IARIA

International Academy, Research, and Industry Association

Internet of Things Architecture and Security

Shuangbao (Paul) Wang, Ph.D.

May 25, 2017, Barcelona, Spain

Metonymy Labs

“Speak only if you have accomplished. “

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

Payment will be raised on

5/15/2017 16:04:06

Time Left

02:23:57:49

Your files will be lost on

5/19/2017 16:04:06

Time Left

06:23:57:49

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

Copy

About bitcoin

How to buy bitcoins?

Contact Us

Check Payment

Decrypt

WannaCry

- Friday, May 12, 2017?
- 100+ countries, 130,000 systems
- Last for 48 hours
- $300 - $400 - $500 - $600 /endpoint, est. 39 million
- WanaCrypt (Shadow Brokers)
- Strong, Asymmetric Encryption (RSA 2048 bit)

- 6,000% increase from 2015-2016 (IBM X-Force)
- $ 1 Billion “income” by end of 2016 (FBI)

DoublePulsar and EternalBlue

- Worming through SMB (TCP port 445, Server Message Block)
- Exploit Backdoor DoublePulsar, EternalBlue
- Knocking the backdoor and injecting DLLs (NSA tool leaked by Shadow Brokers in April 2017)
- 36,000 infected endpoints found in two weeks.

- EnternalBlue scan server for presence of DoublePulsar
- Compromise the system if none if found

DoublePulsar and EternalBlue (cont.)

- Launch a TOR client, apply CTB-Locker etc.
- Call **tasksche.exe** to encrypt files
- Delete shadow copies using **VMIC.exe**, **cssadmin.exe** and **cmd.exe**
- Display ransom note using **SetForegroundWindow()**

- **www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com**

Guard Against WannaCrypt Ransomware

Guard against WannaCrypt ransomware

A wide-spread ransomware attack, known as "WannaCrypt," targets out-of-date Windows devices. Given the severity of this threat, Microsoft recommends that you immediately update your Windows devices.

1. Make sure you have automatic updates turned on, and your system is up to date. On Windows 10, Go to **Settings** > **Update & security**. You'll see your update status there.
2. For Windows 8.1, go to **Settings** > **Change PC Settings** > **Update and recovery.**
3. In Windows 7, go to **Control Panel** > **Windows Update.**
4. For more information about older versions of Windows, see Customer guidance for WannaCrypt and Microsoft Security Bulletin MS17-010.

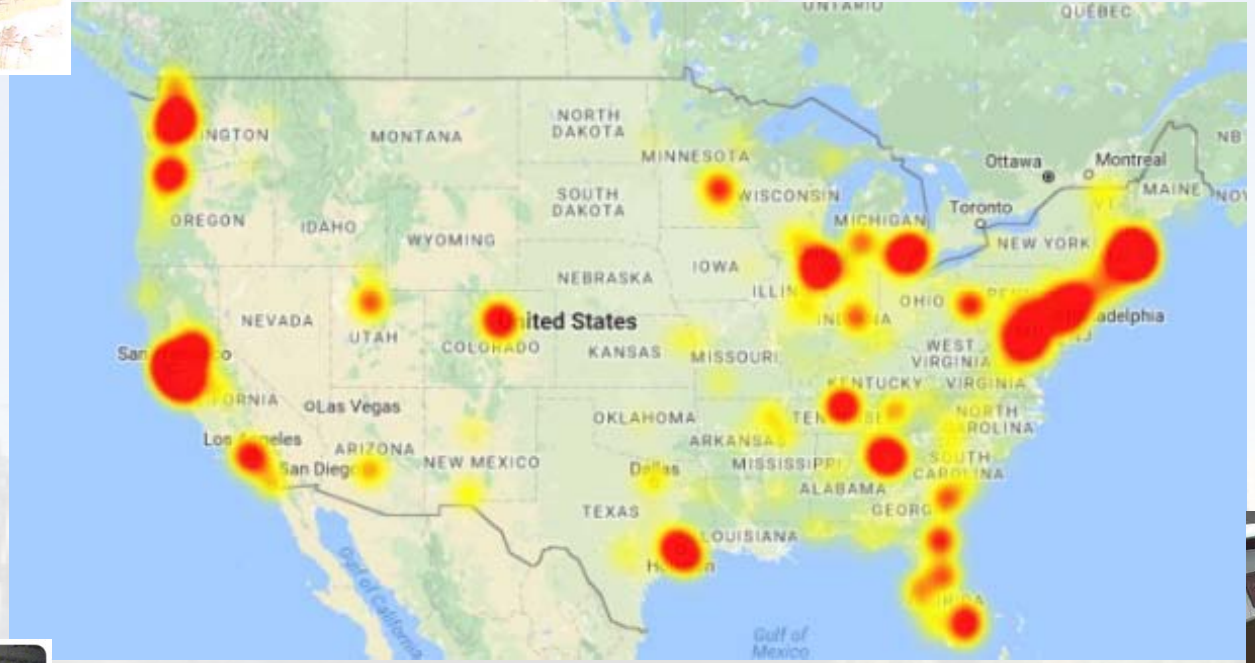
Help from Microsoft

Was this helpful?

Applying update operation 13726 of 34379 (\Registry\machine\

© Microsoft Corporation

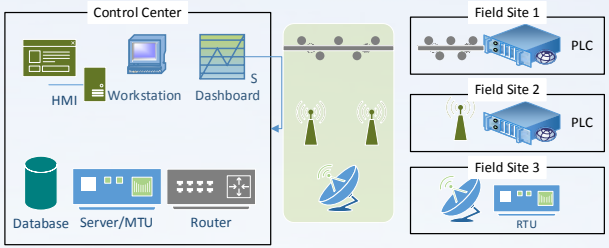
Paul Wang
5/10/2017 3:05 PM
10.3.1

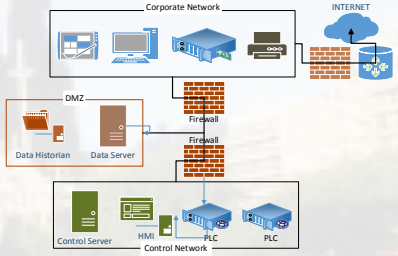

QUÉBEC
MONTANA
NORTH DAKOTA
MINNESOTA
SOUTH DAKOTA
WISCONSIN
MICHIGAN
Ottawa
Montreal
Toronto
MAINE
NEW YORK
OREGON
IDAHO
WYOMING
NEBRASKA
IOWA
OHIO
NEVADA
UTAH
COLORADO
KANSAS
MISSOURI
WEST VIRGINIA
VIRGINIA
Las Vegas
OKLAHOMA
ARKANSAS
ARIZONA
NEW MEXICO
San Diego
MISSISSIPPI
ALABAMA
TEXAS
LOUISIANA
Gulf of Mexico


Oct/26/2016 09:52:21

Contents

- SCADA Architecture
- Security Issues
- A Case Study





Internet of Things Reference Model

Architecture

Collaboration & Processes

People and Business Process

Application

Report, Analytics, Control

Data Abstraction

Aggregation and Access

Data Accumulation

Storage

Edge Computing

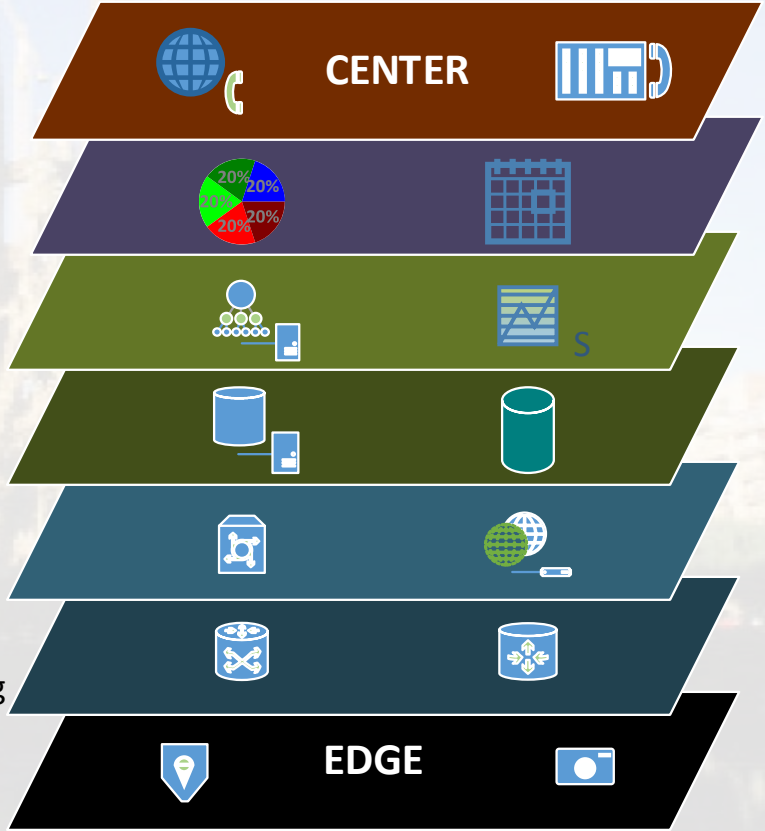
Data Element Analysis

Connectivity

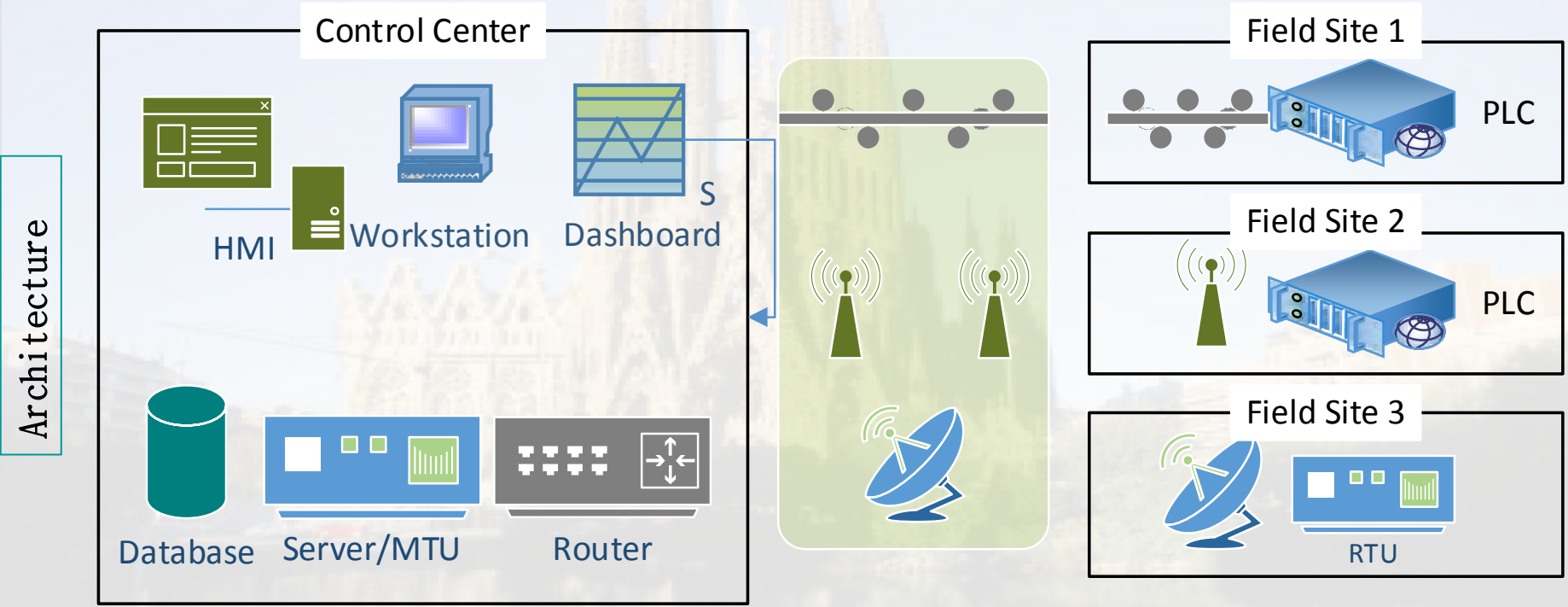
Communication & Processing

Devices and Controllers

The "Things" in IoT

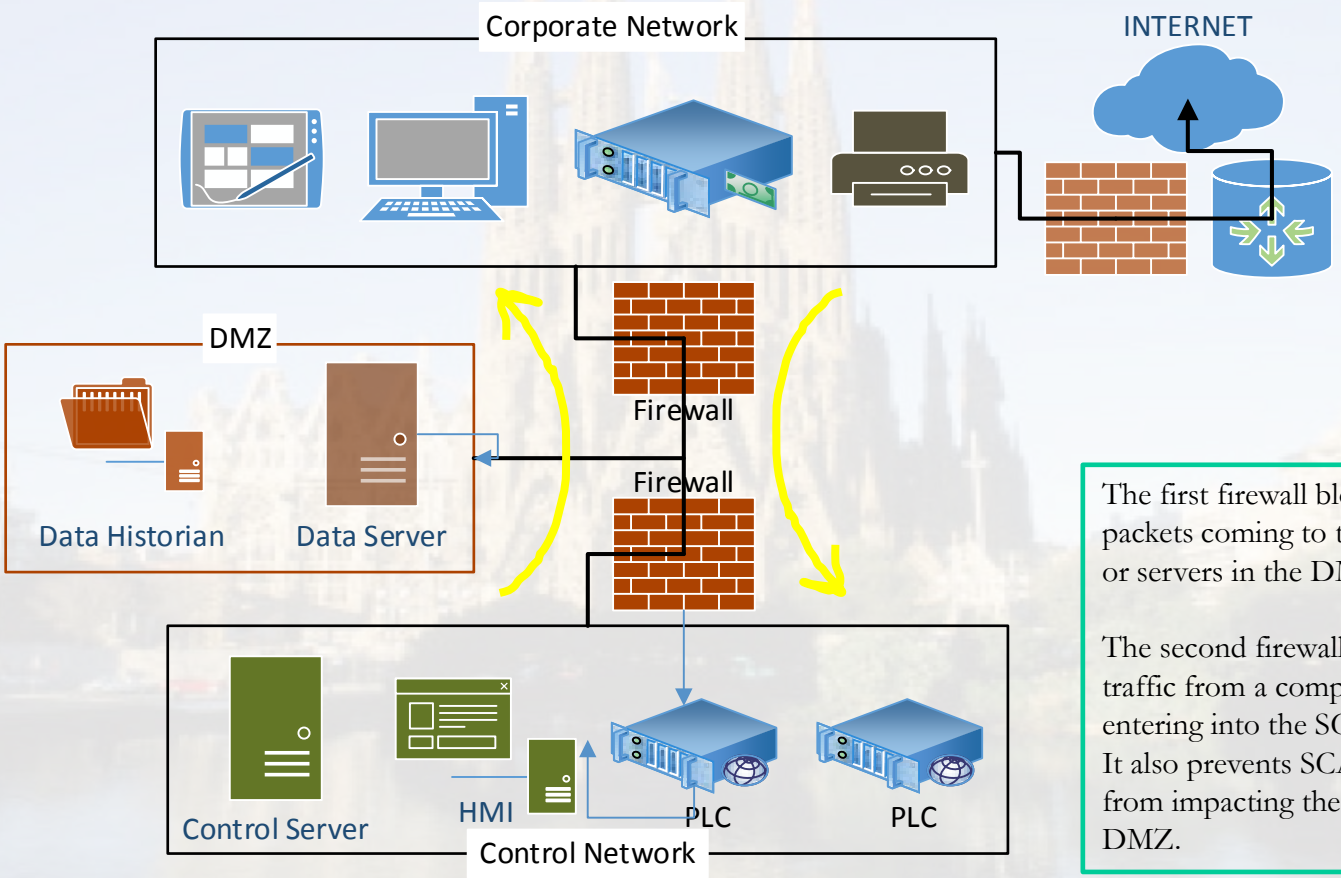


SCADA System Architecture



Paired Firewall Architecture

Architecture

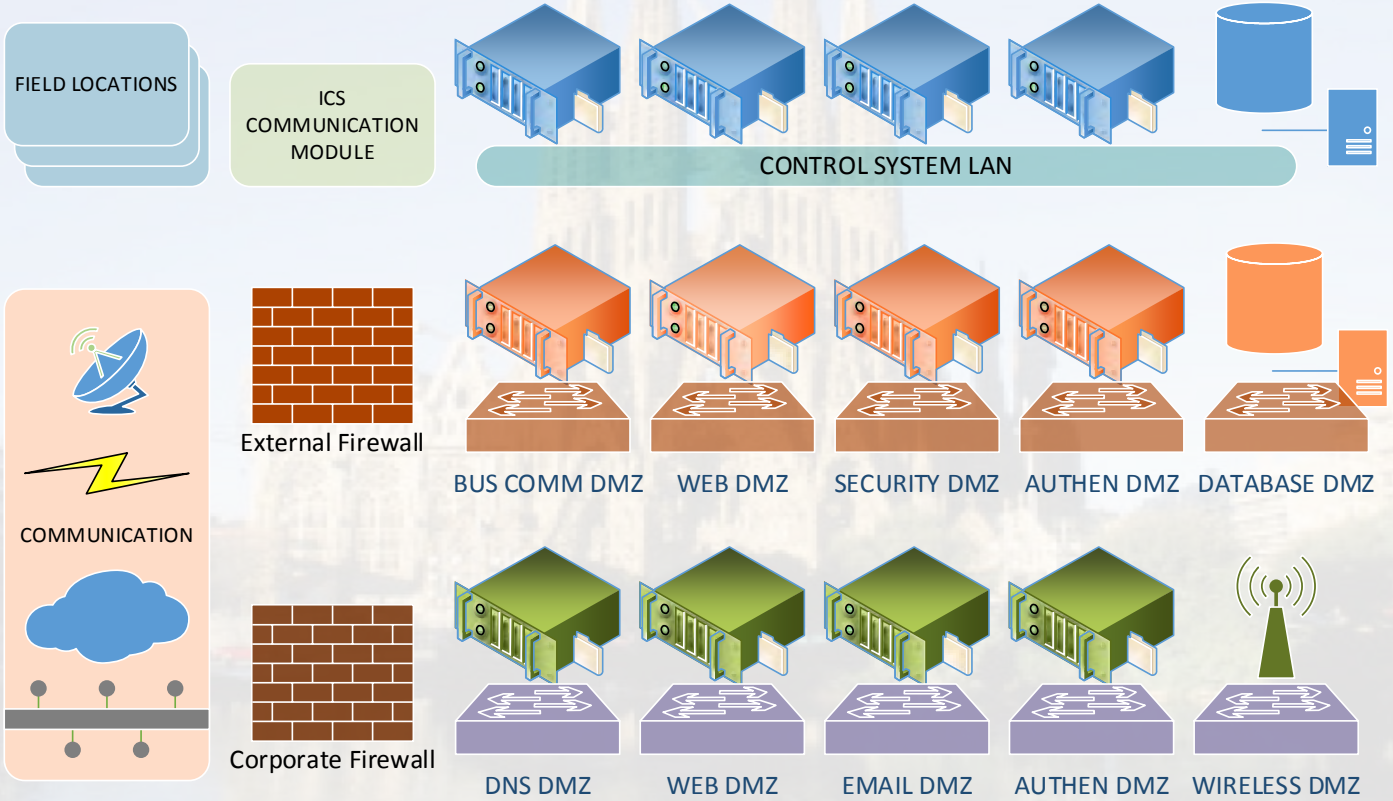


The first firewall blocks the arbitrary packets coming to the SCADA network or servers in the DMZ.

The second firewall prevents unwanted traffic from a compromised device from entering into the SCADA network.
It also prevents SCADA network traffic from impacting the shared servers in the DMZ.

Defense-in-Depth Architecture

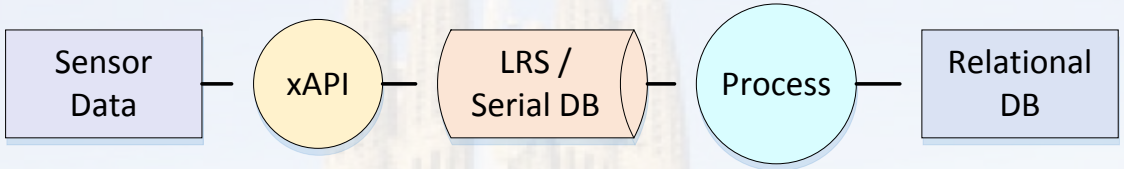
Architecture

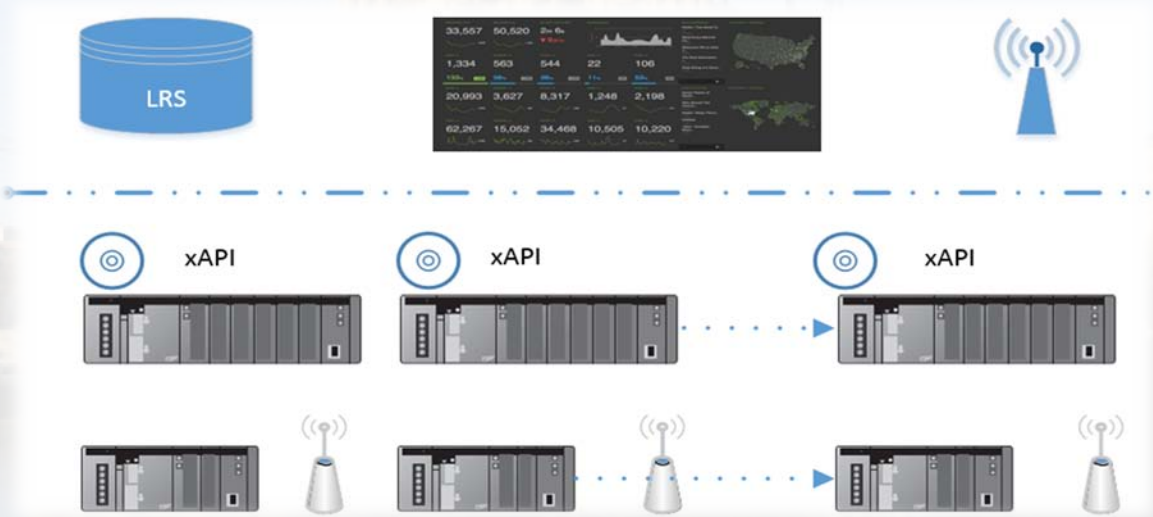


- Multiple layer architecture
- Two or more security mechanisms
- Impact of a failure in one measure cannot cause failure of the whole system
- Minimizes the business services to be interrupted.

Dual-Data Abstraction Model

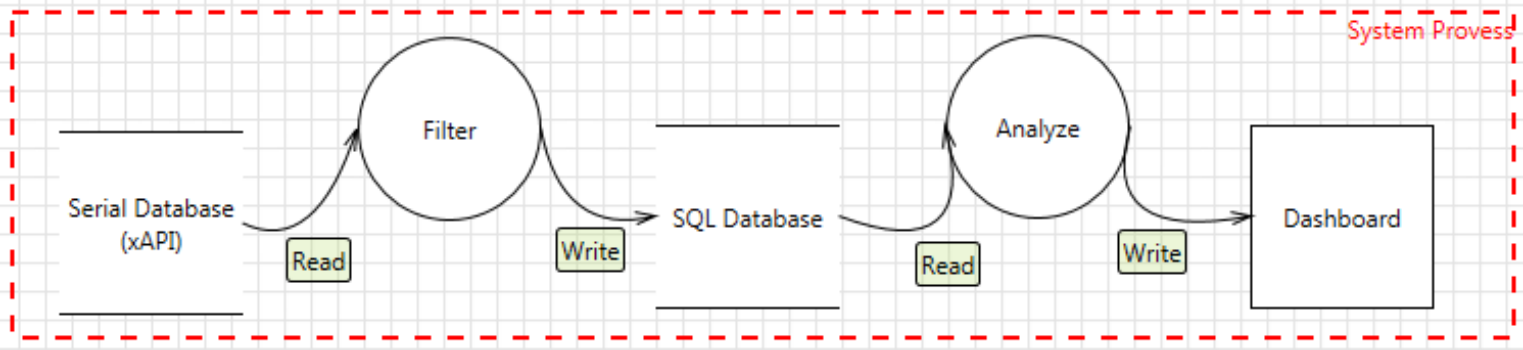
Architecture





DDM System Process

Architecture



- Read data from serial DB
- Filter data
- Send data to a relational DB
- Data can then be further analyzed and displayed on a dashboard

Question: Why use two databases to gather data?

Architecture

A robust **architecture** can reduce the possibility of SCADA systems from being compromised.

A good **data model** makes it easy for collecting sensor data securely

50 billion IoT devices
In 2020

Security and Privacy

Security

- Executive Order 13010 – critical infrastructure protection
- NIPP – secure critical infrastructure
- Vulnerabilities in IoT systems: S7-1200 (v2 and v3)
  - S7-1200 has a web server built in
  - Port 80/443 could allow cross-site scripting attacks
  - Local users click the malicious links.
  - NVD/CVSS score 4.3/10

Cookies
Sessions
APIs

- Vulnerable to DoS attacks via the web server, weak authentication.

DoD xAPI

Security

- Vulnerability in xAPI configuration file:

```
//globals: equal, responseText, statement, ok, deepEqual, QUnit, module, asyncTest, Util,
start, golfStatements, console
/*jslint bitwise: true, browser: true, plusplus: true, maxerr: 50, indent: 4 */
function Config() {
    "use strict";
}

//5/19/2015
Config.endpoint = "https://lrs.adlnet.gov/xapi/";
Config.user = "William Kelly";
Config.password = "wKelly$377!";
Config.actor = { "mbox":"william.kelly@gmail.com", "name":"William"

};
```

- Strong authentication (such as oAuth2) is necessary.

Networked Cameras

Security

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http.request.method == "POST" Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Lengtl	Info
52	2.111391000	10.0.0.4	[redacted]	HTTP		[redacted]

Mark Packet (toggle)
Ignore Packet
Set Time Refe
Time Shift...
Packet Comme
Manually Resc
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream

Frame 52: 621 bytes on wire (4968 bits), 621 bytes capt
Ethernet II, Src: [redacted]
Internet Protocol Version 4, Src: 10.0.0.4 (10.0.0.4),

File Edit View Go Capture Analyze Stat

Filter: http.request.method == "POST"

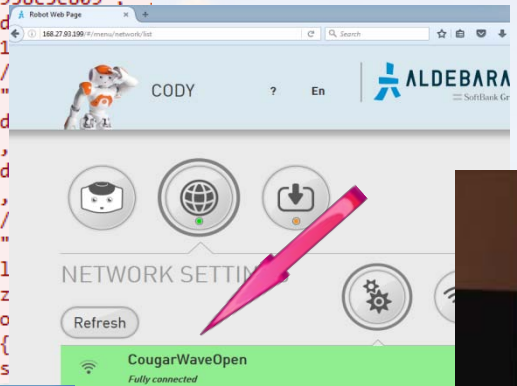
No.	Time	Source	Destination
52	2.111391000	10.0.0.4	

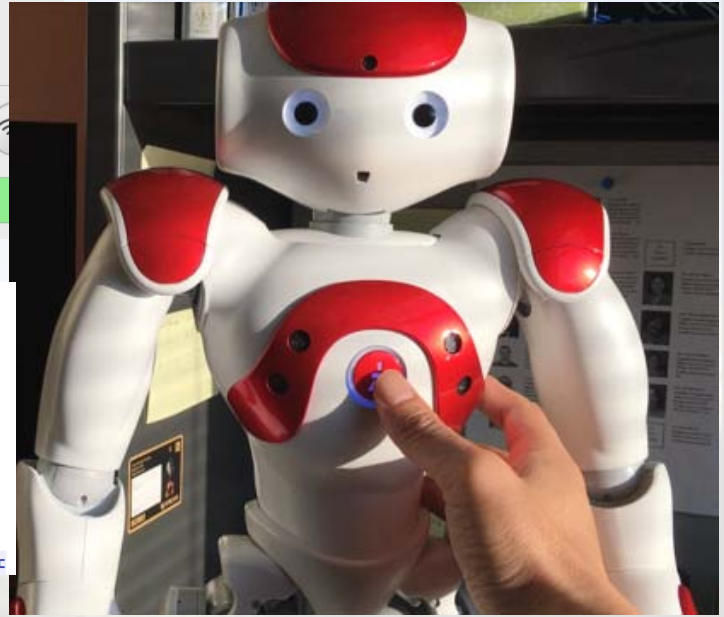
```
Set-Cookie: password=e4b7c855be6e3d4307b8d6ba4cd4ab91; expires=Thu, 07-N
Set-Cookie: scifu r=sampleuser; expires Thu, 07-Nov-2024 23:52:21 GMT;
Location: logged n.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
NOTE: press enter for status-scree
e4b7c855be6e3d4307b8d6ba4cd4ab91:simplepassword

All hashes have been recovered

Input.Mode: Dict (/root/rockyou.txt)
Index.....: 1/5 (segment), 3627099 (words), 33550339 (bytes
Recovered.: 1/1 hashes, 1/1 salts
Speed/sec.: - plains, 39.29M words
Progress..: 2395328/3627099 (66.04%)
Running...: --:--:--:--
Estimated.: --:--:--:--
```

“Hello, I’m Cody. My Internet address is 168.27.93.199.”


```
lexicon", "version": "1.0.28", "md5": "89538d3e95476796a512456958c5e809", "
_meta", "url": "https://cloud.aldebaran-robotics.com/ade/api/1/d
meta", "version": "1.0.6", "md5": "656c0741ce0b0cb64f3b86153871
"url": "https://cloud.aldebaran-robotics.com/ade/api/1/download/
"version": "1.0.2", "md5": "9e55492140529772ee8f0e1822ceeed7", "
"url": "https://cloud.aldebaran-robotics.com/ade/api/1/download
"version": "1.0.13", "md5": "23520206f8b617e3018c75b2b90eea13",
"url": "https://cloud.aldebaran-robotics.com/ade/api/1/download
"version": "1.0.21", "md5": "e6f6ba79af57d9707782260276c2ec76",
"url": "https://cloud.aldebaran-robotics.com/ade/api/1/download/
"version": "0.1.7", "md5": "4392b21bc8847ae3b2bf81beb4f272e9", "
": "https://cloud.aldebaran-robotics.com/ade/api/1/download/appl
sion": "0.0.16", "md5": "db089d9c77a073db607d0293f0e12fb4", "siz
/cloud.aldebaran-robotics.com/ade/api/1/download/appli/304634/fo
.29", "md5": "d32390ce078c98d578a50395ce4f80f2", "size": 317}, {
aldebaran-robotics.com/ade/api/1/download/appli/304237/go-to-res
```



Wireshark · Follow TCP Stream (tcp.stream eq 4) · wireshark_B04AB7B7-5D26-4D95-B5F9-AF43DE87931C_20161027205532_a03188

```
..GET /libs/qimessaging/1.0/qimessaging.js?v=1.1.4 HTTP/1.1
Host: 168.27.93.199
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW6
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://168.27.93.199/
Connection: keep-alive
Authorization: Basic bmFvOk5hbzIwMDE=

HTTP/1.1 200 OK
Server: nginx/1.3.14
Date: Fri, 28 Oct 2016 00:55:49 GMT
Content-Type: application/x-javascript
Content-Length: 51959
Last-Modified: Thu, 27 Aug 2015 20:11:23 GMT
Connection: keep-alive
ETag: "55df6eeb-caf7"
Accept-Ranges: bytes

/*
**  Copyright (C) Aldebaran Robotics
**  See COPYING for the license
**
**  Author(s):
**   - Laurent LEC    <llec@aldebaran-robotics.com>
**
*/

/*! Socket.IO.min.js build:0.9.11, production. Copyright(c) 2011 LearnBoost <dev@learnboost.com> MIT L
var io="undefined"==typeof module?{}:module.exports;(function(){(function(a,b){var
c=a;c.version="0.9.11",c.protocol=1,c.transports=[],c.j=[],c.sockets={},c.connect=function(a,d){var
e=c.util.parseUri(a),f,g;b&&b.location&&(e.protocol=e.protocol||b.location.protocol.slice(0,-1),e.host=
b.document.domain:b.location.hostname),e.port=e.port||b.location.port),f=c.util.uniqueUri(e);var
h={host:e.host,secure:"https"==e.protocol,port:e.port||("https"==e.protocol?
443:80),query:e.query||""};c.util.merge(h,d);if(h["force new connection"]||!c.sockets[f])g=new c.Socket
```

```
0000149A  43 b6                                          C.
0000A55B  81 52 35 3a 3a 3a 7b 22  61 72 67 73 22 3a 20 7b   .R5:::{" args": {
0000A56B  22 69 64 6d 22 3a 20 38  38 2c 20 22 72 65 73 75   "idm": 8 8, "resu
0000A57B  6c 74 22 3a 20 22 77 73  75 6d 6d 65 72 73 40 63   lt": "ws ummers@c
0000A58B  6f 6c 75 6d 62 75 73 73  74 61 74 65 2e 65 64 75   olumbuss tate.edu
0000A59B  22 7d 2c 20 22 6e 61 6d  65 22 3a 20 22 72 65 70   "}, "nam e": "rep
0000A5AB  6c 79 22 7d                                        ly"}
0000A5AF  81 3a 35 3a 3a 3a 7b 22  61 72 67 73 22 3a 20 7b   .:5:::{" args": {
0000A5BF  22 69 64 6d 22 3a 20 38  39 2c 20 22 72 65 73 75   "idm": 8 9, "resu
0000A5CF  6c 74 22 3a 20 74 72 75  65 7d 2c 20 22 6e 61 6d   lt": tru e}, "nam
0000A5DF  65 22 3a 20 22 72 65 70  6c 79 22 7d               e": "rep ly"}
0000A5EB  81 03 32 3a 3a                                     ..2::
0000149C  81 83 b7 76 8b ee 85 4c  b1                        ...v...L .
000014A5  81 fe 00 82 20 0e a1 02  15 34 9b 38 5b 2c cf 63   .... ... .4.8[,.c
```


```
"result": "\tALConnectionManager::country\n\tInternal error no value"}, "name": "error"}.~.@5:::{"args": {"idm": 53,
"result": [[["ServiceId", "wifi_6002b4e85095_436f75676172576176654f70656e_managed_none"], ["Name", "CougarWaveOpen"],
["Type", "wifi"], ["State", "online"], ["Favorite", true], ["Autoconnect", true], ["Security", ["none"]], ["Domains",
["ColumbusState.EDU"]], ["Nameserver", ["168.26.188.11", "168.26.188.12"]], ["IPv4", [["Method", "dhcp"], ["Address",
"168.27.93.199"], ["Netmask", "255.255.240.0"], ["Gateway", "168.27.80.1"]]], ["IPv6", [["Method", "auto"]]], ["Proxy",
[["Method", "direct"]]], ["Strength", 55], ["Error", ""]]]}, "name": "reply"}.~..5:::{"args": {"idm": 54, "result":
{"pyobject": 12, "metaobject": {"signals": {"100": {"signature": "(m)", "uid": 100, "name": "signal"}, "86": {"signature":
"((IiIm(ll)<timeval,tv_sec,tv_usec>llII)<EventTrace,id,kind,slotId,arguments,timestamp,userUsTime,systemUsTime,callerConte
t,calleeContext>)", "uid": 86, "name": "traceObject"}}, "description": "", "methods": {"0": {"description": "",
"parameters": [], "parametersSignature": "(IIL)", "name": "registerEvent", "returnDescription": "", "returnSignature": "L"
"uid": 0}, "1": {"description": "", "parameters": [], "parametersSignature": "(IIL)", "name": "unregisterEvent",
"returnDescription": "", "returnSignature": "v", "uid": 1}, "2": {"description": "", "parameters": [],
"parametersSignature": "(I)", "name": "metaObject", "returnDescription": "", "returnSignature":
```

Security

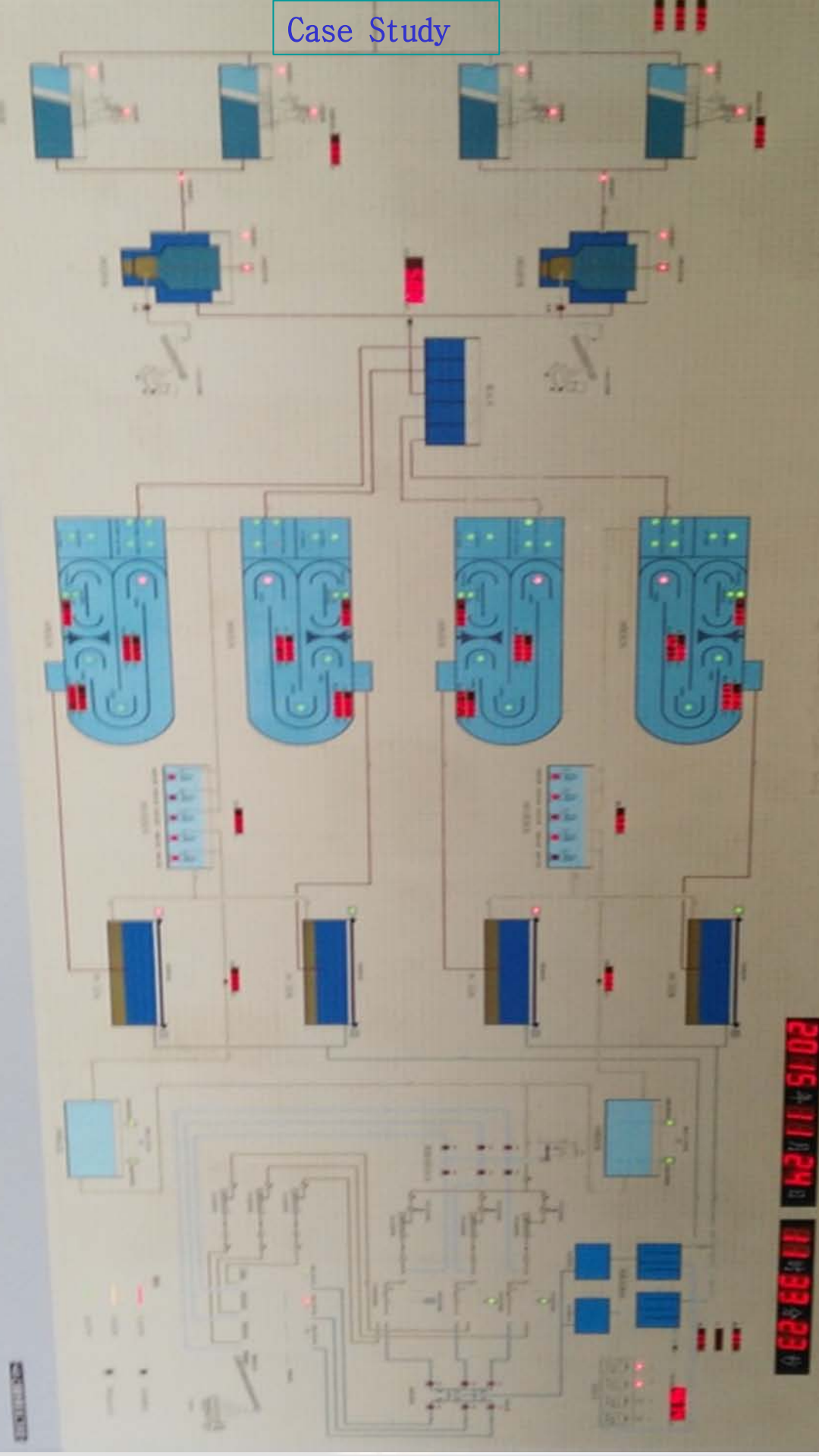
Microcontroller-based sensors, networked video cameras and other IoT devices are more vulnerable to cyber attacks.

Good security practices and approaches have to be put into place.

S ← (H + S) + M (Wang, CSI 2006)

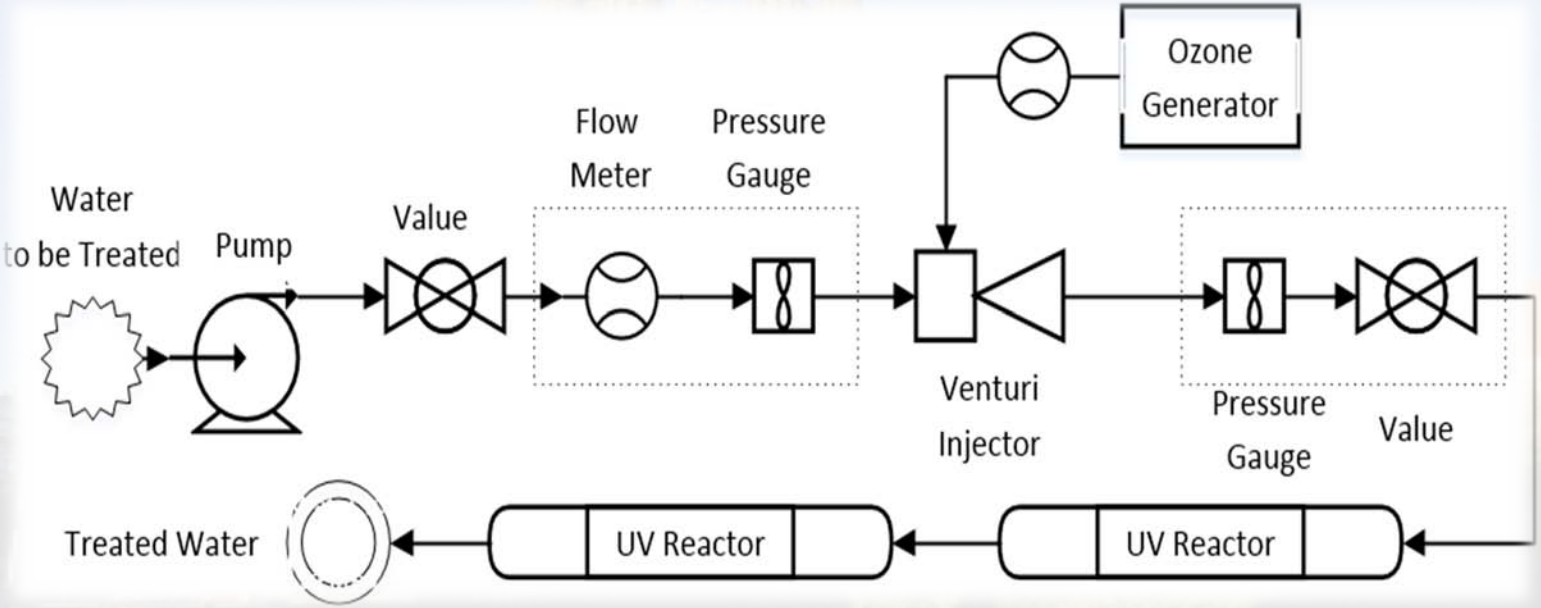
HiSPO (Wang, CISSE 2015)

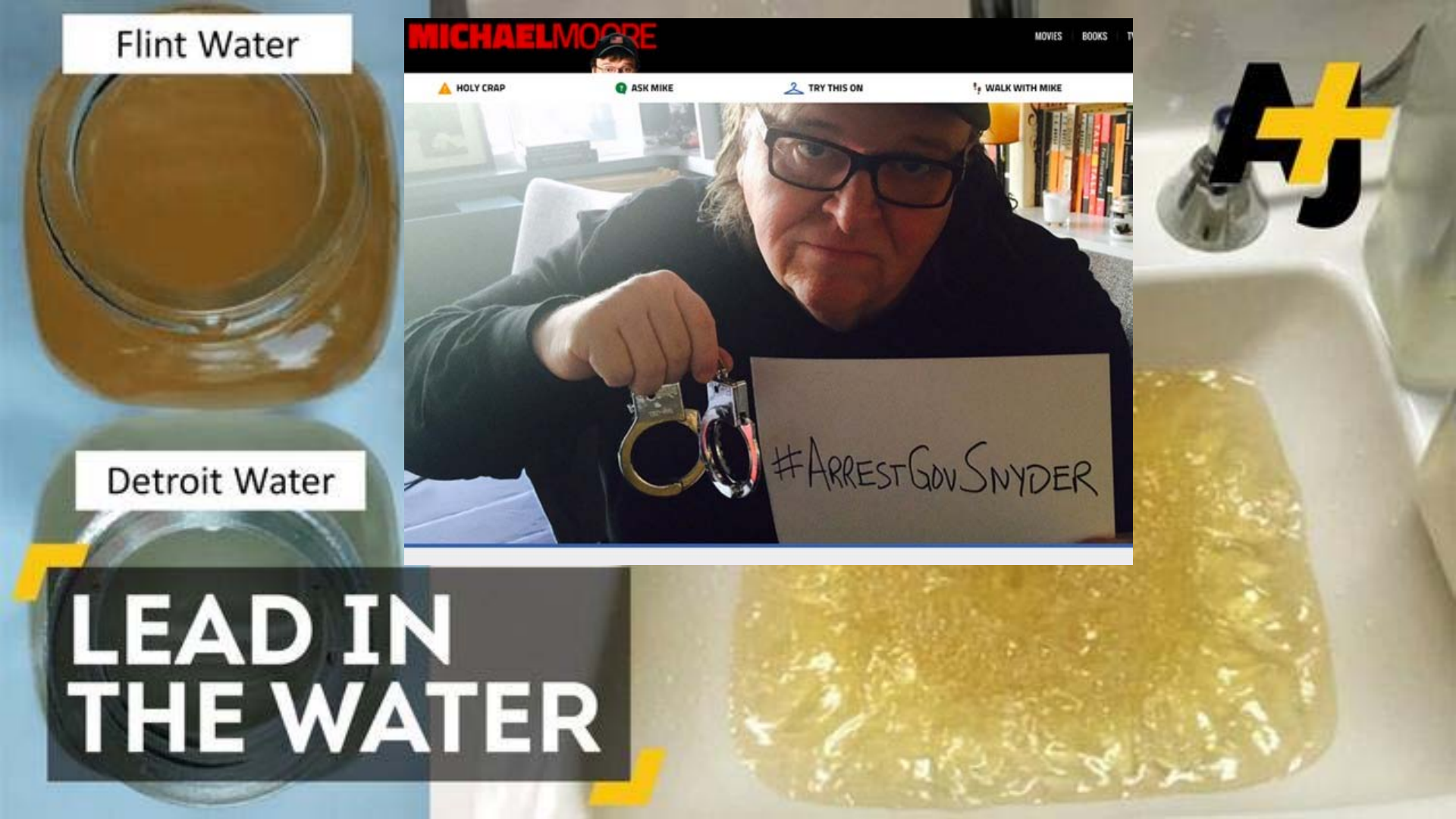
Case Study



Water Treatment Process Diagram

Case Study




Flint Water
Detroit Water
MICHAELMOORE
MOVIES
BOOKS
HOLY CRAP
ASK MIKE
TRY THIS ON
WALK WITH MIKE
#ARRESTGOVSNYDER
LEAD IN THE WATER

Solutions?

Case Study

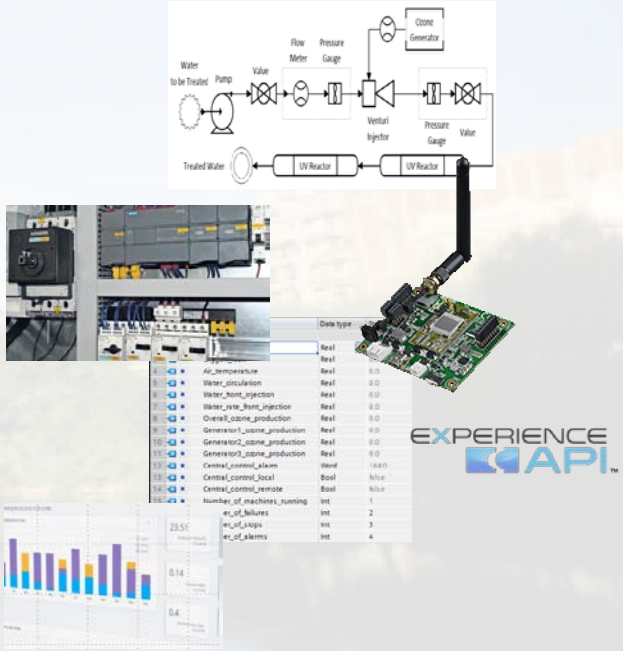
- Work on a **water** treatment system with 3,000+ PLCs
- Build a SCADA system
- Study the architecture for IoT – API, databases
- Look into data acquisition – various sensors
- Focus on PLC/RTU – com, legacy
- Assess vulnerability and security

Research can apply to other critical infrastructure sectors such as power grids, transportation, nuclear facilities etc.

Water Treatment SCADA Systems

Case Study

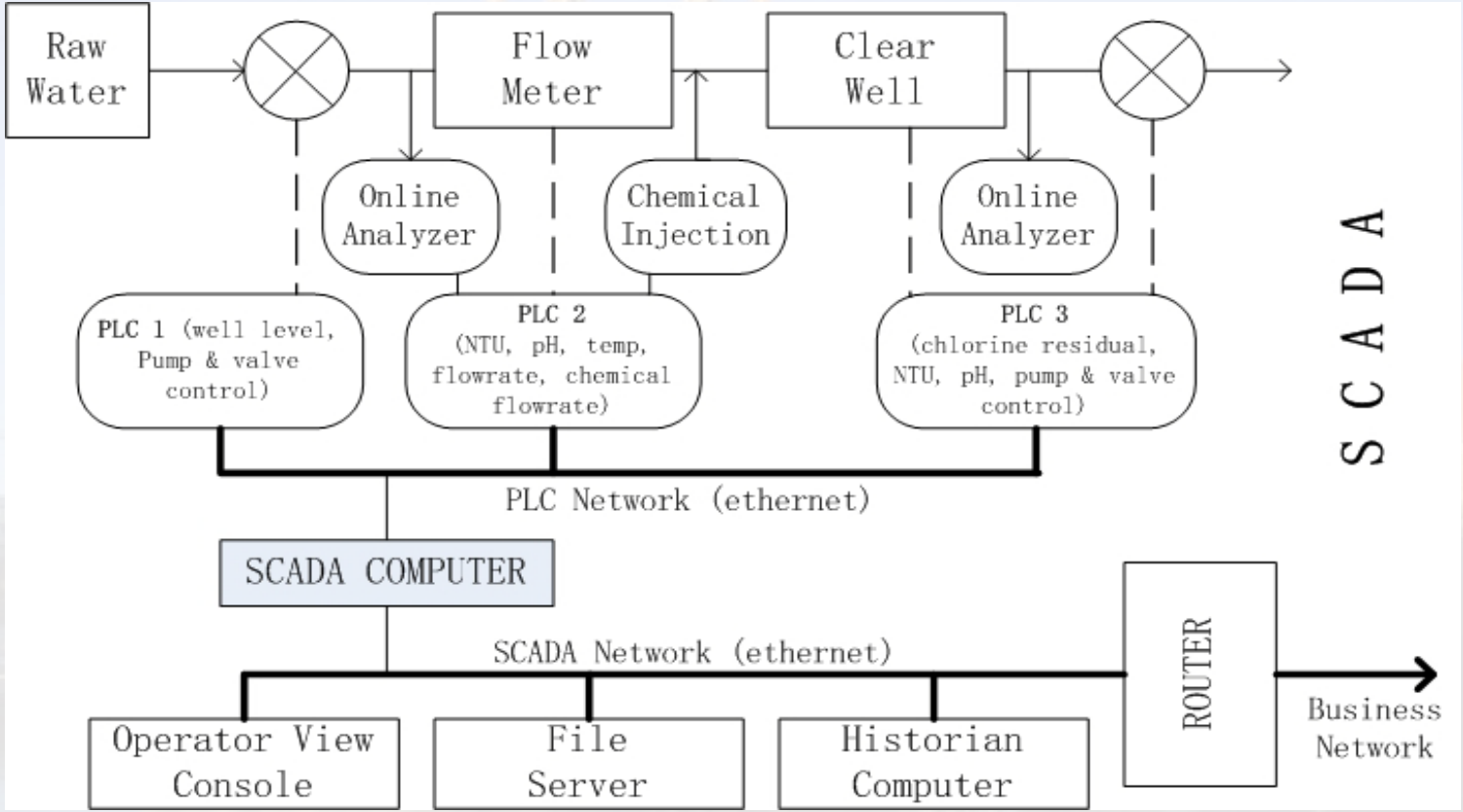
- Before smart city project was launched
  - water treatment plants were linked only by cables or standalone PLC systems,
  - do not connect to the Internet,
  - data flow in a closed environment (not shared).
- With SCADA system
  - the system collects data,
  - it issues commands from dashboard,
  - it can configure or control the PLCs remotely,
  - This also, opens up vulnerabilities to intruders

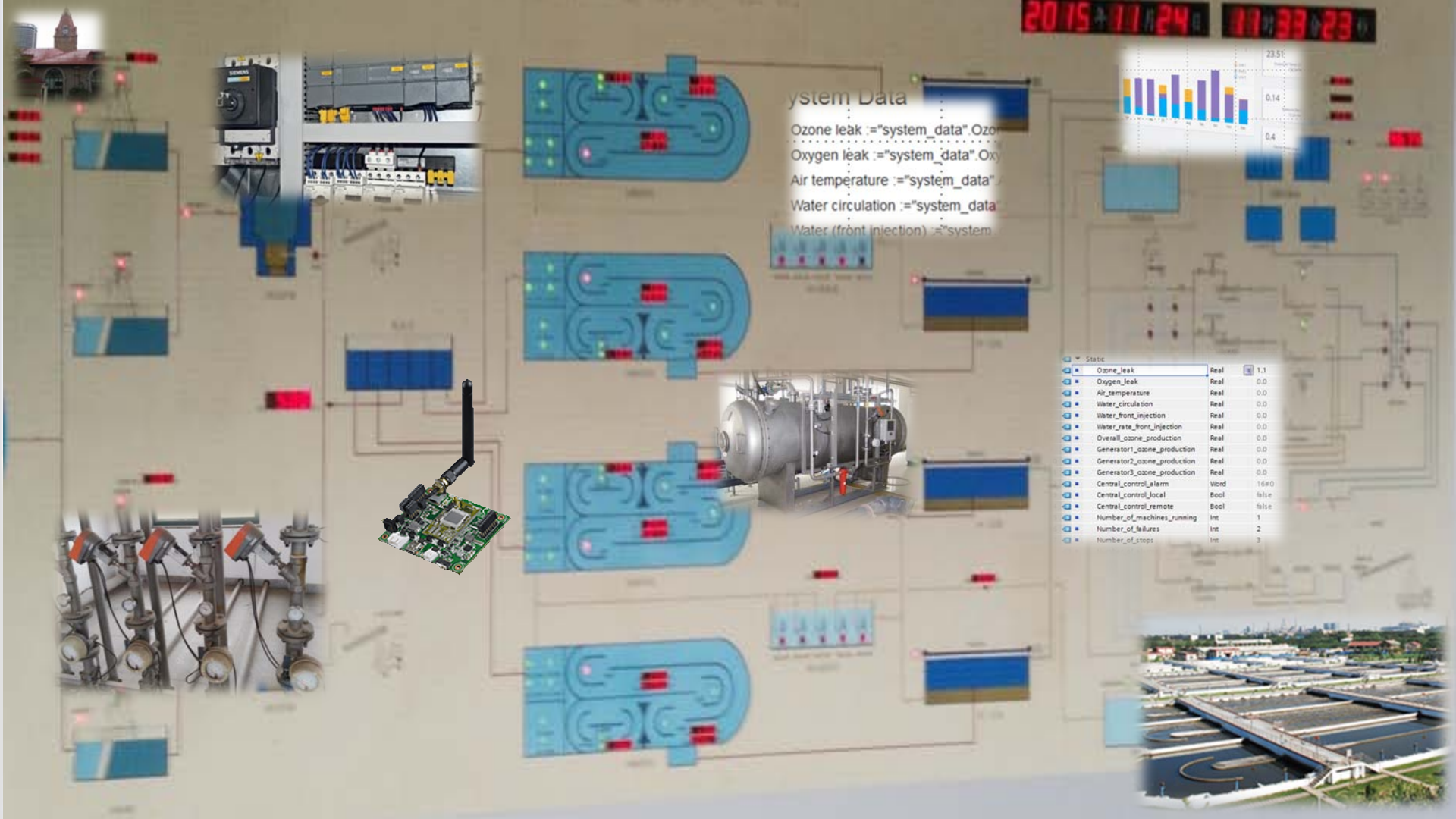


Vulnerabilities?

SCADA System Water Treatment Implementation

Case Study




ystem Data
Ozone leak :="system_data".Ozo
Oxygen leak :="system_data".Oxy
Air temperature :="system_data"
Water circulation :="system_data
Water (front injection) :="system
Static
Ozone_leak Real 1.1
Oxygen_leak Real 0.0
Air_temperature Real 0.0
Water_circulation Real 0.0
Water_front_injection Real 0.0
Water_rate_front_injection Real 0.0
Overall_ozone_production Real 0.0
Generator1_ozone_production Real 0.0
Generator2_ozone_production Real 0.0
Generator3_ozone_production Real 0.0
Central_control_alarm Word 16#0
Central_control_local Bool false
Central_control_remote Bool false
Number_of_machines_running Int 1
Number_of_failures Int 2
Number_of_stops Int 3

Sensors

Case Study

Name	Specifications		
	Scale	*Unit*	*Data Structure*
Ozone leak	0-2	ppm	real
Oxyzen leak	--25	%	real
Air temperature	-80 -- +20	°C	real
Water circulation		m^3/h	real
Ozone production		kg/h	real
Woking pressure	0-0.25	Mpa	real
System status		failure	real
remote			real

Energy harvesting sensors: on bridge, wearable, sensor networks, RFID, crystal radios

PLCs

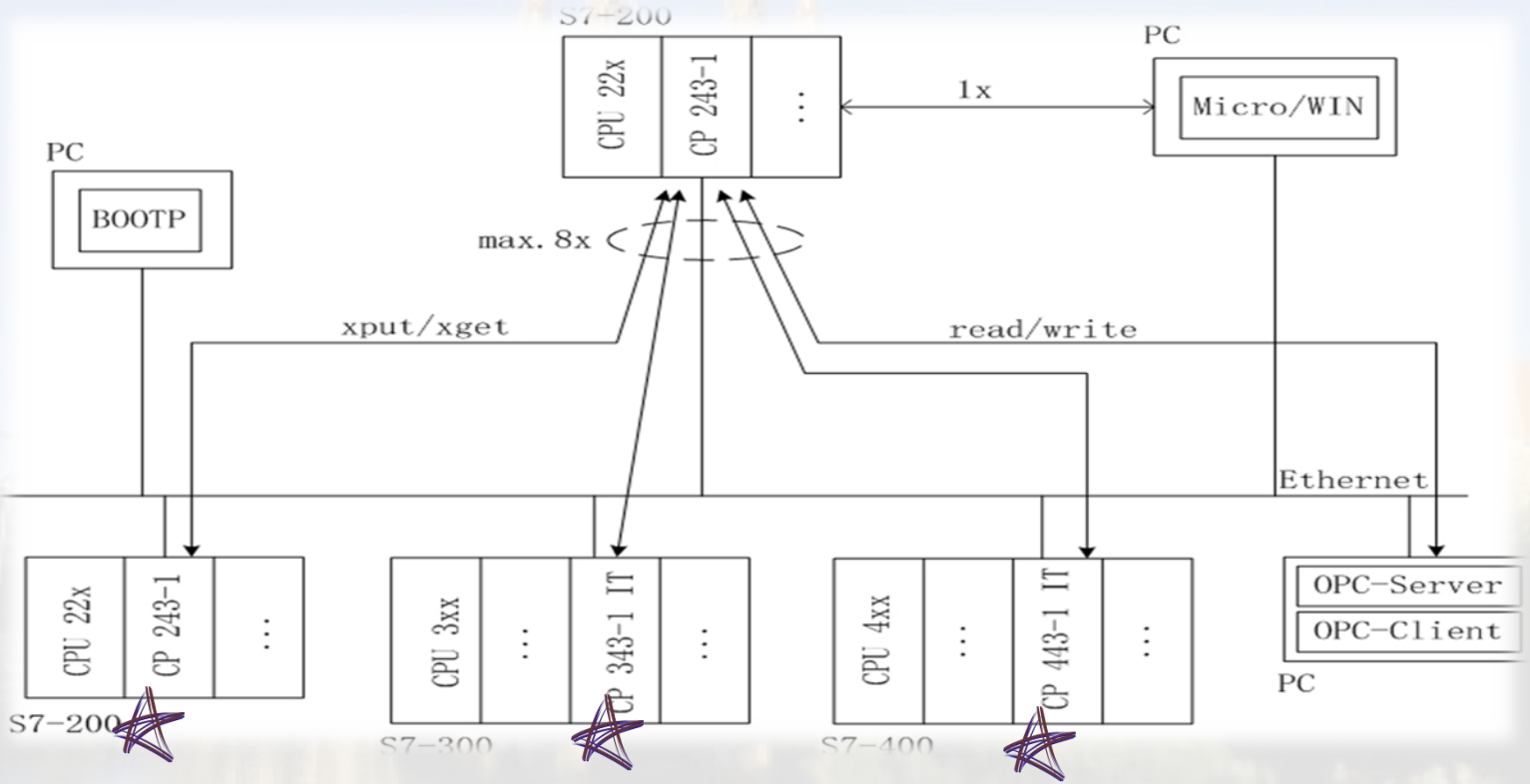
Case Study

Manufacturer	PLCs	
	Name	*Model #*
SIMENS	S7-200 Series	CPU 224
	S7-300 Series	CPU 315-2DP
	S7-200 SMART	CPU SR30
	S7-1500 Series	CPU 1511-1 PN
	S7-1200 Series	CPU 1214C
Allen-Bradley	ControlLogix	5580/5570
Schneider	Modicon	M221/M251

Secure PLCs – Web Servers, authentication, firewall, encryption

PLC and Communication

Case Study



Enable TCP/IP communication on legacy systems

Web Interface

Case Study

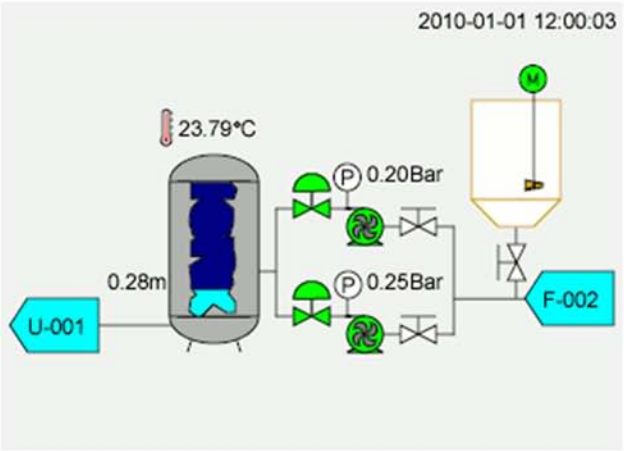
System Data

- Ozone leak :="system_data".Ozone_leak:
- Oxygen leak :="system_data".Oxygen_leak:
- Air temperature :="system_data".Air_temperature:
- Water circulation :="system_data".Water_circulation:
- Water (front injection) :="system_data".Water_front_injection:
- Water rate (front injection) :="system_data".Water_rate_front_injection:
- Overall ozone production :="system_data".Overall_ozone_production:
- #1 generator ozone production :="system_data".Generator1_ozone_production:
- #2 generator ozone production :="system_data".Generator2_ozone_production:
- #3 generator ozone production :="system_data".Generator3_ozone_production:
- Central control alarm :="system_data".Central_control_alarm:
- Central control local :="system_data".Central_control_local:
- Central control remote :="system_data".Central_control_remote:

Show 10 entries Search:

Nornal	Failure
:="system_data".Number_of_machines_running:	:="system_dat

Showing 1 to 1 of 1 entries Previous 1 Next

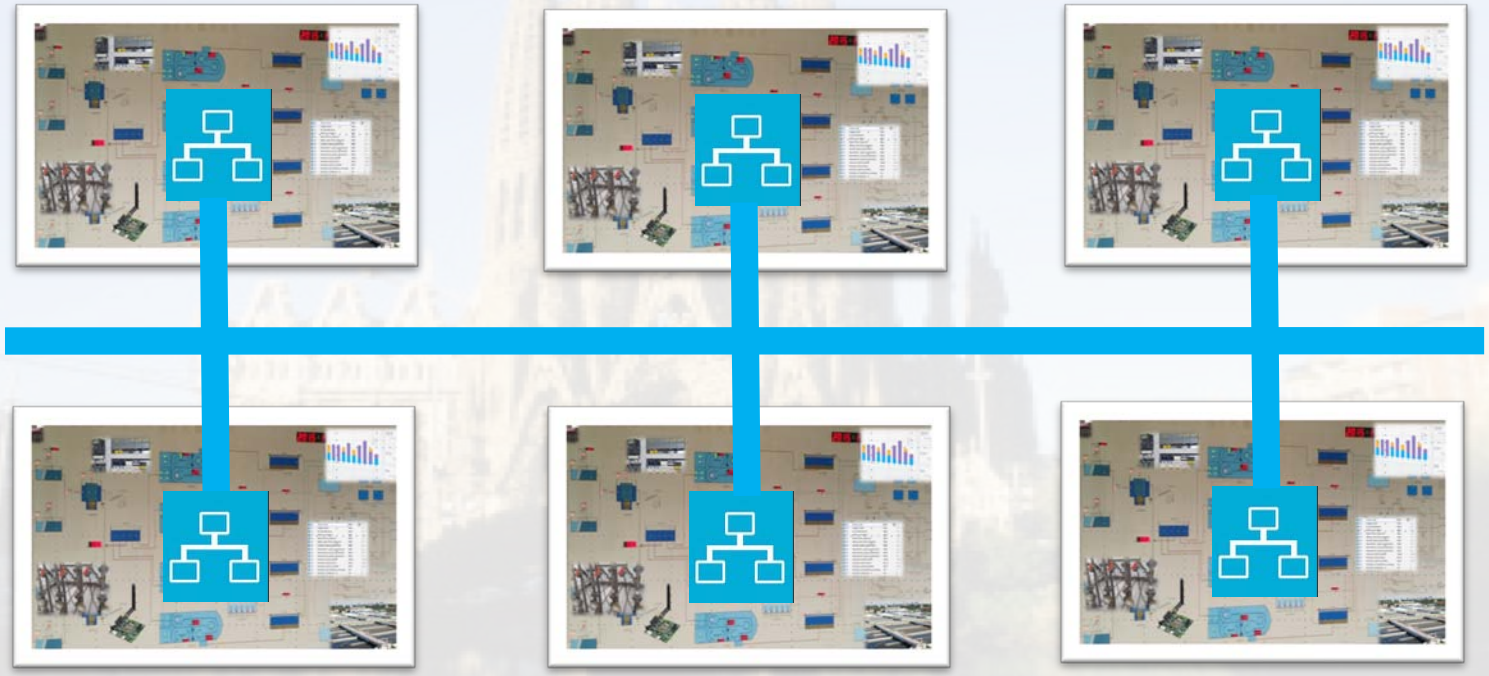


Configuration

Web-based monitoring and control in C&C Center

Data Acquisition

Case Study



Dual Data Model (cont.)

Case Study

- Ozone leak :="system_data".Ozone_leak:
- Oxygen leak :="system_data".Oxygen_leak:
- Air temperature :="system_data".Air_temperature:
- Water circulation :="system_data".Water_circulation:
- Water (front injection) :="system_data".Water_front_injection:
- Water rate (front injection) :="system_data".Water_rate_front_injection:
- Overall ozone production :="system_data".Overall_ozone_production:
- #1 generator ozone production :="system_data".Generator1_ozone_prod
- #2 generator ozone production :="system_data".Generator2_ozone_prod
- #3 generator ozone production :="system_data".Generator3_ozone_prod
- Central control alarm :="system_data".Central_control_alarm:
- Central control local :="system_data".Central_control_local:
- Central control remote :="system_data".Central_control_remote:

Sensors

Field Name	Data Type
ID	AutoNumber
Ozone leak	Number
Oxygen leak	Number
Air temperature	Number
Water circulation	Number
Water rate	Number
Overall ozone production	Number
Central control alarm	Yes/No
Central contral local	Number
Cental contral remote	Number

- Data are **not** inserted in rows.
- Each attribute represents a sensor. DB insertion based on **attributes**, not rows.

Dual-Data Model (cont.)

Case Study

- REST – Jason over HTTP
- MIT - Robotic device for patching for pipeline leaks
- Libelium – smart sensor to monitor water quality in rivers
- Carnegie Mellon Univ. – Water Quest: monitor using GIS
- xAPI
  - serial database: one attribute at a time

```
$( document ).ready(function() {
    ADL.XAPIWrapper.changeConfig(Config);
    $('#example').DataTable();
    $( "input[type='checkbox']" ).each(function() {
        context = $(this).attr("val");
        console.log(context);
        var stat1 = {"actor":{"mbox":actorid,
                      "name":actorname,
                      "objectType":"Agent"},
          "verb": {"id": "http://adlnet.gov/expapi/verbs/
                      "display": {"en-US": "check"}
                    },
          "context": {
            "extensions": {
                "http://adlnet.gov/expapi/extensions/che
                    "beaconid": "34",
                    "checkboxoption": context
                }
            }
          },
          "object":{
            "id": "http://adlnet.gov/expapi/activities/ch
            "definition": {
              "description": {
                "en-US": context
              },
              "name": {
                "en-US":context
```

EXPERIENCE API™

Legacy Systems

- *LibNoDave*
- *Simatic NET*
- *OPC Server*
- *Snap7 Client*

ReadBytes

Bytes read

Ethernet

Wifi

Serial input to Networks Forwarding

Raspberry Pi

Serial

MPI Adapter

HMI

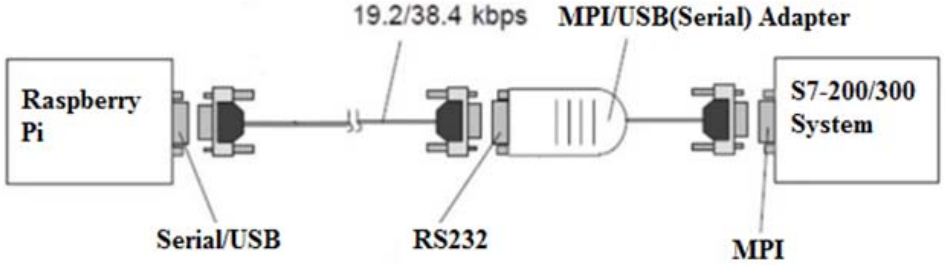
Write var

Ack

PC

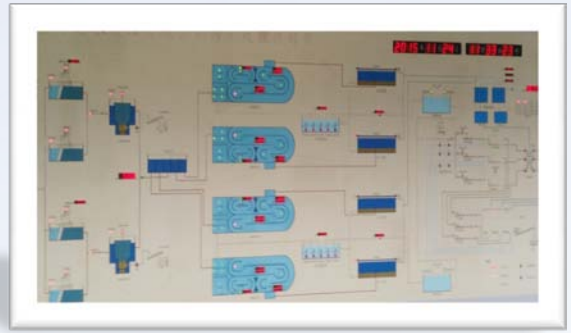
Block Download

Ack



Dashboard

Case Study



Case Study

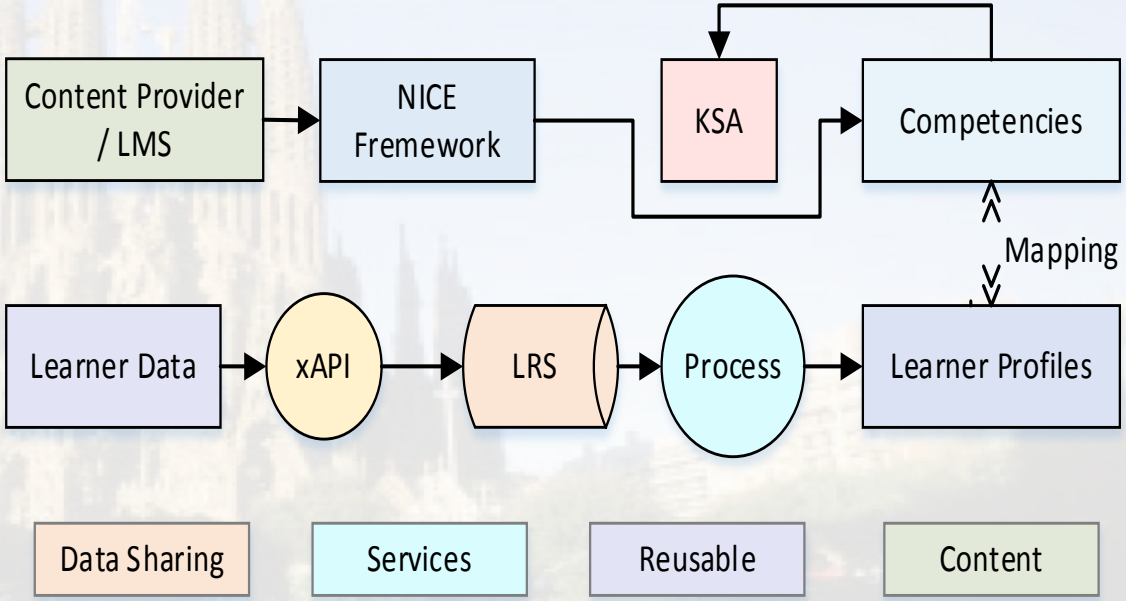
Clean water supply and sewage water treatment are important for cities and communities.

SCADA systems are able to monitor the processes and take control actions when necessary.

Incidents such as Flint water crisis could have been prevented by adopting SCADA systems.

Curriculum Development

- Visualize NICE framework
- Record learners' progress
- Link competencies to profiles
- Assess security and privacy



Takeaways

- SCADA/IoT/Smart city architecture
  - Paired firewalls, defense in depth
  - Dual-data abstraction model
    - Serial database for PLCs and sensors, Relational DB for dashboard
- Security
  - Strong authentication and encryption
  - Smart sensor security
  - HiSPO approach

    Hardware + intelligence + Software + Policy + Operation (Wang 2015)

Shuangbao (Paul) Wang, Ph.D.

paul.wang@computer.org