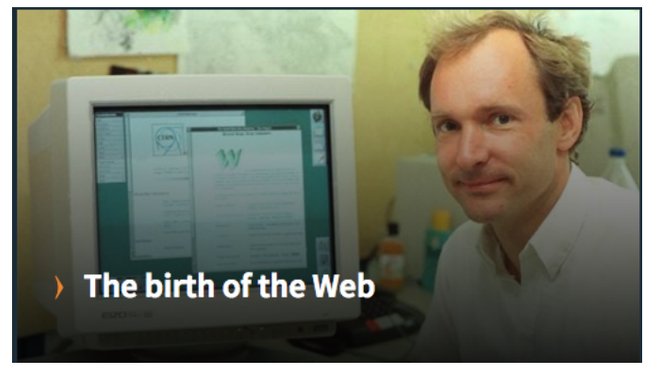
European Organization for Nuclear Research

CERN Globe of Science

Major inventions done at CERN-

1. Invention of the World Wide Web (www)



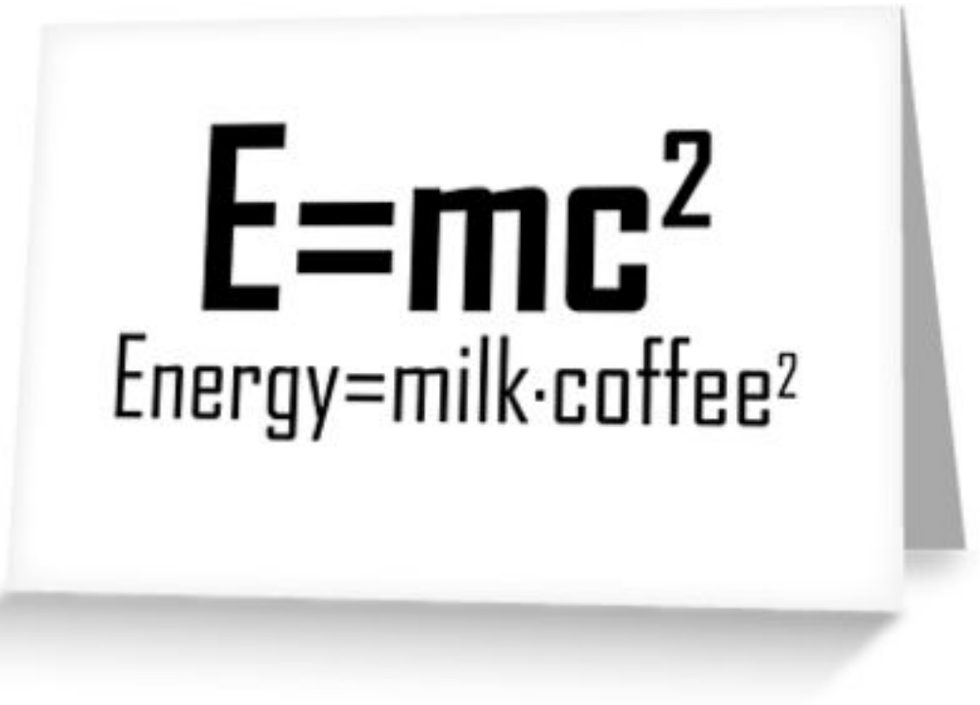
2. Discovery of the Higgs Boson (God Particle)

3. Large Hadron Collider

4. Antimatter

5. The High Luminosity LHC (HL-LHC)

No, I'm not a physicist



Before I joined CERN,
I also thought that scientists/physicists are boring

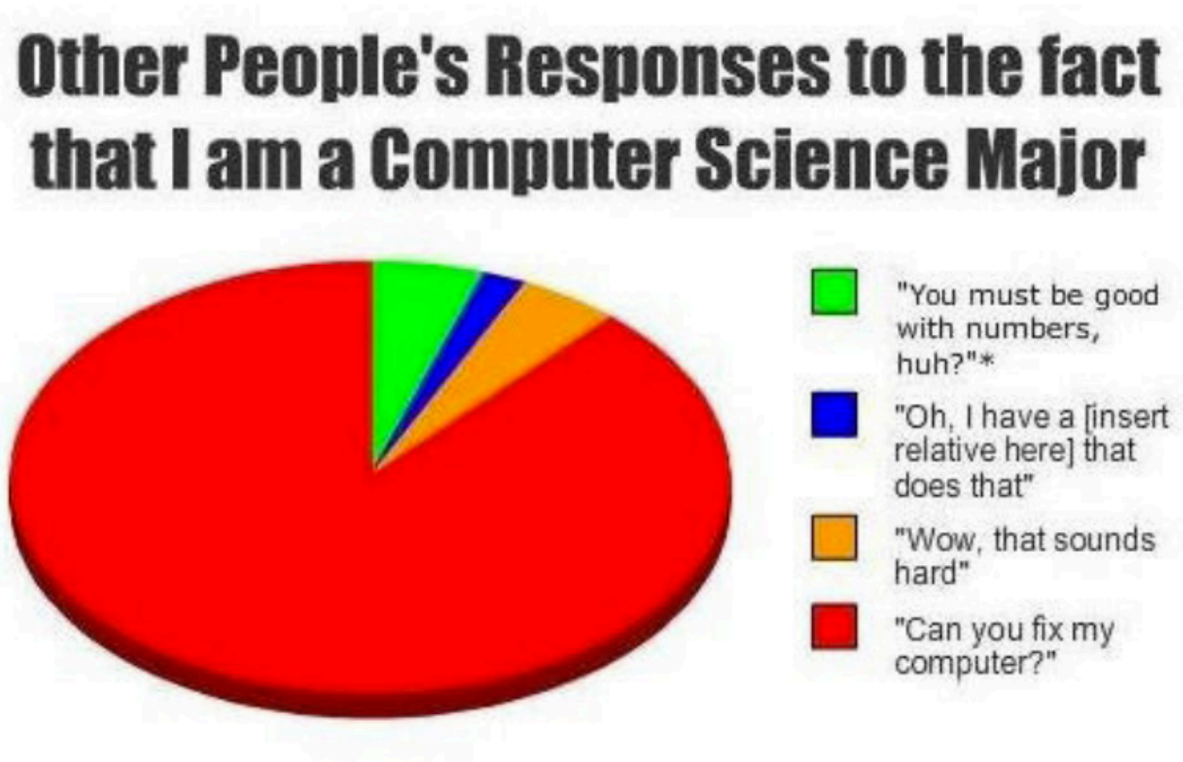
Sharad Agarwal

Computer Science Researcher working at CERN employed by the University of Wisconsin Madison, USA

https://sharad1126.github.io

Reach me @ sharad.agarwal@cern.ch

That’s not what I exactly do!



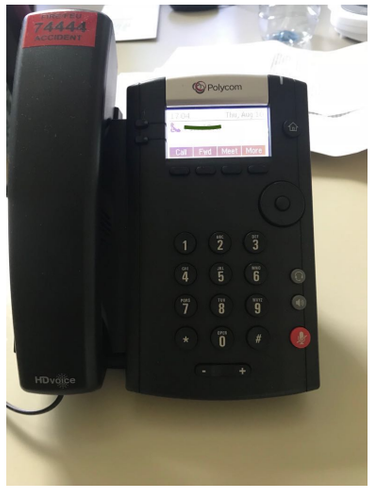
Internet of Things

where the web meets the physical world

Printer

Acces Card Reader

Media Layer Controller



IP Phones

Routers

CCTV Cameras

Sharad Agarwal

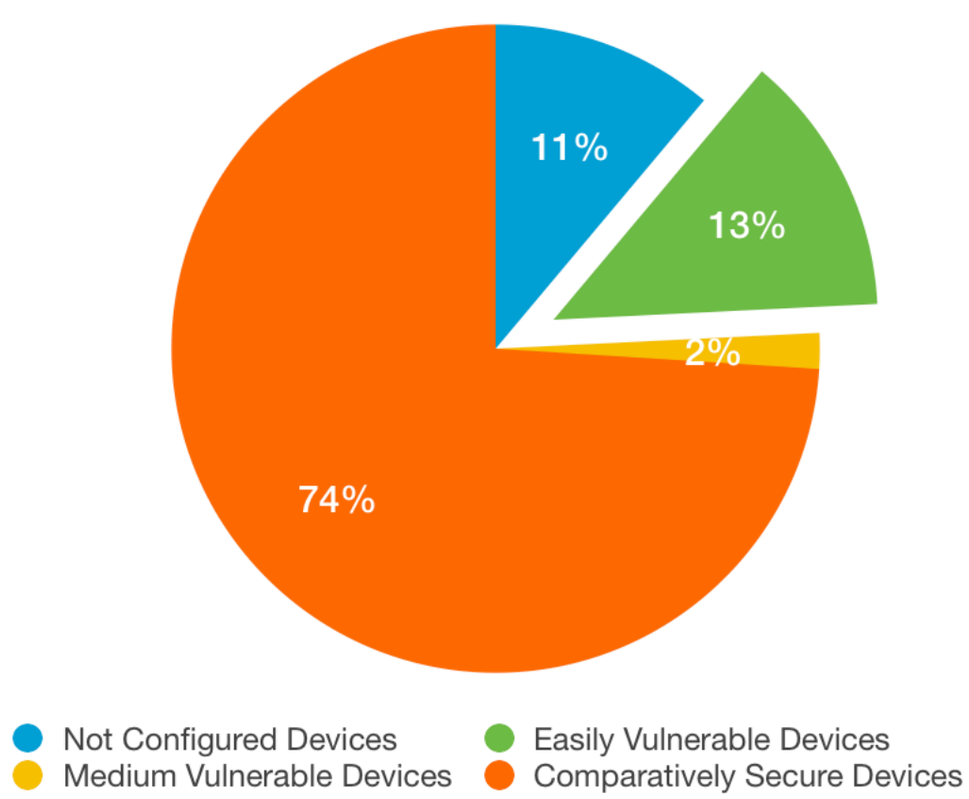
| IoT Security and CMS Workflow Management

CERN has approximately 900 IoT Devices connected on the General Purpose Network (GPN).

IoT Devices in CERN

TYPES	NO. OF DEVICES
Not Configured Devices	100
Easily Vulnerable Devices	118
Medium Vulnerable Devices	16
Comparatively Secure Devices	666

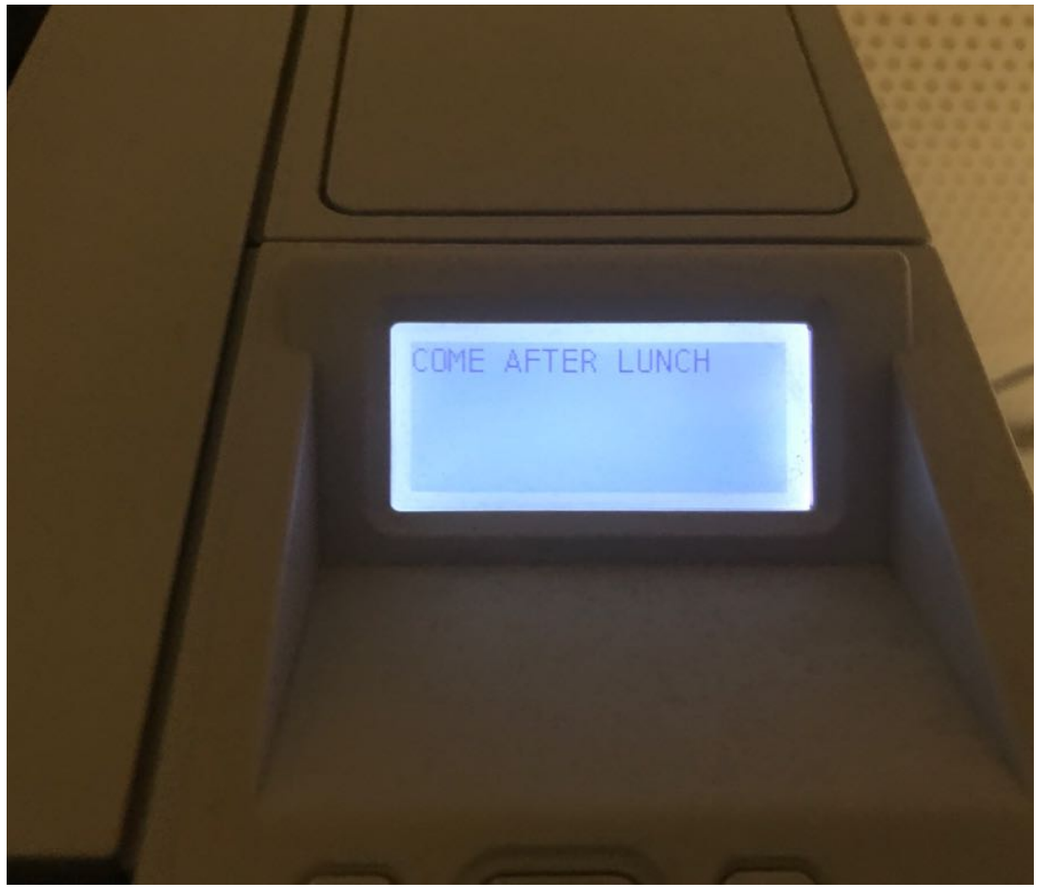
Overview of Vulnerable IoT Devices



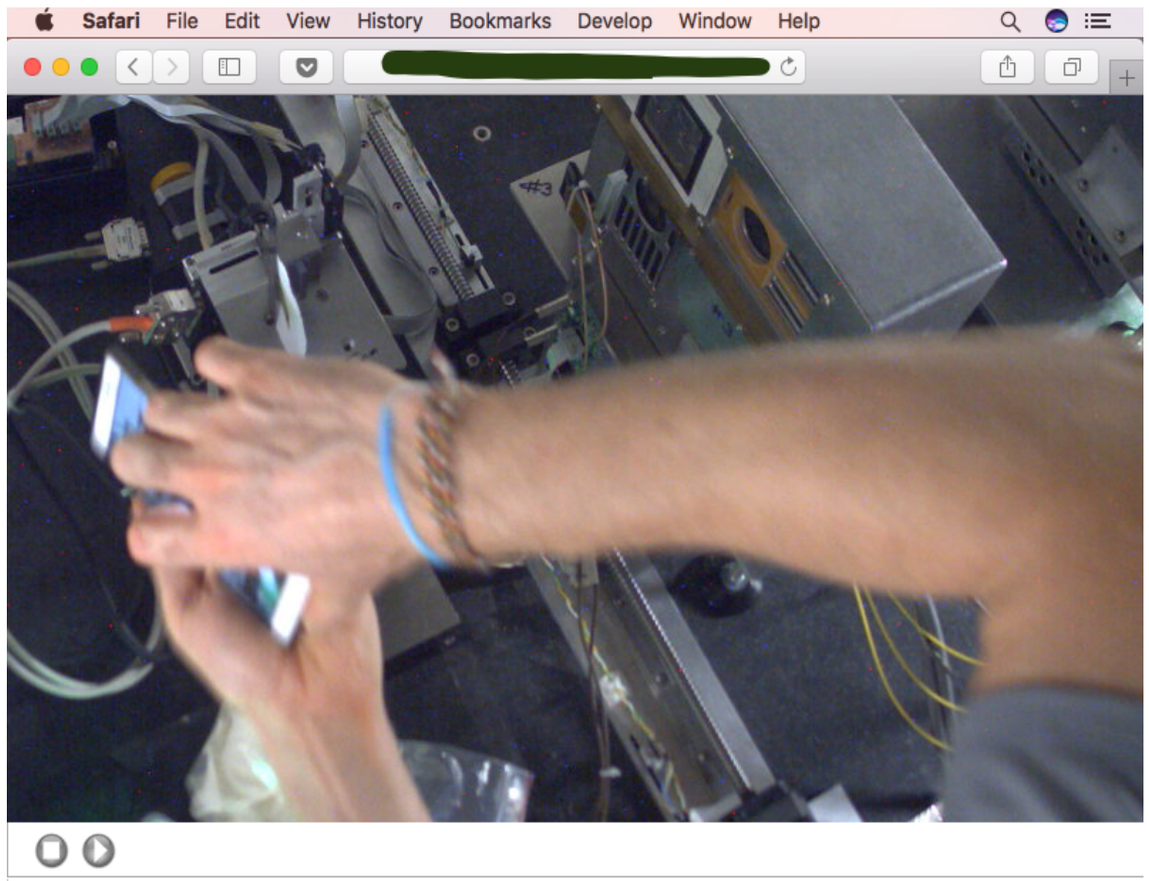
Devices at CERN

1. Switches
2. Routers
3. Thermometers
4. Programmable Logic Controller
5. Webcams/Close Circuit Television Cameras
6. Sensors
7. Oscilloscopes
8. IP Phones
9. Anywhere USB
10. Network Attached Storage
11. Printers
12. Projectors
13. Media Layer Controllers
14. Conference Mics
15. Integrated Lights Out
16. Infoscreens
17. Power Supply
18. Arduinos
19. Raspberry Pi and more

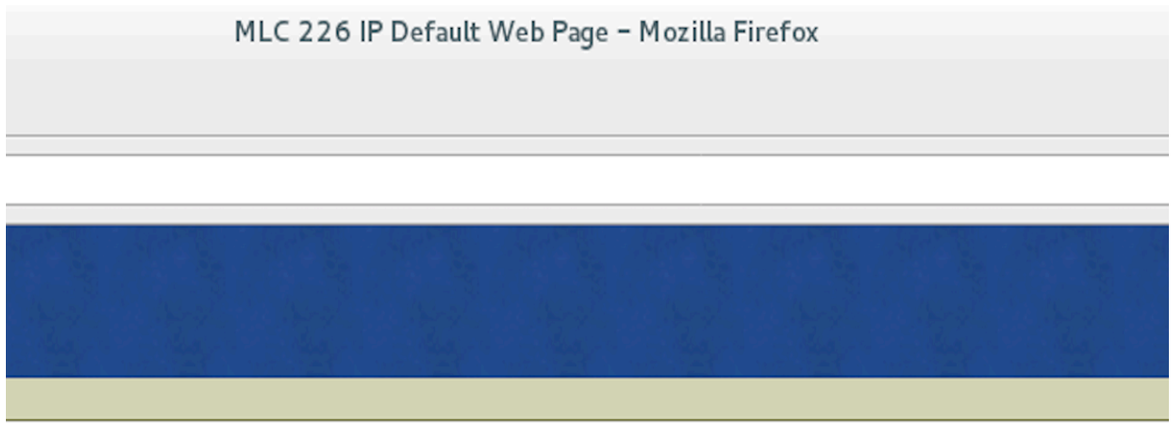
Let's look into some cases of vulnerable devices found in CERN



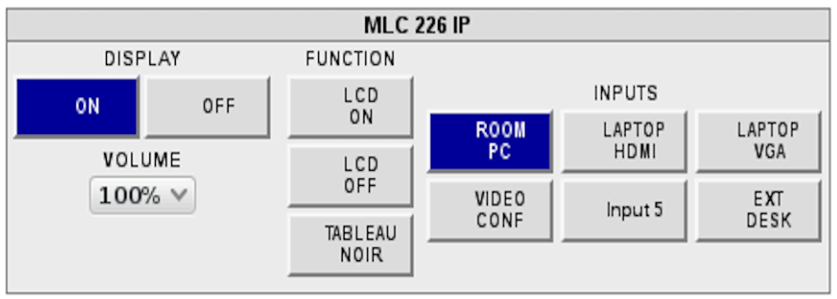
Printers - where I was able to write anything on the display screen



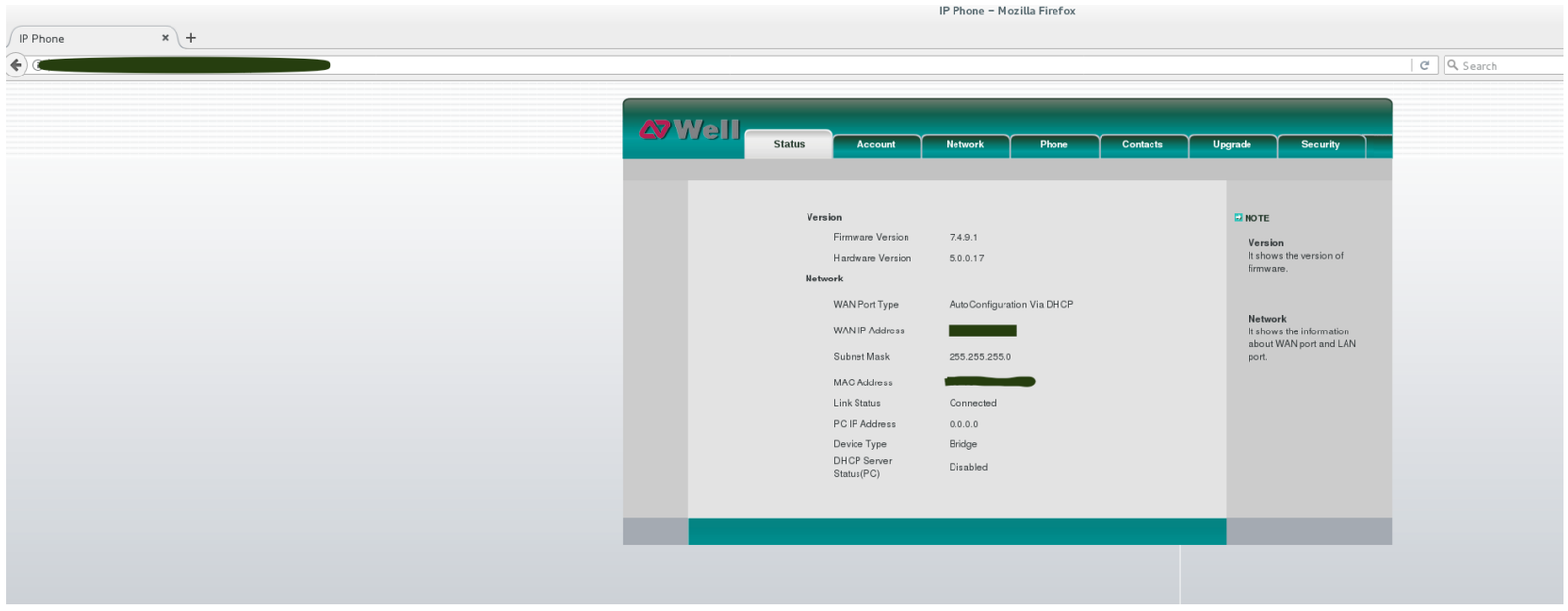
Real time streaming CCTV Camera



Conference room controllers

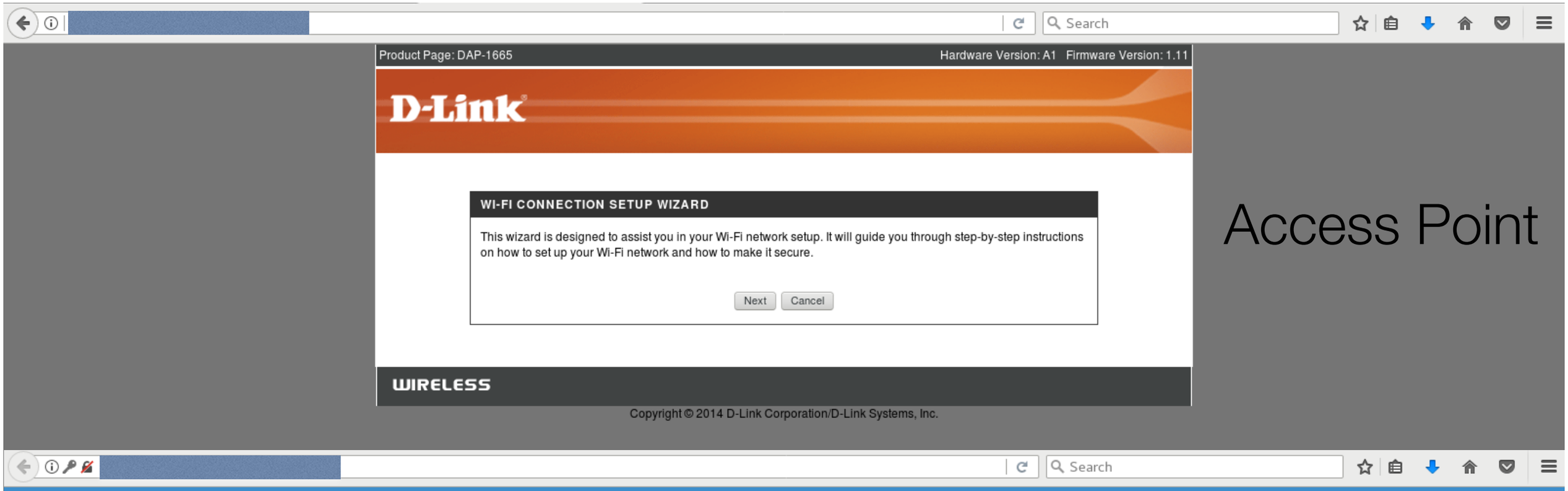


IP Phone

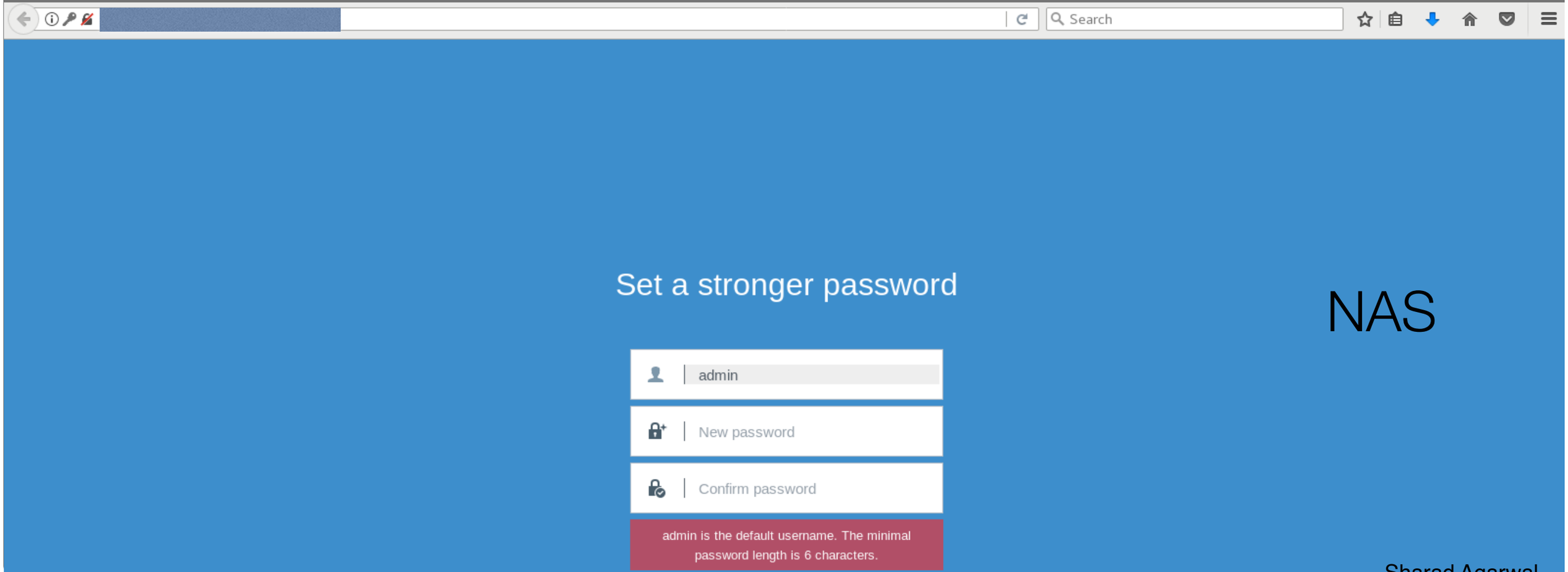


Non Configured Devices

| IoT Security and CMS Workflow Management



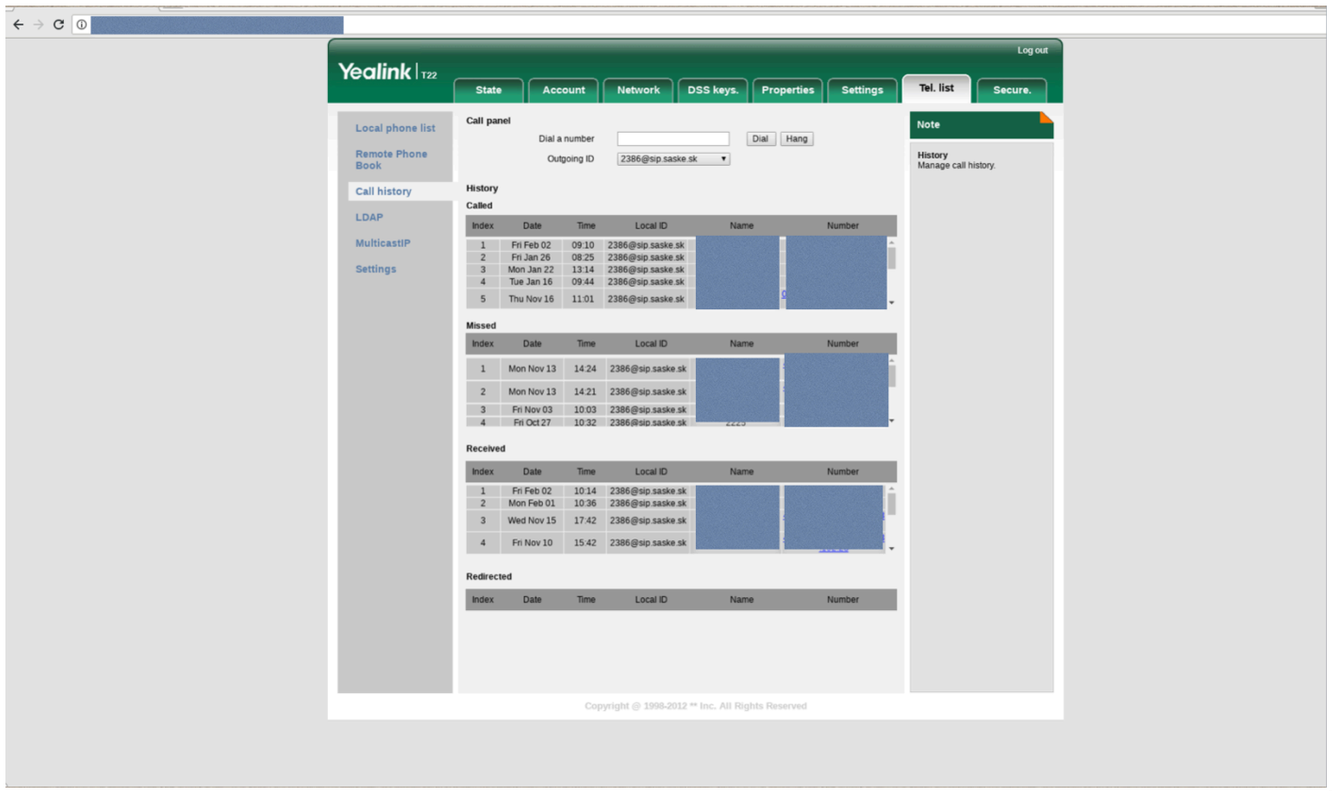
Access Point



NAS

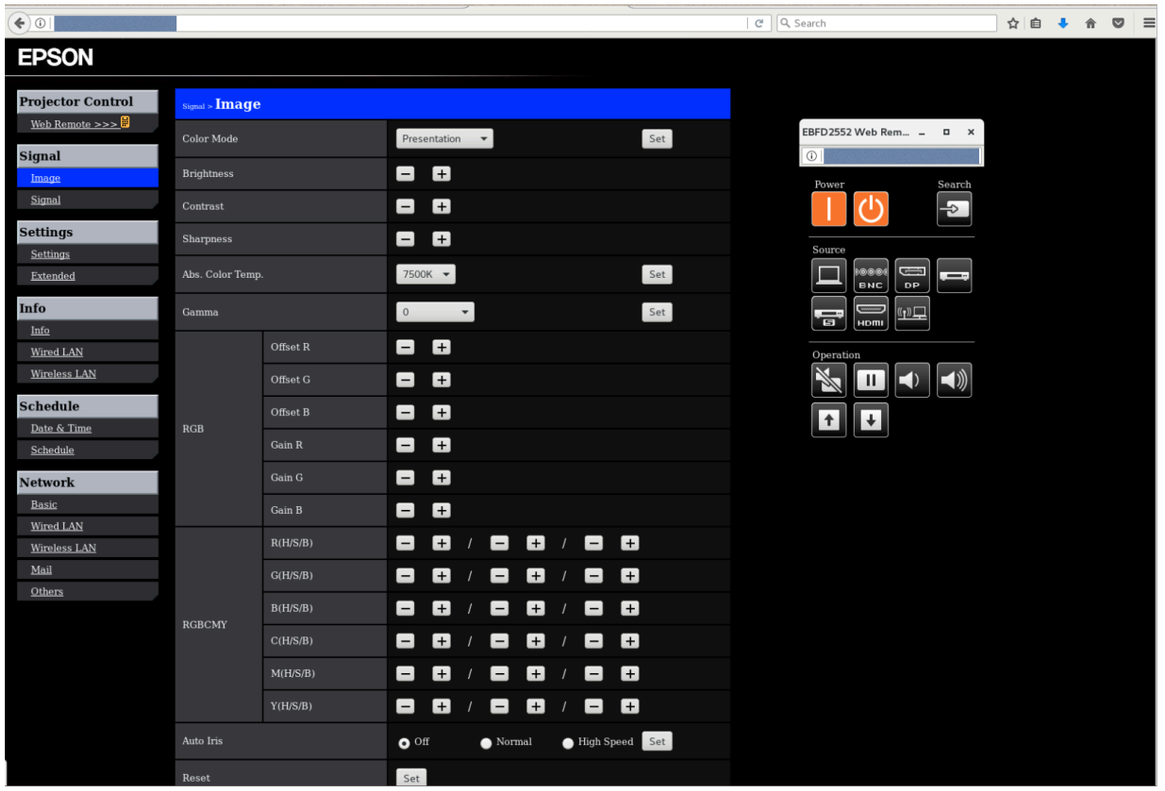
Easily Vulnerable Devices

| IoT Security and CMS Workflow Management



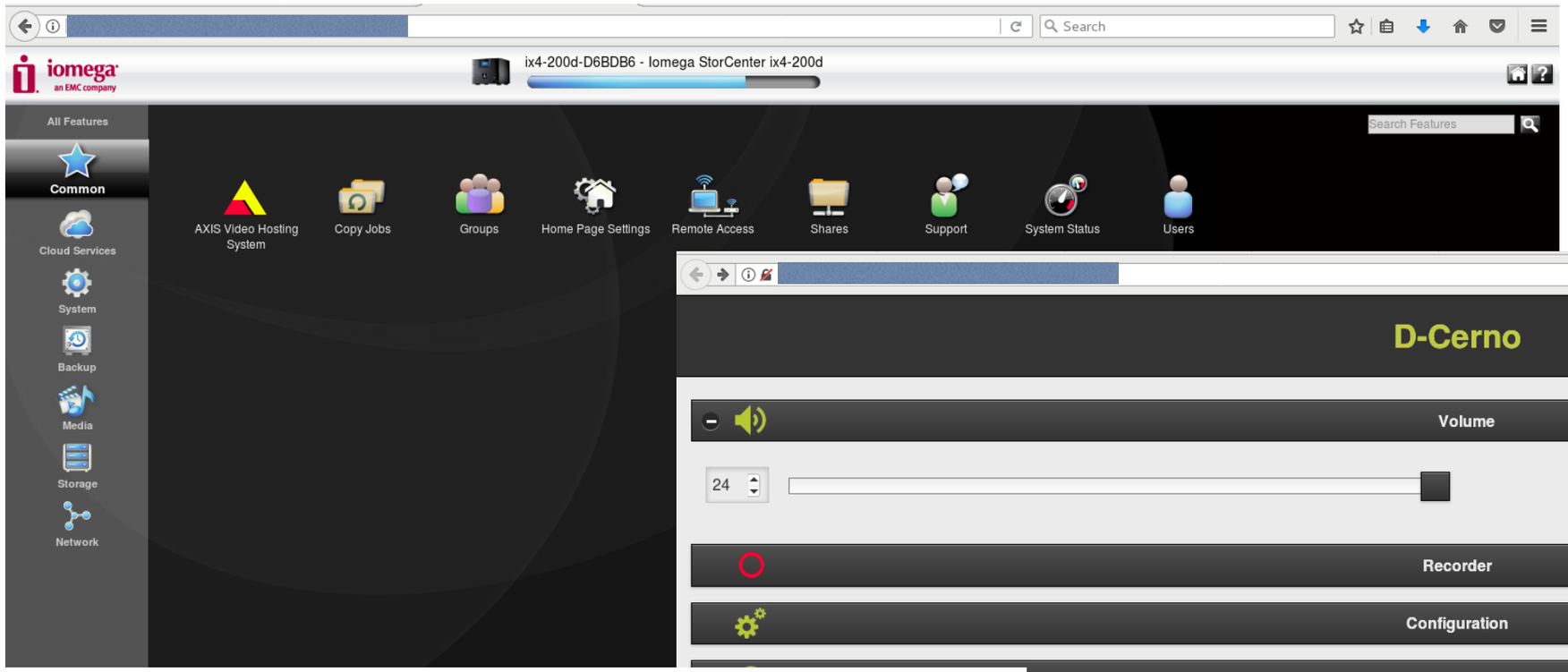
IP Phones - Can access contacts,
call logs and use it to call

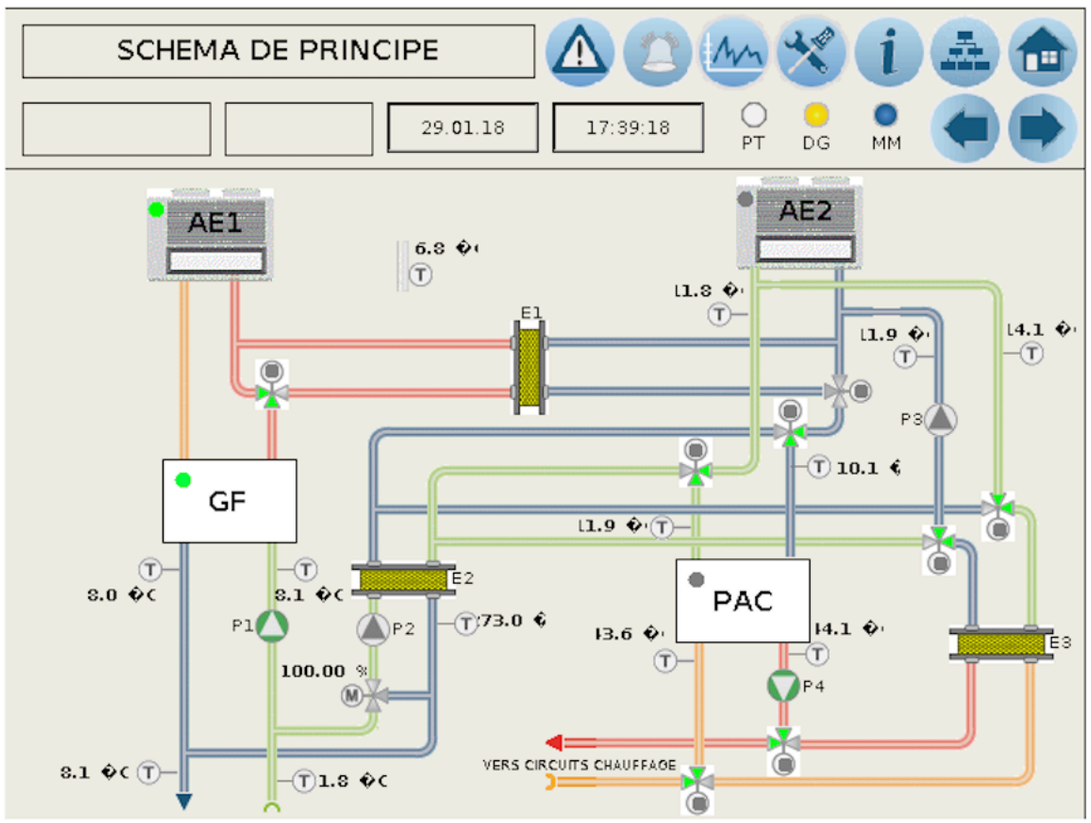
Projectors used in meeting rooms



Sharad Agarwal

| IoT Security and CMS Workflow Management





And Many More

Sharad Agarwal

Medium Vulnerable Devices

| IoT Security and CMS Workflow Management

We have developed a tool that detects IoT Devices and provides model, manufacturer, and firmware details which will be used to predict the security risk score for an IoT device

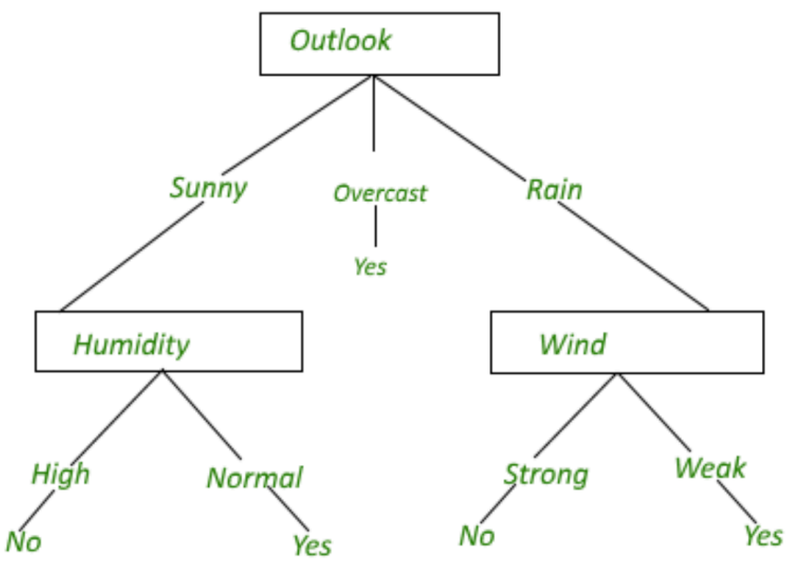
So how we did this :

1. Developed a Machine Learning tool which uses Random Forest Algorithm using TCP Timestamps with a precision of 93.61% and accuracy of 99.67%

2. Developed a tool which analyses webpages to detect the IoT devices and gives manufacturer, model name and firmware version and store these details in a JSON file.

Random Forest Algorithm

- Supervised Learning Approach
- Builds Multiple decision trees and merges them together to to get a more accurate and stable precision



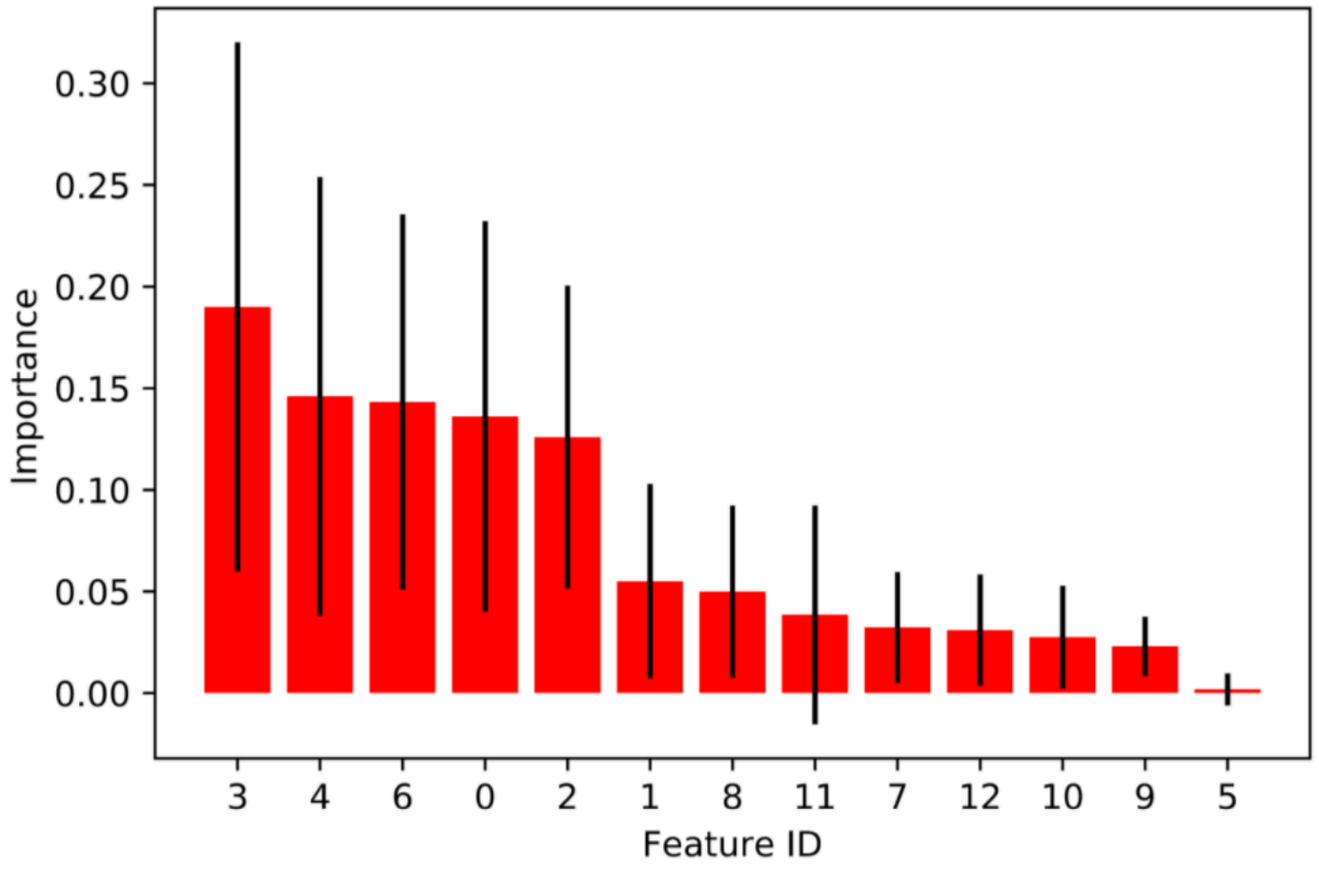
Decision Tree

- Decision Tree generally formulates a set of rules and predicts the result
- The Random Forest algorithm randomly selects observations and features to build several decision trees and then averages the results

Dataset of devices at CERN used for the ML Tool

Device Class	Models	Quantity	Training set	Test set	Validation set
Arduino	1	4	225	49	14
IP to serial converter	1	4	787	224	58
IP phone	1	2	68	9	7
Light management	1	11	63	22	3
Network attached storage	16	35	4021	1054	294
Oscilloscope	1	2	70	21	9
Printer	11	390	78903	21006	5231
Projector	3	12	384	111	28
Telepresence system	4	37	2934	795	195
Video streaming system	1	25	12177	3263	810
Webcam	11	40	2416	658	155

Feature importance for classifiers



Web Analysis for detecting IoT Devices

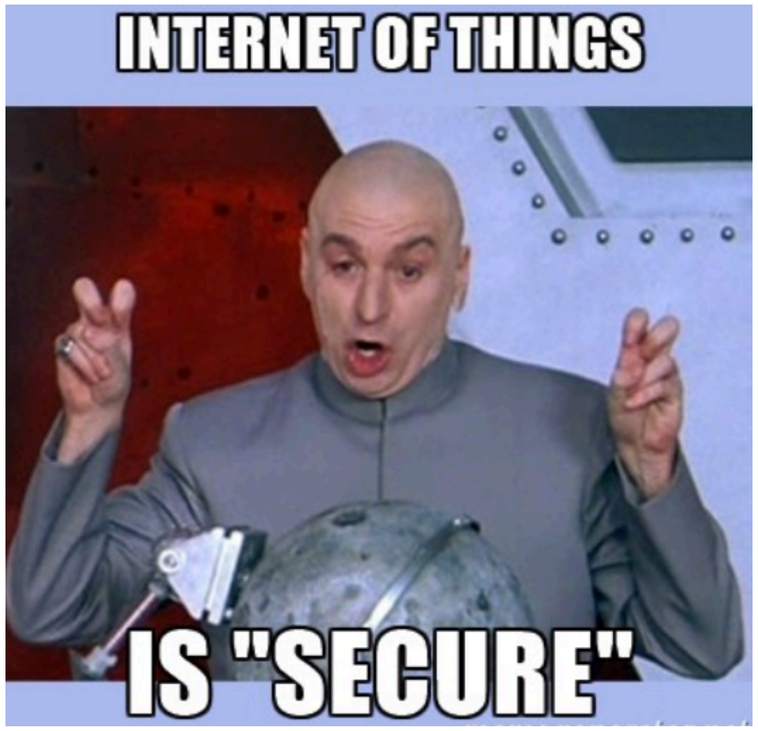
- Scan the General Purpose Network at CERN to detect the IoT Devices
- After trying a lot of popular web scrapping methods - wget, curl, scrapy, python request package, etc, we found the final solution as selenium with chrome driver
- Analysed a lot (100s) of webpages manually
- Detected the Manufacturer, Model and Firmware version of the device
- Constructed a tool to automate the the output of IoT device detection using BeautifulSoup

Output of the Web Analysis Tool

```
sharad:iot_html_analysis SharadAggrawal$ python device_recog.py --ip <ip address>
Matrox Device Found
Firmware: 2.2.0.0008
Model: Monarch HD

classifiers:

<title>
        <device name>
</title>
<span id="ctl00_MainContent_DeviceNameLabel"><device name></span>
<span class="MatroxHD">
<img alt="Matrox MonarchHD" src="images/MonarchHDLogoSmall.png" style="float: right"/></span>
http:// <ip address> /Monarch/About.aspx
<span id="ctl00_MainContent_FirmwareRevisionLabel">2.2.0.0008</span>
sharad:iot_html_analysis SharadAggrawal$
```



Finally after the development of these tools, now we are working to predict the Security Risk Score of these IoT Devices

Compact Muon Solenoid

Scientific Researcher in the Production and Reprocessing in offline computing

Sharad Agarwal

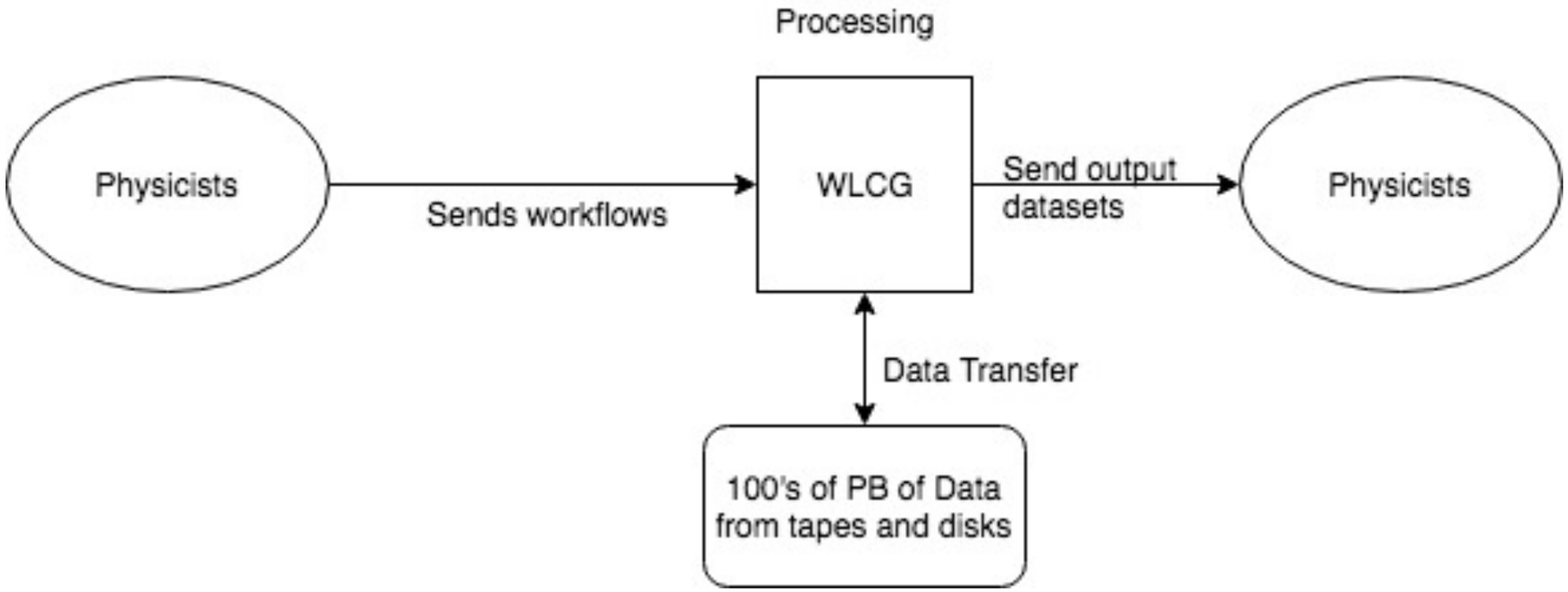
We at CMS work in collaboration with

Fermilab

DESY.

What we do -> Workflow Management

Overview - Workflow Management

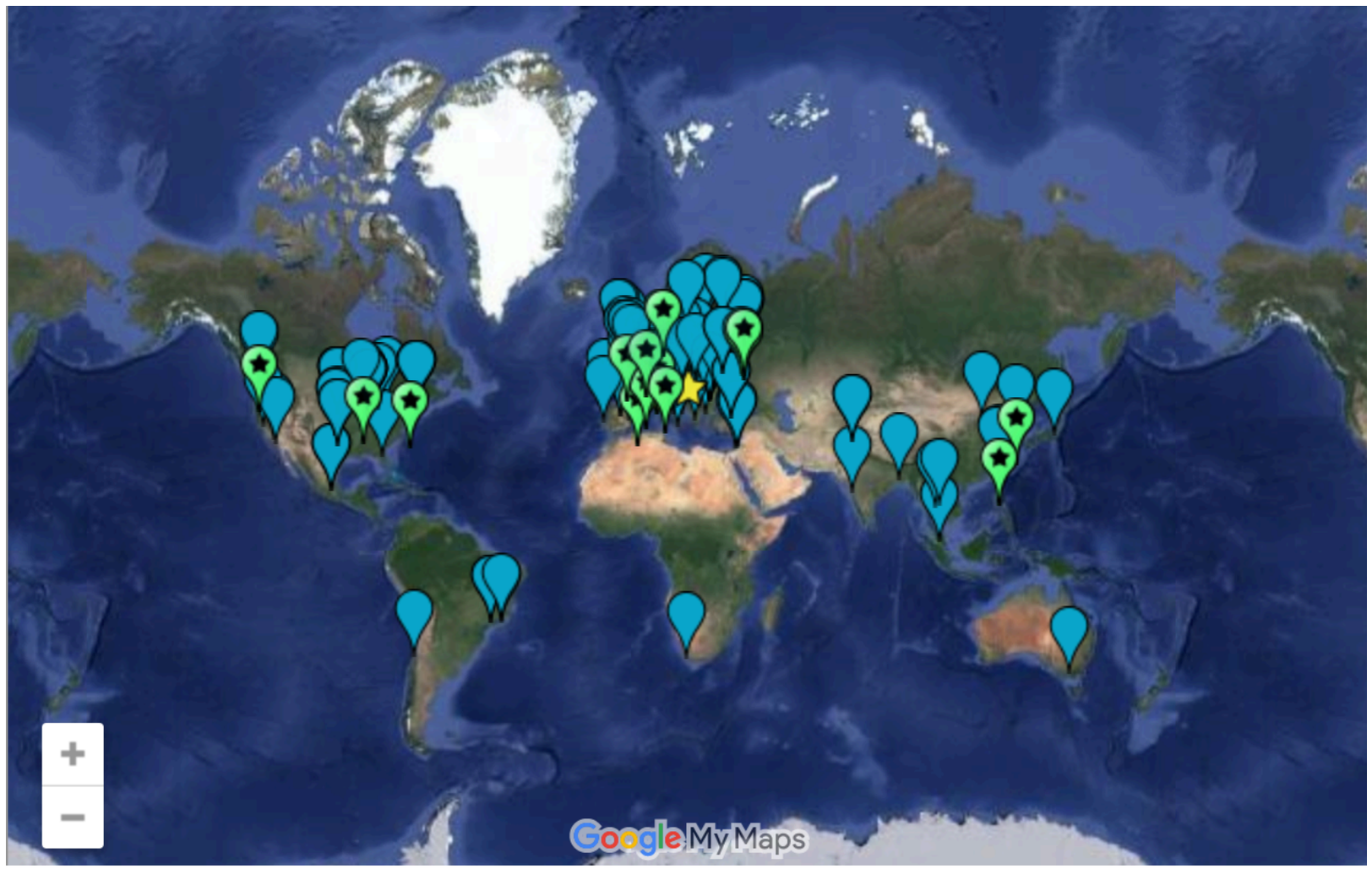


WLCG - Worldwide Large Computing Grid

After handling 100s of workflows everyday to make sure physicists receive what they expect

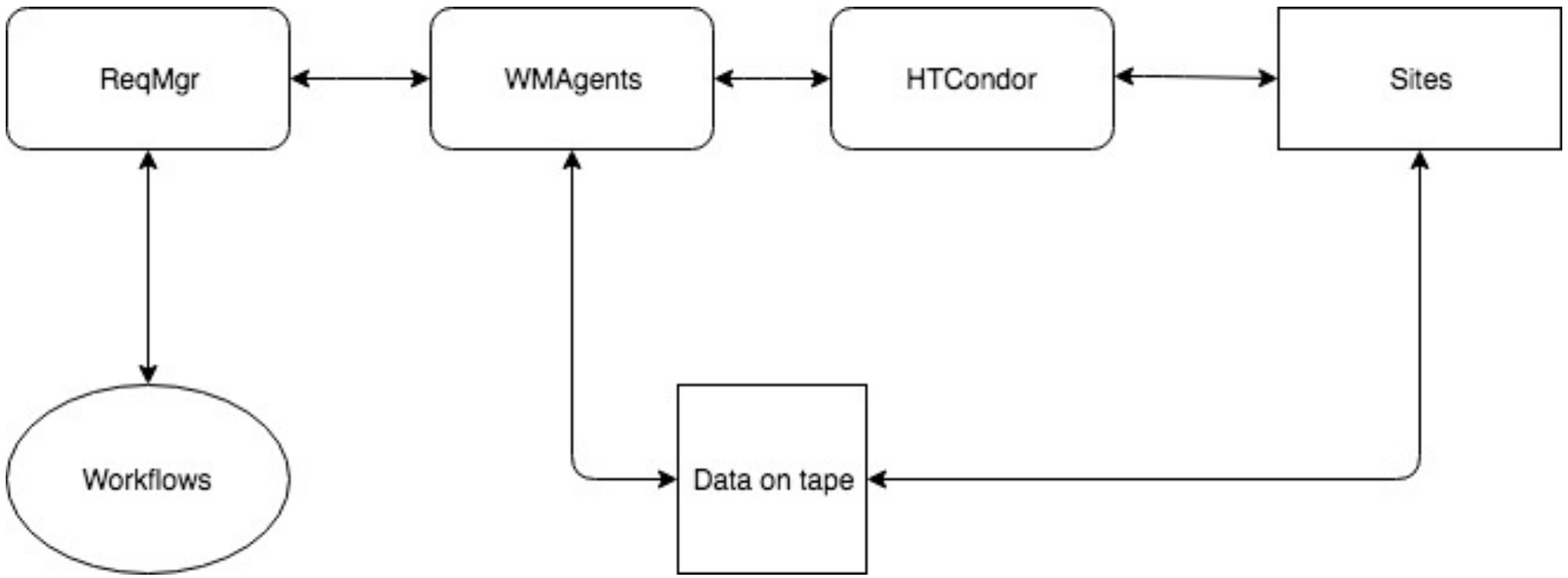
WLCG - Worldwide Large Computing Grid

170 computing centres
in 42 countries running
2 million tasks running
every day on 1 million
computing cores with
1 exabyte of storage

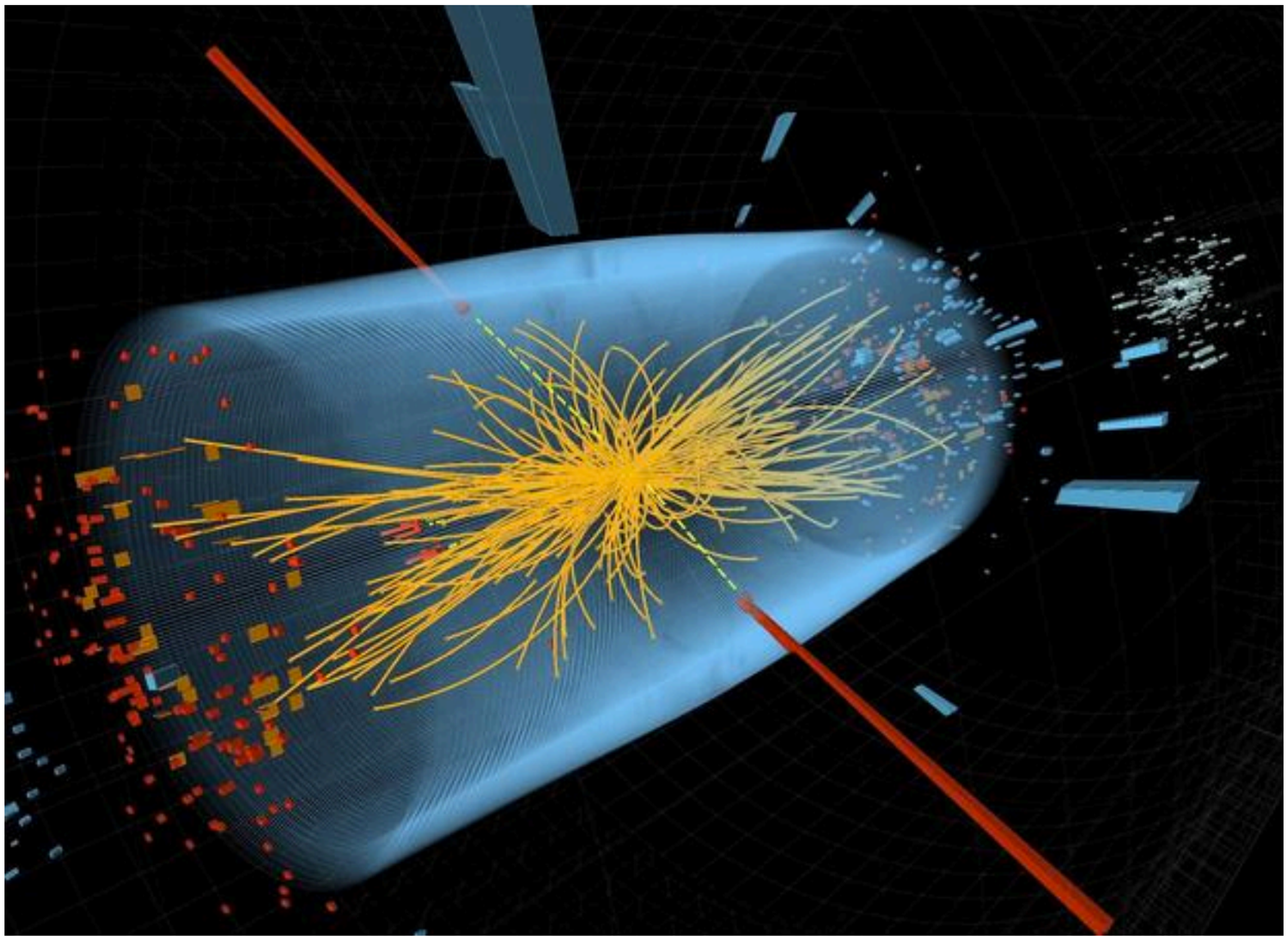


Galaxy of High Performance Computing

Workflow Management Overview



And that's how even Higgs Boson was found



Everyone single person counts!


Thank
you