



Unidirectional data  
transmission

Protection of Critical  
and  
Government  
infrastructures

Transfer video  
data to Security  
Operation Center

Info  
-Diode



Segmentation of ICS  
networks

IT

31.10.2022

AMT Group

Unidirectional data gateway  
solutions - InfoDiode  
(datadiode)



PROBLEMS AND THREATS, STANDARDS AND REGULATORY FRAMEWORKS

NETWORKS PROTECTION, MARKET SOLUTIONS and INFODIODE

PROTECTION WITH UNIDIRECTIONAL SYSTEMS

HARDWARE INFODIODE PRODUCTS

HARDWARE AND SOFTWARE INFODIODE SOLUTIONS

# PROBLEMS AND THREATS



## Modern company is no longer «isolated data network»

- ❑ Typical company could have up to 500 data connections with external suppliers, partners, vendors etc.
  - ❑ Cloud based services
  - ❑ Software technical support, IT support services
  - ❑ Data back-up systems
  - ❑ HVAC systems
  - ❑ Security systems (information, physical etc)
  - ❑ Admin and control systems
  - ❑ Supplier and partner systems
- ❑ Usually software in OT/ICS systems is «legacy» software
  - ❑ Mostly IT/ICS software was built without information security requirements, some industrial protocols don't have authentication by design





# Consequences of hacker attacks can be so dramatic

## ❑ Control systems of objects and processes

- ❑ Power and power distribution
- ❑ Water and cooling systems
- ❑ Airconditioning systems
- ❑ Industrial equipment and systems
- ❑ Physical security systems
- ❑ Software security systems
- ❑ Personal data
- ❑ Critical data networks
- ❑ Communication systems



**Privacy  
Integrity  
Availability**

# Hackers interest to industrial objects grows up! More vulnerabilities – more possibilities to hack Critical Infrastructure

- ❑ **Zero-day vulnerability is today reality**
  - ❑ **Attack propagation speed >> security propagation speed**
  - ❑ **Interconnection channel with «victim-system» is a key to successful attack**
    - ❑ Two-way communications is really important at earlier phases – many hack methods based on two-way communications (RAT, phishing, etc.)
  - ❑ **Long-term scenarios are usual practice for hacking**
    - ❑ Using supporting modules for protecting malware from detection
  - ❑ **Attack vector is shifting to the human factor**
- 
- ❑ **Malware software is public available**
  - ❑ **Usually software in OT/ICS systems is «legacy» software**
    - ❑ Mostly IT/ICS software was built without information security requirements, some industrial protocols don't have authentication by design
  - ❑ **“Mess” between company divisions IT, ISec, ICS**



Current trends

# STANDARDS AND REGULATORY FRAMEWORKS



## International standards

- Series of standards ANSI/ISA-62443 for information security management in industrial automation and control systems
- SANS Institute's docs, e.g. Tactical Data Diodes in Industrial Automation and Control Systems Стандарт API Standard 1164. Pipeline SCADA Security (<https://www.sans.org/reading-room/whitepapers/firewalls/tactical-data-diodes-industrial-automation-control-systems-36057>)





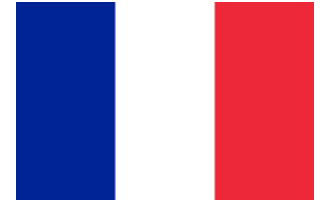
## USA

- «NIST SP800-82. Guide to Industrial Control Systems (ICS) Security» - NIST recommends to use data diodes as an an integral part of boundary protection system  
(<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>)
- NERC. NERC 1300 CIP-002 R3 Routable Protocols and Data Diode Devices  
(<http://www.nerc.com/page.php?cid=3|22|354>)
- NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems  
(<https://us-cert.cisa.gov/ncas/alerts/aa20-205a>)
- Recommended practice: Improving industrial control system cybersecurity with Defense-in-Depth strategies by The Department of Homeland Security (DHS) includes data diodes as a part of security architectures ([https://us-cert.cisa.gov/sites/default/files/recommended\\_practices/NCCIC\\_ICS-CERT\\_Defense\\_in\\_Depth\\_2016\\_S508C.pdf](https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf))
- «Protecting drinking water utilities from cyber threats» by The Department of Energy (DOE)  
(<https://www.osti.gov/biblio/1372266>)
- «Cybersecurity programs for nuclear facilities» by Nuclear Regulatory Commission (NRC)  
(<https://www.nrc.gov/docs/ML1703/ML17031A020.pdf>)



## France

- «Cybersecurity for Industrial Control Systems» by The French National Cybersecurity Agency (ANSSI): ‘The interconnection of a class 3 ICS with an ICS of a lower class shall be unidirectional towards the latter. The unidirectionality shall be guaranteed physically (e.g. with a data diode’.  
([https://www.ssi.gouv.fr/uploads/2014/01/industrial\\_security\\_WG\\_Classification\\_Method.pdf](https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf))



## Great Britain

- «Rail Cyber Security Guidance to Industry» by Department for Transport of Great Britain recommends to use data diodes to protect industry infrastructure  
([https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/732888/rail-cyber-security-guidance-to-industry.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/732888/rail-cyber-security-guidance-to-industry.pdf))



## Germany

- «IT Security In Industrie 4.0» by Federal Ministry for Economic Affairs and Energy (BMWi) recommends to use data diodes for protection and isolation critical zone transitions between IT and OT production systems  
([https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/guideline-it-security-i40-action-fields.pdf?\\_\\_blob=publicationFile&v=3](https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/guideline-it-security-i40-action-fields.pdf?__blob=publicationFile&v=3))



## Singapore

- «Cybersecurity for Industrial Control Systems» by The Singapore Cybersecurity Agency (CSA) recommends to use data diodes for 11 sectors of critical information infrastructure (CII) to increase the network security level  
(<https://www.csa.gov.sg/news/press-releases/press-statement-on-the-government-lifting-the-pause-on-new-ict-systems>)
- «Annex Technology Roadmap» by Cybersecurity Infocom Media Development Authority (IMDA) recommends to use data diodes at the edge of cyber physical systems in facilities such as nuclear power plants, electric power generation/distribution, oil and gas production, water/wastewater and manufacturing  
([https://www.imda.gov.sg/-/media/Imda/Files/Industry-Development/Infrastructure/Technology/Technology-Roadmap/Annexes-A-3-Cyber-Security\\_Full-Report.pdf](https://www.imda.gov.sg/-/media/Imda/Files/Industry-Development/Infrastructure/Technology/Technology-Roadmap/Annexes-A-3-Cyber-Security_Full-Report.pdf))



# NETWORK PROTECTION METHODS





## Typical security methods:

- Using software solutions, primarily - firewalls
- Physical isolation of network segments – «air-gap»



**Each method has its own advantages and disadvantages**

Effectively counteract an attack - means prevent specific stages/consequences of an attack every time such an attack occurs



# INFODIODE from AMT Group



# Unidirectional data gateway works at physical layer

- **Unidirectional data gateway** – device transmitting file and streaming information in one direction only and not allowing reverse transmission
  - One-way transmission guaranteed by hardware solutions
  - Applied to connect different network segments and used in the information security tasks





# All "datadiode" solutions could be divided in two classes

## Hardware «datadiodes»

### Advantages

- Inexpensive
- Solve only basic problems
- Plug & Play
- Don not require maintenance service

### Disadvantages

- Don't have IP, MAC addresses
- Require switching «port-port»
- Can not transfer any two-way directional protocols

## Hardware- software «datadiodes»

### Advantages

- Transmit asynchronous and even synchronous TCP/IP traffic
- Transmit of multiple types of application traffic simultaneously
- Comprehensive information security tool (NAT, access lists, ports, configuration change control, access control)
- Integration: SIEM, SNMP, AD, Syslog, NTP

### Disadvantages

- Can occupy 3 or more rack units
- Require a person to operate with basic skills
- Require periodic (rare) software updates

**Unidirectional, physical  
signal transmitted only  
in one way**

HW InfoDiode effectively combine all the best practices in perimeter protection CI in case of need transmission UDP, Syslog, SPAN, etc. protocols

## HARDWARE INFODIODE



### General description

Basic hardware solution for DIN rail or Desktop installation.

**MINI**



### General description

Basic hardware solution for rack mount

**RACK single**



### General description

Double hardware solution for rack mount (two «diodes» in one device ).

**RACK - double**

HW/SW InfoDiode allows to match best practices in CI perimeter protection, transfer file, industrial and other protocols



## HW/SW INFODIODE PRO

Basic option	Cluster option
InProxy, OutProxy server	2 InProxy, 2 OutProxy servers
InfoDiode, rack module	2 InfoDiode, rack module, cluster
3U rack units	6U rack units

“Diode” outside



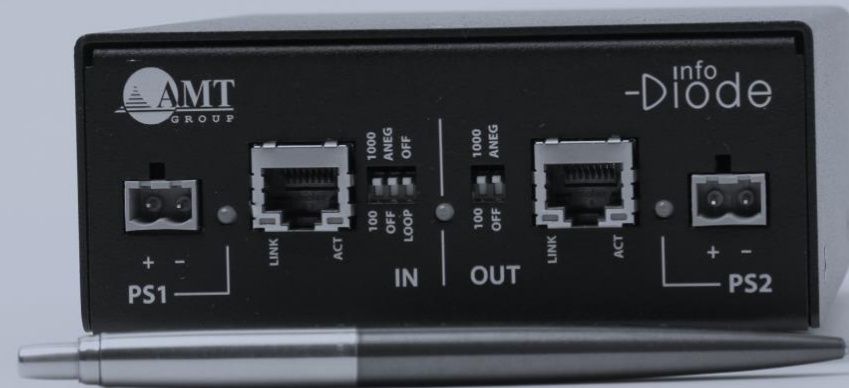
## HW/SW INFODIODE SMART

Basic option
InProxy, OutProxy server
«diode» inside
1U rack unit

“Diode” inside

# HARDWARE SOLUTIONS

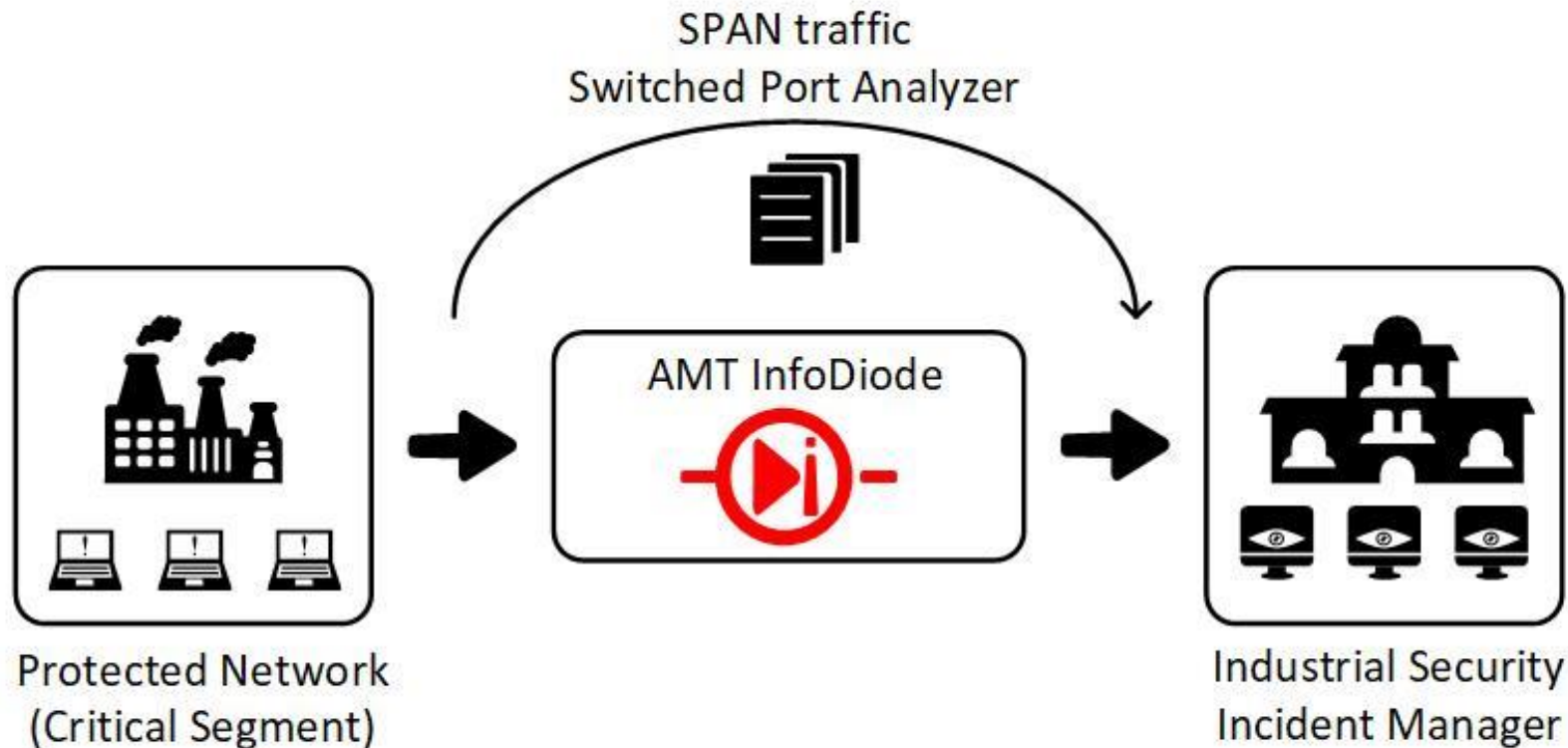
## INFODIODE





# SPAN-mirroring

**Option 1.** Transfer a copy of the technological traffic of the closed segment to the external monitoring system using SPAN. The copy of technological traffic is transmitted to the external system for in-depth traffic analysis, which provides the search for traces of information security violations in the ICS networks, helps at an early stage to detect cyberattacks, malware activity, unauthorized actions of personnel (including malicious acts)

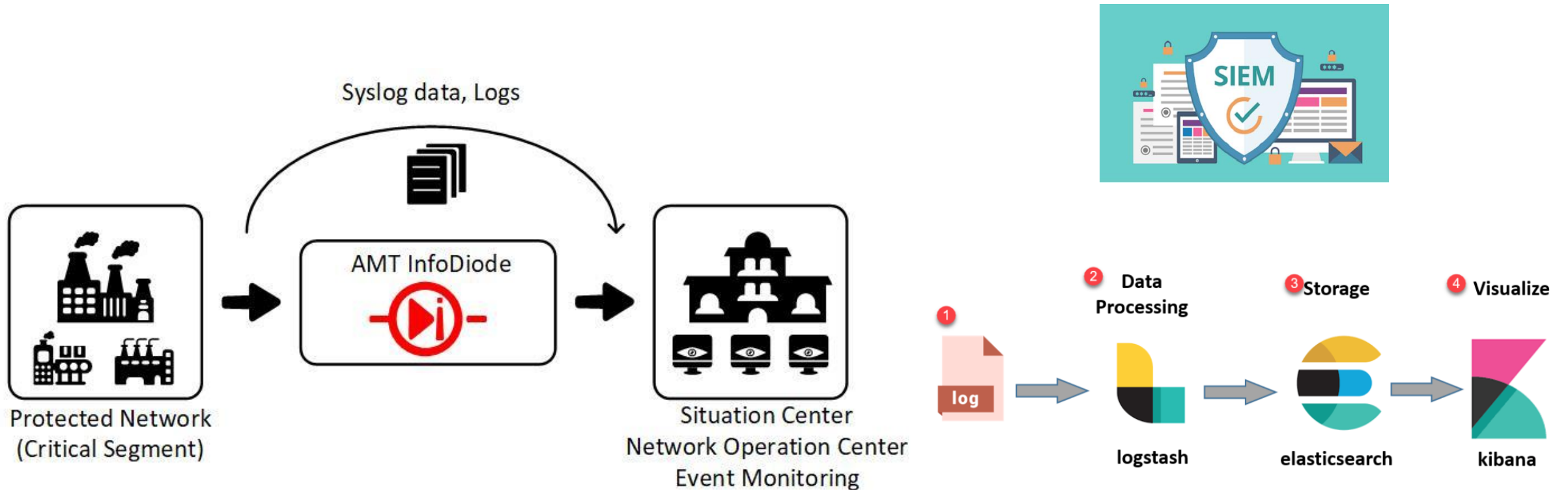


PT ISIM



# Transfer data to NOC or SOC via HW InfoDiode

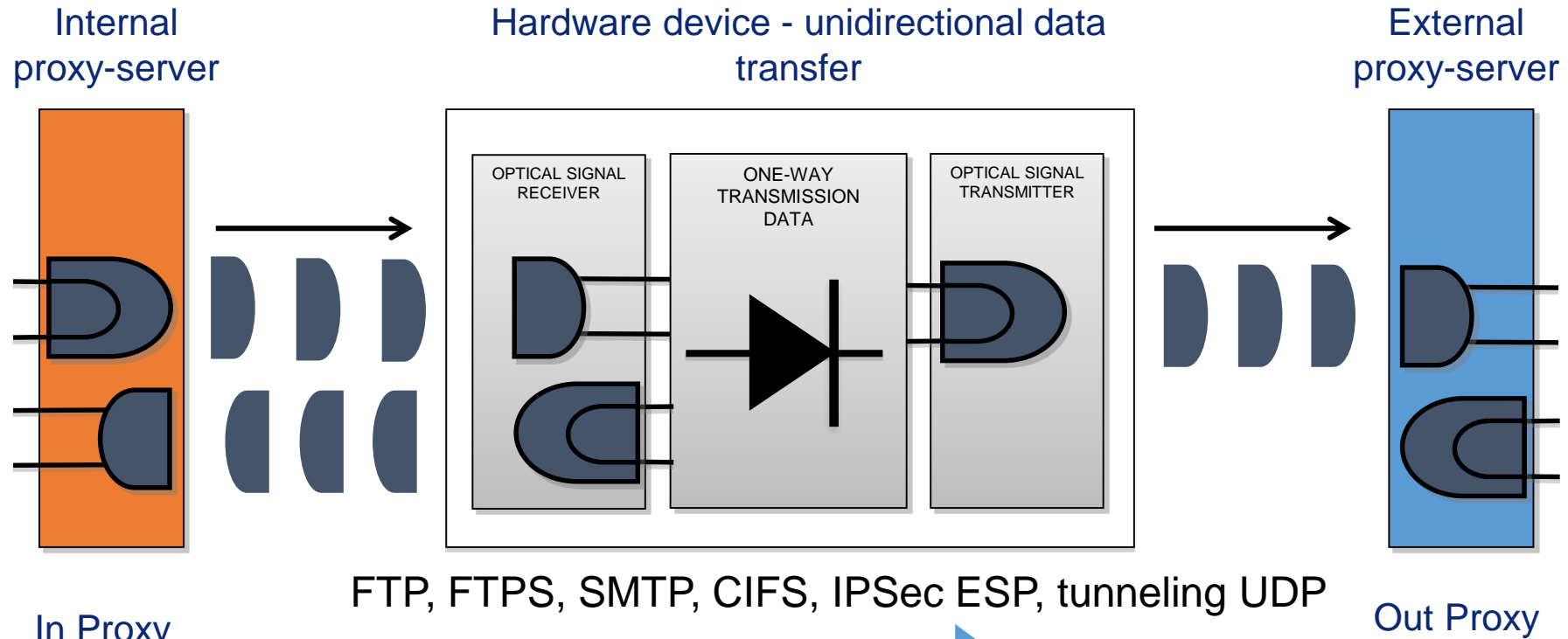
**Option 2.** Transfer ICS network events using Syslog to an external monitoring system. Logging of events within the technological segment in a centralized event monitoring system allows to significantly reduce the probability of occurrence of accidents and consolidate all data in a situation center.



# HARDWARE-SOFTWARE SOLUTIONS

## INFODIODE PRO

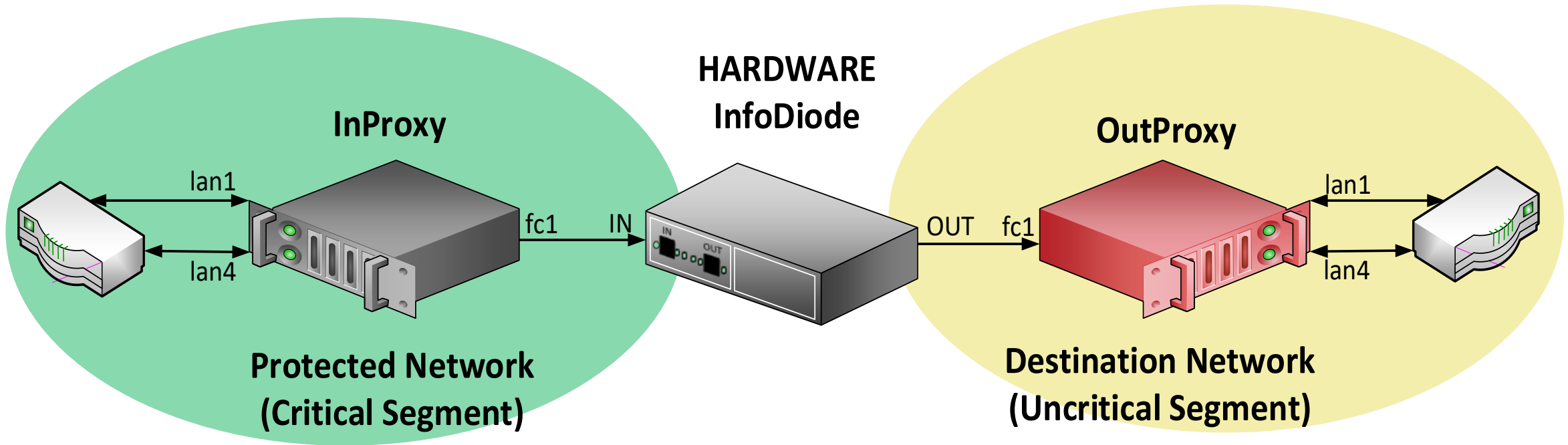




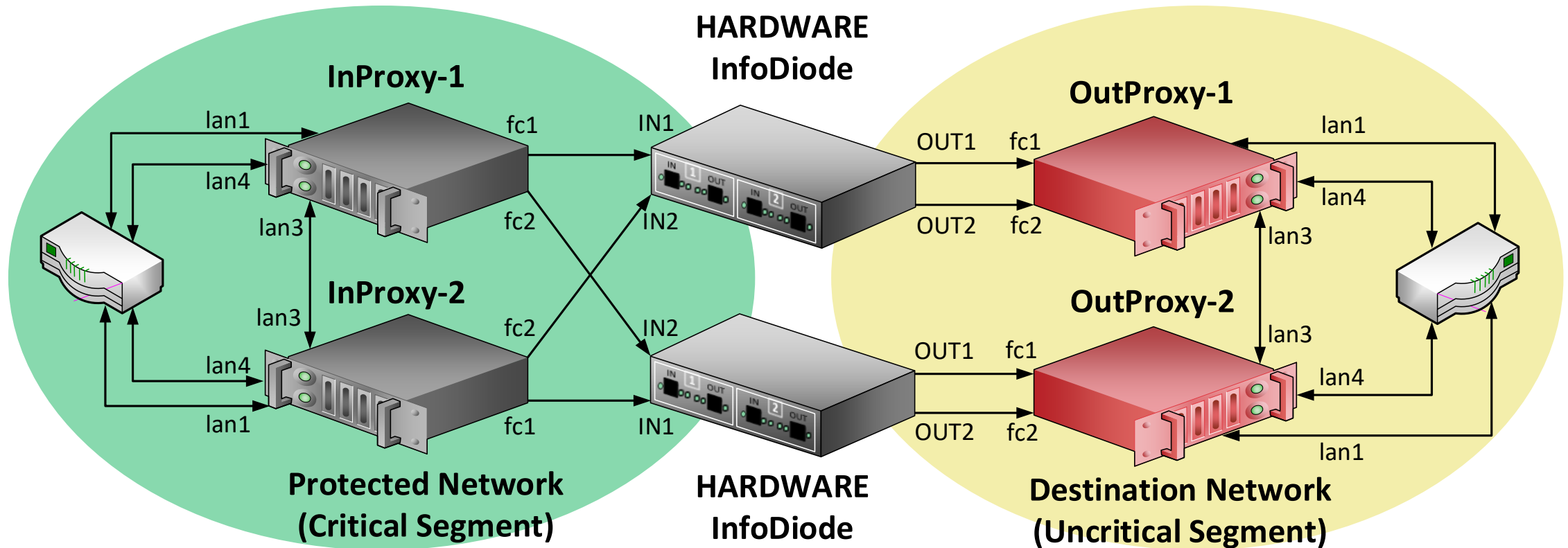
Possible

Impossible





Duplication of all elements



The screenshot shows the 'Network interfaces' section of the InfoDiode PRO web interface. It features a table with columns for ID, Ping, Pub., Man., IP Address, and MAC address. Five interfaces (eth1 to eth5) are listed, each with a power icon, a ping checkbox, and a manual checkbox. A 'Save' button is located below the table.

ID	Ping	Pub.	Man.	IP Address	MAC address
eth1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.50/24	00:e0:ed:35:68:1b
eth2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.1/24	54:a0:50:85:d8:41
eth3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10.0.187.187/24	54:a0:50:85:d8:42
eth4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.50/24	54:a0:50:85:d8:43
eth5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		

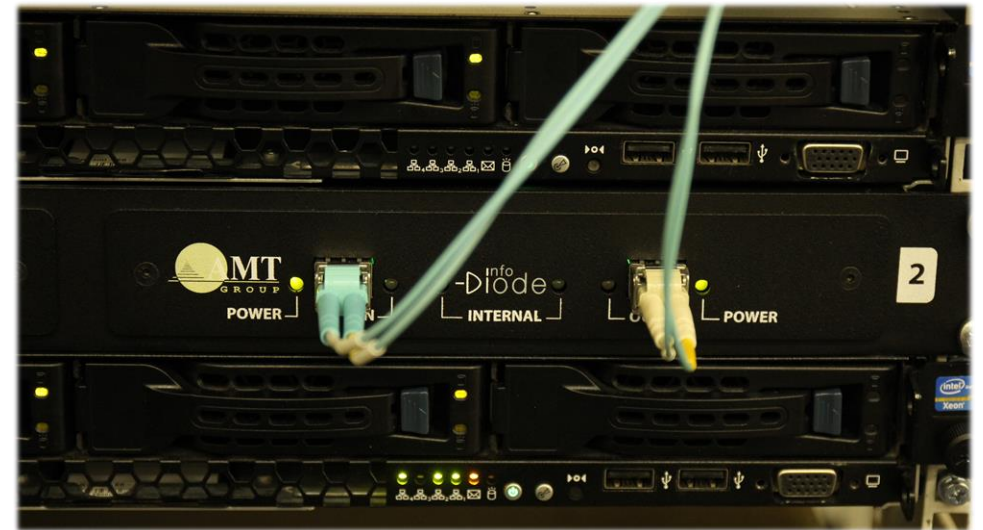
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<server target="tx" version="1.0"
xmlns="urn:ru:amt:diode:config:server:1.0">
  <language>en</language>
  <country>RU</country>
  <timeZone>Asia/Yerevan</timeZone>
  <license/>
  <subsystems>
    <subsystem
xmlns="urn:ru:amt:diode:config:subsystems:udp:1.0">
      <enabled>true</enabled>
      <rule enabled="true">
        <src address="192.168.188.0/24"/>
        <dest address="192.168.188.0/24"/>
      </rule>
    </subsystem>
  </subsystems>
</server>
```

The screenshot shows the 'UDP Tunneling' section of the InfoDiode PRO web interface. It features a table with columns for Enabled, Source, Destination, NAT source, and NAT destination. One tunneling rule is listed, which is enabled and has a source of 0.0.0.0/0 and a destination of 192.168.1.1/32:4000. An 'Add route' button is located below the table.

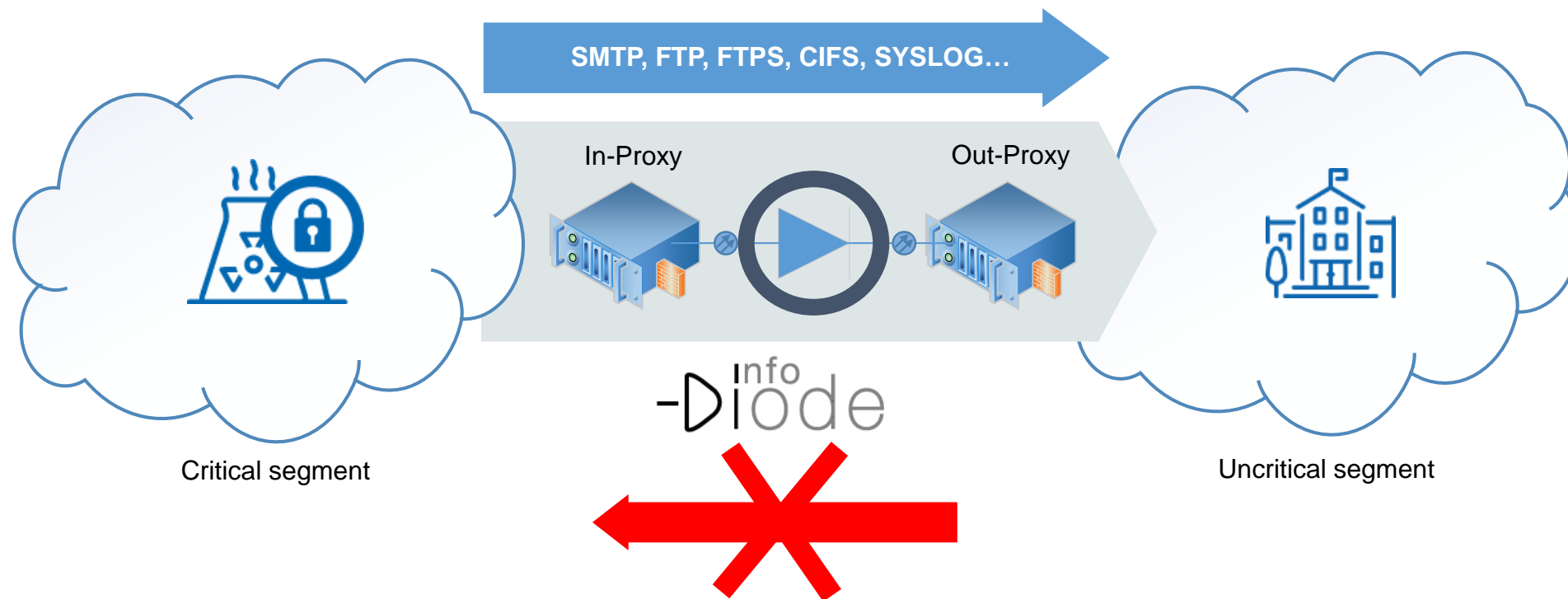
Enabled	Source	Destination	NAT source	NAT destination
<input checked="" type="checkbox"/>	0.0.0.0/0	192.168.1.1/32:4000		192.168.2.2:5000

- User-friendly Web-interface
- Possibility of control using CLI and XML
- Special protection mode against accidental changes

- Throughput UDP - 900 Mbps
- Performance of proxy-services – 300 Mbps
- Protocols: FTP/FTPS, CIFS, SMTP, SFTP etc..
- Prioritization of data/threads
- Noiseless coding
- Configuration/system backup
- Syslog/SIEM integration
- NTP sync
- Integration with AD
- Creating meta-information file for analysis by DLP (Read), Syslog Audit
- SNMP v2c and v3, syslog



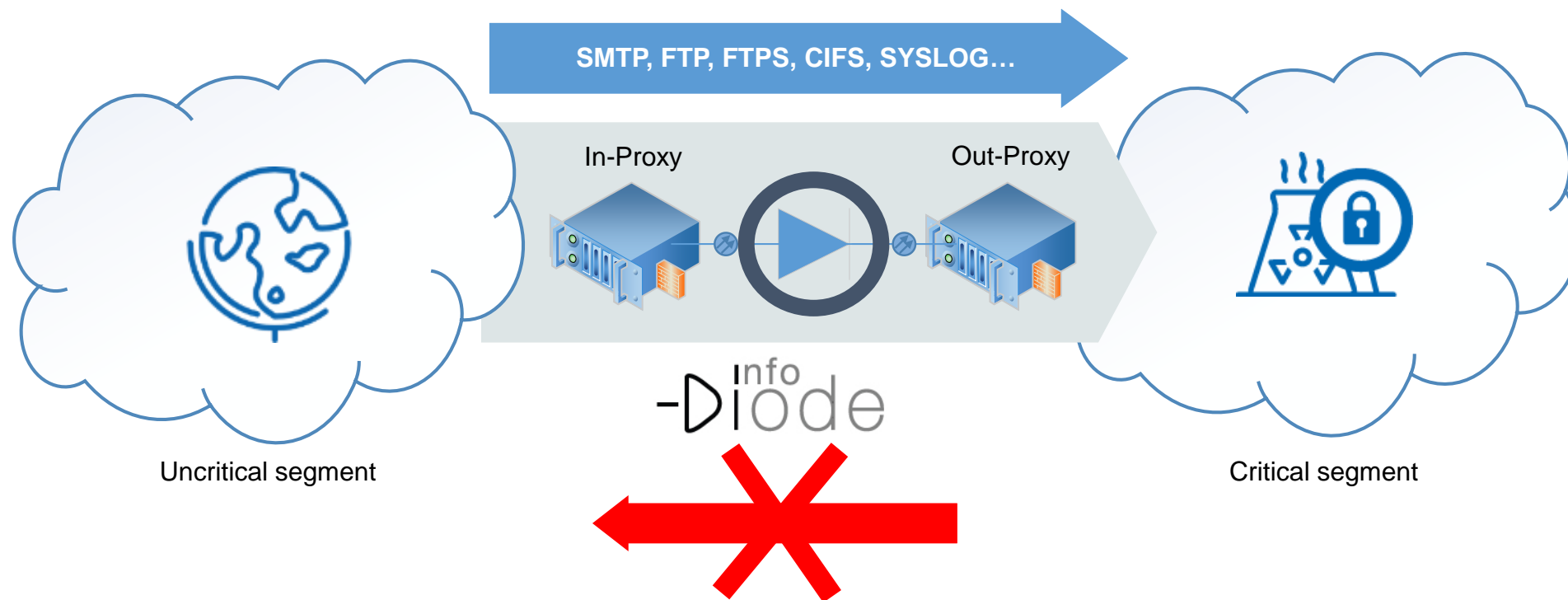
# Scenario 1 - Unidirectional data upload from the critical/ICS technology segment



- **Unloading Data from Critical Segments**
- **Information from outside must be excluded**
- **Possibility of controlling the object must be excluded**



## Scenario 2 - Unidirectional data upload to a protected information system

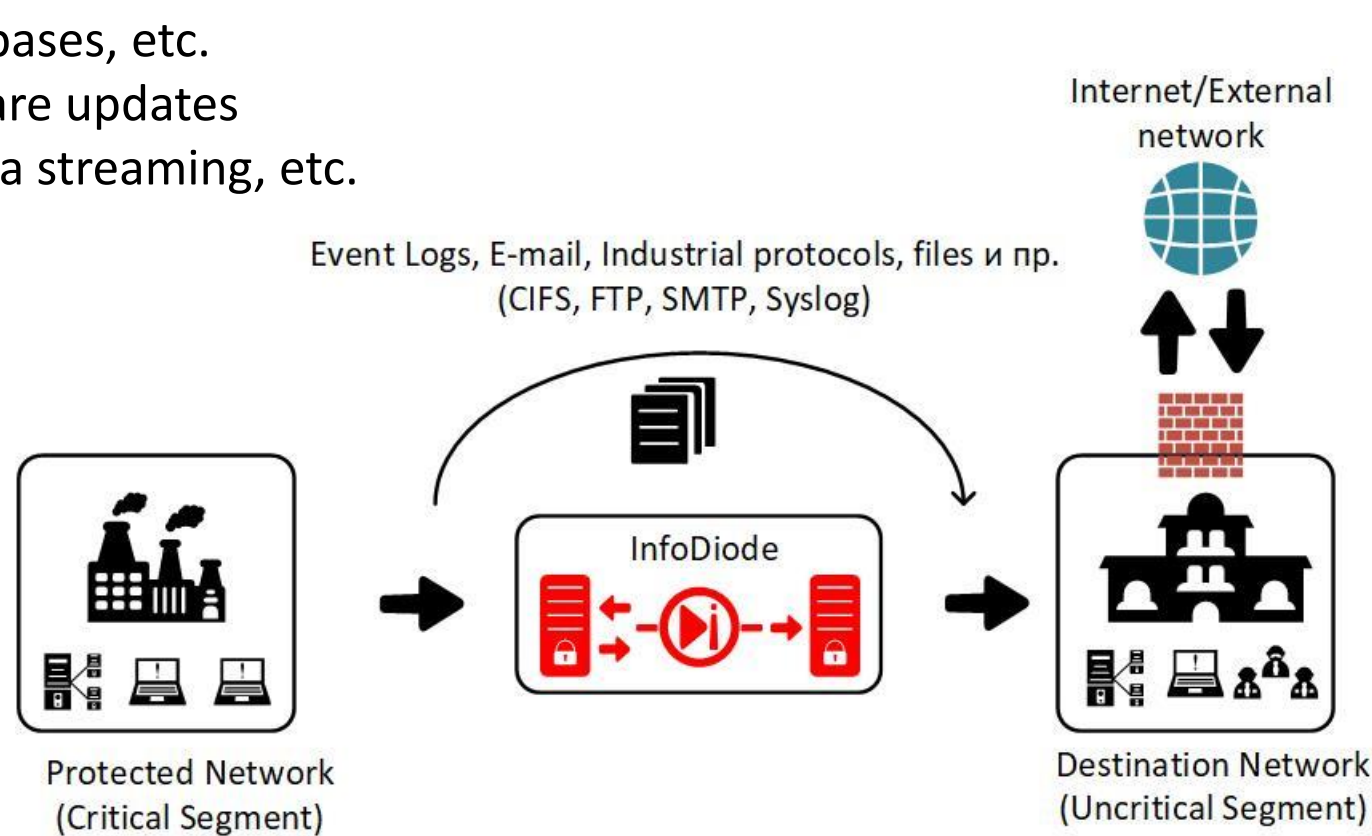


- **Uploading data to confidential information systems**
- **It is not possible to «leak» data from critical information systems**
- **The possibility of controlling the object must be excluded**

## Option 1. Data export

In this scenario, the integrity of the transmitted data is guaranteed.

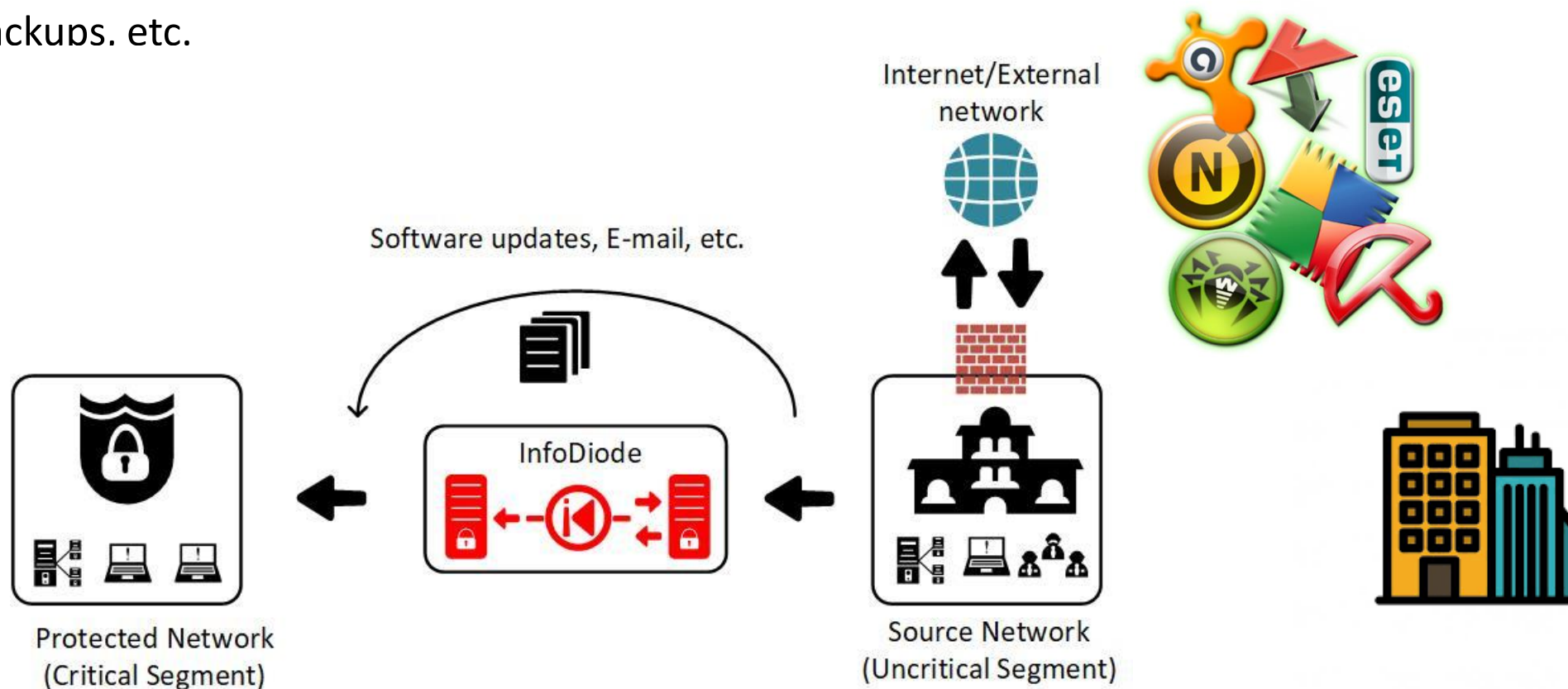
- Export of data to NOC/SOC
- Replica VM, databases, etc.
- Transfer of software updates
- Video camera data streaming, etc.



## Option 2. Data import

In this scenario, the confidentiality of the protected data is guaranteed.

- Download Updates
- Storage of backups. etc.



# HARDWARE-SOFTWARE SOLUTIONS

## INFODIODE SMART





## INFODIODE SMART



### ❑ CI Protection and Monitoring

Provides protection and monitoring of the CI object, excluding any impact on it.

### ❑ Support of industrial protocols OPC UA, Modbus, MQTT

Provides secure remote interaction of critical segments of individual enterprises and organizations through untrusted networks. Transmits data out of the trusted perimeter of the network using protocols OPC UA, Modbus, MQTT, FTP(S), COIFS, SFTP, UDP, etc.

### ❑ The Foundation for Digital Twins

Transfers replicas of critical information resources (OPC servers, SCADA major vendor systems) beyond the perimeter of the ICS and CI for further processing and analysis.

### ❑ Centralized movement control and situation centers

Provides the centers with real online data, including video recording, in conditions of guaranteed isolation of observation objects.

### ❑ Aggregation of data from SCADA systems to ERP, MES and «clouds»

Transmits data from multiple SCADA systems to ERP, MES systems, cloud solutions, eliminating any feedback from these systems.

# Typical scenarios of Infodiode SMART I


1



Office

For management and external workers

2



Aggregation  
SCADA, MES, ERP, Hist.


Control and monitoring of infrastructure

3




NOC/SOC,  
Government, etc


Situation control and reporting



ICS



ICS of company



Corporation




Field/floor level



# Typical scenarios of Infodiode SMART II

4



Head office

Supply chains and nomenclatures

5



Internet

Patches and updates

6



Vendors, suppliers


Replicas, databases



Company



Company



Corporation



Field/floor level

# Typical scenarios of Infodiode SMART III

7



Departments:  
SOC, NOC, archives

Control of IS, network,  
confidential and backup  
segments



Company

8



Counterparties.  
(educational  
institutions, etc.)

Important information,  
data for research



Company

9



End users

Data for infomats, visual  
panels,



Company



Field/floor level

# Thank you