

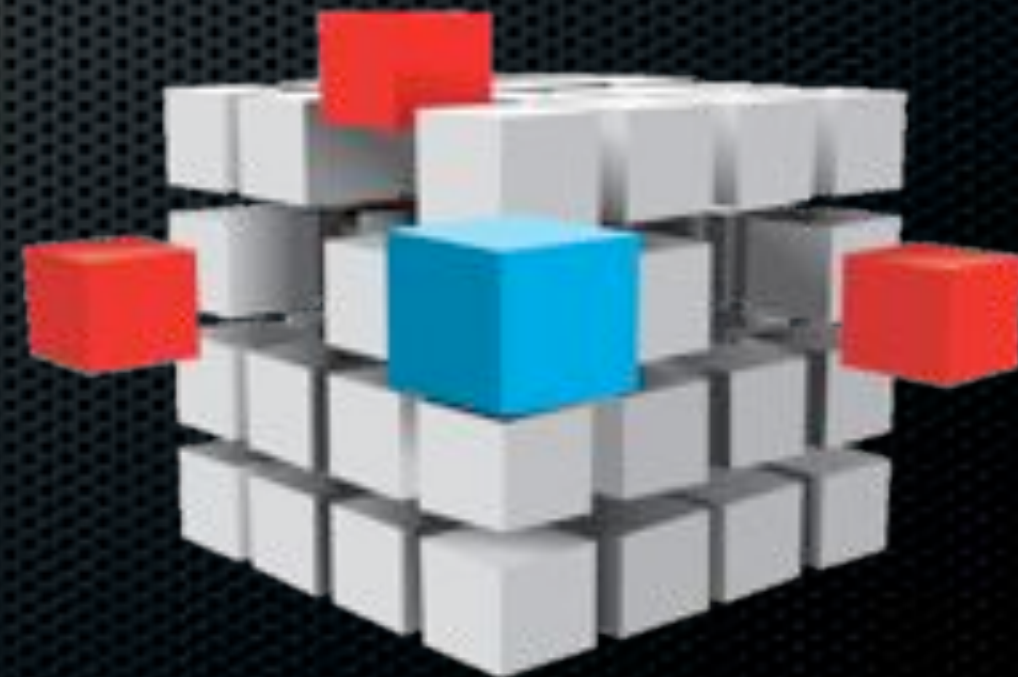
# System Shock: The Shodan computer search engine

I'm Viss. I do security  
research.

I've presented at:

Defcon/BlackHat/ToorCon(s)/  
BSides/BarCamp/OWASP/  
HITB

HITBSECCONF2013  
amsterdam



[HTTP://CONFERENCE.HITB.ORG/HITBSECCONF2013AMS/](http://conference.hitb.org/hitbsecconf2013ams/)



# **Time for some RESPECT.**

**I am here because of someone else's misfortune.**

**It's great for me, but horrible for them.**

**I just want to acknowledge that.**



# Credentials:

- Aaaaahahahahhahahaha
- HHAHAHAhahahAHAhaha!
- omg rofl lolz hahaha seriously
- I can't seriously do this slide with a straight face
- I read an nmap book once
- I totally stole this idea from zfasel and I owe him booze for it.
- my CISSP code of ethics mandates I report you



**Who here has NOT heard  
of Shodan?**



**Who here knows  
what TCP Banners  
are?**



# **Any python coders in here?**

**You guys are gonna love this :D**



# Shodan is like google but for tcp banners.

It also has a python API

You can bridge that API to tools

... like metasploit. Or armitage and cortana

Or you can just screenshot the entire net



# Find an interesting query.

Believe me - there is enough absurdity on the internet - its VERY EASY TO FIND.

2-3 steps of refinement = goldmines



# My first forray into this:

TONS AND TONS OF WEBCAMS.





# Webcams! .. speaking of goldmines..



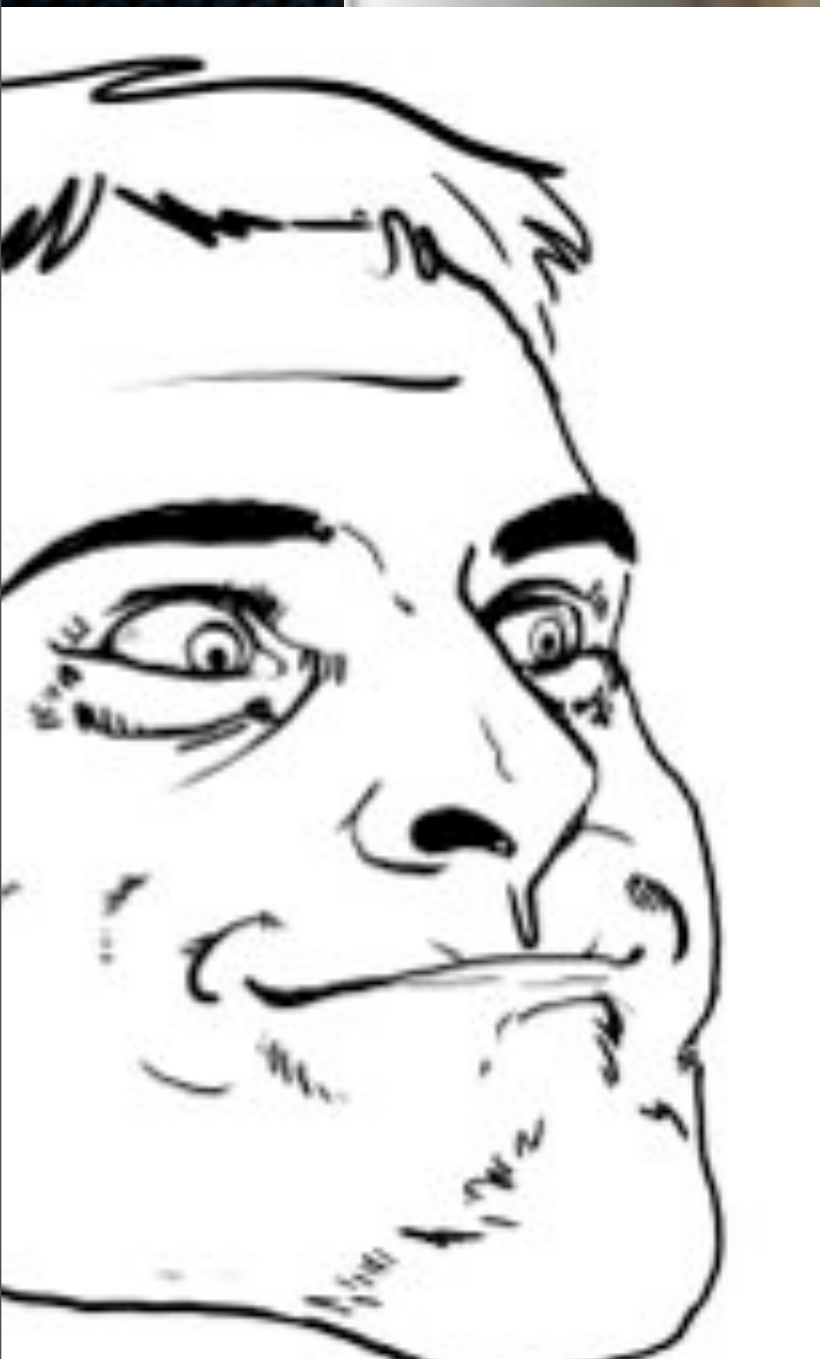


# Who watches the watchers?





# Who watches the watchers?

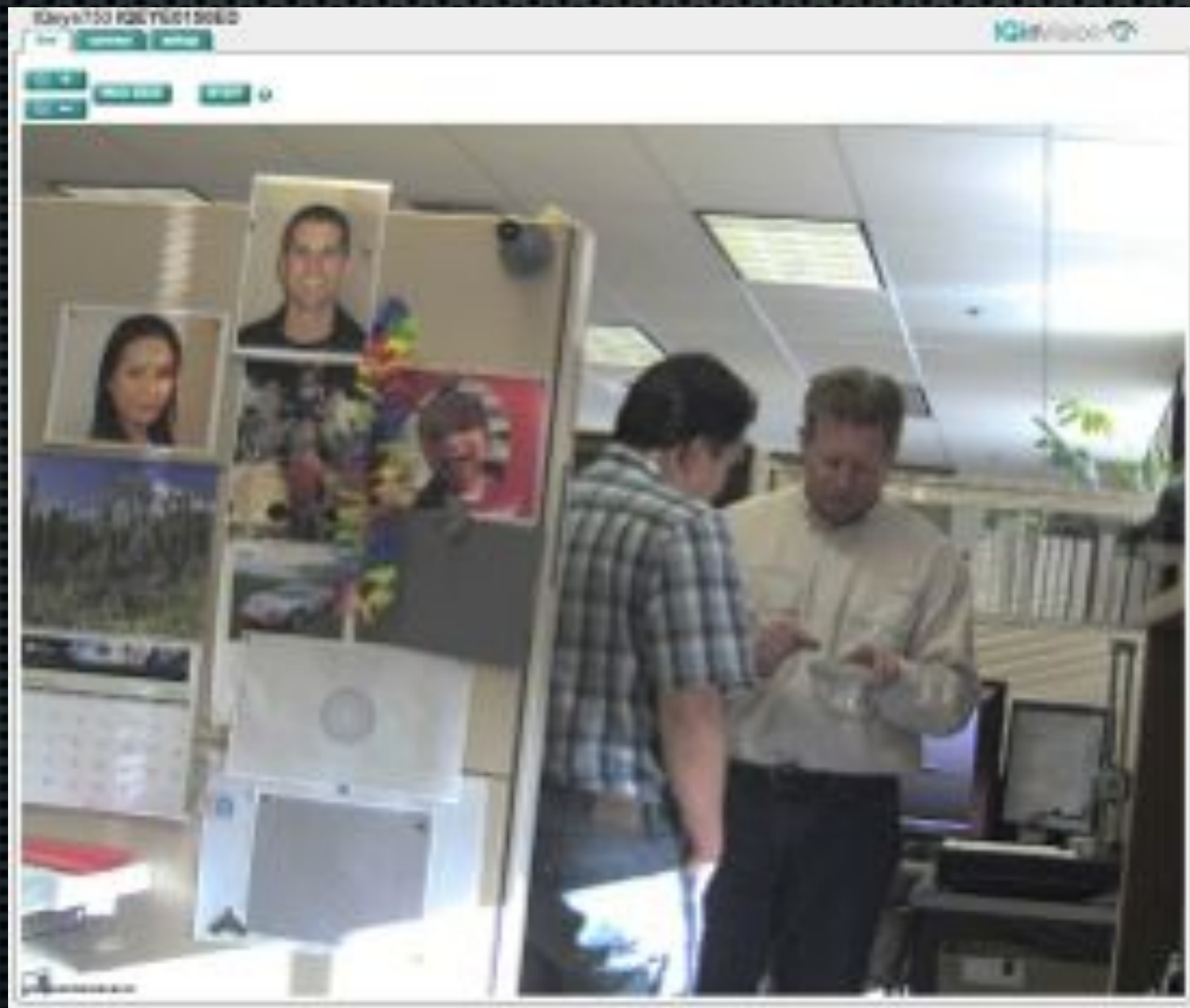


Meeeeeeeeeee >:D



# Now for more meta

a camera in the business that makes the cameras,  
watching people MAKE THE CAMERAS I'm  
watching them with



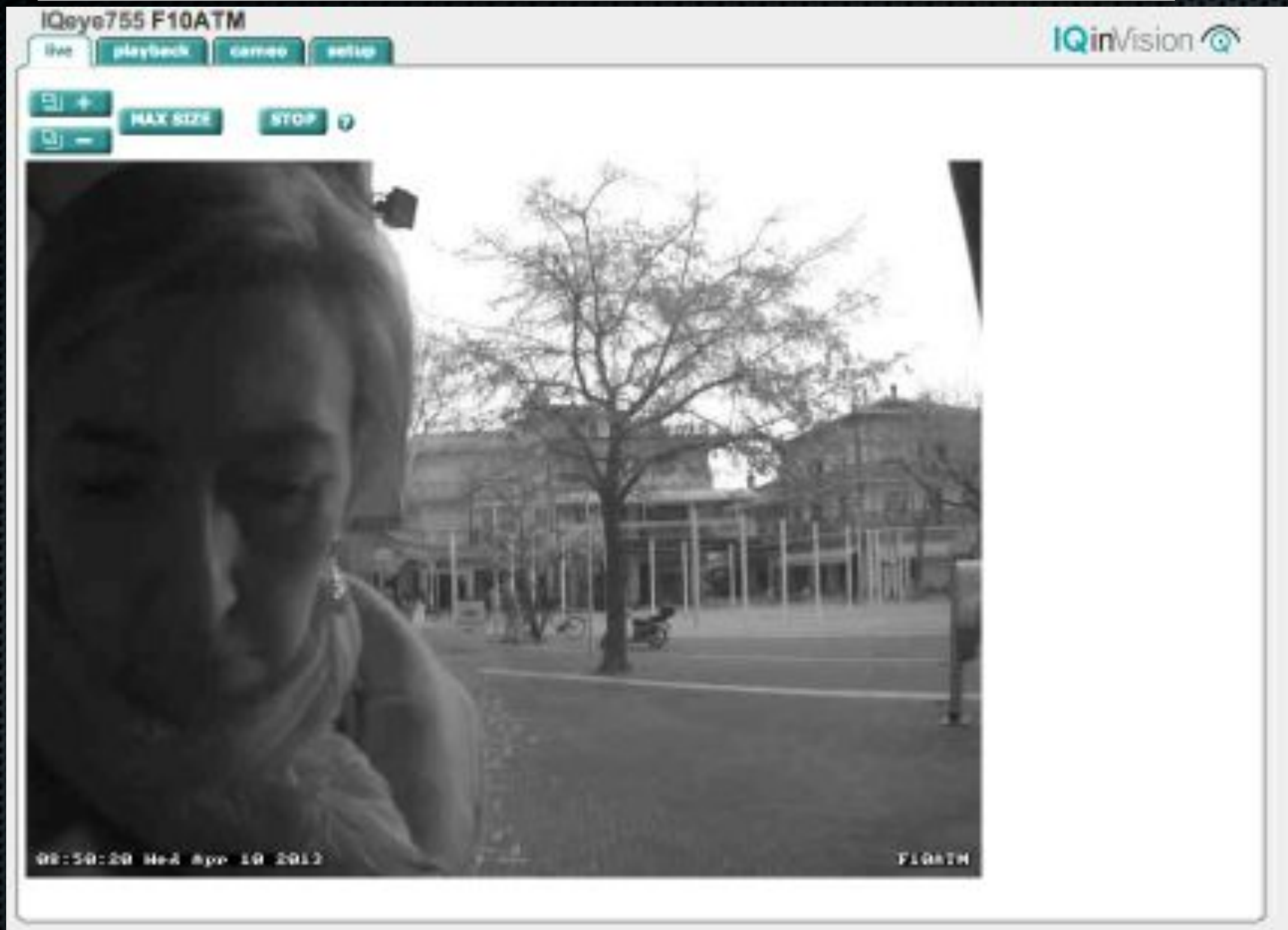


# Scada gear on webcams!



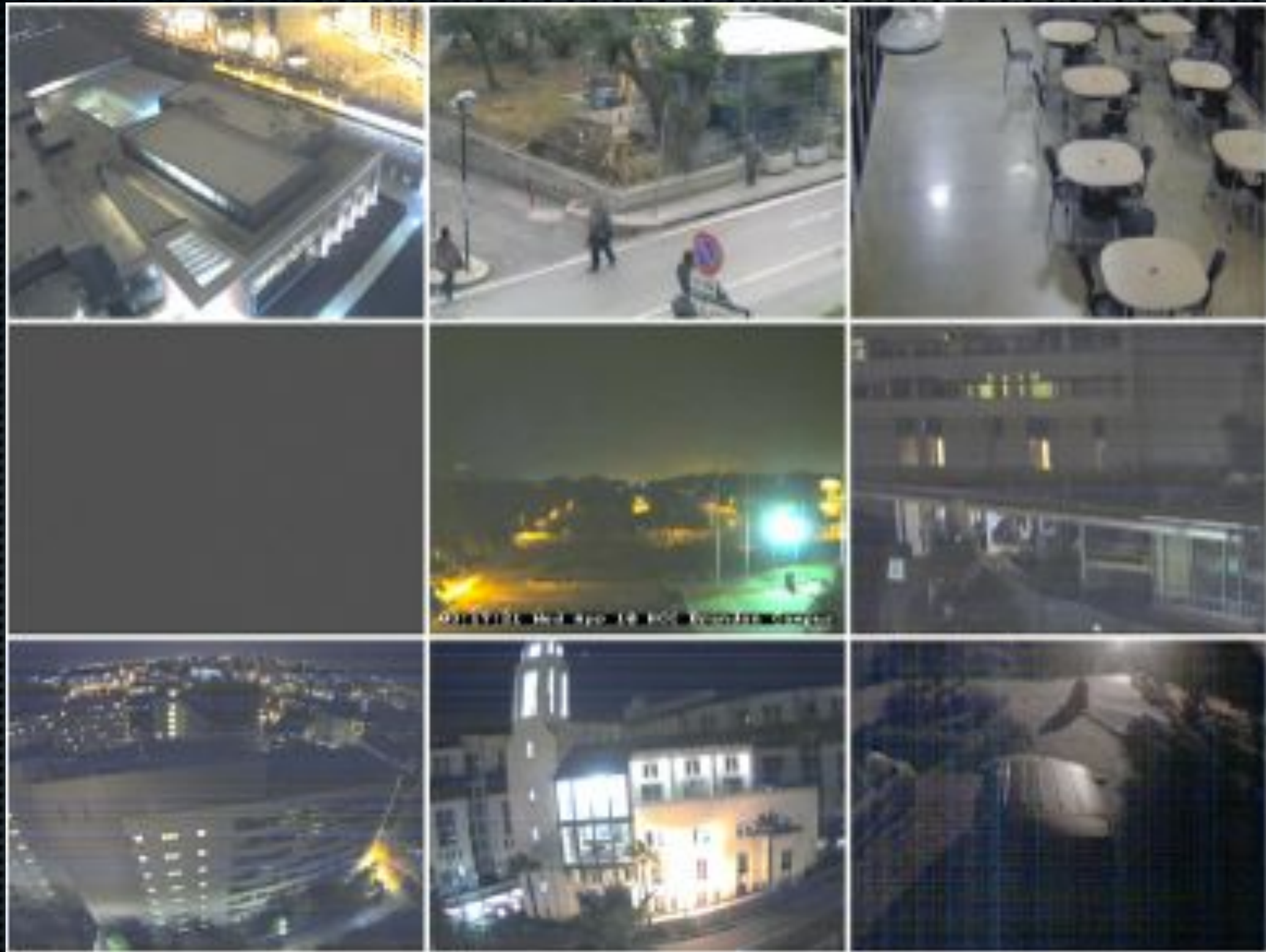


# Other stuff on webcams!





# But most cameras are boring





# This thing!

## ... (no idea)

```
T-2000 CC User Interface [ LOGIN ] (c) 2000 Relion Inc.  
  
      UserName :  
      Password :  
  
-----  
  
Unit Name :  
Unit Location :  
  
Major Alarms : 0  
Minor Alarms : 1  
ACQ Status : OFF 0100  
System Status : STANDBY  
  
Unit Date : 04/17/12  
Unit Time : 23:35:53  
  
Chassis S/M :  
Controller Ver : 02.02.01  
FPGA Ver : 01.01.03  
Comm Card Ver : 02.02.01  
  
-----  
Relion  
15903 E. Euclid Ave  
Spokane, WA 99216  
Tel: +1-509-228-6500  
24 Hour Support: +1-866-661-0020  
techsupport@relion-inc.com  
  
SYSTEM MESSAGES: Alpha Text, TAB-Next Field, Enter-Select, ESC-Abandon
```



# A um.. “T-2000” ! ..

## ... whats a T-2000?.. relion?

```
T-2000 CC User Interface [ LOGIN ] (c) 2000 Relion Inc.  
  
      UserName :  
      Password :  
  
-----  
  
Unit Name :  
Unit Location :  
  
Major Alarms : 0  
Minor Alarms : 1  
ACQ Status : OFF 0100  
System Status : STANDBY  
  
Unit Date : 04/17/12  
Unit Time : 23:35:53  
  
Chassis S/M :  
Controller Ver : 02.02.01  
FPGA Ver : 01.01.03  
Comm Card Ver : 02.02.01  
  
-----  
Relion  
15903 E. Euclid Ave  
Spokane, WA 99216  
Tel: +1-509-228-6500  
24 Hour Support: +1-866-661-0020  
techsupport@relion-inc.com  
  
SYSTEM MESSAGES: Alpha Text, TAB-Next Field, Enter-Select, ESC-Abandon
```



# Its a hydrogen fuel cell.

**Reli On**  
+ - \*

Products

E-200

E-1100

E-1100v

E-2500

T-1000

T-2000

Telecom

Government

Off-Grid

Transportation

Utility

Certifications

Tax Incentives

## PRODUCTS & SOLUTIONS

T-2000 | T-2000: 2kW Outdoor Configuration | T-2000: 4kW Outdoor Configuration  
T-2000: 8kW Outdoor Configuration | T-2000: 8kW Outdoor Configuration  
T-2000: 12kW Outdoor Configuration

### T-2000® 2kW PEM Fuel Cell

The T-2000® fuel cell system is designed specifically for larger communications backup power loads within the wireless and wireline telecommunications, utility and government sectors. The T-2000® fuel cell uses ReliOn's patented Modular Cartridge Technology® for not-swappable high reliability, ease of maintenance and simplicity of design. Modular electronics cards enable scalability by providing flexible configuration from 600 Watts to a full 2,000 Watt capacity in one chassis. Or combine multiple T-2000® fuel cells to provide higher outputs for a variety of site requirements up to 12kW.

[Click for specifications in English \[197KB\]](#)  
[Click for specifications in Spanish \[130KB\]](#)  
[Click for specifications in Portuguese \[213KB\]](#)  
[Click for specifications in Chinese \[595KB\]](#)

---

#### Features:

- Output: 0 to 2,000 Watts - 24 or 48 VDC nominal output
- 23 " Rack Mountable (Indoors)
- Multiple Outdoor Configurations
- Remote Monitoring Capability
- Dimensions: 26"h x 23" w x 21.5" d [66cm x 53cm x 54.6cm]
- Fuel: Industrial Grade Hydrogen

---

#### Applications:

Wireless Telecommunications  
WiMAX, Backhaul applications, Microwave, Fiber, Cellular/PCS, GSM/CDMA





# Looks industrial!

## Field Trial Prototype

- Relion's modular cartridge approach normally operates with six cartridges connected to a common BUS. Each cartridge supplies a nominal power of 200W.
- In case a cartridge is damaged, the replacement procedure can be performed in a few seconds while the fuel cell continues to provide power to the load.
- Figure 2 – Relion's T-1000 hydrogen fuel cell





# Gets used a lot in .mil...

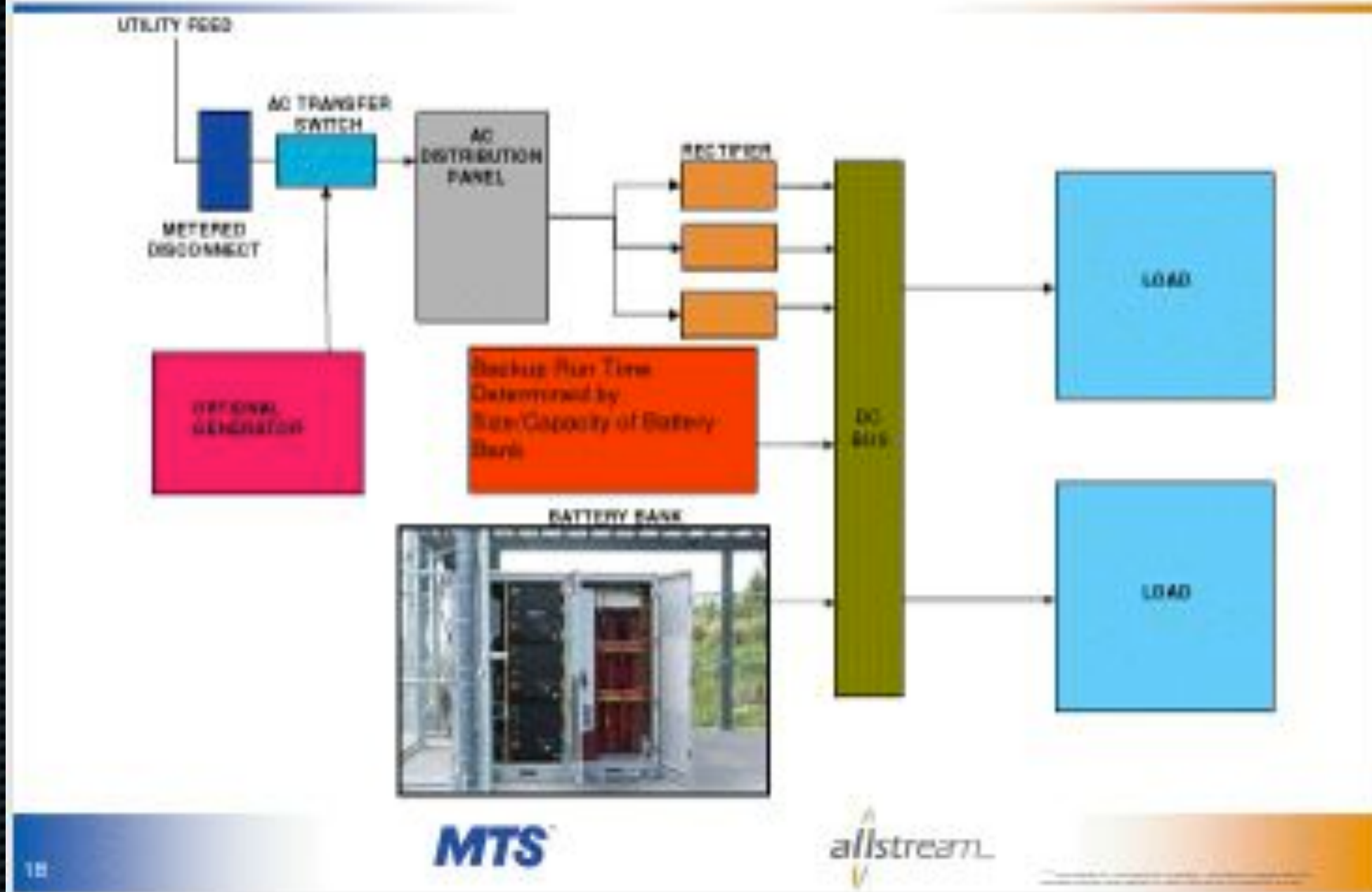
## DOE/DOD Back-Up Power Demonstration

Site	kW Req'd	Buildings Backed-up	Fuel Cell Units Used
Aberdeen Proving Ground	15; 20; 8	Energy Management Building, Range Control and Coordination, DPW Conservation Branch	(3) IdaTech ElectroGen 5; Hyrogenics HyPM Rack 20; ReOn T-2000 8kW
Fort Bragg	15	Training Range Control Building	(3) IdaTech ElectroGen 5
Picatinny Arsenal	10; 10	Sewage Lift Pump Sewage Lift Pump	(2) IdaTech ElectroGen 5; (2) IdaTech ElectroGen 5
West Point	20; 20	Internet Switch Internet Service and Telecom Closet	Albergy FPS-20; Albergy FPS-20
Cheyenne Mountain	24	911 Call Center	ReOn T-2000 4kW, 8kW, 12kW
Fort Hood	9; 10	Wastewater Pretreatment Plant, Wastewater Pretreatment Plant	ReOn T-2000 8kW, ReOn T-1000 1.2 kW; Albergy FPS - 10
Ohio Nat'l Guard	20; 20	Command Headquarters, Civil Support Administration	(4) IdaTech ElectroGen 5; (4) IdaTech ElectroGen 5
Marines 29 Palms	4	Internet Switch	ReOn T-2000 4kW



# This is how you use it

Fig 3-Typical Back-up Power





So where do you  
find these things in  
meatspace?



# Oh..

## Site Details - Continue

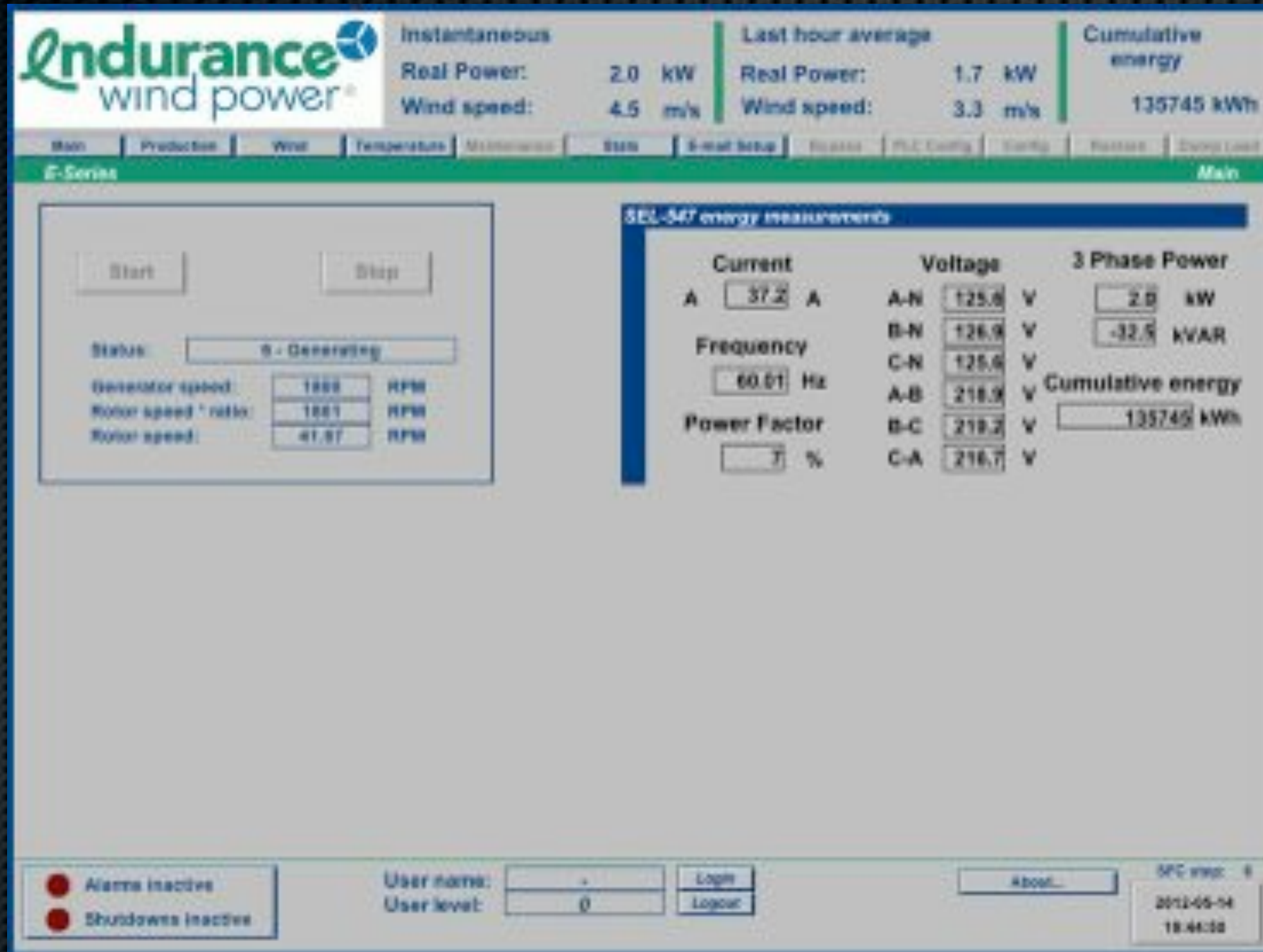


Fuel Cell  
Here





# Wind farms!





# Lighting, HVAC, Alarms





# More hvac/lighting



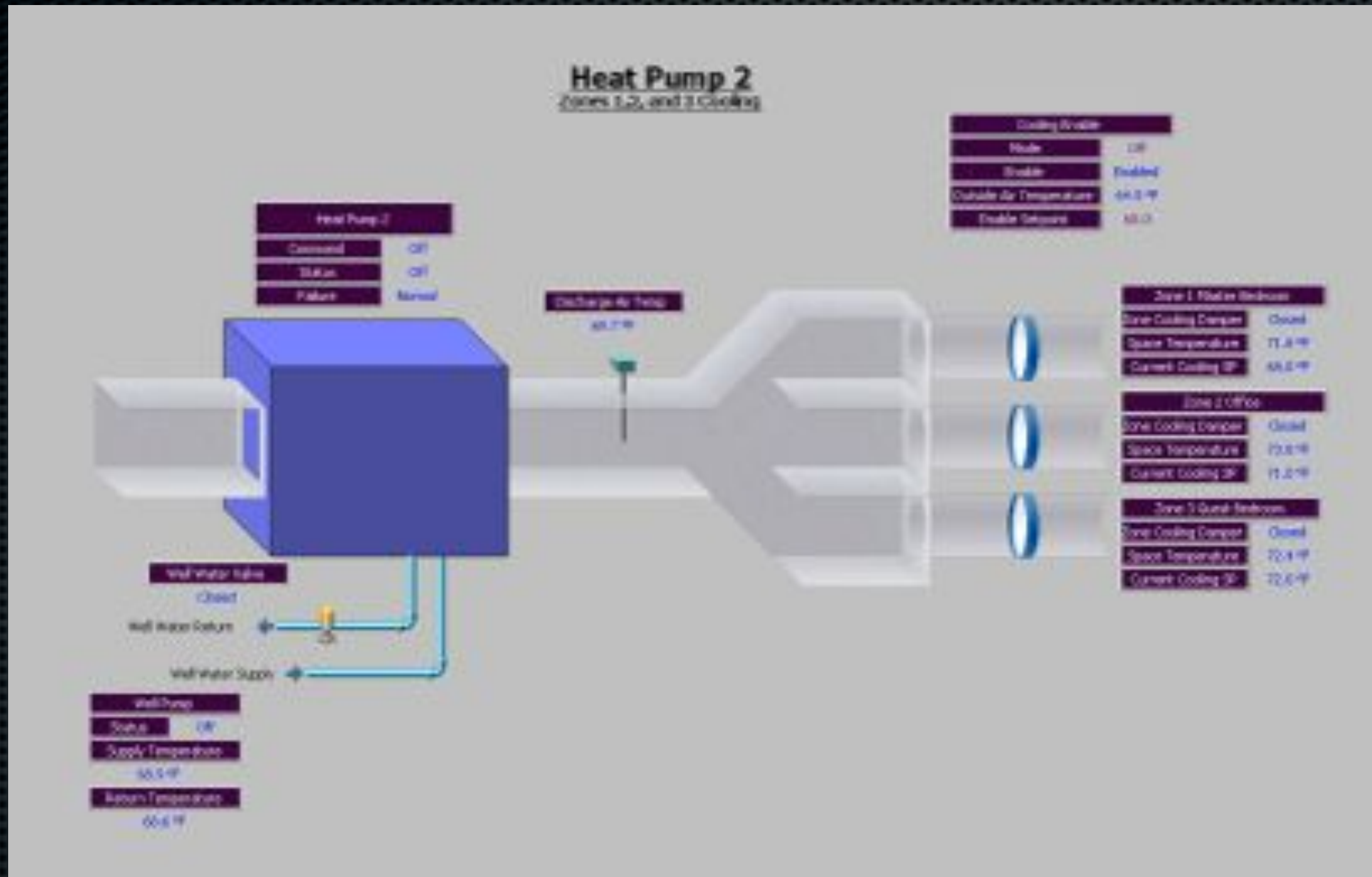


# Power meters?



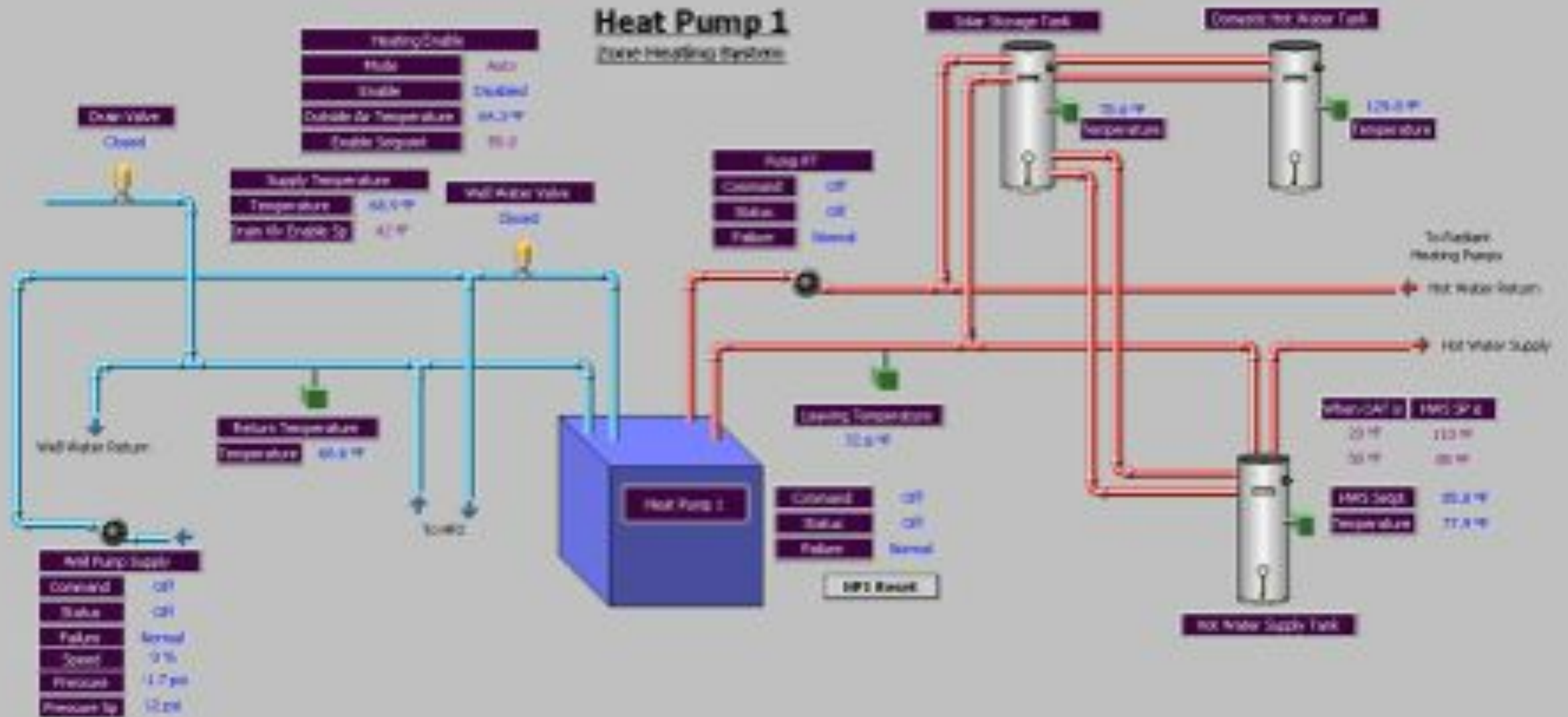


# Heat pumps



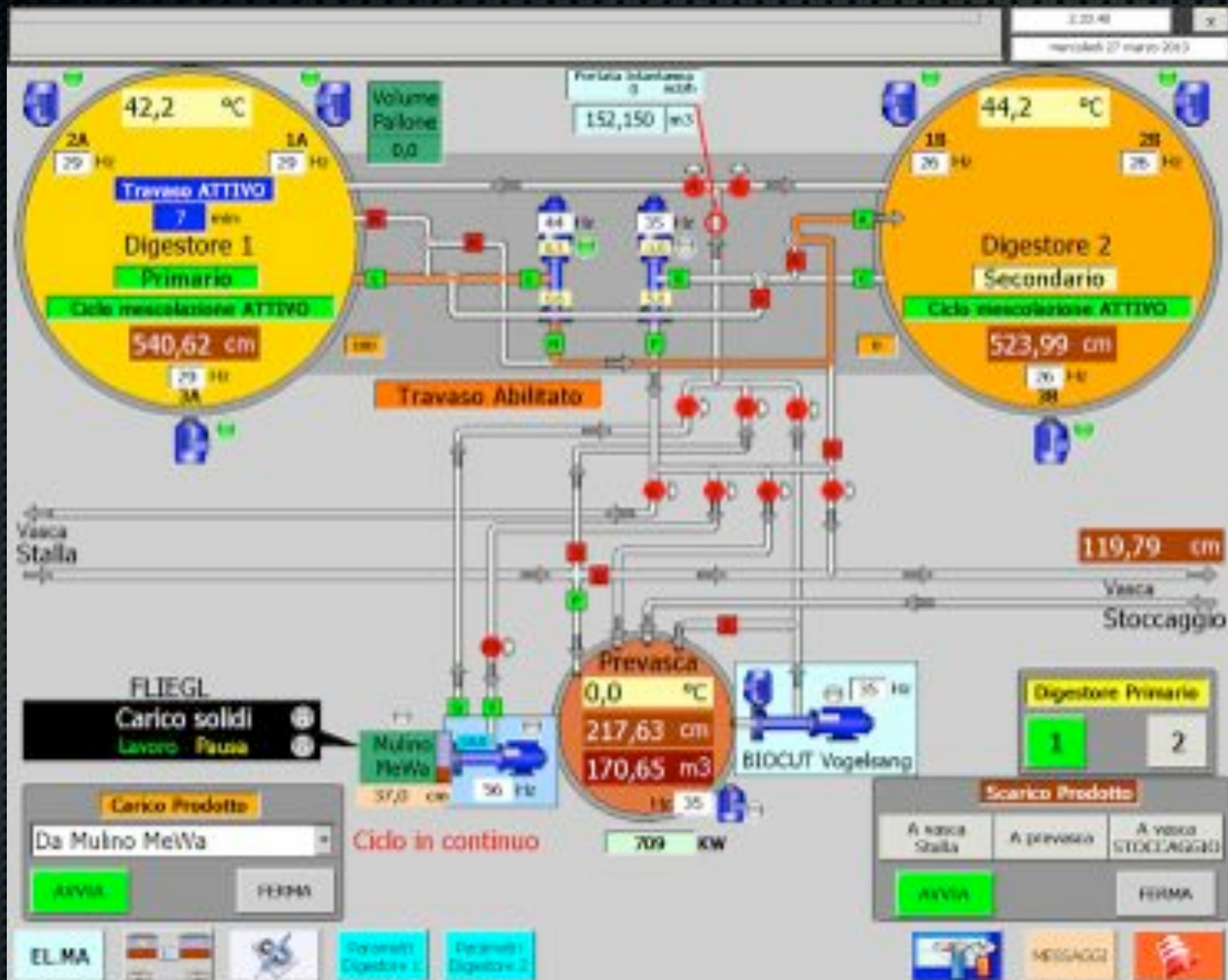


# Bigger heat pumps



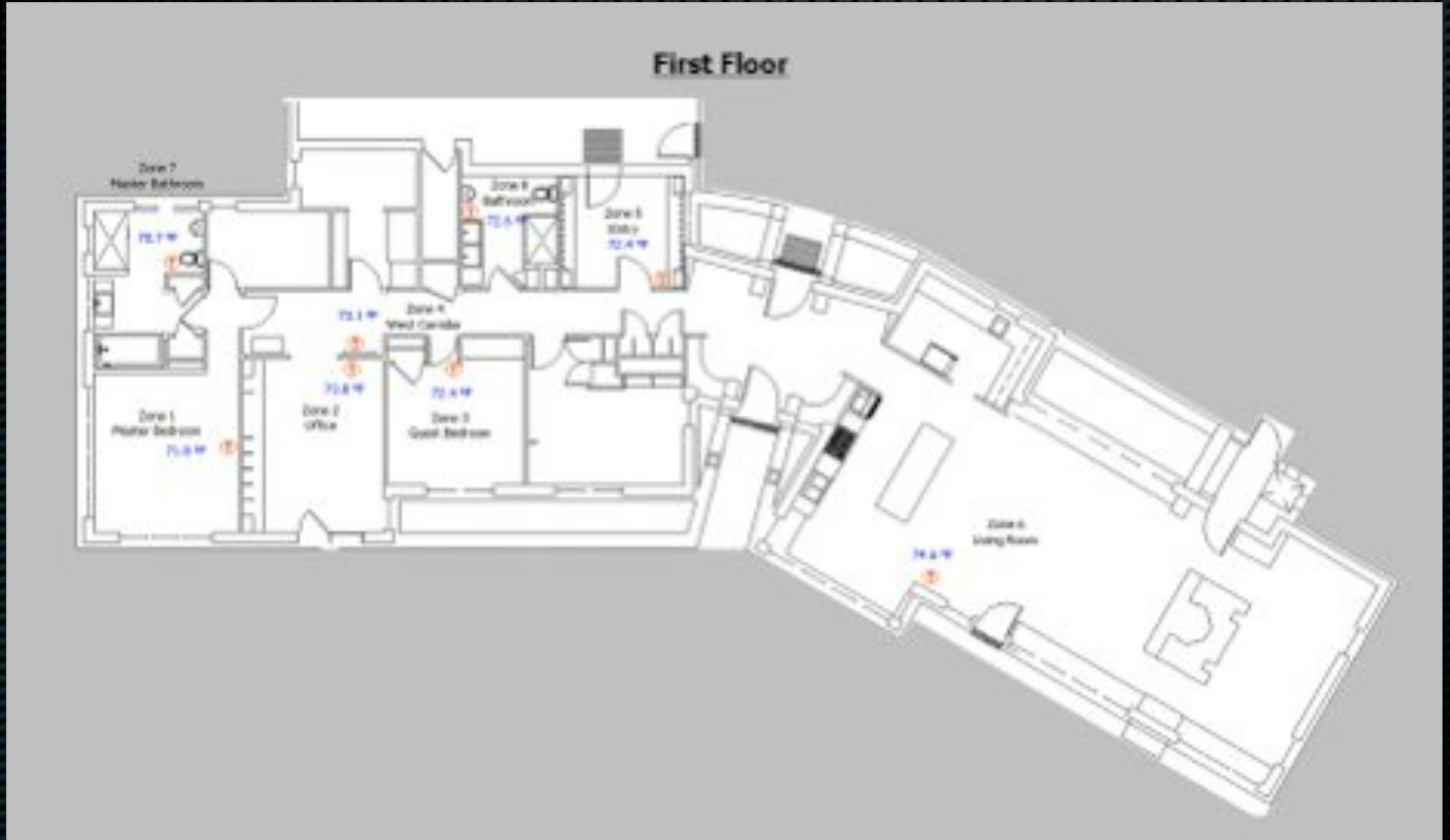


# REALLY REALLY big heat pumps





# Private residences?!



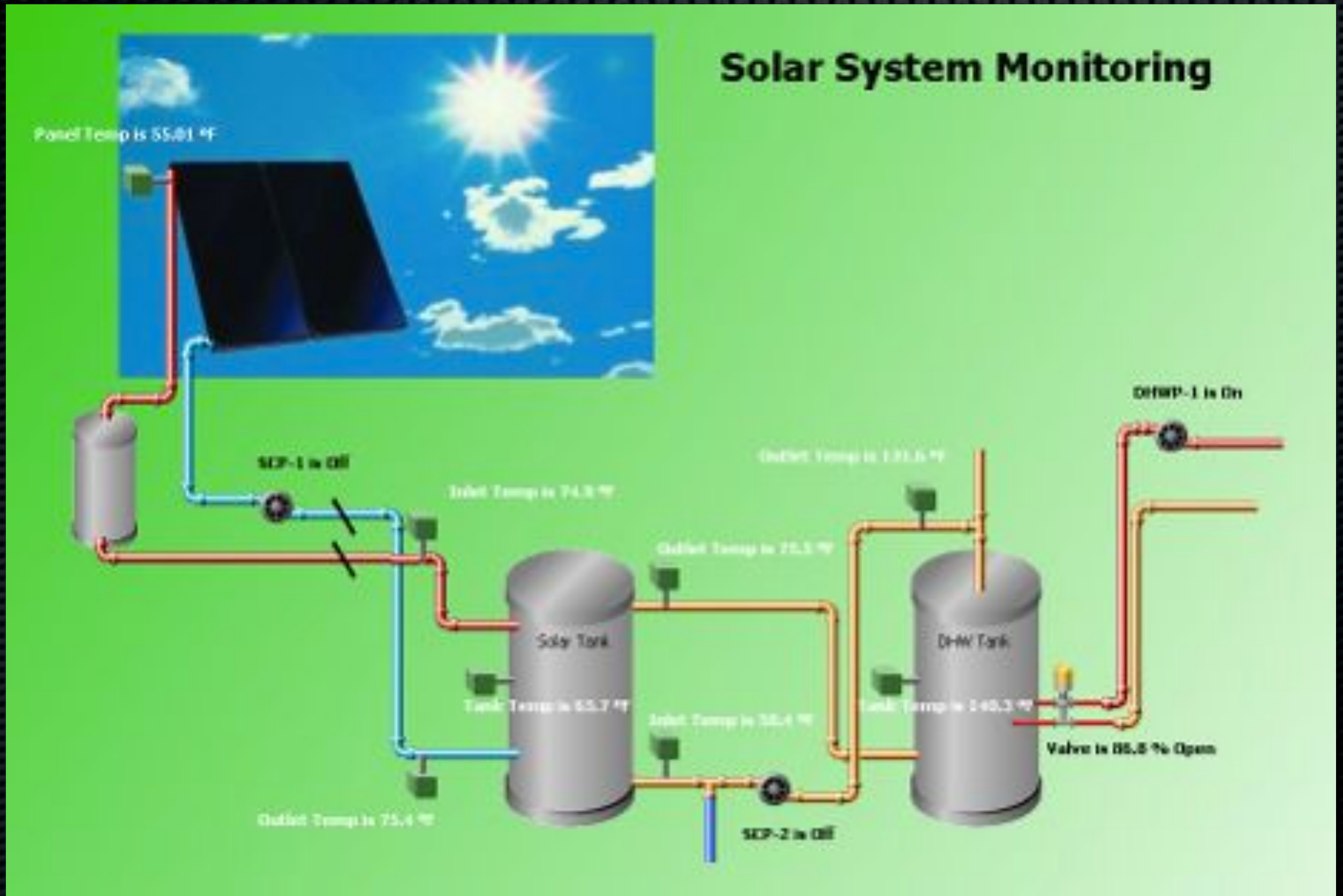


... with trending data?!



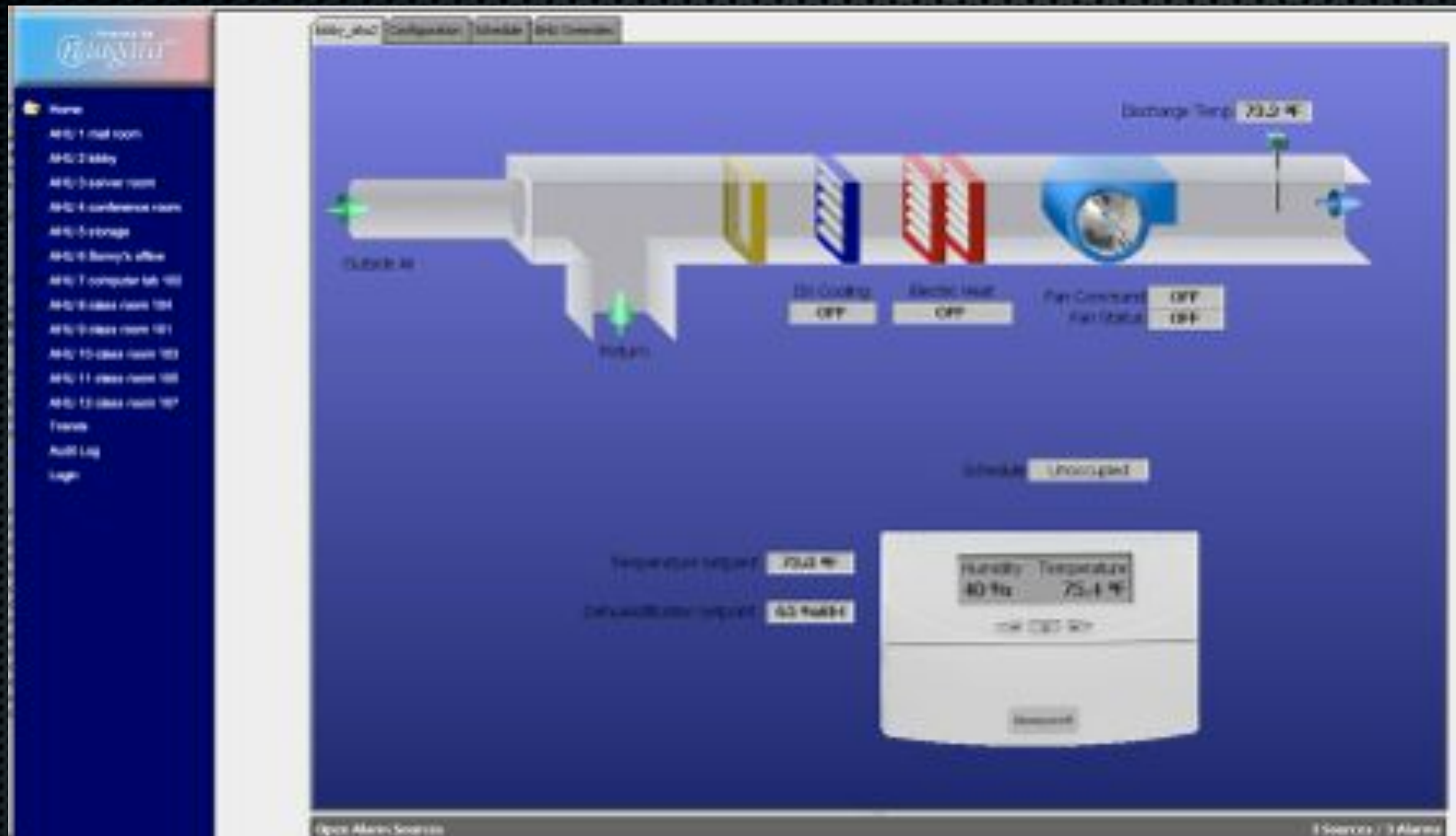


# Water heaters





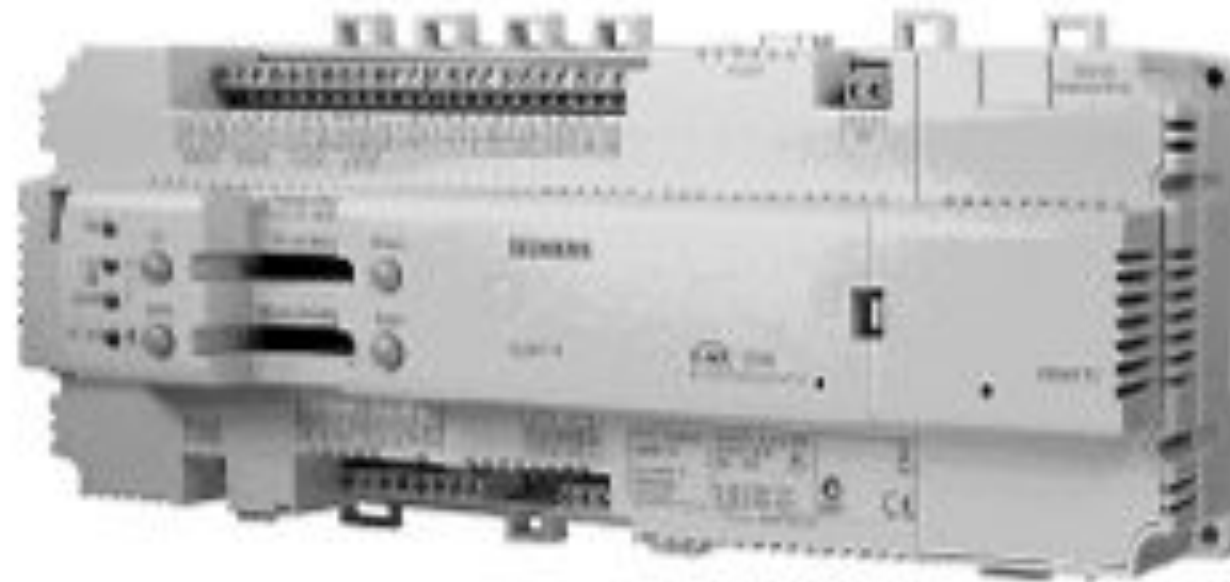
# Familiar displays!





# Larger industrial systems

**SIEMENS**



**Synco™**

**Central communication unit OZW775 V2.0**

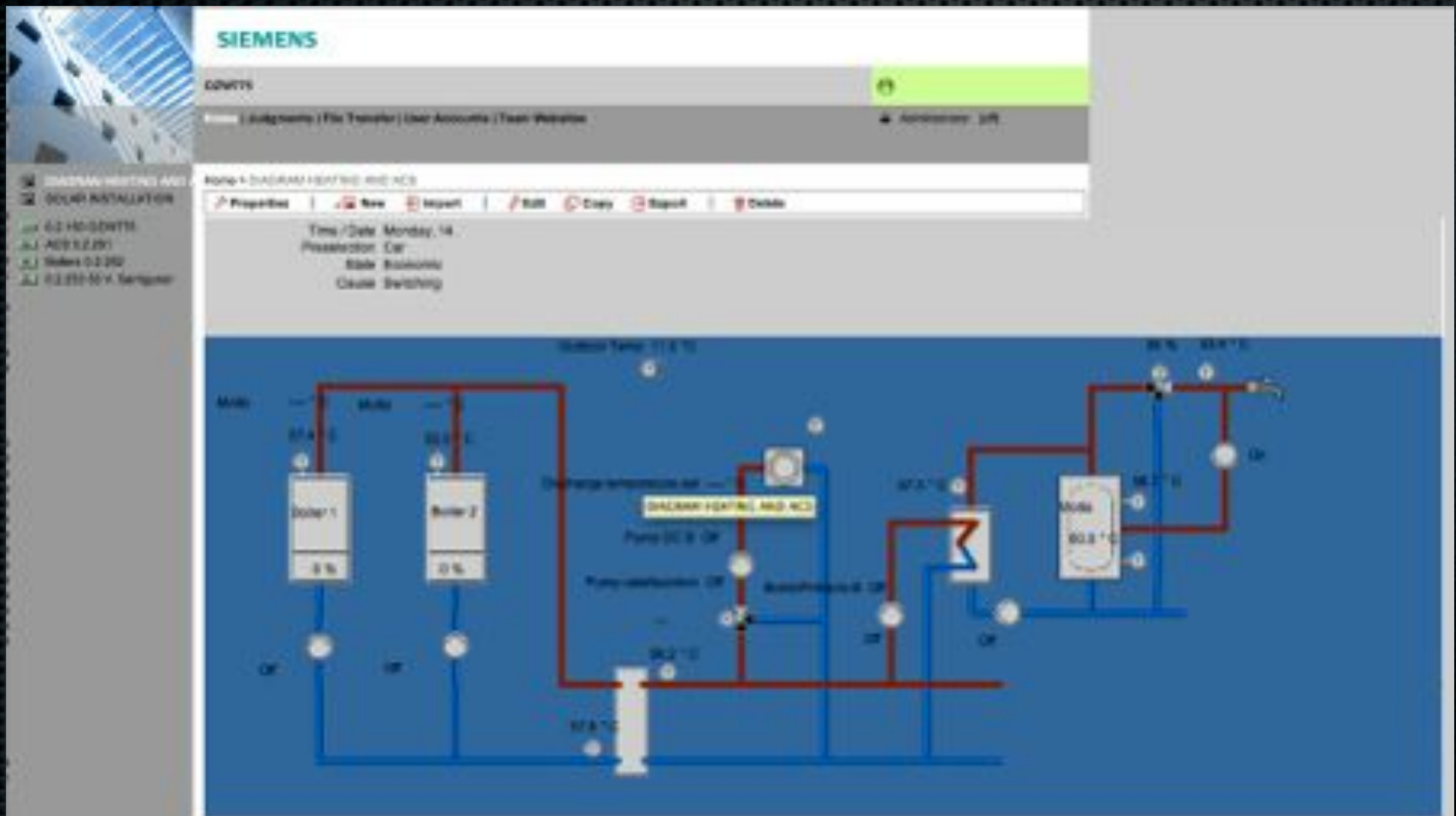
with integrated web server function

Commissioning instructions





# Contents under pressure





Overall, security is a joke.

[illegible]



Overall, security is a joke.

[illegible]



So what can one do with  
these sorts of findings?

It's like a fountain of  
information disclosure.

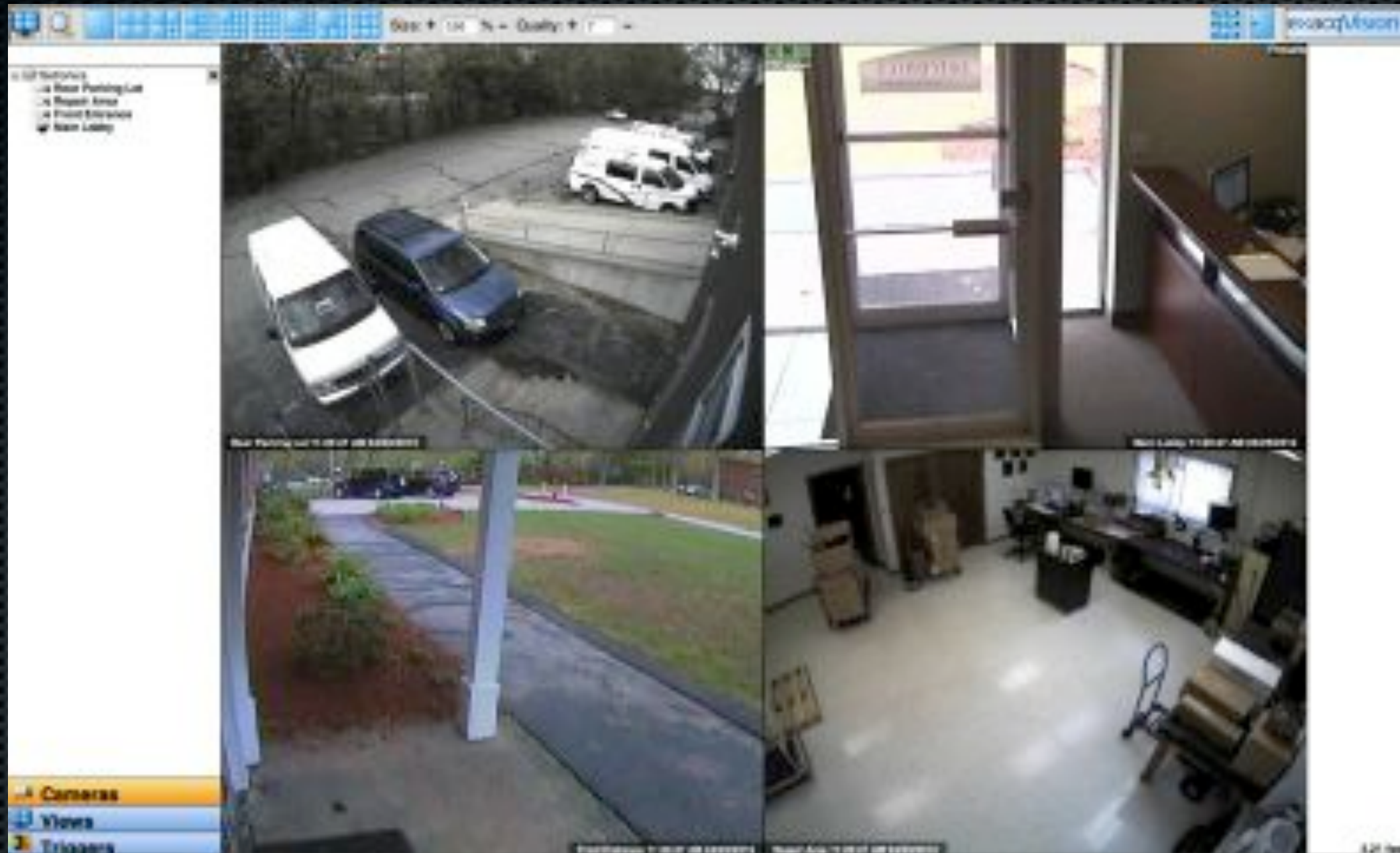


# Level One:

## Simple recon

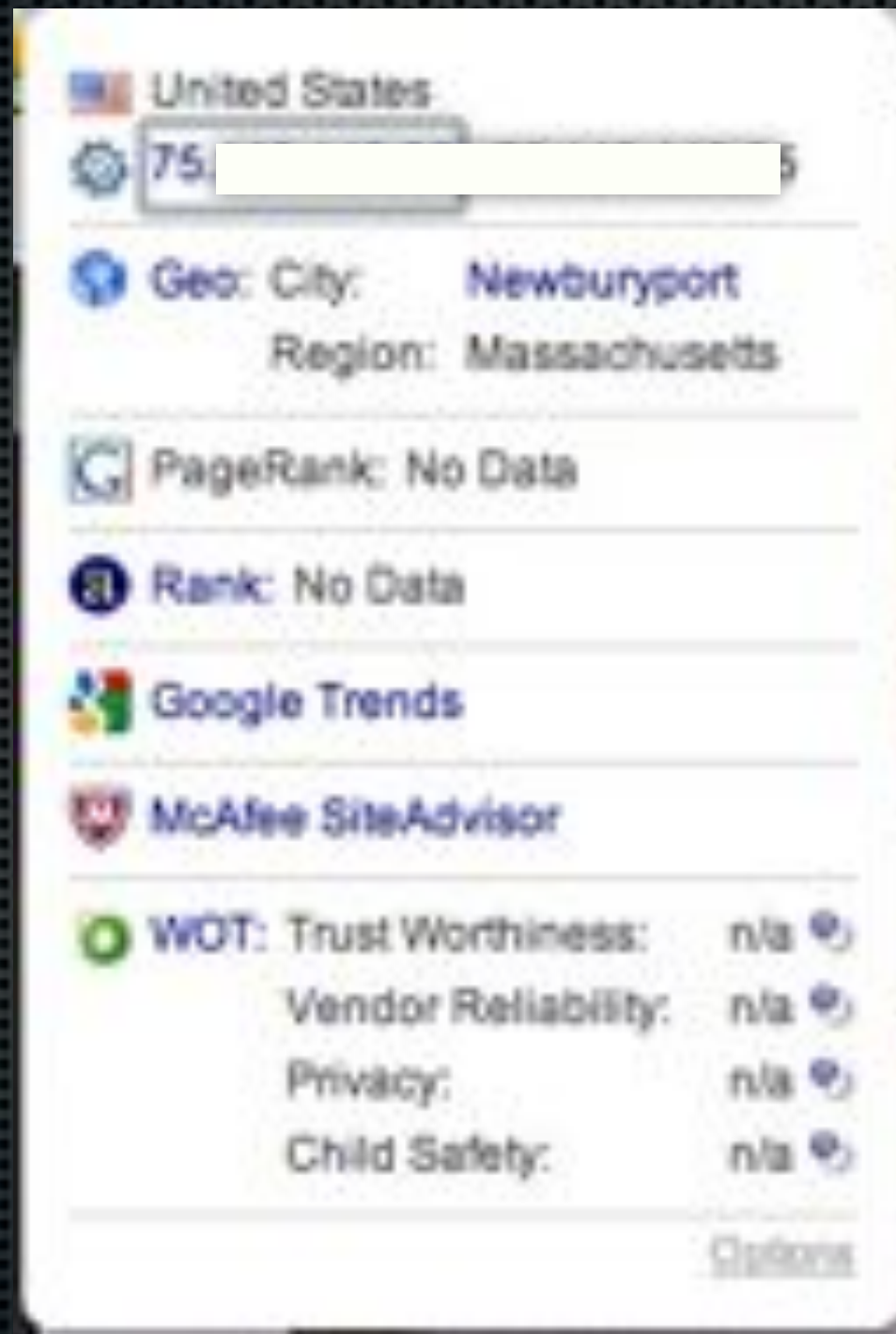


# What details can we see?





# Quick observations..





# We've got their scent!





# They smell all the way to google maps!





# Level Two: Interactions



# DISCLAIMER:

I didn't have any idea this happened until someone showed me a gallery of screencaps...



# Simple social engineering









# Massive coolers

LeadChillerSelect : South Chiller

OUTSIDE AIR TEMP	72.73 °F
LOW SPACE TEMP	44.38 °F
HIGH SPACE TEMP	44.38 °F
AVERAGE SPACE TEMP	44.38 °F
NETEMP	44.38 °F
SWTEMP	44.38 °F
NWTEMP	43.87 °F
SCTEMP	44.64 °F

CHW Loop Temp.

41.83 °F

N\_CHILLER2

Leaving CHW Temp.

41.86 °F

S\_CHILLER1

Leaving CHW Temp.

43.43 °F

Active CHW Delta Temp.

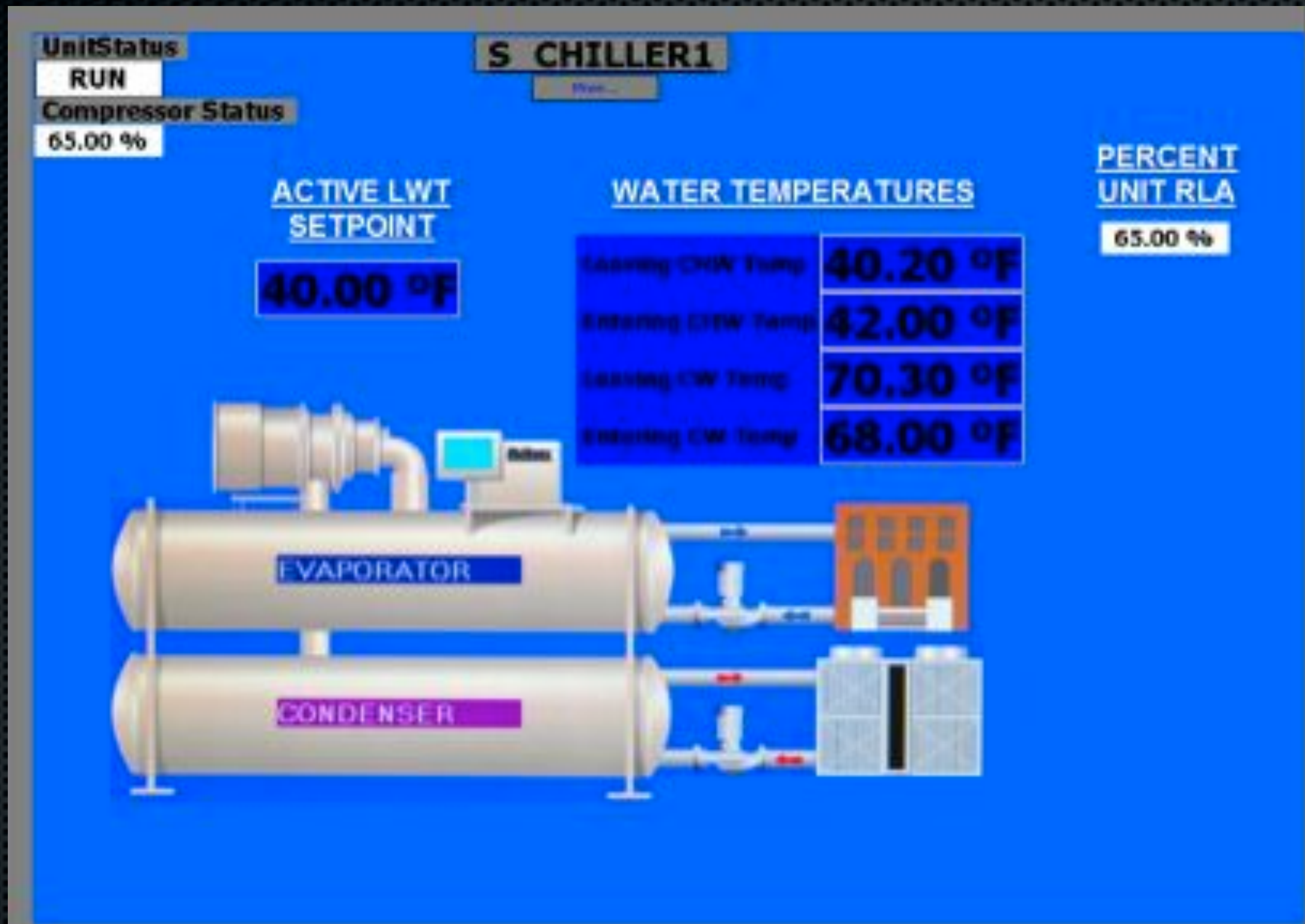
1.52 °F

<a href="#">VIEW_EVAP1</a>	<a href="#">VIEW_EVAP8</a>
<a href="#">VIEW_EVAP2</a>	<a href="#">VIEW_EVAP9</a>
<a href="#">VIEW_EVAP3</a>	<a href="#">VIEW_EVAP10</a>
<a href="#">VIEW_EVAP4</a>	<a href="#">VIEW_EVAP11</a>
<a href="#">VIEW_EVAP5</a>	<a href="#">VIEW_EVAP12</a>
<a href="#">VIEW_EVAP6</a>	<a href="#">VIEW_EVAP13</a>
<a href="#">VIEW_EVAP7</a>	<a href="#">VIEW_EVAP14</a>
<a href="#">VIEW_EVAP15</a>	

[EVAP DEFROST SCHEDULEs...](#)



# Massive coolers with details!





# Some scada keeps logs!

13-Apr-12 7:16:15 AM MDT	fox	1	Opened: 165 <- 0 :: WbApplet [guest] @ Owner-PC
13-Apr-12 7:23:07 AM MDT	fox	1	Opened: 166 <- 0 :: WbApplet [admin] @ Denniss-MacBook-Pro.local
13-Apr-12 7:24:40 AM MDT	fox	1	Opened: 167 <- 0 :: WbApplet [admin] @ Denniss-MacBook-Pro.local
13-Apr-12 7:25:19 AM MDT	fox	1	Closed: 166 <- 0 :: WbApplet [admin] @ Denniss-MacBook-Pro.local
13-Apr-12 7:28:09 AM MDT	fox	1	Closed: 167 <- 0 :: WbApplet [admin] @ Denniss-MacBook-Pro.local
13-Apr-12 7:31:53 AM MDT	fox	1	Closed: 165 <- 0 :: WbApplet [guest] @ Owner-PC
13-Apr-12 7:31:54 AM MDT	fox	1	Opened: 168 <- 1 :: WbApplet [guest] @ Owner-PC
13-Apr-12 7:56:51 AM MDT	fox	1	Closed: 168 <- 1 :: WbApplet [guest] @ Owner-PC
13-Apr-12 9:19:37 AM MDT	fox	1	Opened: 169 <- 0 :: WbApplet [admin] @ Denniss-MacBook-Pro.local
13-Apr-12 9:22:55 AM MDT	fox	1	Closed: 169 <- 0 :: WbApplet [admin] @ Denniss-MacBook-Pro.local
13-Apr-12 9:24:02 AM MDT	sys	1	Saving station...
13-Apr-12 9:24:04 AM MDT	history.db	1	Saved history archive (494ms)



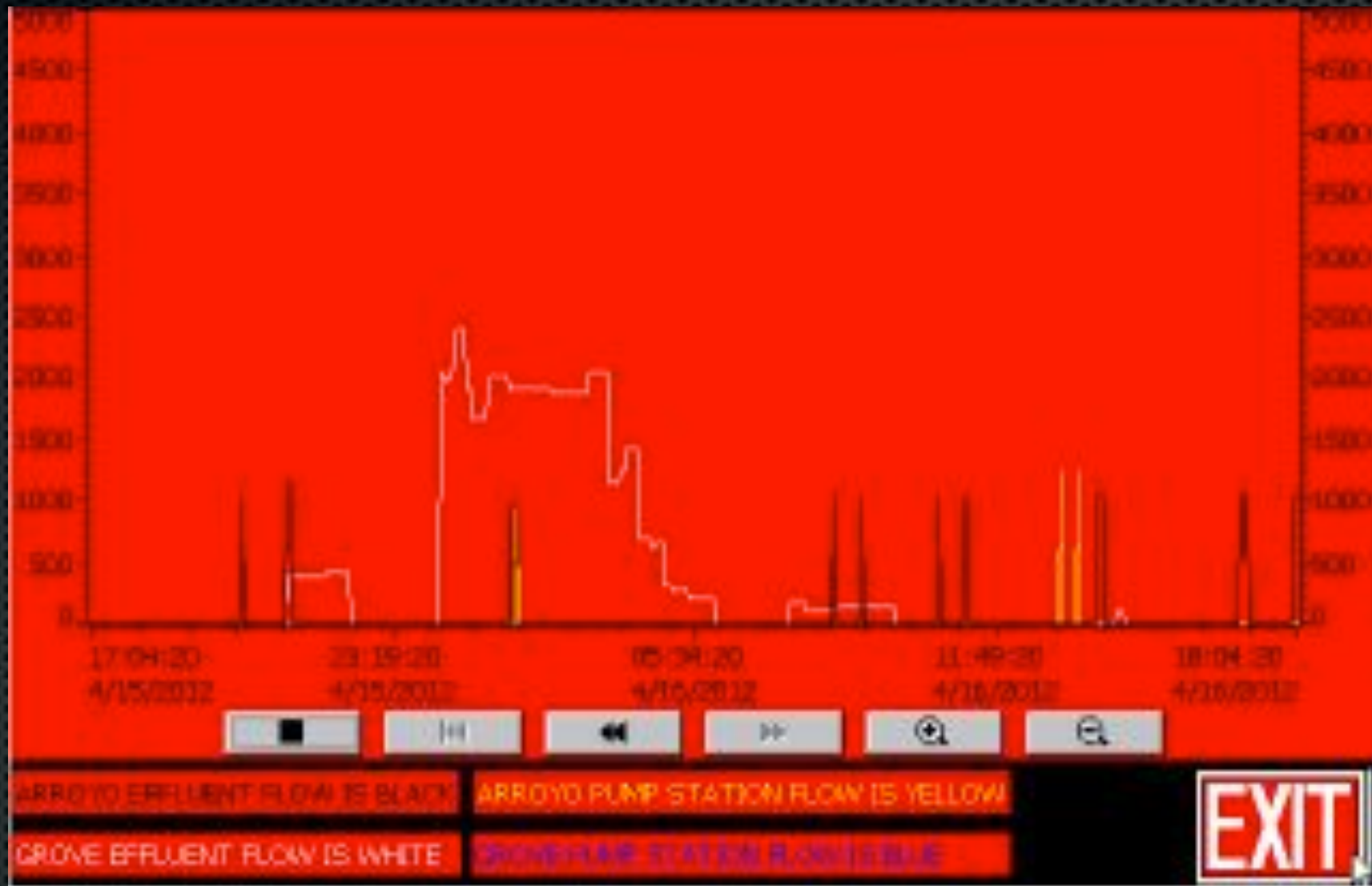
# Massive power/UPS gear.

The screenshot displays the Liebert Comprehensive View web interface. On the left is a navigation menu with categories: Control MENU, UPS Monitoring, UPS Management, Liebert Management, UPS History, and Language Selection. The main area shows a table of system parameters.

Comprehensive View	
UPS Status	On-Line
Current Utility Line Voltage (Vrms)	197.3
Output Voltage (Vrms)	230.7
Output Load (%)	14
Battery Capacity Remaining (%)	100
Current Battery Voltage (Vrms)	193.4
UPS Temperature (°C)	31.5
Input Frequency (Hz)	49.5
UPS Next Off Time (Month/Day/Year)	
UPS Next On Time (Month/Day/Year)	
Liebert System Date (Month/Day/Year)	17/04/2012
Liebert System Time (Month/Day/Year)	04:36:12
Liebert Up Time (days Month/Day/Year)	8days 18:19:11



# VNC Touchpanels





Level Three:

Stuff that can be abused  
and is actually kind of  
scary



# Lonworks devices





# Its stackable! Like devo hats!

**i.LON SmartServer** POWERED BY ECHOLON

SETUP VIEW SETTINGS HELP LOG OFF

Submit Back

## ATP\_SktPaulsGa/Channel 1/iLON App/AN\_Omega: Configure

Name: ATP\_SktPaulsGa/Channel 1/iLON App/AN\_Omega

Description:

**Summary**

Format: CSV  
Size: 50 KB  
Entries: ~ 201  
File: ATP\_SktPaulsGa/Channel 1/iLON App/AN\_Omega

**History**

Format: CSV  
Size: 100 KB  
Entries: ~ 433  
File: ATP\_SktPaulsGa/Channel 1/iLON App/AN\_Omega

Log

Alert

Delay

Output

Aggregation Time (seconds)

0 Seconds

**Navigate**

- General
- Driver
- AN\_Omega
- OL\_Omega
- LHS Network Interface (1)
- LON.MT (Internet)
- Router (Internet)
- B
- C
- A
- IP
- 193.163.37.10
- 193.163.37.12
- 9200.mn
- ATP\_Aboutward
- ATP\_Dashboard
- ATP\_SktPaulsGa
- Comcast.Demo
- Gigamon
- Gladstone.02
- Gladstone.bust1
- HL\_A/MD
- Hedesho
- Hedesho.Camping
- Hedesho.a.Smart
- LightMaster
- MarinFerrying
- Ny\_Shalleroo
- Retrospect.02
- SV





# GIGANTIUM

Idræts - og Kulturcenter

forside

GIGANTIUM

presentation

nyheder

arrangementer

anvendelse

referencer

## Presentation

Storhal

Isarena

Is training

Ice skating on private

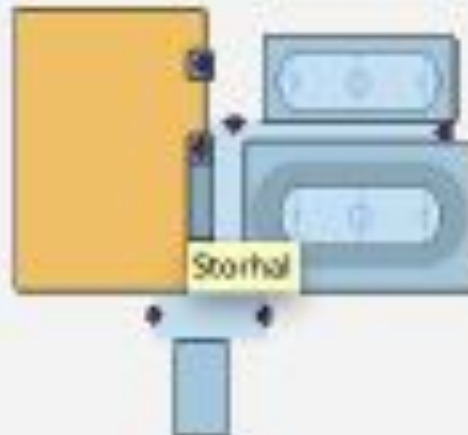
Isarrangement for  
companies / individuals

Sports hall

Foyer

Meeting Rooms

Outdoor



## Storhal



Great Hall is a heated limtræs-buehal, with more than 6,000 square meters of DIN-approved sport linoleum brand BoFlex and a further 3,000 square meters of concrete floor. Great Hall is based on a flexible system of props, mobile telescopic grandstands and other facilities that make the hall suitable for virtually all types of events.







## Contents

Hedebo Strandcamping  
Camp Information  
Location Map  
Cabin Rental  
Camper Rental  
Activities  
Sights  
Atmosphere Pictures  
Directions  
Hedebo Classic MC  
Season Room Rates  
Offers  
Prices  
Query  
Links

## Site Info



Hedebo Strandcamping  
Frederikshavnvej 108  
9,300 Sæby  
Tel 98461449  
Fax 98401313 [Email the site](#)

Open: 30.03. - 09.09.

Lon 10 ° 30 '54.7308 "

LAT 57 ° 21 '20.2752 "



## Features

# Welcome to Hedebo Strandcamping



Directly by the child-friendly sandy beach with blue flag

Our place has something for you if you bring your boat, want to fish like to swim, want to surf, want to sunbathe on the beach, loves long walks in nature or perhaps just want to sit on the bench down at havbakken and enjoy the view above sea level.



## Calendar

26-05-2012

Flan at Hedebo

[Read more](#)

[More events](#)



## Sæby Svømmebad

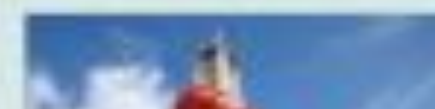


Discount Appointment:

Adults: DKK 30

Children: £ 16

Wellness: 45 kr







# Skallerup Klit



## 365 dejlige dage

[HOLIDAY HOMES & PRICES](#) | [ACTIVITIES](#) | [WELLNESS](#) | [FOOD & DRINKS](#) | [TOURIST GUIDE](#) | [CONFERENCE](#) | [FAQ](#) | 

[Booking](#)

[Offers](#)

[Brochures](#)

[Newsletter](#)

[Gift certificates](#)

[Activity summary](#)

### HOLIDAY HOMES & PRICES

#### Prices 2012

[Lævpriskalender 2012](#)

[Worth knowing](#)

[Have a REAL holiday...](#)

Skallerup offers over 262 stylish year-end holiday cottages, divided into 8 different types. You can always find a place to stay here that suits your wishes and needs and can serve as the perfect setting for a delightful holiday - right close to the beautiful nature and crashing North Sea.

Smoking is prohibited in all holiday accommodations and pets are not permitted in the E4 and E2 apartments.



WHAT TO SEE AND DO [in North Jutland](#)



CONTACT US [in North Jutland](#)

Phone: 0045 9924 8400  
[info@skallerup.dk](mailto:info@skallerup.dk)

HOW TO FIND US [in North Jutland](#)



### Classic cottages



#### Classic cottage A4

Number of people: 4

[Info](#)

[Prices](#)



[BOOK](#)

#### Classic cottage A6

Number of people: 6 + 2

[Info](#)

[Prices](#)



[BOOK](#)

### Sea cottage



So I can control the:  
power, lights, hvac  
ice skating rink, garage doors  
water pressure and boilers

Of something like 36  
businesses  
all in one town?



# What about phones?

Phones indexed by shodan!





# Stoplights.

Escape character is '^['.

OS-9/68K V3.3 Econolite 2070-1B(68360) 2002 TEES Erratum 2 - 68300 12/05/24 04:24:21

User name?:

Who?

URPS: DAT/dot

2070

Diagnostics Acceptance Test

Caltrans Version 2.1

DANGER!

DO NOT USE WHILE CONTROLLER IS  
BEING USED FOR TRAFFIC CONTROL  
OR SERIOUS DAMAGE, INJURY OR  
DEATH MAY OCCUR !!!

Warning!

Shutting off controller while running  
the flash memory test may corrupt files,  
or other data on the flash drive

\*\*\* DAT Main Menu \*\*\*

- 1) Processor
- 2) Front Panel
- 3) Field I/O
- 4) Async Ports
- 5) Sync Ports
- 6) Modem Tests
- 7) Utility Functions
- 8) Run Continuum
- 9) Configure Standard Tests



# AUTOPLATE.

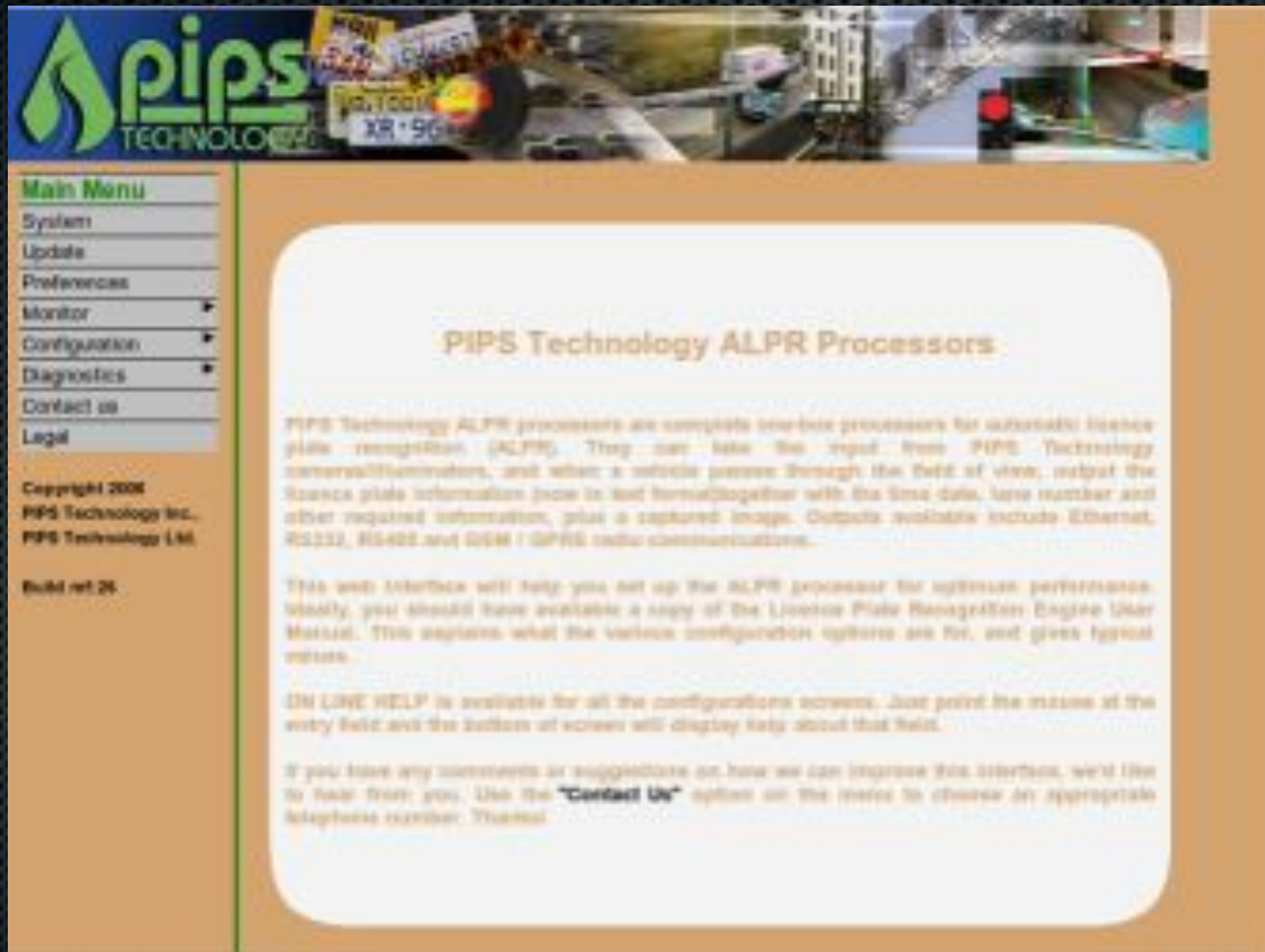
Not red-light cameras..  
something else

```
Escape character is '^['.

ATZ
POST application Apr 03 2006 09:42:23
POST Serial Number: 5998
pcb:1, vers:03, rel:06, build:003
RAM: 128M @ 128M      EPROM: 512K
Flash capabilities: 003F
  Camera Firmware: 4.34
  362 kpid vers: 13
  ABR enabled for: ISA New York & surrounding , 2262
  Operating system: C EXECUTIVE 3.3
  system image checksum: 1400
    application crc: 3a57
    current config crc: 4d8f
    reference config crc: 4d8f
  * Installed options: 00000000
  * ... Basic YES with no security
  * ... ISA Licenseplate recognition
  * PIPS Technology AUTOPLATE (ta) license plate recognition
  * YES - (violation enforcement system)
>>TTM
Available Commands are:
  system
  active
  client
  vt
  jpeg
  bap
  yes
```



# PIPS: The company that makes autoplate.





# PIPS: want license plates?

Display Type:  Data transfer:

Gain/Shutter: 2/11 Plate: VO8939 Width: 720 Confidence: 86:1824		MPA279 511ms 1 1019.1741051.1, MPA279.91.00005914.148629092 wes_image set recvd after 1126 ms on cam:1, lane:0 wes_head: using 980 next is 981 wes_create_er: slot 0 p:11ms, f:0ms, c:558ms wes_image: evidential record overall size: 51136 bytes inc 15 padding crc:f63a wes_image: jpeg:569ms, hmac:0ms, encrypt:0ms, crc: 18ms wes_image: recvd slot 0 open_link: 10000 servers 0 udp_ping: (36 ms) recvd 98.172.63.198 98.175.128.190 5081e513 01315155 0000021f 5791 881 0 wes_image: cap to host IRI: 1793ms, req to host: 79ms, f_tx:7ms wes_clear_slot: 0 wes_tail: set to 981 wes_tx: scan pass wes_del: periodic delete wes_tx - servers found wes_tx: scanning for BSRs wes_tx: BSR scan complete wes_tx: scanning for summaries wes_summary_scan: starting summary scan wes_tx: summary scan complete wes_tx: scanning for VQSI wes_tx: starting vosi ER scan wes_tx: VQSI scan complete wes_tx: scanning for SERs wes_tx: starting SER scan wes_tx: SER scan complete wes_tx: scanning for ERs wes_tx: starting normal ER scan wes_tx: ER scan complete
Gain/Shutter: 2/9 Plate: DBCF177 Width: 720 Confidence: 81:1773		
Gain/Shutter: 2/11 Plate: X289102 Width: 720 Confidence: 84:1853		
Gain/Shutter: 2/11 Plate: MPA279 Width: 720 Confidence: 91:1867		



# DakTronics.

The screenshot shows the DakTronics website with a blue header. The main navigation bar includes links for Products & Services, Support, Company, Employment, and Investors. A secondary navigation bar lists Products, Applications, Services, Archived Resources, Photo Gallery, and Video Gallery. A breadcrumb trail reads: DakTronics > Products & Services > Products > Software & Controllers > DMS Software & Controllers > Vanguard.

**DAKTRONICS**  
Scoreboards, Displays, Video, Sound

Products & Services | Support | Company | Employment | Investors

Products | Applications | Services | Archived Resources | Photo Gallery | Video Gallery

← DakTronics → Products & Services → Products → Software & Controllers → DMS Software & Controllers → Vanguard

**DMS Software & Controllers**

- > DMS Control Hardware
- > Vanguard v4 Control Software
  - > Professional
  - > Standard

**TRANSPORTATION BLOG**

**TRANSPORTATION**  
ISO 9001:2008 REGISTERED  
QUALITY MANAGEMENT SYSTEM

Vanguard Professional Message Scheduler

Vanguard Professional Display Monitor

Vanguard Professional Content Studio

**Vanguard® v4 Professional Software**

Vanguard Professional enacts powerful control over large DMS networks from traffic management centers. Professional includes all the monitoring, message creation, and



# DakTronics.





# Ruggedcom!

**N4-DLC**

**Passwords**

Auth Type:

Guest Username:

Guest Password:

Confirm Guest Password:

Operator Username:

Operator Password:

Confirm Operator Password:

Admin Username:

Admin Password:

Confirm Admin Password:



# Ruggedcom!

**N4-DLC**

**Passwords**

Auth Type: Local

Guest Username: guest

Guest Password: guest

Confirm Guest Password: guest

Operator Username: operator

Operator Password: operator

Confirm Operator Password: operator

Admin Username: admin

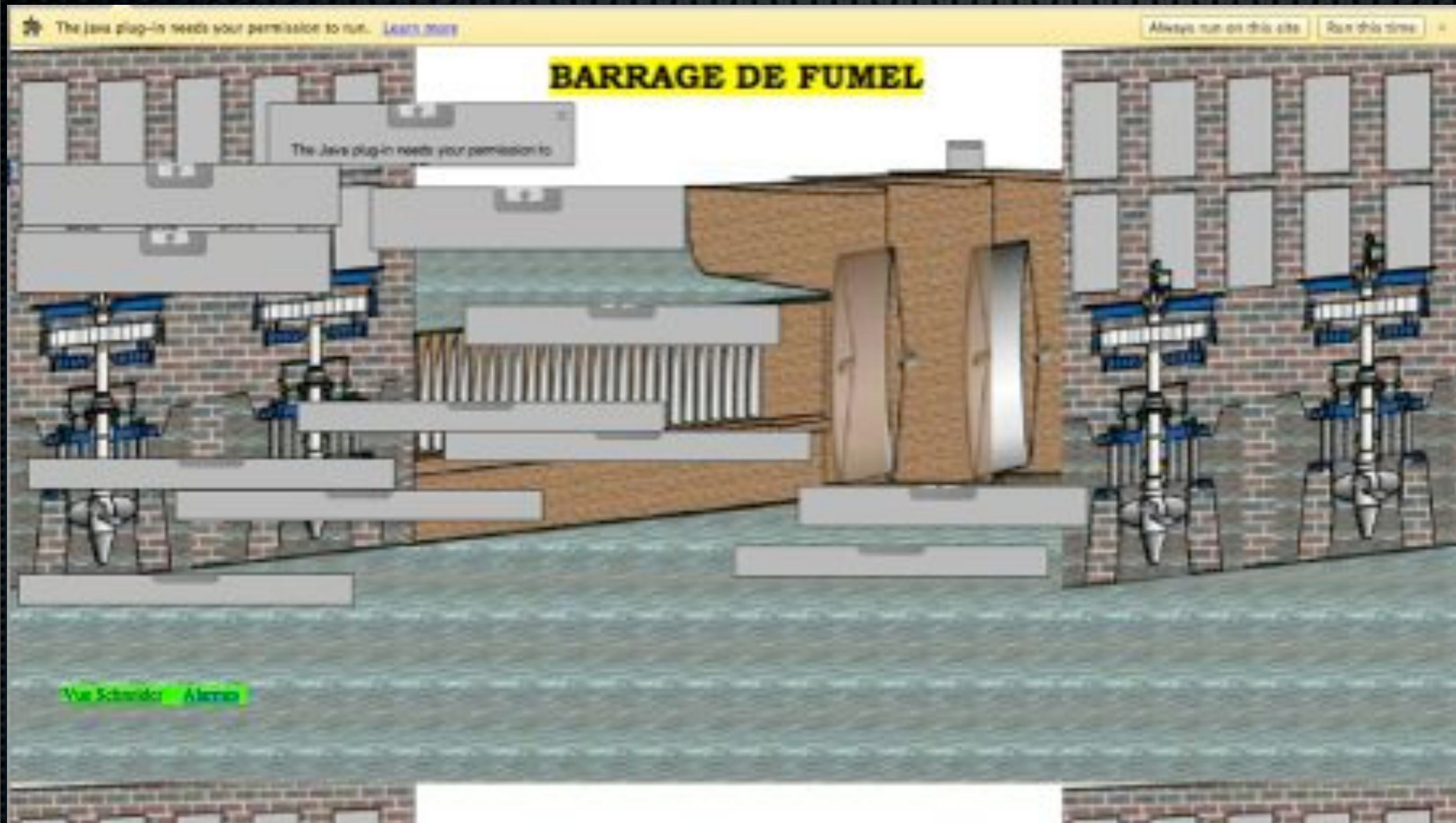
Admin Password: admin

Confirm Admin Password: admin

Apply Reload

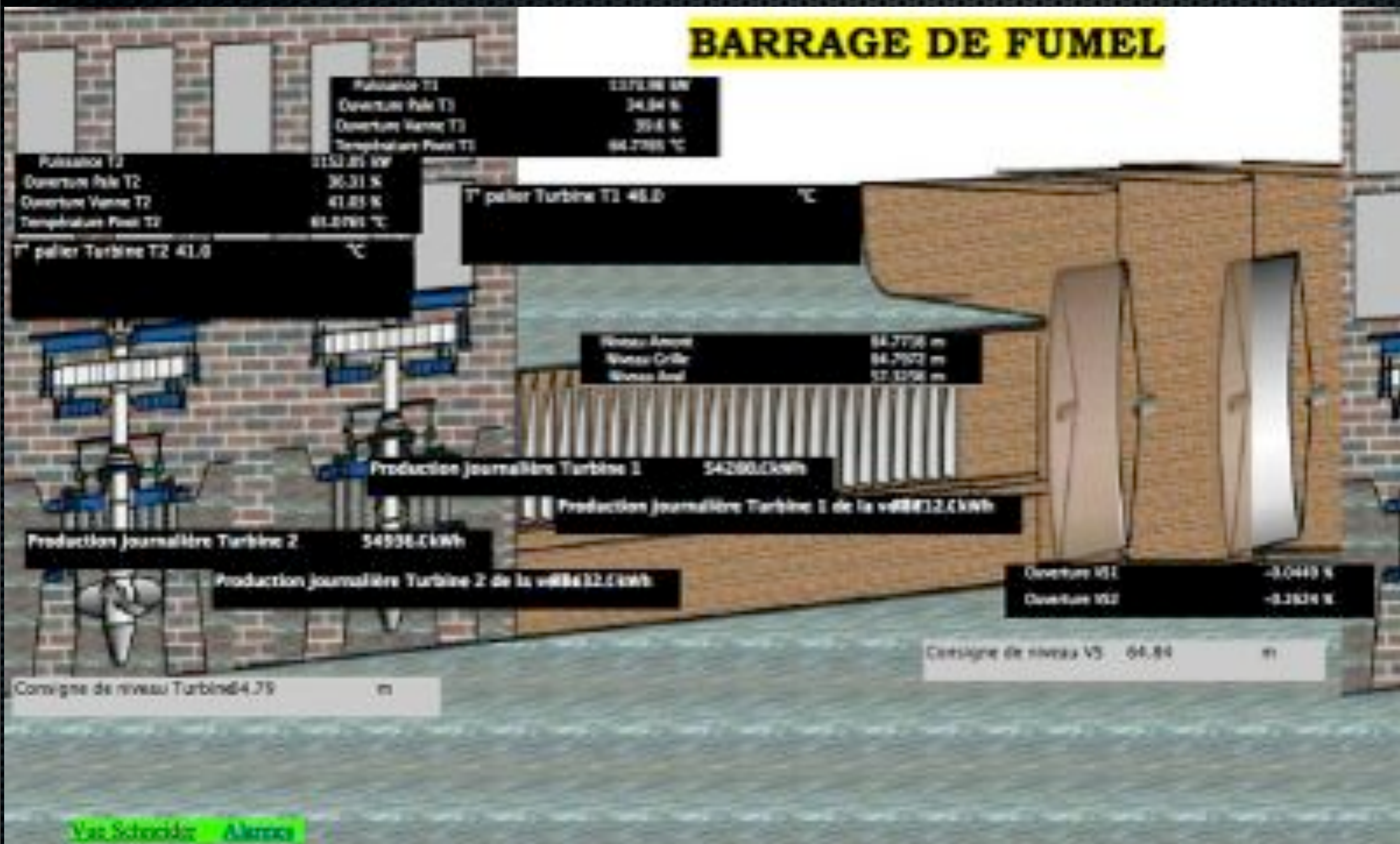


# Malware on safari?





# kW? .. wat.





POSTED ON 22/01/2008 8:59

[ADD A COMMENT](#)

## Dam Fumel residents want assurances

A MEETING WAS HELD YESTERDAY IN FUMEL THE FLOODS LAST FRIDAY, IN THE PRESENCE OF ALL PARTIES AND RESIDENTS.

How to live next to a dam. Delicate question which rested on Friday when the waters of the dam Fumel began to rise. Quickly. Very quickly. Too fast for riparian floods. At that point one of them even got up to 50 inches of water in his house. Some seniors even had "the fear of their lives when some electrical appliances began to crack." How to live next to a dam if you do not know what can happen. Yesterday, a meeting was organized in Fumel in the presence of all the authorities to take stock of the situation. And very soon, it seems that the appearance of criminal acts Friday has passed. This confirmed that the building manager Philippe Gronchi for "energy Fumel": "We fully recognize our responsibility and of course we will draw the consequences. This dam is an old building which dates from 1943, bought the company in 2005 Sogetec. We have already achieved more than 14 million euro investment and probe this issue, because it is a problem of probe will be resolved as soon as possible. " In the audience, listening but we are still angry. "Before, it never happened. There, that's three that we suffer floods in 9 years. You understand that we are tired all the more that we are not and never prevents as soon as the water rises, it is we who call the fire department. In addition, there are many older people who live in fear. We would like this to stop," said a local resident.

an alarm float

Philippe Gronchi speaks again: "We had a second warning that Sunday has confirmed that this was a concern of the probe. Of course, we will soon be remedied this problem by doubling the particular probe. In the meantime, there will be someone who will be present to manage the flow. " Later, an alarm float should be installed at Condat to prevent rising waters. And the head of the DRIRE adds: "In the past, there was an agreement that was signed between EDF and the factory. At each rising waters, signaling was performed. It might be good to update this agreement. " But certainly the rising water was normally regulated in recent years without automatic warning from the factory.

Another point discussed during the meeting last night, the insurance. Again, residents were reassured by the firm that provides the dam. Damage will be covered only necessary that such residents concerned make a declaration to their insurance as soon as possible, which will then return. And the mayor of Fumel, Jean-Louis Costes, also ask that the insurance can pay more quickly damaged equipment.

*Laurent Michel Lasserre with Moary*



I put that on twitter.

A day later DHS  
called my cellphone.



Also, that UI was  
built in  
frontpage.



**YES,  
FRONTPAGE.  
  
ON SCADA.**



**AND  
SOMEONE  
BOUGHT  
IT**



**THEN PUT IT  
ON THE  
INTERNETkajelj  
kalsjknbfllkajbe  
gkbja**



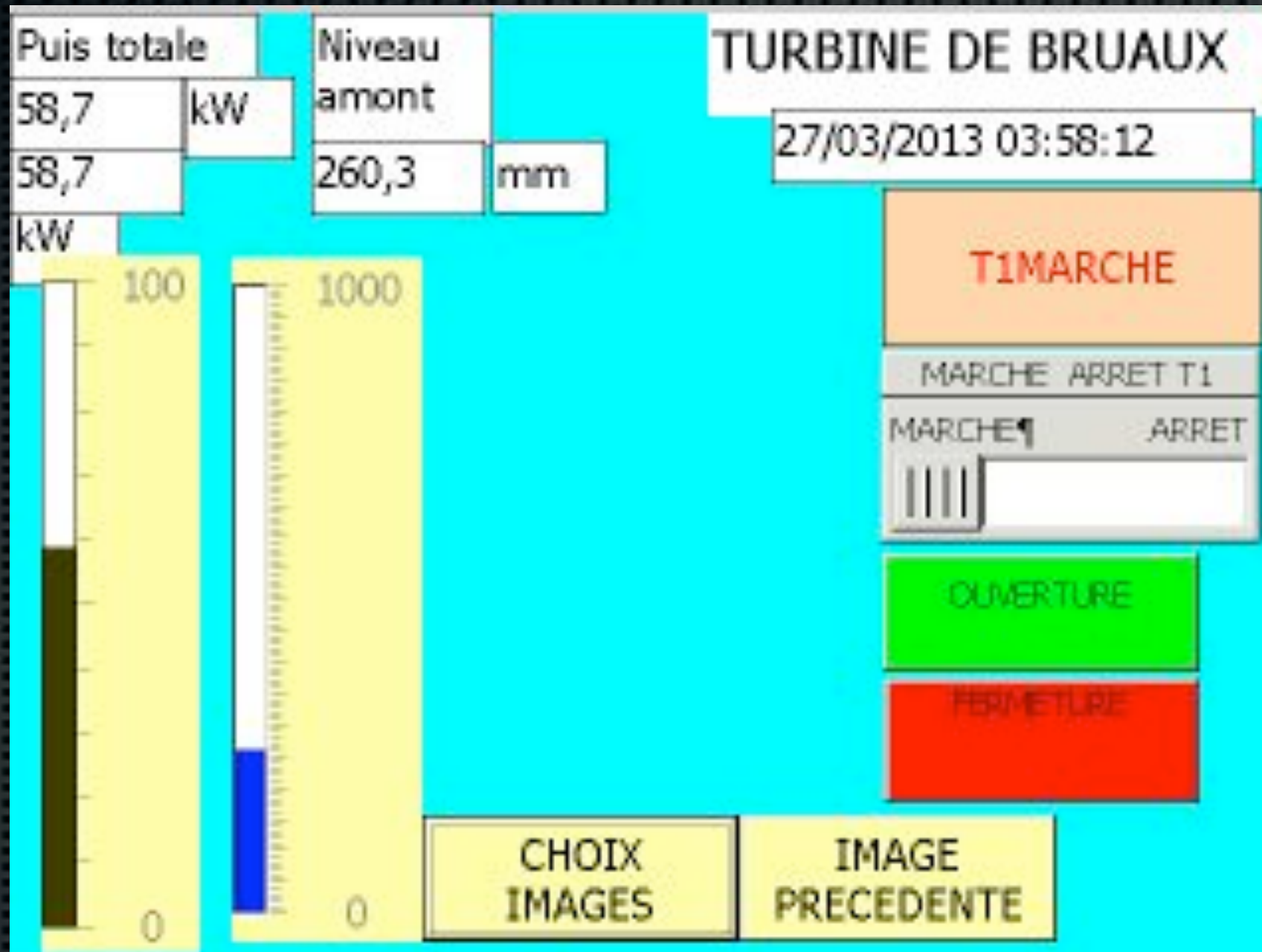
**\*ahem\***



**You'd think they'd  
LEARN.**

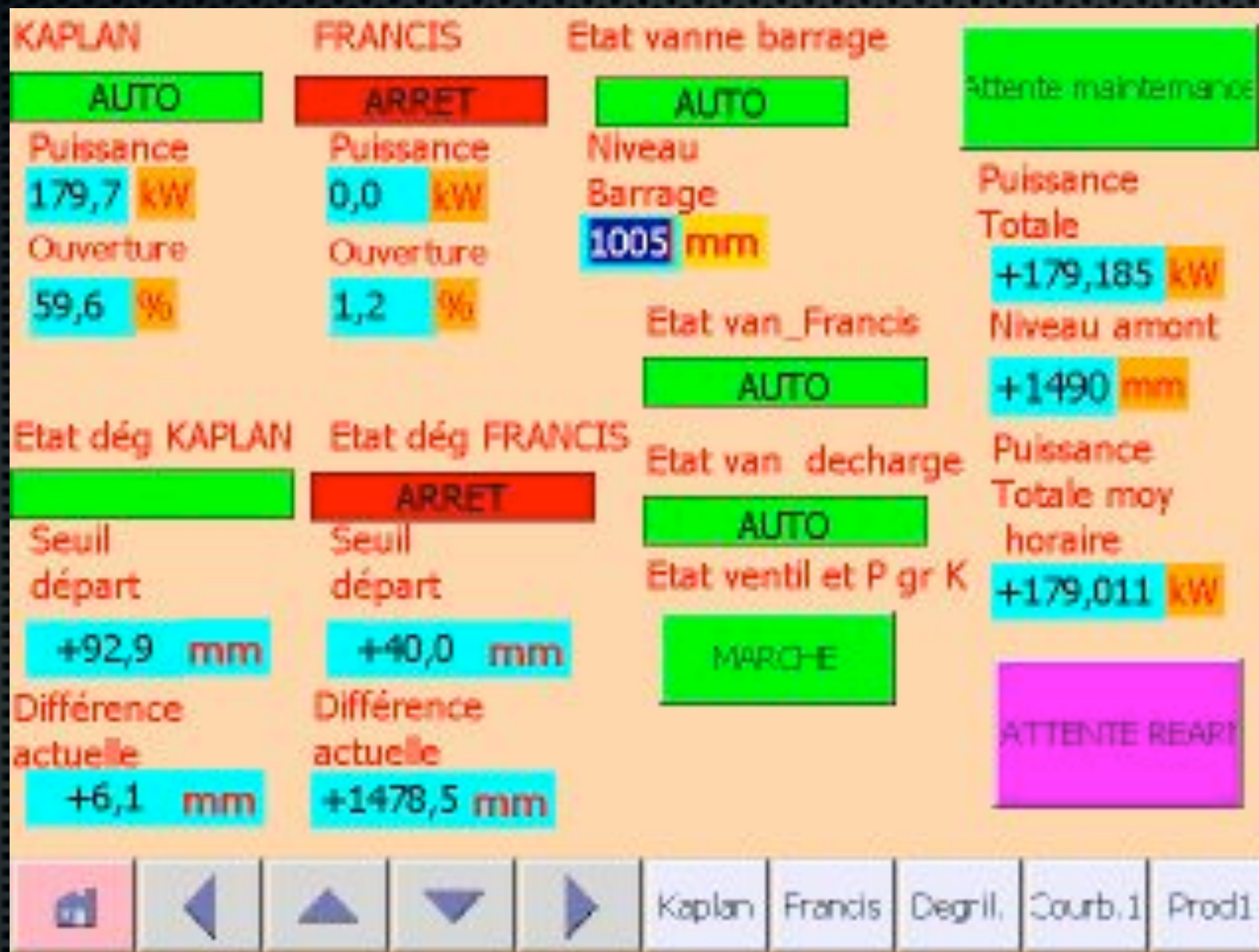


# .. but they dont.



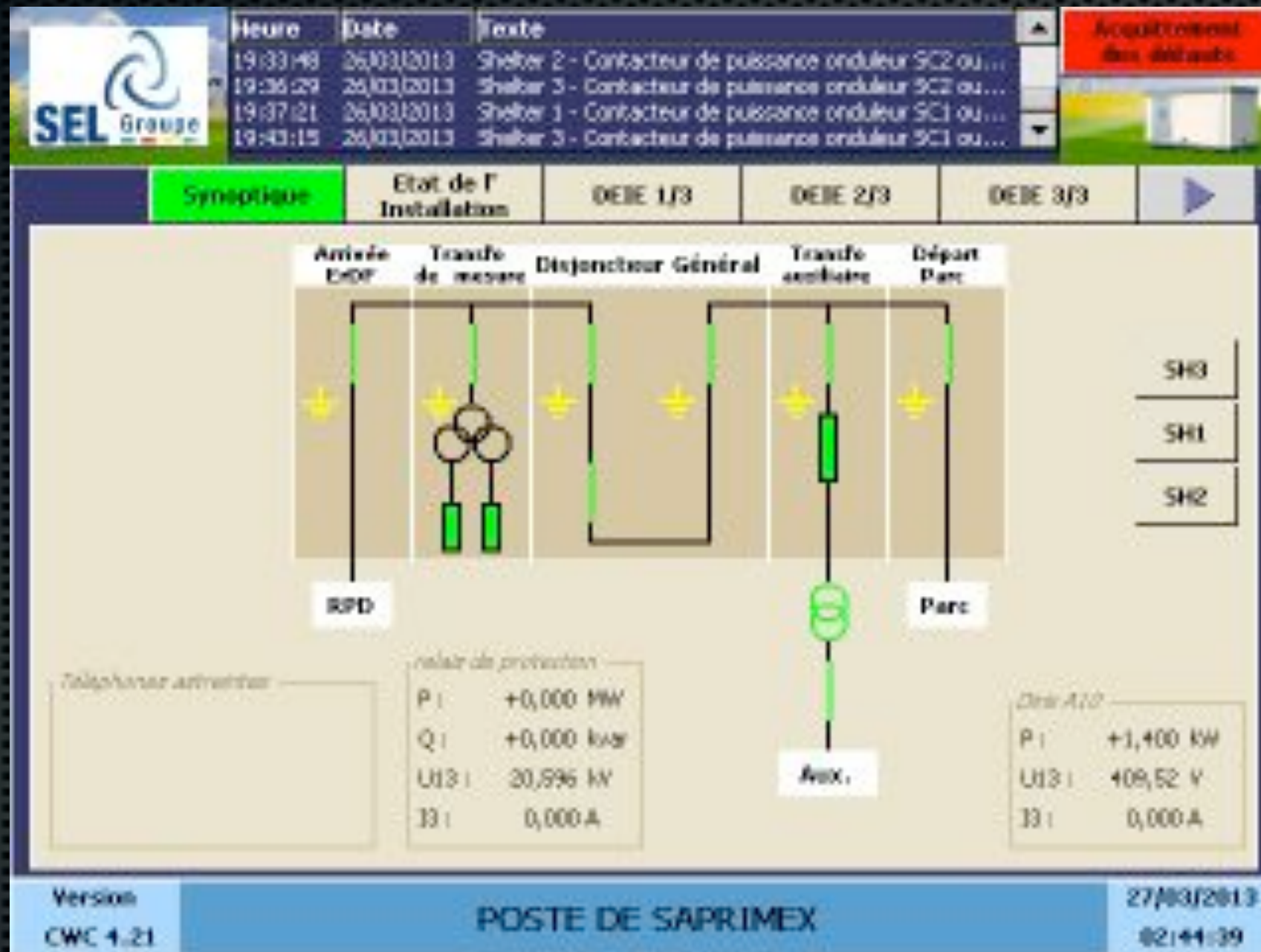


# .. they really dont.





# .. they really dont.





# Satellite systems





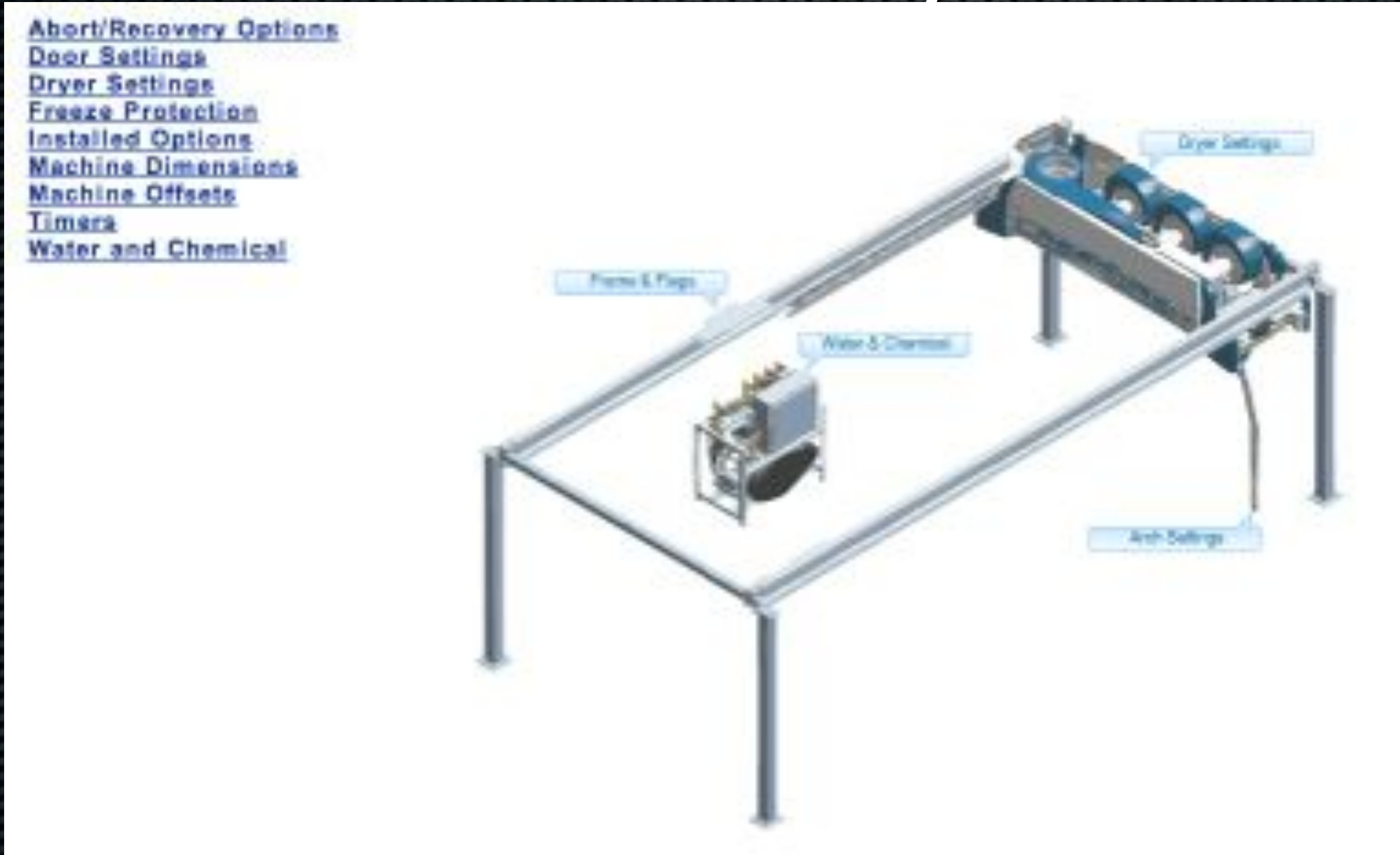
# NAS storage arrays





# “LaserWash”

## Car Wash Systems





# Humidifiers

**DRISTEEM**

Vapor-logic4

**STATUS**

**ALARMS**

**DIAGNOSTICS**

**SETUP**

**HELP**

## System Status

**DEMAND**

44.9%

**OUTPUT**

44.8%

**RUN MODE**

Auto

**TANK  
STATUS**

Boiling

## Alarms

**0 active alarms**

> [View Alarms](#)

## Messages

**0 active messages**

> [View Messages](#)

Wed Jul 11 2012 22:28:31 GMT-0700 (PDT)

Data stream is LIVE

View all humidifier settings below. Some settings can be changed here. Go to the Setup tab to change settings that cannot be changed from this page.

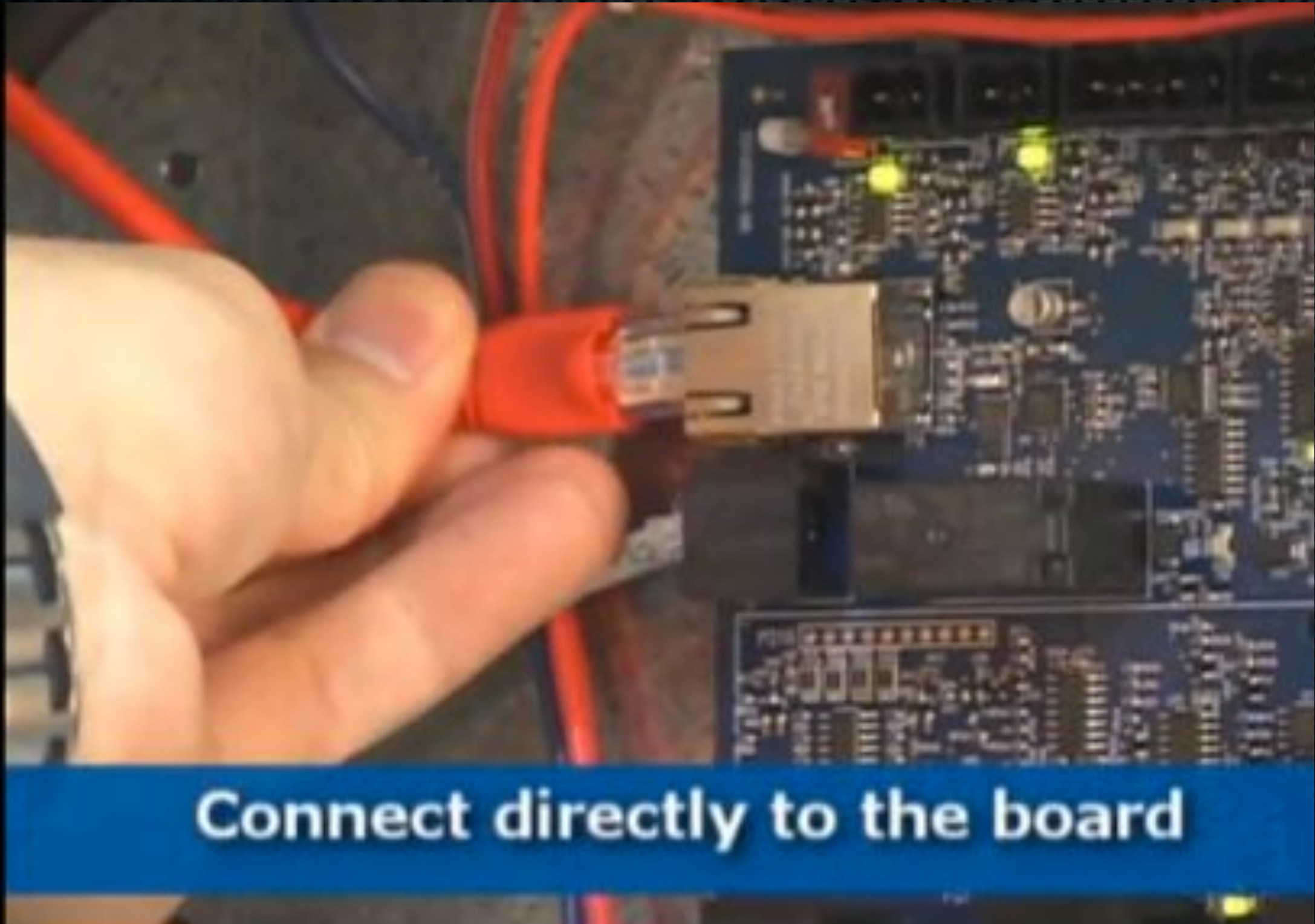
## TANK STATUS:

Run Mode	Auto	<a href="#">CHANGE</a>
Input signal	4.5 VDC	
Steam output	44.8%	
Steam production	8 lbs/hr	
Duct HL switch	Closed	
Tank temperature	218°F	
Tank temp signal	1745 Ohms	
DE low water switch	Water	
Fill valve	Open	
Drain valve	Closed	
Airflow switch	Flow	
Interlock switch	Closed	
H2O until service	1163 lbs	

© Copyright 2010 DRI-STEEM Corporation. All rights reserved. Vapor-logic is a registered trademark of DRI-STEEM Corporation.



# Humidifiers





# Emergency Telco gear



Switch reliably.



aztek  
NETWORKS

[HOME](#) [PRODUCTS](#) [SOLUTIONS](#) [WHERE TO BUY](#) [COMPANY](#) [SUPPORT](#) [CONTACT](#)

## Resources

- [5000S](#)
- [5000L](#)
- [5000S-1](#)
- [5000S-2](#)
- [5000S-3](#)



## 5000S ESA Switch

Aztek Networks' 5000S ESA switch is the first and only purpose-built true emergency stand-alone switching device that is fully redundant, field cabinet ready and truly capable of seamless interoperability with any open-standard GR-303 access element or host switch.

The Aztek 5000S continuously monitors the signal between a host switch and an access device such as a DUC, DLD or MSAF, and becomes the active switching element only if the signaling link between the host switch and the access device becomes inactive.

### FEATURES


- True ESA switching
- Based on standard GR-303
- Works with legacy DUCs or new BUCs and MSAFs
- Compact design
- Environmentally hardened
- 16 DLI (8+8)
- Most solution for switch collapse or replacement of proprietary RSUs

©2012 Aztek Networks. All Rights Reserved.



# Emergency Telco gear

**Aztek 5000S**

**aztek**   
NETWORKS

Slot A Status: **Active** Mode: **Monitoring** **Logout**

**Operations**  
Shelf Management  
**Alarms**  
Logs  
Call Detail Record  
Lock Mode  
**Provisioning**  
OLC  
DST  
**Configuration**  
Alarm Severity  
911 Designee Barge-In  
Timeouts and Delays  
ACTS  
Networking  
Password  
**System Update**  
Dial Plan  
Software Download  
Software Swap  
**Support**  
On Demand Tests

Date/Time	Severity	Object Type	Object ID	Location	Category	Description
1970/02/02 - 20:10:19	Minor	SWUPDATE_SERVICE	0	CTA Slot B	Equipment	Dial Plan download fault
1970/01/01 - 00:00:19	Minor	RESOURCE_SERVICE	0	CTA Slot A	Equipment	ACTS time fault

Refresh this page every  seconds.



# wait what?

```
//*****  
// You are free to copy the "Folder-Tree" script as long as you  
// keep this copyright notice:  
// Script found in: http://www.geocities.com/marcelino\_martins/foldertree.html  
// Author: Marcelino Alves Martins (http://www.mmartins.com)  
// 1997--2001.  
//*****  
  
// Log of changes:  
//      10 Aug 01 - Support for Netscape 4  
//  
//      17 Feb 98 - Fix initialization flashing problem with Netscape  
//  
//      27 Jan 98 - Root folder starts open; support for OSSTEXTLINKS;  
//                  make the ftien4 a js file  
  
// Definition of class Folder  
// *****
```



# ...speakers?





# A massive wine cooler

Station
Root
Device Networks
N2 Network
1-FX07-02
Points

Navigation

- 74.101.128.141 (Mark\_Hotel\_Wine\_...
- Device Networks
  - N2 Network
    - 1-FX07-01
      - Points
    - 1-FX07-02
      - Points
  - Nagana Network
  - Schedule Manager
  - Link Manager
  - Point Groups
  - Global Point Extension Manager
  - Alarm Console
  - Point Histories
  - Administration
    - Files
      - Custom Control
    - AlarmService
    - EmailService
      - EmailRecipient
      - OutgoingAccount
    - History Container View
    - Point Extension Defaults
    - BackupService
    - Users
    - Time Sync
    - Platform
    - Web Service
    - Serial Port Configuration
    - Display Configuration

Database

Name	Long Name	Type	Unit	Network Point Type	Network
Temp Champagne	T3	Numeric Point	75.0 °F {ok}	Analog Data Float	1
Humidity Champagne	H3	Numeric Point	58.3 %RH {ok}	Analog Data Float	4
Setpoint Temp Champagne	SpT3	Numeric Writable	44.0 °F {overridden} @ 8	Analog Data Float	17
Diff Temp Champagne	DiffT3	Numeric Writable	3.0 Δ°F {overridden} @ 8	Analog Data Float	18
Alarm Diff Champagne	ReferenceShiftT3Avg	Numeric Writable	15.0 Δ°F {overridden} @ 8	Analog Data Float	20
Alarm Delay Champagne	DelayTimeAlt3avg	Numeric Writable	3600.0 s {ok} @ def	Analog Data Float	21
Cooling Champagne	SV3	Enum Point	Off {ok}	Binary Data	1
Alarm Champagne		Boolean Point	Alarm {alarm,unackedAlarm}	Binary Data	3
Avg Temp Bar Right	AvgT4	Numeric Point	53.0 °F {ok}	Analog Data Float	5
Temp Bar Right Left	T4A	Numeric Point	52.7 °F {ok}	Analog Data Float	2
Temp Bar Right Right	T4B	Numeric Point	53.2 °F {ok}	Analog Data Float	3
Setpoint Temp Bar Right	SpT4	Numeric Writable	44.0 °F {ok} @ def	Analog Data Float	22
DiffAlarmT3Avg	DiffAlarmT3Avg	Numeric Writable	2.0 °F {ok} @ def	Analog Data Float	19
Diff Temp Bar Right	DiffT4	Numeric Writable	3.0 Δ°F {overridden} @ 8	Analog Data Float	23
Alarm Diff Bar Right	ReferenceShiftT4	Numeric Writable	10.0 Δ°F {ok} @ def	Analog Data Float	24
DiffAlarmT4	DiffAlarmT4	Numeric Writable	2.0 °F {ok} @ def	Analog Data Float	25
Alarm Delay Bar Right	AlarmDelayT4	Numeric Writable	3600.0 s {ok} @ def	Analog Data Float	26
Cooling Bar Right	SV4	Enum Point	Off {ok}	Binary Data	2
Alarm Bar Right		Boolean Point	Normal {ok}	Binary Data	5
Alarm	Alarm	Enum Point	Alarm {ok}	Binary Data	4
OffsetT3	OffsetT3	Numeric Writable	0.0 °F {ok} @ def	Analog Data Float	13
OffsetT4A	OffsetT4A	Numeric Writable	0.0 °F {ok} @ def	Analog Data Float	14
OffsetT4B	OffsetT4B	Numeric Writable	0.0 °F {ok} @ def	Analog Data Float	15
OffsetH3	OffsetH3	Numeric Writable	0.0 % {ok} @ def	Analog Data Float	16
RemoteValue401	RemoteValue401	Numeric Writable	0.0 °F {fault} @ def	Analog Data Float	6
RemoteValue402	RemoteValue402	Numeric Writable	0.0 °F {fault} @ def	Analog Data Float	7
RemoteValue403	RemoteValue403	Numeric Writable	0.0 °F {fault} @ def	Analog Data Float	8



# A massive wine cooler





# Science!

Functional Tests monitoring page *generated*

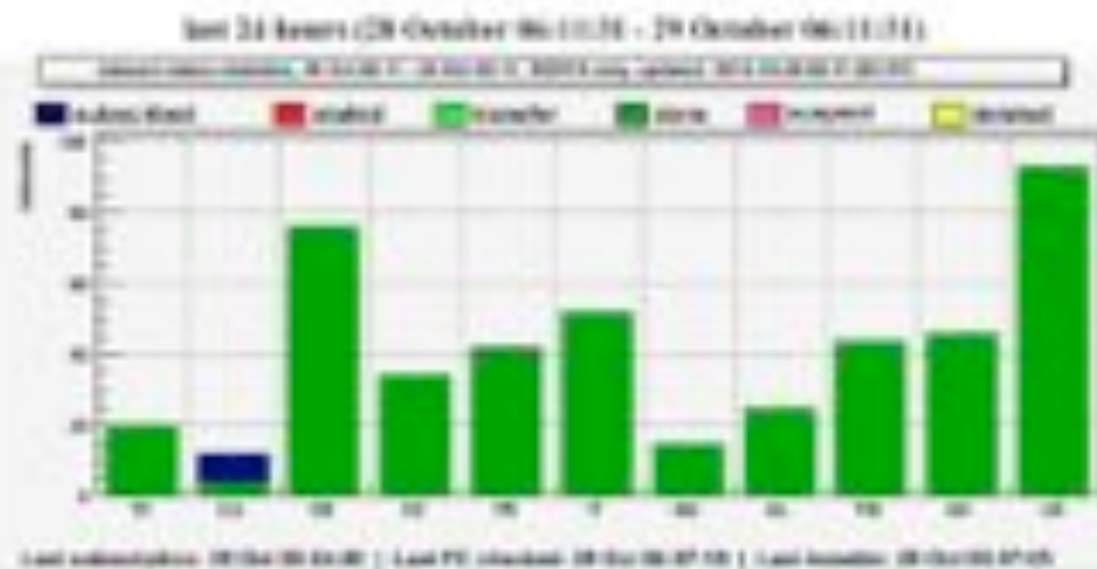
2012-09-07 11:11:00

[illegible]

This page shows database trends statistics for **TEEN** by country, by time, by city for last 72 hours and all test period



## TIERIS by clouds

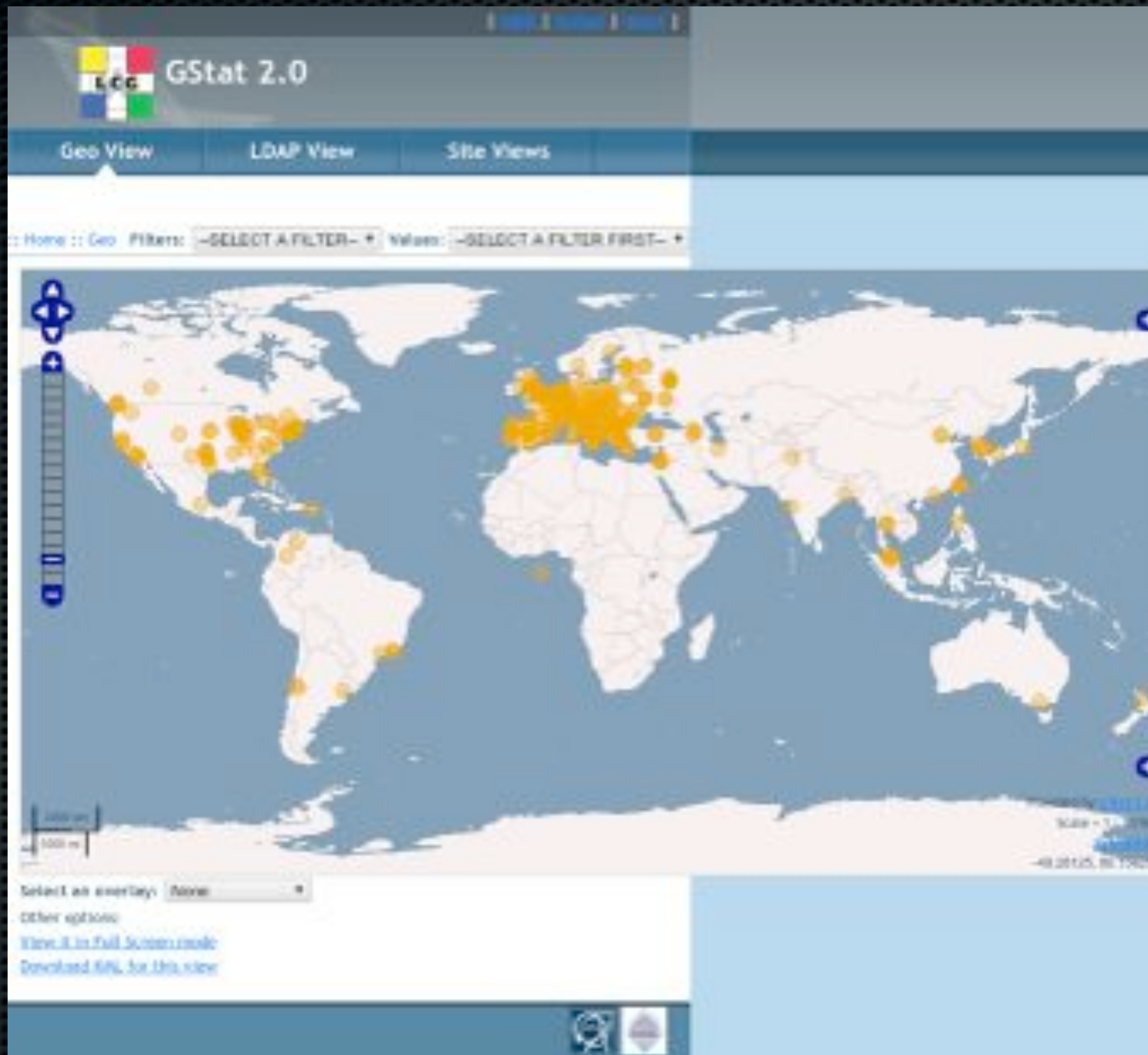


### THERIS by time





# Science!



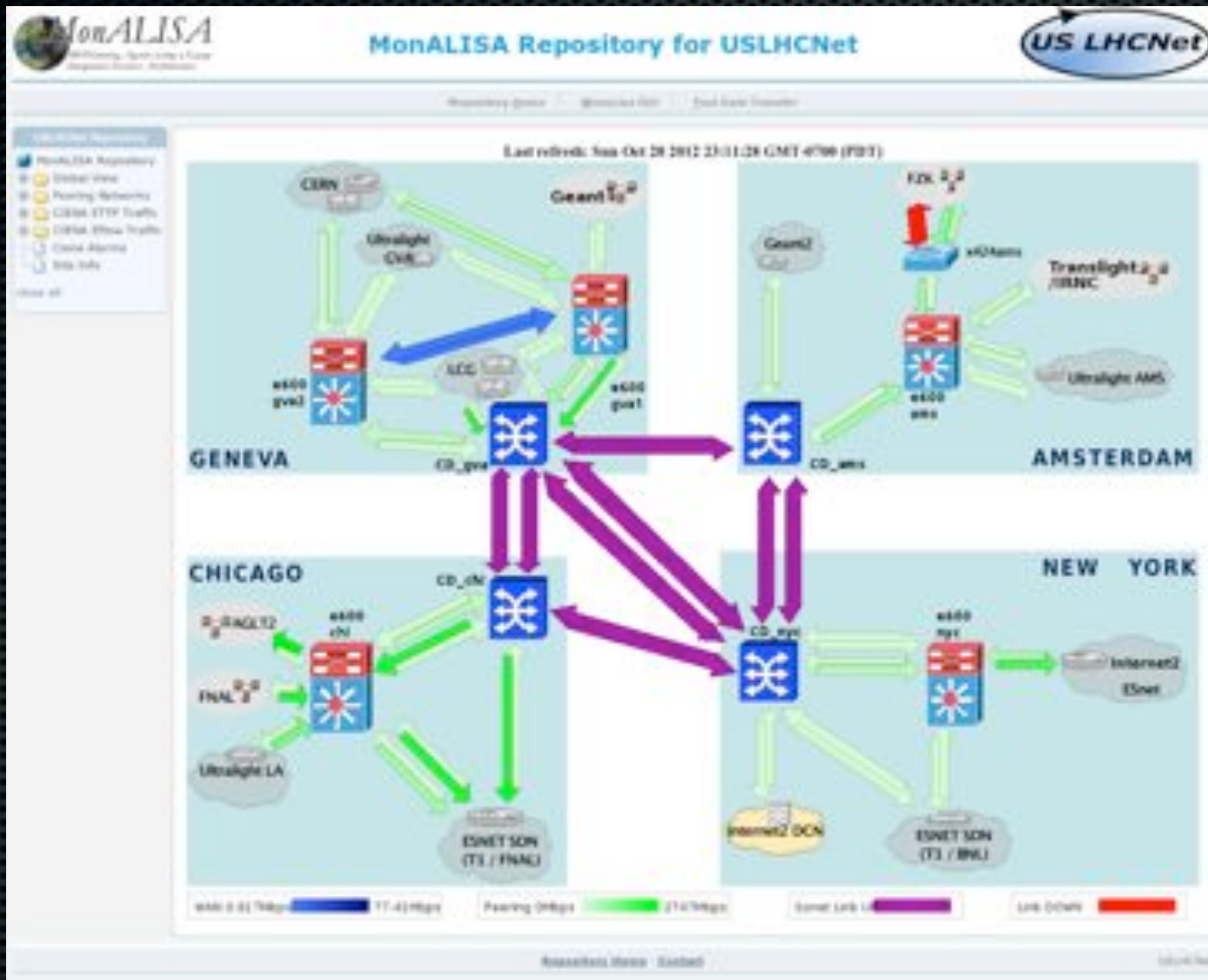


# Science!





# Science!





# Science!





# Science!





Almost all of those  
are offline now.

THANK YOU CERN  
:D



# Ski trip, anyone?

27/03/2013 07:06:50

DEFAUTS NIVEAU 1/2

CONDUITE

REARMEMENT

DEFAUTS NIVEAU 0

DEFAUTS VEHICULE

VITESSE (VEHICULE)

VEHICULE

COUPLE

NIVEAU : 0

0,00 m/s 43,2 m 21,3 m 0 %Cn

MONTEE

V 1

V 2

V 3

V 4

PORTES FERMÉES

SHIFT PRET

NIVEAU 2

NIVEAU 1

NIVEAU 0

VEHICULE

FREIN DE SERVICE SERRE


FREIN DE SECURITE SERRE

ARRET FREIN DE SECURITE

ARRET FREIN DE SERVICE

ARRET ELECTRIQUE

SKIRAIL



SEMER

05 135

CLOS DE LA MADRAGUE


CONSIGNE : 0,75 m/s CONSIGNE +/- VITE : 0,75 m/s

MODE MAINTENANCE : CONDUITE DEPUIS PUPITRE MOTRICE


ARRET EXPLOITATION PORTES FERMÉES

ARRET EXPLOITATION PORTES OUVERTES

NIVEAU 2



NIVEAU 1



NIVEAU 0

PIN DE COURSE

PRESENCE VEHICULE

NEZ DE GARE

FINS DE COURSE

POINT FIXE

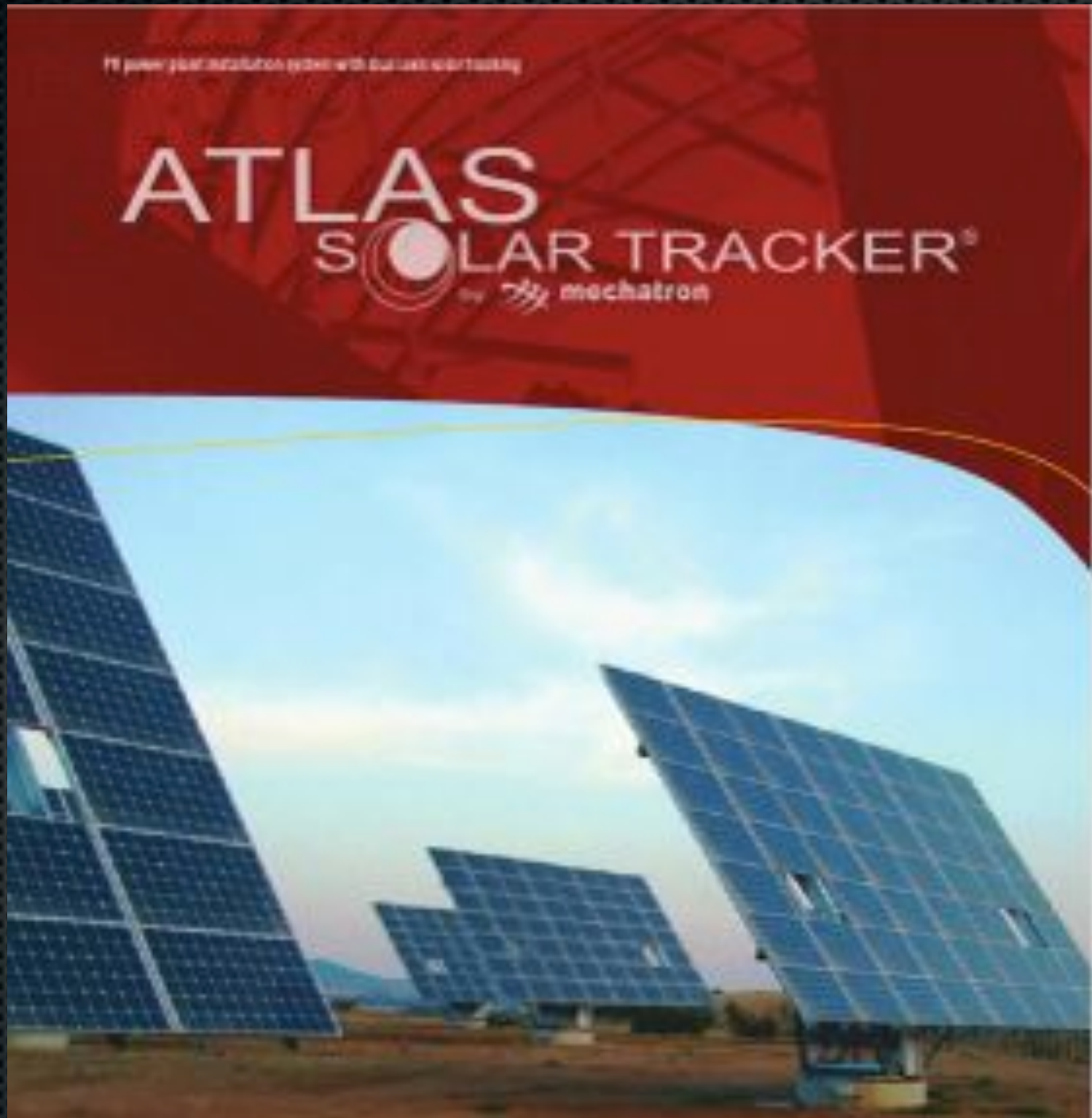


# Massive solar arrays





# Massive solar arrays





# Massive solar arrays

ATLAS  
SOLAR TRACKER

Firmware Version: 1.01.54

Setup

ZHTML ERROR: No read access to variable

ZHTML ERROR: No read access to variable  
ZHTML ERROR: No read access to variable  
ZHTML ERROR: No read access to variable  
ZHTML ERROR: No read access to variable  
ZHTML ERROR: No read access to variable  
ZHTML ERROR: No read access to variable  
ZHTML ERROR: No read access to variable

ZHTML ERROR: No read access to variable  
ZHTML ERROR: No read access to variable  
ZHTML ERROR: No read access to variable  
ZHTML ERROR: No read access to variable

## Plant / Overview

Trackers

ZHTML ERROR: No read access to variable

Wind speed

Wind speed 1

Wind speed 2

Wind speed 3

0 Km/h

Operating status

Tracking: ZHTML ERROR: No read access to variable

Horiz.Park: ZHTML ERROR: No read access to variable

Alarm: ZHTML ERROR: No read access to variable

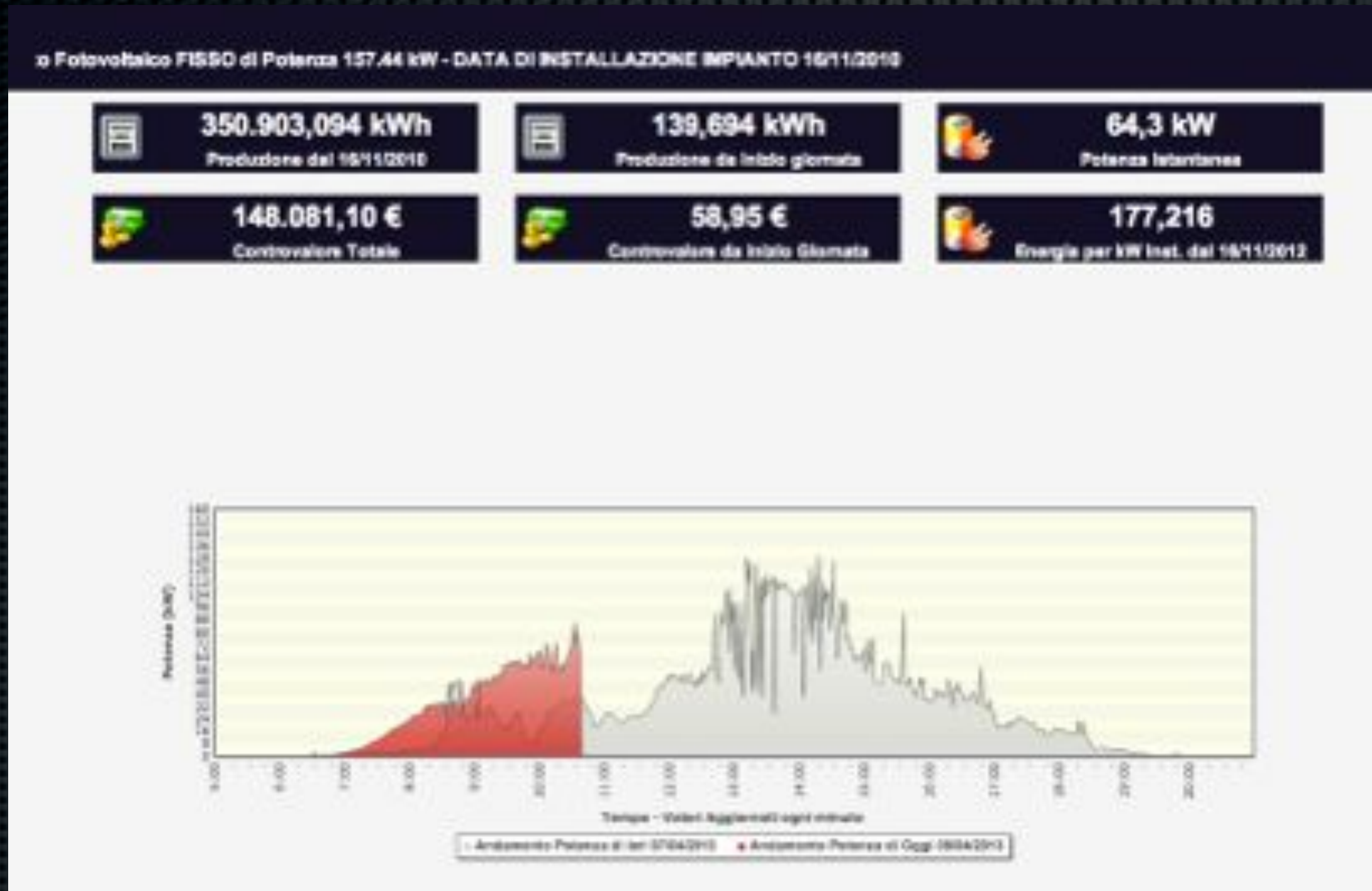
No Comm: ZHTML ERROR: No read access to variable

Wind Statistics

Clear

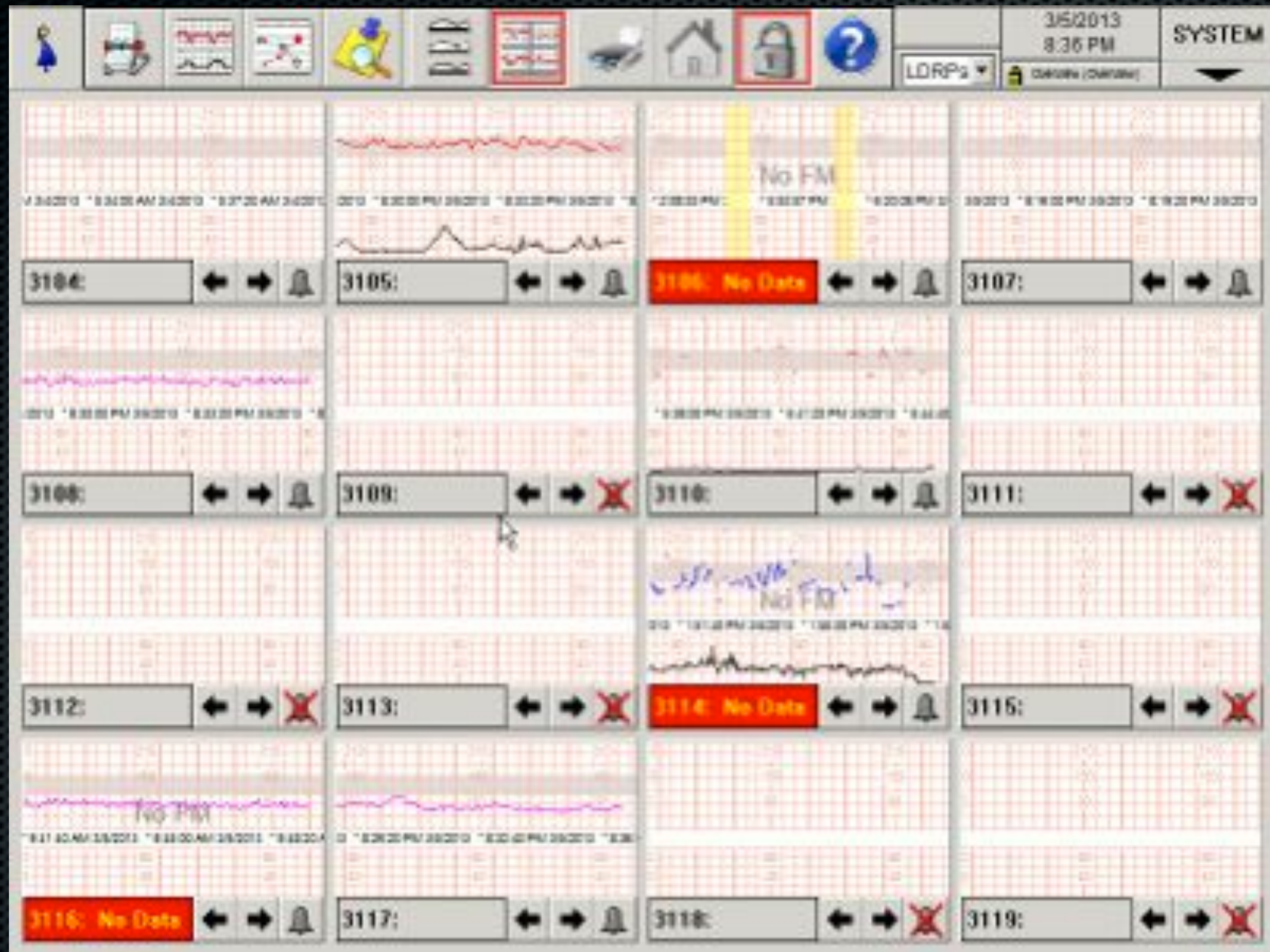


# Massive solar arrays





# TraceVue





# Home Automation

myHome Control

Status	Off
Occupancy	Occupied Night >
Upstairs Temp	69.0
Upstairs Setpoint	70 °F >
Downstairs Temp	66.6
Downstairs Setpoint	67 °F >
Garage Door	<input type="checkbox"/> OFF
Alarm State	Disarmed >

Lighting

Security

HVAC

Weather



# .gov oopsies






# .gov oopsies

**:: TR-49 Series**

**Images** (click thumbnail for larger image)



**Key Features:**

- » Supports 802.11a/g modes
- » OFDM Technologies
- » Configurable in Point-to-Point, Access Point or Client modes
- » Quality of Service (QoS)
- » Dual Powered Ethernet Ports
- » Web-based administration interface
- » Robust Routing
- » Security (WEP, WPA, MAC Authentication)
- » Tunneling Protocol Support
- » Configuration LEDs (if in Access Point mode)
- » Alignment LEDs (if in Client Adapter mode)
- » SNMP
- » Latest firmware releases have support for 5, 10 & 20 MHz channel bandwidths
- » Includes: PoE, Boot-cover, Mounting Kit (Dual Ethernet Boot Cover Optional)



# .gov oopsies

## Overview:

Tranzeo Wireless Technologies has received FCC approval on the TR-49 Series of product which is designed specifically for Homeland Security use in the 4.9 GHz frequency band. This spectrum has been allocated by the Federal Communications Commission for the exclusive use of Municipal, State and Federal Agencies.

Tranzeo Wireless Technologies products in this spectrum allow for the rapid deployment of Wireless Networks facilitating such varied uses as Video Conferencing; rapid internet and database access to vital data such as maps, building layouts, medical files and missing person images; Voice over IP (VoIP) communication; and audio/video surveillance.

These product lines represent a monumental shift in Tranzeo's product offerings, as all previous products operated on unlicensed frequencies.




# .gov oopsies

```
SMFPv2-MIB::sysDescr.0 = STRING: Tronzo TR496t, OS 6.6.6(1624), FW TR49-5.6.76t  
, 4.5GHz, 19dBi int. antenna  
SMFPv2-MIB::sysObjectId.0 = DID: SMFPv2-SMI::enterprise.24575  
DISMAN-EVENT-MIB::sysUpTimeInstance = TimeTicks: (29675695) 3 days, 18:59:16.95  
SMFPv2-MIB::sysContact.0 = STRING: Contact  
SMFPv2-MIB::sysName.0 = STRING: [REDACTED] Ser 155  
SMFPv2-MIB::sysLocation.0 = STRING: Location  
SMFPv2-MIB::sysServices.0 = INTEGER: 15  
IF-MIB::ifNumber.0 = INTEGER: 3  
IF-MIB::ifIndex.1 = INTEGER: 1  
IF-MIB::ifIndex.2 = INTEGER: 2  
IF-MIB::ifIndex.3 = INTEGER: 3  
IF-MIB::ifDescr.1 = STRING: Wi-Fi802.11a  
IF-MIB::ifDescr.2 = STRING: Ethernet0  
IF-MIB::ifDescr.3 = STRING: Ethernet1  
IF-MIB::ifType.1 = INTEGER: ieee80211(71)  
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)  
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)  
IF-MIB::ifMtu.1 = INTEGER: 1500  
^C
```



# ... a fishery?



Control Systems

## HAYMANS FISHERIES RIOT

List

Input

---

Inputs

1 <a href="#">Freezer 1</a>	Log	Edit	Delete
2 <a href="#">P.P. Cooked Chilli</a>	Log	Edit	Delete
3 <a href="#">Smoked Fish Chilli</a>	Log	Edit	Delete
4 <a href="#">Lobster Chilli 1</a>	Log	Edit	Delete
5 <a href="#">Filleting Process Area</a>	Log	Edit	Delete
6 <a href="#">Fresh Wet Fish Chilli</a>	Log	Edit	Delete
7 <a href="#">Cutting Preparation Area</a>	Log	Edit	Delete
8 <a href="#">Dispatch Chiller</a>	Log	Edit	Delete
9 <a href="#">By Products Waste</a>	Log	Edit	Delete
10 <a href="#">R.U Display Cabinet 1</a>	Log	Edit	Delete
11 <a href="#">R.U Display Cabinet 2</a>	Log	Edit	Delete
12 <a href="#">R.U Display Cabinet 3</a>	Log	Edit	Delete
13 <a href="#">R.U Display Cabinet 4</a>	Log	Edit	Delete
14 <a href="#">Smoked Prep Area</a>	Log	Edit	Delete
15 <a href="#">Smoked Packing Room</a>	Log	Edit	Delete
16 <a href="#">IT Room</a>	Log	Edit	Delete

Templates

[10 IT](#) Edit Delete

New Input Delete all inputs Cancel



# ... a fishery?

Inputs

- 1 [Freezer 1](#)
- 2 [P.P. Cooked Chill](#)
- 3 [Smoked Fish Chill](#)
- 4 [Lobster Chill 1](#)
- 5 [Filleting Process Area](#)
- 6 [Fresh Wet Fish Chill](#)
- 7 [Cutting Preparation Area](#)

**WAT**

Log 4 Ed

Log 4 Ed

Log 4 Ed

Log 4 Ed

Log 4 Ed

Log 4 Ed





# I'm in your scadas..





# Wait, no, lobster chillmode



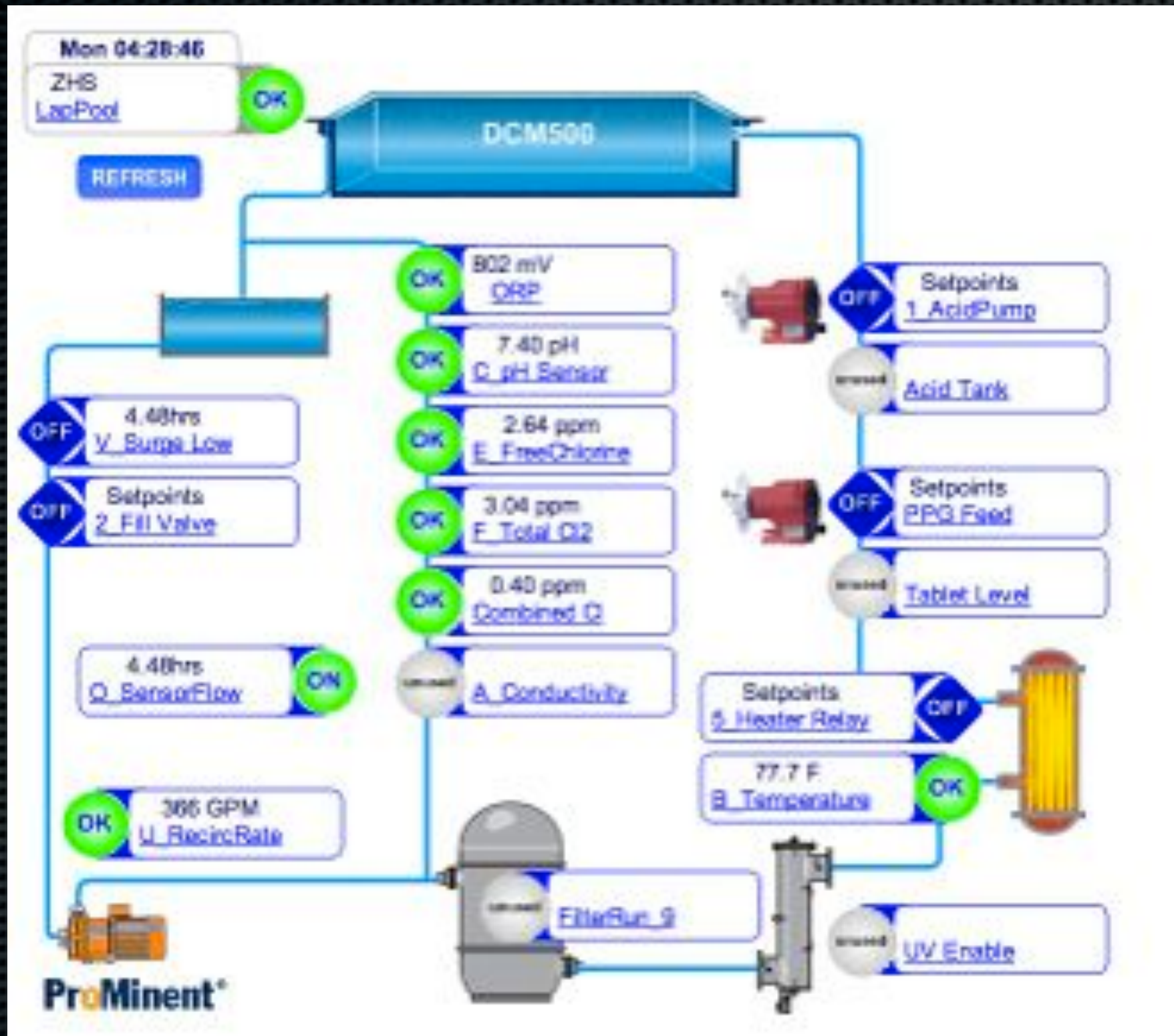


# Cant forget the champagne!



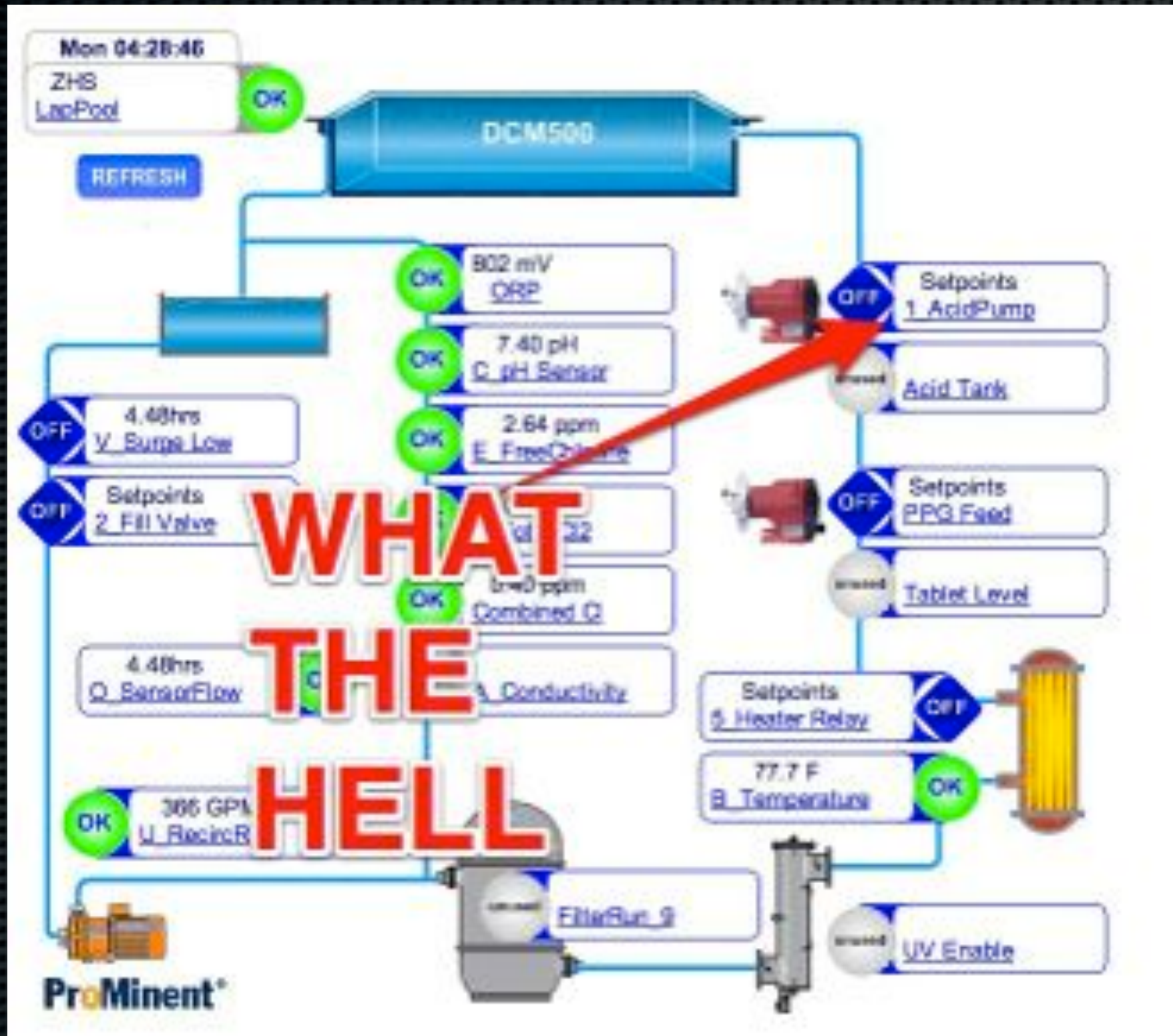


# Swimming pools!





# Swimming pools!





# Swimming pools!

1\_AcidPump:1

Diagnostic

Status	Special Control,OFF
Mode	<div>Auto</div> <div>Manual</div> <div>OFF</div>
Control by: C	7.40 pH
TurnON setpoint	7.48 pH
TurnOFF setpoint	7.43 pH
Control Type	Feed Acid

---

0.0m ON today	0.0m ON, actuation
---------------	--------------------

---

Time Modulate Period: 120	OFF Countdown: 0, seconds
------------------------------	------------------------------

---

REFRESH

SUBMIT



# ... really? An acid pump?

Installation Guide

**ProMinent®** DCM 200 series

Aquatic Water Quality Controller



... really?  
An acid pump?









# so 80s style horror flick scenario



(these are actually defcon goons in a pile..)



so jason vorhees  
shows up...





But his victims  
are soup.





# He's gonna be PISSSED.





**So, Say you find stuff  
on your banjo dinosaur  
knitting adventure**

**A lot of stuff.**

**50,000+ results...wat do?**

**h/t @travisgoodspeed**

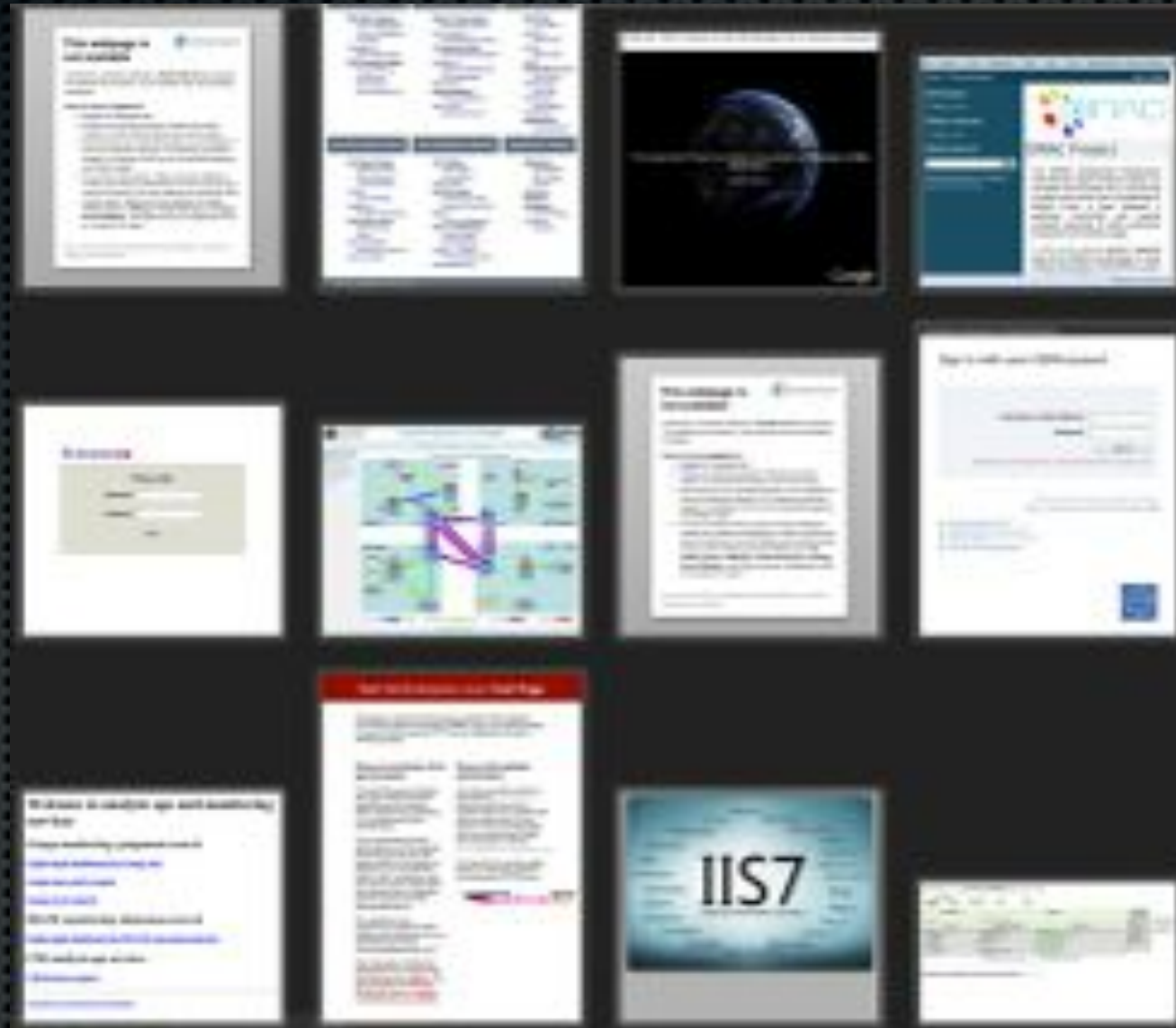


**Screenshot  
All  
THE THINGS!**

**:D**



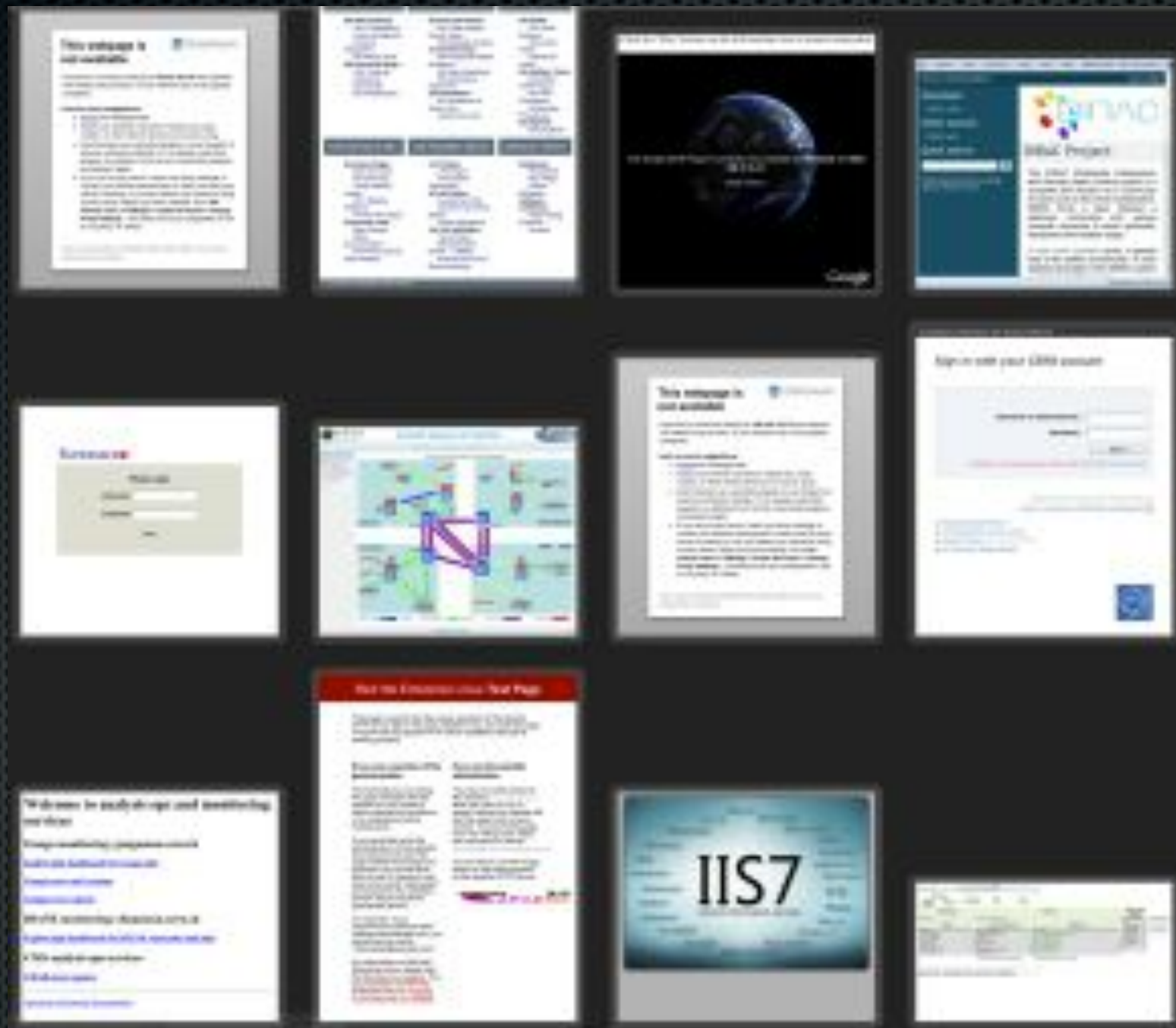
# 50k sites by hand sucks



# screenshots are WAY faster! :D



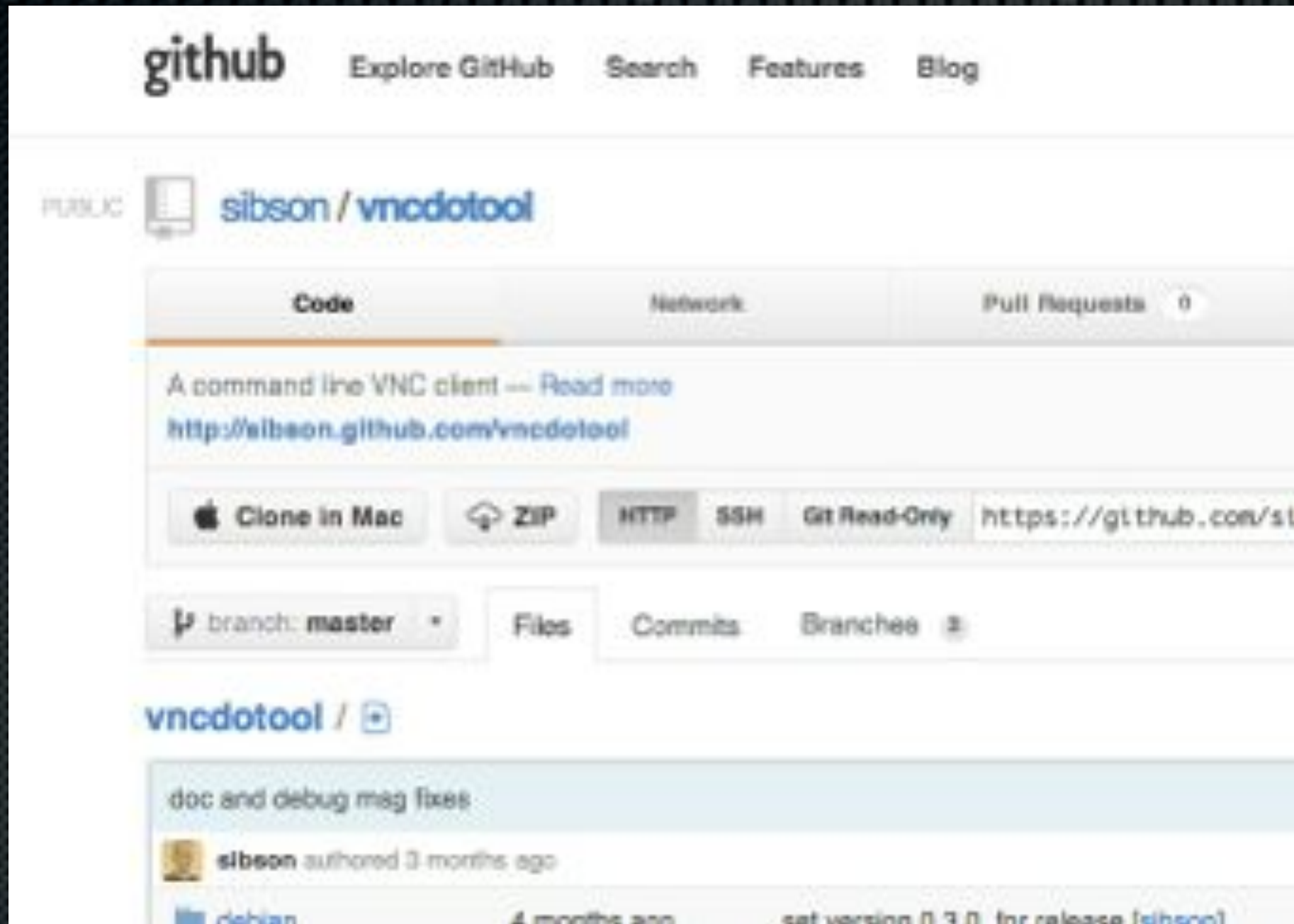
# I had help too



<https://github.com/PaulMcMillan/eagleeye2>



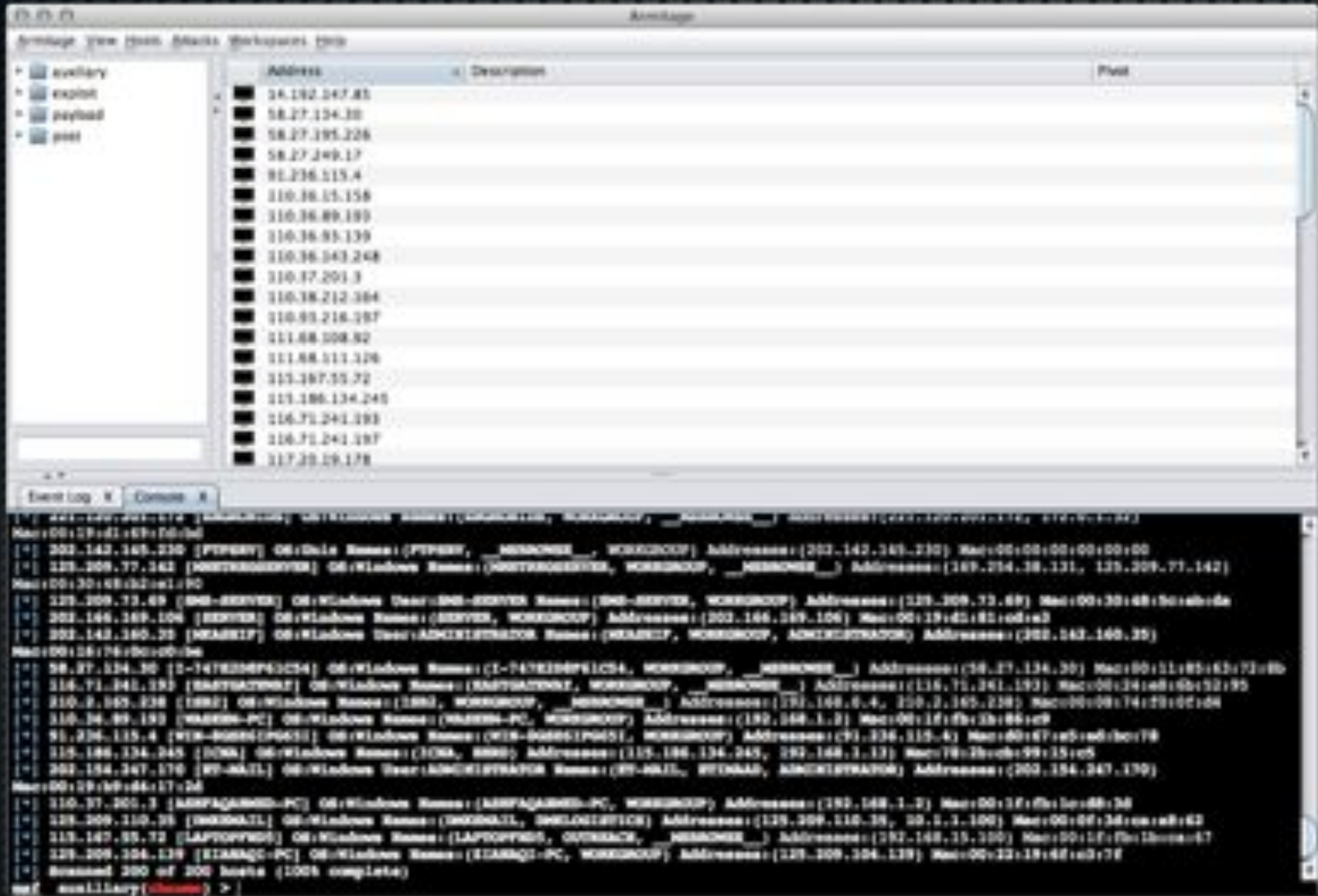
# you can do this with vnc





# Maybe you want to pwn

# Pipe output to metasploit/armitage/teamserver!





# The best defense is a good offense, right?

Run this stuff on yourself. The attackers already do.



# Spot outliers.

Does your staff setup EC2 instances without approval from the business? Other sites?

What else is connected to the internet, with YOUR COMPANIES NAME on it, that you don't know about?

Who actually LIKES random, unknown liability?



# Some cool new features:

You can search by:::

org:

city:

country:

state:

net:



**You guys are awesome  
Thank you for letting me  
rant!**

**[github.com/Viss/Eagleeye](https://github.com/Viss/Eagleeye)**

**[github.com/PaulMcMillan/eagleeye2](https://github.com/PaulMcMillan/eagleeye2)**

**Twitter: @Viss  
[atenlabs.com](http://atenlabs.com)**