DEFCON

Exploiting and attacking seismological networks .. Remotely

Bertin B – James jara NetDB Search Engine

DEFCON 24 Las Vegas, Nevada

Disclaimer

- This is not a typical talk

-Probably it is the first research of this kind

-All vulnerabilities have been reported to U.S CERT

-We are not responsible of the actions that someone can take after attend this talk

-Peace on earth

Agenda

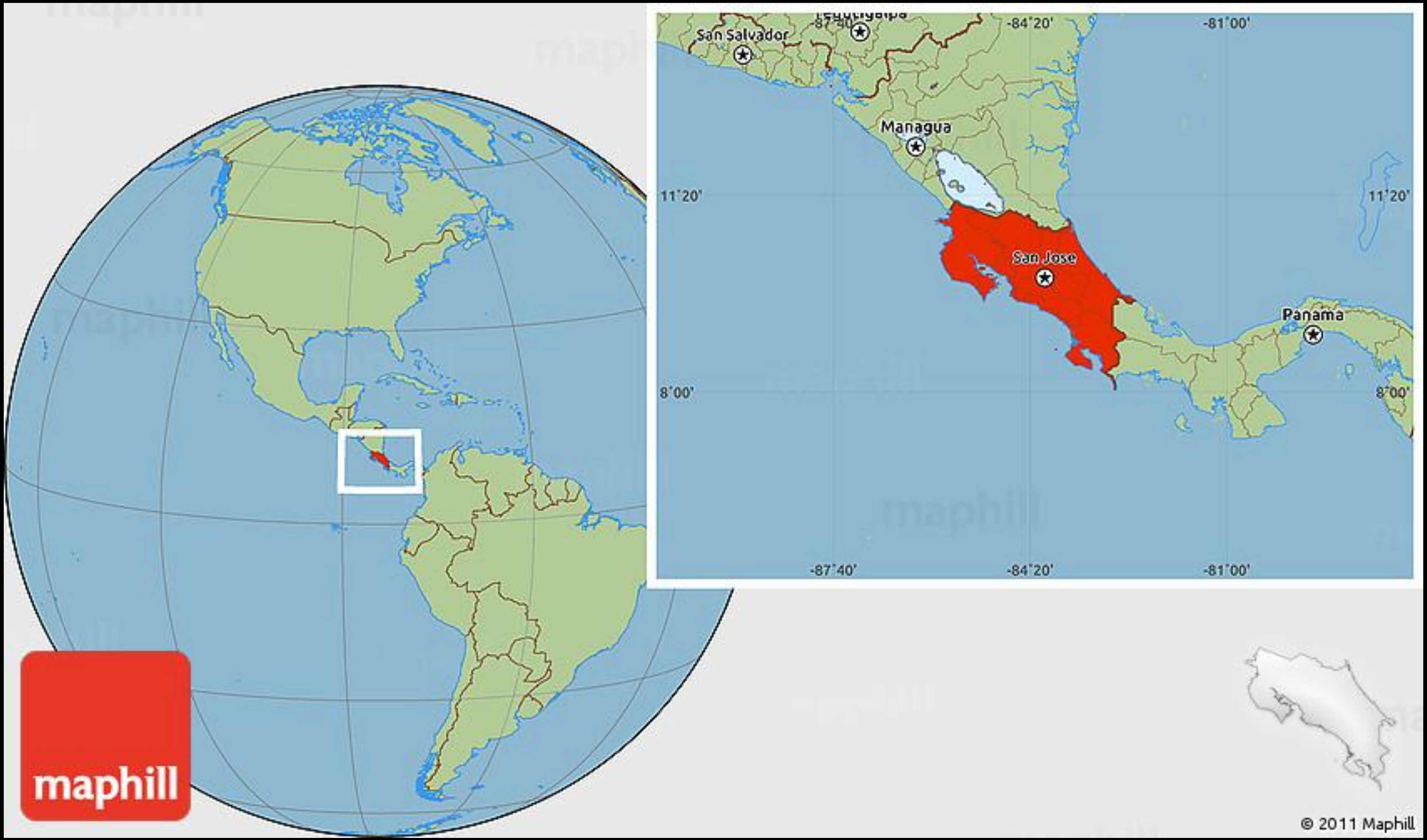
-Who we are
-Motivation
-How we discovered this devices?
-Risk /Impact , who is affected by attacking this devices ?
-Seismological instrumentation
-Internals /Deployment/Networking
-Vulnerabilities /firmware analysis
-Attack vectors / post exploitation
-Recommendations/conclusions

Bertin Bervis
NetDB Co-founder
@bertinjoseb

James Jara
NetDB Co-founder
@jamesjara

netdb
Iot Search Engine

We are from San Jose Costa Rica



Motivation

Why we are interested in seismological networks?

An average attacker is not interested for this attacks

Governments are interested.. you know.. …..!@#$% WAR

Cool and new attack scenario ¨extreme environment¨

You are playing with devices that measure natural disasters

Could lead to a financial sabotage to a specific company/country

The vendors of this instruments doesn’t have any sense of computer security

Remote access, remote exploitation

Ok let’s continue this project…

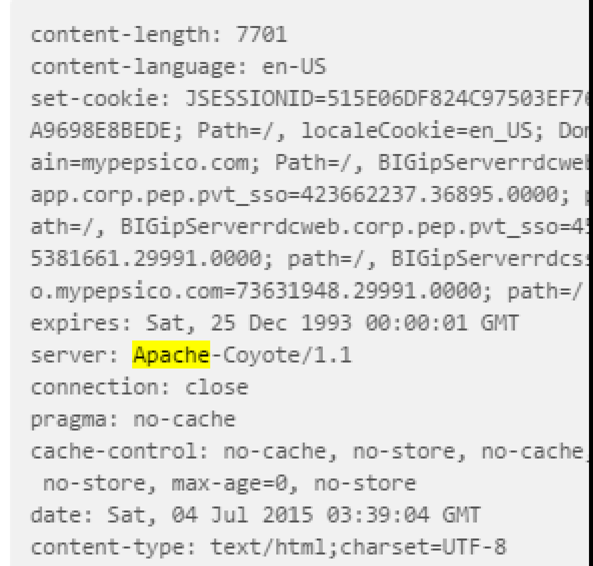
How we discovered this devices?

netdb

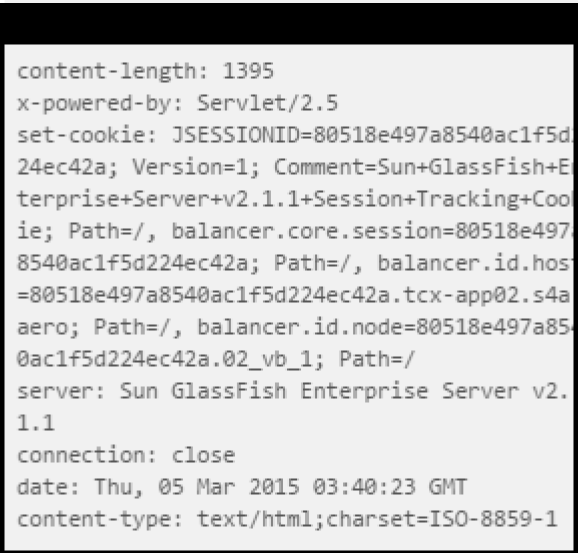
Iot Search Engine

DEMO

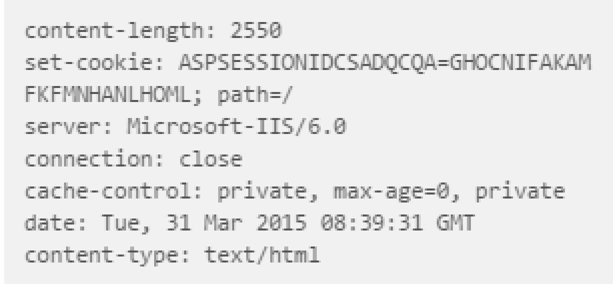
Fingerprints too many fingerprints



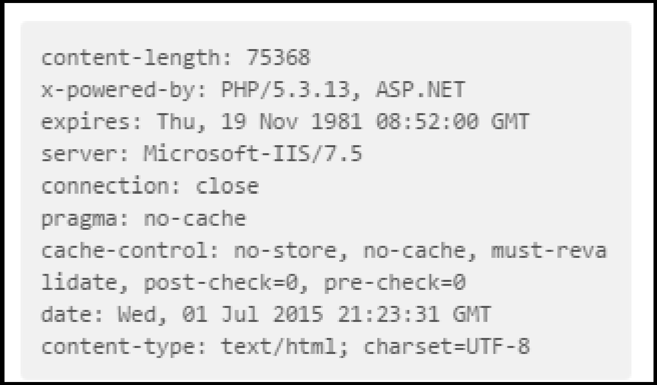
```
content-length: 7701
content-language: en-US
set-cookie: JSESSIONID=515E06DF824C97503EF7
A9698E8BEDE; Path=/, localeCookie=en_US; Do
ain=mypepsico.com; Path=/, BIGipServerrdcwe
app.corp.pep.pvt_sso=423662237.36895.0000; 
ath=/, BIGipServerrdcweb.corp.pep.pvt_sso=4
5381661.29991.0000; path=/, BIGipServerrdcs
o.mypepsico.com=73631948.29991.0000; path=/
expires: Sat, 25 Dec 1993 00:00:01 GMT
server: Apache-Coyote/1.1
connection: close
pragma: no-cache
cache-control: no-cache, no-store, no-cache
 no-store, max-age=0, no-store
date: Sat, 04 Jul 2015 03:39:04 GMT
content-type: text/html;charset=UTF-8
```



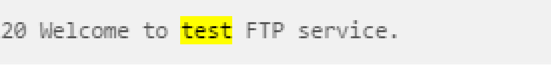
```
content-length: 1395
x-powered-by: Servlet/2.5
set-cookie: JSESSIONID=80518e497a8540ac1f5d
24ec42a; Version=1; Comment=Sun+GlassFish+E
terprise+Server+v2.1.1+Session+Tracking+Coo
ie; Path=/, balancer.core.session=80518e497
8540ac1f5d224ec42a; Path=/, balancer.id.hos
=80518e497a8540ac1f5d224ec42a.tcx-app02.s4a
aero; Path=/, balancer.id.node=80518e497a85
0ac1f5d224ec42a.02_vb_1; Path=/
server: Sun GlassFish Enterprise Server v2.
1.1
connection: close
date: Thu, 05 Mar 2015 03:40:23 GMT
content-type: text/html;charset=ISO-8859-1
```



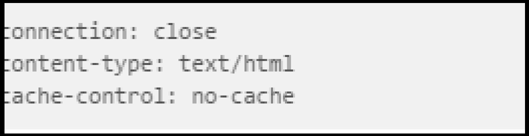
```
content-length: 2550
set-cookie: ASPSESSIONIDCSADQCQA=GHOCNIFAKAM
FKFMNHANLHOML; path=/
server: Microsoft-IIS/6.0
connection: close
cache-control: private, max-age=0, private
date: Tue, 31 Mar 2015 08:39:31 GMT
content-type: text/html
```



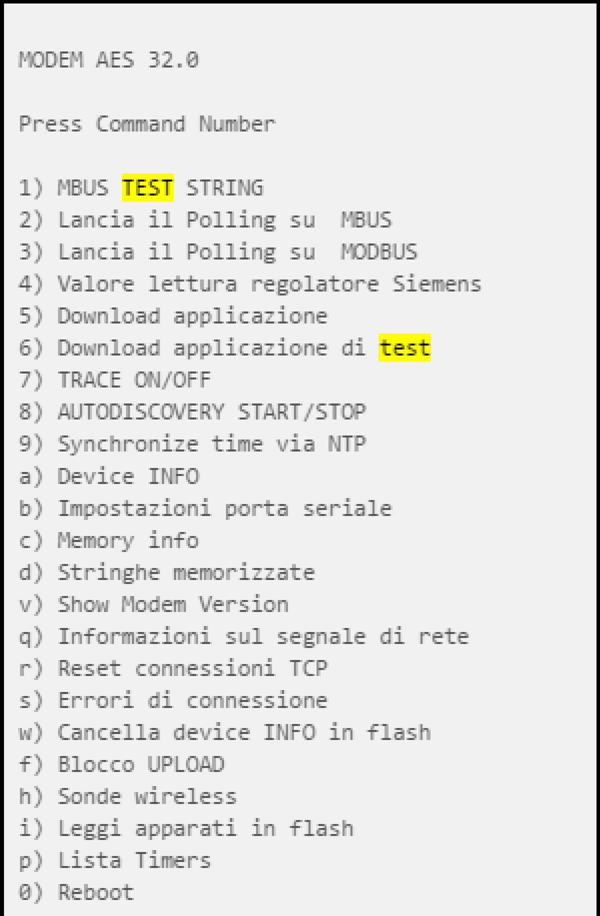
```
content-length: 75368
x-powered-by: PHP/5.3.13, ASP.NET
expires: Thu, 19 Nov 1981 08:52:00 GMT
server: Microsoft-IIS/7.5
connection: close
pragma: no-cache
cache-control: no-store, no-cache, must-reva
lidate, post-check=0, pre-check=0
date: Wed, 01 Jul 2015 21:23:31 GMT
content-type: text/html; charset=UTF-8
```



```
20 Welcome to test FTP service.
```

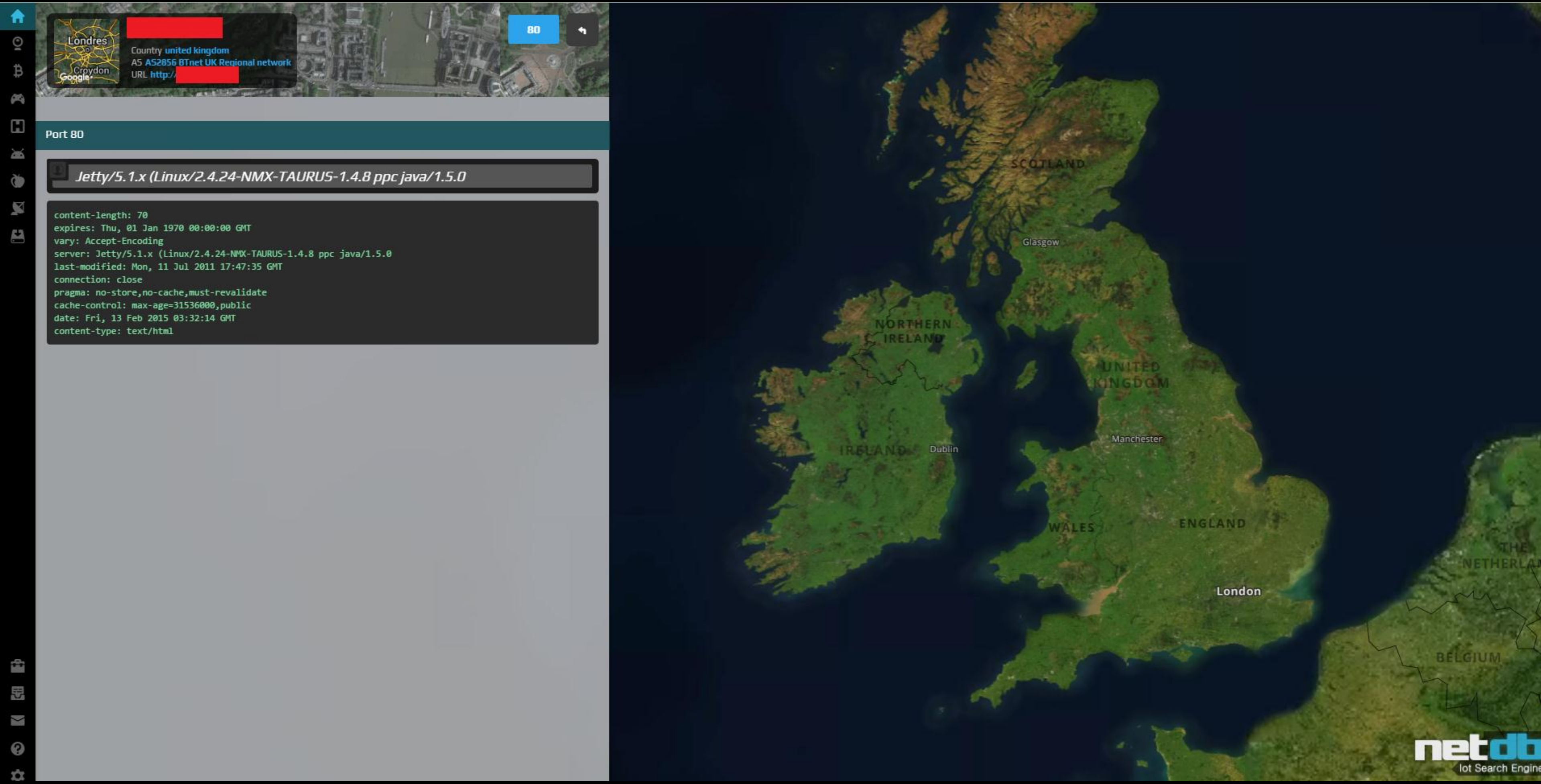


```
onnection: close
ontent-type: text/html
ache-control: no-cache
```



```
MODEM AES 32.0

Press Command Number

1) MBUS TEST STRING
2) Lancia il Polling su  MBUS
3) Lancia il Polling su  MODBUS
4) Valore lettura regolatore Siemens
5) Download applicazione
6) Download applicazione di test
7) TRACE ON/OFF
8) AUTODISCOVERY START/STOP
9) Synchronize time via NTP
a) Device INFO
b) Impostazioni porta seriale
c) Memory info
d) Stringhe memorizzate
v) Show Modem Version
q) Informazioni sul segnale di rete
r) Reset connessioni TCP
s) Errori di connessione
w) Cancella device INFO in flash
f) Blocco UPLOAD
h) Sonde wireless
i) Leggi apparati in flash
p) Lista Timers
0) Reboot
```

For some strange reason you find a unique fingerprint in millions…



[redacted]

Country united kingdom
AS AS2856 BTnet UK Regional network
URL http:/[redacted]

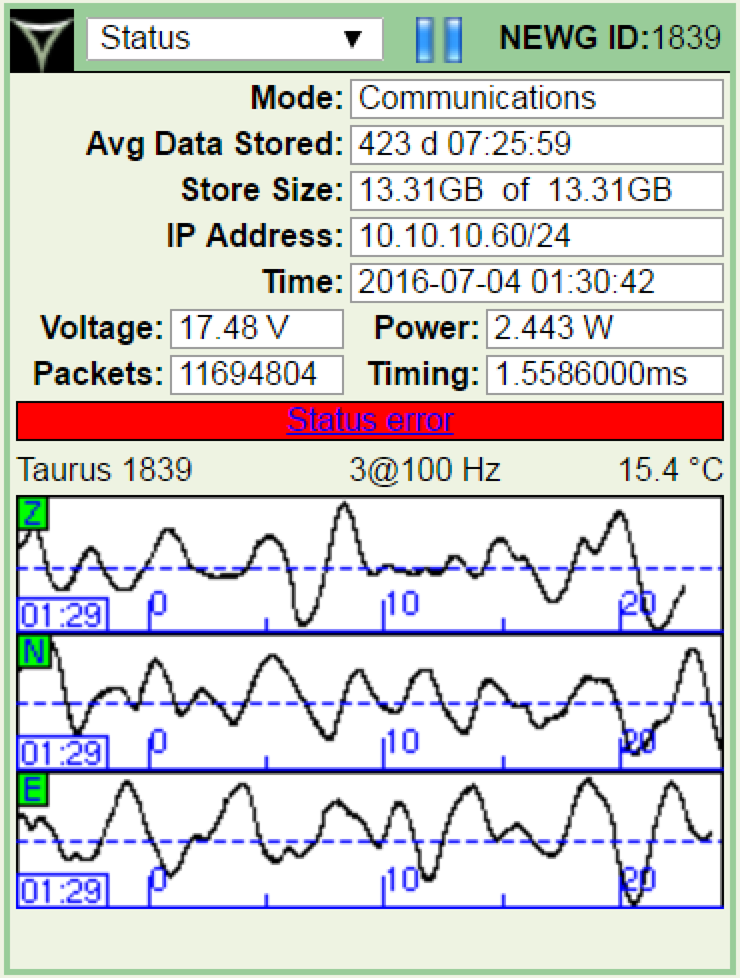
Port 80

Jetty/5.1.x (Linux/2.4.24-NMX-TAURUS-1.4.8 ppc java/1.5.0

```
content-length: 70
expires: Thu, 01 Jan 1970 00:00:00 GMT
vary: Accept-Encoding
server: Jetty/5.1.x (Linux/2.4.24-NMX-TAURUS-1.4.8 ppc java/1.5.0
last-modified: Mon, 11 Jul 2011 17:47:35 GMT
connection: close
pragma: no-store,no-cache,must-revalidate
cache-control: max-age=31536000,public
date: Fri, 13 Feb 2015 03:32:14 GMT
content-type: text/html
```

DEMO

So.. WTF is TAURUS ???? Let´s connect to that shit NOW!



Mode: Communications

Avg Data Stored: 423 d 07:25:59

Store Size: 13.31GB of 13.31GB

IP Address: 10.10.10.60/24

Time: 2016-07-04 01:30:42

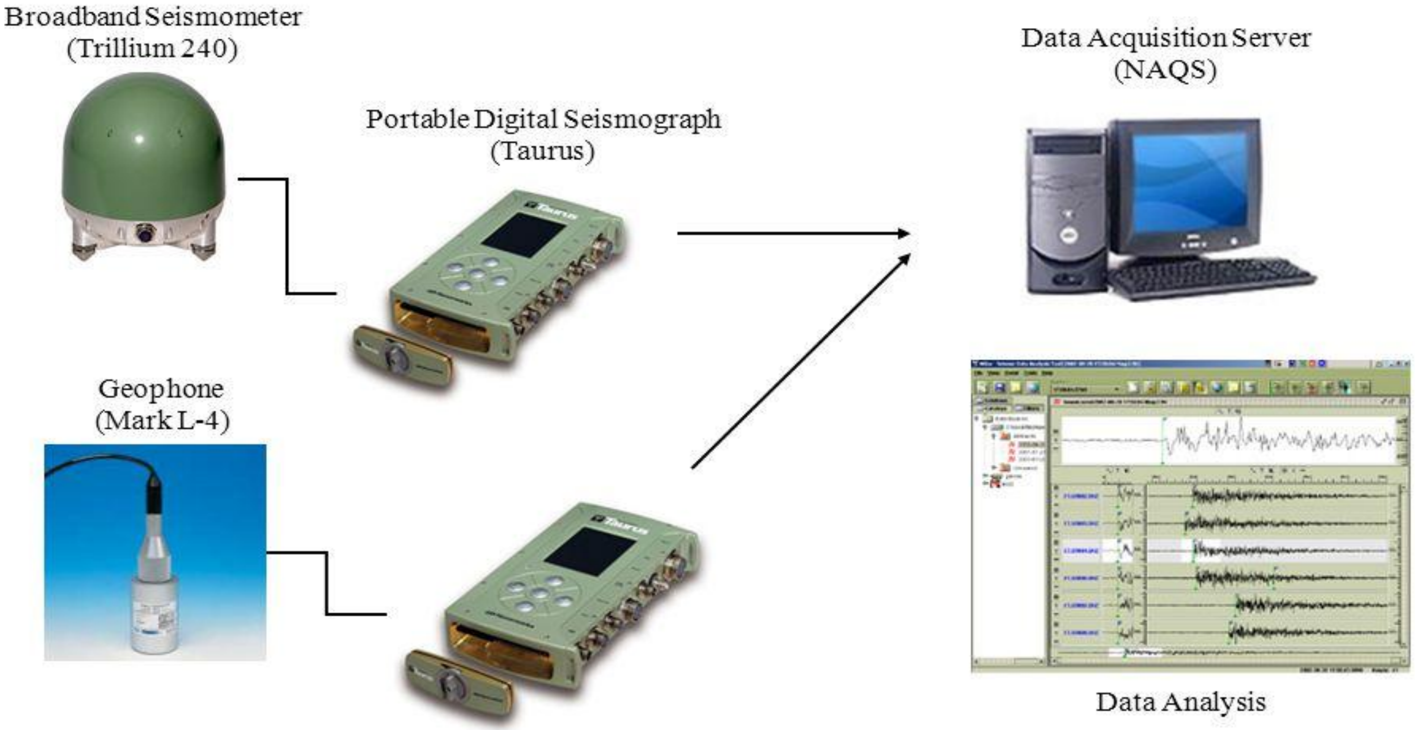
Voltage: 17.48 V Power: 2.443 W

Packets: 11694804 Timing: 1.5586000ms

Status error

Taurus 1839 3@100 Hz 15.4 °C

What is a Taurus?



Broadband Seismometer
(Trillium 240)

Geophone
(Mark L-4)

Portable Digital Seismograph
(Taurus)

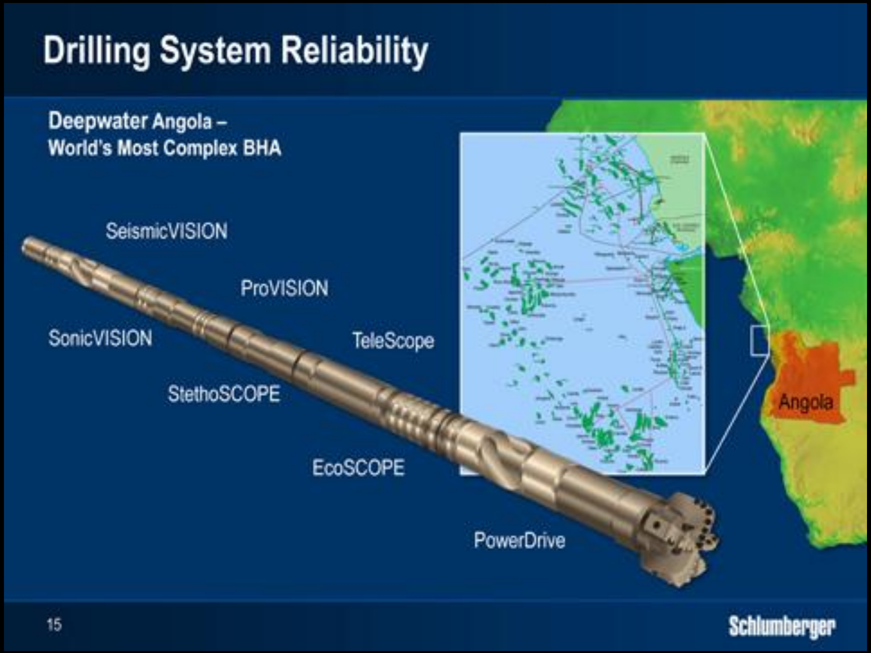
Data Acquisition Server
(NAQS)

Data Analysis

Seismometers are instruments that measure motion of the ground, including those of seismic waves generated by earthquakes, volcanic eruptions, and other seismic sources. Records of seismic waves allow seismologists to map the interior of the Earth, and locate and measure the size of these different sources.

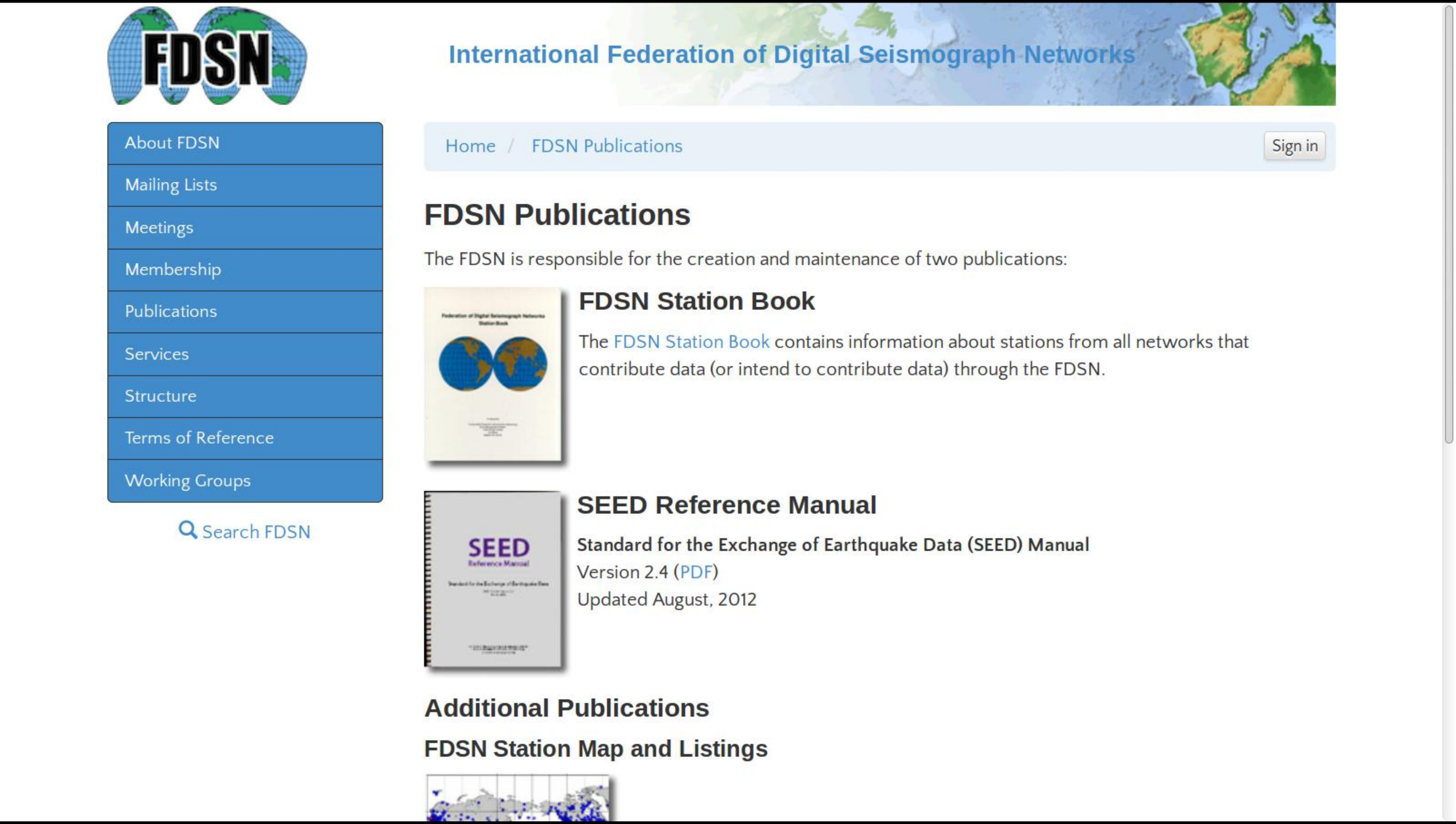
Wikipedia

Common aplications:
-Earthquake detection
-Geophysics, geothermal development
-Structural analysis
-Mine safety
-Fracking / Drilling



Drilling System Reliability

Deepwater Angola –
World's Most Complex BHA



International Federation of Digital Seismograph Networks

FDSN Publications

The FDSN is responsible for the creation and maintenance of two publications:

FDSN Station Book

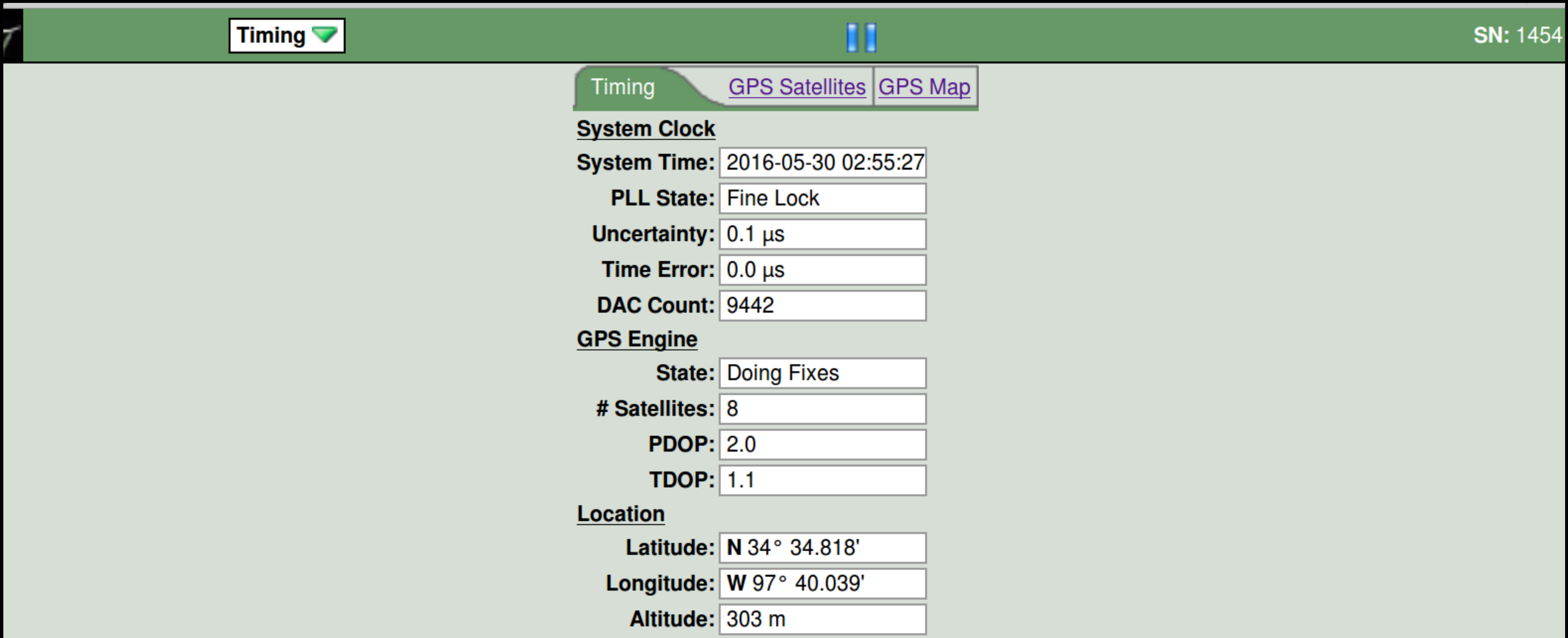
The FDSN Station Book contains information about stations from all networks that contribute data (or intend to contribute data) through the FDSN.

SEED Reference Manual

Standard for the Exchange of Earthquake Data (SEED) Manual
Version 2.4 (PDF)
Updated August, 2012

Additional Publications

FDSN Station Map and Listings



System Clock

System Time: 2016-05-30 02:55:27

PLL State: Fine Lock

Uncertainty: 0.1 μs

Time Error: 0.0 μs

DAC Count: 9442

GPS Engine

State: Doing Fixes

Satellites: 8

PDOP: 2.0

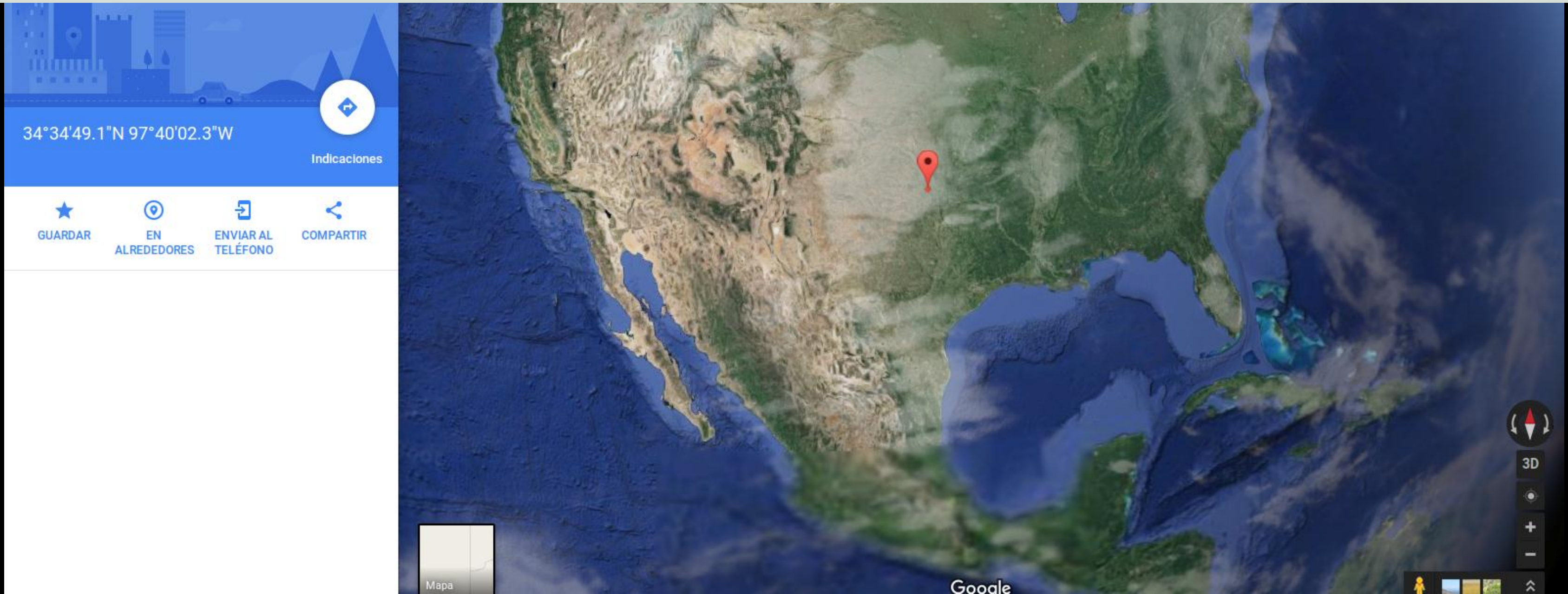
TDOP: 1.1

Location

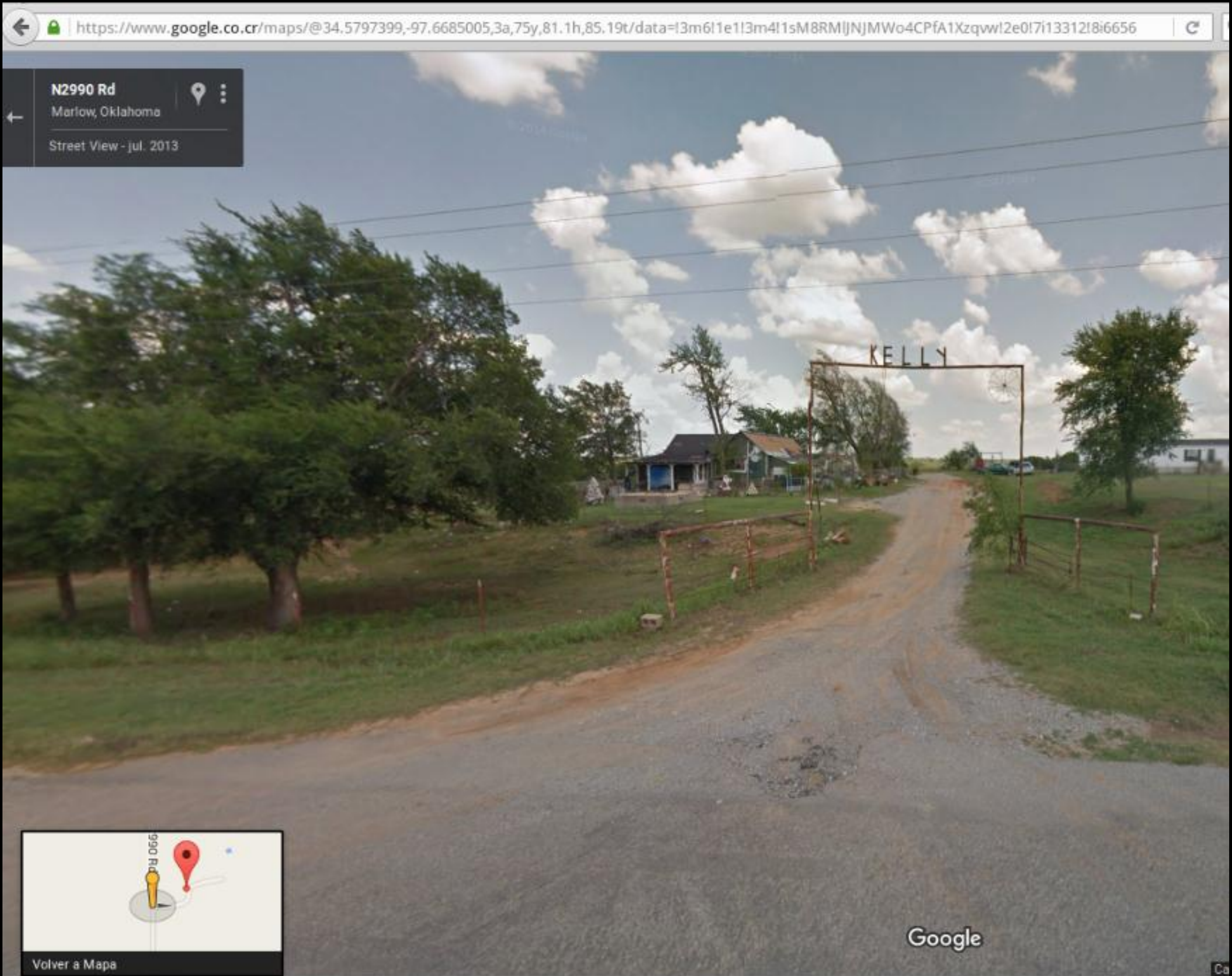
Latitude: N 34° 34.818'

Longitude: W 97° 40.039'

Altitude: 303 m



34°34'49.1"N 97°40'02.3"W



https://www.google.co.cr/maps/@34.5797399,-97.6685005,3a,75y,81.1h,85.19t/data=!3m6!1e1!3m4!1sM8RMIJNJMWo4CPfA1Xzqvw!2e0!7i13312!8i6656

N2990 Rd
Marlow, Oklahoma

Street View - jul. 2013

GPS REAL DATA LOCATION DEMO

Ocean bottom seismograph

Impact

-No one else has ever done a research about security of this devices or networks before

-Remote Denial of service

-Remote management

-Several Bugs

-Sabotage seismological country’s network

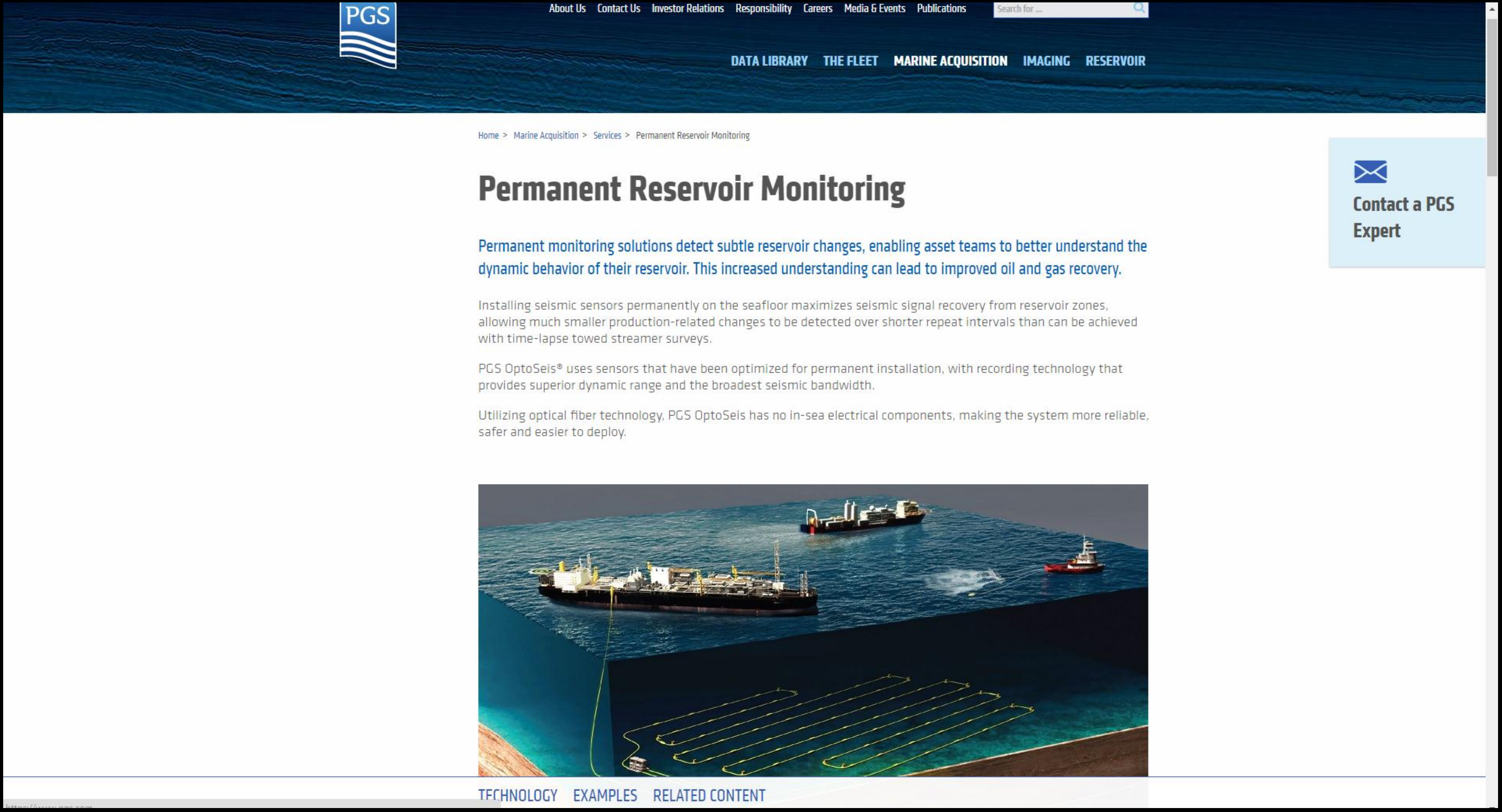
-Economic impact for Oil and Gas research for specific company

-Drug trafficking submarine detection

-Military

-Unknow

This increased understanding can lead to improved oil and gas recovery.



Permanent Reservoir Monitoring

Permanent monitoring solutions detect subtle reservoir changes, enabling asset teams to better understand the dynamic behavior of their reservoir. This increased understanding can lead to improved oil and gas recovery.

Installing seismic sensors permanently on the seafloor maximizes seismic signal recovery from reservoir zones, allowing much smaller production-related changes to be detected over shorter repeat intervals than can be achieved with time-lapse towed streamer surveys.

PGS OptoSeis® uses sensors that have been optimized for permanent installation, with recording technology that provides superior dynamic range and the broadest seismic bandwidth.

Utilizing optical fiber technology, PGS OptoSeis has no in-sea electrical components, making the system more reliable, safer and easier to deploy.

Vendors found

Nanometrics INC.
SEISMOLOGICAL INSTRUMENTS
The world leader in seismological instruments & networks

GURALP SYSTEMS

OSOP Distributes

Nanometrics INC.

Jewell Instruments

Met One Instruments

Xeos Technologies Inc.

IESE Institute of Earth Science and Engineering Aotearoa

gempa

sara

Instrumentation

in

Earthquake Seismology

Jens Havskov, Institute of Solid Earth Physics
University of Bergen
Norway

and

Gerardo Alguacil
Instituto Andaluz de Geofisica
University of Granada
Spain

Chapter 1

Introduction

Seismology would be a very different science without instruments. The real big advances in seismology happened from around 1900 and onwards and was mainly due to advancement in making more sensitive seismographs and devising timing systems, so that earthquakes could be located. Later, the importance accurate measurement of the true ground motion became evident for studying seismic wave attenuation, and the Richter magnitude scale depends on being able to calculate the ground displacement from our recorded seismogram (Figure 1.1).

The ability to do earthquake location and calculate magnitude immediately brings us into two basic requirement of instrumentation: keeping accurate time and determining the frequency dependent relation between the measurement and the real ground motion.

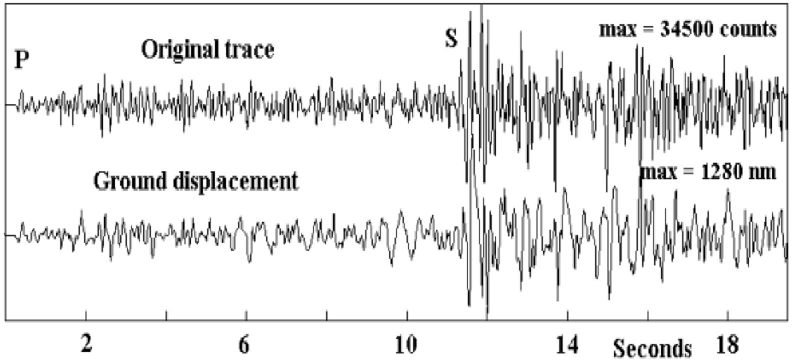


Figure 1.1. The top trace shows the original digitally recorded signal from a magnitude 3 earthquake recorded at a distance of 120 km. The maximum amplitude is just a number (called counts). The bottom trace shows the signal converted to true ground displacement in nm from which the magnitude can be calculated. The distance to the earthquake is proportional to the arrival time difference between the S-wave and P-wave, so having 3 stations makes it possible to locate the earthquake. The seismometer is a 1 Hz sensor with velocity output.

The poles and zeros of the transfer function are most easily determined from Eq. (5.18). W read immediately that a triple zero is present at $s = 0$. Each factor $s^2 + 2s\omega_0 h + \omega_0^2$ in the denominator has the zeros

$$s_0 = \omega_0(-h \pm j\sqrt{1-h^2}) \qquad \text{for } h < 1$$

$$s_0 = \omega_0(-h \pm \sqrt{h^2-1}) \qquad \text{for } h \geq 1$$

so the poles of $H_d(s)$ in the complex s plane are (Fig. 5.2):

$$s_1 = \omega_s(-h_s + j\sqrt{1-h_s^2}) \quad = -0.2513 + 0.3351j \quad [\sec^{-1}]$$

$$s_2 = \omega_s(-h_s - j\sqrt{1-h_s^2}) \quad = -0.2513 - 0.3351j \quad [\sec^{-1}]$$

$$s_3 = \omega_g(-h_g + j\sqrt{1-h_g^2}) \quad = -0.0628 + 0.0304j \quad [\sec^{-1}]$$

$$s_4 = \omega_g(-h_g - j\sqrt{1-h_g^2}) \quad = -0.0628 - 0.0304j \quad [\sec^{-1}]$$

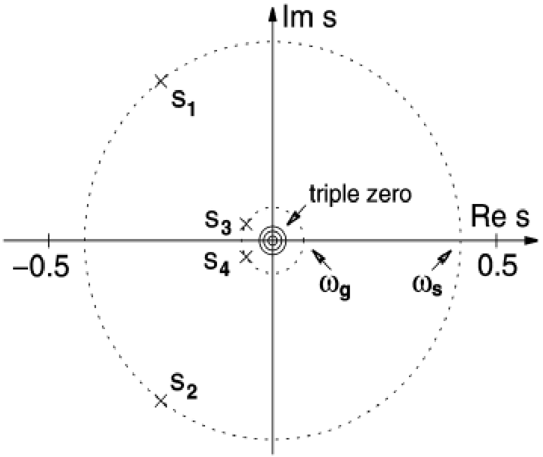


Fig. 5.2 Position of the poles of the WWSSN-LP system in the complex s plane

In order to reconstruct $H_d(s)$ from its poles and zeros and the gain factor, we write

$$H_d(s) = \frac{Cs^3}{(s-s_1)(s-s_2)(s-s_3)(s-s_4)}.$$

5.3.3 Sensitivity of horizontal seismometers to tilt

We have already seen (Eq. (5.25)) that a seismic acceleration of the ground has the same effect on the seismic mass as an external force. The largest such force is gravity. It is normally cancelled by the suspension, but when the seismometer is tilted, the projection of the vector of gravity onto the axis of sensitivity changes, producing a force that is in most cases undistinguishable from a seismic signal (Fig. 5.11). Undesired tilt at seismic frequencies may be caused by moving or variable surface loads such as cars, people, and atmospheric pressure. The resulting disturbances are a second-order effect in well-adjusted vertical seismometers but otherwise a first-order effect (see Rodgers, 1968; Rodgers, 1969). This explains why horizontal long-period seismic traces are always noisier than vertical ones. A short, impulsive tilt excursion is equivalent to a step-like change of ground velocity and therefore will cause a long-period transient in a horizontal broadband seismometer. For periodic signals, the apparent horizontal displacement associated with a given tilt increases with the square of the period (see also 5.8.1).

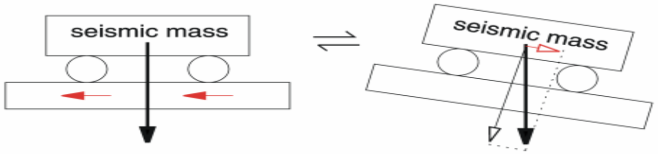


Fig. 5.11 The relative motion of the seismic mass is the same when the ground is accelerated to the left as when it is tilted to the right.

Fig. 5.12 illustrates the effect of barometrically induced ground tilt. Let us assume that the ground is vertically deformed by as little as ± 1 µm over a distance of 3 km, and that this deformation oscillates with a period of 10 minutes. A simple calculation then shows that seismometers A and C see a vertical acceleration of $\pm 10^{-10}$ m/s² while B sees a horizontal acceleration of $\pm 10^{-8}$ m/s². The horizontal noise is thus 100 times larger than the vertical one. In absolute terms, even the vertical acceleration is by a factor of four above the minimum ground noise in one octave, as specified by the USGS Low Noise Model (see 5.5.1)

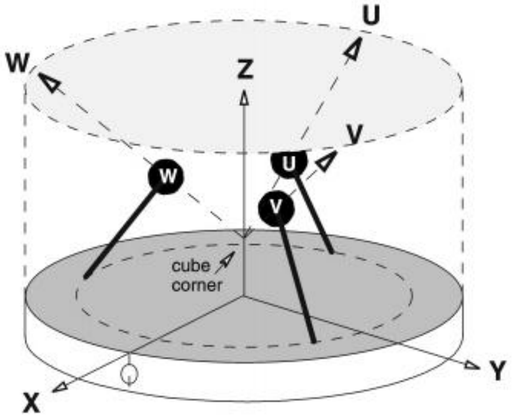


Fig. 5.13 The homogeneous triaxial geometry of the STS2 seismometer

Taurus

Taurus
Ethernet
SOH
Nanometrics
Taurus
Nanometrics

Internals

Linux based OS
Remote management
SSH TELNET FTP Web Server
GPS
Ocean bottom
Battery /Solar panels

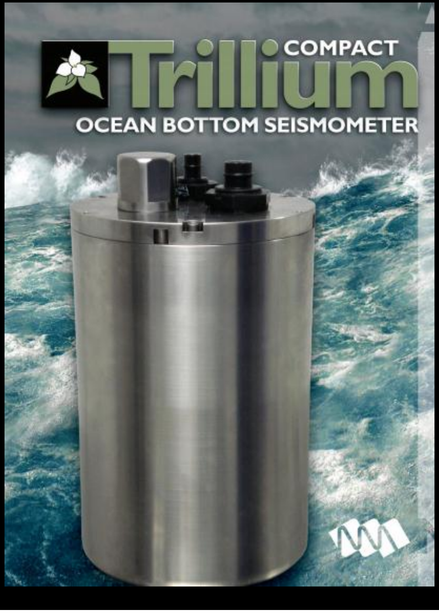


Figure 10-1 Top view

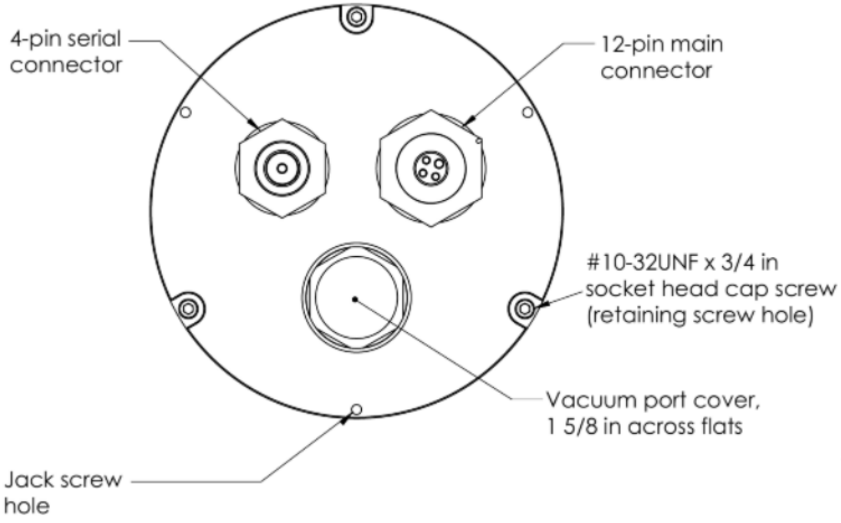
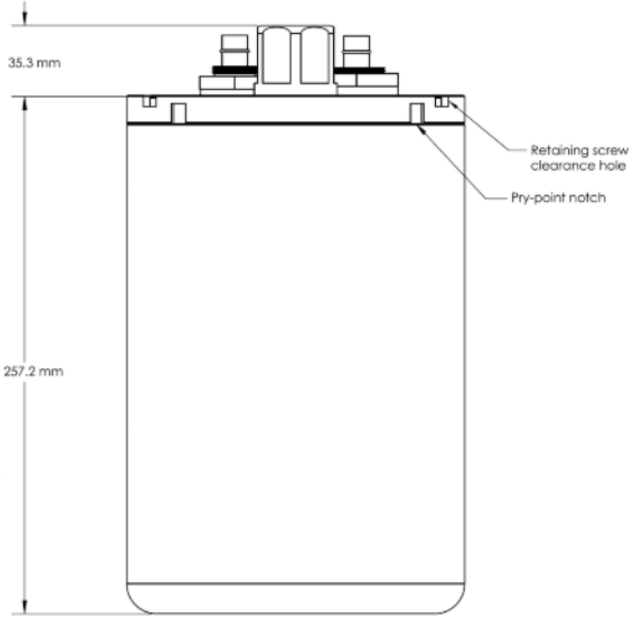
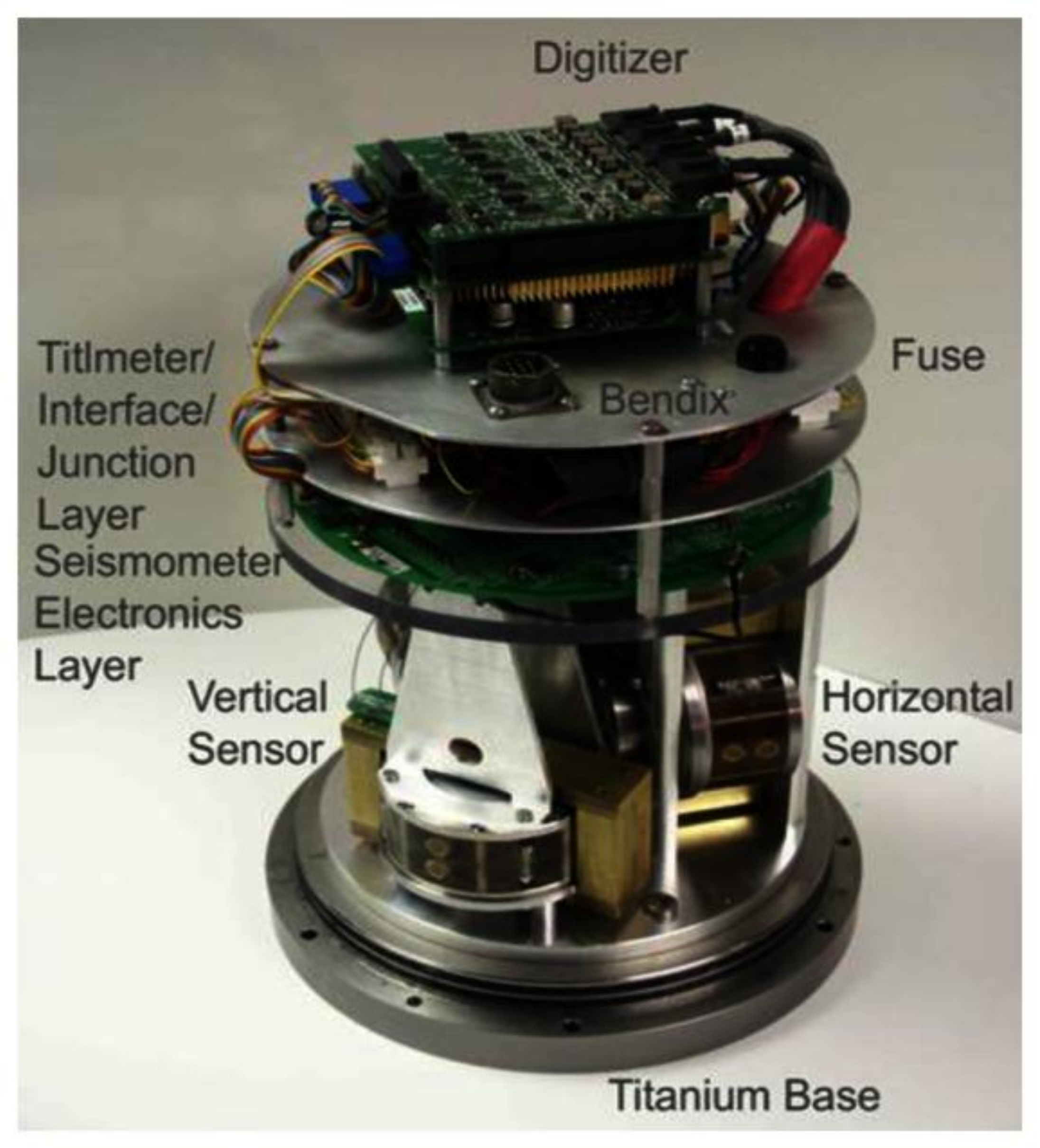
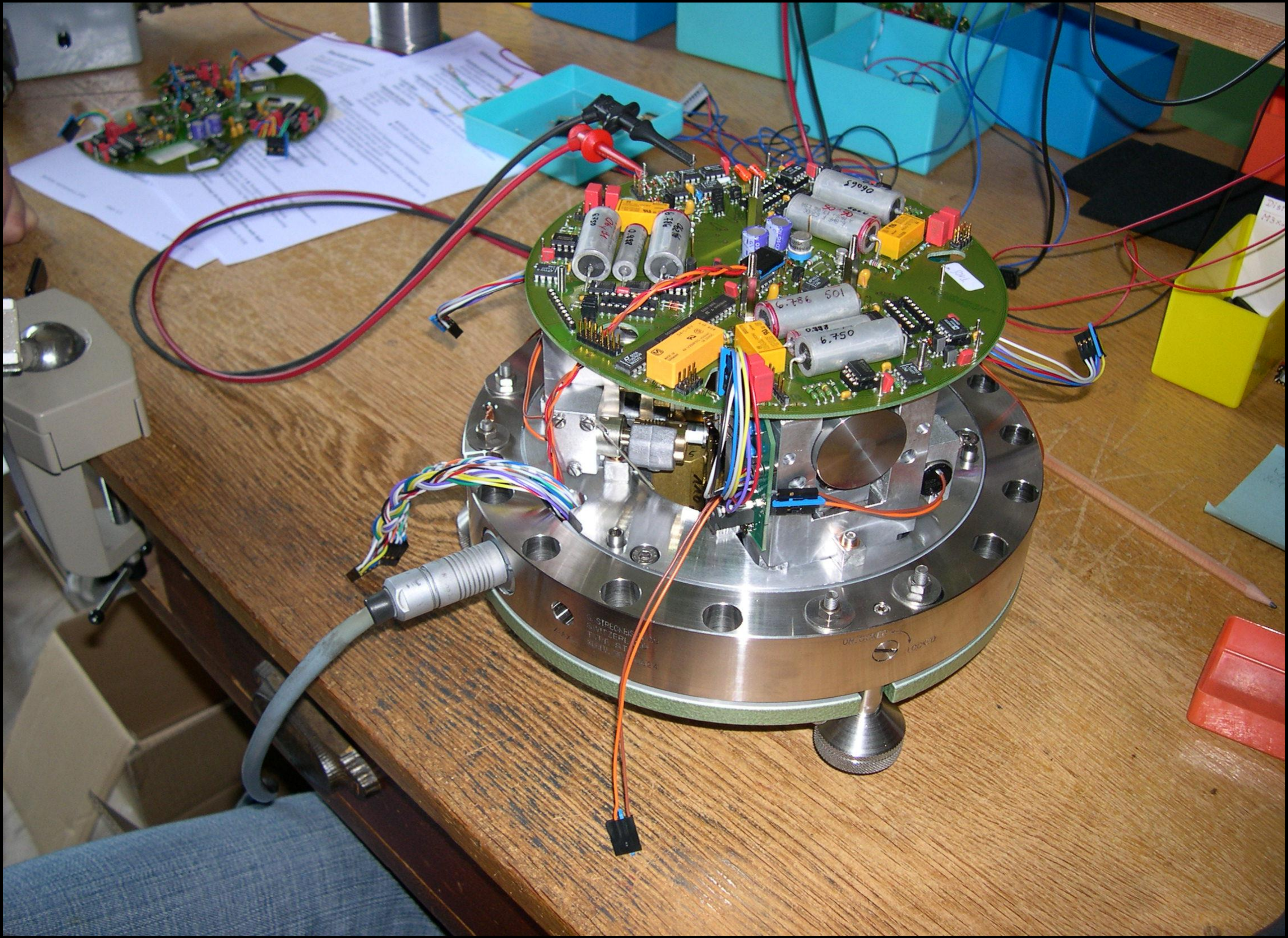

4-pin serial connector
12-pin main connector
#10-32UNF x 3/4 in socket head cap screw (retaining screw hole)
Vacuum port cover, 1 5/8 in across flats
Jack screw hole

Figure 10-2 Side view



Sophisticated




6.786 501
6.750
UNLOCKED
LOCKED

Deployment options

The Taurus may be deployed as either a stand-alone data recorder or as a network component.

For stand-alone recording where network access is not required, typically you would configure the Taurus to run in Buffered mode. It consumes less power in this mode as the Controller only runs when the Taurus is recording buffered data to the Store. ⍰

For networked operation you must configure the Taurus to run in Communications mode and configure the appropriate network options. In this mode, the Controller is running continuously. It consumes more power than Buffered mode but allows continuous access via an IP connection.

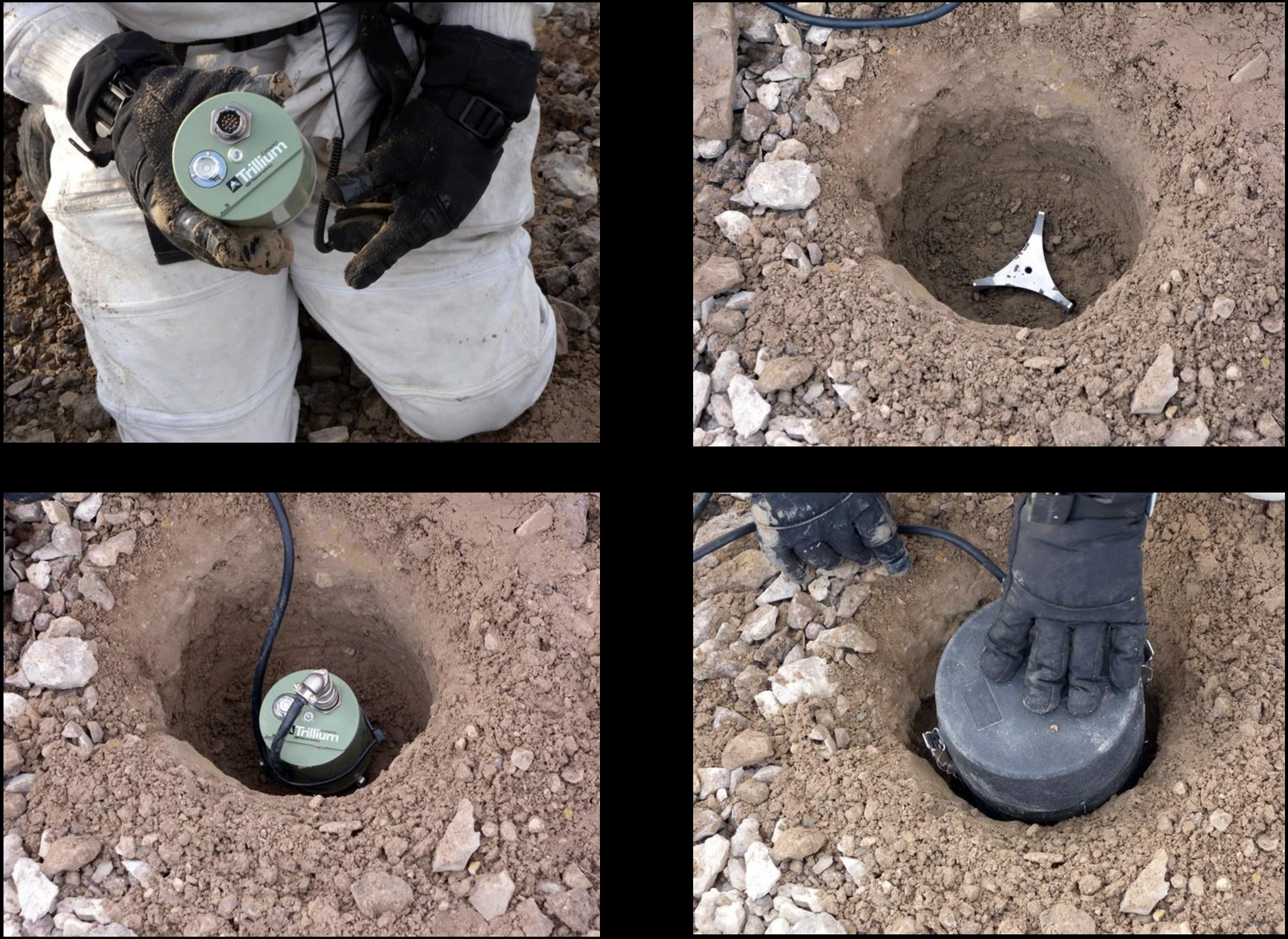
You can stream time-series data from a Taurus to a central acquisition server, for example to write the data to NAQS ringbuffers. To stream Taurus data to NAQS, the NpToNmxp utility must be running on the NAQS server

• Stream NP Packets – Set Taurus to stream data to the specified destination; enabled , not enabled . Factory default is not enabled. • IP Address – The address of the streaming destination (for example, a NAQS server); a valid IP address in dotted decimal format

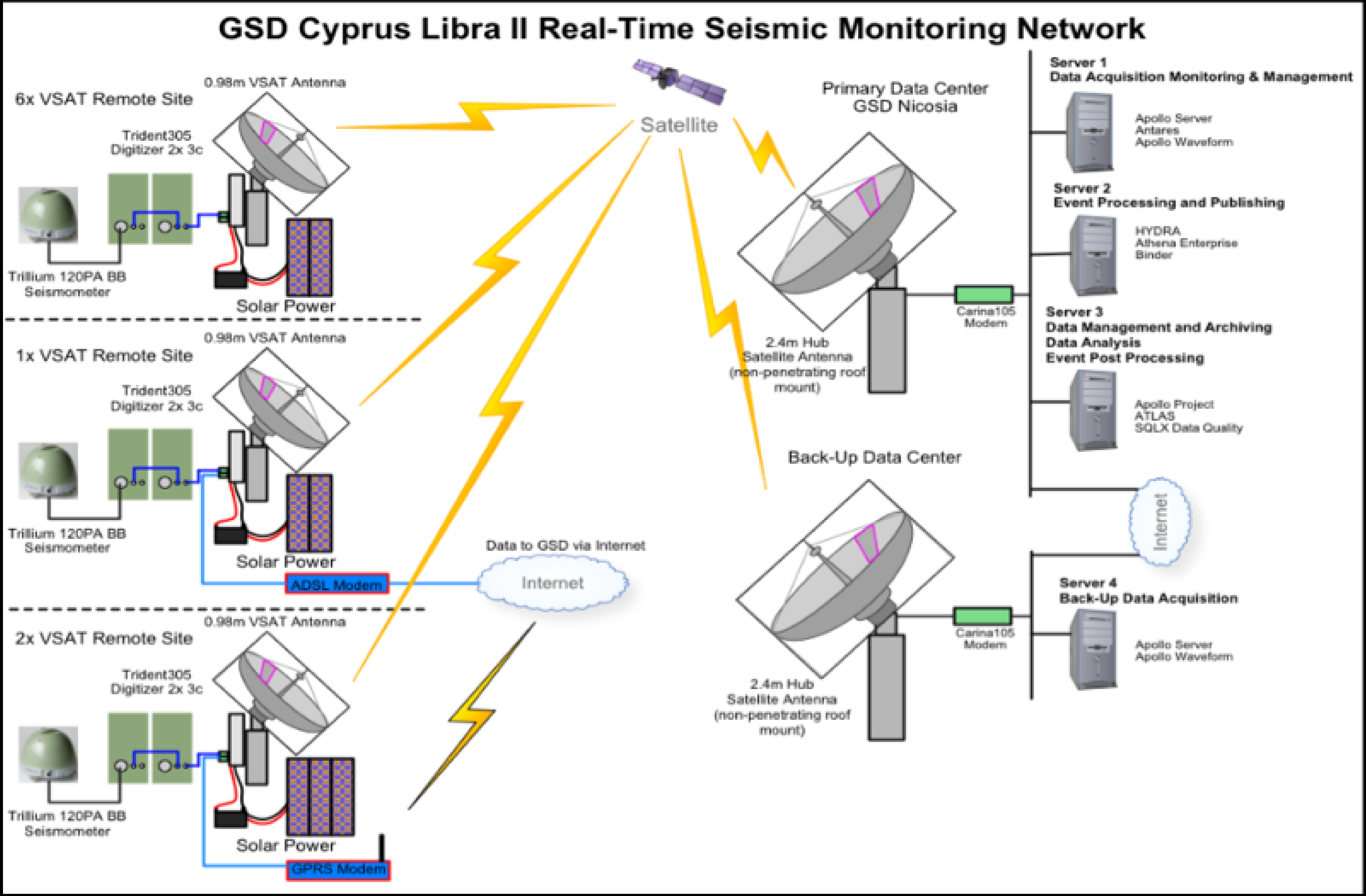
Applications software Nanometrics Apollo acquisition server with web interface

Geophysicists depend on seismometers to monitor earthquakes generated by the motion of the tectonic plates that form the Earth’s crust. In order to function, the instruments need to be leveled prior to operation. That’s easy enough for a device deployed on dry land, but when it comes to seismometers placed on the ocean floor thousands of feet below the surface, the process gets a bit more challenging. To solve it, Nanometrics Inc. (Kanata, Ontario) combines sophisticated gimbals and microprocessors, along with ultra-reliable, efficient motors from MICROMO (Clearwater, FL).

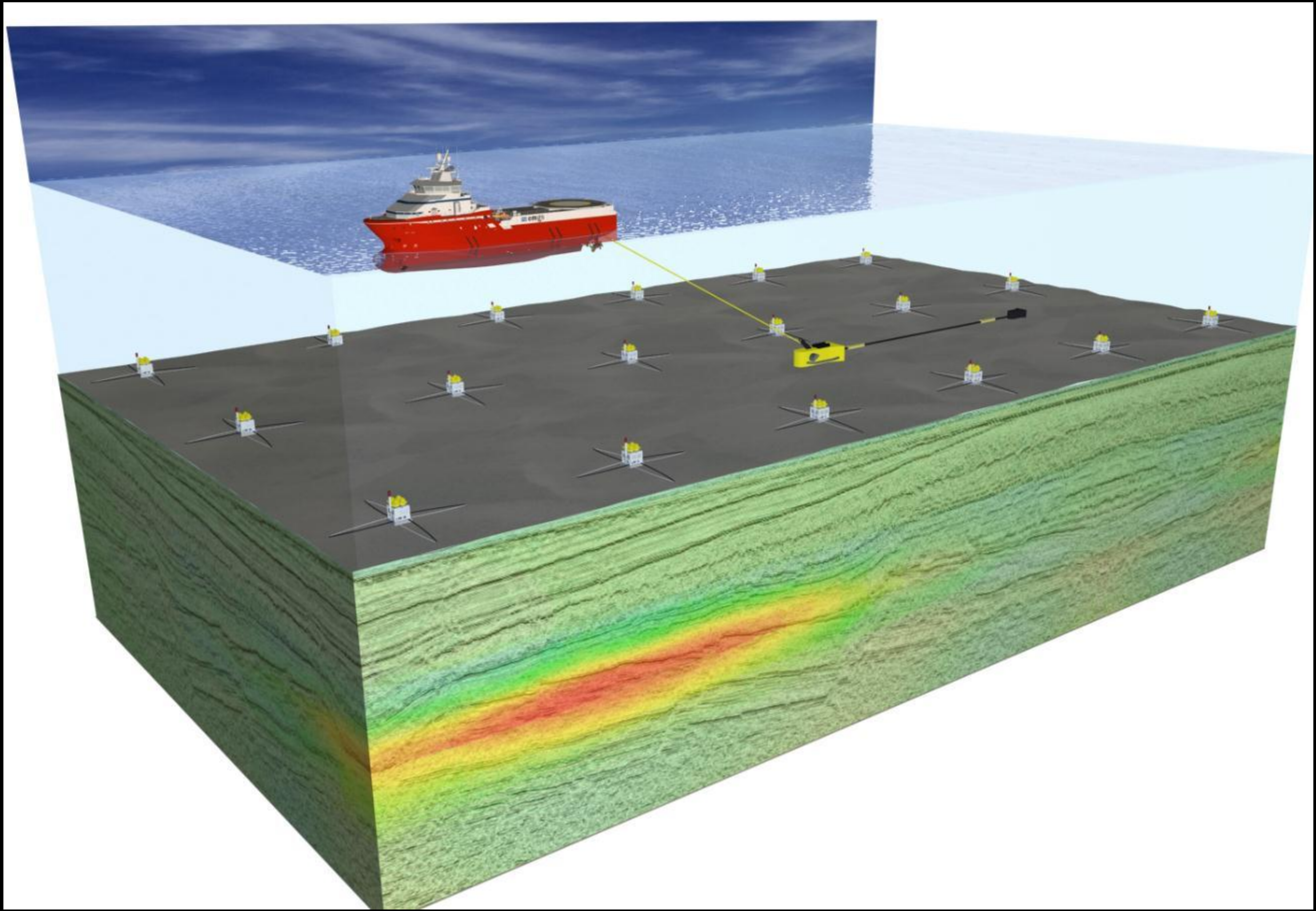
Sensor Earth Deployment



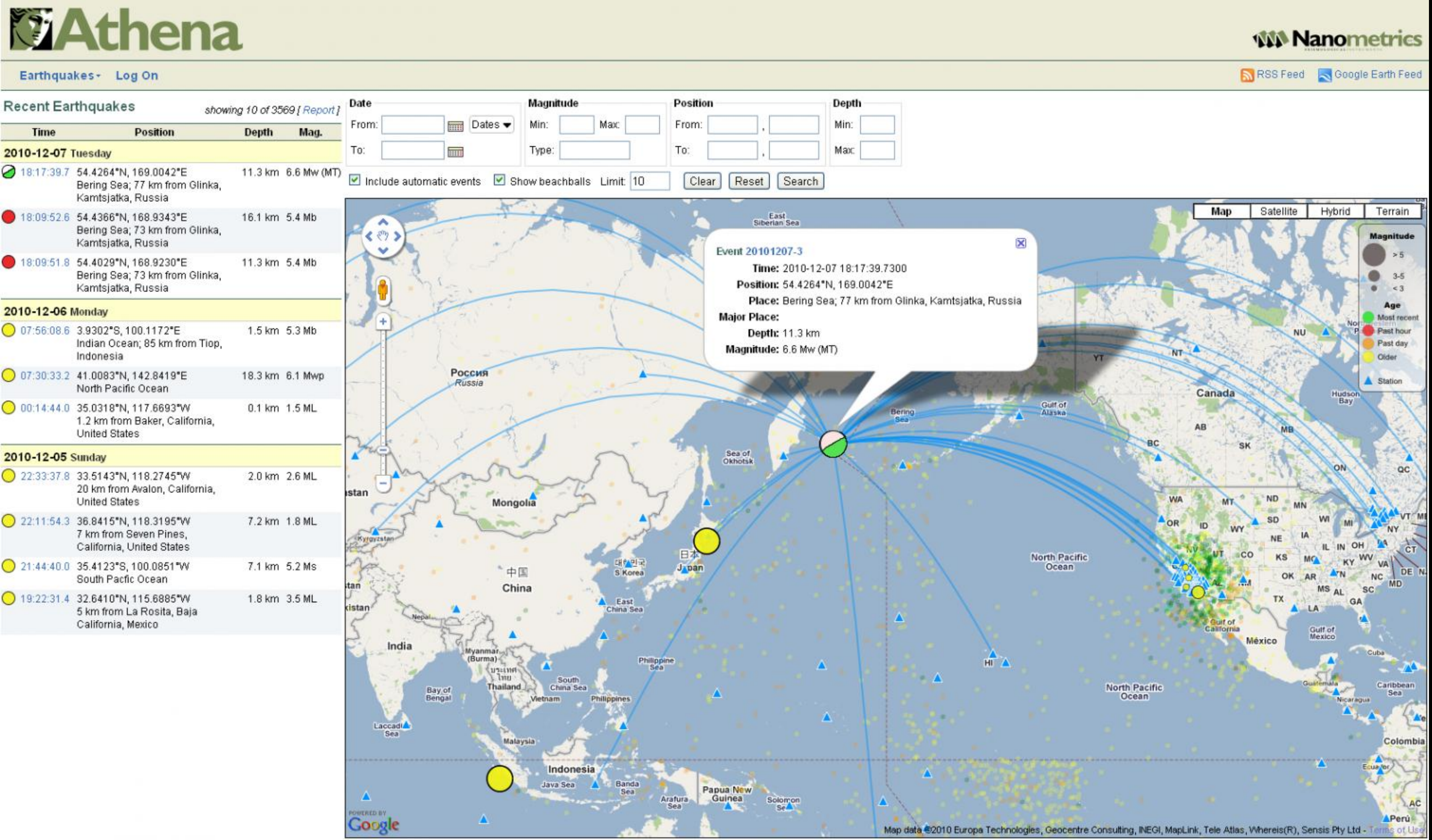
The seismological network



Ocean Bottom seismic network - Autonomous Underwater Vehicles (AUVs)



Athena: Event Cataloging and Notification Management



Athena

Nanometrics

Earthquakes▾ Log On

RSS Feed Google Earth Feed

Recent Earthquakes

showing 10 of 3569 [Report]

Time	Position	Depth	Mag.
2010-12-07 Tuesday			
18:17:39.7	54.4264°N, 169.0042°E Bering Sea; 77 km from Glinka, Kamtsjatka, Russia	11.3 km	6.6 Mw (MT)
18:09:52.6	54.4366°N, 168.9343°E Bering Sea; 73 km from Glinka, Kamtsjatka, Russia	16.1 km	5.4 Mb
18:09:51.8	54.4029°N, 168.9230°E Bering Sea; 73 km from Glinka, Kamtsjatka, Russia	11.3 km	5.4 Mb
2010-12-06 Monday			
07:56:08.6	3.9302°S, 100.1172°E Indian Ocean; 85 km from Tiop, Indonesia	1.5 km	5.3 Mb
07:30:33.2	41.0083°N, 142.8419°E North Pacific Ocean	18.3 km	6.1 Mwp
00:14:44.0	35.0318°N, 117.6693°W 1.2 km from Baker, California, United States	0.1 km	1.5 ML
2010-12-05 Sunday			
22:33:37.8	33.5143°N, 118.2745°W 20 km from Avalon, California, United States	2.0 km	2.6 ML
22:11:54.3	36.8415°N, 118.3195°W 7 km from Seven Pines, California, United States	7.2 km	1.8 ML
21:44:40.0	35.4123°S, 100.0851°W South Pacfic Ocean	7.1 km	5.2 Ms
19:22:31.4	32.6410°N, 115.6885°W 5 km from La Rosita, Baja California, Mexico	1.8 km	3.5 ML

Date From: To: Dates ▾

Magnitude Min: Max: Type:

Position From: , To: ,

Depth Min: Max:

☑ Include automatic events ☑ Show beachballs Limit: 10 Clear Reset Search

Event 20101207-3

Time: 2010-12-07 18:17:39.7300

Position: 54.4264°N, 169.0042°E

Place: Bering Sea; 77 km from Glinka, Kamtsjatka, Russia

Major Place:

Depth: 11.3 km

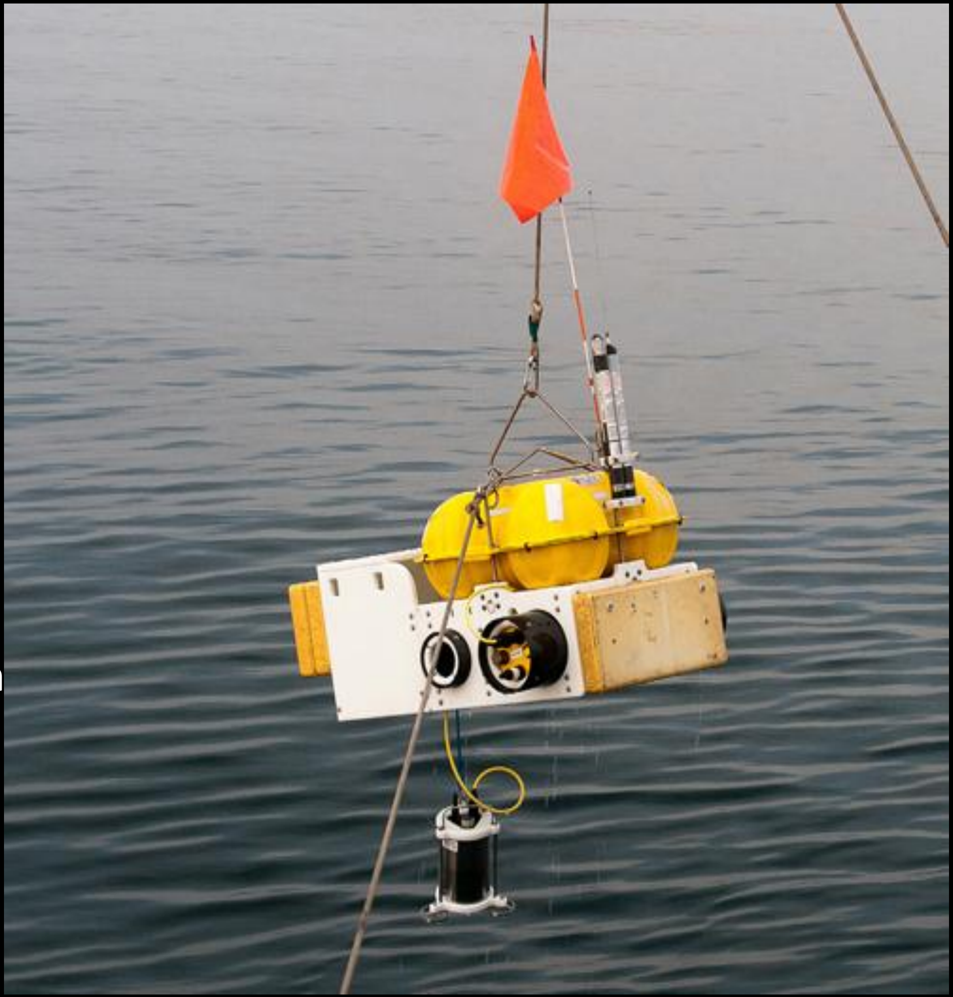
Magnitude: 6.6 Mw (MT)

Map data ©2010 Europa Technologies, Geocentre Consulting, INEGI, MapLink, Tele Atlas, Whereis(R), Sensis Pty Ltd - Terms of Use

Challenge: In order to function, the instruments need to be leveled prior to operation. Not easy when it is thousands feet on the ocean floor.

Solution: To solve it, Nanometrics Inc. (Kanata, Ontario) combines sophisticated gimbals and microprocessors, along with ultra-reliable, efficient motors from MICROMO (Clearwater, FL)

Results: A Trillium 240 was deployed at the South Pole and it operated perfectly. The turn-on temperature was -58°C (-136°F). The system temperature settled eventually to -50° C (-122°F) and stayed there for a long period of time. The motors turned on and did exactly what they were supposed to do



OCEAN BOTTOM DEPLOYMENT VIDEO DEMO

To deploy the Trillium OBS (black cylinder), users attach the seismometer to a metal sled that carries it down to the sea floor. At the end of the experiment, the transponder signal triggers the release of ballast and the instrument floats to the surface. (Courtesy of Nanometrics Inc.

Inside the Solution

Seismometers capture transient phenomenon. If an instrument malfunctions, whether it’s at the bottom of the ocean or atop a polar ice cap, that data is lost forever. “You need to be absolutely sure the sensor will perform perfectly every time,” says Jeff Potter, director of marketing at Nanometrics. “Seismometers also need to be small and consume very little power when they level themselves, and that’s where MICROMO has helped.”
The leveling mechanism integrates the following devices:
The AM1020-V-6-65, a in a 10-mm-diameter, two- phase stepper motor that provides a peak torque of 1.6 mNm. With 20 steps per revolution, and PRECIstep technology, the motor offers reliable, accurate motion, even in harsh environments.
A 10/1 planetary gearbox provides a 256:1 reduction ratio in a 10-mm-diameter package.

Vulnerability research

-We want a shell in that thing

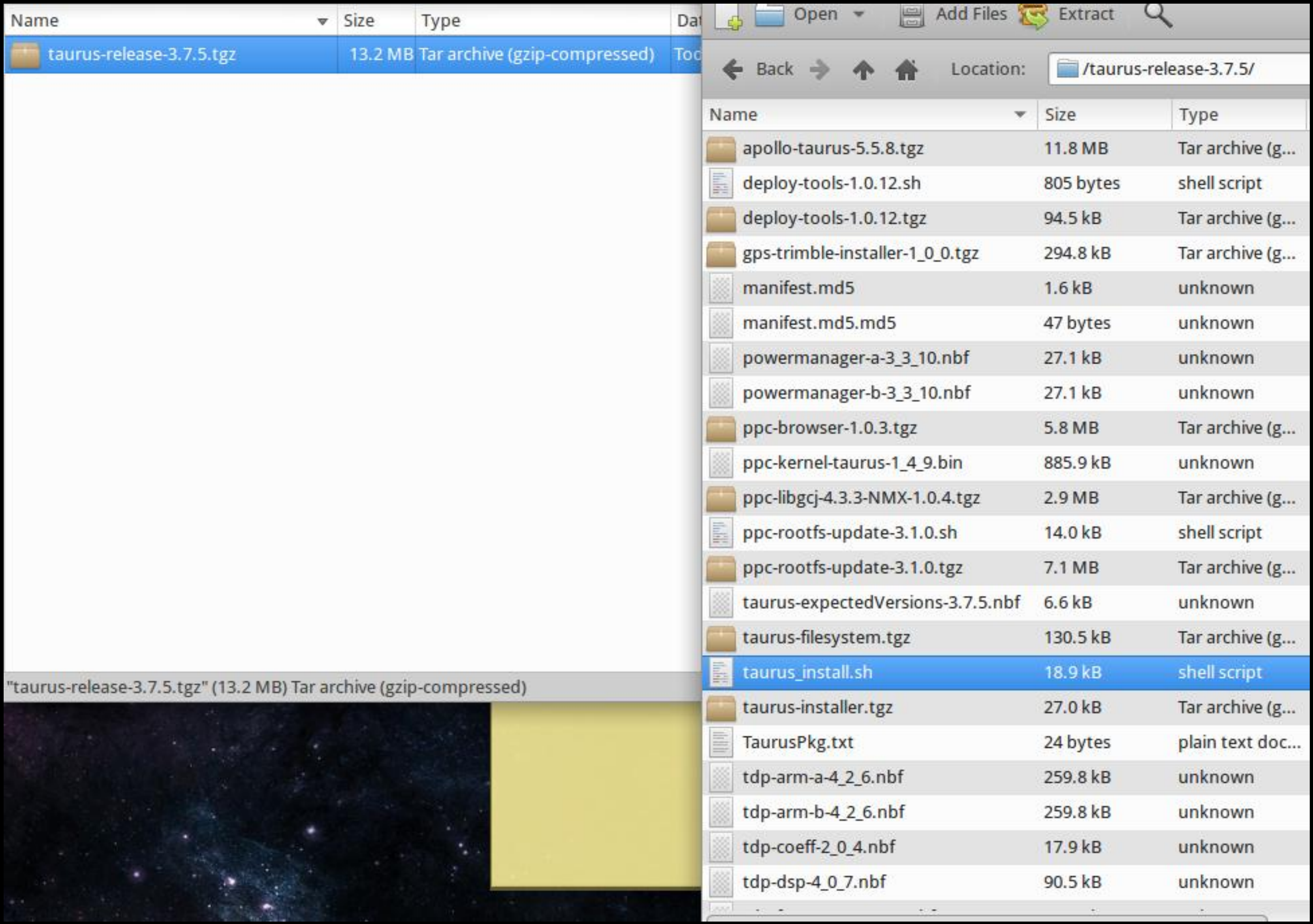
-The firmware was not easy to find in the internet

-This equipment is very expensive

-Not everyone can buy these things directly to the vendor, you need to be an organization/academics .

-Let tell you the story about how i was be able to get the firmware …..

FUCK YEAH!!!!!!



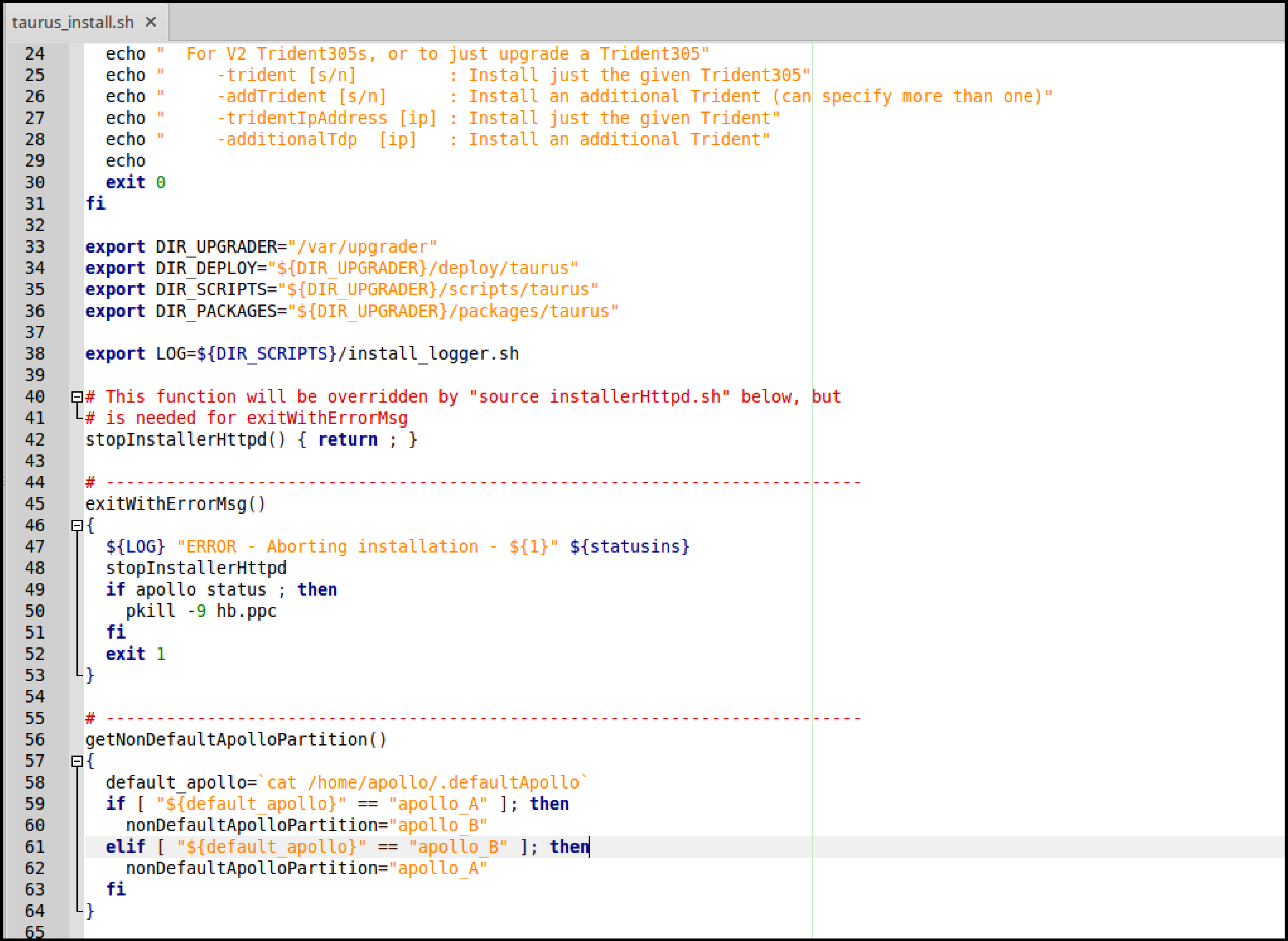
Name	Size	Type	Dat
taurus-release-3.7.5.tgz	13.2 MB	Tar archive (gzip-compressed)	Toc

"taurus-release-3.7.5.tgz" (13.2 MB) Tar archive (gzip-compressed)

Location: /taurus-release-3.7.5/

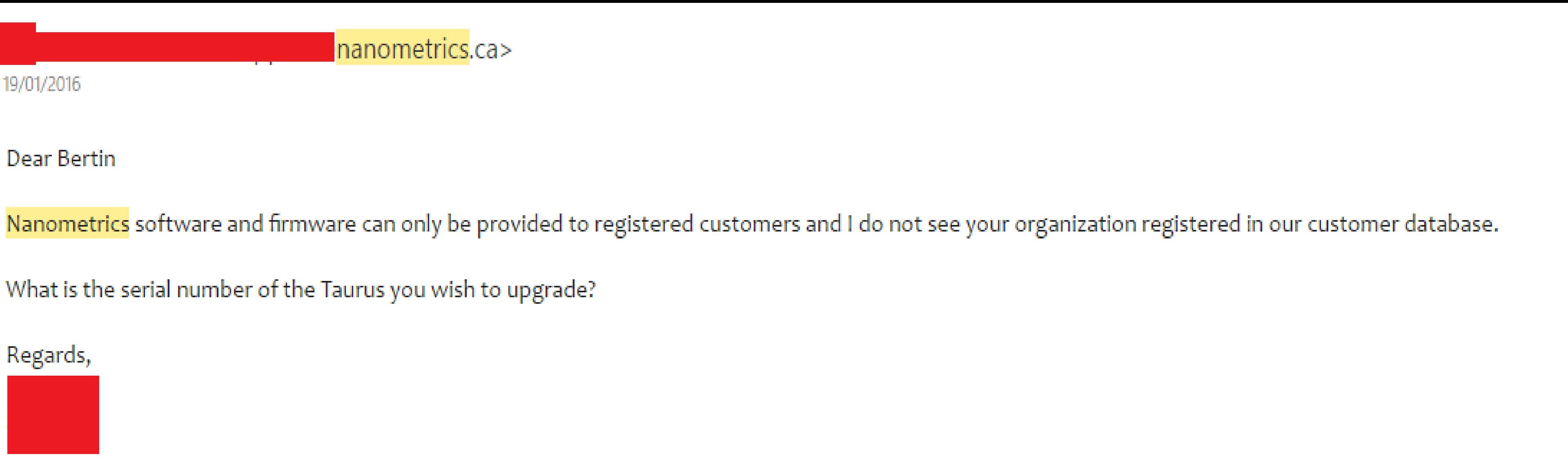
Name	Size	Type
apollo-taurus-5.5.8.tgz	11.8 MB	Tar archive (g...
deploy-tools-1.0.12.sh	805 bytes	shell script
deploy-tools-1.0.12.tgz	94.5 kB	Tar archive (g...
gps-trimble-installer-1_0_0.tgz	294.8 kB	Tar archive (g...
manifest.md5	1.6 kB	unknown
manifest.md5.md5	47 bytes	unknown
powermanager-a-3_3_10.nbf	27.1 kB	unknown
powermanager-b-3_3_10.nbf	27.1 kB	unknown
ppc-browser-1.0.3.tgz	5.8 MB	Tar archive (g...
ppc-kernel-taurus-1_4_9.bin	885.9 kB	unknown
ppc-libgcj-4.3.3-NMX-1.0.4.tgz	2.9 MB	Tar archive (g...
ppc-rootfs-update-3.1.0.sh	14.0 kB	shell script
ppc-rootfs-update-3.1.0.tgz	7.1 MB	Tar archive (g...
taurus-expectedVersions-3.7.5.nbf	6.6 kB	unknown
taurus-filesystem.tgz	130.5 kB	Tar archive (g...
taurus_install.sh	18.9 kB	shell script
taurus-installer.tgz	27.0 kB	Tar archive (g...
TaurusPkg.txt	24 bytes	plain text doc...
tdp-arm-a-4_2_6.nbf	259.8 kB	unknown
tdp-arm-b-4_2_6.nbf	259.8 kB	unknown
tdp-coeff-2_0_4.nbf	17.9 kB	unknown
tdp-dsp-4_0_7.nbf	90.5 kB	unknown

WTF?



```
  echo "  For V2 Trident305s, or to just upgrade a Trident305"
  echo "     -trident [s/n]         : Install just the given Trident305"
  echo "     -addTrident [s/n]      : Install an additional Trident (can specify more than one)"
  echo "     -tridentIpAddress [ip] : Install just the given Trident"
  echo "     -additionalTdp  [ip]   : Install an additional Trident"
  echo
  exit 0
fi

export DIR_UPGRADER="/var/upgrader"
export DIR_DEPLOY="${DIR_UPGRADER}/deploy/taurus"
export DIR_SCRIPTS="${DIR_UPGRADER}/scripts/taurus"
export DIR_PACKAGES="${DIR_UPGRADER}/packages/taurus"

export LOG=${DIR_SCRIPTS}/install_logger.sh

# This function will be overridden by "source installerHttpd.sh" below, but
# is needed for exitWithErrorMsg
stopInstallerHttpd() { return ; }

# ---------------------------------------------------------------------------
exitWithErrorMsg()
{
  ${LOG} "ERROR - Aborting installation - ${1}" ${statusins}
  stopInstallerHttpd
  if apollo status ; then
    pkill -9 hb.ppc
  fi
  exit 1
}

# ---------------------------------------------------------------------------
getNonDefaultApolloPartition()
{
  default_apollo=`cat /home/apollo/.defaultApollo`
  if [ "${default_apollo}" == "apollo_A" ]; then
    nonDefaultApolloPartition="apollo_B"
  elif [ "${default_apollo}" == "apollo_B" ]; then
    nonDefaultApolloPartition="apollo_A"
  fi
}
```

BUSTED…but too late for them



[redacted]nanometrics.ca>

19/01/2016

Dear Bertin

Nanometrics software and firmware can only be provided to registered customers and I do not see your organization registered in our customer database.

What is the serial number of the Taurus you wish to upgrade?

Regards,

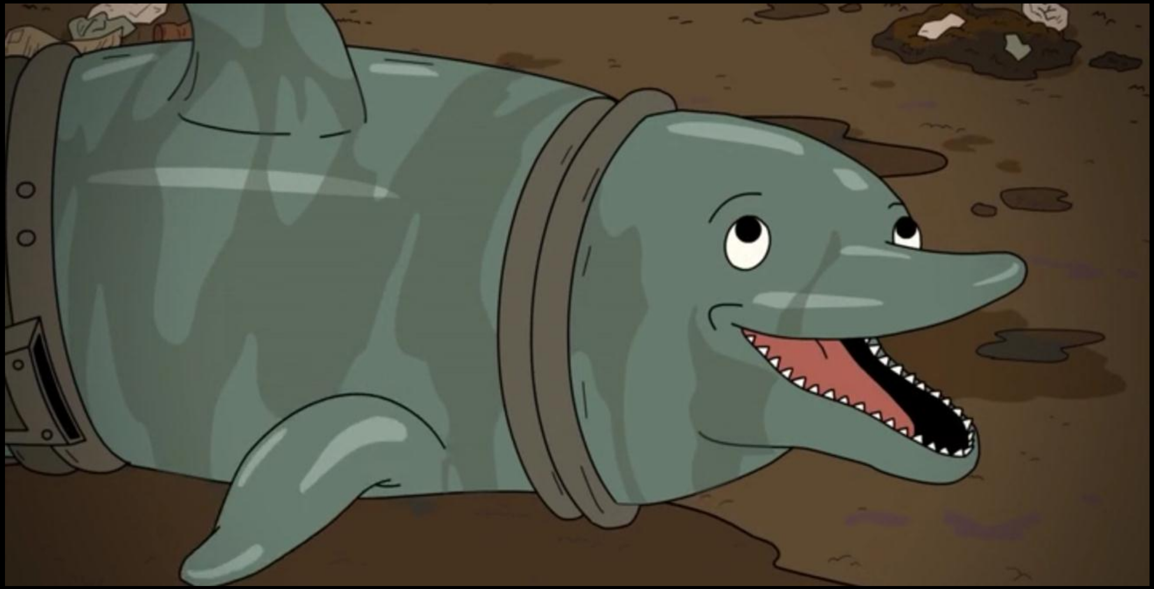
[redacted]

Too much talk!!

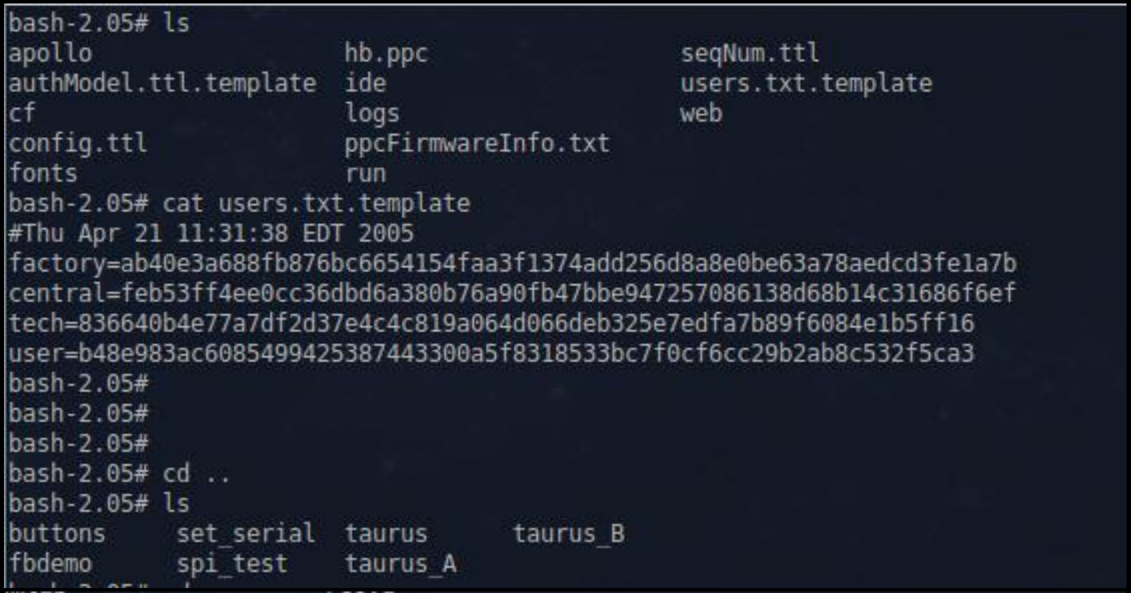
root@root

DEMO TIME

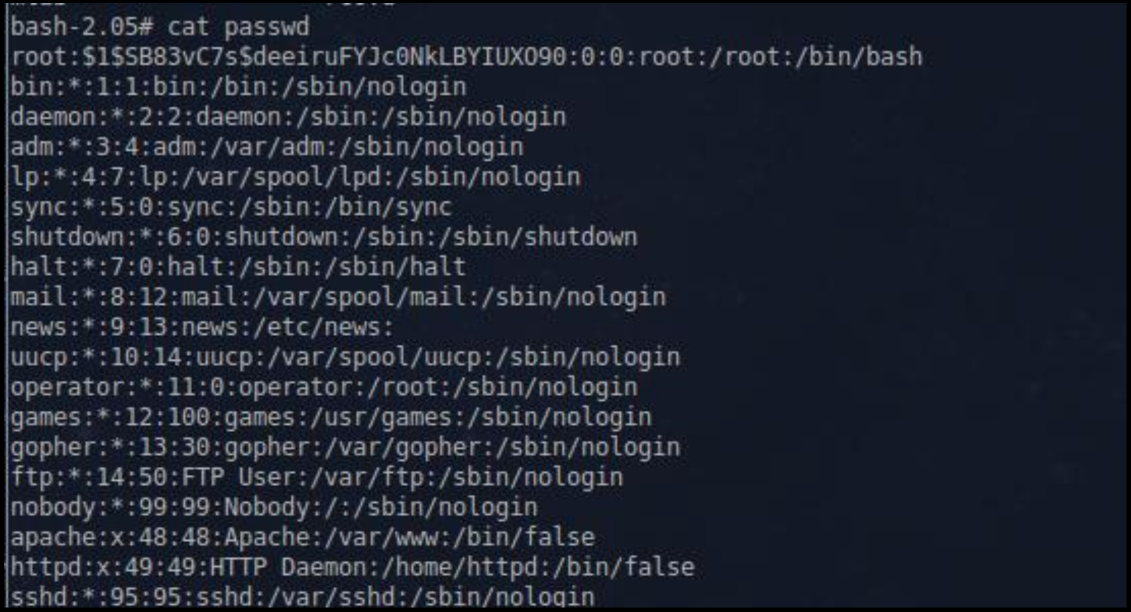
dolphin18



There is backdoor, factory user is not in official documentation.

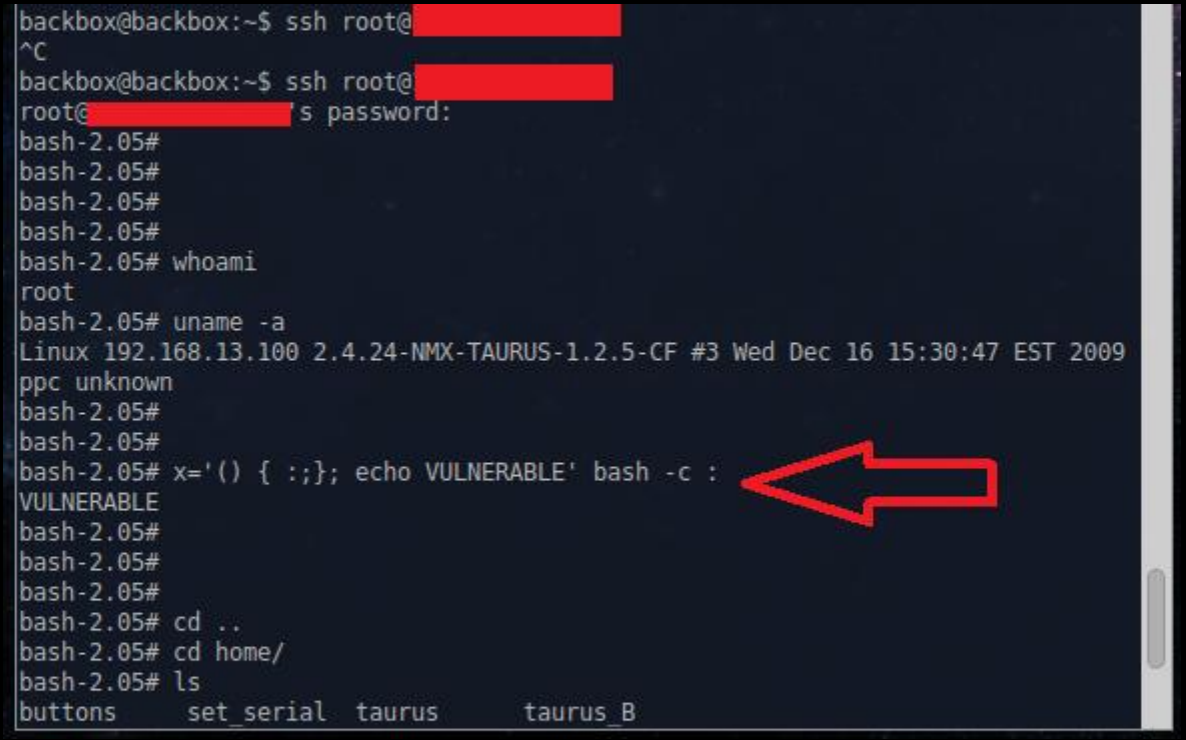


```
bash-2.05# ls
apollo                  hb.ppc                  seqNum.ttl
authModel.ttl.template  ide                     users.txt.template
cf                      logs                    web
config.ttl              ppcFirmwareInfo.txt
fonts                   run
bash-2.05# cat users.txt.template
#Thu Apr 21 11:31:38 EDT 2005
factory=ab40e3a688fb876bc6654154faa3f1374add256d8a8e0be63a78aedcd3fe1a7b
central=feb53ff4ee0cc36dbd6a380b76a90fb47bbe947257086138d68b14c31686f6ef
tech=836640b4e77a7df2d37e4c4c819a064d066deb325e7edfa7b89f6084e1b5ff16
user=b48e983ac6085499425387443300a5f8318533bc7f0cf6cc29b2ab8c532f5ca3
bash-2.05#
bash-2.05#
bash-2.05#
bash-2.05# cd ..
bash-2.05# ls
buttons     set_serial  taurus      taurus_B
fbdemo      spi_test    taurus_A
```



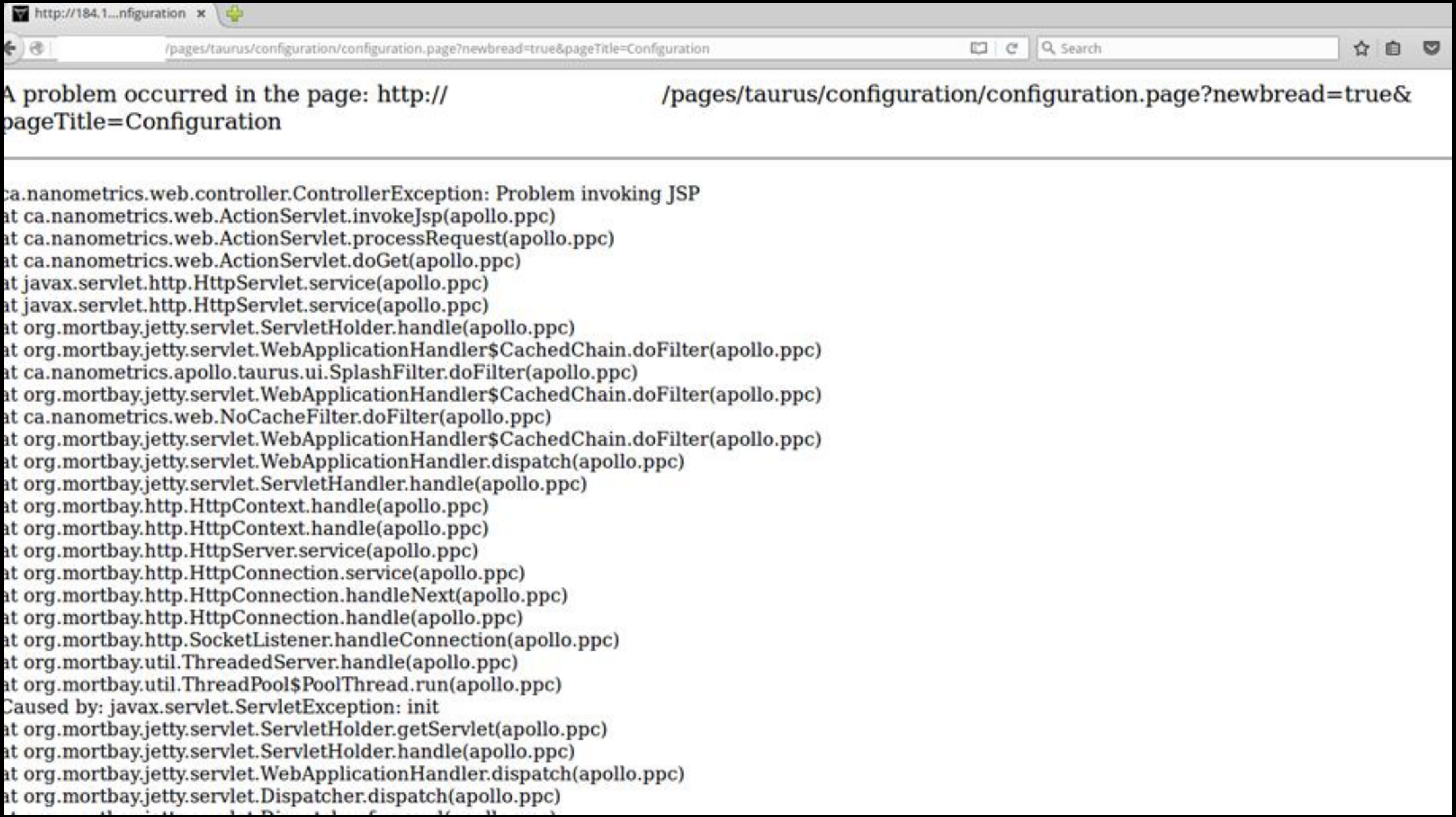
```
bash-2.05# cat passwd
root:$1$SB83vC7s$deeiruFYJc0NkLBYIUXO90:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:/sbin/nologin
daemon:*:2:2:daemon:/sbin:/sbin/nologin
adm:*:3:4:adm:/var/adm:/sbin/nologin
lp:*:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:*:5:0:sync:/sbin:/bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:/sbin/nologin
news:*:9:13:news:/etc/news:
uucp:*:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:*:11:0:operator:/root:/sbin/nologin
games:*:12:100:games:/usr/games:/sbin/nologin
gopher:*:13:30:gopher:/var/gopher:/sbin/nologin
ftp:*:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:*:99:99:Nobody:/:/sbin/nologin
apache:x:48:48:Apache:/var/www:/bin/false
httpd:x:49:49:HTTP Daemon:/home/httpd:/bin/false
sshd:*:95:95:sshd:/var/sshd:/sbin/nologin
```

Test some vulnerabilities.. You know..
PWD !! Shellshock



```
backbox@backbox:~$ ssh root@[redacted]
^C
backbox@backbox:~$ ssh root@[redacted]
root@[redacted]'s password:
bash-2.05#
bash-2.05#
bash-2.05#
bash-2.05#
bash-2.05# whoami
root
bash-2.05# uname -a
Linux 192.168.13.100 2.4.24-NMX-TAURUS-1.2.5-CF #3 Wed Dec 16 15:30:47 EST 2009
ppc unknown
bash-2.05#
bash-2.05#
bash-2.05# x='() { :;}; echo VULNERABLE' bash -c :
VULNERABLE
bash-2.05#
bash-2.05#
bash-2.05#
bash-2.05# cd ..
bash-2.05# cd home/
bash-2.05# ls
buttons     set_serial  taurus      taurus_B
```

Bugs and errors everywhere

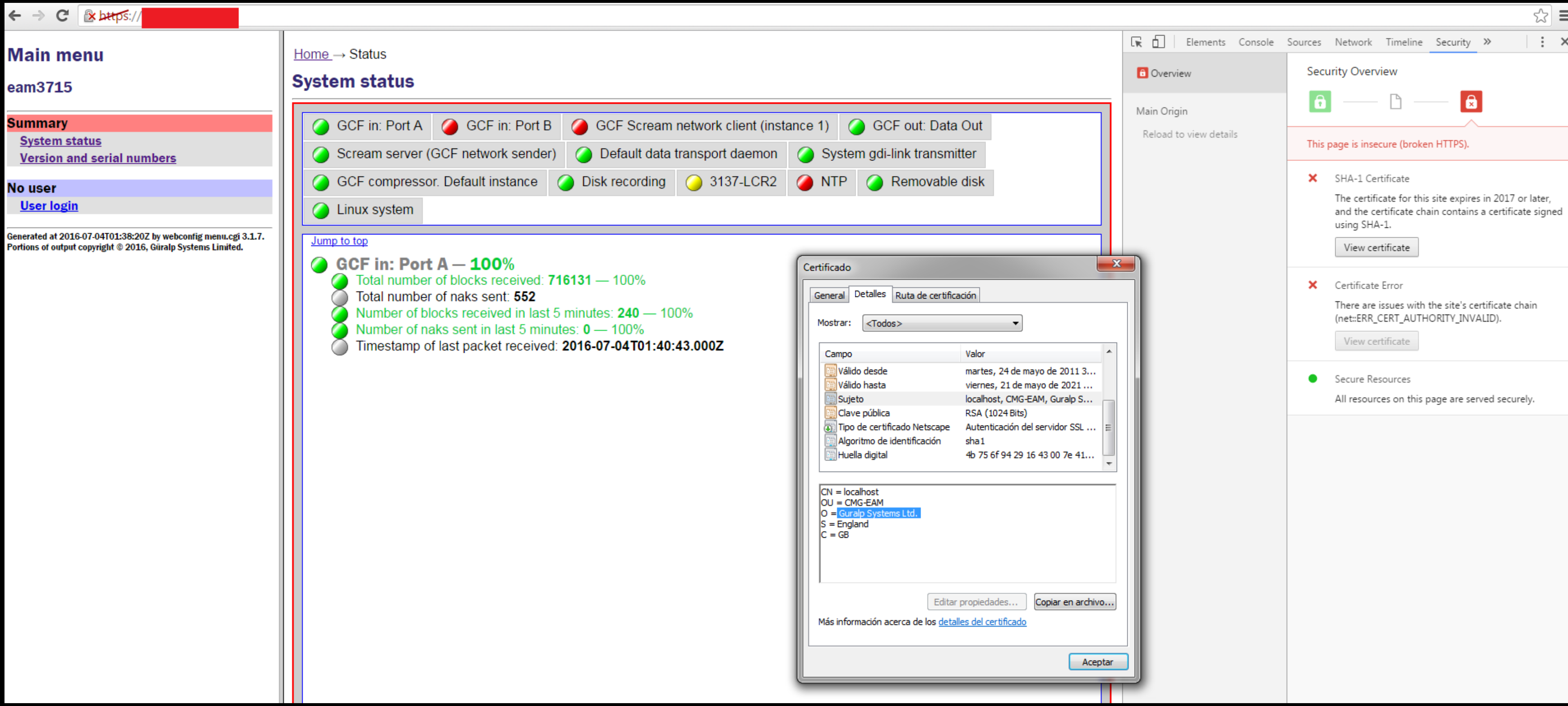


http://184.1....nfiguration
[redacted]/pages/taurus/configuration/configuration.page?newbread=true&pageTitle=Configuration
Search

A problem occurred in the page: http://[redacted]/pages/taurus/configuration/configuration.page?newbread=true&pageTitle=Configuration

```
ca.nanometrics.web.controller.ControllerException: Problem invoking JSP
at ca.nanometrics.web.ActionServlet.invokeJsp(apollo.ppc)
at ca.nanometrics.web.ActionServlet.processRequest(apollo.ppc)
at ca.nanometrics.web.ActionServlet.doGet(apollo.ppc)
at javax.servlet.http.HttpServlet.service(apollo.ppc)
at javax.servlet.http.HttpServlet.service(apollo.ppc)
at org.mortbay.jetty.servlet.ServletHolder.handle(apollo.ppc)
at org.mortbay.jetty.servlet.WebApplicationHandler$CachedChain.doFilter(apollo.ppc)
at ca.nanometrics.apollo.taurus.ui.SplashFilter.doFilter(apollo.ppc)
at org.mortbay.jetty.servlet.WebApplicationHandler$CachedChain.doFilter(apollo.ppc)
at ca.nanometrics.web.NoCacheFilter.doFilter(apollo.ppc)
at org.mortbay.jetty.servlet.WebApplicationHandler$CachedChain.doFilter(apollo.ppc)
at org.mortbay.jetty.servlet.WebApplicationHandler.dispatch(apollo.ppc)
at org.mortbay.jetty.servlet.ServletHandler.handle(apollo.ppc)
at org.mortbay.http.HttpContext.handle(apollo.ppc)
at org.mortbay.http.HttpContext.handle(apollo.ppc)
at org.mortbay.http.HttpServer.service(apollo.ppc)
at org.mortbay.http.HttpConnection.service(apollo.ppc)
at org.mortbay.http.HttpConnection.handleNext(apollo.ppc)
at org.mortbay.http.HttpConnection.handle(apollo.ppc)
at org.mortbay.http.SocketListener.handleConnection(apollo.ppc)
at org.mortbay.util.ThreadedServer.handle(apollo.ppc)
at org.mortbay.util.ThreadPool$PoolThread.run(apollo.ppc)
Caused by: javax.servlet.ServletException: init
at org.mortbay.jetty.servlet.ServletHolder.getServlet(apollo.ppc)
at org.mortbay.jetty.servlet.ServletHolder.handle(apollo.ppc)
at org.mortbay.jetty.servlet.WebApplicationHandler.dispatch(apollo.ppc)
at org.mortbay.jetty.servlet.Dispatcher.dispatch(apollo.ppc)
at org.mortbay.jetty.servlet.Dispatcher.forward(apollo.ppc)
```

GURALP Systems are easy to find looking in the SSL certificate metadata in NetDB



~~https~~:// [redacted]

Main menu

eam3715

Summary

- System status
- Version and serial numbers

No user

- User login

Generated at 2016-07-04T01:38:20Z by webconfig menu.cgi 3.1.7.
Portions of output copyright © 2016, Güralp Systems Limited.

Home → Status

System status

🟢 GCF in: Port A | 🔴 GCF in: Port B | 🔴 GCF Scream network client (instance 1) | 🟢 GCF out: Data Out

🟢 Scream server (GCF network sender) | 🟢 Default data transport daemon | 🟢 System gdi-link transmitter

🟢 GCF compressor. Default instance | 🟢 Disk recording | 🟡 3137-LCR2 | 🔴 NTP | 🟢 Removable disk

🟢 Linux system

Jump to top

🟢 GCF in: Port A — 100%

- 🟢 Total number of blocks received: **716131** — 100%
- ⚪ Total number of naks sent: **552**
- 🟢 Number of blocks received in last 5 minutes: **240** — 100%
- 🟢 Number of naks sent in last 5 minutes: **0** — 100%
- ⚪ Timestamp of last packet received: **2016-07-04T01:40:43.000Z**

Certificado

General | Detalles | Ruta de certificación

Mostrar: <Todos>

Campo	Valor
Válido desde	martes, 24 de mayo de 2011 3...
Válido hasta	viernes, 21 de mayo de 2021 ...
Sujeto	localhost, CMG-EAM, Guralp S...
Clave pública	RSA (1024 Bits)
Tipo de certificado Netscape	Autenticación del servidor SSL ...
Algoritmo de identificación	sha1
Huella digital	4b 75 6f 94 29 16 43 00 7e 41...

```
CN = localhost
OU = CMG-EAM
O = Guralp Systems Ltd.
S = England
C = GB
```

Editar propiedades... | Copiar en archivo...

Más información acerca de los detalles del certificado

Aceptar

Overview

Main Origin

Reload to view details

Security Overview

This page is insecure (broken HTTPS).

✗ SHA-1 Certificate

The certificate for this site expires in 2017 or later, and the certificate chain contains a certificate signed using SHA-1.

View certificate

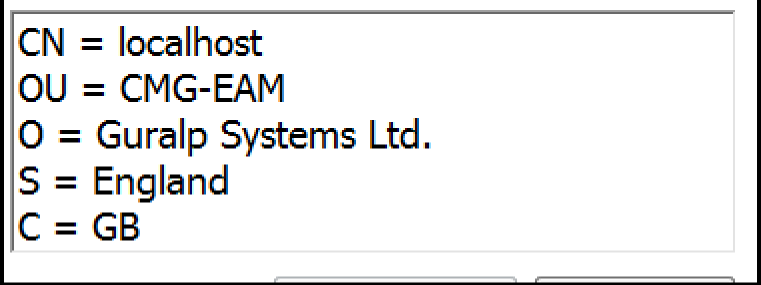
✗ Certificate Error

There are issues with the site's certificate chain (net::ERR_CERT_AUTHORITY_INVALID).

View certificate

● Secure Resources

All resources on this page are served securely.



```
CN = localhost
OU = CMG-EAM
O = Guralp Systems Ltd.
S = England
C = GB
```

Ok , now we are root so .. What’s next ?

PROTOCOL / COMMUNICATIONS

The Standard for the Exchange of Earthquake Data (SEED) is a data format intended primarily for the archival and exchange of seismological time series data and related metadata. The format is maintained by the International Federation of Digital Seismograph Networks and documented in the SEED Manual (PDF format). Originally designed in the late 1980s, the format has been enhanced and refined a number of times and remains in widespread use.

Data identification nomenclature

The SEED format uses 4 name components to uniquely identify a time series and provide attribution to the owner of the data:

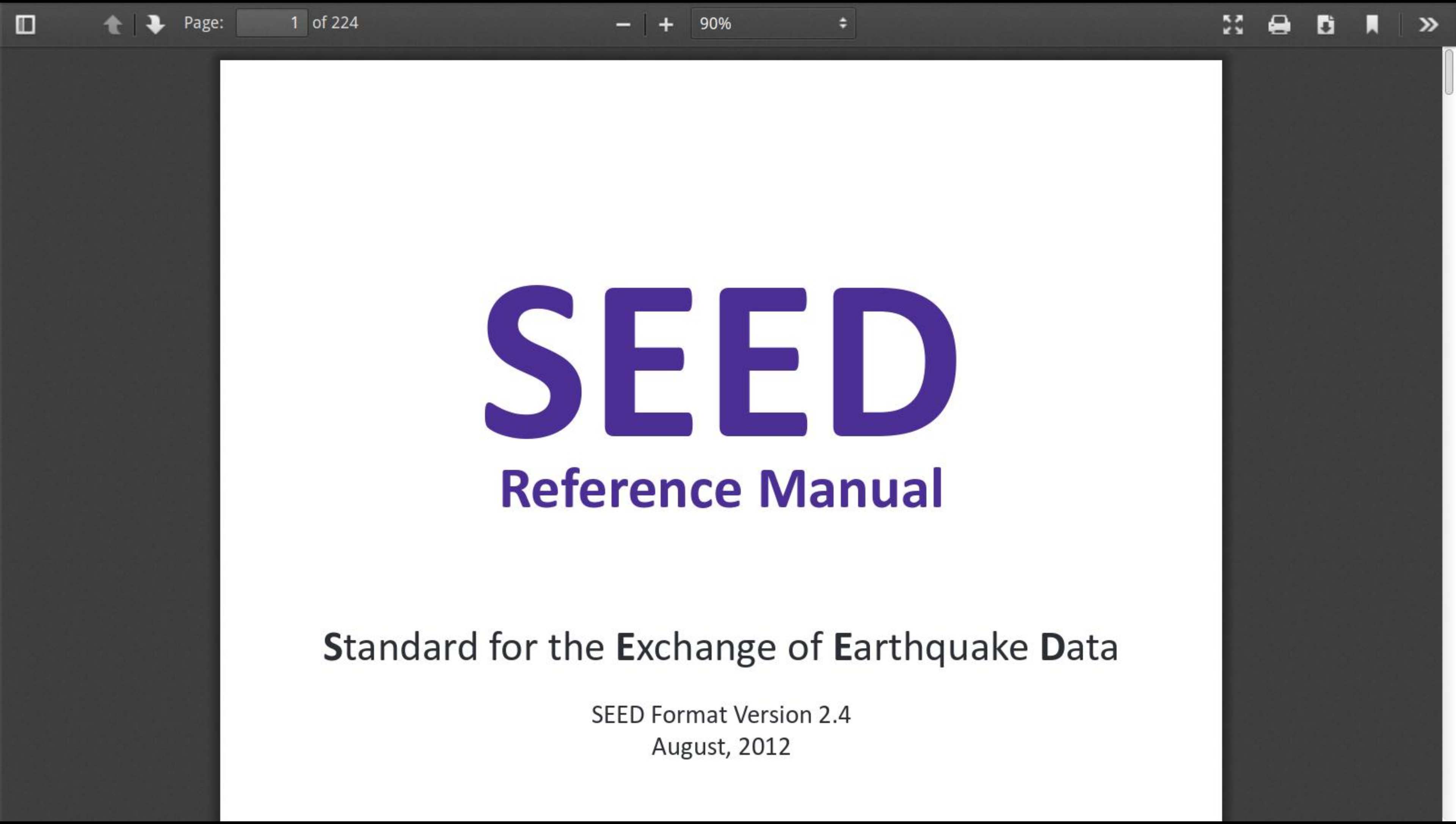
Network code: a 1 or 2 character code identifying the network/owner of the data. These codes are assigned by the FDSN to provide uniqueness to seismological data, new codes may be requested.

Station code: a 1 to 5 character identifier for the station recording the data.

Location ID: a 2 character code used to uniquely identify different data streams at a single station. These IDs are commonly used to logically separate multiple instruments or sensor sets at a single station.

Channel codes: a 3 character combination used to identify the 1) band and general sample rate 2) the instrument type and 3) the orientation of the sensor. A convention for these codes has been established and is documented in Appendix A of the SEED Manual.

What if……



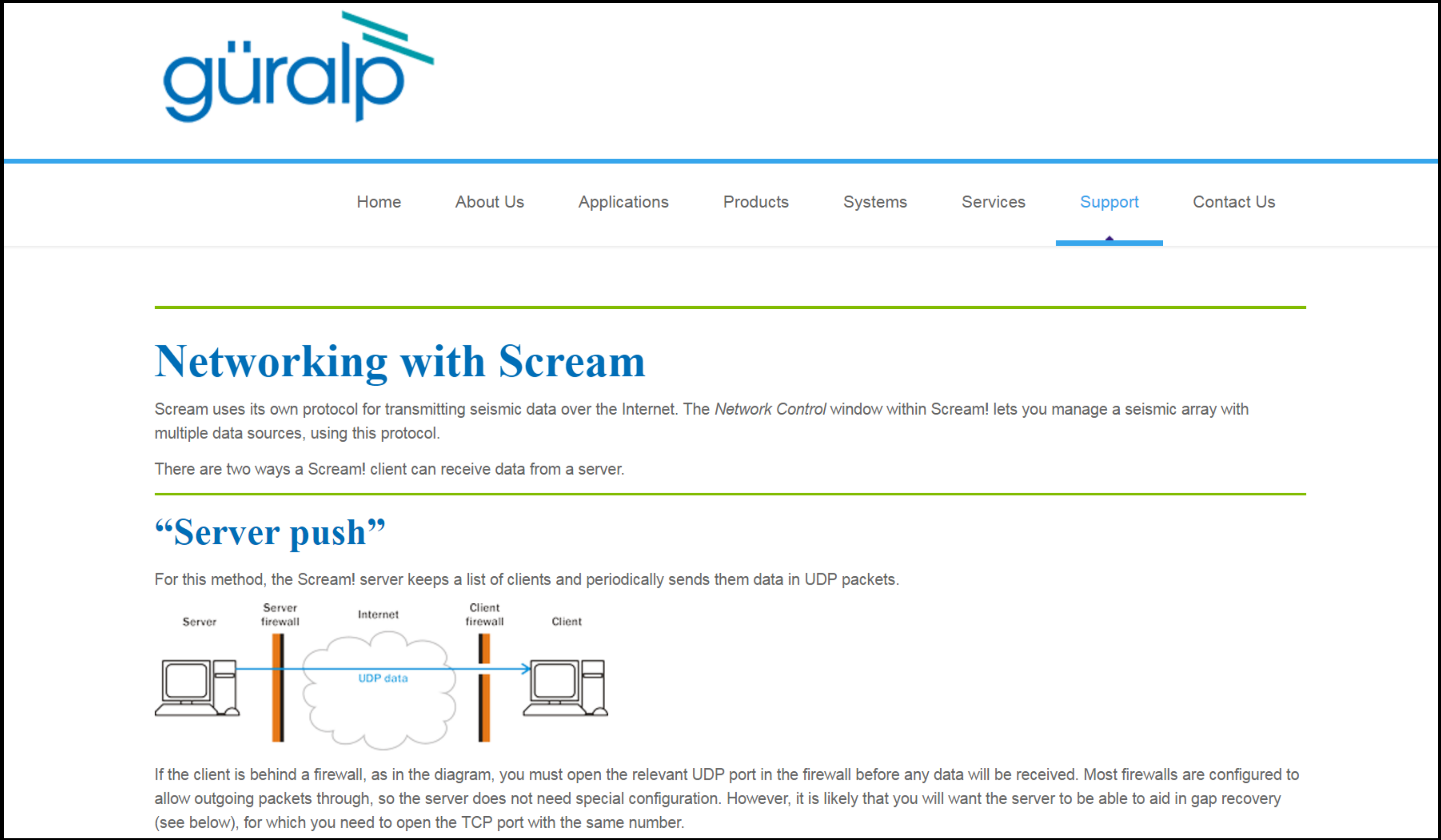
SEED

Reference Manual

Standard for the **E**xchange of **E**arthquake **D**ata

SEED Format Version 2.4
August, 2012

Guralp systems SCREAM protocol for transmitting seismic data over the internet



Networking with Scream

Scream uses its own protocol for transmitting seismic data over the Internet. The *Network Control* window within Scream! lets you manage a seismic array with multiple data sources, using this protocol.

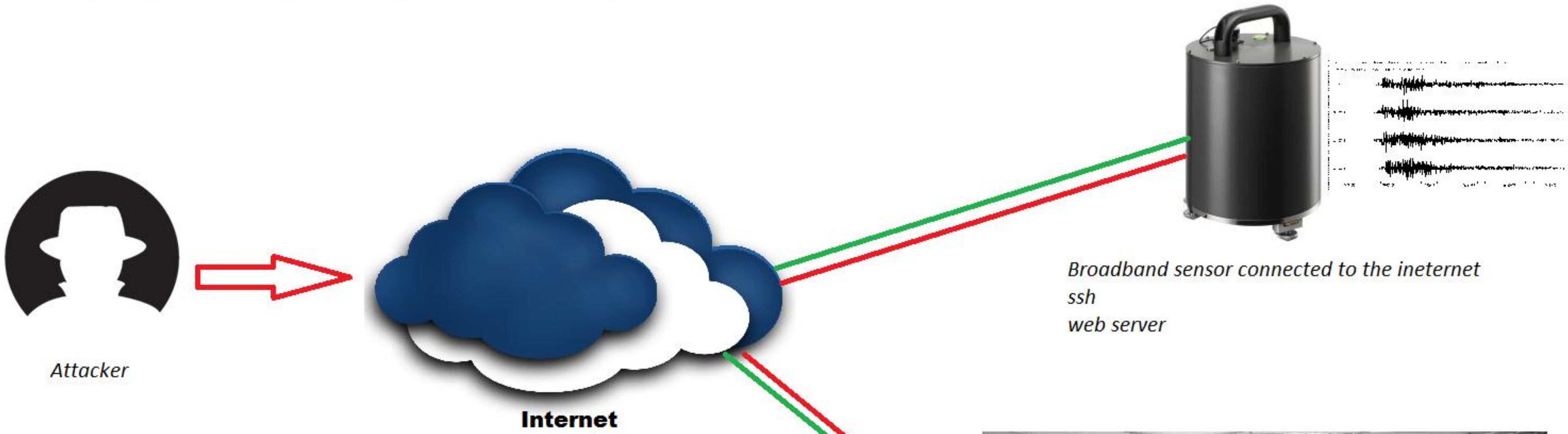
There are two ways a Scream! client can receive data from a server.

"Server push"

For this method, the Scream! server keeps a list of clients and periodically sends them data in UDP packets.

If the client is behind a firewall, as in the diagram, you must open the relevant UDP port in the firewall before any data will be received. Most firewalls are configured to allow outgoing packets through, so the server does not need special configuration. However, it is likely that you will want the server to be able to aid in gap recovery (see below), for which you need to open the TCP port with the same number.

Exploiting and attacking a seismological network… remotely



Attacker

Internet

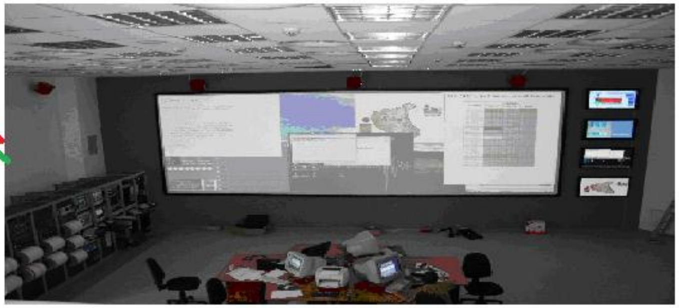
Broadband sensor connected to the ineternet
ssh
web server

Several attack vectors can compromise the security of a broadband sensor used to measure the seismological activity in a specific geo-spatial area (ex.ground,sea).

The problem is :

This devices are connected to the public internet

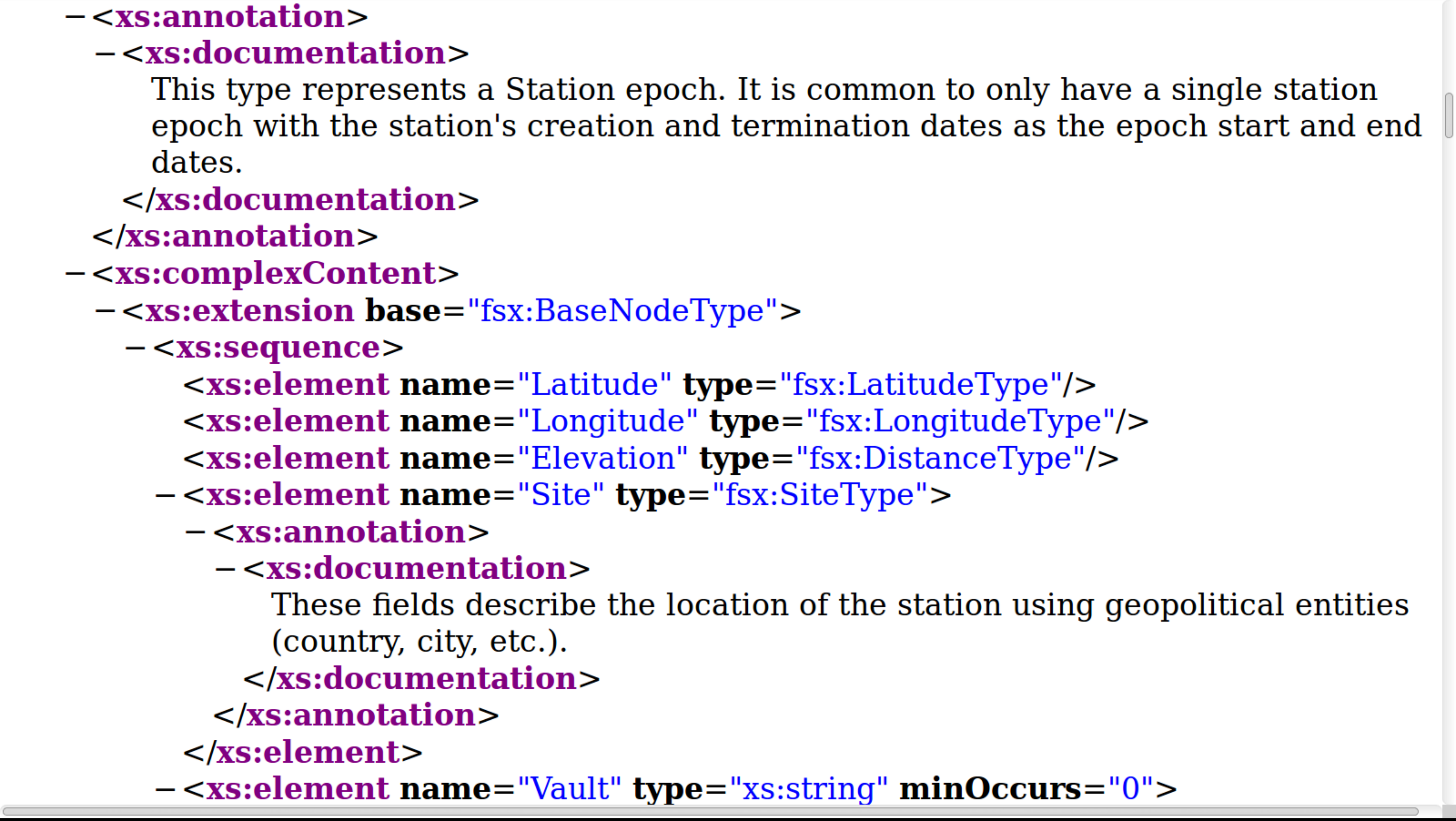
We're going to demonstrate in a real attack scenario how we can take control REMOTELY of one of this devices and modify the data sent to the acquisition network in order to inject a false positive in the seismological network research.



Data acquisition/research center - seismological network owner

Bertin B NetDB Research lab 2015

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          np version          |          pcketsize             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| metaSequence    |    Sequence Number  |        starttime      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Originate Timestamp                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Latitude   |    Longitude      |        Altitude          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          DataSource                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



```
 -<xs:annotation>
   -<xs:documentation>
       This type represents a Station epoch. It is common to only have a single station
       epoch with the station's creation and termination dates as the epoch start and end
       dates.
     </xs:documentation>
   </xs:annotation>
 -<xs:complexContent>
   -<xs:extension base="fsx:BaseNodeType">
     -<xs:sequence>
         <xs:element name="Latitude" type="fsx:LatitudeType"/>
         <xs:element name="Longitude" type="fsx:LongitudeType"/>
         <xs:element name="Elevation" type="fsx:DistanceType"/>
       -<xs:element name="Site" type="fsx:SiteType">
         -<xs:annotation>
           -<xs:documentation>
               These fields describe the location of the station using geopolitical entities
               (country, city, etc.).
             </xs:documentation>
           </xs:annotation>
         </xs:element>
       -<xs:element name="Vault" type="xs:string" minOccurs="0">
```

Conclusions

-We are be able to locate this devices anywhere in the world

-We are in control of the device , the network and the software running on it.

-There is no SSL in communications

-This devices help engineers to save people and understand the earth

-Vendors please… code better and think in security

Recommendations

THANKS

SEE YOU NEXT TIME !!