Особенности обеспечения информационной безопасности в системах SCADA

Гарбук Сергей Владимирович
(начальник ИАЦ, ФГУП «НИИСУ», Минпромторг России)
Комаров Андрей Андреевич
(технический директор, ITDefence)

Области использования и назначение систем SCADA / DCS и их элементов

Сфера применения

- Электроэнергетические системы

- Системы транспортировки углеводородов

- Транспорт (ж/д, УВД, автомобильный)

- Системы жизнеобеспечения (канализация, отопление, водоснабжение, очистные сооружения и др.)

Supervisory Control And Data Acquisition,
(Диспетчеризация и сбор данных)

Distributed Control Systems
(Распределённые системы управления)

Human Machine Interface
(Человеко-машинный интерфейс)

Remote Terminal Unit
(Удаленный оконечный блок)

Programmable Logic Controller
(Программируемый логический контроллер)

Решаемые задачи

- Управление объектом инфраструктуры в реальном времени
- Получение телеметрической и измерительной информации
- Аварийное сигнализирование и контроль выполнения технологических процессов
- Непосредственное управление технологическими процессами

Разновидности систем SCADA / DCS и их функциональные особенности

Распределенные системы

- Используют разнородные среды передачи данных (проводные, беспроводные)
- Элементы систем децентрализованы и географически рассредоточены
- Используют несколько «Master» станций, множество «Slave»
- Используются портативные и мобильные средства управления и диагностики
- Защищённость требуется не только на внутренних, но и трансграничных участках
- Децентрализованное интегрирование SCADA с системами корпоративного уровня (ERP/SAP/GIS) и зонами ведения непосредственного бизнеса (Business Area Network)
- Применение беспроводных решений на участках ЛЭП, протяжённых магистралях теплопередачи, транспортировки углеводородов
- Обилие технических мер обеспечения ИБ

Локальные сетевые решения

- Вся сетевая и прикладная инфраструктура сосредоточена в одном месте
- BAN (Business Area Network) территориально совмещена со SCADA
- Управление и диагностика значительны упрощены
- Передача данных по открытым общедоступным каналам связи не производится
- Организационные меры обеспечения ИБ преобладают над техническими
- Относительно высокая осведомлённости сотрудников в области ЗИ/ИБ

Сравнительный анализ

Категория	ИС общего назначения	SCADA / DCS / АСУ ТП
Аутсорсинг	Используется	Практически никогда
Время технологической поддержки	3-5 лет	до 20 лет
Разработка и применения обновлений безопасности	Систематически, сравнительная простота взаимодействия с вендорами	Редко, длительность и своевременность установки в зависимости от реакции вендора ПО АСУ ТП
Внесение изменений	Достаточно часто	Очень редко, при явной необходимости
Доступность	Возможен временный сбой	Необходимо постоянное функционирования (24x7x365)
Физическая безопасность	Достигается регламентным путём, все физические меры безопасности локализованы и централизованы	На удалённых и территориально протяжённых участках АСУ не подконтрольна (unmanned), либо обеспечена слабо

Состав и масштабы

Что входит в SCADA?

- Серверное ПО и Head-End Software АСУ ТП
- ПО «Master» и «Slave» станций
- Компоненты распределённой системы управления (DCS)
- Полевые устройства сбора информации (телеметрия, датчики, сенсорная аппаратура)
- Полевые устройства передачи информации
- Полевые устройства технологического контроля, учёта, измерений (AMI)
- Устройства HAND (Home Area Network Device)

Инциденты

Факты и события

- В сетевой инфраструктуре ядерной станции штата Огайо обнаружен червь «Slammer»

- Взлом California Independent System Operator (CaISO) со стороны китайских хакеров нарушило функционирование высоковольтных линий электропередачи

- Сбой в компьютерной системе стал причиной того, что американская авиакомпания US Airways ненадолго вышла в явные лидеры по части продажи самых дешевых авиабилетов на внутренние рейсы в США. Путешествие в оба конца между двумя американскими городами в результате этой накладки обошлось нескольким путешественникам всего в 1 доллар 86 центов, а с учетом всех полагающихся налогов и аэропортовых сборов - примерно в 40 долларов.

Учёт инцидентов

- Некоммерческие организации (Repository of Industrial Security Incidents, RISI)
- Технические сообщества специалистов
-Координирующие органы (CERT, CIRT)
- Государственный сектор

Модель злоумышленника

Основные категории

-Службы безопасности конкурирующих организаций (экономические мотивы, стремление к достижению и закреплению конкурентных преимуществ)

- Внутренние злоумышленники (Insider) – уволенные, нелояльные, халатные работники (уволенный сотрудник корпорации Chevron отключил систему аварийного оповещения, обслуживающую 22 штата США, что не было выявлено до появления первой технологической аварии)

-Экстремистские группировки и террористические группы (2003 год, после подавления нескольких тренировочных баз Аль-Каиды были конфискованы материалы об устройстве SCADA-систем)

- Специальные службы иностранных государств

- «Хакеры», не имеющие рациональных мотивов

Мотивы осуществления злонамеренных воздействий

- Экономические
- Военно-политические
- Социально-психологические (самоутверждение, интерес, любопытство, месть)

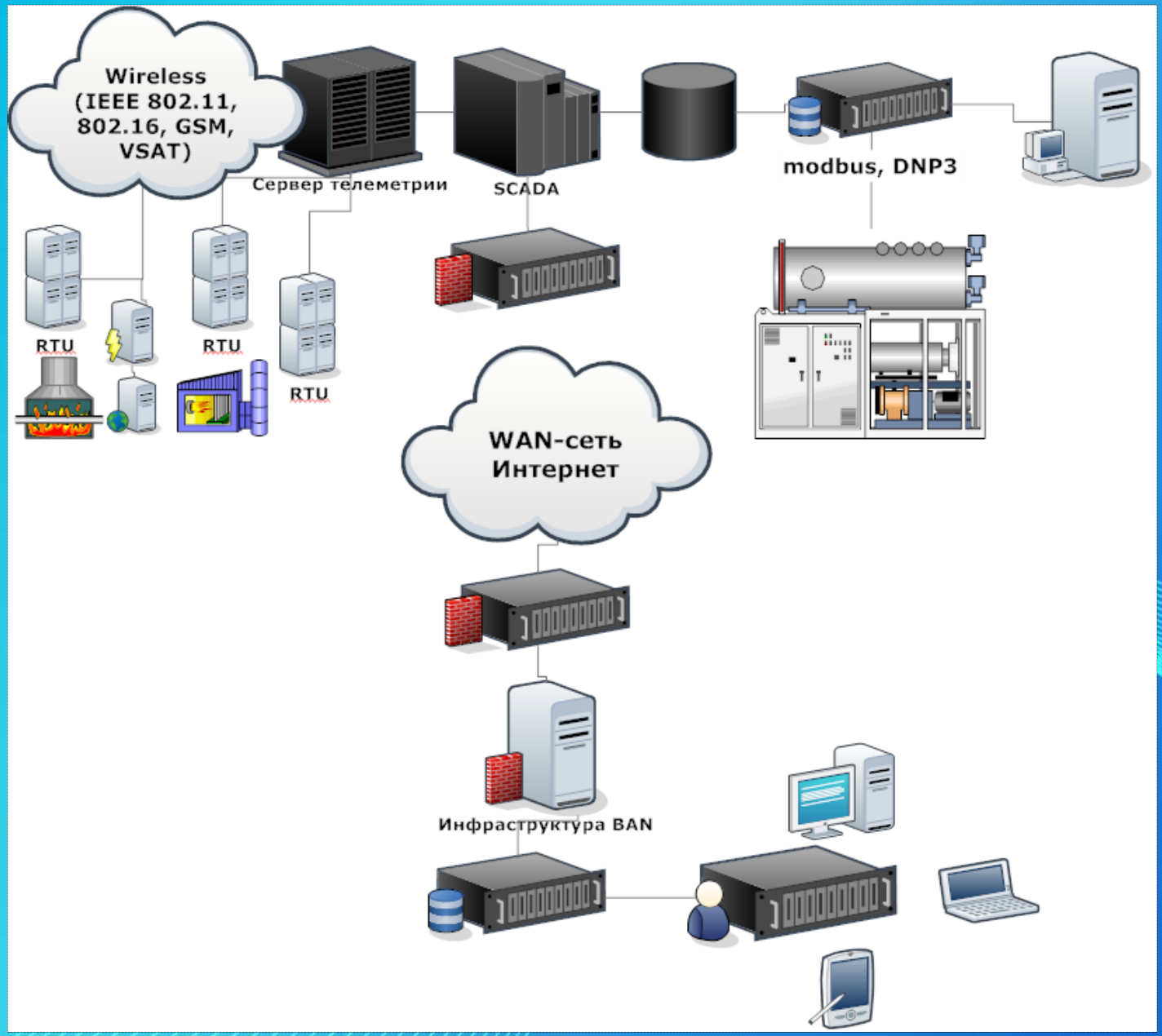
Доступность для злоумышленника

Информационные факты

- Возможные сценарии воздействия публично регламентированы (SP 800-82DRAFT Guide to Industrial Control Systems (ICS) Security)
- Географическая привязка, указывающая на диапазоны соответствующих подсетей
- Ресурсы и «знания», полученные путём разведки из открытых источников (OSINT)
- Изучение лент публикации уязвимостей

Технический инструментарий и дополнительные средства

- Случайность при проведении массовых заражений позволяет воздействовать на SCADA/DCS и её элементы в такой же мере, как и на целевого клиента
- Наличие публичных средств активной и пассивной разведки позволяют частично выявить инфраструктуру SCADA
- Некоторые из PoC, эксплуатирующие ПО SCADA-систем, включены в свободно распространяющиеся продукты на базе открытого исходного кода (Metasploit Project, Nessus)
- Возможность использования существующих средств эксплуатации в отношении ПО, не являющегося самой SCADA (WEB-серверы, операционные системы, сторонние службы и сервисы)
- Информационное воздействие на «client-side» осуществимо в зоне функционирования BAN, а так же сопряжённых корпоративных сегментов, которые имеют непосредственную «обратную связь» с ходом технологического процесса


Wireless
(IEEE 802.11,
802.16, GSM,
VSAT)
Сервер телеметрии
SCADA
modbus, DNP3
RTU
RTU
RTU
WAN-сеть
Интернет
Инфраструктура BAN

Методики сетевой разведки

Актуальные

- Изучение и анализ ответов WEB-серверов, обслуживающих SCADA (HTTP-printing)
- Выявление устройств телеметрии (их доступность «из вне» порой необходима)
- Апробация средств выявления характеристик систем реального времени (RTOS)
- Перечисление конечных клиентов беспроводных сетей с последующим анализом MAC-адресов сетевых карт по базе OUI или сторонним источникам
- Изучение специфических сетей, характерных GPRS-пулам операторов
- Сетевые атаки на сторонние обслуживающие сервисы (DNS, NTP Time Server, FTP)

Способы предотвращения

- Техническое скрытие устройств телеметрии путём модификации штатной процедуры авторизации и аутентификация
- Изменение MAC-адресов средствами изменения «прошивок» устройств телеметрии
- Использование доверенных и защищённых обслуживающих сетевых сервисов
- Применение техник, противодействующих OS-fingerprinting при активном и пассивном анализе целевой операционной системы

Применение HTPP-printing

Сигнатуры ответов

HTTP/1.0 401 Authorization Required
Date: Sun, 29 Nov 2009 21:18:47 GMT
Content-length: 401
Content-type: text/html; charset=iso-8859-1
Www-authenticate: Digest realm="RTS SCADA Server",
nonce="q9EMEol5BAA=92208aedcfb6c52d91fdc964fd19ade94d64a87a",
algorithm=MD5, domain="/ http://twinbutte.fieldlinq.com/", qop="auth"
Server: Apache/2.0.63 (FreeBSD) mod_python/3.3.1 Python/2.5.2

HTTP/1.0 302 Object moved
Content-length: 224
X-powered-by: ASP.NET
Set-cookie: ASPSESSIONIDCCARDRTS=KMPBMIOCJCBGGPHIPJDPFMJN; path=/
Server: Microsoft-IIS/5.0
Location: ./broadWeb/system/bwviewpg.asp?proj=SDCC-SCADA&node=SCADA-EXTRANET&capt=0&stat=0&Tool=0
Cache-control: private
Date: Fri, 27 Nov 2009 04:25:06 GMT
Content-type: text/html
X-ua-compatible: IE=EmulateIE7

Уязвимые элементы SCADA электроэнергетической системы

Объект воздействия	Угроза	Метод
Система распределения электрической энергии (EMS – Energy Management System)	Критические уязвимости обнаружены в	Эксплуатация переполнения буфера в стеке и многочисленных программных дефектов (CVE-2009-0210 CVE-2009-0211)
Сервер накопления информации (Historian)	Ошибки в модуле аутентификации OsiSoft PI Server	Воздействие векторов сетевых атак, направленных на эксплуатацию небезопасных методов авторизации (CVE-2009-209)
Инфраструктура телеметрии (RTU)	Возможность осуществления НСД к модулю телеметрии (Schneider Electric) через беспроводной bluetooth-канал	Атаки на WPAN-сети
Программируемый логический контроллер (PLC)	Беспроводной доступ к PLC (Omron PLCs), используя Apple iPhone ScadaMobile	Обход авторизации
OLE for Process Control (OPC)	MatrikonOPC – небезопасное использование OLE COM-объекта	Эксплуатация программного дефекта (JS+HTML)

Специфические атаки

Методы и описание воздействий

- ICCP-фаззинг служб и сервисов, взаимодействующих с серверами Historian, информационных хранилищ, приложениями для мониторинга данных

- Эксплуатация уязвимостей в OPC

- Исследование DDE-общедоступных ресурсов

Using OPC via DCOM with Microsoft Windows XP Service Pack 2

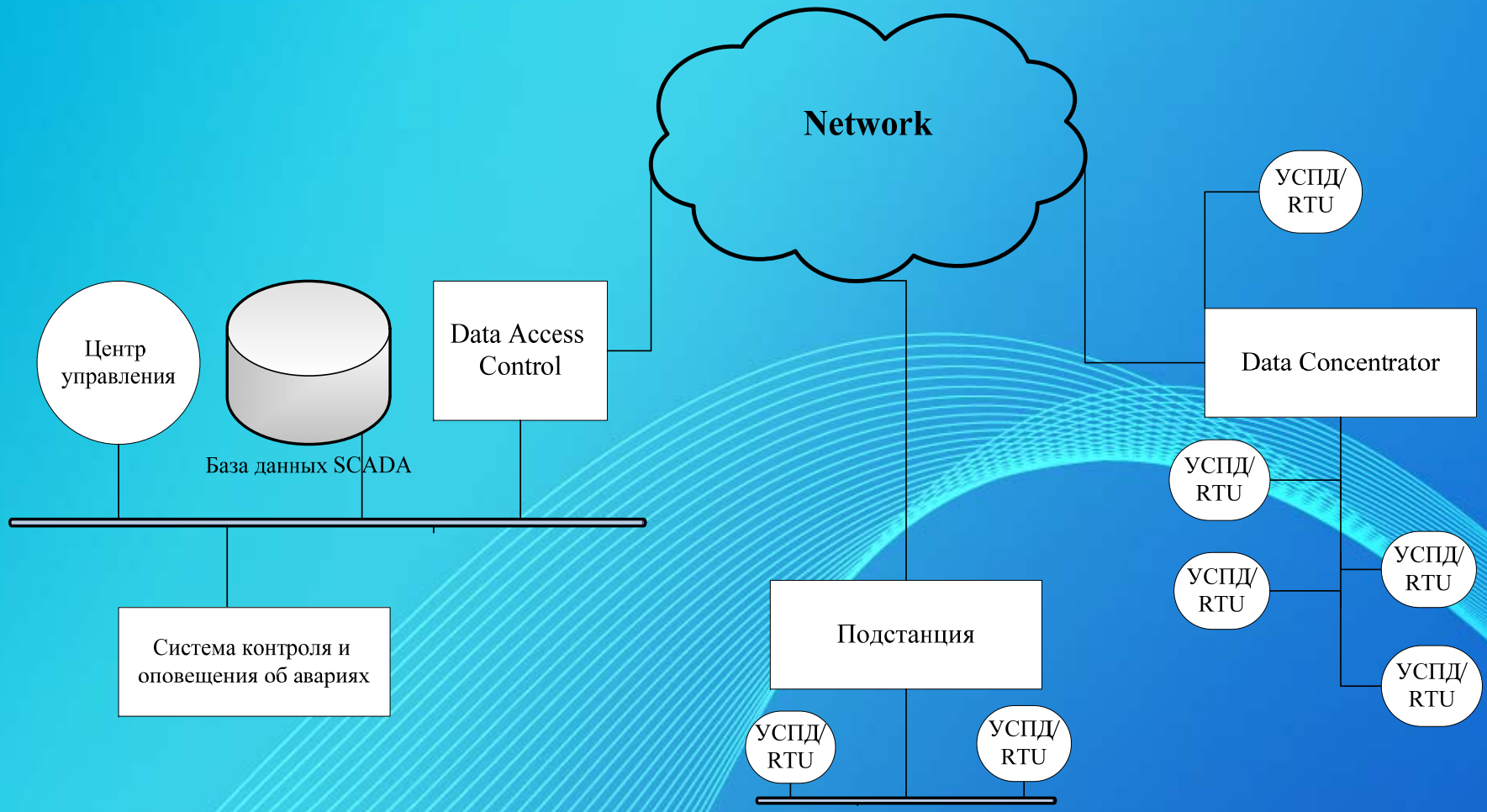
OPC FOUNDATION

6. Edit the Limits for Access and Launch
   a. Access Permissions – **Edit Limits...**
      You need to check the Remote Access box for the user labeled ANONYMOUS LOGIN in this dialog.

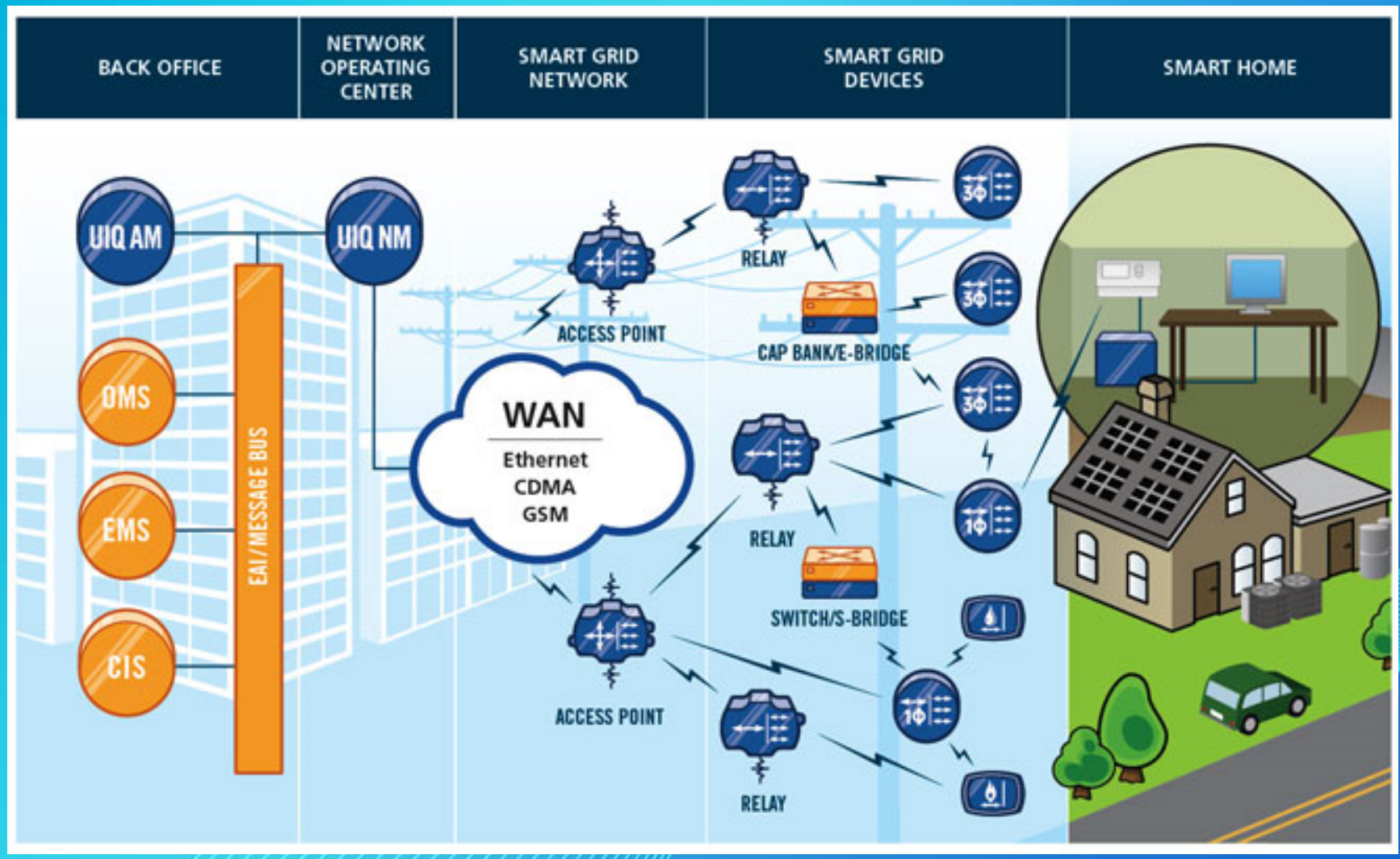
Объекты критически важных инфраструктур США, управляемые SCADA

Сельское хозяйство и продовольствие	1 912 000 ферм; 87 000 фабрик по производству продовольственных продуктов
Водные ресурсы	1 800 федеральных резервуаров; 1 600 муниципальных водостоков
Обслуживание в условиях чрезвычайных ситуаций	87 000 населенных пунктов
Энергетика	
Электроэнергия	2800 электростанций
Нефть и природный газ	300 000 производственных пунктов
Транспорт	
Авиация	5000 аэропортов
Пассажирские железные дороги	120 000 миль железных дорог
Автодороги и автомобильный транспорт	590 000 дорожных мостов
Нефтепроводы	2 миллиона миль нефтепроводов
Морской транспорт	300 портов
Массовые перевозки граждан	500 главных городских операторов перевозок
Химические и опасные материалы	66 000 химических производств
Ключевые активы	
Атомные электростанции	104 коммерческих ядерных электростанций
Дамбы	80 000 дамб
Средства обслуживания правительства	3000 средств принадлежащих/используемых правительством
Коммерческие ключевые активы	460 небоскребов

Типовая АСУ ТП электроэнергетической системы



SCADA в сети управления электроэнергетической системой SmartGRID



Основные производители SCADA для систем электроэнергетики

Компания	Сайт
Schneider electric	www.schneider-electric.com
	www.schneider-electric.ru
ABB Group	www.abb.com
	www.abb.ru
GE (GE Energy)	www.ge.com
	www.gepower.com
Siemens	www.siemens.ru
	http://w3.siemens.ru/solutions_and_services/energy/
KEMA	www.kema.com
Toshiba	http://www.toshiba.co.jp/f-ene/tands/english/protect/f_sas.htm
	www.toshiba.ru
	www.toshiba.com
COOPER Power Systems	www.cooperpowereas.com
BPL Global	www.bplglobal.net
CD Nova Ltd.	www.cdnova.com
HARRIS Corporation	http://www.harris.com

Специфические особенности организации защиты

Особенности

- **Контроллеры, устройства телеметрии (RTU) имеют достаточно слабые вычислительные мощности, исторически взаимодействуют с управляющими элементами через промышленные последовательные протоколы с практически полным отсутствием от традиционных сетевых атак («сниффинг», перенаправление трафика на участке сети) и ПМВ**

- **Внедрение средств СКЗИ**

- **Реконфигурация доступа в отношении открытых общедоступных каналов связи**

- **Выстраивание эшелонированной модели защиты (Defence in depth)**

- **Инвентаризация стороннего обслуживающего ПО**

Спасибо за внимание!

http://itdefence.ru