NCP

NATIONAL CYBERSECURITY PLATFORM

Polish Approach to Protect the State’s Cyberspace

Michal Marks, Marek Amanowicz

Research and Academic computer network (Poland)

About project

Project Consortium:

NASK

Warsaw University of Technology

NATIONAL CENTRE FOR NUCLEAR RESEARCH ŚWIERK

INSTYTUT ŁĄCZNOŚCI
PAŃSTWOWY INSTYTUT BADAWCZY

PROJECT DATES:

01.09.2017 – 31.08.2020

Financing Institution:

The National Centre
for Research and Development

Work done as part of the CYBERSECIDENT/369195/I/NCBR/2017 project supported by the National Centre of Research and Development in the frame of CyberSecIdent Programme.

Motivation

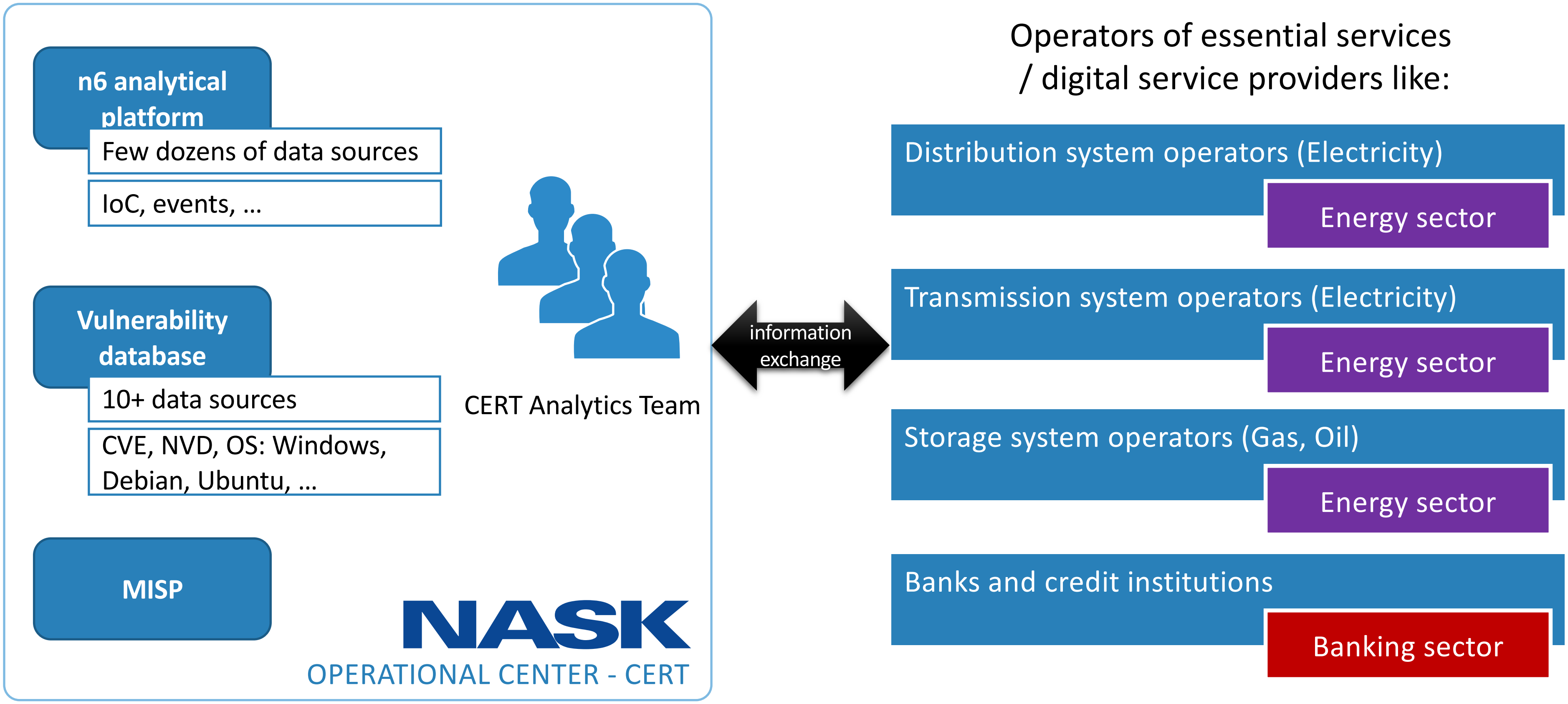
National and International regulations

- The Directive concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – 2016
- Polish Law: National Cybersecurity System (2018)

- US Department of Homeland Security: Need for resilience framework in CIs
- US Department of Homeland Security: National Infrastructure Protection Plan

Motivation

Distributed knowledge and crowdsourcing idea



n6 analytical platform

Few dozens of data sources

IoC, events, …

Vulnerability database

10+ data sources

CVE, NVD, OS: Windows, Debian, Ubuntu, …

MISP

CERT Analytics Team

NASK

OPERATIONAL CENTER - CERT

information exchange

Operators of essential services
/ digital service providers like:

Distribution system operators (Electricity)

Energy sector

Transmission system operators (Electricity)

Energy sector

Storage system operators (Gas, Oil)

Energy sector

Banks and credit institutions

Banking sector

Motivation

Types of exchanged data

Indicator of compromise (IoC)

Events

Sightings

Quality data / comments / confidence ratings

Reports / analysis

RAW data

- logs
- binary files
- context (eg. malware configuration)

Incidents

Vulnerabilities in OS, software, configuration

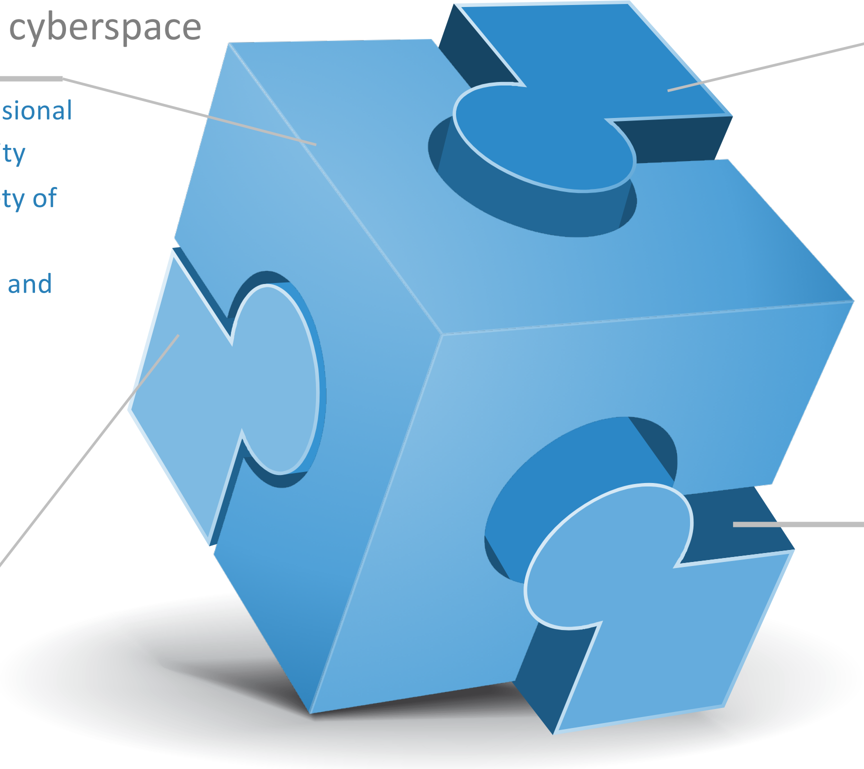
Risk assessments

Surveys coming from essential services providers

Project results

Prototype of interactive system for monitoring and visualization of actual security status of national cyberspace

Operator interface with multidimensional visualization of national cybersecurity status, taking into account the variety of information including threats, sectoral and geographical affiliation and the criticality for national security.



Expert system for decision support

Identification of essential services operators, digital service providers and relationships between services and entities in key sectors.

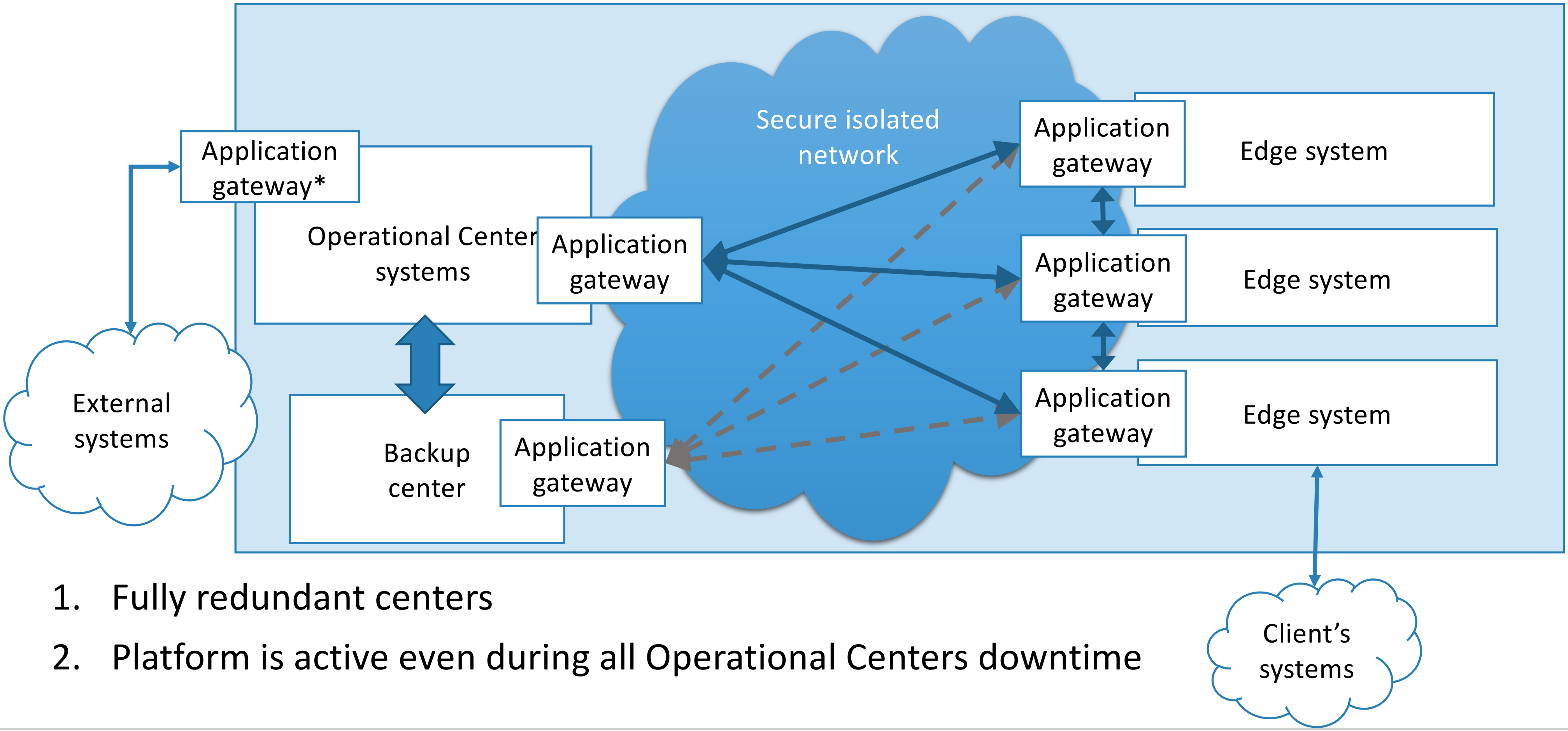
Methods for dynamic and static risk analysis

Based on actual cyberspace security status, estimating risks for essential cyber services.

Tools for vulnerabilities and threats detection

Tools and methods for detection of threats in ICT, IoT and Industrial Automation environments.

Platform architecture



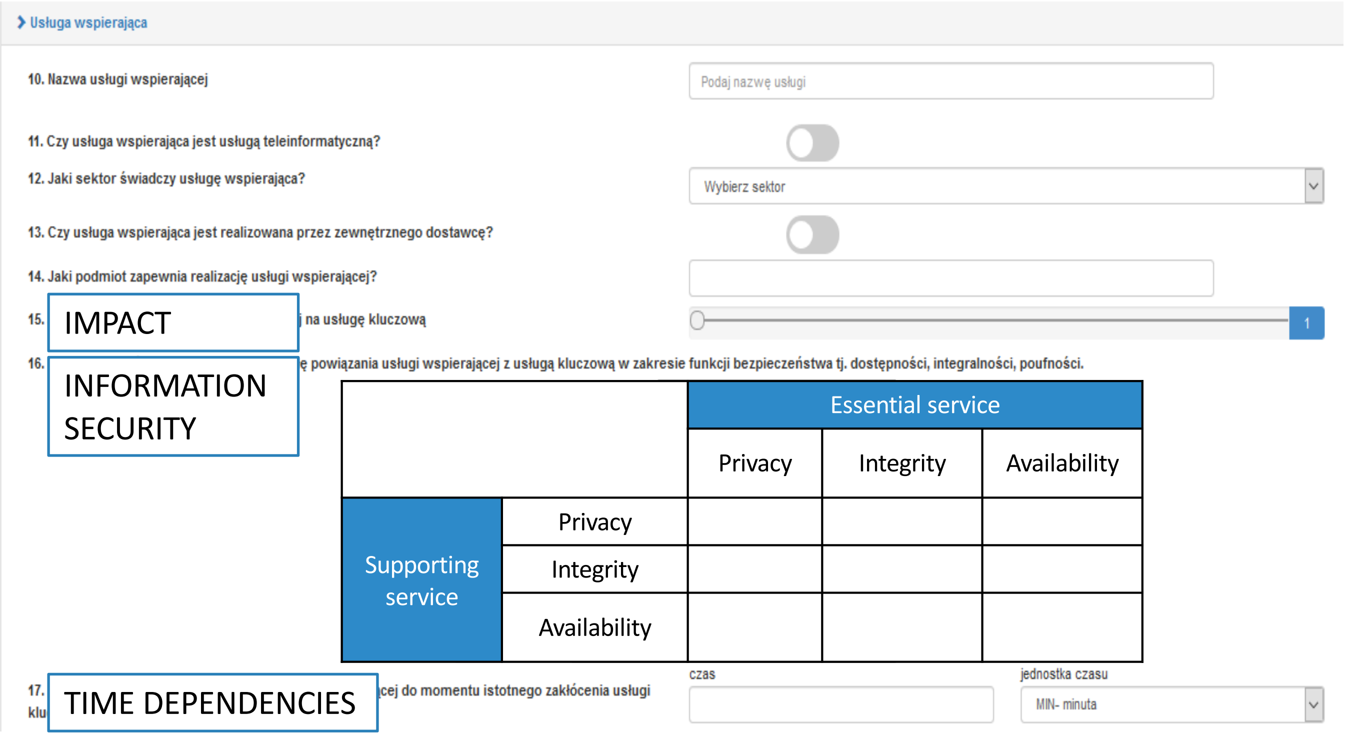
1. Fully redundant centers
2. Platform is active even during all Operational Centers downtime

Decision support system based on crowdsourcing

Modelling essential and supporting services

The relationship is modelled by:

- impact
- information security
- time dependencies



Usługa wspierająca

10. Nazwa usługi wspierającej — Podaj nazwę usługi

11. Czy usługa wspierająca jest usługą teleinformatyczną? ○

12. Jaki sektor świadczy usługę wspierająca? — Wybierz sektor

13. Czy usługa wspierająca jest realizowana przez zewnętrznego dostawcę? ○

14. Jaki podmiot zapewnia realizację usługi wspierającej?

15. IMPACT j na usługę kluczową — 1

16. INFORMATION SECURITY ę powiązania usługi wspierającej z usługą kluczową w zakresie funkcji bezpieczeństwa tj. dostępności, integralności, poufności.

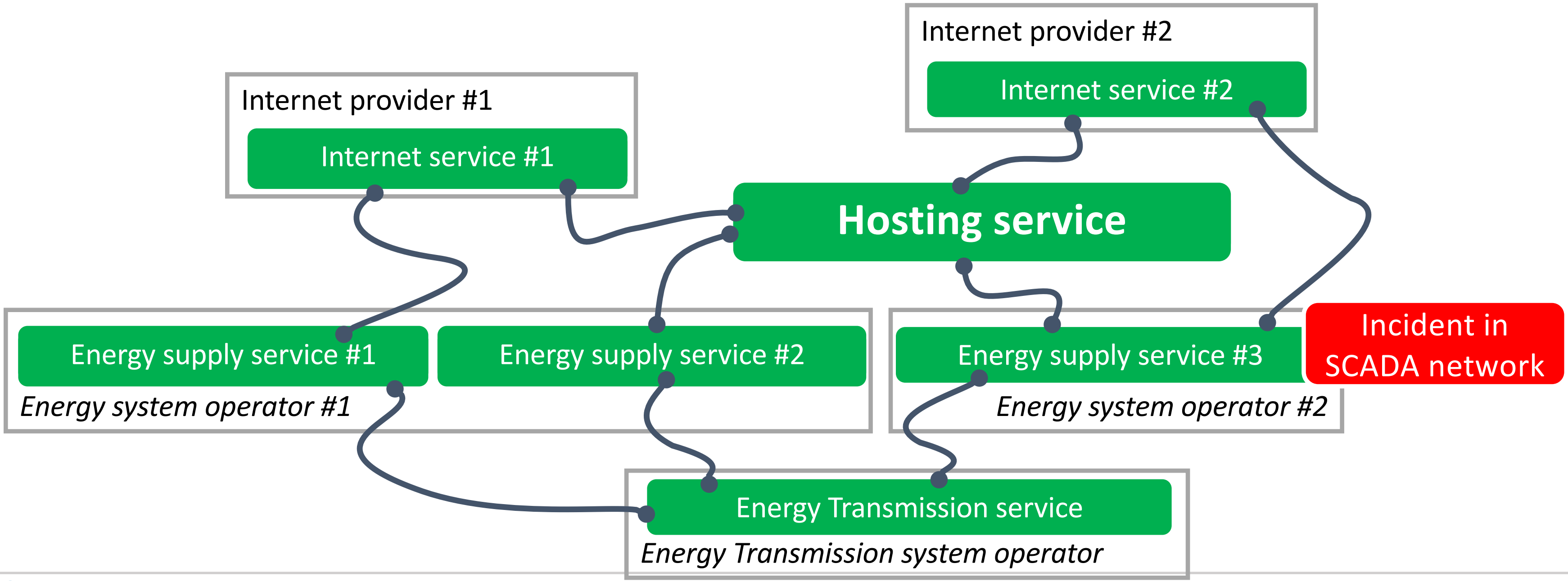
		Essential service		
		Privacy	Integrity	Availability
Supporting service	Privacy			
	Integrity			
	Availability			

17. klu TIME DEPENDENCIES ącej do momentu istotnego zakłócenia usługi — czas: — jednostka czasu: MIN- minuta

Decision support system based on crowdsourcing

Map illustrating the links between essential services

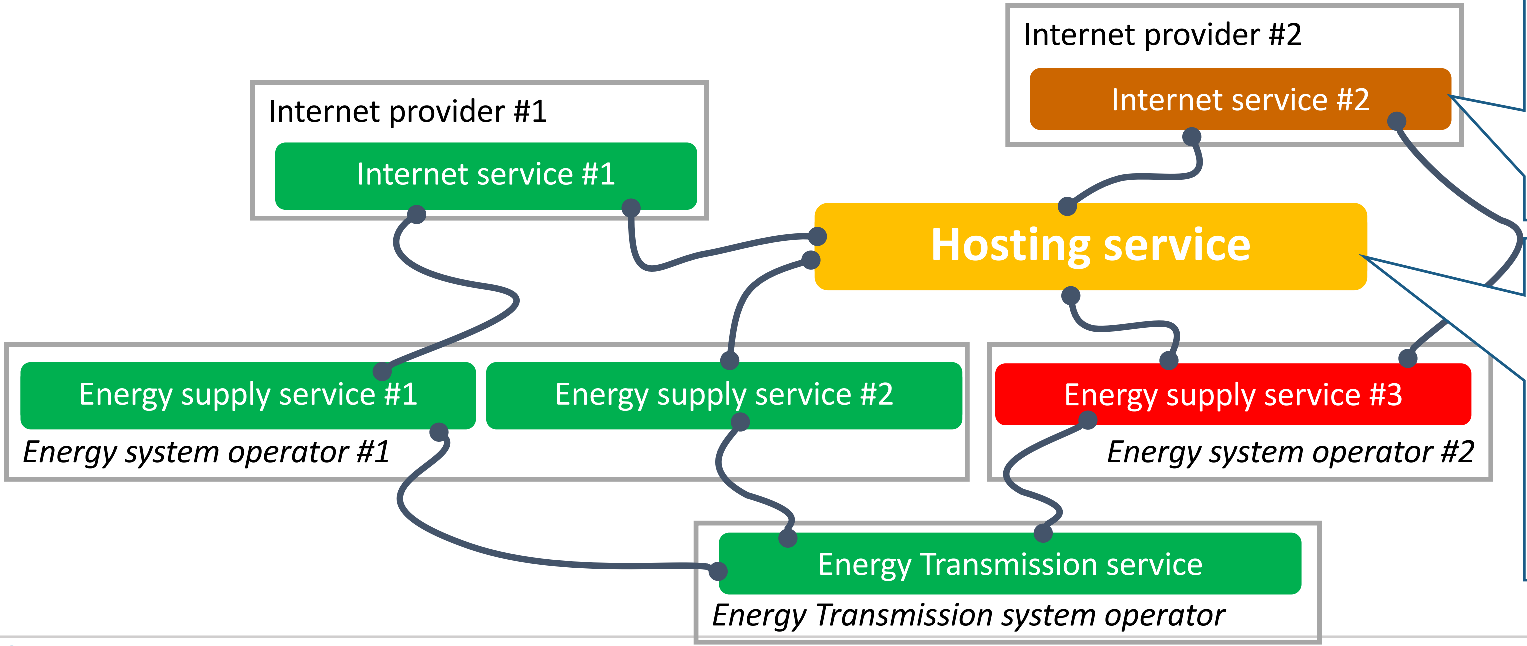
The map illustrating the links between essential services offered by different providers is created to assess the risk of threats propagation between different sectors of economy and their impact on State's security.



Decision support system based on crowdsourcing

Map illustrating the links between essential services

The map illustrating the links between essential services offered by different providers is created to assess the risk of threats propagation between different sectors of economy and their impact on State's security.



The only energy source is broken!
The operator is able to provide it's service by 8 hours!

In 8 hours the hosting company will have just one Internet connection!

One of energy supply services is unavailable!

NCP NATIONAL CYBERSECURITY PLATFORM

NASK

Warsaw University of Technology

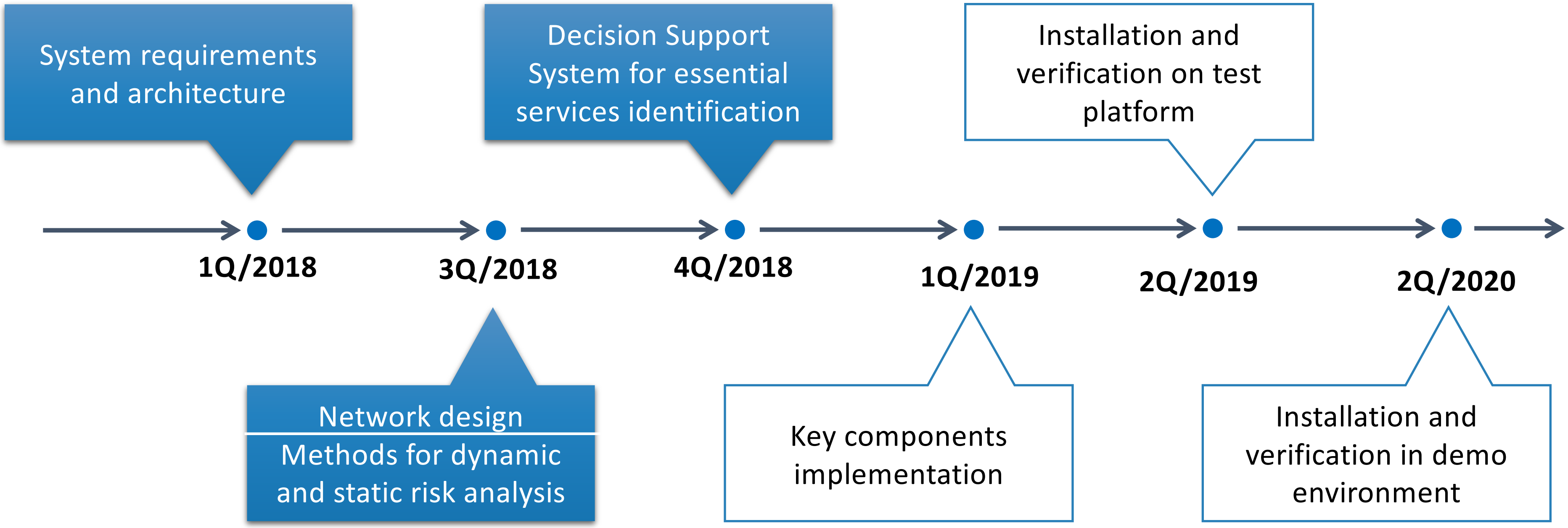
NATIONAL CENTRE FOR NUCLEAR RESEARCH ŚWIERK

INSTYTUT ŁĄCZNOŚCI PAŃSTWOWY INSTYTUT BADAWCZY

The National Centre for Research and Development

CYBERSECIDENT/369195/I/NCBR/2017

Project Timeline


System requirements and architecture
Decision Support System for essential services identification
Installation and verification on test platform
1Q/2018
3Q/2018
4Q/2018
1Q/2019
2Q/2019
2Q/2020
Network design
Methods for dynamic and static risk analysis
Key components implementation
Installation and verification in demo environment