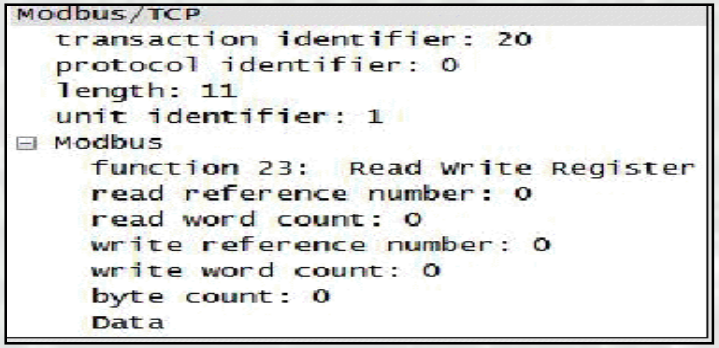
SCADA Networks



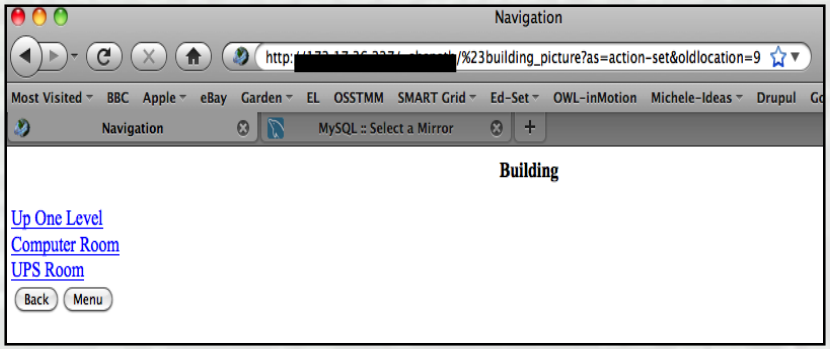


Top Left, Initiation string for cooling plant shutdown…attached to a reactor.

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



Worst Case… No Rules

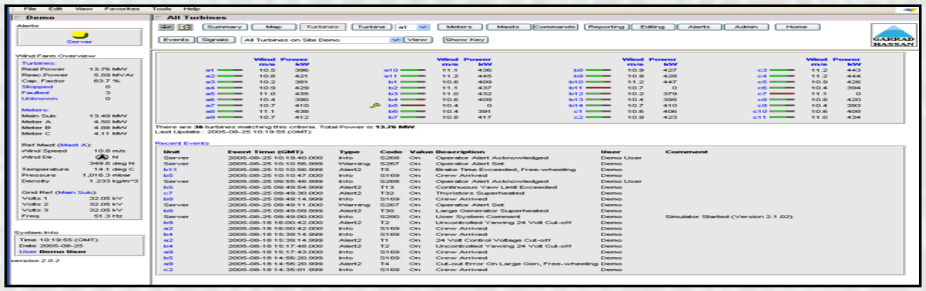


Environmental controls for buildings, including Datacenter and UPS Suite. Mostly web enabled…..and 3rd party accessible

First you are cooked……

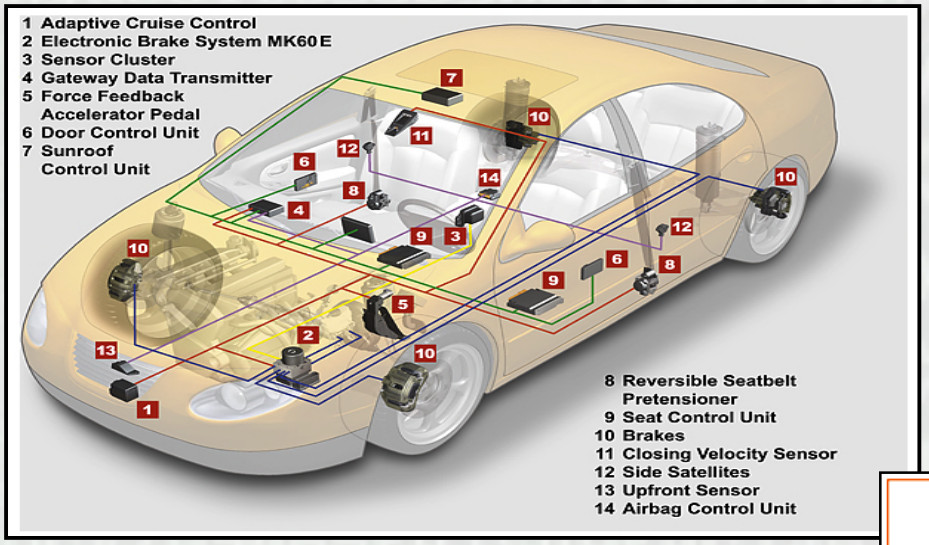
Then, using the devices to the right, it's possible to duplicated your RFID tags, and lock you out of the Datacenter……

So now you get to watch from afar…



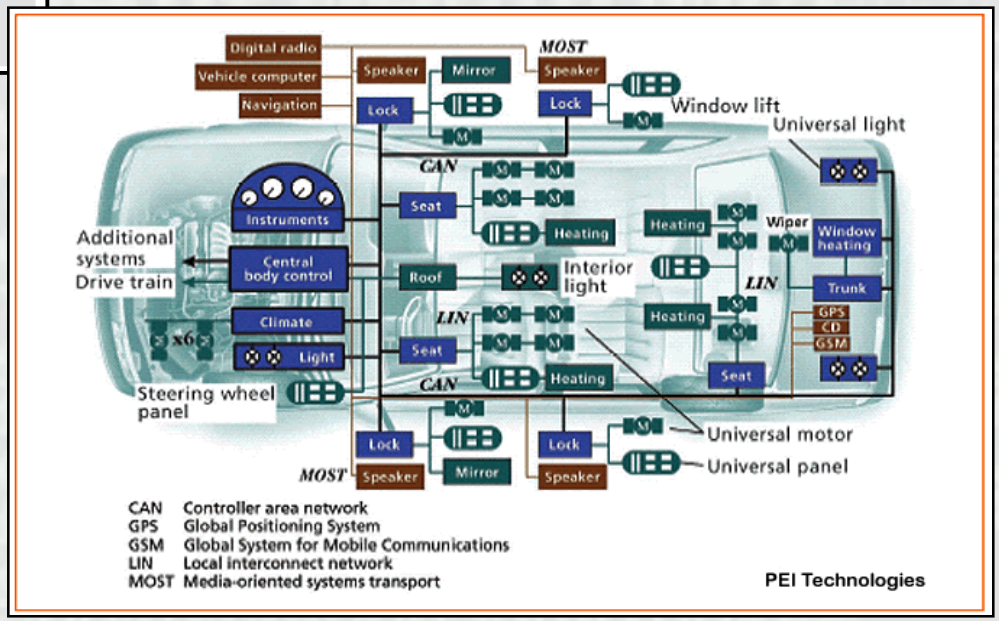
As a SCADA vulnerability is used to traverse the power grid and turn off your electricity ☺ …Would Sir/Madam Like their server rare, medium or well done?

Cars – Overview (and updates)



Main CAN networks within a vehicle, the image only shows a low number of devices attached to the networks.

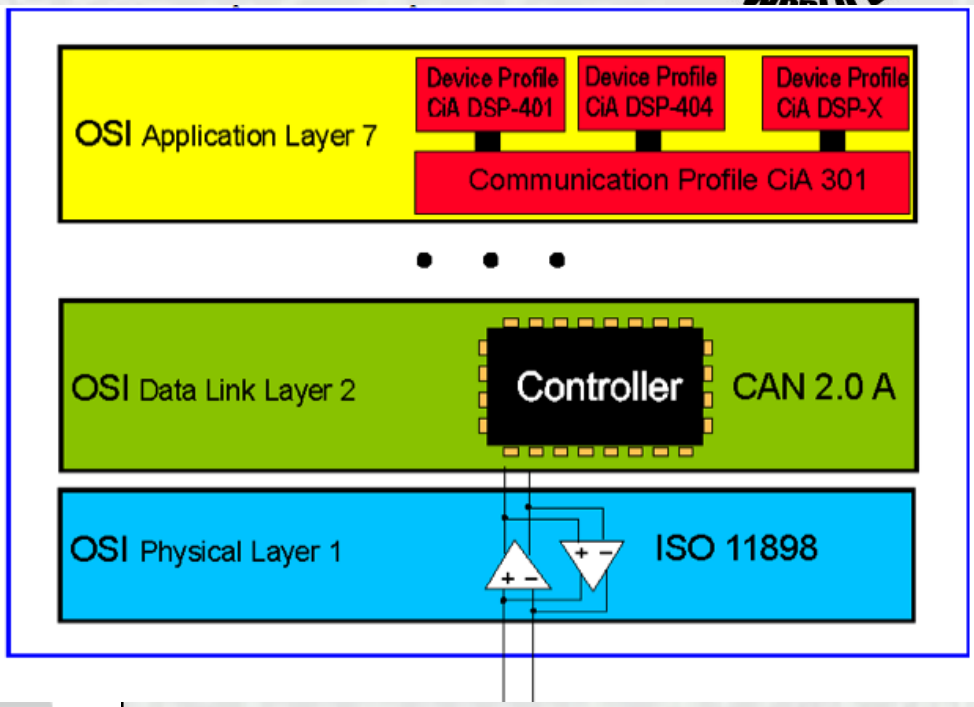
CAN and MOST networks interoperability within the vehicle. Primary access is via the Bluetooth interface which can be on either system (we love standards…not!)

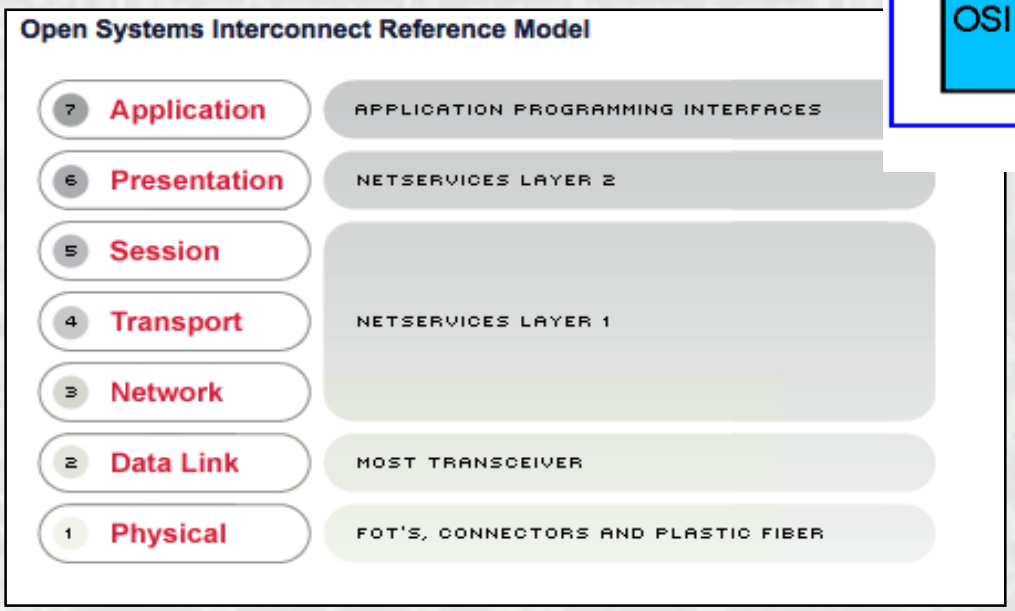


MOST Architecture

The communication profile defines that in a CANopen network there must be at least one master application and one or several slave applications, the main target for the management of this is the CGW (gateway module)

Applications being defined as ABS, Cruise control etc…



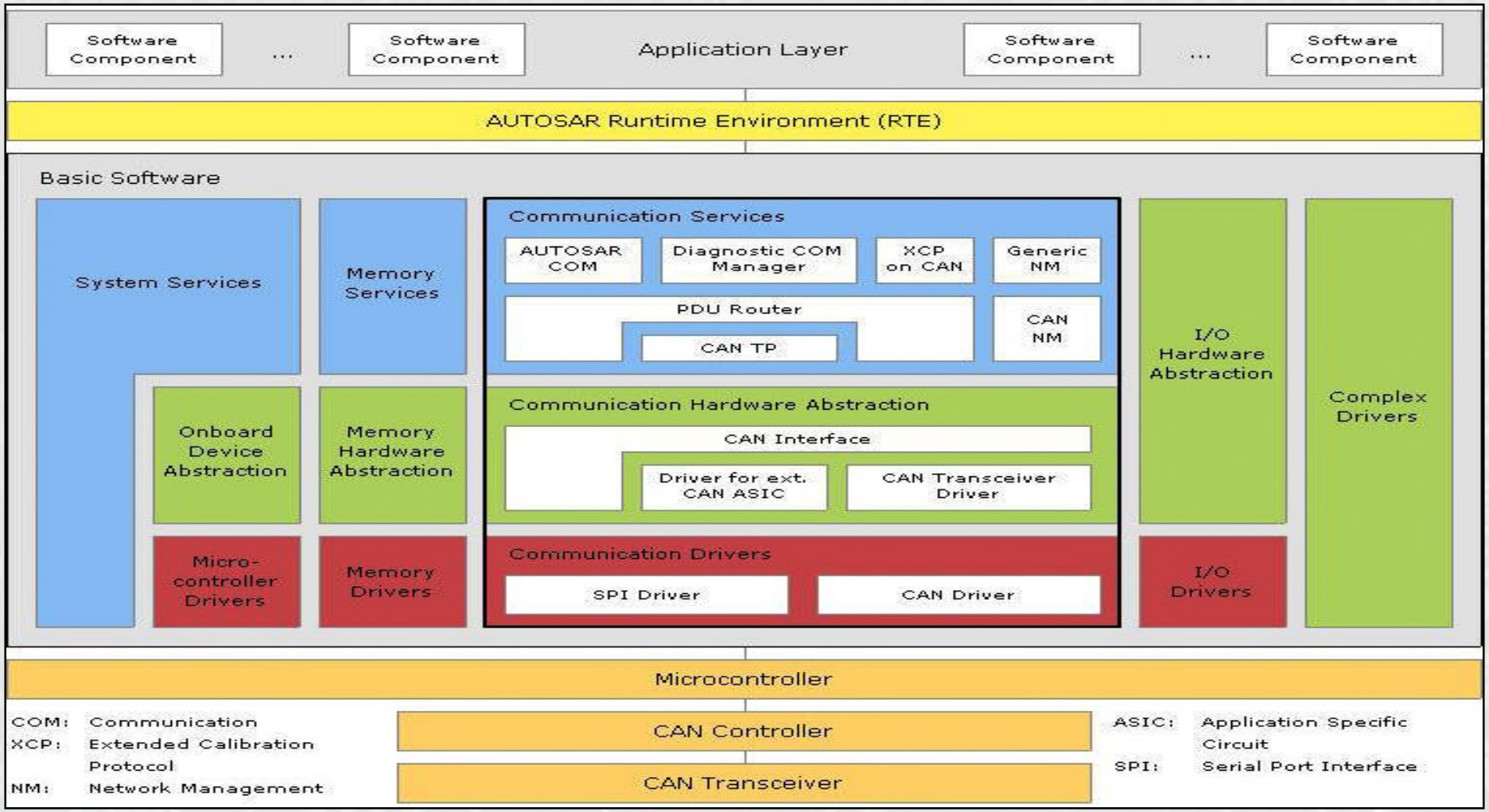


Every slave node contains a state machine with the four states called:
1. Initialization,
2. Pre-Operational
3. Operational
4. Prepared

There's primarily 5 different management messages that can be sent to these nodes:

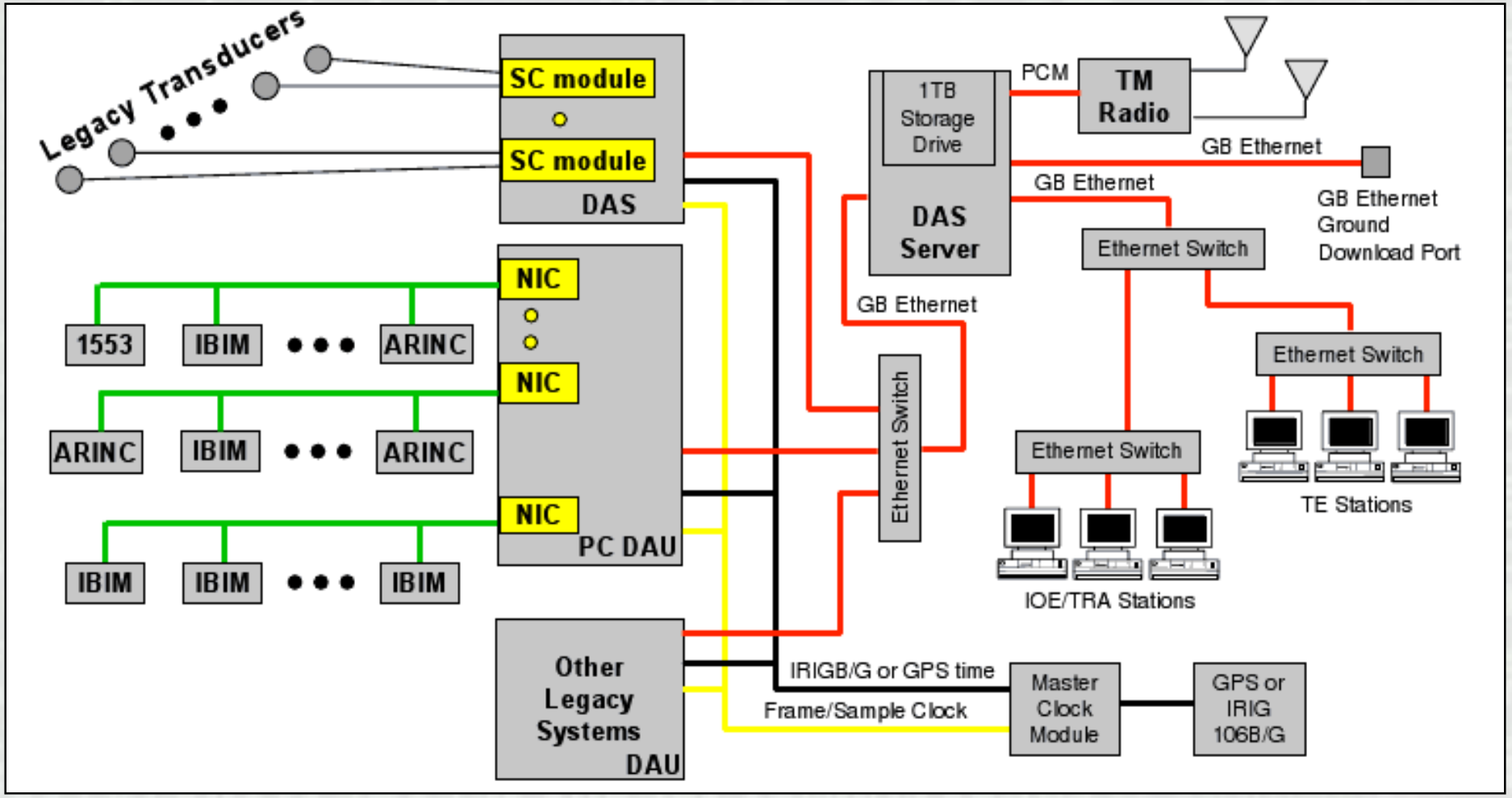
CAN (Bus) and AUTOSAR

(Controller Area Network) AND (AUTomotive Open System Architecture)



Thanks to jcelectronica.com for the graphics!

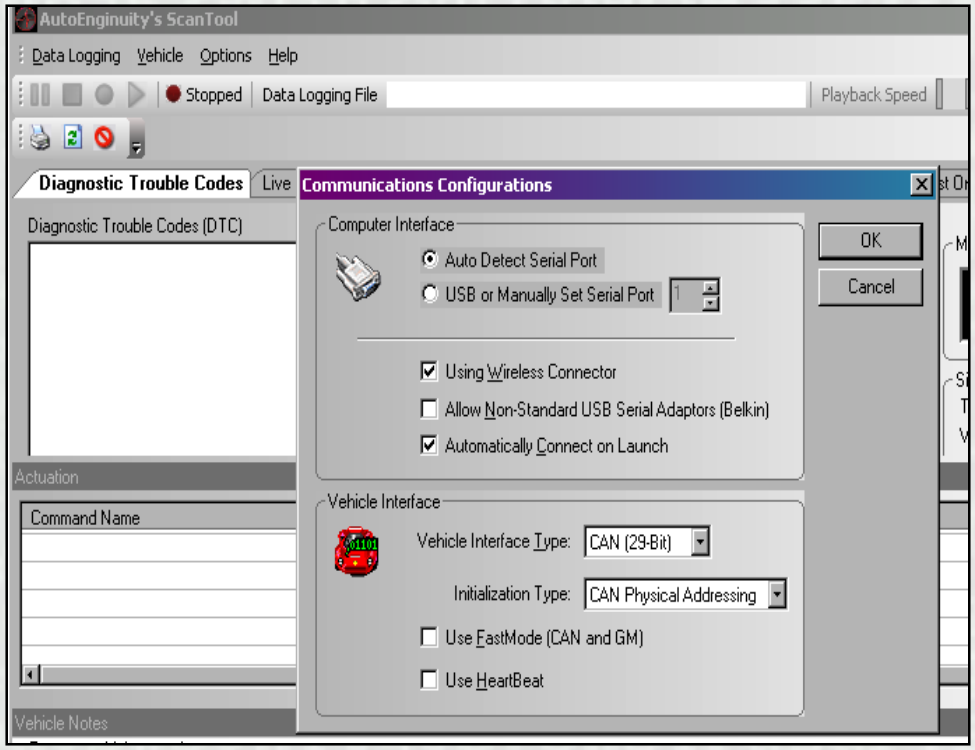
Intellibus Exploded

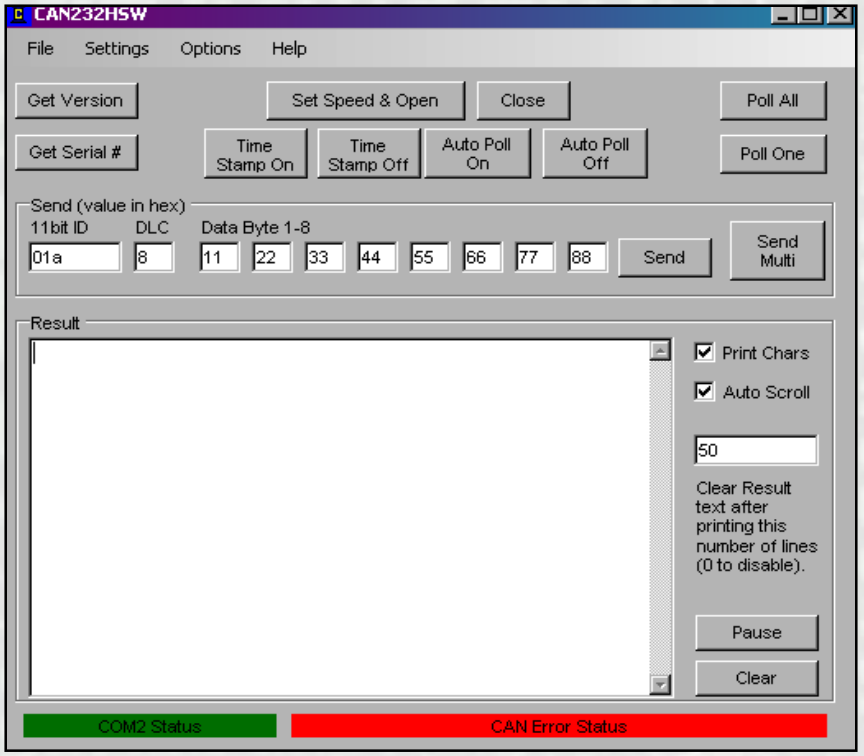


Thanks Boeing for the graphics…..now, pick your entry point!

The Easier Way……

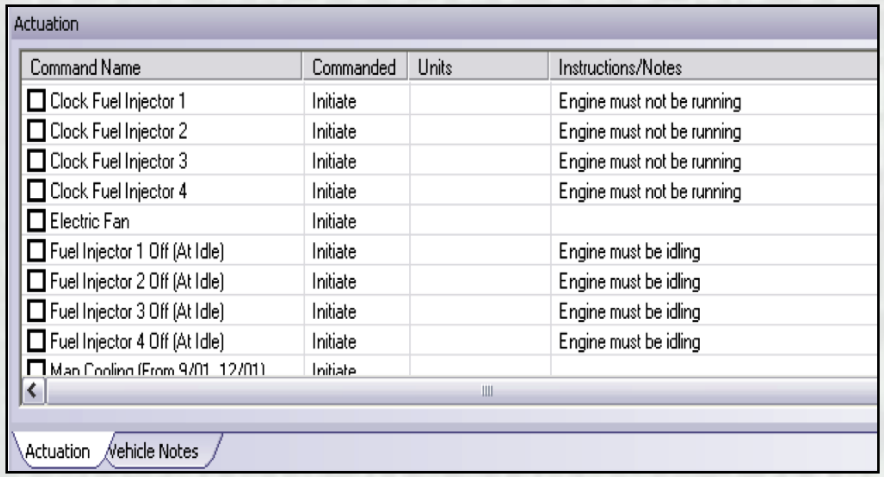
Vehicle tuning software freely available, most of the systems have the necessary embedded logging, monitoring and management software.



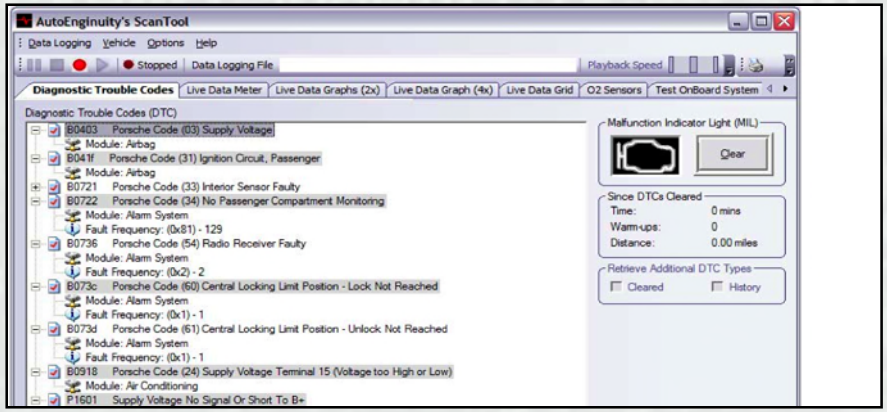


There is also logging software that once connected to the vehicle will initiate a sniffer/management interface to be able to query what devices are embedded. (ALL can be run via Bluetooth over RS232)

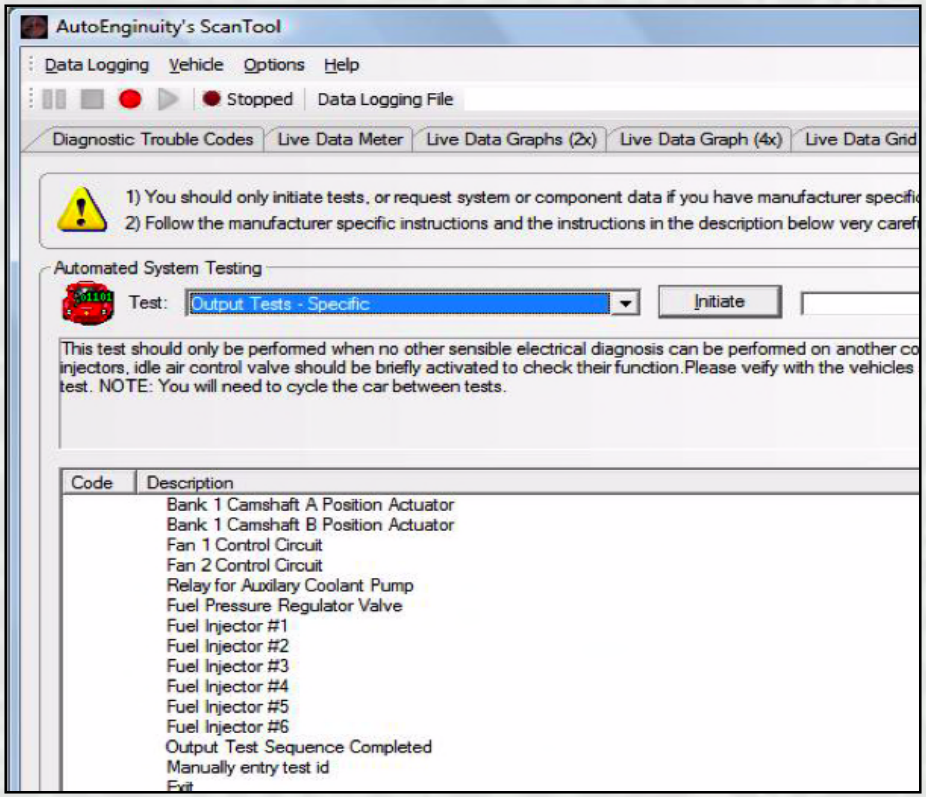
Our Test Subjects…



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)

Targets

Engine ignition (spark, timing

Emissions controls

Heating/air conditioning

Suspension systems

Lights, horn, wipers, defrosters …

Braking (anti-lock brakes)

Seat & pedal positions

Safety systems

Security systems

Fuel injection

Collision avoidance systems

Navigation systems

Transmission controls

Entertainment systems

Steering (steering assist Etc)

Communication systems

Noise cancellation

- **Current vehicle designs have +/- 100 processors/microprocessors/chipsets**
- **Number of processors expected to double within the next 5 years.**
- **A typical car contains about 5 miles of wiring**

Tractors…

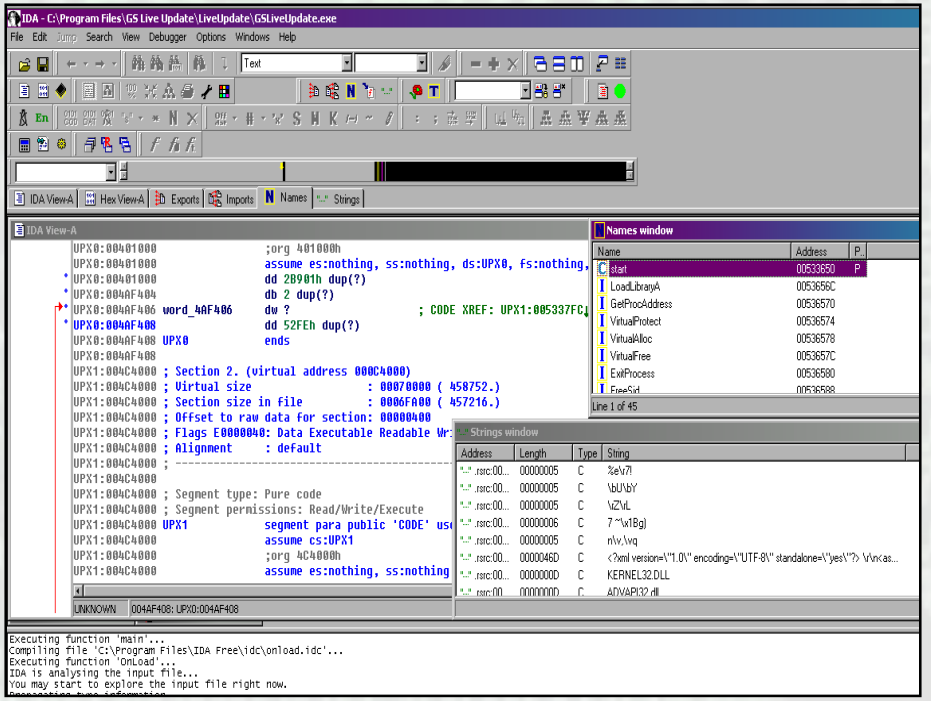
- Why
  - Blame Jesse, and a late evening over pancakes
- Why again?
  - Because cars are single/one-time hits
  - Because nobody else has done it
  - 2 Billion metric tons of food (more on that later)
- Seriously?
  - Yes, seriously, bear with us on this…we are not going to give away the code, but we'll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

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 (John 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

Need Beer Image

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

Busses, Reasons and Logic.

- **Transportation:**
  - 1,100 targets in Denver, Lots in Chicago!, and those are just the ones we know have Cummins Diesels (Las Vegas ones have Cummins ISL and hybrid engines…and we've tested those in-situ)
  - Freely available data on the Internet on city by city location for assessing impact.

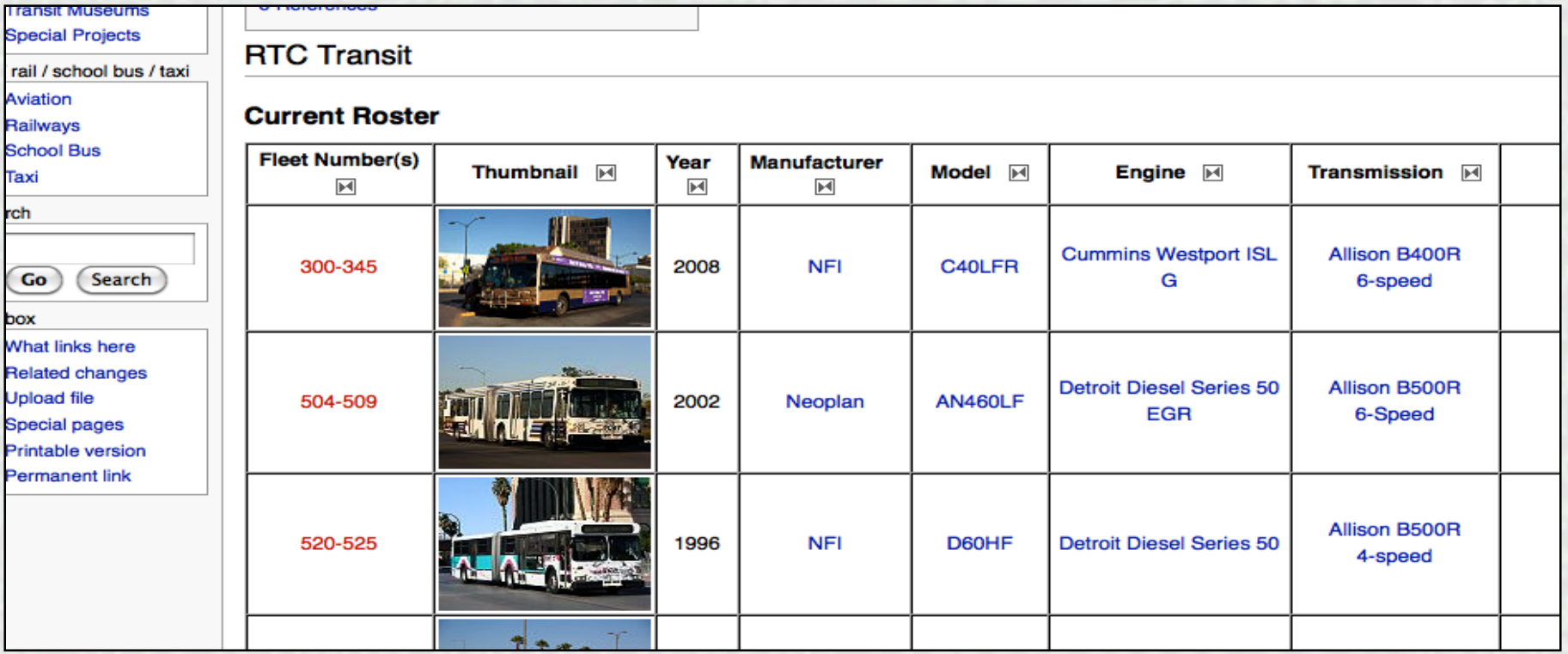
- **Ease of access:**
  - Wireless and other methodologies for management of the facilities, busses, engines is readily available and does not take a genius to acquire.
  - None of the 3rd party software packages consider security in their design/implementations

- **It's a mobile target.**
  - 40-60 human capacity, seen the movie "speed?" we can do it better, faster and cleaner.
  - It's a bus, its there, there's lots of them and they frequently stop and present themselves in easily locations…lot less hassle than taking out a bank these days!

Architecture and Access Points

- Location, location, location:
  - Bus depots, unguarded, lack of security and ease of access, most major hubs have insufficient controls both physical and electronic.
  - Refueling points, these are already stocked with the necessary AP's that can be watched, cracked and eventually cloned onto your own AP.
  - Just ride the damm things, take public transportation ☺
- Architecture:
  - Wireless, several different implementations observed/tested/used so far, some simple 802.11, some utilizing the 850-1900MHz (Cellular modem systems that also have the GPS units embedded)
  - OBDII/J1939 connectors if you have to do the physical connections first to check out what your quarry looks like close up (SAE standard connectors)
- Access Controls:
  - Access Point (used both a re-configured AirMagnet AP as well as a Sprint MiFi to test out.
  - AirMagnet's wireless suite through to Backtracks arsenal of tools, this gave both the initial "what am I dealing with, through to providing the cracked WEP keys necessary for the build

Bus Menu, Pick your Targets…



Thanks to a Canadian transit discussion boards we have a full menu of what's running, where it's running and what engine, transmission and systems are installed.

Think of it as "fishing with a menu" it's coordinated, target practice.

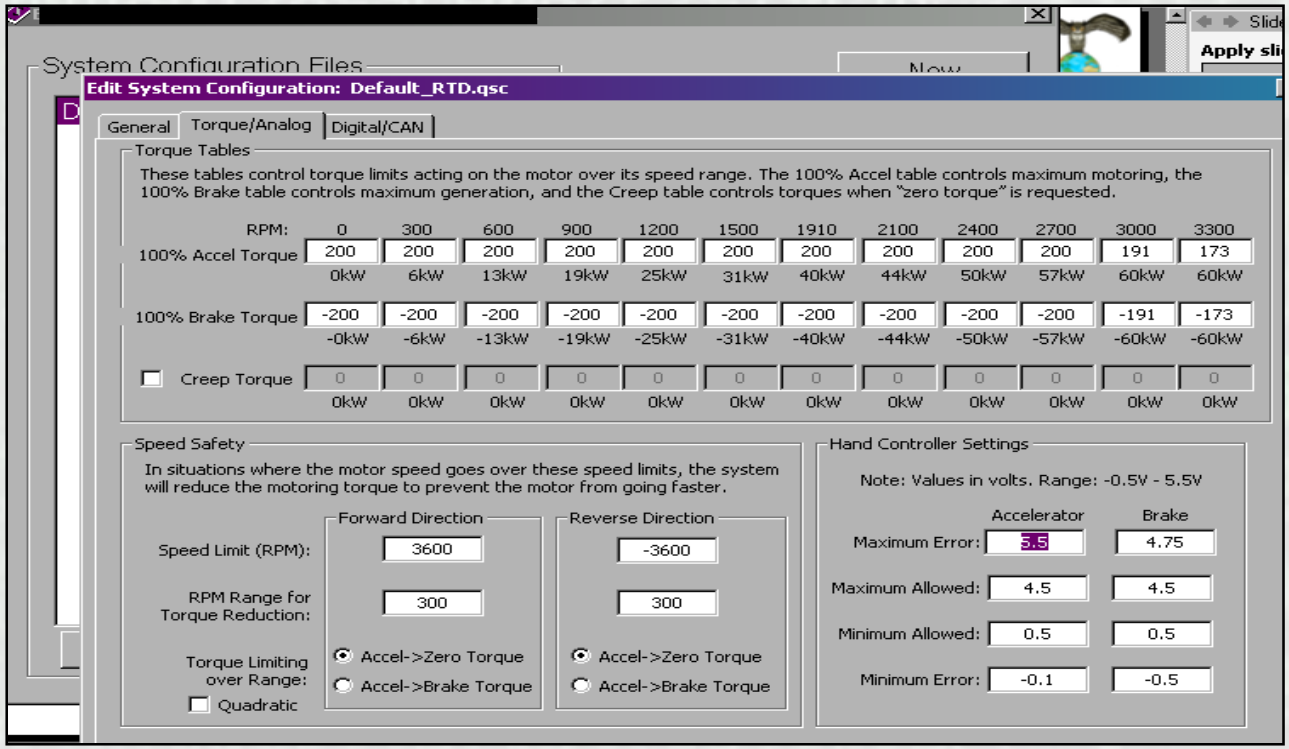
Busses, the “take down”

- Game:
  - Configure access point based on prior work done (wardriving the bus depot, crack the WEP password and then configure “duplicate/secondary”
  - If you are going in S/W based they you’ll need the necessary Cummins software downloaded, installed and your wireless cards communicating on the COM ports ready to work. (if using CAN only then CAN232HSW is a good program for USB/Wireless activities.)
- Set:
  - Wait for your bus…ensuring your AP is advertising, and you have Cummins INSITE program locked, loaded and waiting. (as above this is necessary for both S/W as well as the
  - If you are going for a simple re-flash instead of full access you’ll need the INLINE program with the modified configuration files locked/loaded and ready to send.
- Match:
  - On the busses tested there’s a 4 digit code between the cellular/802.11 access controls and the main driver interface units, lockouts are not enabled, let the brute force begin. (simple port login code/authentication retry)
  - Controls accessed once on the network (and authenticated) now it’s possible to use the INSITE/INLINE programs to interface with the Cummins engine management systems.

Busses, the variables

- Eco Friendly things:
  - Some of those damm busses now have batteries, never fear, UQM comes to the rescue, same basic methodology, however instead of working with RPM and other stuff, you get to play with voltage.
- Detroit:
  - Wait for your bus, accurately identify it as a Detroit, and go get coffee, they are old and they run on coal and capacitors….they are also leaving the playing field….if anyone gets a crack on one let me know (Caterpillar too)
- If you have to go find the codes:
  - Details on the CANBUS and AUTOSAR speed/modules and offsets get that data in h
- Physical:
  - Two main options, either OBDII connected engine management scanner (several options available) or there's now a lot of Palm pilot management systems that will read the majority of engines, however not used these on the busses….play/experiment at your peril etc.

Bus not stopping? Wifi to the rescue



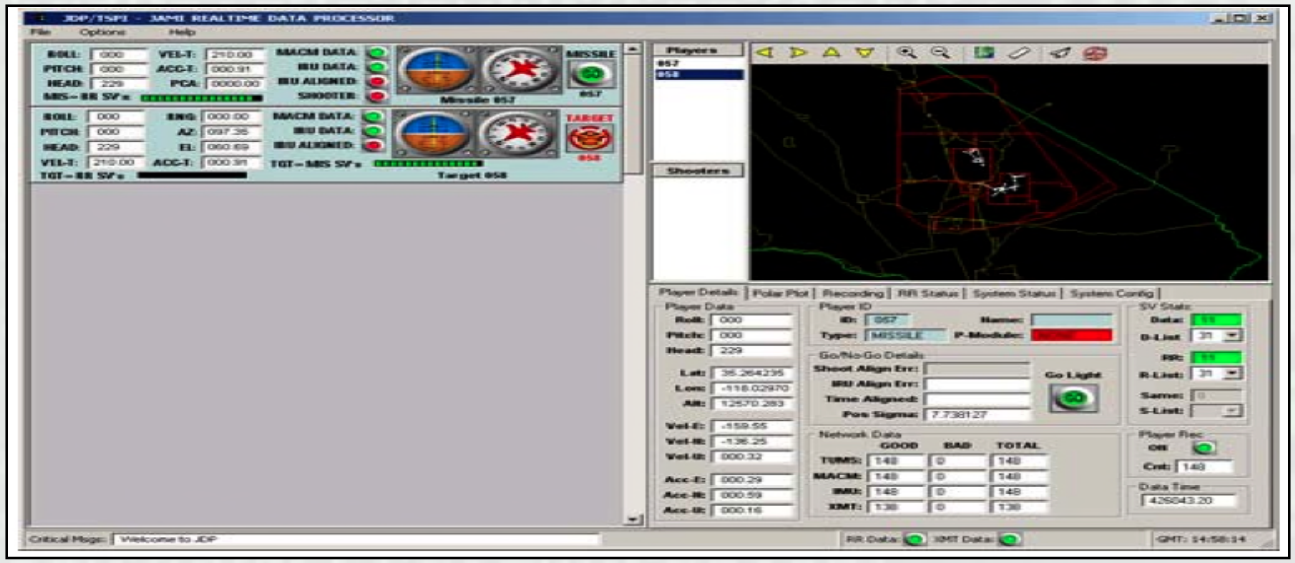
Management software for the hybrid engines, this also works for the mall type busses (tried and tested)

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

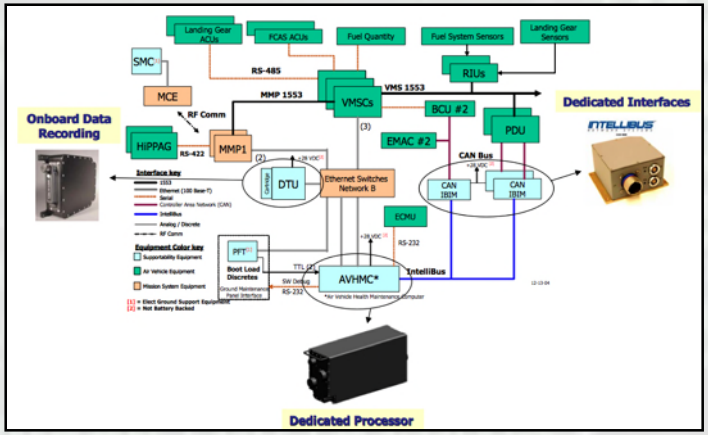
There's two options on these types of assessments, either a rapid re-flash of the configuration files (UQM configuration package) or the "Reader" which can be configured to run either wireless or Bluetooth over the Com1/3 port (serial re-mapped or just use O/S built in options)

Things That go Bang…



Intellibus Missiles and X-47 UCAV's Boeing & Northrop networks…

Intellibus meets IVHM Health management



Pause for Thoughts….

Data Security Is…

Protect information from those who are not authorized to receive it (intrusion and espionage)

Protect against the misuse of information (authorized users included in this!)

Anticipate and monitor threats to a company and build effective countermeasures

(Left) companies on PC/HIPAA/SOX Etc…..The auditor's eaten the only portion they care about….the rest of the pie doesn't need to be PCI compliant…..who's watching it??

Back to the **"if you're going to do it then do it right…first time"**

Hence the need for a more in-depth analysis than just the penetration testing. A malicious hacker WILL have interest in the rest of that pie….

Thank you! (Questions?)

One World Labs (OWL) works with individuals and organizations ranging from small operations through to multinational corporations and regularly partners with some of the leading organizations in the field of Information Security.

OWL assists businesses with all areas of data security, architecture and design, including security assessments, and critical incident response. Our in-house laboratory allows us to work at the forefront of vulnerability research, and provides valuable intelligence integrated into our service offerings. All security services are conducted by experienced and certified information security specialists.

OWL maintains a presence in the community with regular presentations both at conferences and on TV/Cable channels.

Doing what little one can to increase the general stock of knowledge is as respectable an object of life, as one can in any likelihood pursue
- Charles Darwin

Legal Stuff…

Data contained in this document serves informational purposes only and does not constitute legal, regulatory, or technical advice to any specific person or entity for any particular purpose. (Nor does it demonstrate a legitimate reason to go and duplicate what you see!)

O.W.L has no control over any information that you may access through the use of links contained in these materials and does not endorse your use of third-party Web pages nor provide any warranty whatsoever relating to third-party Web pages or any information found therein.

There’s probably more legal language, but you get the idea, you are on your own insofar as your actions (I’m around for any questions)