пт 15.03.2024

Комплексные проекты с применением решений InfoDiode.

Решения InfoDiode – как интеграционный элемент в ИТ и ИБ инфраструктуре промышленного объекта.

ПЛАН

- Контекст, «новости», следующие шаги развития InfoDiode
- Сценарии применения InfoDiode как части интеграционных решений

ПЛАН

- Контекст, «новости», следующие шаги развития InfoDiode
- Сценарии применения InfoDiode как части интеграционных решений

Значимые аспекты применения СЗИ на объектах АСУ ТП

1. СЗИ это не только средство защиты, но и интеграционный инструмент, **сопрягающий системы и данные на прикладном уровне**

2. Для ряда предприятий выполнение 166 Указа Президента критично и не сводится просто к закупке каких-то решений. Нужны Ad hoc решения. **Сроки выполнения близятся**

3. **Процессы пуско-наладки и установки СЗИ.** Процесс не должен предполагать остановки объекта

4. **Процессы обновлений СЗИ и того, что защищают СЗИ**. В условиях «усиленной защиты» или изоляции объекта по-новому встает вопрос обновлений ПО и мониторинга – особенно выполняемых централизованно и мультивендорно

Инфраструктура СЗИ по некоторым направлениям строится фактически с нуля

AMT GROUP

Обмен данными между сегментами с разными уровнями доверия – это множество вызовов

1. **Увеличение интенсивности обмена** в рамках производственных циклов, обмена данными с контрагентами и органами власти

2. **Возможность утечки данных по тем же каналам**, которые используются для сопряжения доменов, систем

3. **Рост атак на ранее редко атакуемые типы устройств:** ПЛК, IP камеры, UPS, СХД, СРК

4. Появление в составе вредоносного кода **фрагментов «под АСУ ТП»** (конкретного сектора, предприятия)

5. Атаки не всегда ведут к «убыткам». У части киберпреступников мотивом является **длительное присутствие**

6. **Компрометация вендоров** (в том числе СЗИ) для организации атаки, использование обновлений ПО, патчей в качестве инструмента атаки

7. **Рост количества атак на ИТ-ресурсы топ-менеджеров, руководство**, в том числе в целях использования в качестве «плацдарма» для развития атаки

AMT GROUP

АМТ-ГРУП: полная линейка решений класса «диод» для защиты КИИ, ОПО, АСУ ТП и ИТ инфраструктуры

1. **АК InfoDiode** – базовое аппаратное решение, гарантирующее защиту на аппаратном уровне и эффективно решающее задачу по передаче UDP, Syslog, SPAN трафика

2. **АПК InfoDiode PRO** – решение для передачи значимых файловых потоков, дистрибутивов, реплик ВМ и баз данных, электронной почты, бэкапов и т.п.

3. **АПК InfoDiode SMART** – решение для передачи за пределы периметра КИИ промышленных протоколов, в том числе видео, для интеграции SCADA систем, организации удаленных ситуационных центров за границей периметра, в условиях гарантированной изоляции КИИ

InfoDiode включен в реестры, завершена его сертификация

1. **Сертификаты ФСТЭК (УД4)** – на всю линейку решений
2. **Реестр Минпромторга** – включены и аппаратный, и программно-аппаратный комплексы
3. **Реестр Минцифры** – программное обеспечение
4. **Сертификаты и декларации ЕАС** – на всю линейку решений

Продукты InfoDiode совместимы со многими СЗИ, АСУ ТП, ИТ решениями

DIASOFT всё по-настоящему

ТЕРРАЛИНК ТЕХНОЛОДЖИС

КРУГ

Wonderware Historian

kepware

Decima

СВД Встраиваемые Системы

MasterOPC www.masteropc.ru

ISS

TIA V17

Атомик Софт

MasterSCADA

NAUMEN

WinCC Professional

PostgreSQL

Windows Server Update Services

Microsoft SQL Server

ELK

ZABBIX

kafka

RabbitMQ

Kaspersky Private Security Network

КВАЗАР

ARMA INFOWATCH ARMA

CyberLympha DATAPK

MaxPatrol SIEM

PT ISIM

axxtel

Kaspersky Industrial CyberSecurity

AMT GROUP

ПЛАН

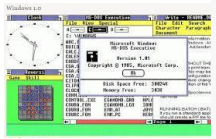
Контекст, «новости», следующие шаги развития InfoDiode

Сценарии применения InfoDiode как части интеграционных решений

Новые сценарии интеграционных обменов

1. Обмен в файлами в неспецифичных условиях
2. Специфичные отраслевые протоколы (типа IEC104)
3. Видео-потоки из закрытого сегмента
4. «Цифровой двойник»
5. Передача данных через интеграционные шины
6. Передача данных из систем класса Deception
7. Защита АСУ ТП со стороны «полевого» уровня

Файловый обмен в «старых» сегментах



1. «Старая» операционная система
2. Нет специалистов для написания скриптов
3. Старый софт – не предполагает какой-либо настройки

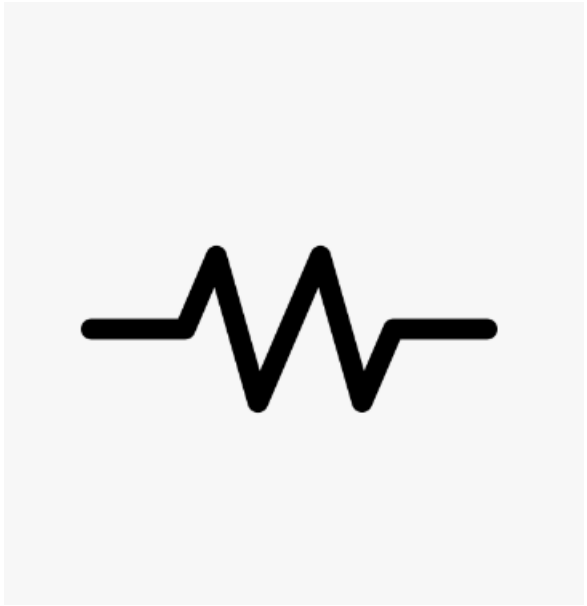
- Забираем по расписанию
- Поддерживаем FTP/CIFS/SFTP
- Поддерживаем действия с забираемыми файлами
- Несколько endpoint – несколько систем

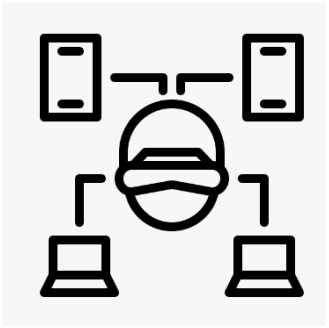
1. Новый софт (сервисы, обработка нескольких файлов)
2. Требуется получать информацию о приеме файла
3. Файлы читаются, как только приходят

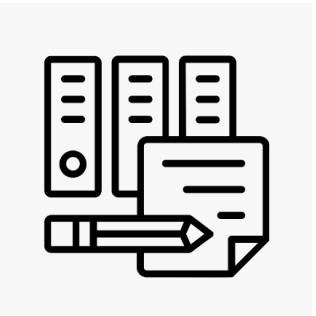
- Выкладываем во временные папки
- Выкладываем с временным расширением
- Уведомляем по REST
- Выкладываем по нужному протоколу
- Несколько endpoint – несколько систем

AMT GROUP

Передача специальных отраслевых протоколов типа IEC104 и др.



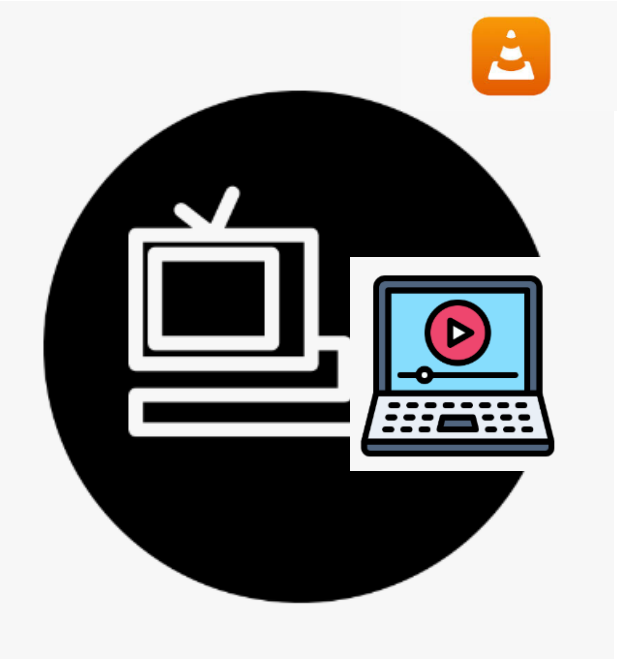




- Решается не только применением InfoDiode
- Нужны профильные системы, которые используются в конкретной инфраструктуре
- Большая часть SCADA решений, которые работают на местах, умеют отдавать данные в InfoDiode

- Получатели данных с объекта энергетики - не только РДУ, но и иные потребители, не связанные с диспетчеризацией
- Часто инф. потоков и протоколов с объекта энергетики несколько (FTP в АСКУЭ, IEC-104 и вариации, OPC UA)

Передача данных систем видеонаблюдения за пределы сетевого периметра

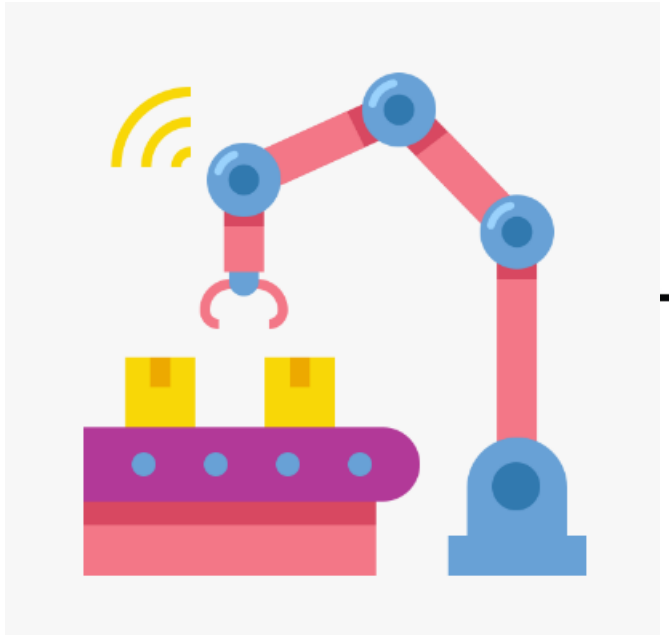


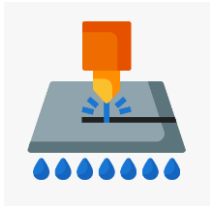
- InfoDiode позволяет передавать выборочный трафик из комплексной системы видеонаблюдения
- Есть возможность стримить конкретные камеры по запросу

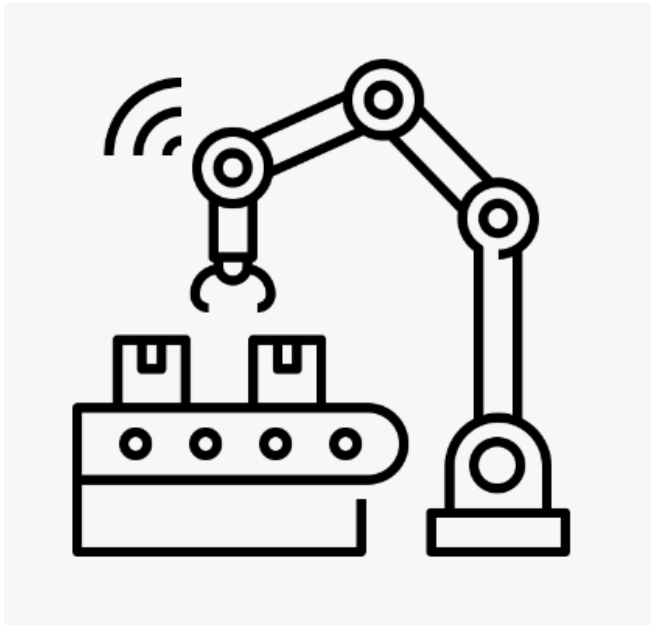
- InfoDiode позволяет передавать трафик видеонаблюдения, исключая воздействие на систему видеонаблюдения
- Возможно просматривать трафик обычными средствами операционных систем

AMT GROUP

«Цифровые двойники»







- InfoDiode может передавать и «атомарные данные», и агрегированные показатели (OEE и т.п.)
- Типовым протоколом в такого рода обменах через InfoDiode служит OPC UA
- Производительность InfoDiode достаточна (свыше 100 тыс. тегов/сек)

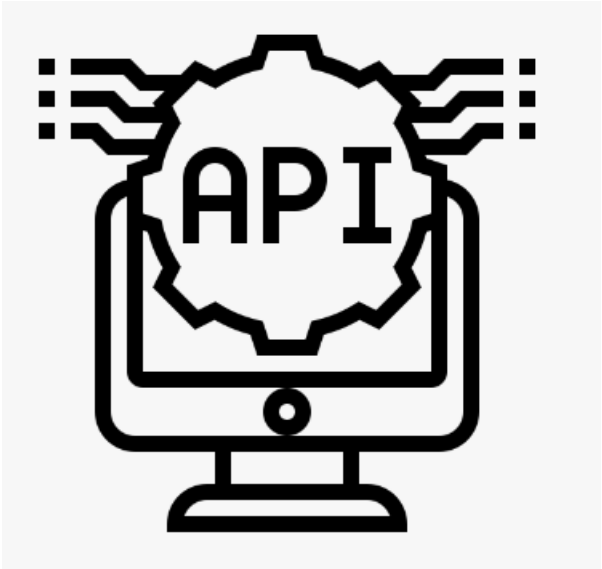
- InfoDiode позволяет создавать «цифровой двойник» предприятия как в целях диспетчеризации, так и в целях прогнозирования и планирования, обучения
- InfoDiode позволяет передать все данные, необходимые для MES

AMT GROUP

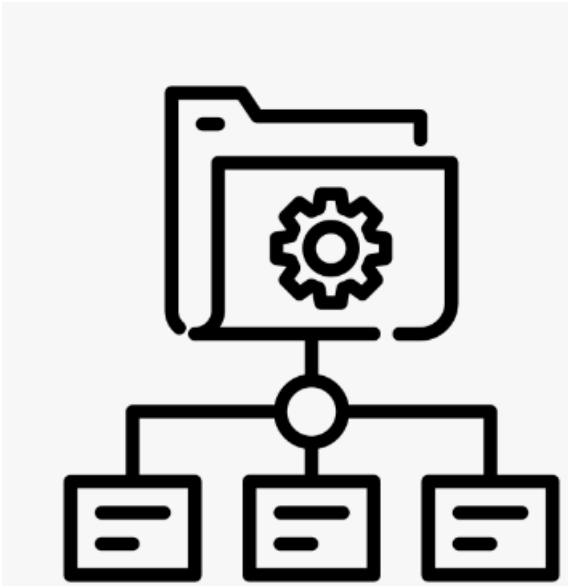
Обмен данными через интеграционные шины

RabbitMQ

kafka



info Diode



RabbitMQ

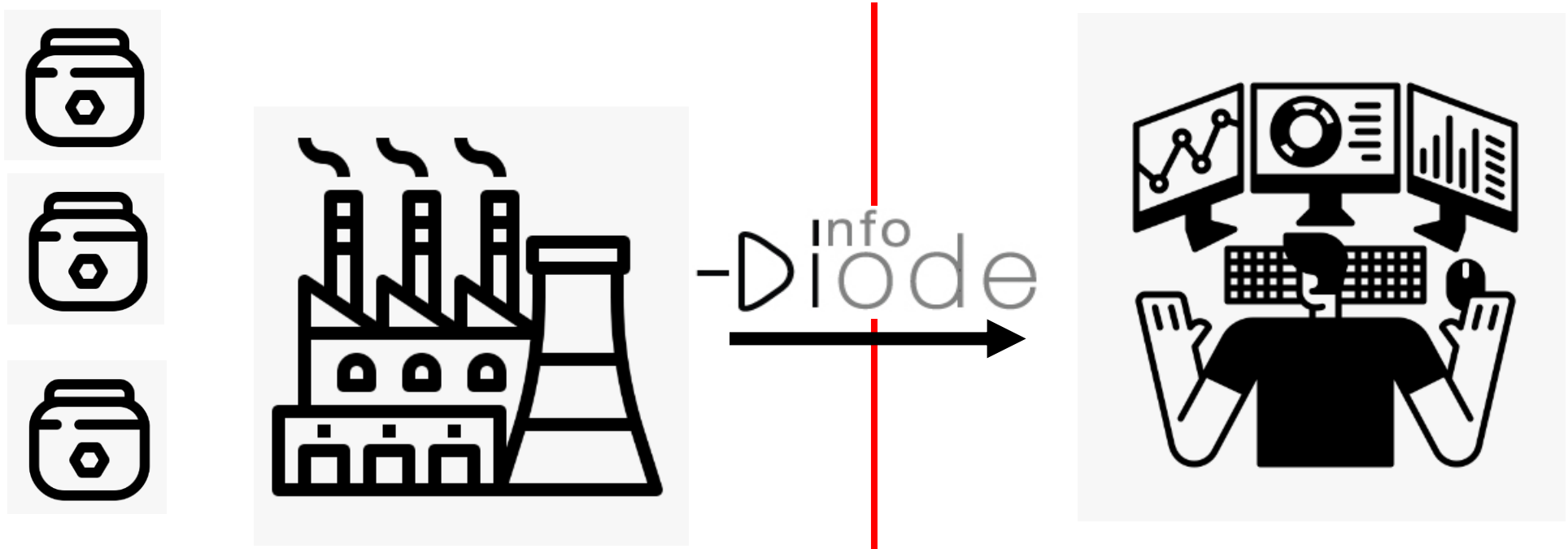
kafka

- InfoDiode поддерживает крупнейшие opensource интеграционные шины
- InfoDiode выступает брокером, на который шины публикуют сообщения
- InfoDiode сам подписывается на шины, ожидая получения сообщений для передачи вовне

- InfoDiode поддерживает крупнейшие opensource интеграционные шины
- InfoDiode выступает брокером, с которого читают
- InfoDiode сам публикует данные на интеграционные шины

AMT GROUP

Передача данных из систем класса Deception и систем IDS в целом

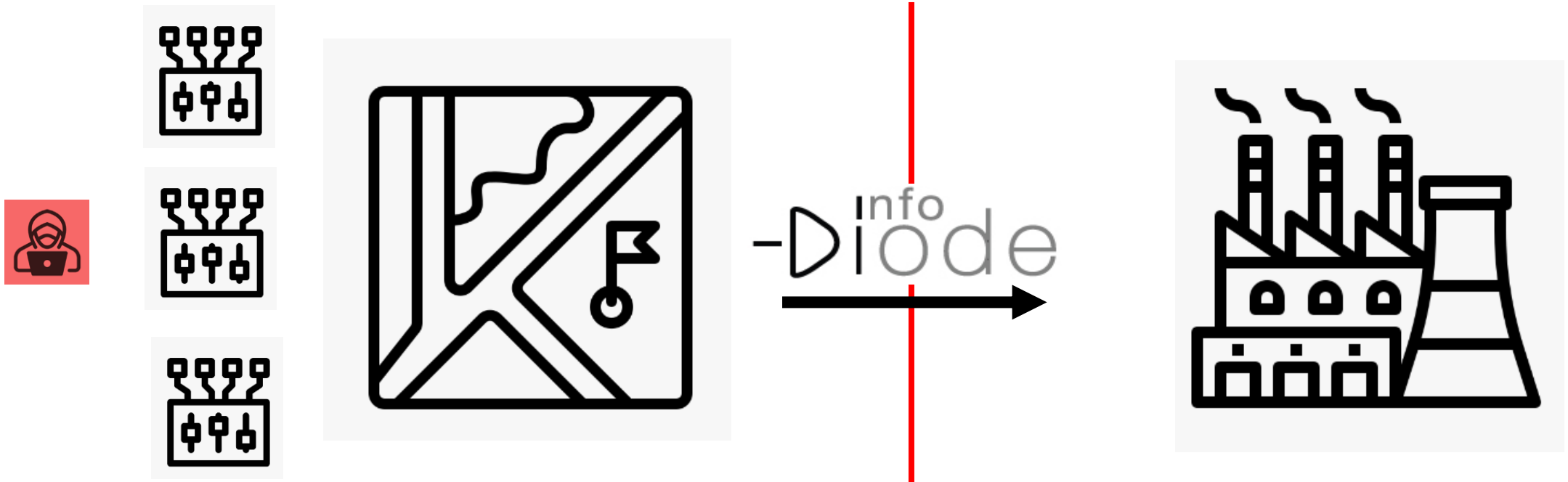


- Требуется контролировать объект на предмет событий ИБ в условиях его изоляции
- Требуется мониторинг сетевого трафика, аномалий
- Требуется обнаруживать несанкционированную активность, вызванную причинами внутри объекта

- Для сопряжения с SOC могут быть использованы разные решения InfoDiode (аппаратные или InfoDiode SMART)
- Срабатывания с «ловушек» наравне с данными SPAN (трафик закрытого сегмента) передаются в единый SOC

AMT GROUP

Защита АСУ ТП со стороны «полевого» уровня

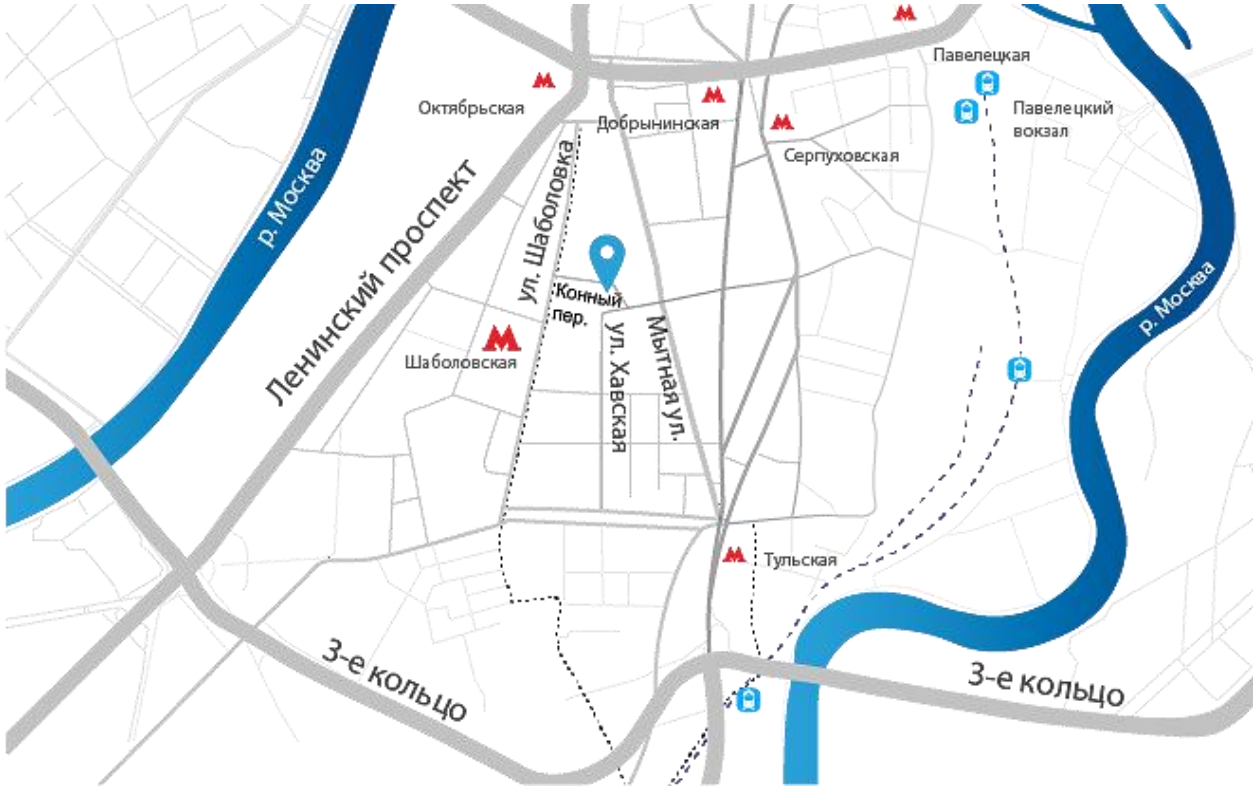


- Средства измерения и контроля установлены вне контролируемого периметра
- При передаче/сборе данных используются общедоступные сети
- SCADA и «полевой» сегмент в целом имеет слабые средства защиты

- Исключить возможность TCP/IP подключений к SCADA, сканирования топологии технологической сети
- Сохранить только однонаправленный поток, атаки с использованием которого хорошо локализуются средствами МСЭ

Как с нами связаться

- Адрес: 115162, Россия, Москва, ул. Шаболовка, д. 31, корп. Б, подъезд 3, этаж 2, вход с Конного переулка
- Телефон/Факс: +7 (495) 725-7660, +7 (495) 646-7560
- Факс: +7 (495) 725-7663
- E-mail: **InfoDiode@amt.ru**
- Сайт: **InfoDiode.ru**
- Техническая поддержка: **https://support.amt.ru**



СПАСИБО ЗА ВНИМАНИЕ!