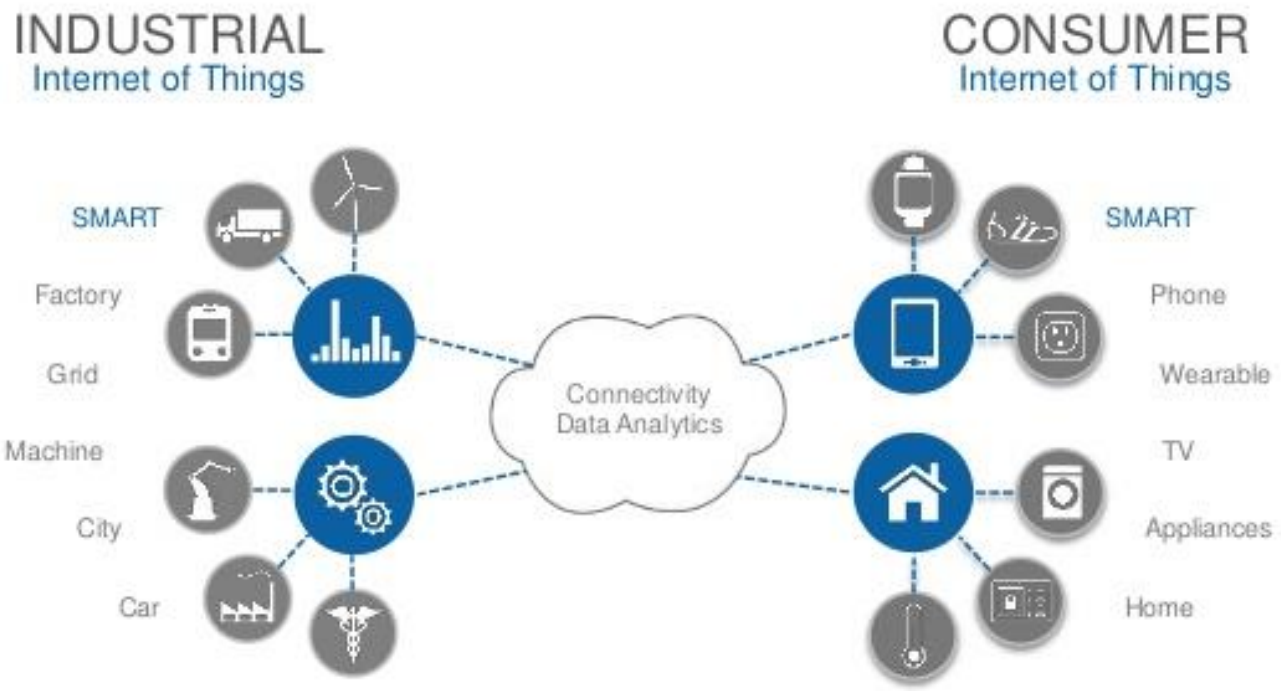
# Industrial IoT Security – convergence of IT and OT worlds

Dr Theodoros Stergiou, CEng, CPMM, CISM
Security Solutions Product Manager & Cloud Security Officer

*@thster, thster@intracom-telecom.com*

# Industrial IoT (IIoT)



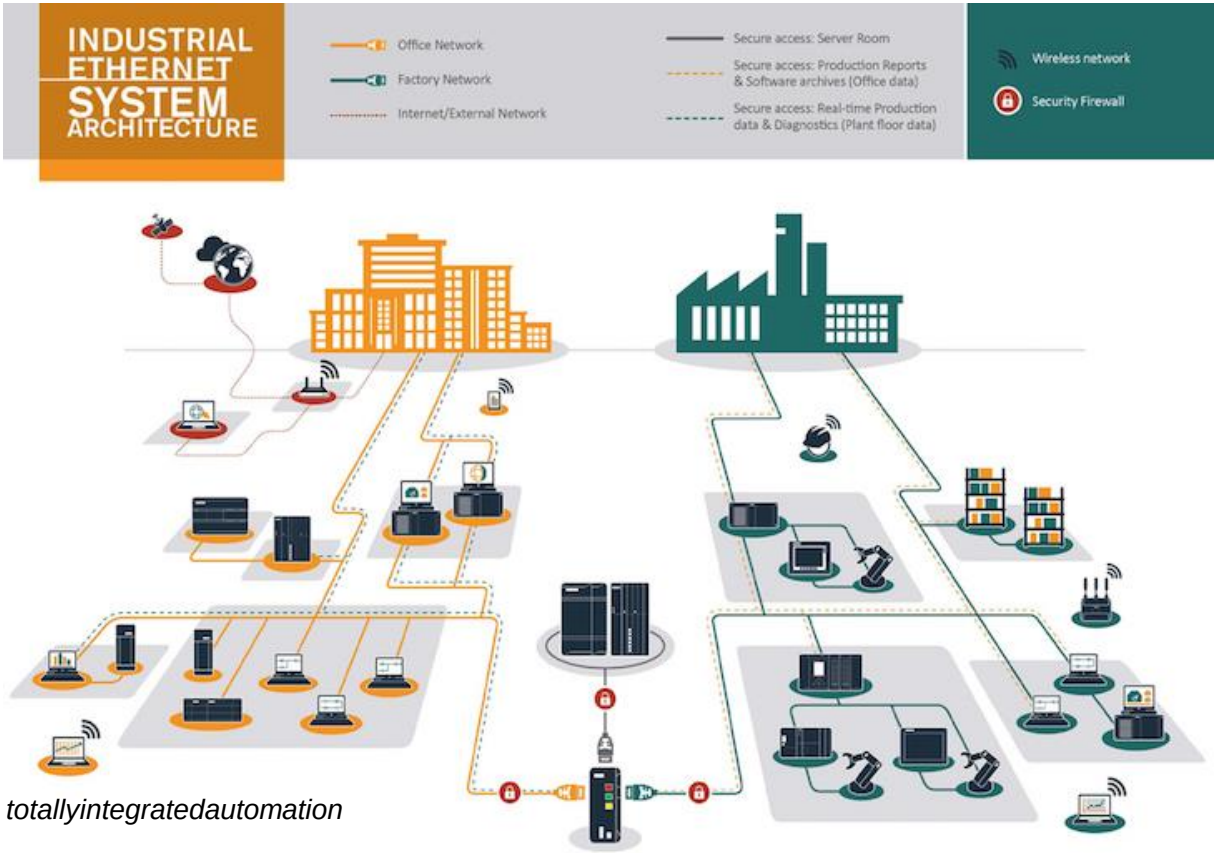

*Source: Voltimum UK, National Instruments*

# Connected industry


*Source: National Instruments*

# Security Challenges

- Information Technology (IT) security involves protecting data
- Operations Technology (OT) security involves preserving safety and ensuring production availability.
- OT security involves compliance to additional set of standards




*Source: totallyintegratedautomation*

# A whole range of different questions

- IT Security
  - Who are you?
  - What systems you want to access?
  - Are you coming from a trusted domain?
  - Are you properly authorized?
  - …
- OT Security
  - Are you instructing the machine to do something unsafe?
  - Are you requesting data the system should not be sending you?
  - Are the instructions legitimate?
  - …
- How do we converge these two worlds?

# Different worlds – same vulnerabilities

- Default credentials for more than 100 products (wireless gateways, routers, programmable logic controllers (PLC), servers and network modules)

Branch: master ▾ **SCADAPASS** / **scadapass.csv** Find file | Copy path

**scadastrangelove** Merge pull request #2 from attritionorg/patch-2 — 7aa1139 5 hours ago

2 contributors

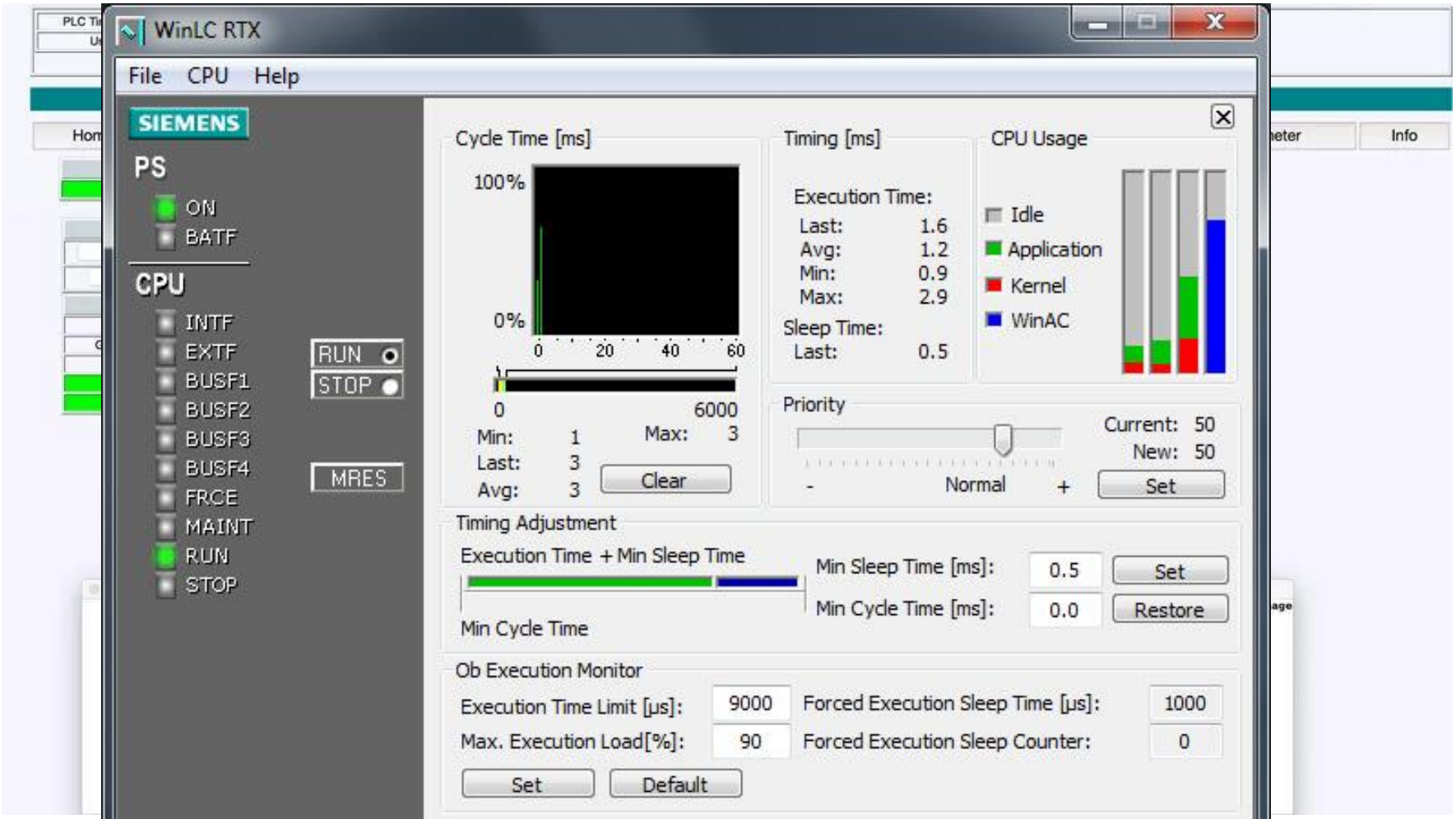
113 lines (112 sloc) | 19.7 KB — Raw | Blame | History

Search this file…

| | | |
|---|---|---|
| 1 | **#SCADA StrangeLove Default/Hardcoded Passwords List** | |
| 2 | #Find more at http://www.scada.sl | |
| 3 | #release 1.0 by Oxana Andreeva (oxana.andreeva@inbox.ru) | |
| 4 | | |
| 5 | Vendor | Device |
| 6 | ABB | AC 800M |
| 7 | ABB | SREA-01 |
| 8 | B&B ELECTRONICS | CR10 v2 |
| 9 | B&B ELECTRONICS | Conel 4.0.1 |
| 10 | B&B ELECTRONICS | SPECTRE Router |
| 11 | B&B ELECTRONICS | ER75i/ER 75i DUO/ER 75i SL/ER75i v2 |

# Different worlds – same vulnerabilities

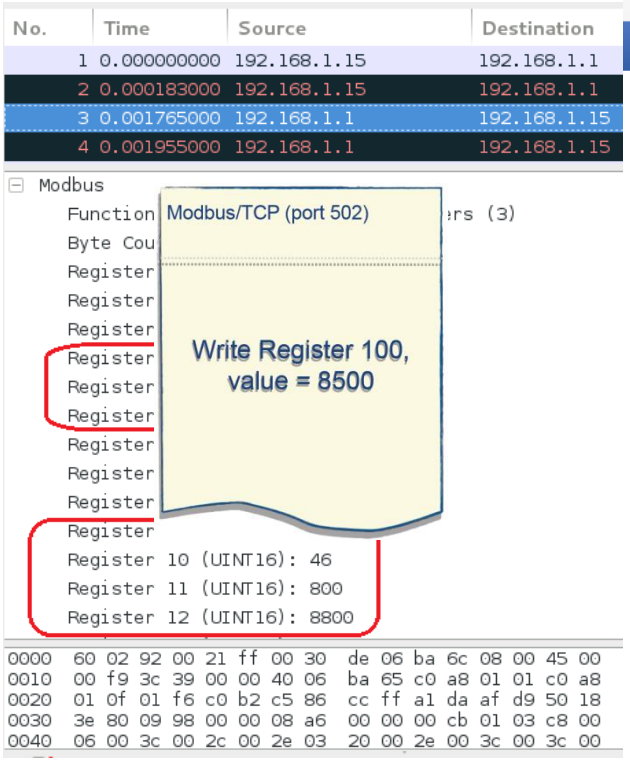
- Hardcoded credentials

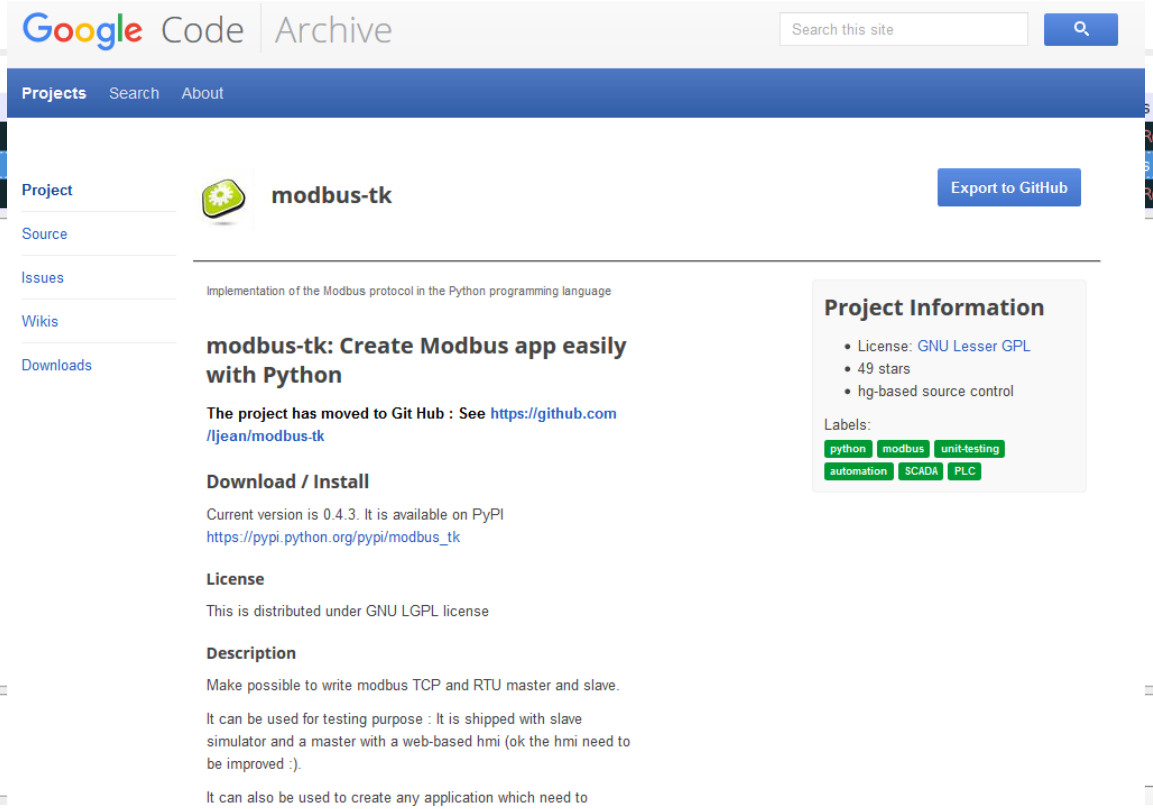


# OT protocols

## ICS/SCADA related protocols are not that proprietary

- Modbus – published in 1979, runs on serial, **502/TCP**

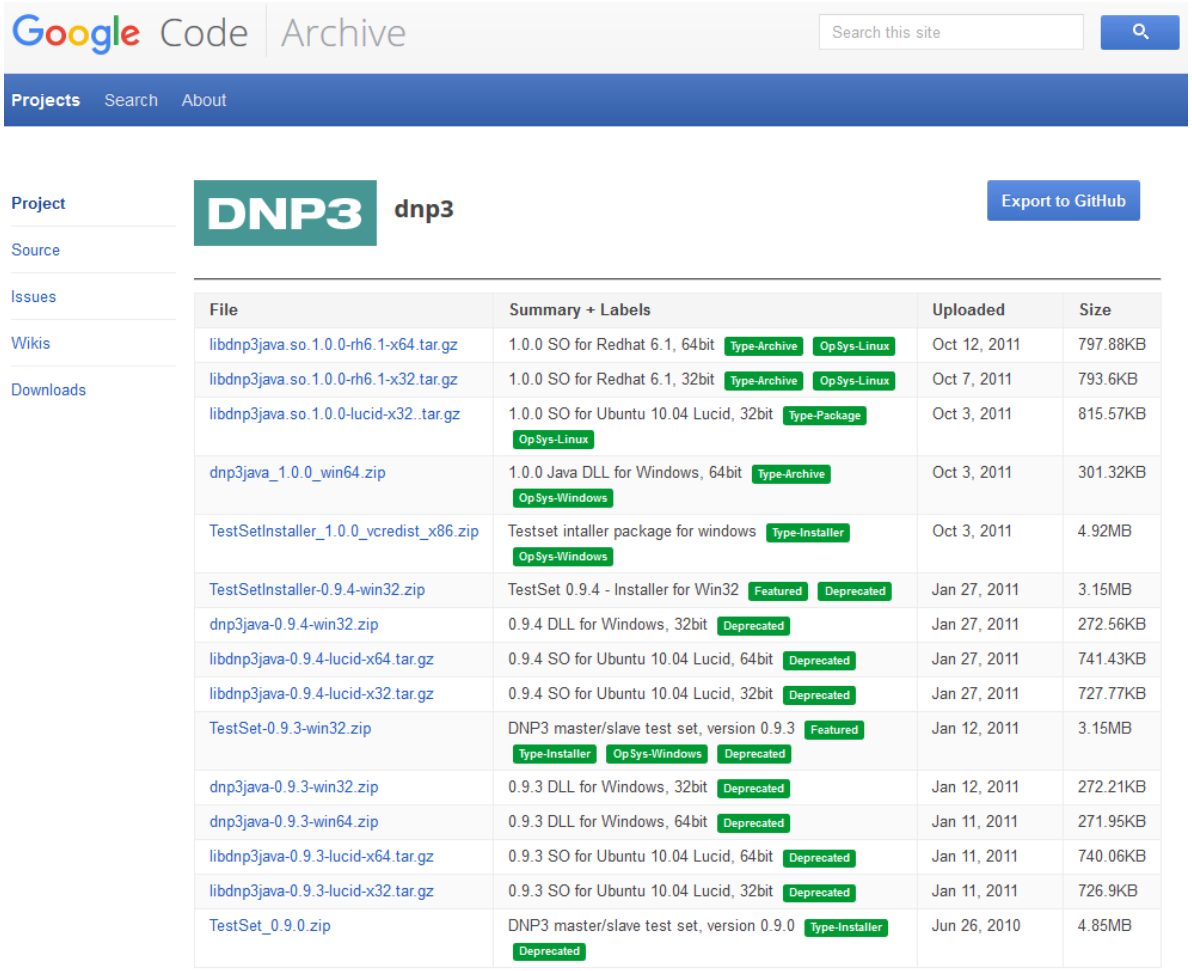


# OT protocols

**ICS/SCADA related protocols are not that proprietary**

- Dnp3 – published in 1990, **20000/TCP-UDP**




| File | Summary + Labels | Uploaded | Size |
|---|---|---|---|
| libdnp3java.so.1.0.0-rh6.1-x64.tar.gz | 1.0.0 SO for Redhat 6.1, 64bit Type-Archive OpSys-Linux | Oct 12, 2011 | 797.88KB |
| libdnp3java.so.1.0.0-rh6.1-x32.tar.gz | 1.0.0 SO for Redhat 6.1, 32bit Type-Archive OpSys-Linux | Oct 7, 2011 | 793.6KB |
| libdnp3java.so.1.0.0-lucid-x32..tar.gz | 1.0.0 SO for Ubuntu 10.04 Lucid, 32bit Type-Package OpSys-Linux | Oct 3, 2011 | 815.57KB |
| dnp3java_1.0.0_win64.zip | 1.0.0 Java DLL for Windows, 64bit Type-Archive OpSys-Windows | Oct 3, 2011 | 301.32KB |
| TestSetInstaller_1.0.0_vcredist_x86.zip | Testset intaller package for windows Type-Installer OpSys-Windows | Oct 3, 2011 | 4.92MB |
| TestSetInstaller-0.9.4-win32.zip | TestSet 0.9.4 - Installer for Win32 Featured Deprecated | Jan 27, 2011 | 3.15MB |
| dnp3java-0.9.4-win32.zip | 0.9.4 DLL for Windows, 32bit Deprecated | Jan 27, 2011 | 272.56KB |
| libdnp3java-0.9.4-lucid-x64.tar.gz | 0.9.4 SO for Ubuntu 10.04 Lucid, 64bit Deprecated | Jan 27, 2011 | 741.43KB |
| libdnp3java-0.9.4-lucid-x32.tar.gz | 0.9.4 SO for Ubuntu 10.04 Lucid, 32bit Deprecated | Jan 27, 2011 | 727.77KB |
| TestSet-0.9.3-win32.zip | DNP3 master/slave test set, version 0.9.3 Featured Type-Installer OpSys-Windows Deprecated | Jan 12, 2011 | 3.15MB |
| dnp3java-0.9.3-win32.zip | 0.9.3 DLL for Windows, 32bit Deprecated | Jan 12, 2011 | 272.21KB |
| dnp3java-0.9.3-win64.zip | 0.9.3 DLL for Windows, 64bit Deprecated | Jan 11, 2011 | 271.95KB |
| libdnp3java-0.9.3-lucid-x64.tar.gz | 0.9.3 SO for Ubuntu 10.04 Lucid, 64bit Deprecated | Jan 11, 2011 | 740.06KB |
| libdnp3java-0.9.3-lucid-x32.tar.gz | 0.9.3 SO for Ubuntu 10.04 Lucid, 32bit Deprecated | Jan 11, 2011 | 726.9KB |
| TestSet_0.9.0.zip | DNP3 master/slave test set, version 0.9.0 Type-Installer Deprecated | Jun 26, 2010 | 4.85MB |

# OT protocols

**ICS/SCADA related protocols are not that proprietary**

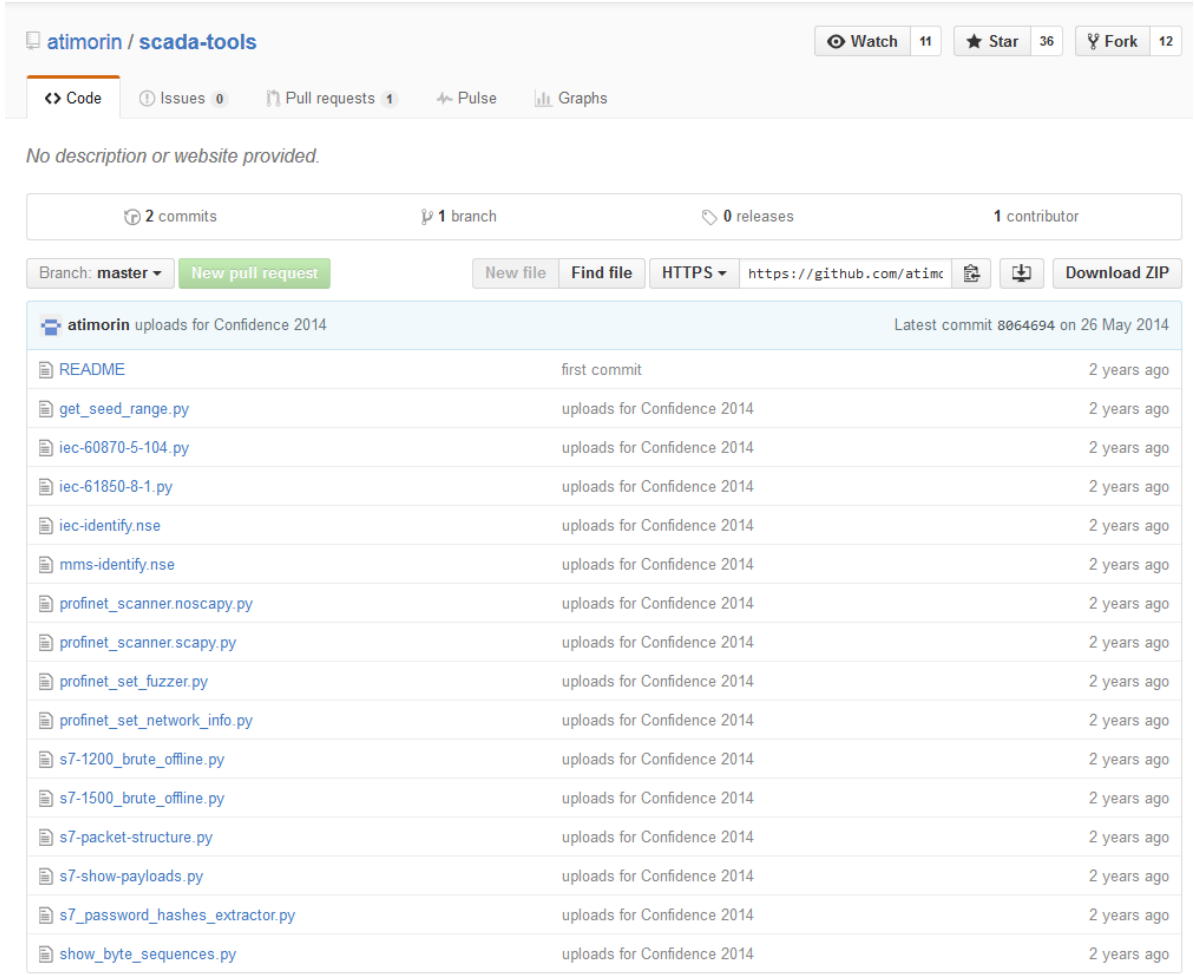
- IEC 60870-5 – published in 2000, 2404/TCP

~nmap –script iec-identify.nse –script-args='iec-identify.timeout=500' –p 2404 <host>

```
Host is up, received user-set (0.0037s latency).
Scanned at 2013-10-31 07:09:06 EDT for 1s
PORT     STATE SERVICE          REASON
2404/tcp open  IEC 60870-5-104 syn-ack
| iec-identify:
|   testfr sent / recv: 680443000000 / 680483000000
|   startdt sent / recv: 680407000000 / 68040b000000
|   c_ic_na_1 sent / recv: 680e00000000640106000fff00000000 / 680e
|_  asdu address: 65535
Final times for host: srtt: 3654 rttvar: 5000  to: 100000
```

# OT protocols

- For every known protocol, at least one exploit tool is freely available – for educational purposes of course



atimorin / scada-tools

Watch 11 | Star 36 | Fork 12

Code | Issues 0 | Pull requests 1 | Pulse | Graphs

*No description or website provided.*

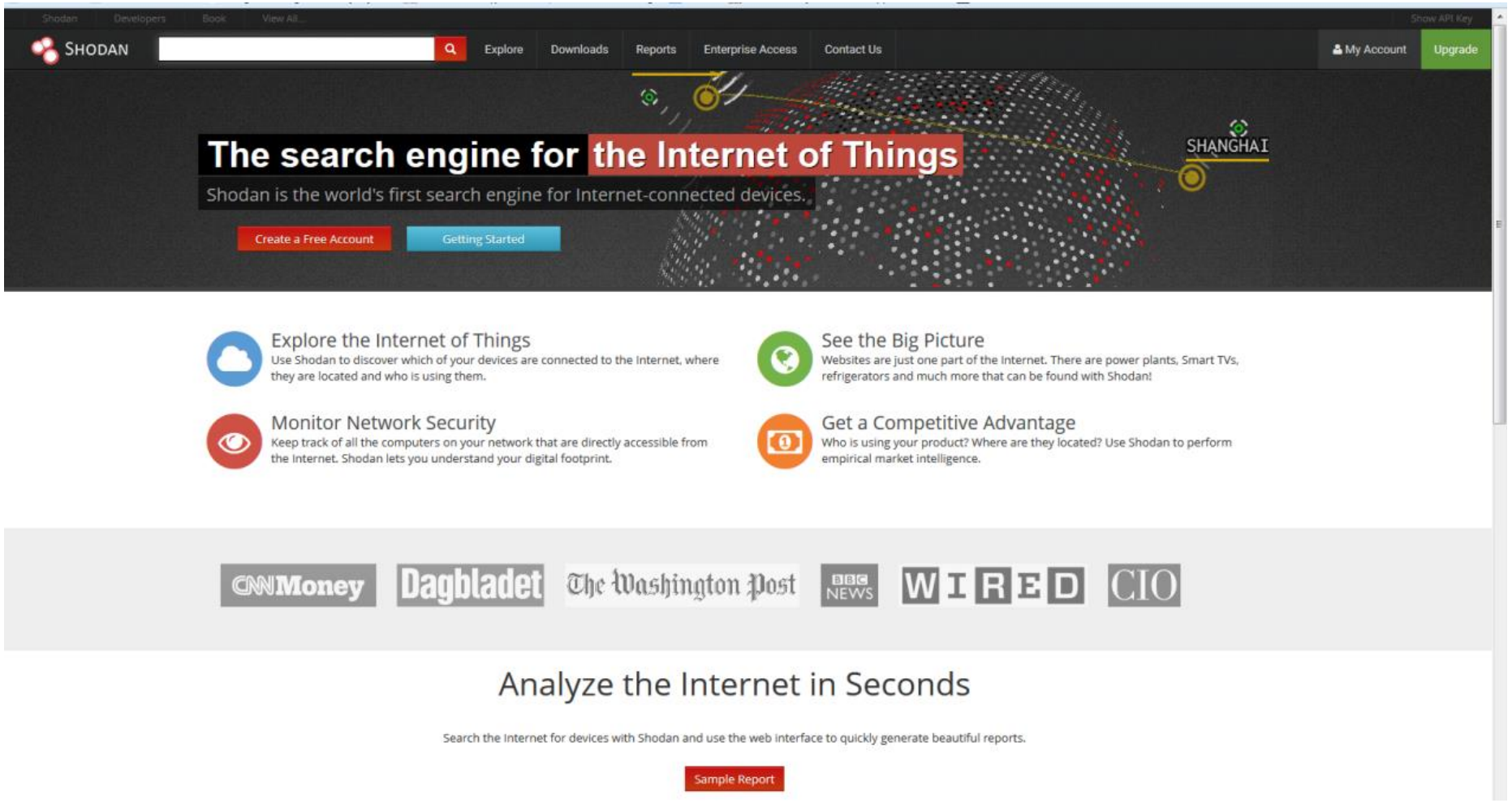
2 commits | 1 branch | 0 releases | 1 contributor

Branch: master | New pull request | New file | Find file | HTTPS | https://github.com/atimc | Download ZIP

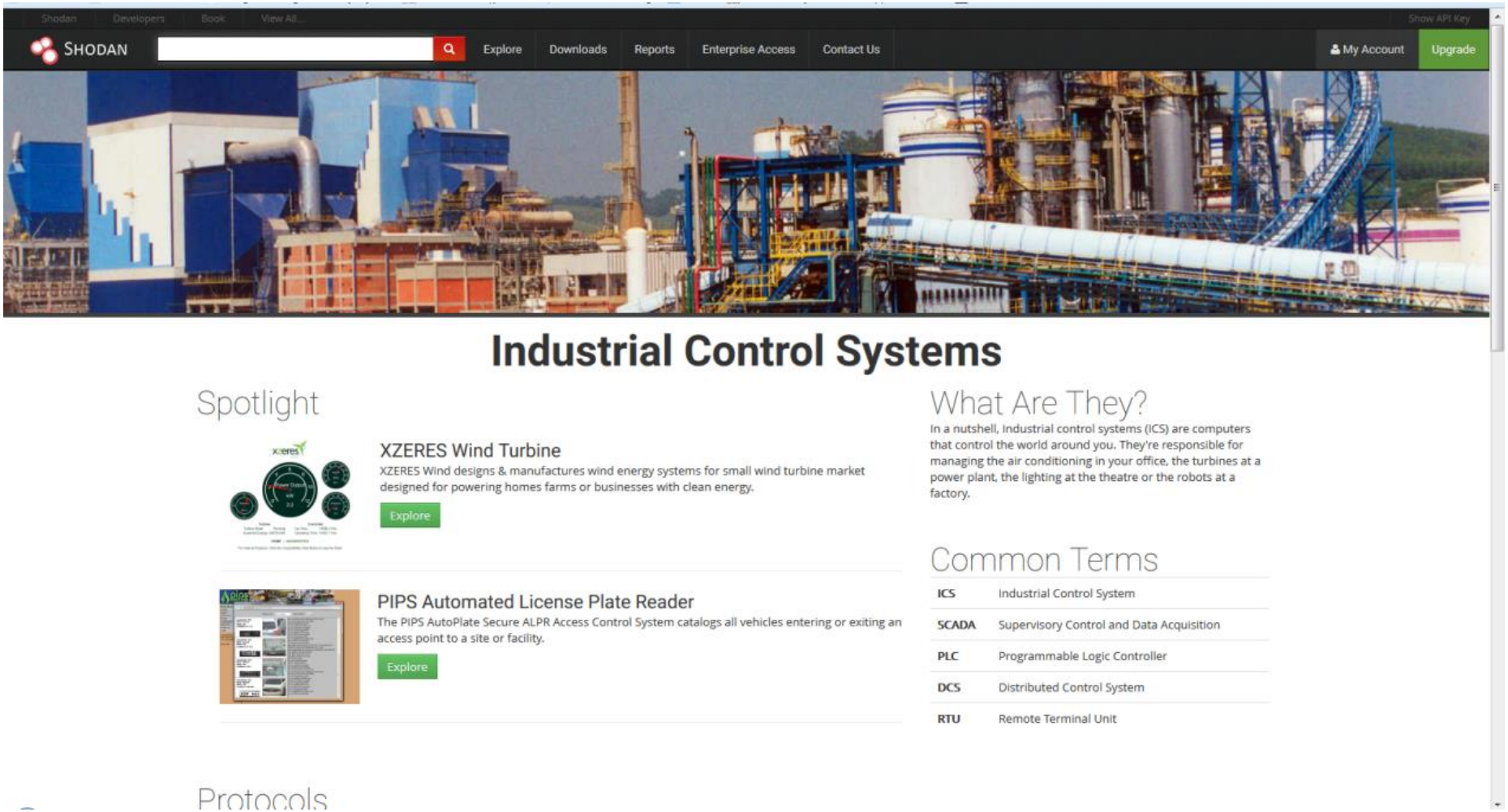
atimorin uploads for Confidence 2014 — Latest commit 8064694 on 26 May 2014

| | | |
|---|---|---|
| README | first commit | 2 years ago |
| get_seed_range.py | uploads for Confidence 2014 | 2 years ago |
| iec-60870-5-104.py | uploads for Confidence 2014 | 2 years ago |
| iec-61850-8-1.py | uploads for Confidence 2014 | 2 years ago |
| iec-identify.nse | uploads for Confidence 2014 | 2 years ago |
| mms-identify.nse | uploads for Confidence 2014 | 2 years ago |
| profinet_scanner.noscapy.py | uploads for Confidence 2014 | 2 years ago |
| profinet_scanner.scapy.py | uploads for Confidence 2014 | 2 years ago |
| profinet_set_fuzzer.py | uploads for Confidence 2014 | 2 years ago |
| profinet_set_network_info.py | uploads for Confidence 2014 | 2 years ago |
| s7-1200_brute_offline.py | uploads for Confidence 2014 | 2 years ago |
| s7-1500_brute_offline.py | uploads for Confidence 2014 | 2 years ago |
| s7-packet-structure.py | uploads for Confidence 2014 | 2 years ago |
| s7-show-payloads.py | uploads for Confidence 2014 | 2 years ago |
| s7_password_hashes_extractor.py | uploads for Confidence 2014 | 2 years ago |
| show_byte_sequences.py | uploads for Confidence 2014 | 2 years ago |

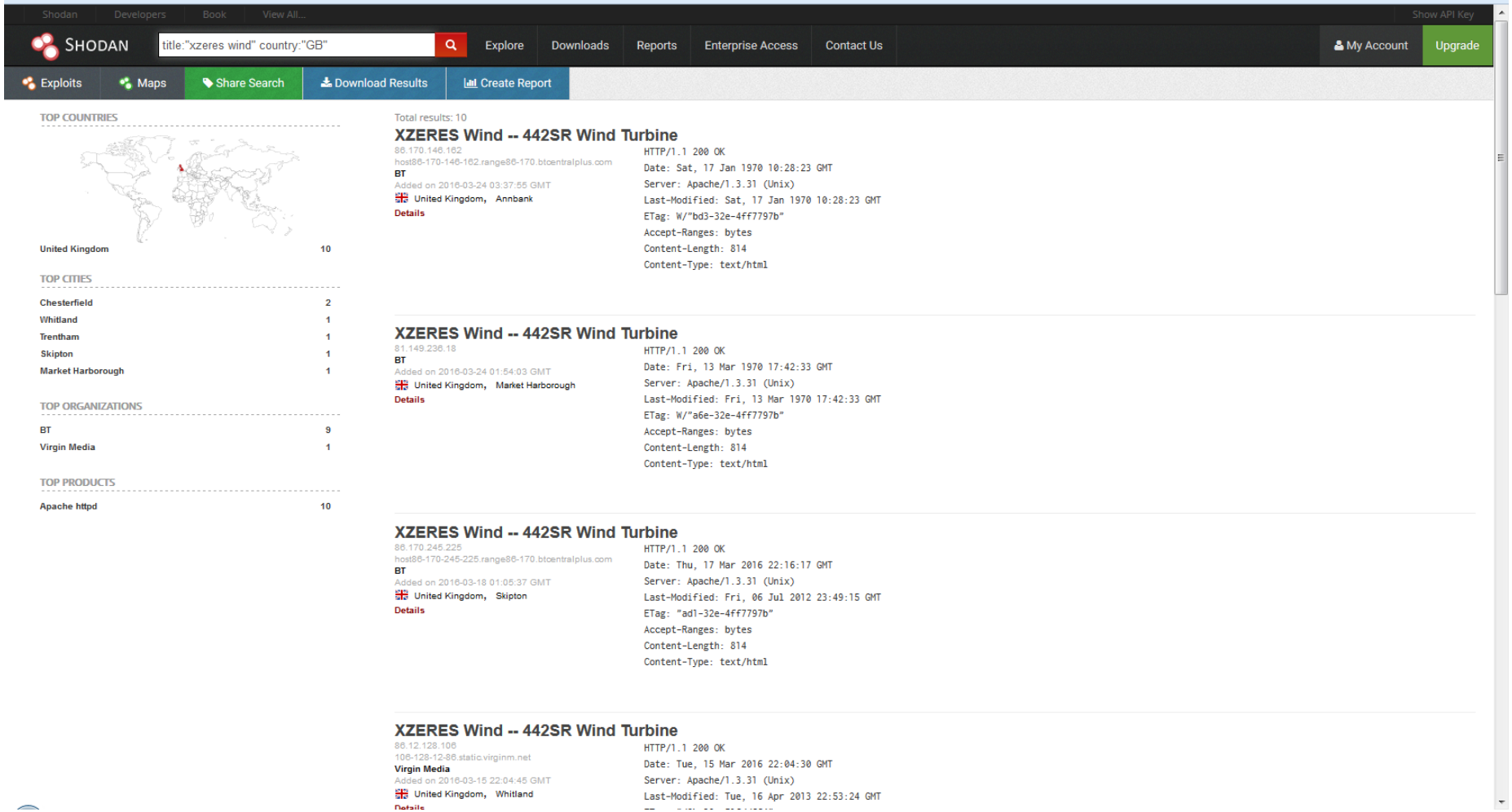
# Enter Shodan



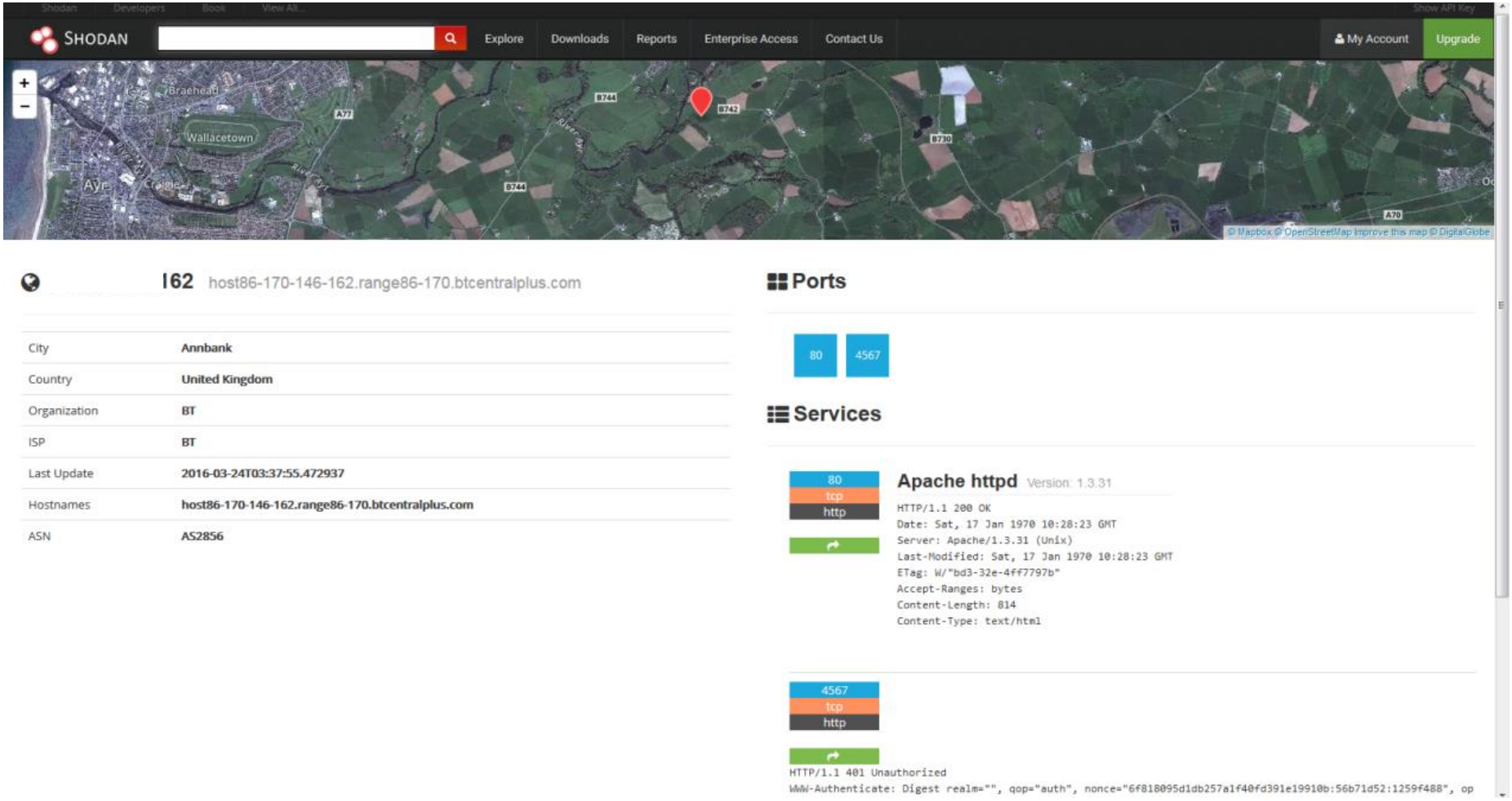
# Enter Shodan



# Enter Shodan



# Enter Shodan

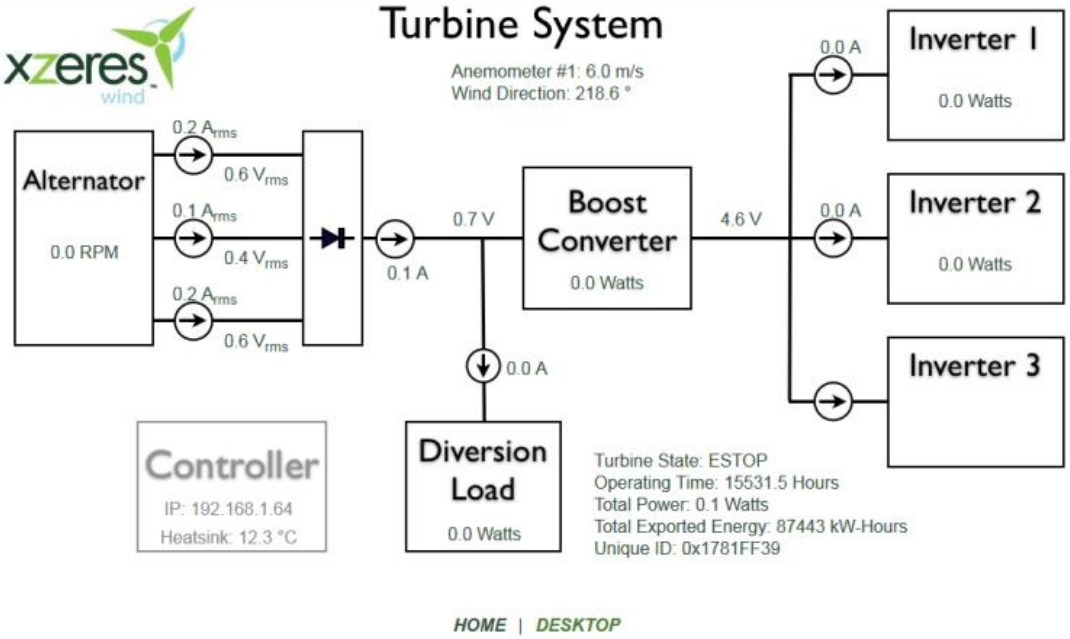


# Enter Shodan

xzeres wind

HOME | DESKTOP | MOBILE | DIAGNOSTICS | INSTALLER | DOCUMENTATION

# Enter Shodan



# Enter Shodan

**Boost Detailed Channel List**

| Channel | Value | Channel | Value |
|---|---|---|---|
| VBOOST | 4.6 | ENABLE_BOOST | OFF |
| DB_OCFLT | 209584 | DB_OVFLT | 0 |
| **Configuration** | | | |
| BOOST_LOOP_P | 512 | BOOST_LOOP_I | 150 |
| INV_LOW_V | 250.0 | | |
| INV_MID_V | 450.0 | INV_MID_P | 1000 |
| INV_MAX_V | 500.0 | INV_MAX_P | 6100 |

***BACK***

# Enter Shodan

# Enter Shodan – Greek WIND farms

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

In other projects
Wikimedia Commons

Languages
Русский
Edit links

Article | Talk | Read | Edit | View history | Search

## Wind power in Greece

From Wikipedia, the free encyclopedia

**Wind power in Greece** was due to expand by 352% by 2010 to meet the European target of 20% coverage of energy needs from renewable sources. Previously, there were 1,028 wind turbines installed throughout Greece and the number was set to reach 2,587 wind turbines before the end of 2010.[1]

According to the Ministry of Environment and Public Works, the system would have a nameplate capacity of 3,372MW of power from wind alone compared to 746MW at the end of 2006.[2] Greece chose to invest primarily to wind power by 77%, while the rest of renewable sources altogether comprise the remaining 23% of production with hydroelectric power being second with 11%.[3][4]

View of a wind farm, Panachaiko mountain.

### Capacity [ edit ]

| Wind Energy Capacity (MW)[5][6] | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Country** | **1998** | **1999** | **2000** | **2001** | **2002** | **2003** | **2004** | **2005** | **2006** | **2007** | **2008** | **2009** | **2010** | **2011** | **2012** | **2013** | **2014** |
| Greece | 39 | 112 | 189 | 272 | 297 | 383 | 473 | 573 | 746 | 871 | 985 | 1,087 | 1,208 | 1,634 | 1,749 | 1,865[7] | 1,980 [8] |

### See also [ edit ]

- Energy in Greece

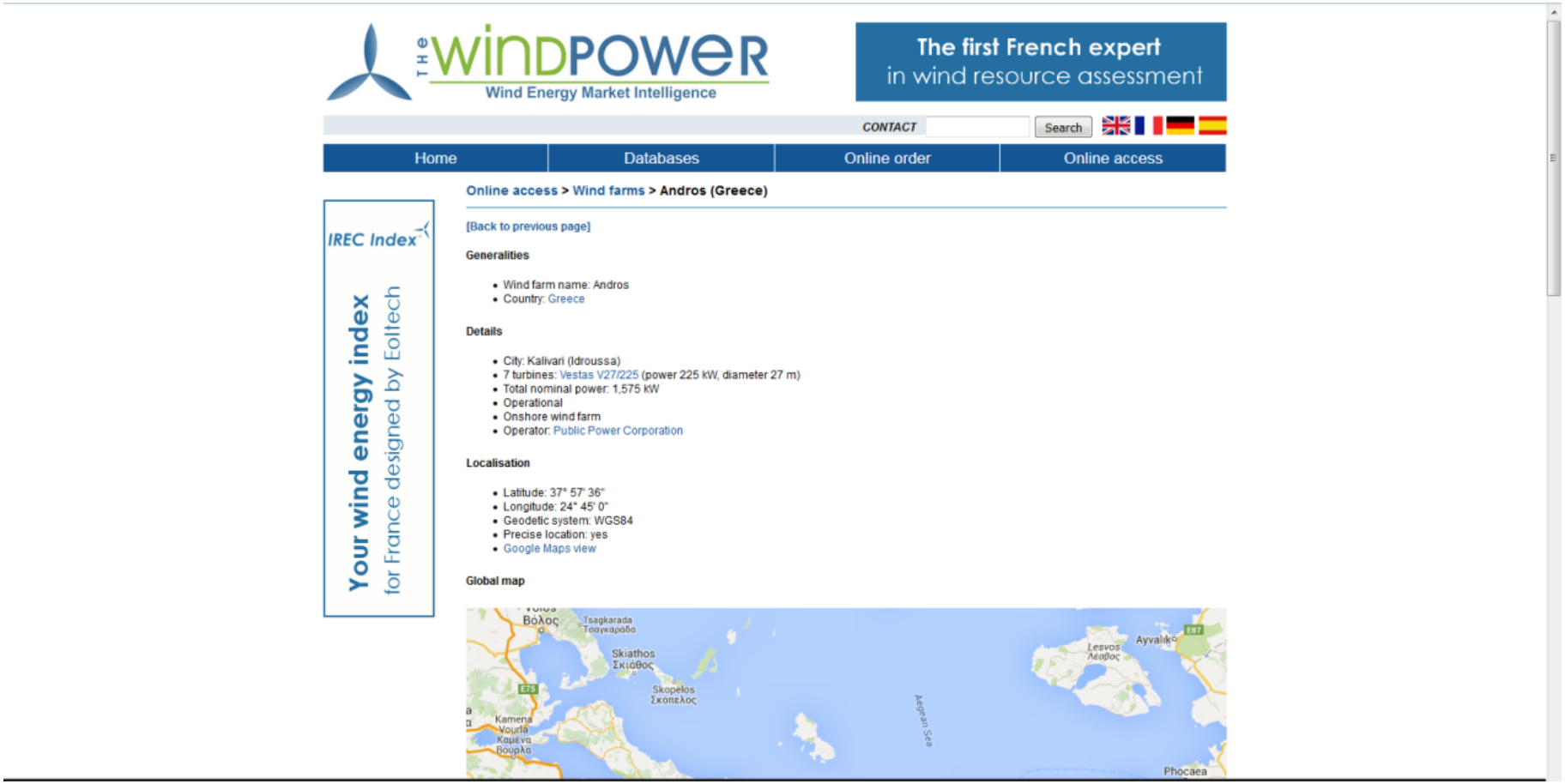
### Sources [ edit ]


1. ^ Greece commits for 2,587 wind turbines
2. ^ Rising to the Challenge:the growth of wind power generation in Greece
3. ^ Greek Ministry of Environment
4. ^ Greece Renewable Energy - Europa Fact Sheet
5. ^ EWEA Staff (2010). "Cumulative installed capacity per EU Member State 1998 - 2009 (MW)". European Wind Energy Association. Retrieved 2010-05-22.
6. ^ EWEA Staff (February 2011). "EWEA Annual Statistics 2010" (PDF). European Wind Energy Association. Retrieved 2011-01-31.
7. ^ Greek wind power market picks up again
8. ^ http://eletaen.gr/wp-content/uploads/2015/01/2014_-HWEA_Statistics_Greece.pdf

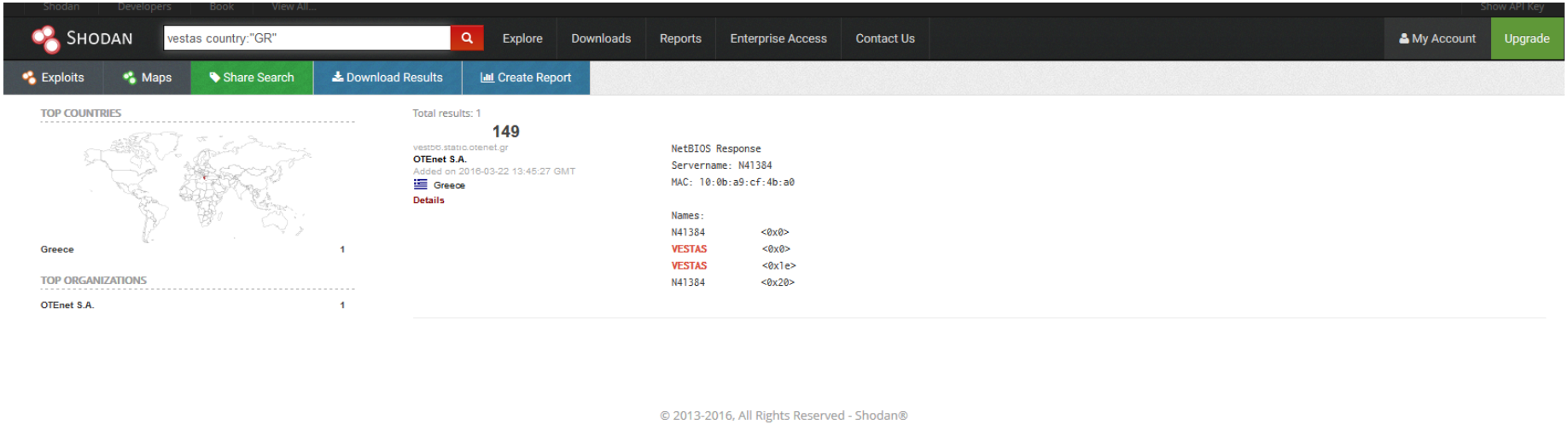

| | | |
|---|---|---|
| v·t·e | **Wind power** | [show] |
| v·t·e | **Wind power by country** | [show] |
| v·t·e | **Renewable energy by country** | [show] |

Categories: Wind power in Greece

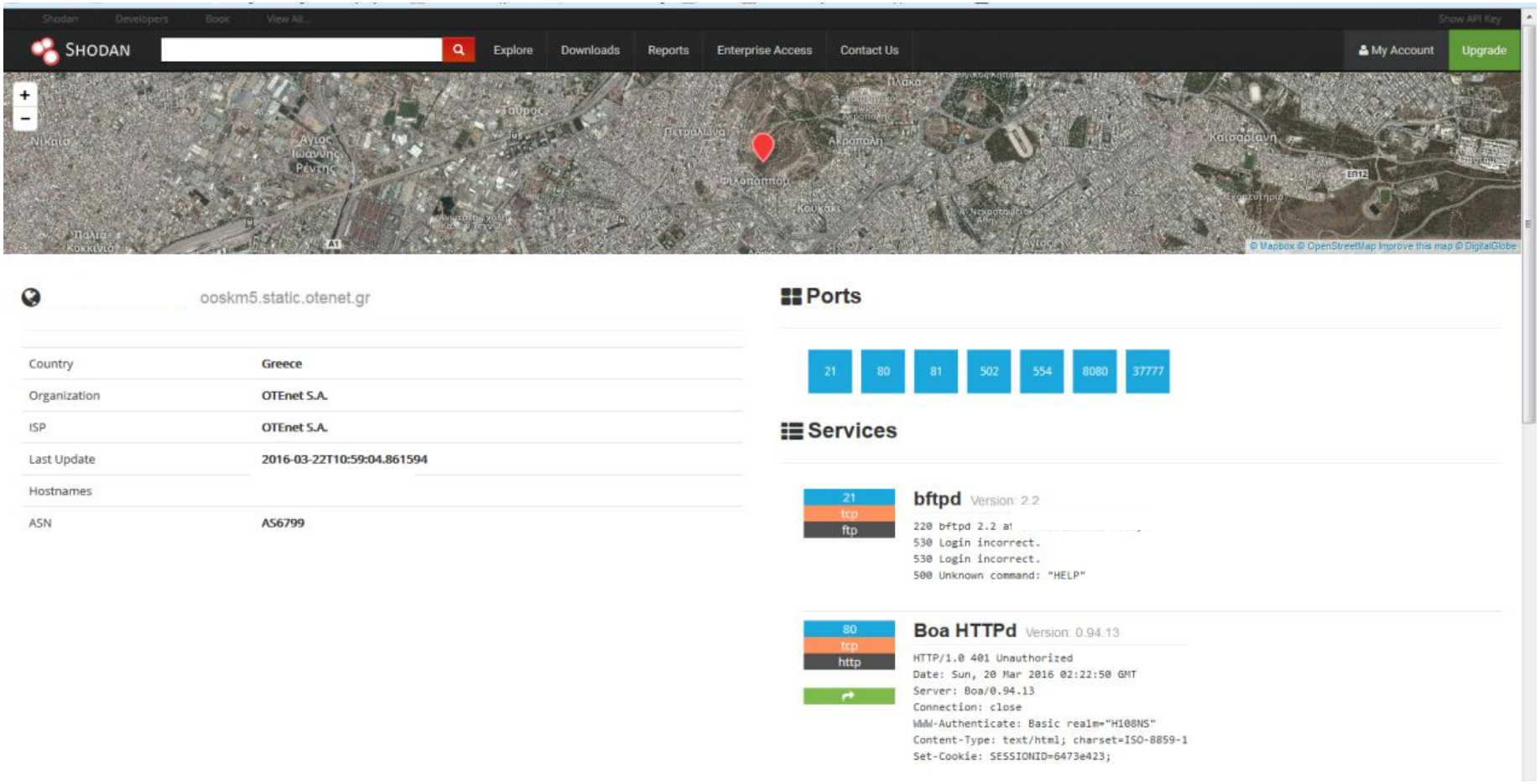
# Enter Shodan – Greek WIND farms



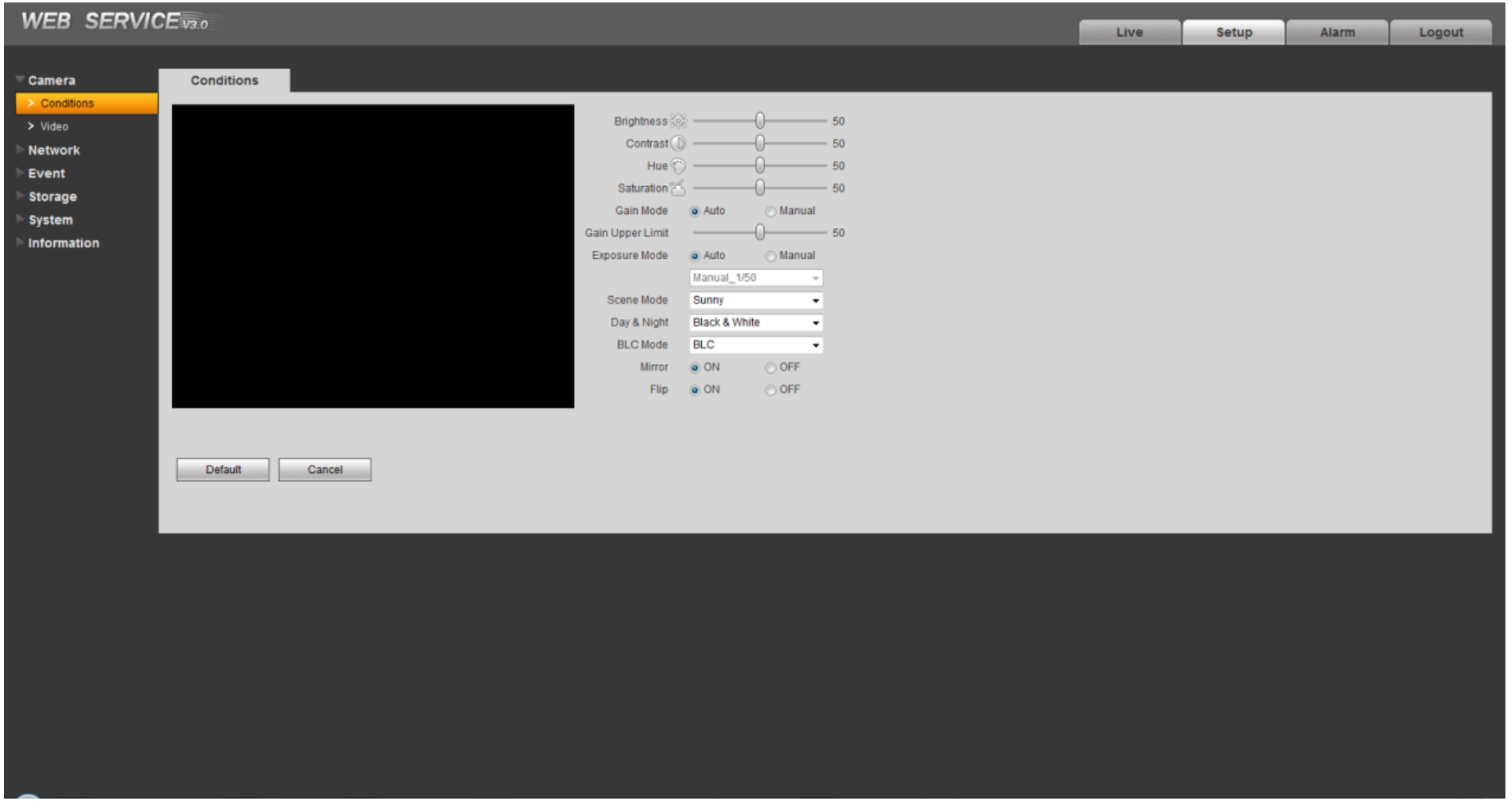
# Enter Shodan – Greek WIND farms



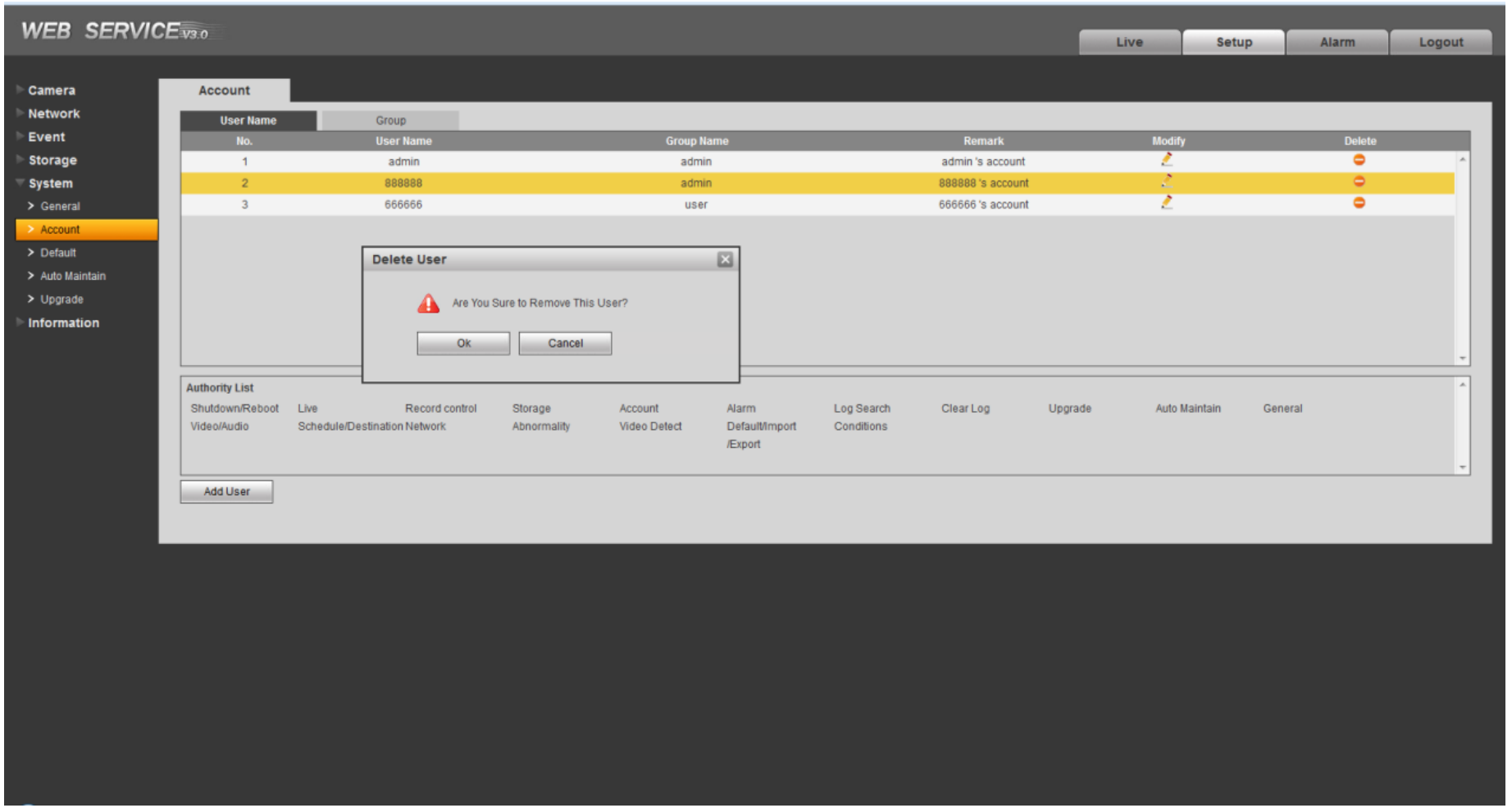
# Enter Shodan – Greek WIND farms



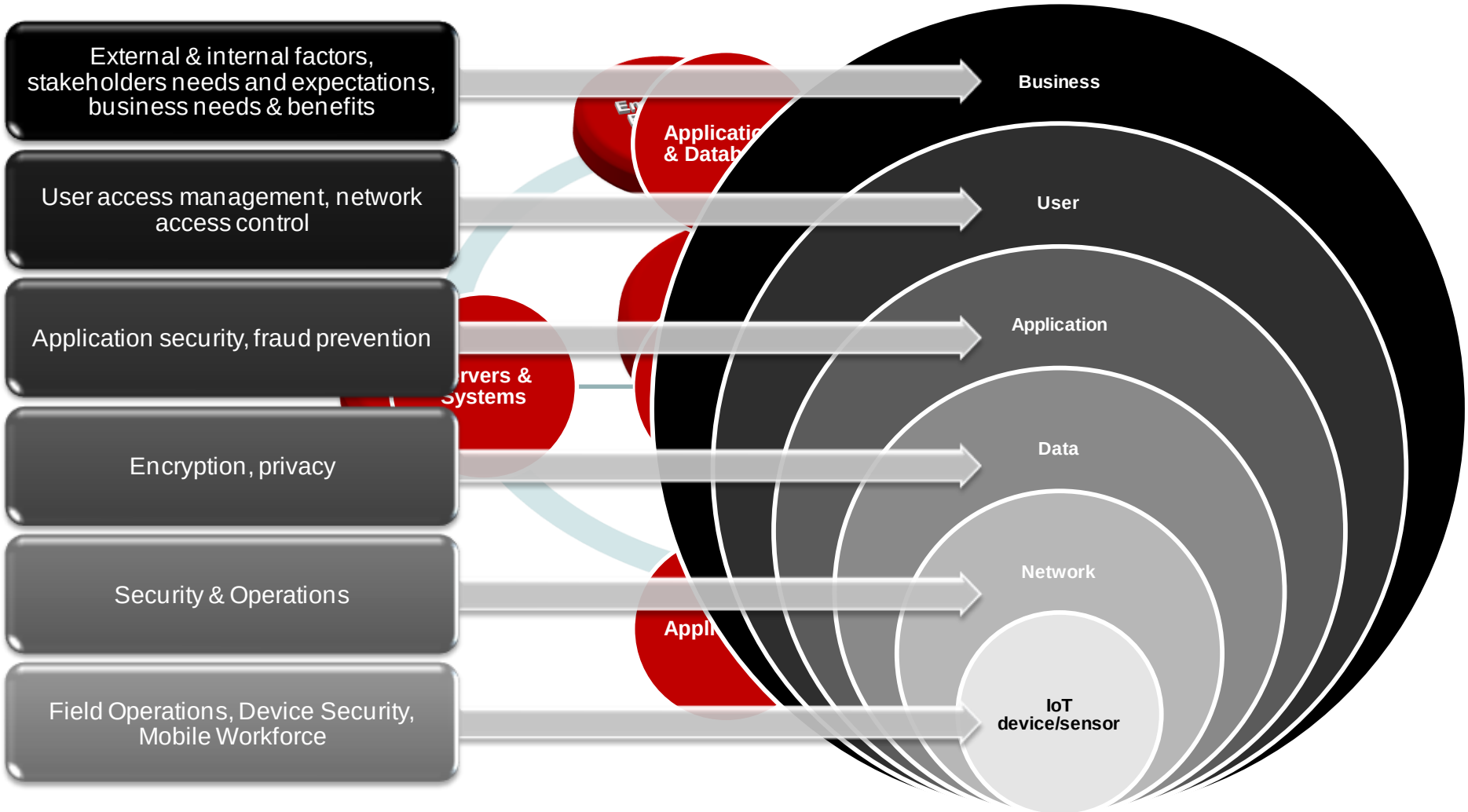
# Enter Shodan – Greek WIND farms



# Enter Shodan – Greek WIND farms

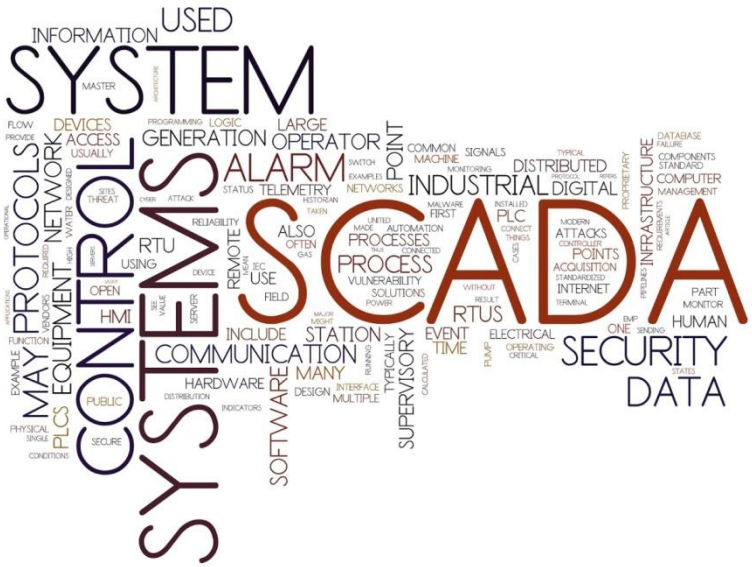


# Addressing Converged Security [1]

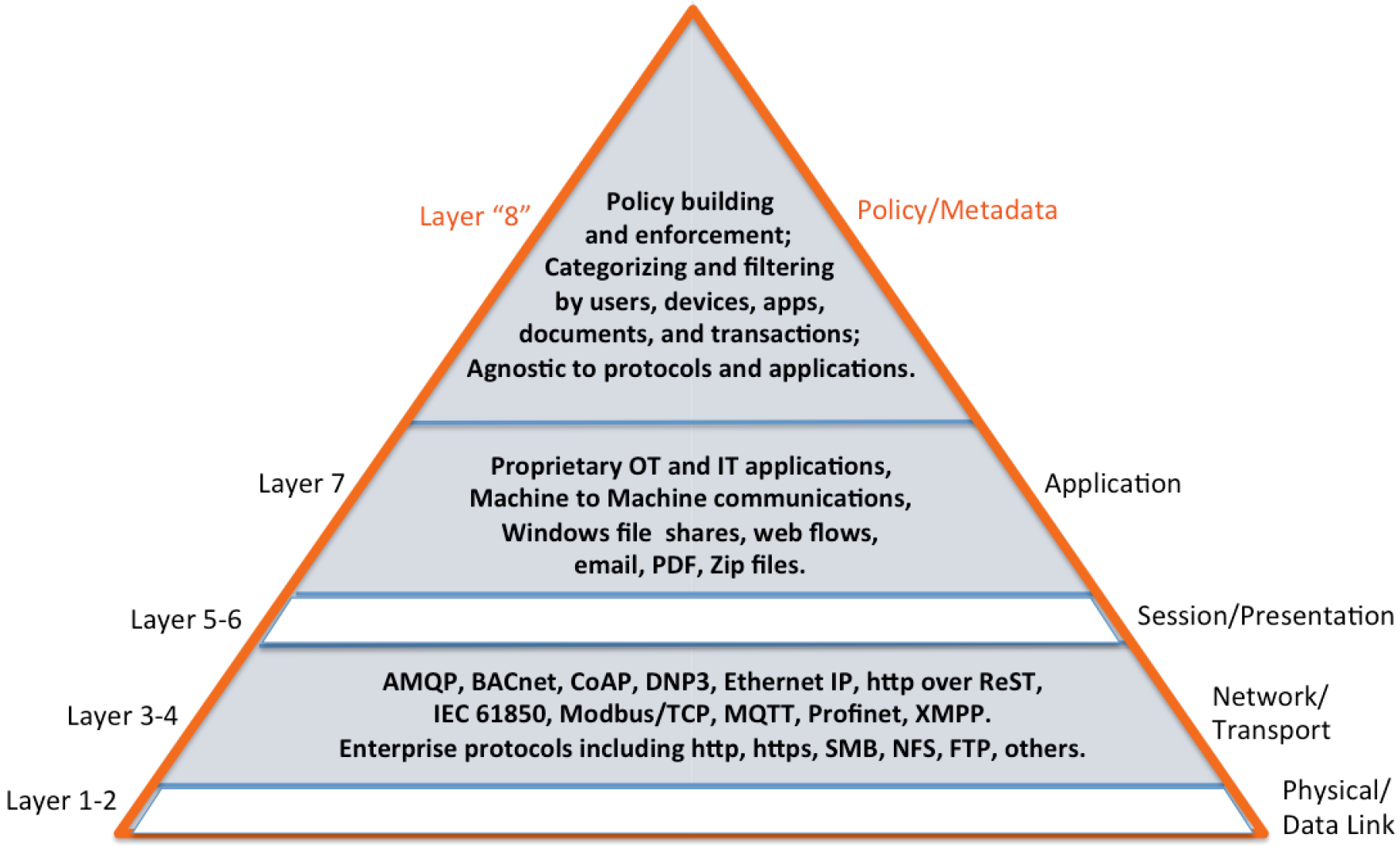


# Addressing Converged Security [2]

- Content-based rules policy engine platform
- Safety and Security Policy Enforcement
- Support for major industrial standards
- Deep Packet Inspection and filtering of industrial IoT protocols
- Understanding of OT and what needs to be protected

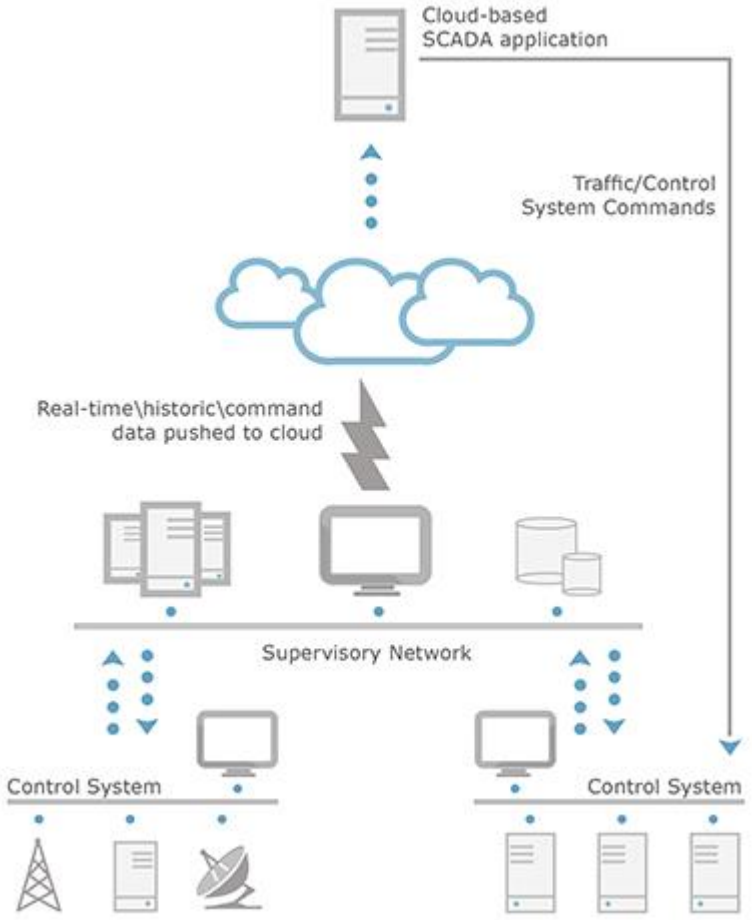


# Addressing Converged Security [3]



# Addressing Converged Security [4]

- Cloud-based platforms
- Cloud Federation
- Partnerships with service providers
- Legal and regulatory requirements (data protection, etc)




*Source: TrendMicro*

# Summary

- Operations Technology  (OT) environment features unique characteristics
- IT and OT security must be addressed in a converged manner
- New challenges, new approaches, new capabilities
- Intracom Telecom is the trusted advisor for the industrial cybersecurity sector
- Intracom Telecom is the cloud enabler and provider to fulfill IIoT requirements

# thank you

For more information, visit

www.intracom-telecom.com

INTRACOM TELECOM

Follow | Link | Watch