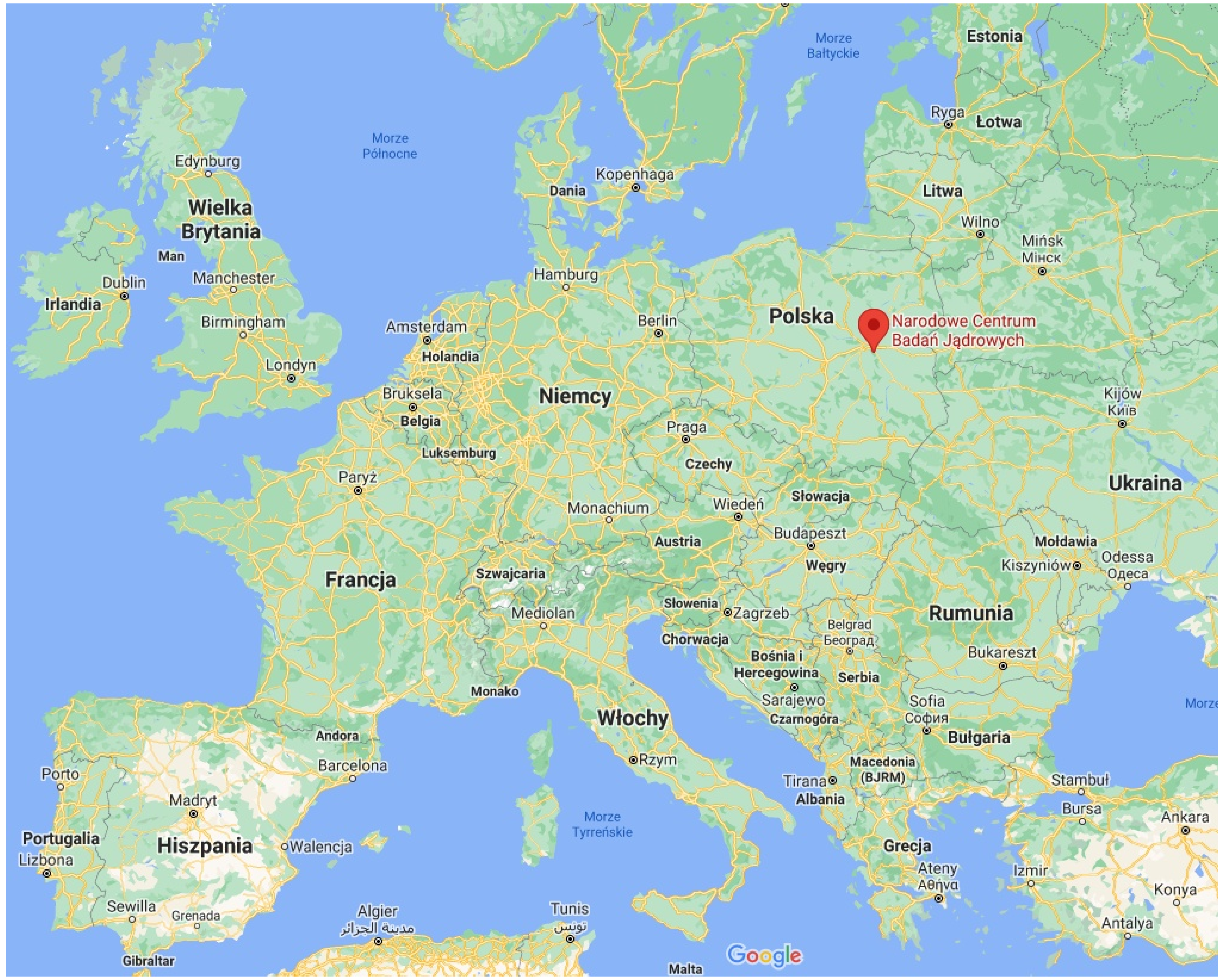
National Centre for Nuclear Research

Jarosław Szewiński

NATIONAL CENTRE FOR NUCLEAR RESEARCH ŚWIERK

NCBJ Location



NCBJ Today

- Institute joins basic and applied research combines the following domains:
  - particle physics, nuclear physics,
  - astrophysics, plasma physics,
  - material physics,
  - reactor and accelerator physics,
  - nuclear energy
  - industry & medical accelerators,

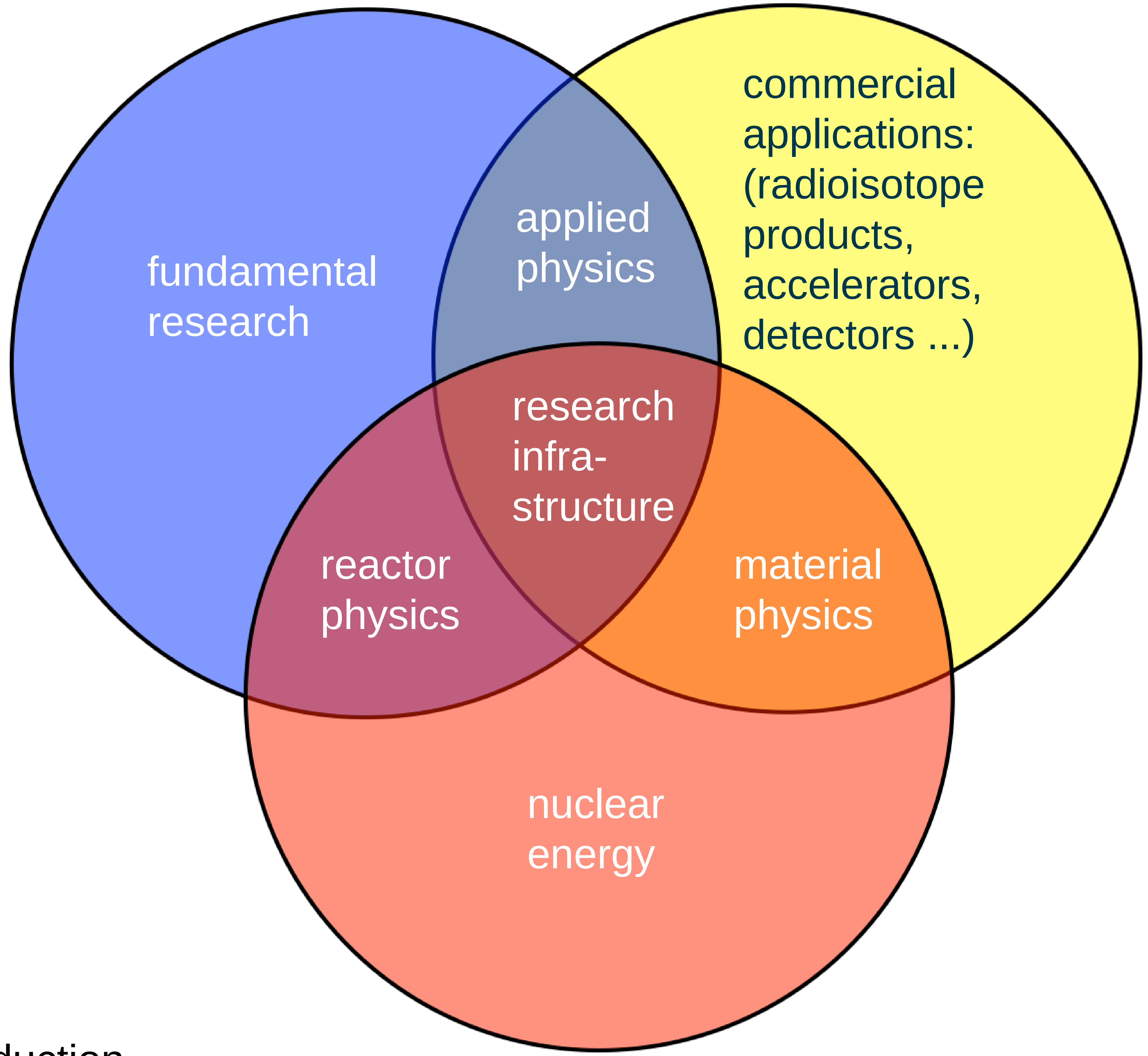
HITEC ZAKŁAD APARATURY JĄDROWEJ

- radioisotope products

Radioisotope Center

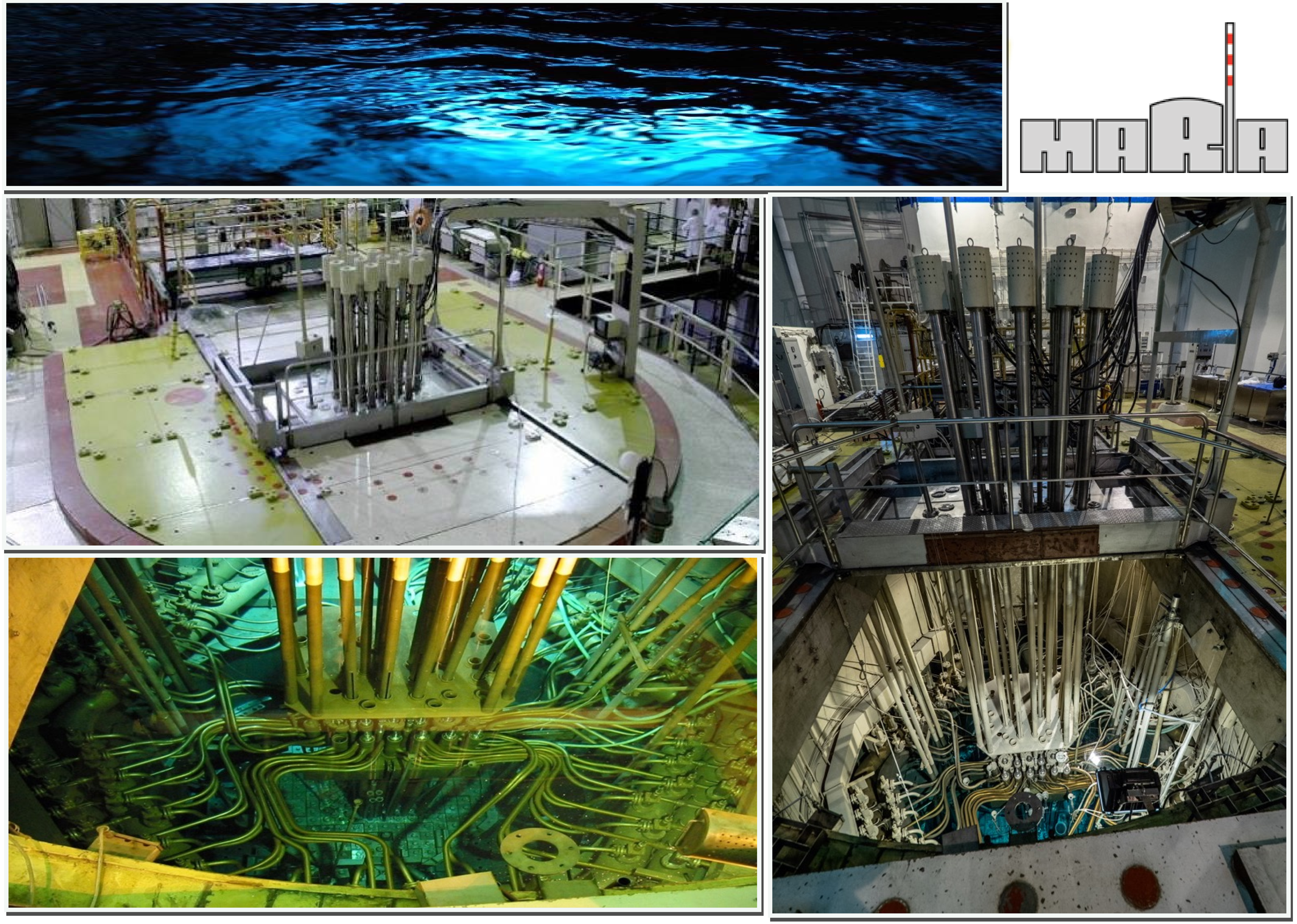
POLATOM

export to 80 countries,
^{99}Mo - in 2016 6% of world production
(up to 18% of world production in 2013)



fundamental research
applied physics
commercial applications: (radioisotope products, accelerators, detectors ...)
research infra- structure
reactor physics
material physics
nuclear energy

Nuclear research reactor Maria



- built in 1974
- upgrade 1992, 2011, 2017-…
- pool type
- H_2O, Be moderated
- 30 MW thermal power
- neutron flux:
  - thermal $4 \cdot 10^{14}$ n/cm^{2}s
  - fast $2 \cdot 10^{14}$ n/cm^{2}s

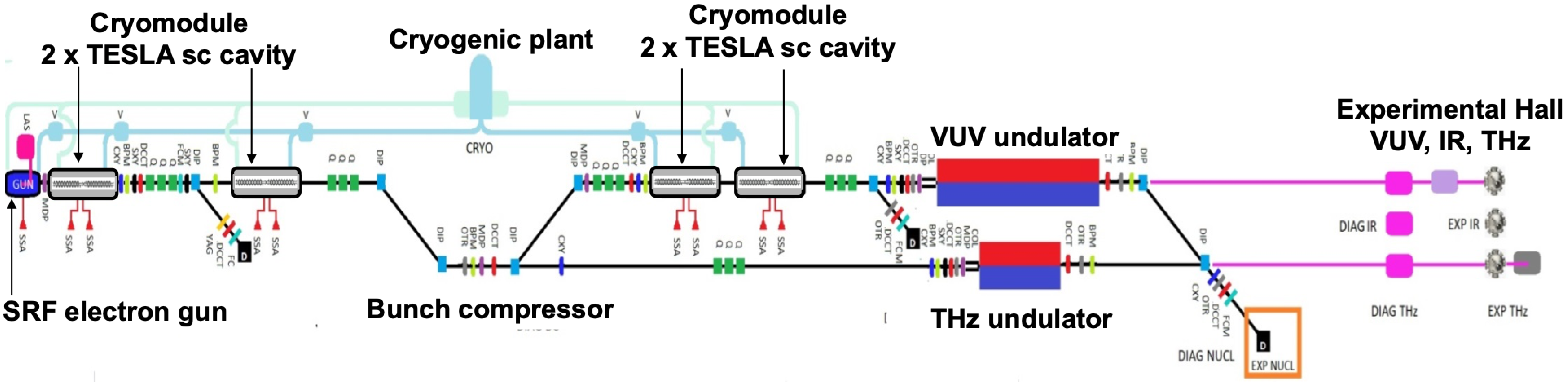
One of the best neutron sources!

- Curium
- POLATOM-NCBJ

Radioisotopes
for 400k patients a week!

Polish Free electron Laser

Design of the facility has been adjusted accordingly to both the technical progress in the accelerator components and requirements of experiments.



Cryomodule
2 x TESLA sc cavity

Cryogenic plant

Cryomodule
2 x TESLA sc cavity

VUV undulator

Experimental Hall
VUV, IR, THz

SRF electron gun

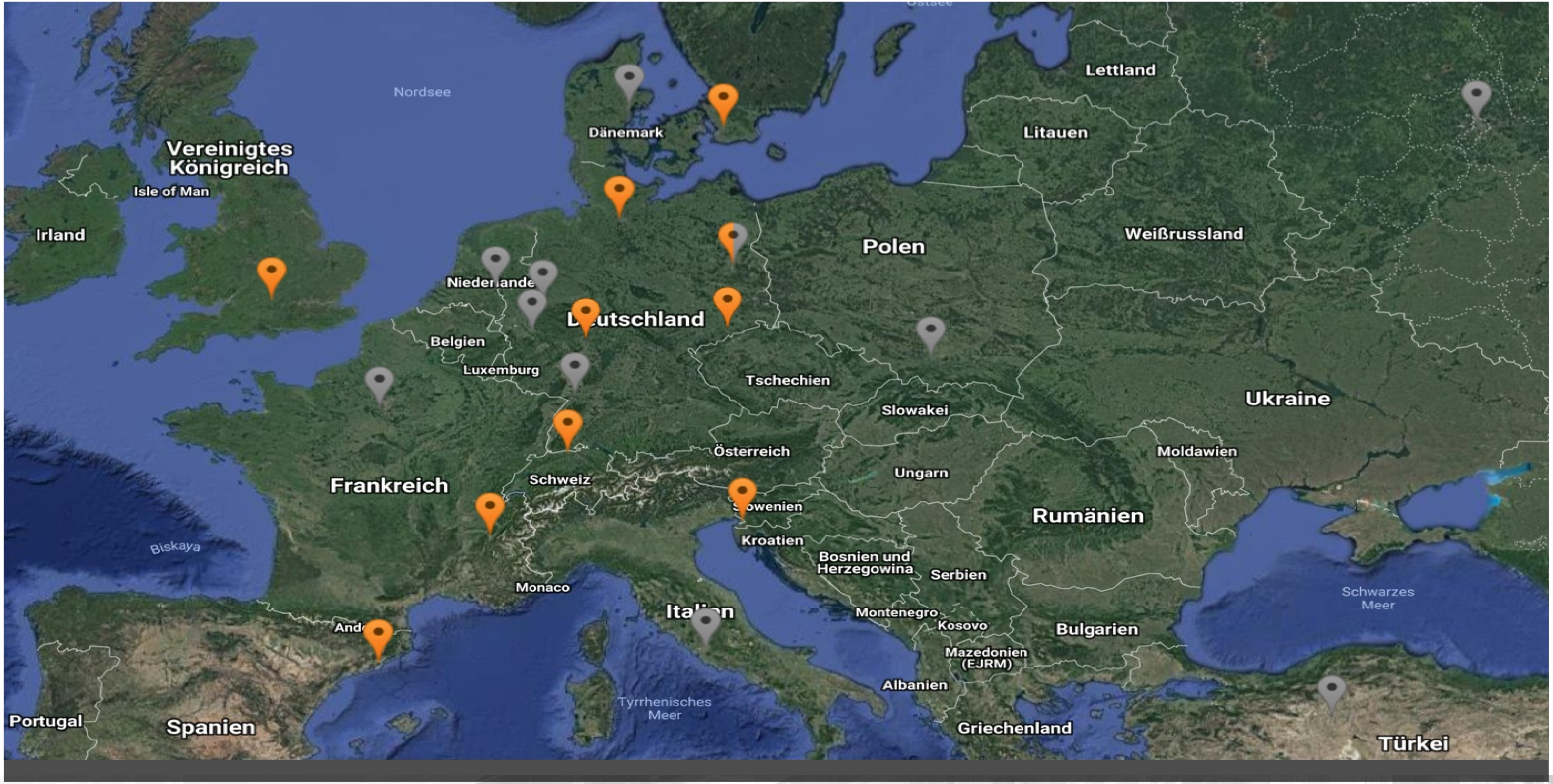
Bunch compressor

THz undulator

Electron beam
cw: up to 130 MeV
Lp: up to 187 MeV

Polish Free electron Laser

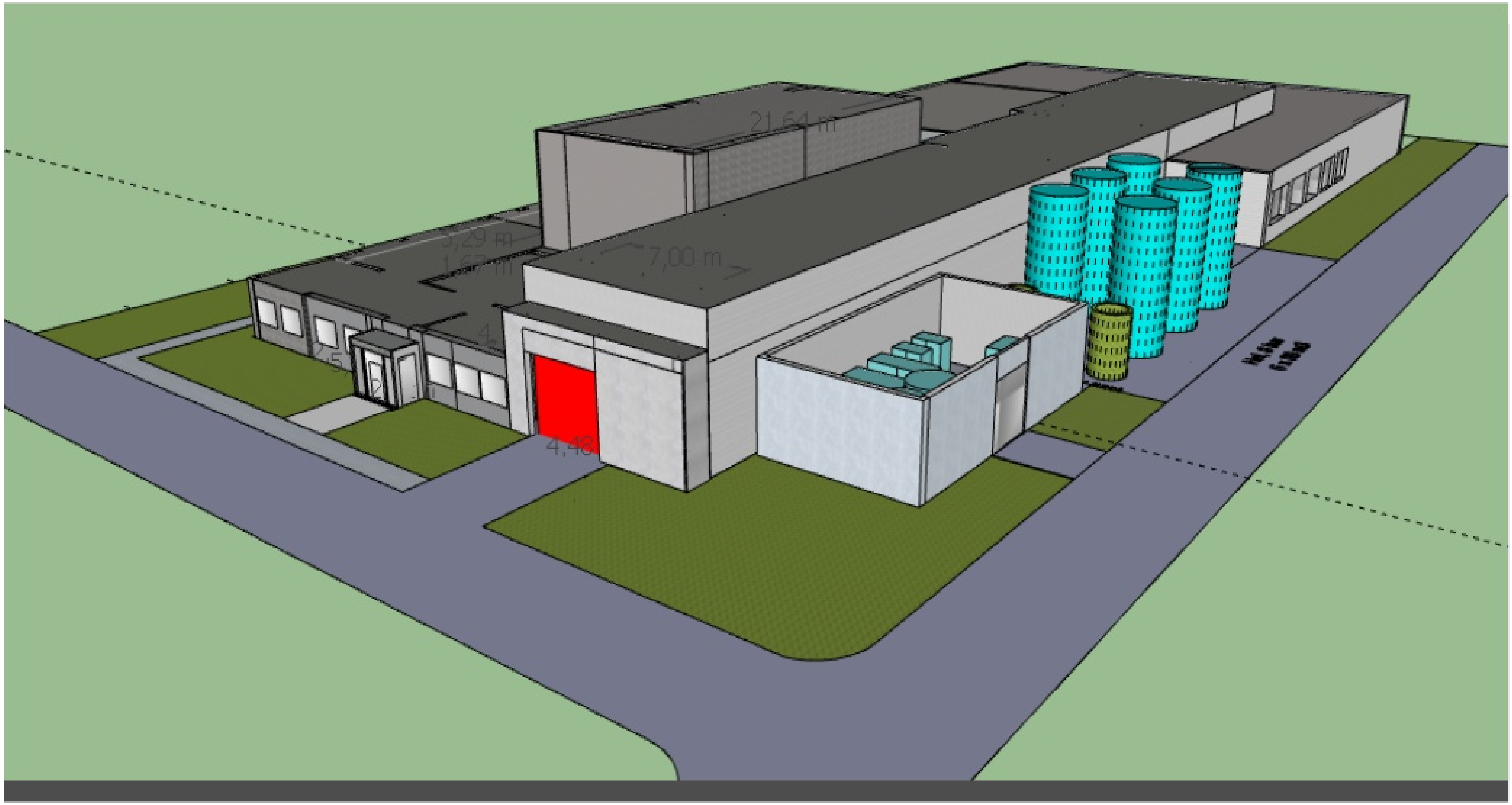
Photon sources are available mostly in the western Europe and very few facilities operate in the eastern European countries.



Courtesy Lightsources.org

● Orange marked laboratories are members of the Lightsourcce.org

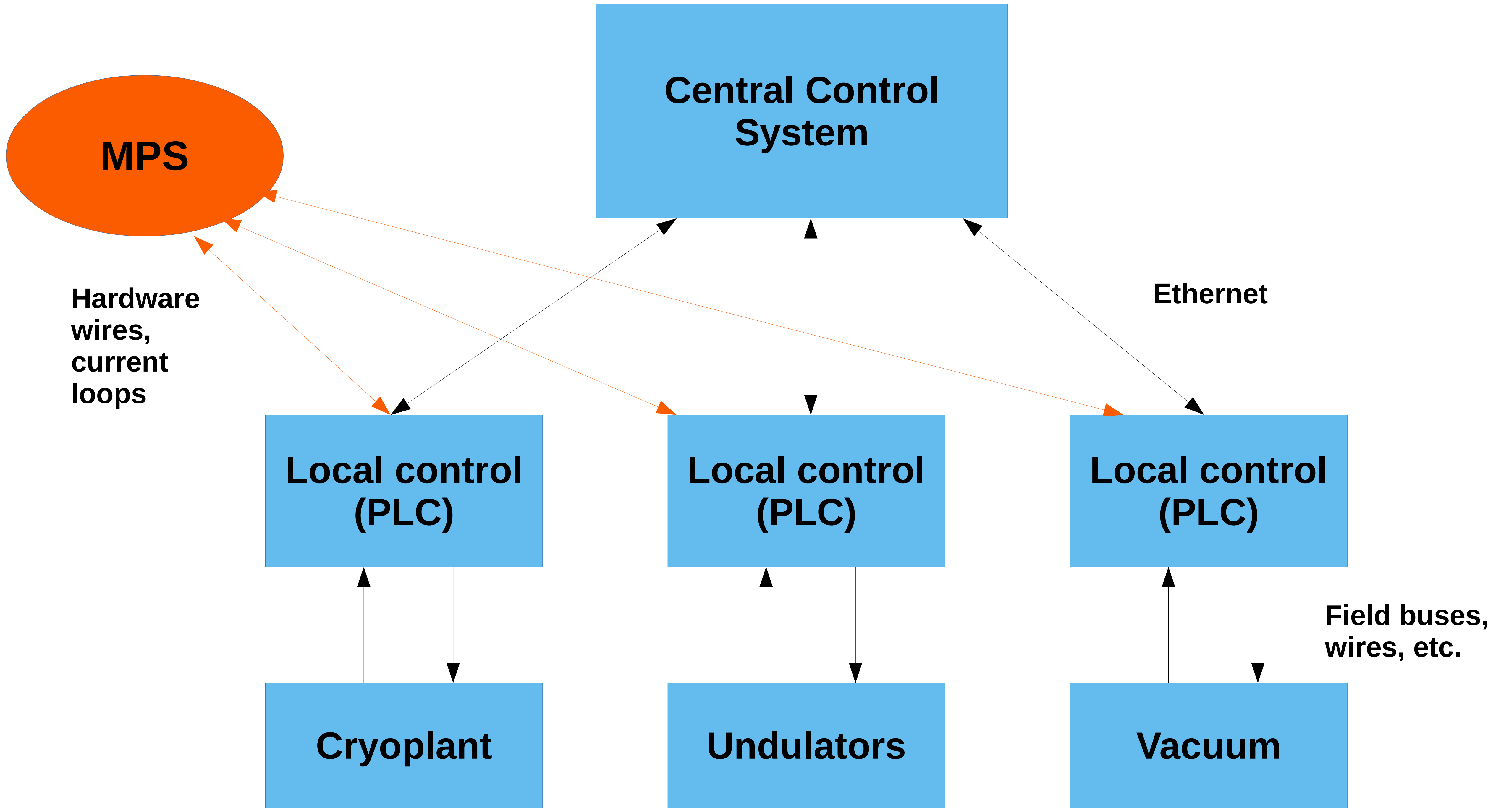
Polish Free electron Laser



PolFEL will need PLC control for (at least) following areas:

- MPS, PSS & Interlocks
- Cryogenic system distribution
- Cryogenic helium liquefier system
- Vacuum control
- Undulators adjustment
- Solid-state RF Power Amplifiers
- User experimental stations
- Possibly also other systems like conventional installations (such as power distribution, HVAC, etc.)

Philosophy: independent local control system managed from the central level



CyberLAB – a PLC testing group

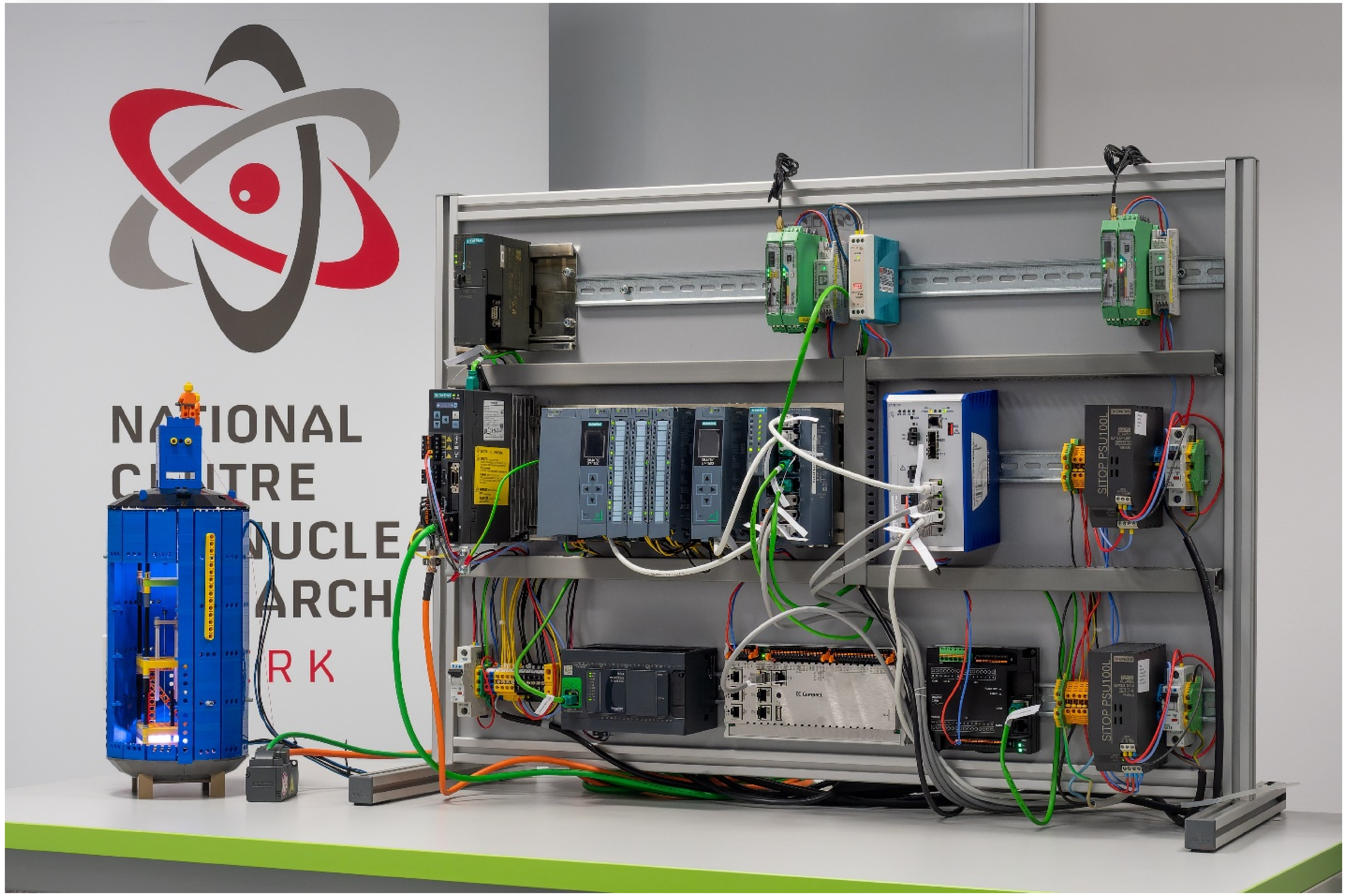
- Founded in 2016 as a part of large IAEA project gathering 20 institutes from 13 countries:
  „**Enhancing Computer Security Incident Analysis at Nuclear Facilities**”

- The detailed project (task) was defined as:
  „**Testing of PLCs Used in Nuclear Installations by Fuzzing methodology for Cyber Vulnerabilities**”

- The aim of work was to workout methodology of testing PLCs against the vulnerabilities

- The “**Fuzzing**” method was chosen, which is smart, automated and adaptive error injection based on the protocol analysis

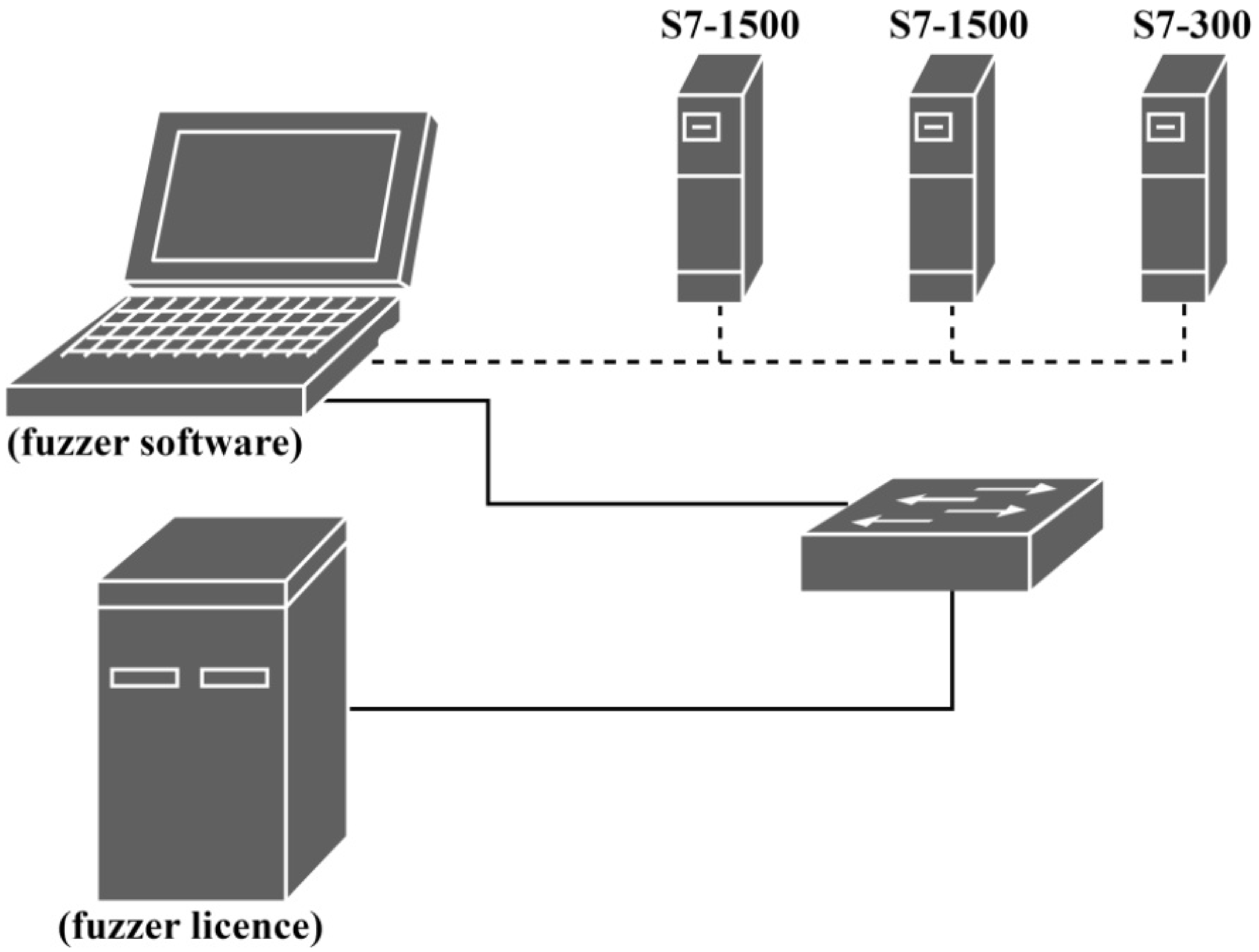
CyberLAB – a PLC testing group



- Well-equipped laboratory:
  - Multi-vendor PLCs,
  - HMIs,
  - Virtual systems (VMs) with different PLC vendors software software,
- Fuzz testing of PLCs using the *Defensics* Fuzzer,
- Advanced cyber-attacks simulations
  - Testing security solutions
  - Education and building threat awareness

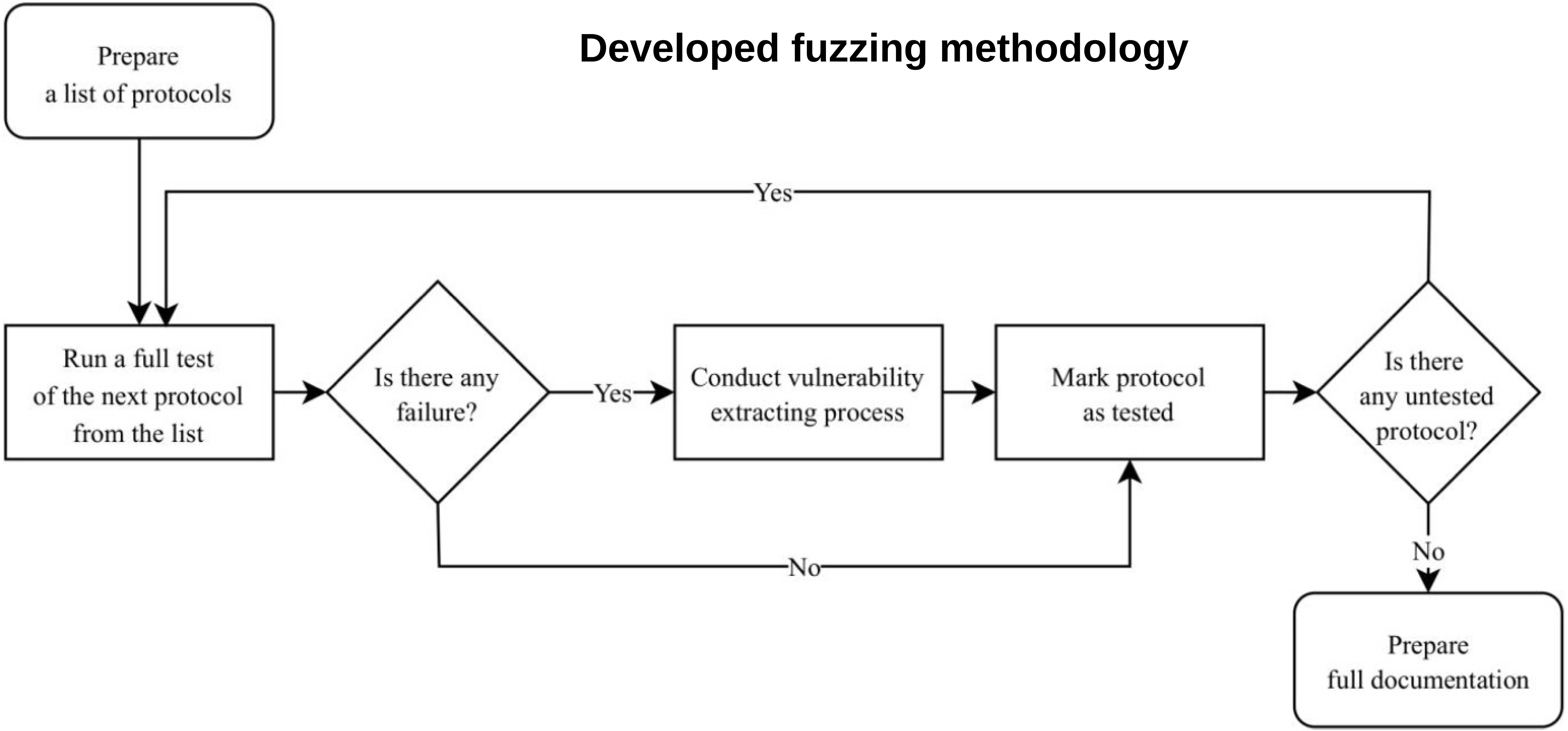
CyberLAB – a PLC testing group

Test setup in the laboratory



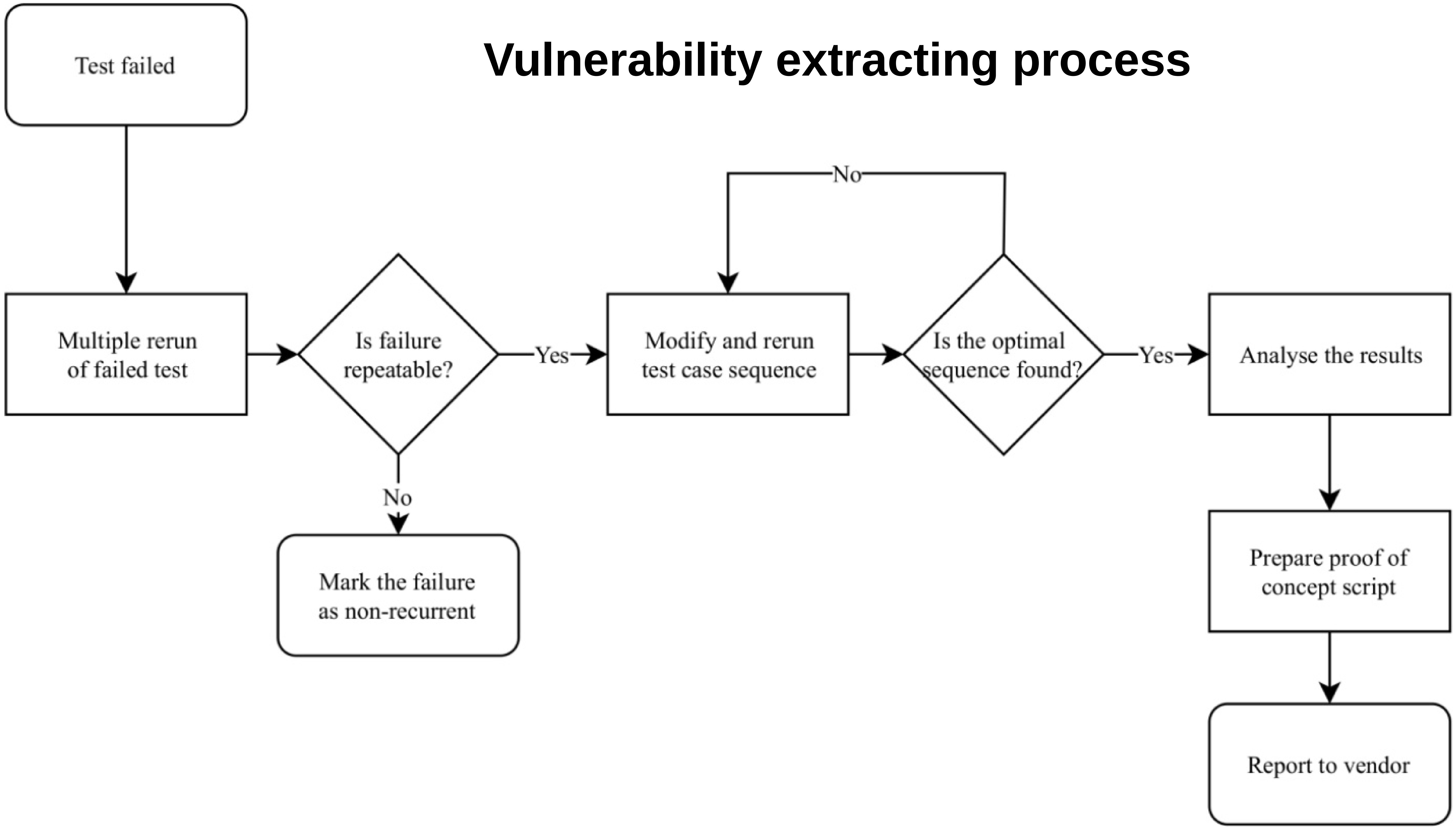
CyberLAB – a PLC testing group

Developed fuzzing methodology



CyberLAB – a PLC testing group

Vulnerability extracting process



Test failed
Multiple rerun of failed test
Is failure repeatable?
Yes
No
Mark the failure as non-recurrent
Modify and rerun test case sequence
Is the optimal sequence found?
No
Yes
Analyse the results
Prepare proof of concept script
Report to vendor

CyberLAB – a PLC testing group

Several vulnerabilities has been found

Most important ones:

- a zero-day vulnerability in Siemens S7-1500 controller (**CVE-2018-13805**)

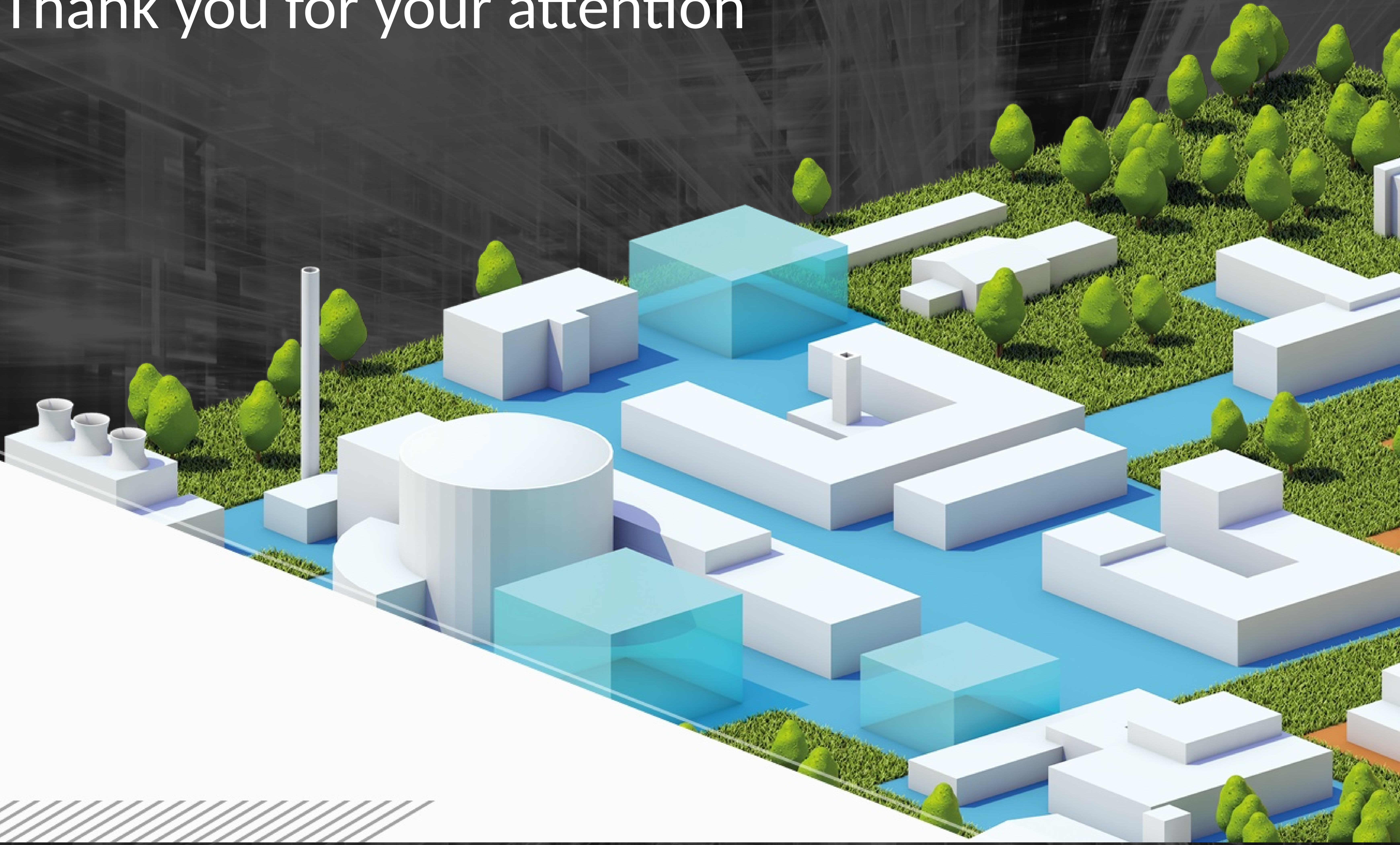
- a zero-day vulnerability in Schneider Electric M241 controller (**CVE-2021-22699**)

The team:

- Joanna Walkiewicz,
- Jakub Suchorab,
- Krystian Szefler,
- Marcin Dudek,
- Jacek Gajewski

Contact: CyberLab@ncbj.gov.pl

Thank you for your attention



NATIONAL
CENTRE
FOR NUCLEAR
RESEARCH
ŚWIERK

www.ncbj.gov.pl