Kaspersky Industrial Cybersecurity Conference 2021

Into the Dark

switching off (some) solar power Parks

Stephan Gerling

Into the Dark

switching off (some) solar power parks

Stephan Gerling

Senior Security Researcher
Kaspersky ICS-CERT

@ObiWan666

What,

if someone can control

The Sun

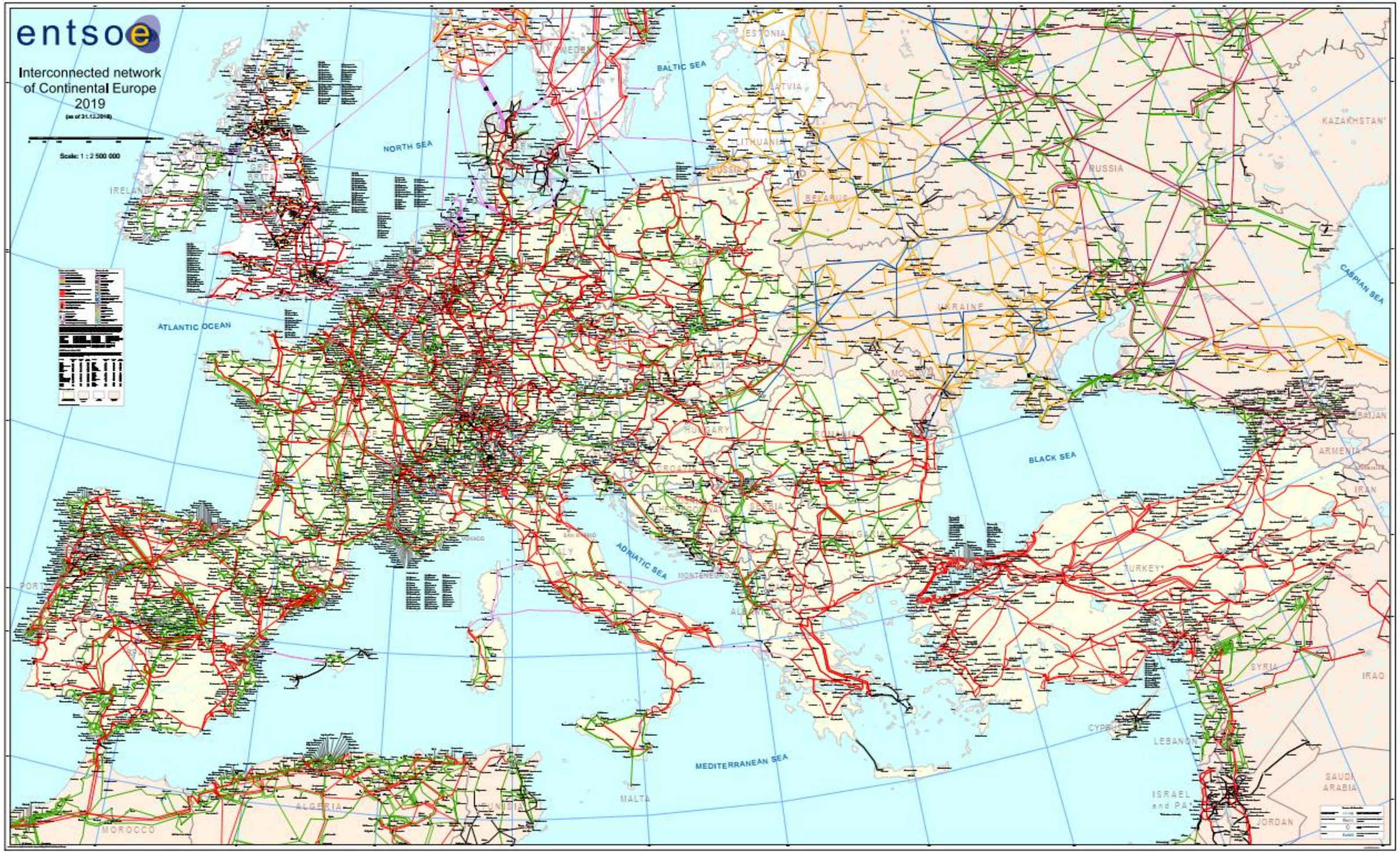
Kaspersky ICS-CERT
found a vulnerability in a product
for solar power generation

Current status:
Vendor working on Patch

How is the European Grid working?

A small introduction and what has this to do with the vulnerability

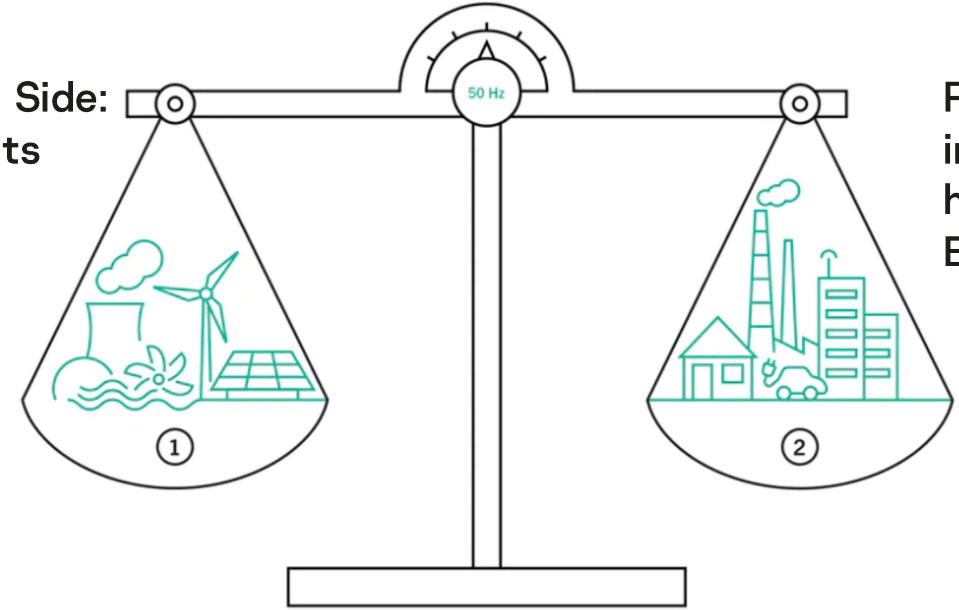
The Grid



Interconnected Network of continental Europe (entso-e) https://www.entsoe.eu/data/map/downloads/

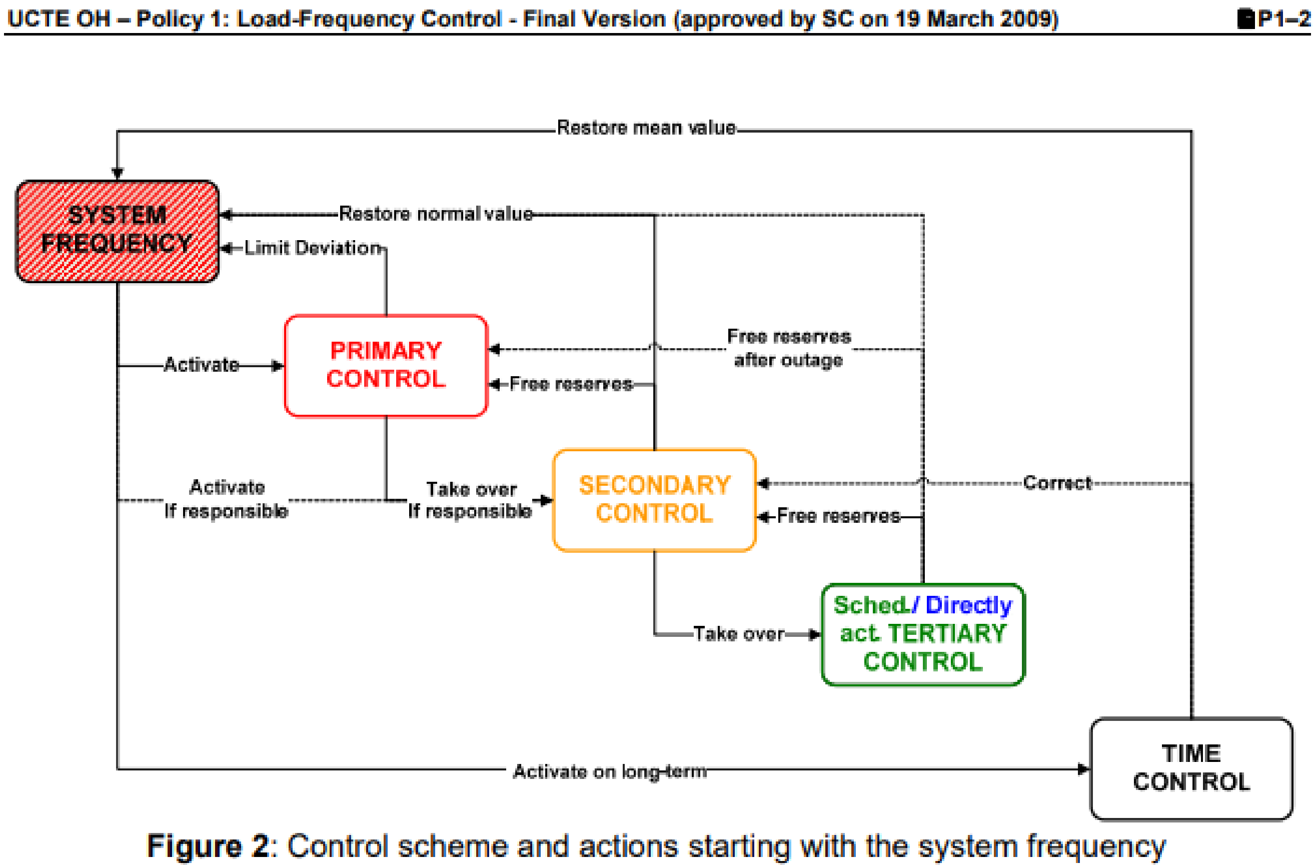
50 Hertz is the base frequency in Europe Grid

Production Side:
Power plants
Wind
Solar



Production Side:
industry
houses
EV

Picture: (https://www.swissgrid.ch/de/home/operation/regulation/grid-stability.html)



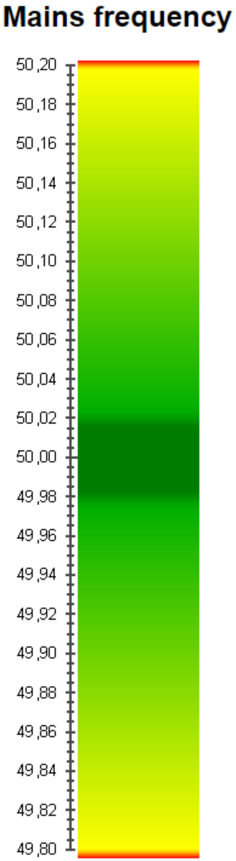
UCTE OH – Policy 1: Load-Frequency Control - Final Version (approved by SC on 19 March 2009) P1–2

Figure 2: Control scheme and actions starting with the system frequency

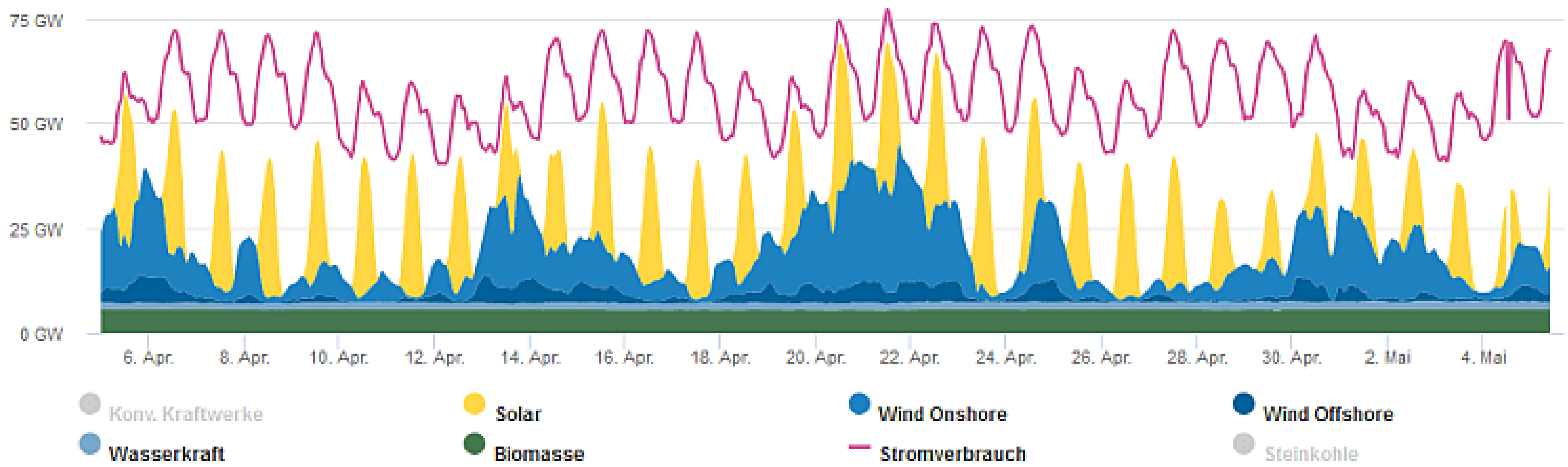
Picture: (https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/ce/oh/Policy1_final.pdf)

grid frequency levels

Frequency	Action	load sum	activation
51,5 Hz	all renewable energy disconnected from grid	100%	automatic
50,2 Hz	starting of demand side management renewable energy		automatic
50,1 Hz	no action		
50,0 Hz	Baseline		
49,9 Hz	no action		
49,8 Hz	immediately activating +control power & load shedding of pumps (t<10s)		manual/automatic
49,2 Hz	direct load shedding of storage pumps		automatic
49,0 Hz	load shedding LEVEL 1 , ca. 12,5 %	ca. 12,5 %	automatic
48,8 Hz	load shedding LEVEL 2, ca. 12,5 %	ca. 25,0 %	automatic
48,6 Hz	load shedding LEVEL 3, ca. 12,5 %	ca. 37,5 %	automatic
48,4 Hz	load shedding LEVEL 4, ca. 12,5 %	ca. 50,0 %	automatic
47,5 Hz	disconnecting power plants from grid		automatic


Mains frequency

Energy usage in Germany April 2020



Germany has 4 grid operator

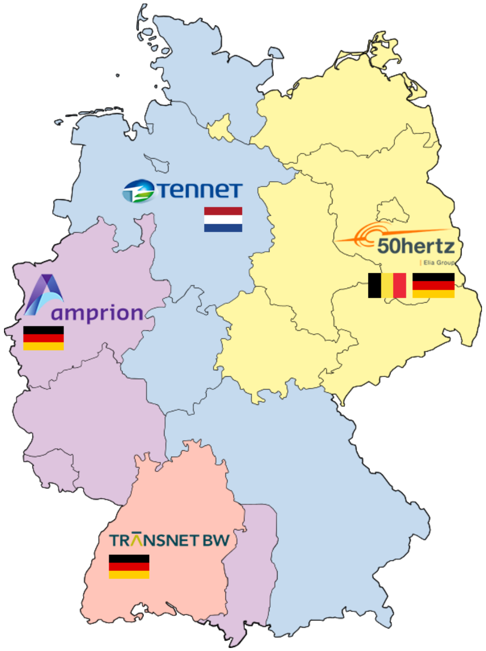
In total:

7000MW +control power

5500MW -control power

+CP = stand by power plants

-CP = disconnect solar power



How does the “load shedding” work

Germany use “ripple controller”

Done by

- Powerline communication
- RF signals (TETRA)

What do we know now

- Grid frequency
- Load shedding
- Demand side management
- + & - control power needed

How does the “load shedding” work

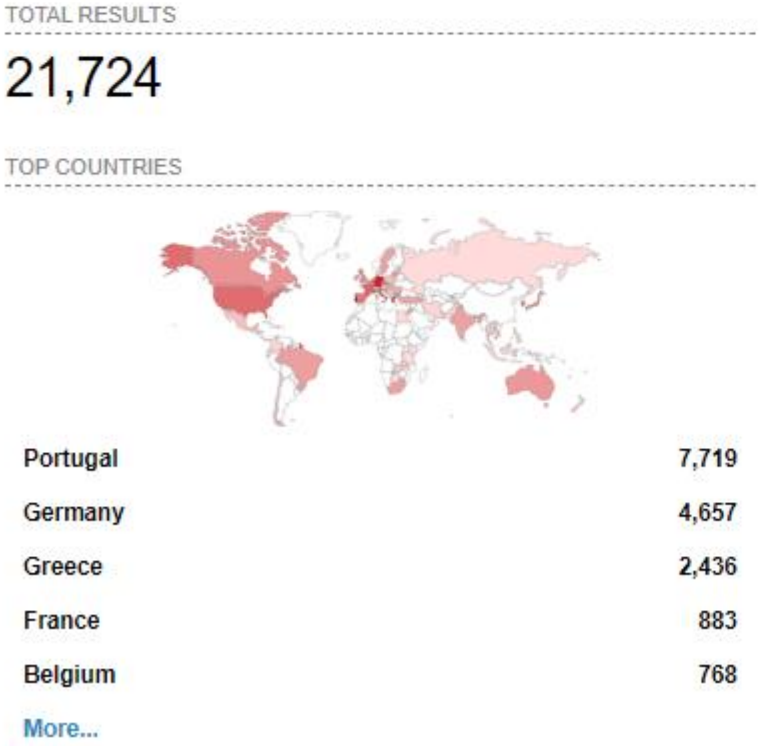
Germany use “ripple controller”

Done by

- Powerline communication
- RF signals (TETRA)

The year Kaspersky was founded

Shodan results



TOTAL RESULTS

21,724

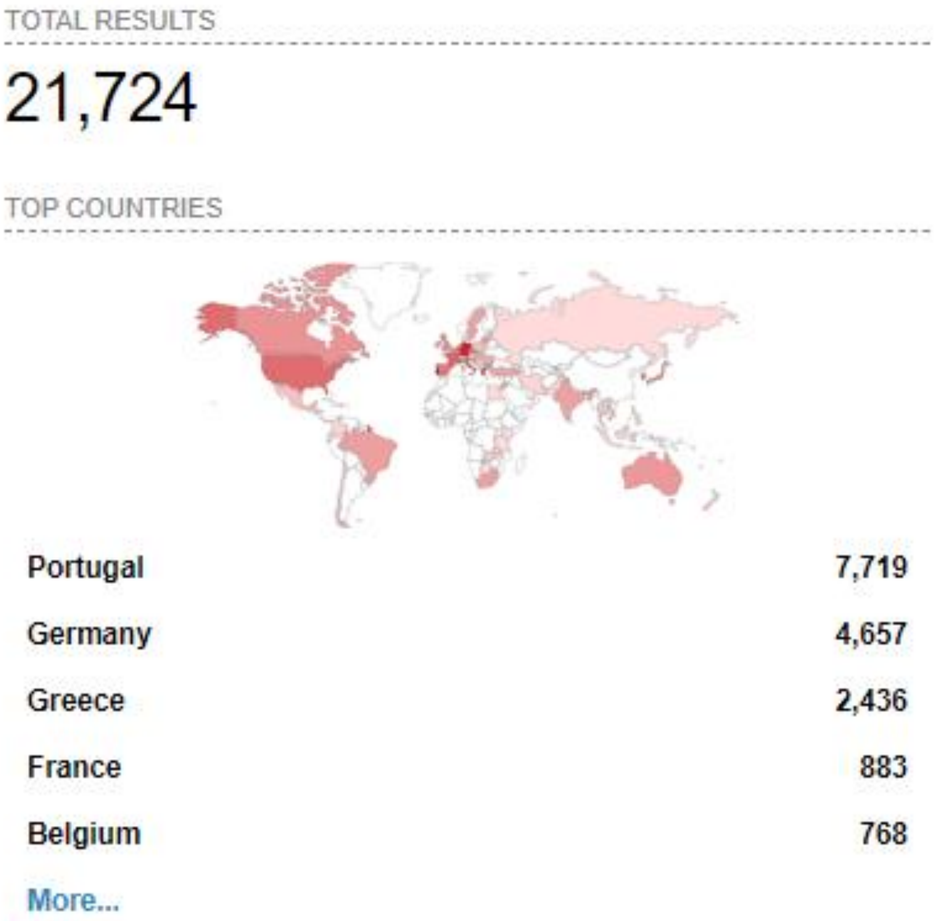
TOP COUNTRIES

Portugal	7,719
Germany	4,657
Greece	2,436
France	883
Belgium	768

More...

query

Online solar systems



TOTAL RESULTS

21,724

TOP COUNTRIES

Portugal	7,719
Germany	4,657
Greece	2,436
France	883
Belgium	768

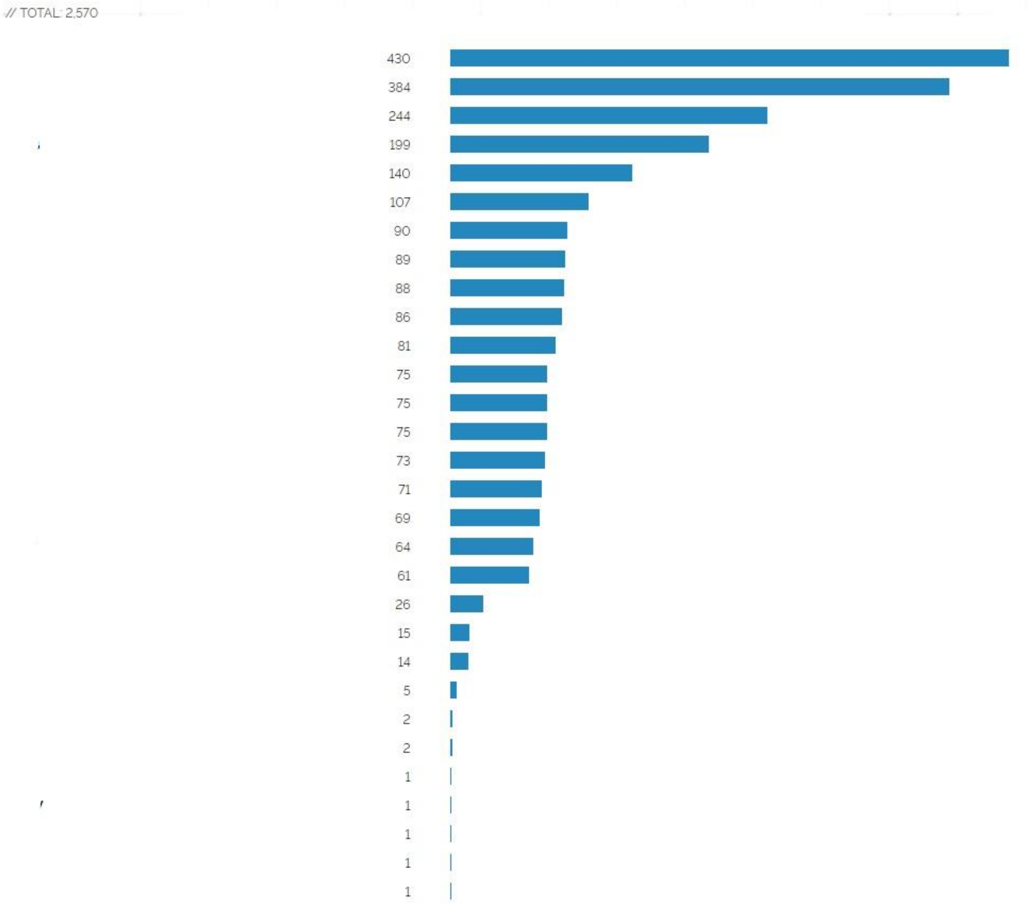
More...

(shodan.hq querry)

query

Only vulnerable Solar generator shown

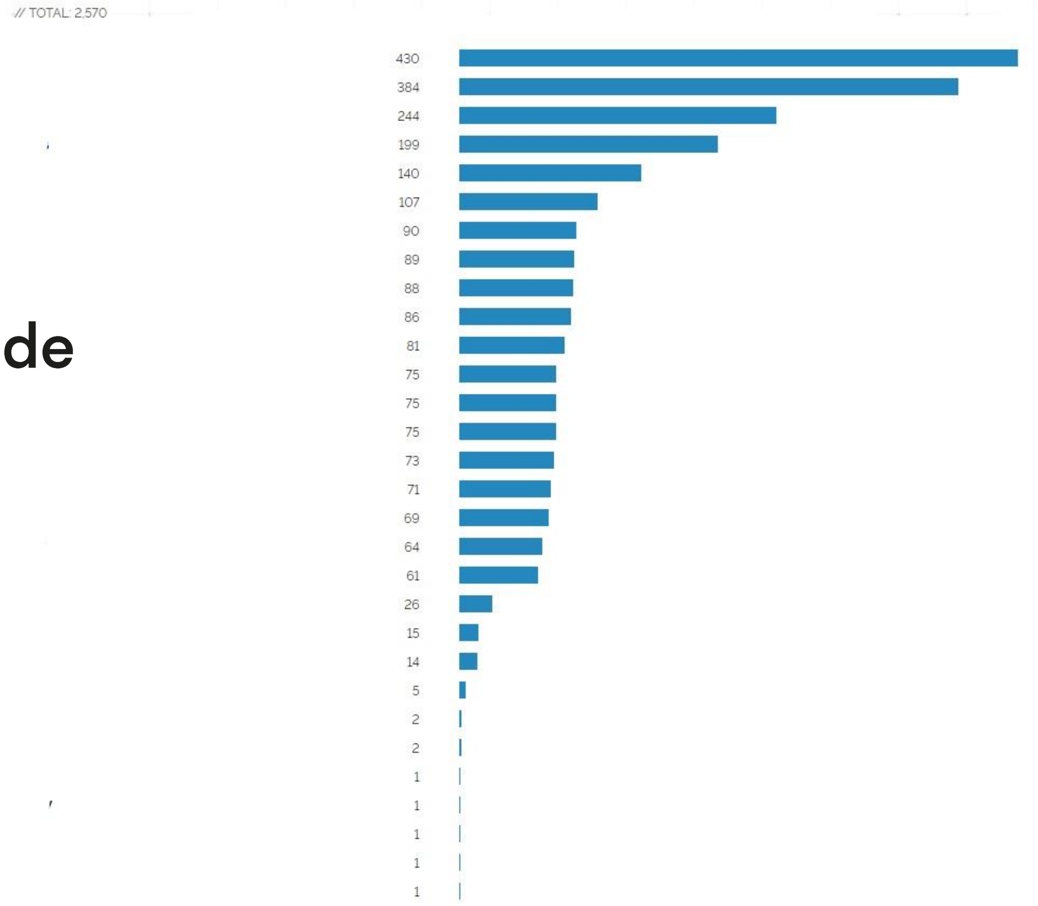
#total ~2570



(shodan.hq querry)

~2570 devices

~ 7200 MW worldwide
~ 2800 MW Europe



Germany has 7000MW reserve (+CP)

destabilization with ~2800MW now possible

= not enough to directly force a blackout

We need to find a amplifier trigger event or something else.

Load shedding

- TETRA
- LF (SEMAGYR TOP)
- others

How to prevent the risk:

Is Internet connectivity needed?

- Mostly yes to get the Data

Use of VPN

- Configure the devices into a VPN to avoid exposure to the Internet

Encrypt over Air Data traffic for load shedding

What can we do?

A presentation and a leave-behind document are different in terms of audience and delivering content.

Presentation
You are talking to a live audience that has to be focused and engaged and wired into your topic.

Leave-behind document
This means you are leaving the document with a potential reader. Still make it clear and detailed.

It’s intended for both

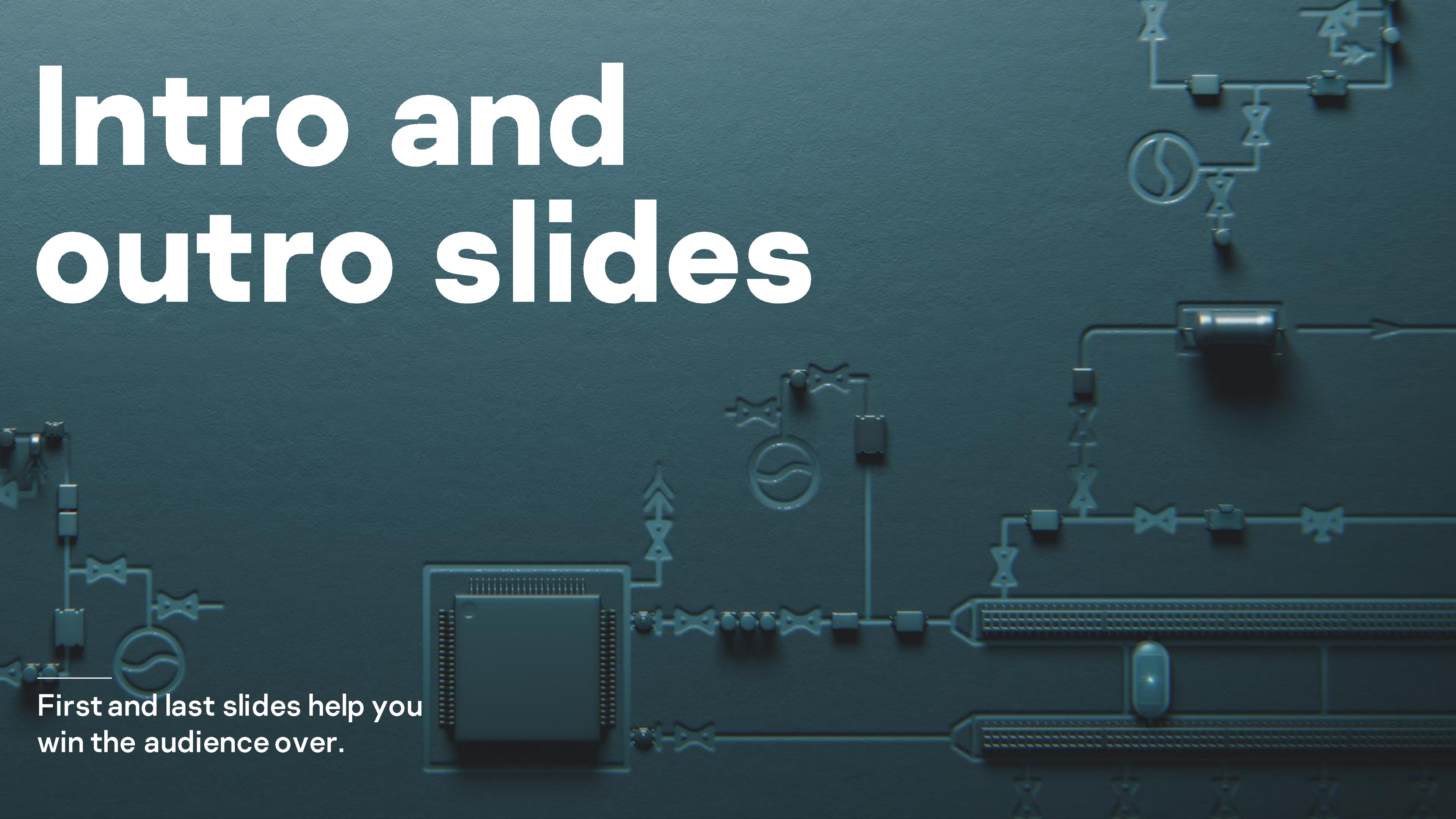
This document is intended to help you easily create any type of presentation.

Treat your first notes like it’s a leave-behind. No matter which type of the two you are preparing.

Write down all information about each point but keep it clear and concise.

Complete the draft, save a version of the file, and move long text to Notes below.

Intro and outro slides

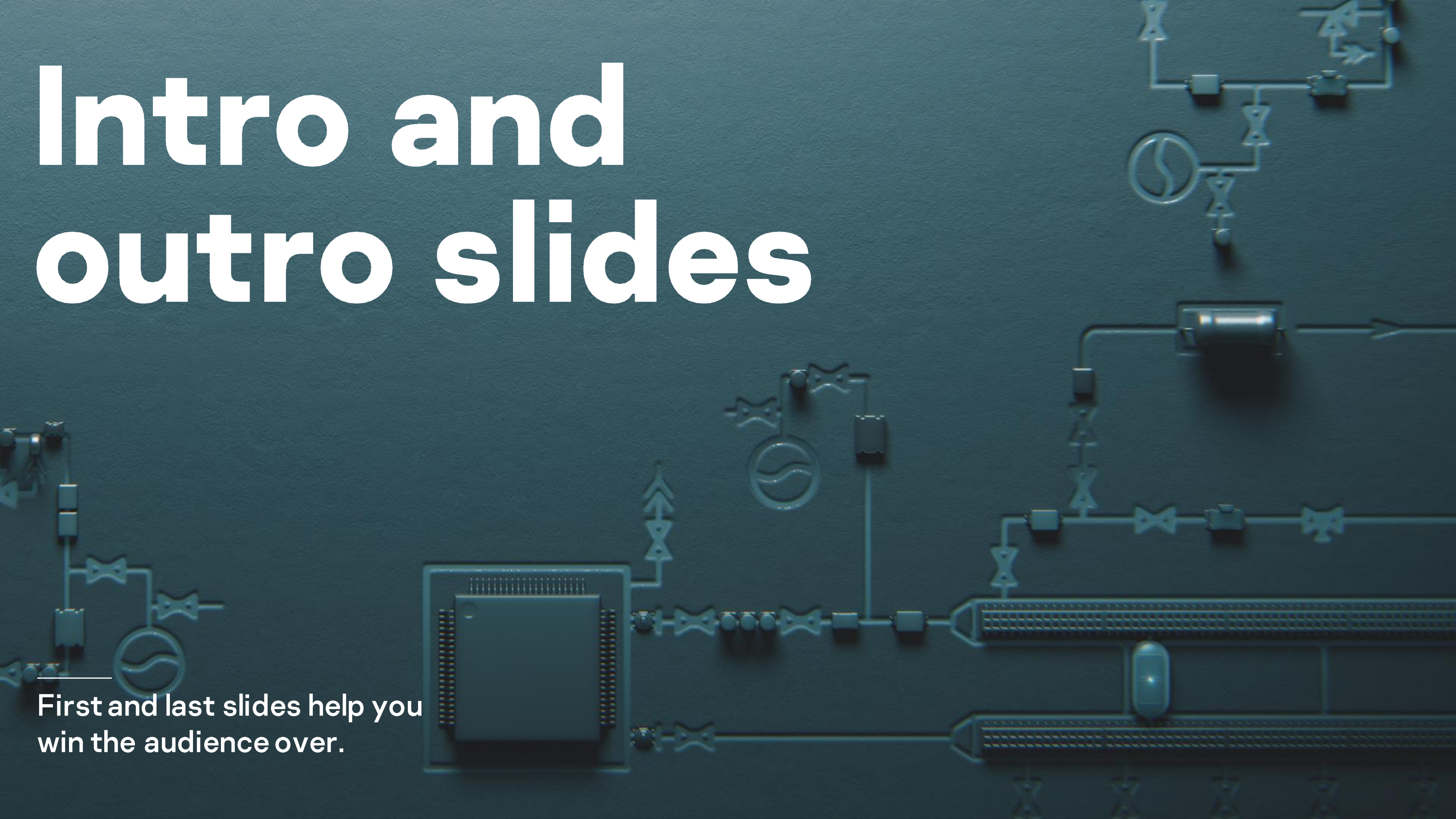


First and last slides help you win the audience over.

> “ I am very confident that there will be no blackout

Jochen Homan, Nov. 2013

Intro and outro slides



First and last slides help you win the audience over.

Thank you!

Subtitle

Stephan Gerling

Senior Security Researcher
Kaspersky ICS-CERT

@obiwan666

kaspersky