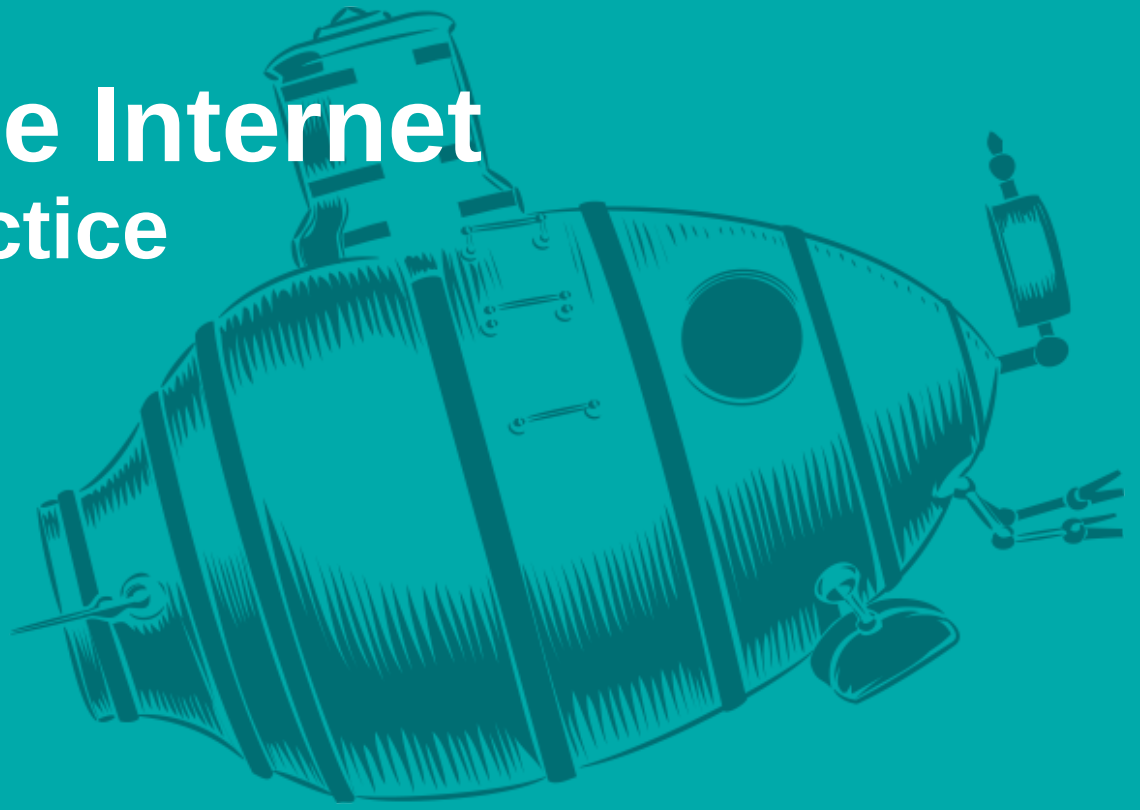
ALEF

# ICS accessible from the Internet
## bad (and very common) practice



**Jan Kopřiva**

jan.kopriva@alef.com

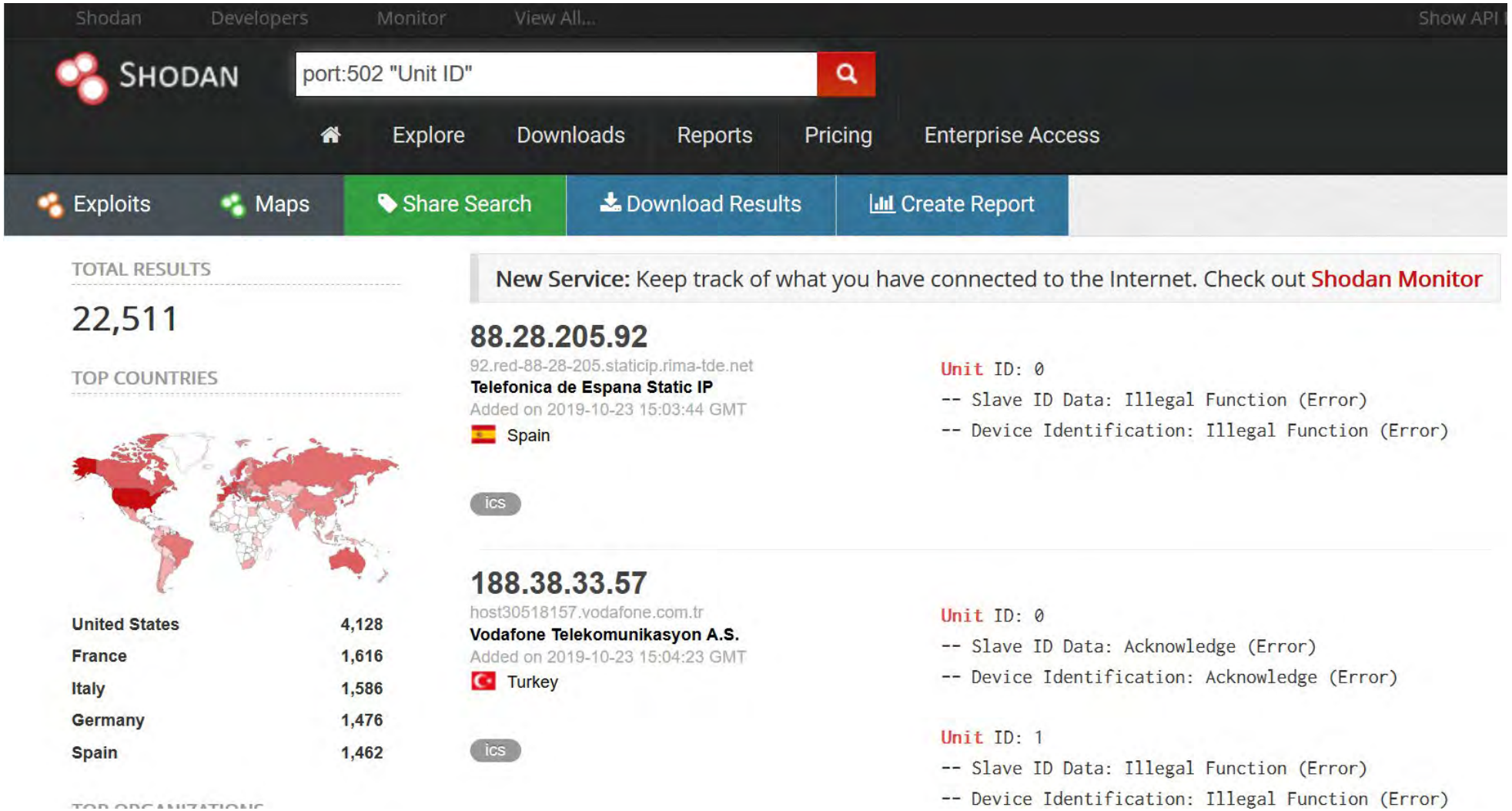
ALEF CSIRT

TLP: GREEN

# Are ICS connected to the internet common?

- Only few cases a year make it to mainstream media
- We tend to assume there is a lot more, but very few studies on the topic exist

# How would an attacker find connected ICS?




ALEF

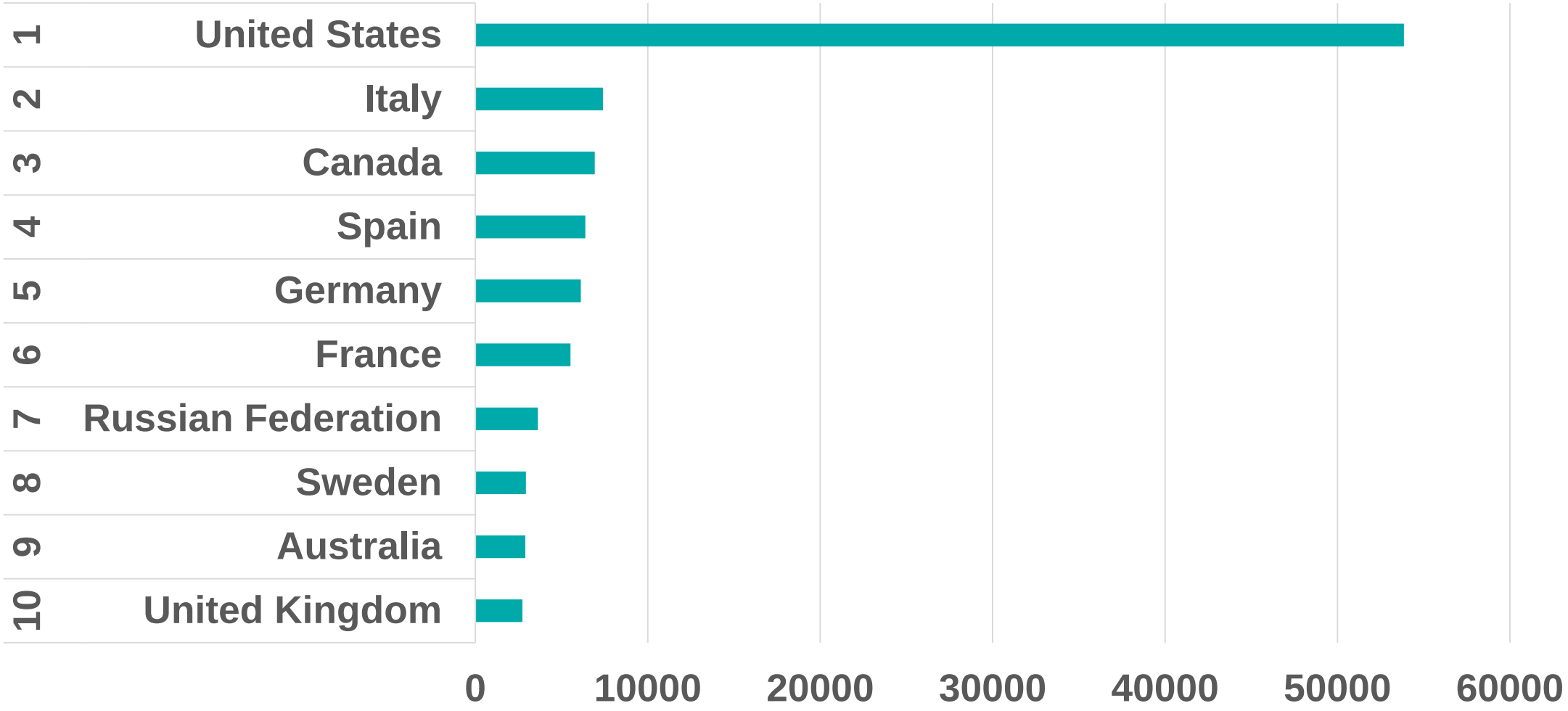
# Is ICS connected to the internet dangerous?

- Many industrial protocols lack any security functionalities…
- …so the short answer is „yes“

Command Prompt

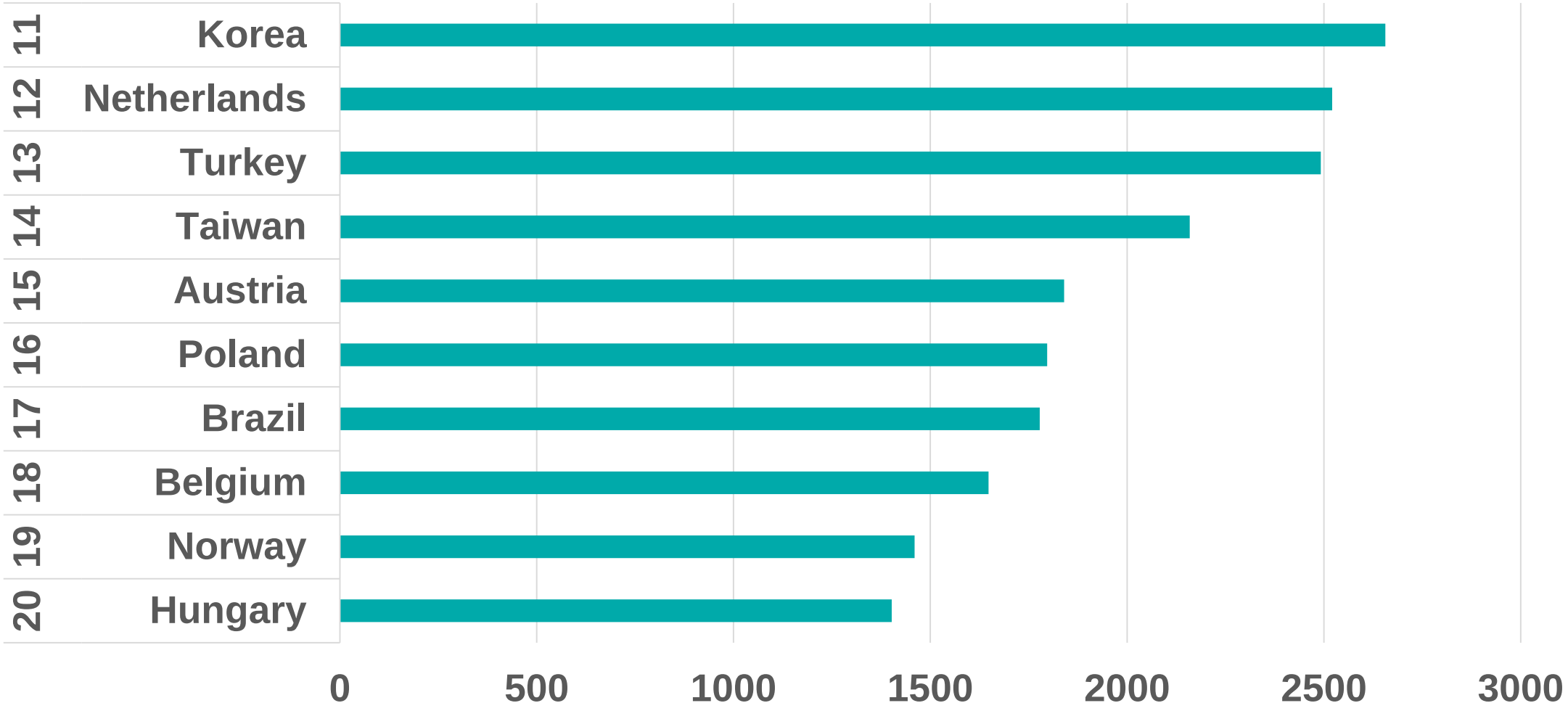
```
C:\Tools\TriOp\scada>python3 triop.py -h

TriOp
Tool for interacting with Shodan.IO to get statistical information/numbers of IPs which satisfy the
 queries submitted in bulk

Usage: triop.py [options]

Options:
  -h, --help            show this help message and exit
  -k KEY, --key=KEY     API key for Shodan
  --save_key            save key in a plaintext key file, used in conjunction
                        with option -k   !!!DO NOT USE ON SHARED COMPUTERS!!!
  -s SEARCH, --search=SEARCH
                        comma-separated list of search criteria
  -S SEARCH_FILE, --search_file=SEARCH_FILE
                        input CSV file(s) with search definitions
  --list_file=LIST_FILE
                        input file containing list of CSV files with search
                        definitions
  --filename_load=FILENAME_LOAD
                        use all files in the same directory which contain the
                        string in their names as search inputs
  -n, --new_file(s)     create new file(s) for results to be saved into
  -c COUNTRY, --country=COUNTRY
```

# How many ICS are out there?



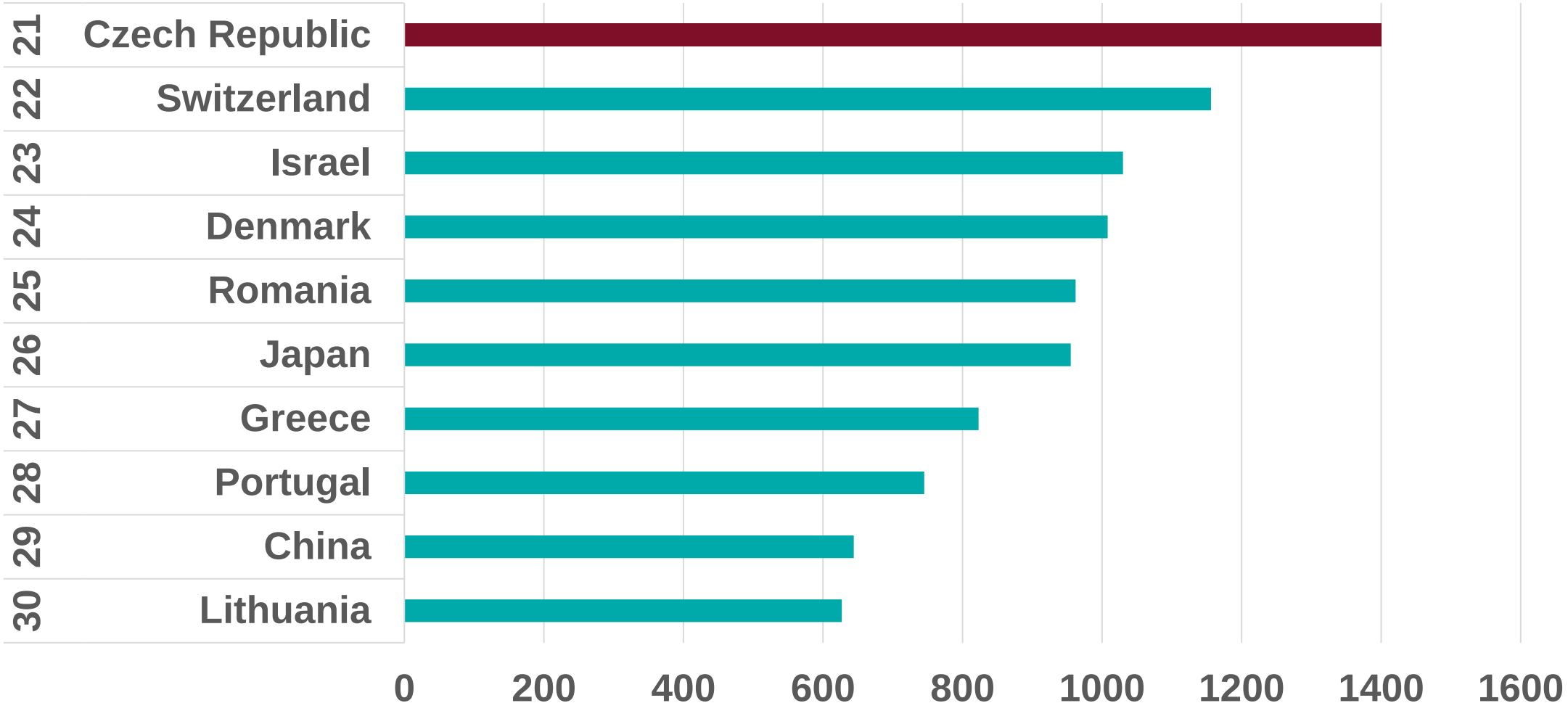

ALEF

# How many ICS are out there?




ALEF

# How many ICS are out there?

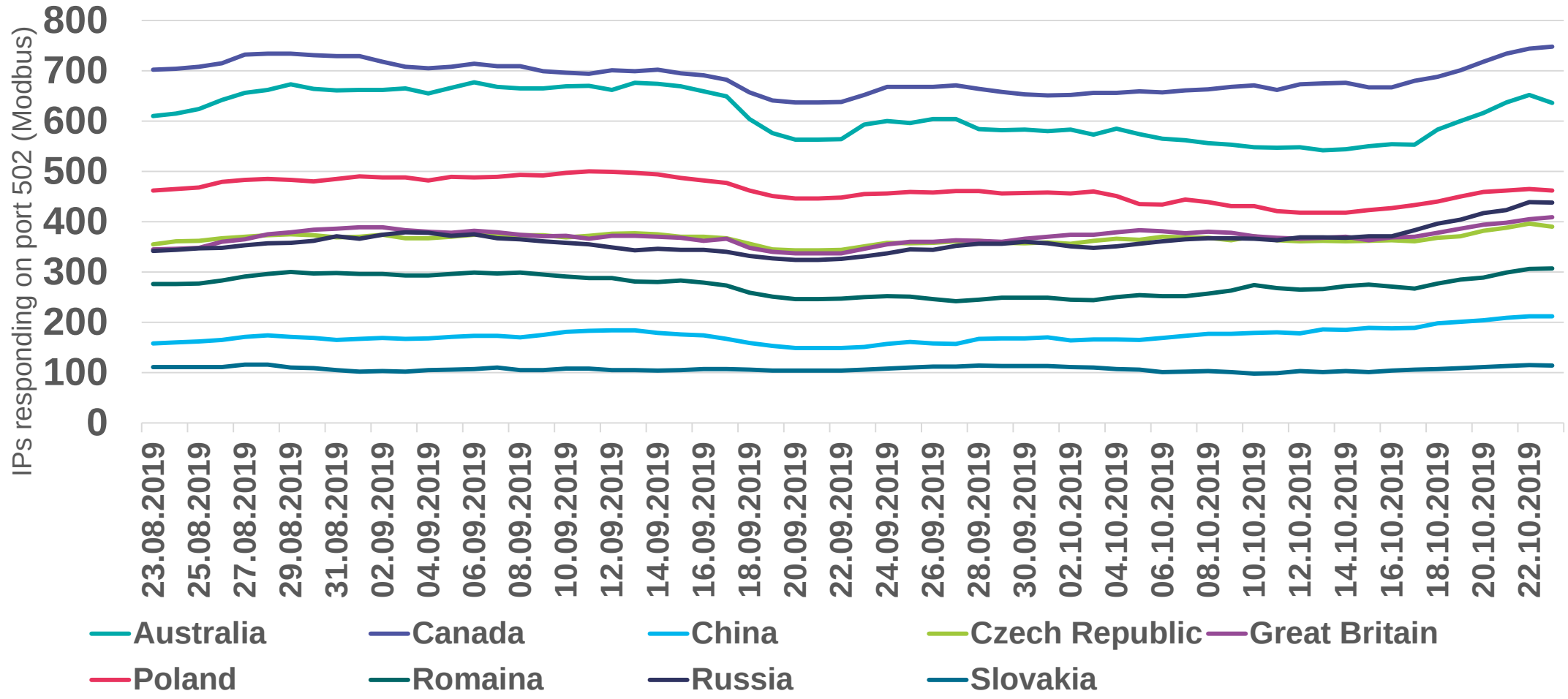



ALEF

# That‘s not great…

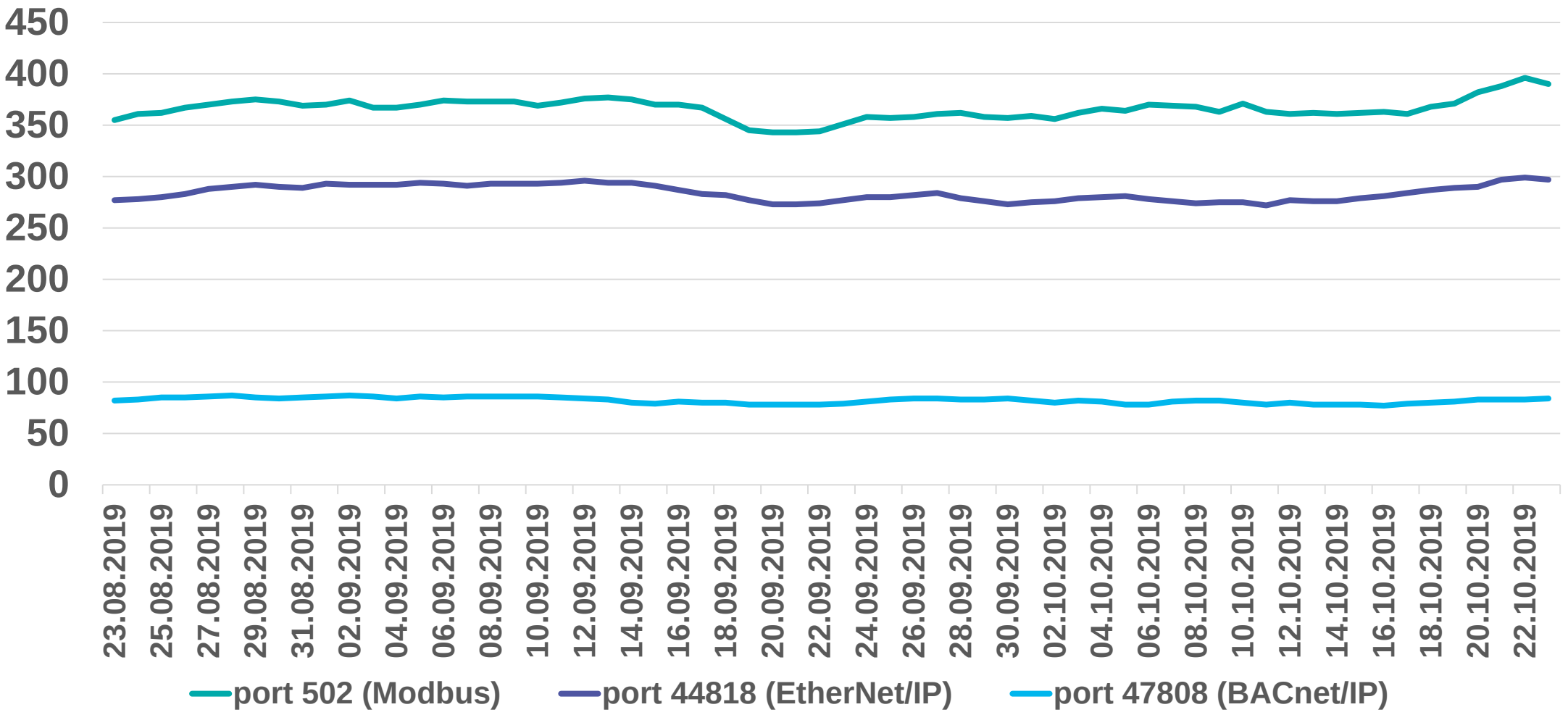
- If Shodan data were representative for all IPs in a country
  - Czech Republic ~ 0,1% IPs
  - Russia ~ 0,03% IPs
  - United States ~ 0,02% IPs
  - China ~ 0,002% IPs

# …but is this normal?



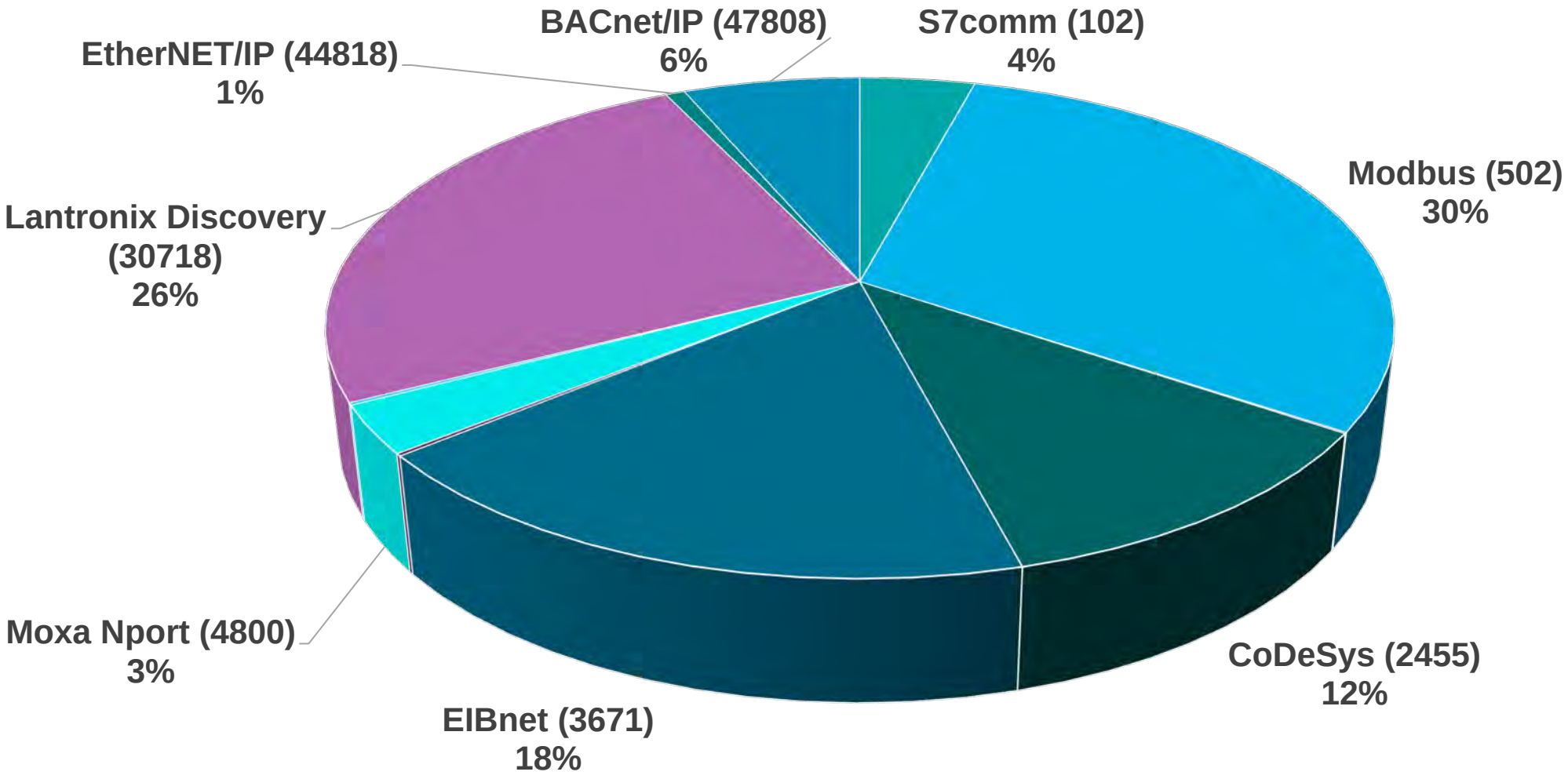

ALEF

# Let‘s take a look at the Czech Republic…




ALEF

# What is/was out there?

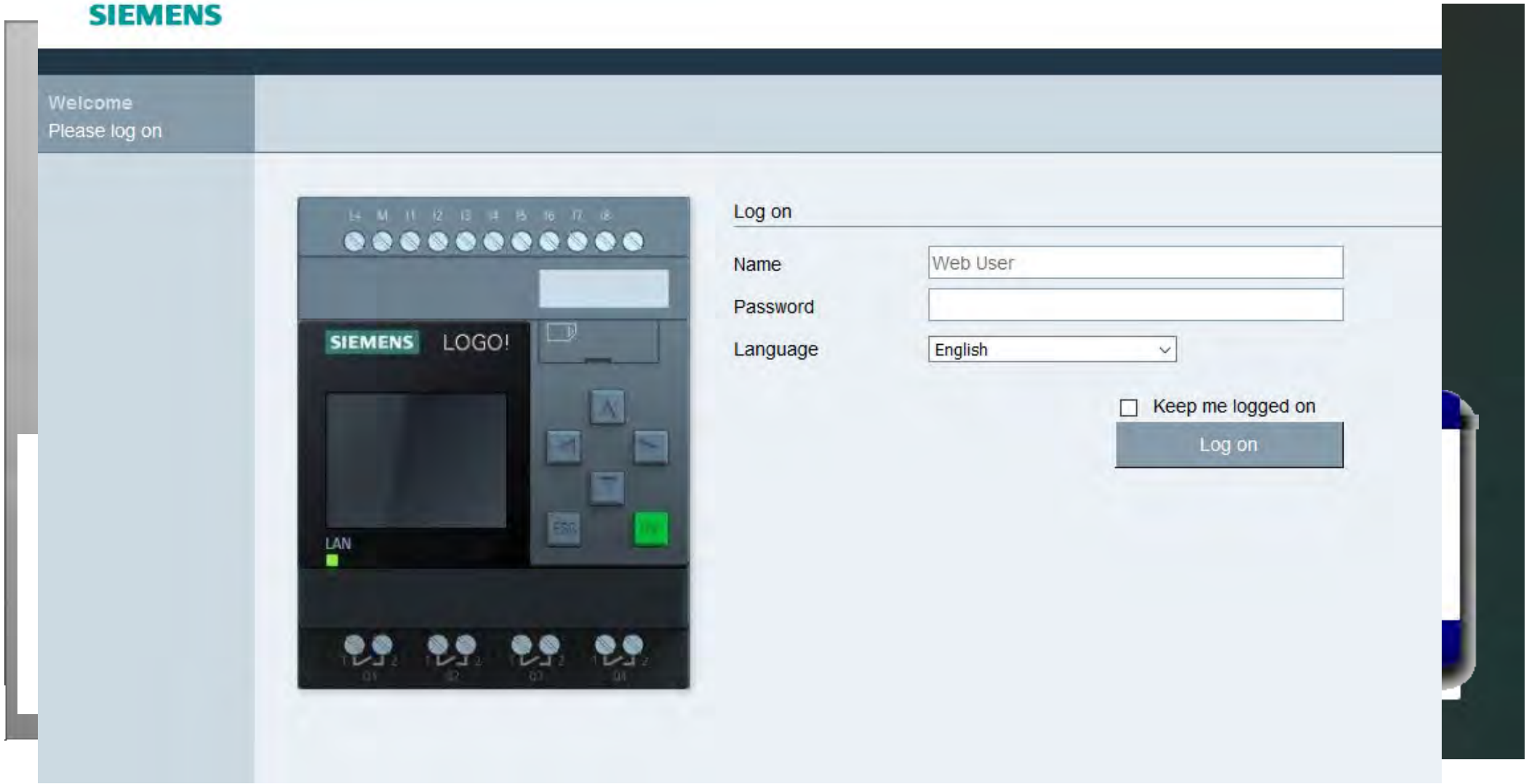



ALEF

# What is/was (probably) out there?

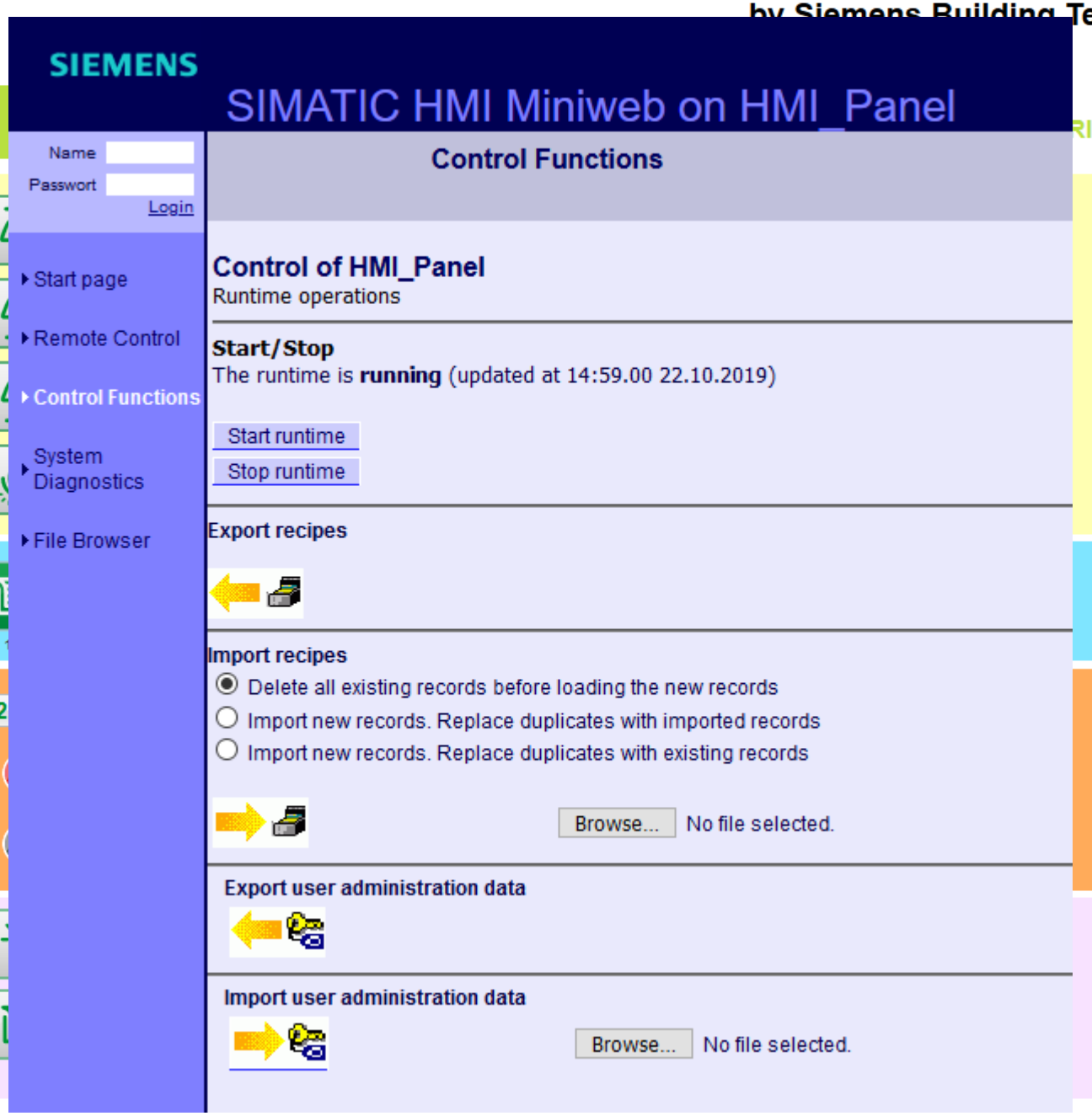
- HVAC and temperature controllers
- „Smart“ buildings
- Solar power plants
- Biogas plant
- Local power grid controller
- General use PLCs
- Elevator controller
- Camera systems controller
- Physical security systems
- Industrial processes controllers
- Industrial measuring equipment

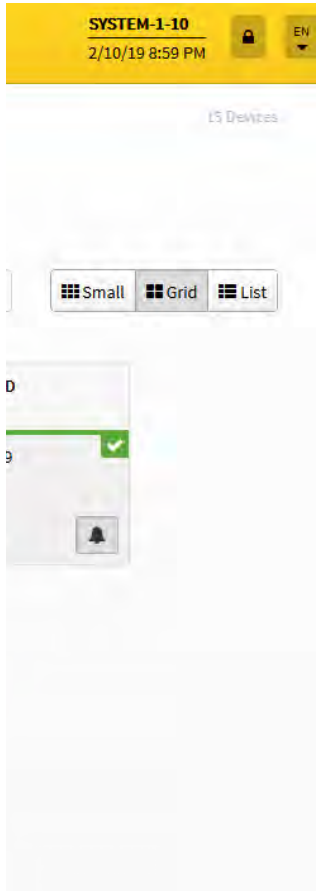
# Some control panels required authentication…



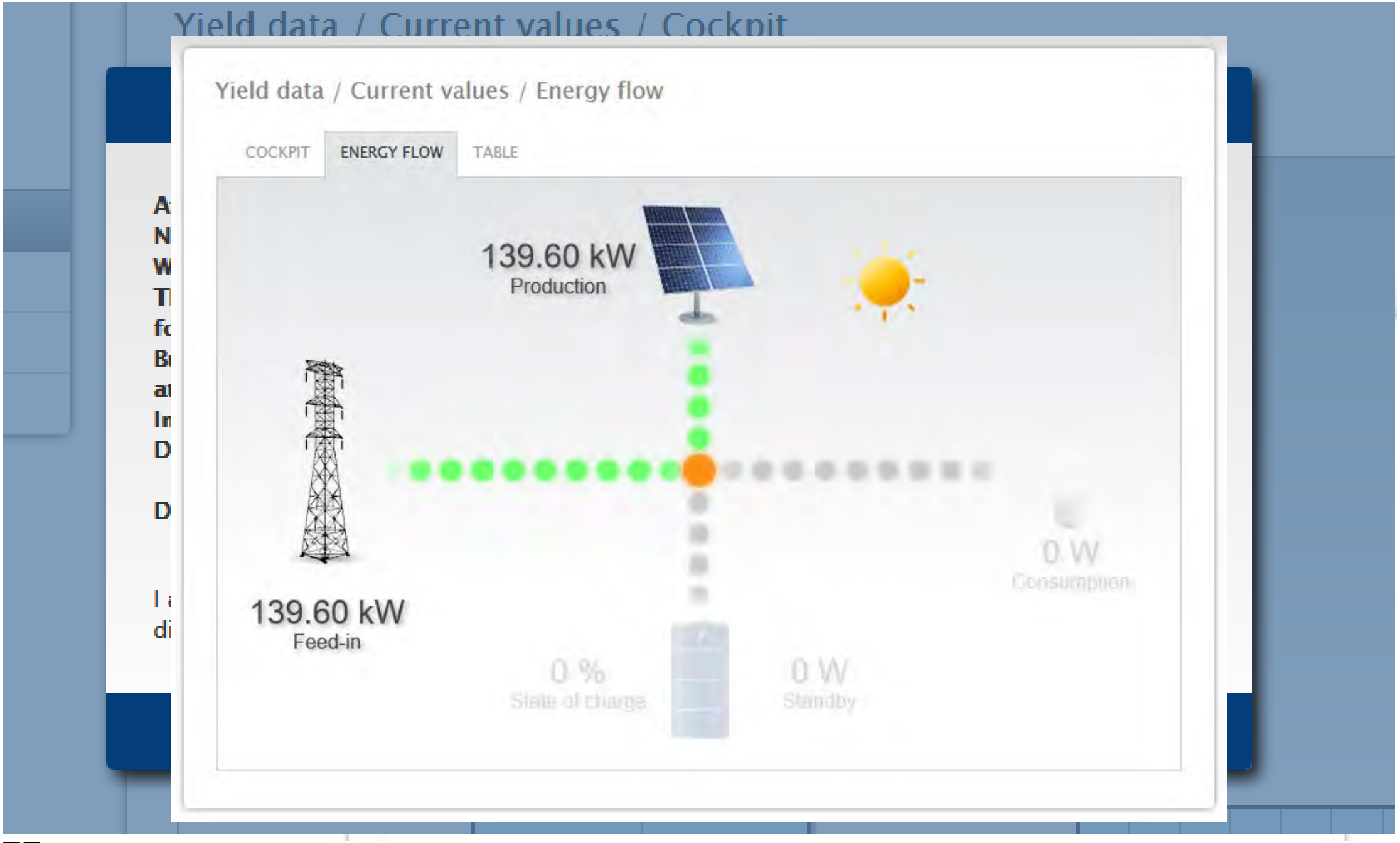

ALEF

# Climatix - BACnet Communication Card by Siemens Building Technologies


ALEF


Yield data / Current values / Energy flow
COCKPIT
ENERGY FLOW
TABLE
139.60 kW
Production
0 W
Consumption
139.60 kW
Feed-in
0 %
State of charge
0 W
Standby

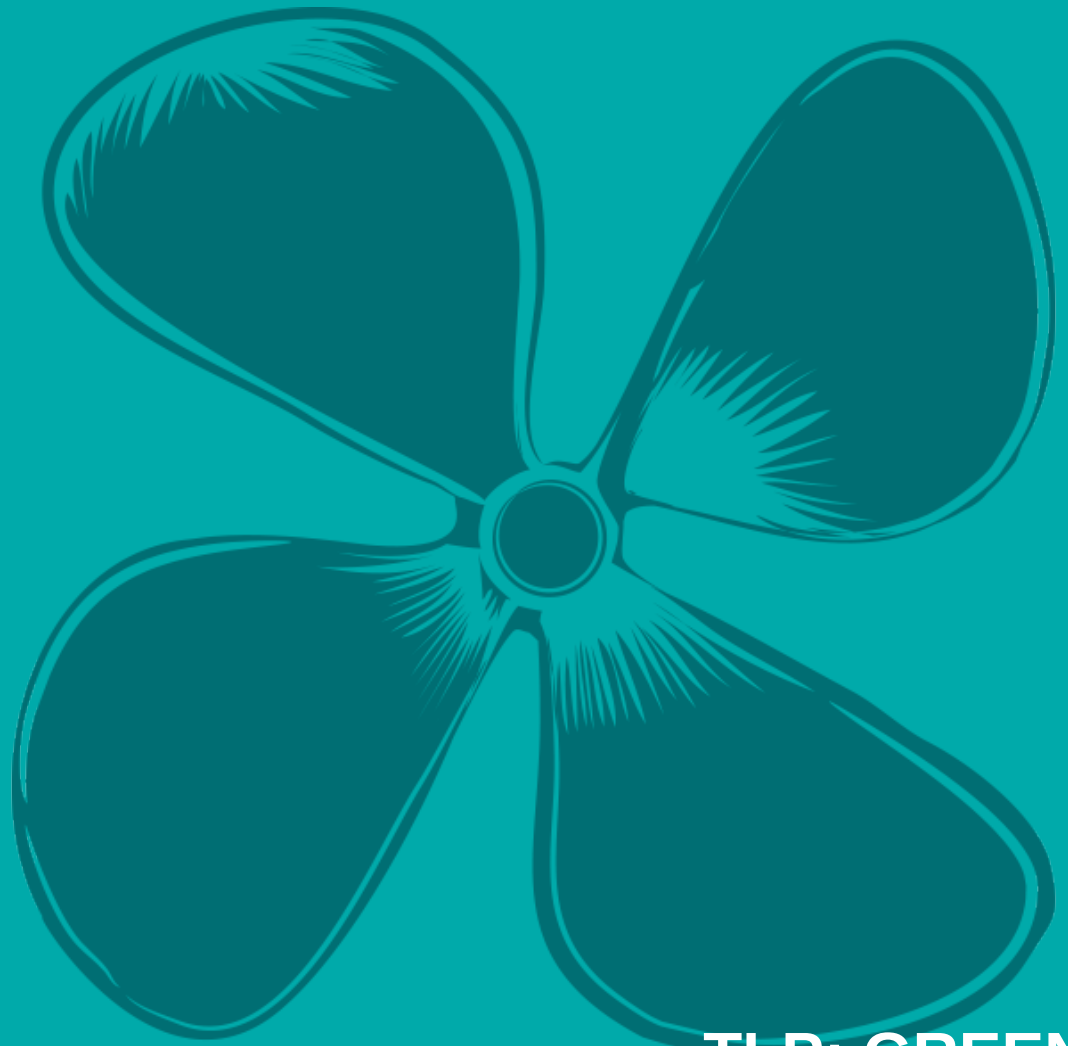
ALEF

# Informing interested parties

- Big help from (and big thanks to)
  - CZ.NIC – National Registrar for CZ TLD
  - NCISA/NÚKIB – National Cyber and Information Security Agency

ALEF

# Thank you for your attention



TLP: GREEN