SCADA Testbed for Vulnerability Assessments, Penetration Testing and Incident Forensics

Sundar Krishnan & Dr. Mingkui Wei

Department of Computer Science
Sam Houston State University, Huntsville, Texas

SCADA – Overview

- SCADA (Supervisory Control and Data Acquisition) -> critical infrastructure
- SCADA security is often an add-on -> Focus on safety
- SCADA's integration with cyberspace
- Vendors seldom upgrade, invest -> Aging infrastructure
- Growing cyber threats -> Insider-threats (employees), Hackers
- Few labs for students that focus on SCADA Cyber-Vulnerability Assessments, SCADA Pen-tests & SCADA Incidents Forensic research
- Growing job market & a niche skill in the Industry

… SCADA world is a ripe target for Cyber threats with limited security and forensic expertise.

LAB – Problem Statement

Lack of a SCADA LAB at SHSU for Vulnerability assessments, Penetration testing and Incident Forensics research

LAB - Benefits

1. Learn and understand SCADA, HMI, PLC concepts
2. Lab designed with a *real-world* scenario in mind
3. Supports a **B**uild-**E**xploit-**B**reak-**I**nvestigate study approach
4. Conduct Cybersecurity tasks and Forensics research in SCADA world
5. SCADA Penetration-testing/Vulnerability testing using tools like Wireshark, Metasploit, CANVAS, SQLMap, NETCAT, BurpSuite, HPING etc.
6. Perform live SCADA Incident management and forensics.
7. Conduct Cyber Vulnerability Assessments prescribed in NERC's, NIST, DHS standards

LAB – Highlights

SCADA LAB Design

1. LAB design is modelled after generally found deployment architecture in the ICS world
2. Devoid of servers, minimum firewalls, use of WIN-XP machines, missing OS security patches and unsecure Wi-Fi

ICS/SCADA Design:

1. Use of PLC/RTU and stimulators
2. Top **5** SCADA protocols used in Oil and Gas Industry (MODBUS/TCP-IP,

   KOYO-ECOM, OPC-UA,OPC-DA, CodeSys ARTI, DNP3)
3. SCADA/HMI software: InduSoft studio
4. Custom user interface developed to invoke SCADA protocol traffic
5. Use of InduSoft's thin client (web/browser based) and InduSoft's secure viewer

KOYO-ECOM: Automationdirect protocol OPC: OLE for Process Control MODBUS: Modicon's protocol DNP3 (Distributed Network Protocol)
OPC UA: OPC Unified Architecture OPC Data AccessCodesys Arti (Asynchronous Runtime Interface)

LAB – Highlights *(contd.)*

Database

SQL Server Database (2000 and 2008)

Websites

1. Websites custom programmed using classic ASP and JavaScript
2. Using ODBC for DB connectivity
3. Hosted on IIS with shallow security features

Design features with a purpose..

1. Minimal use of firewalls, switches, routers
2. Missing security patches
3. Scatter of WIN-XP and WIN7 O/S
4. Unsecure Wireless Access Point
5. Wireless security camera

.. all to mimic a real-world scenario..

Lab - Project Risks

RISK	Consequence	Level	Mitigation
SCADA/ICS Hardware procurement (donation) from vendors	Delay to schedule	High	Plan and co-ordinate procurement with vendors
Lab space availability	Delay to schedule	Medium	Work closely with Dept. Facilities
SCADA/ICS Hardware Configuration	Delay to schedule	Medium	Plan, schedule and co-ordinate with InduSoft Engineers
Lab IT-Hardware (desktops, switches) availability	Delay to schedule	Medium	Work closely with Dept. and IT Support

LAB – Project schedule

Phase	Task
Planning	Project Proposal & Approvals
	Source hardware (SCADA, desktops, switches)
	Project Kick-Off (stakeholder meeting)
Execution Phase-I	Configure SCADA hardware (with guidance from InduSoft Engineers)
	Coding using InduSoft Studio
	Verification (Testing) of Protocol Traffic
	Milestone - stakeholder meeting
Execution/Verification Phase-II	Install and configure Penetration-testing software
	Install and configure Forensics software
	Verification (Testing) of pen-test and forensics tools
	Milestone - stakeholder meeting
Validation Phase-III	Demonstrate/Validate Lab
	Lab Go-Live
Close-out	Project close-out (project documentation, metrics, lab documentation, manuscript preparation)

LAB - KAT Engineering and Chemicals

Company Overview

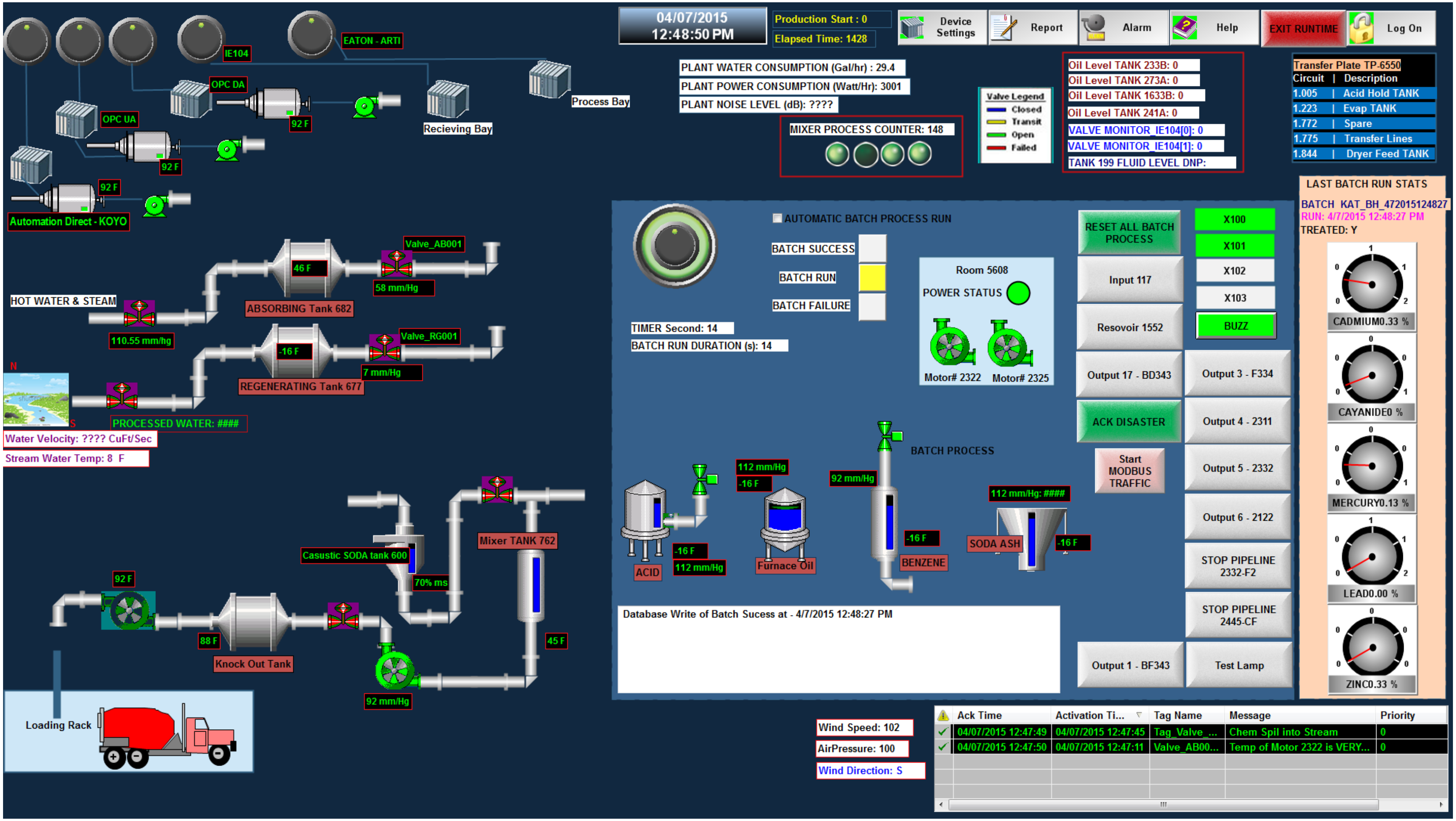
1. Fictious chemical manufacturing company
2. It's manufacturing plant processes batches of chemicals during manufacturing process involving batch-mixing, motors, pipelines, furnaces, storage tanks and loading.
3. Releases processed water into environment (a nearby stream/bayou). Valid permits exist for certain toxicity limits.
4. Financial penalties if toxicity limits breached. Reduced penalties if reported to government agencies within SLAs.
5. PLCs monitor and report (on HMI screens) various processes including quality of processed water being released into nearby stream.

Red and Blue teams

1. KAT employs in-house IT-security for operational support, incident management and forensics – traditional Blue team
2. Red Team are external hackers or disgruntled employees depending on the lab exercise.

Prized capture by Red Team is access-to Operator's HMI screen.

LAB – HMI Screen



04/07/2015
12:48:50 PM

Production Start : 0
Elapsed Time: 1428

PLANT WATER CONSUMPTION (Gal/hr) : 29.4
PLANT POWER CONSUMPTION (Watt/Hr): 3001
PLANT NOISE LEVEL (dB): ????

MIXER PROCESS COUNTER: 148

Oil Level TANK 233B: 0
Oil Level TANK 273A: 0
Oil Level TANK 1633B: 0
Oil Level TANK 241A: 0
VALVE MONITOR_IE104[0]: 0
VALVE MONITOR_IE104[1]: 0
TANK 199 FLUID LEVEL DNP:

Transfer Plate TP-6550

Circuit	Description
1.005	Acid Hold TANK
1.223	Evap TANK
1.772	Spare
1.775	Transfer Lines
1.844	Dryer Feed TANK

LAST BATCH RUN STATS
BATCH KAT_BH_472015124827
RUN: 4/7/2015 12:48:27 PM
TREATED: Y

CADMIUM0.33 %
CAYANIDE0 %
MERCURY0.13 %
LEAD0.00 %
ZINC0.33 %

□ AUTOMATIC BATCH PROCESS RUN

TIMER Second: 14
BATCH RUN DURATION (s): 14

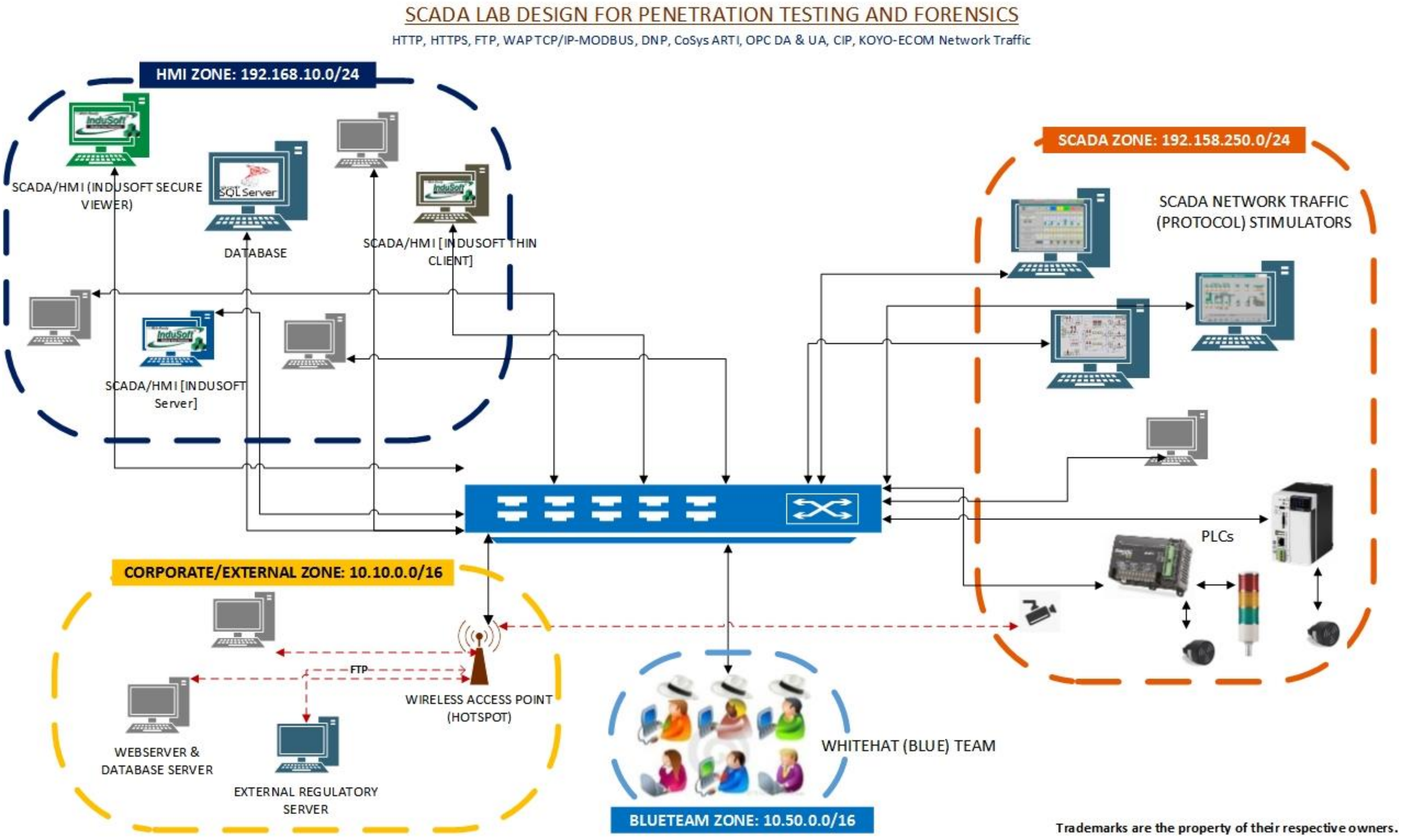
Database Write of Batch Sucess at - 4/7/2015 12:48:27 PM

HOT WATER & STEAM
PROCESSED WATER: ####
Water Velocity: ???? CuFt/Sec
Stream Water Temp: 8 F

Wind Speed: 102
AirPressure: 100
Wind Direction: S

Ack Time	Activation Ti...	Tag Name	Message	Priority
✓ 04/07/2015 12:47:49	04/07/2015 12:47:45	Tag_Valve_...	Chem Spil into Stream	0
✓ 04/07/2015 12:47:50	04/07/2015 12:47:11	Valve_AB00...	Temp of Motor 2322 is VERY...	0

LAB – Network Architecture of KAT Engineering and Chemicals Company

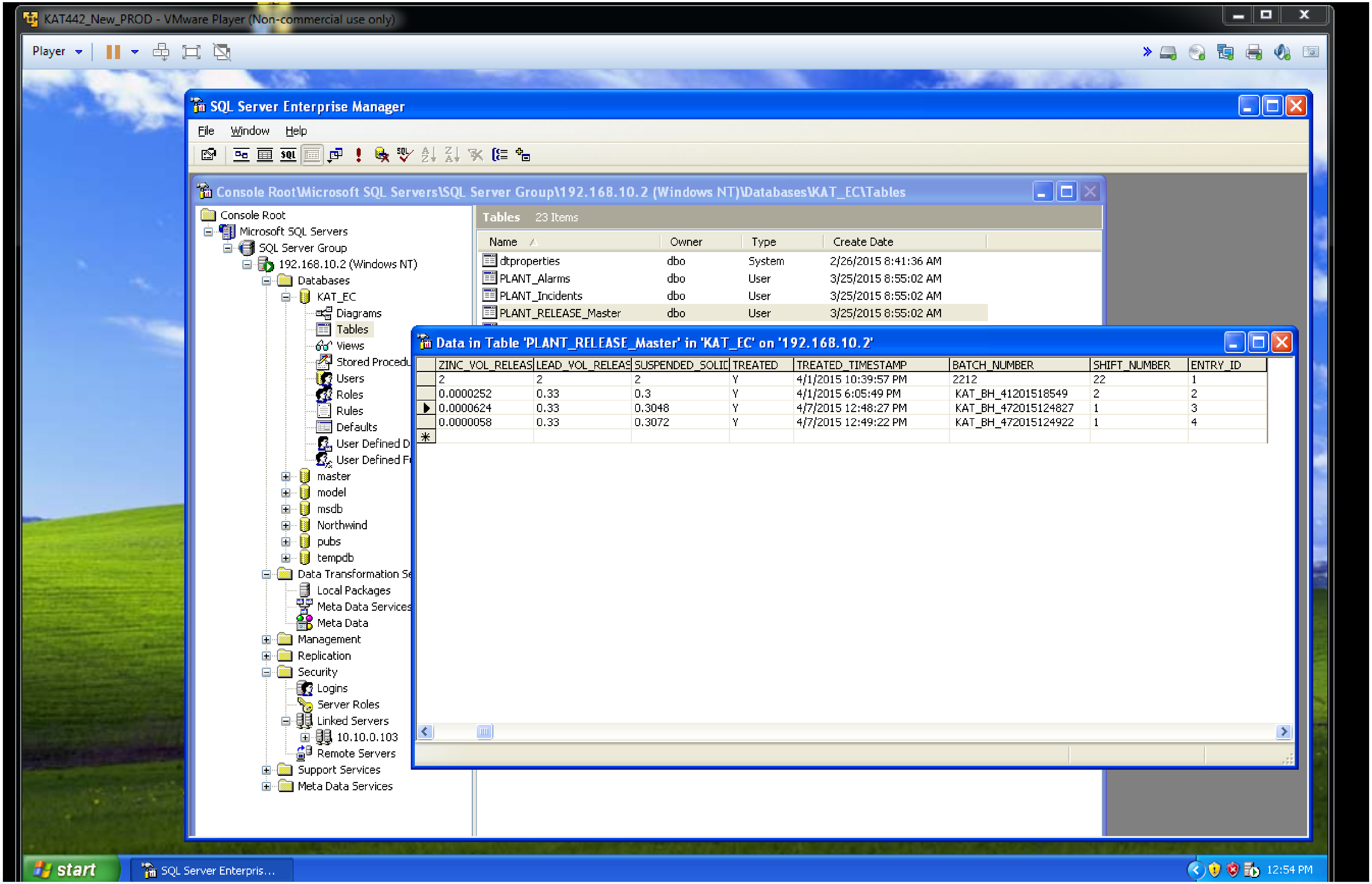

SCADA LAB DESIGN FOR PENETRATION TESTING AND FORENSICS
HTTP, HTTPS, FTP, WAP TCP/IP-MODBUS, DNP, CoSys ARTI, OPC DA & UA, CIP, KOYO-ECOM Network Traffic
HMI ZONE: 192.168.10.0/24
SCADA/HMI (INDUSOFT SECURE VIEWER)
DATABASE
SCADA/HMI [INDUSOFT THIN CLIENT]
SCADA/HMI [INDUSOFT Server]
SCADA ZONE: 192.158.250.0/24
SCADA NETWORK TRAFFIC (PROTOCOL) STIMULATORS
PLCs
CORPORATE/EXTERNAL ZONE: 10.10.0.0/16
FTP
WIRELESS ACCESS POINT (HOTSPOT)
WEBSERVER & DATABASE SERVER
EXTERNAL REGULATORY SERVER
WHITEHAT (BLUE) TEAM
BLUETEAM ZONE: 10.50.0.0/16
Trademarks are the property of their respective owners.

- ➢ Network Firewall rules help segment network. Switches and routers present. Dynamic and static IPs issued.
- ➢ System Patching irregular - tuned per lab exercise.
- ➢ A “timed incident bomb” will cause disruption (if Red team is unsuccessful).

SCADA LAB – Project verification controls

#	Test Case(s)	Primary Software tool used
1	Test for MODBUS protocol traffic	Wireshark
2	Test for OPC DA protocol traffic	Simulator logs
3	Test for OPC UA protocol traffic	Wireshark
4	Test for KOYO protocol traffic (KOYO is transmitted as UDP packets)	Wireshark
5	Test for EATON's CodeSYS ARTI protocol traffic	Simulator logs
6	Test for DNP 3.0 protocol traffic	Wireshark
7	Verify network for IE104 protocol traffic	Simulator logs
8	Verify if Direct06 PLC is configured to respond via HMI (Indusoft) interface	HMI alarms and logs
9	Verify if Eaton PLC is configured to respond via HMI (Indusoft) interface	HMI alarms and logs
10	Test for password strength using password cracker tools	John the Ripper
11	Perform a penetration test using any known exploit against the lab network	Metasploit
12	Test for Windows security patches to expose backdoors	Microsoft Baseline Security Analyzer
13	Test for SQL Injection against lab websites	SQL Map
14	Test for open and vulnerable ports against lab network	NMap
15	Test for website vulnerabilities against lab network	Vega
16	Test for MD5 or SHA1 cryptographic hashes on drives for forensic evidence integrity	Microsoft File Checksum Integrity Verifier

LAB – Historian database

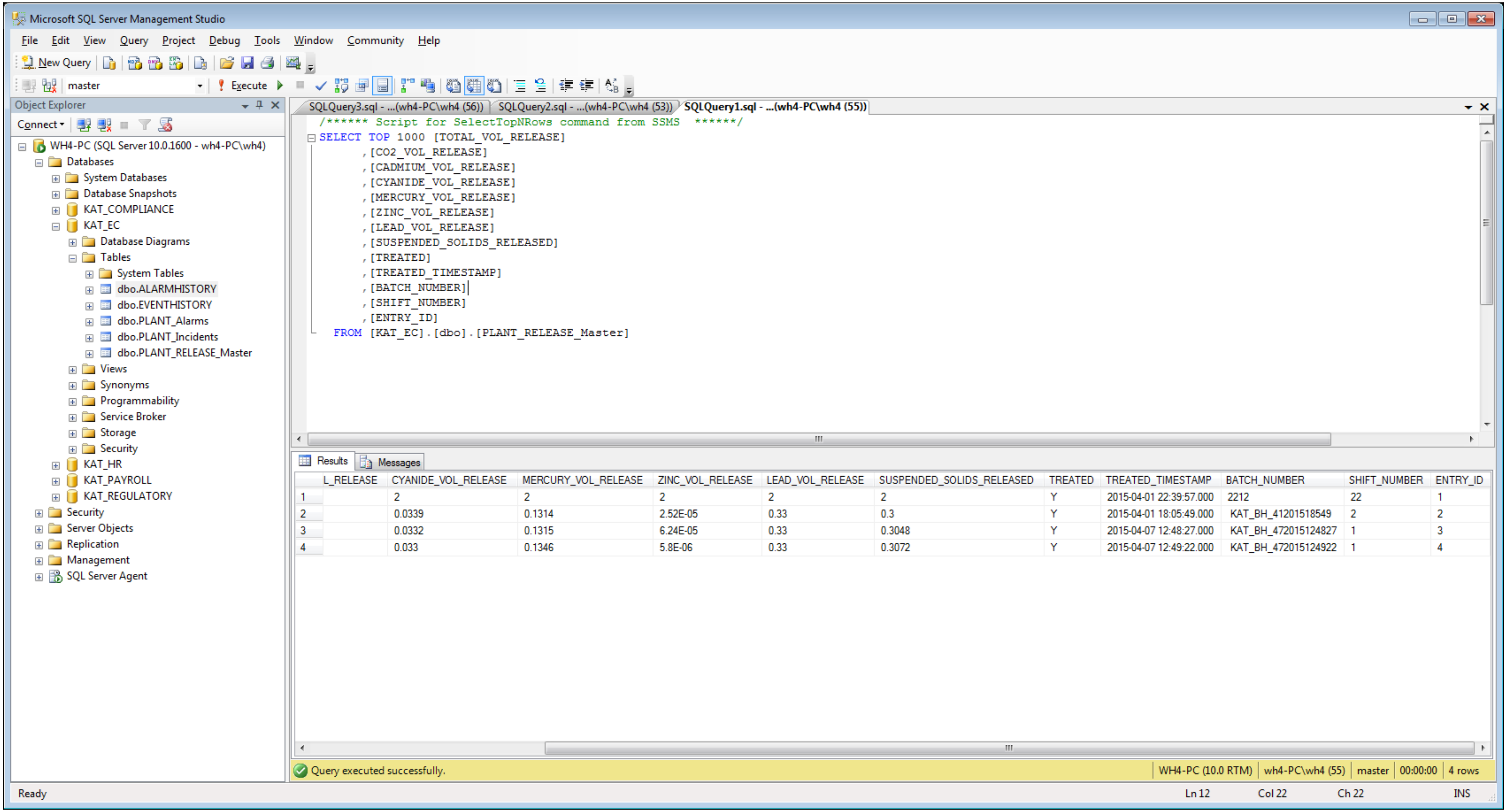


Name	Owner	Type	Create Date
dtproperties	dbo	System	2/26/2015 8:41:36 AM
PLANT_Alarms	dbo	User	3/25/2015 8:55:02 AM
PLANT_Incidents	dbo	User	3/25/2015 8:55:02 AM
PLANT_RELEASE_Master	dbo	User	3/25/2015 8:55:02 AM

Data in Table 'PLANT_RELEASE_Master' in 'KAT_EC' on '192.168.10.2'

ZINC_VOL_RELEAS	LEAD_VOL_RELEAS	SUSPENDED_SOLID	TREATED	TREATED_TIMESTAMP	BATCH_NUMBER	SHIFT_NUMBER	ENTRY_ID
2	2	2	Y	4/1/2015 10:39:57 PM	2212	22	1
0.0000252	0.33	0.3	Y	4/1/2015 6:05:49 PM	KAT_BH_41201518549	2	2
0.0000624	0.33	0.3048	Y	4/7/2015 12:48:27 PM	KAT_BH_472015124827	1	3
0.0000058	0.33	0.3072	Y	4/7/2015 12:49:22 PM	KAT_BH_472015124922	1	4

LAB – SQL Server 2008

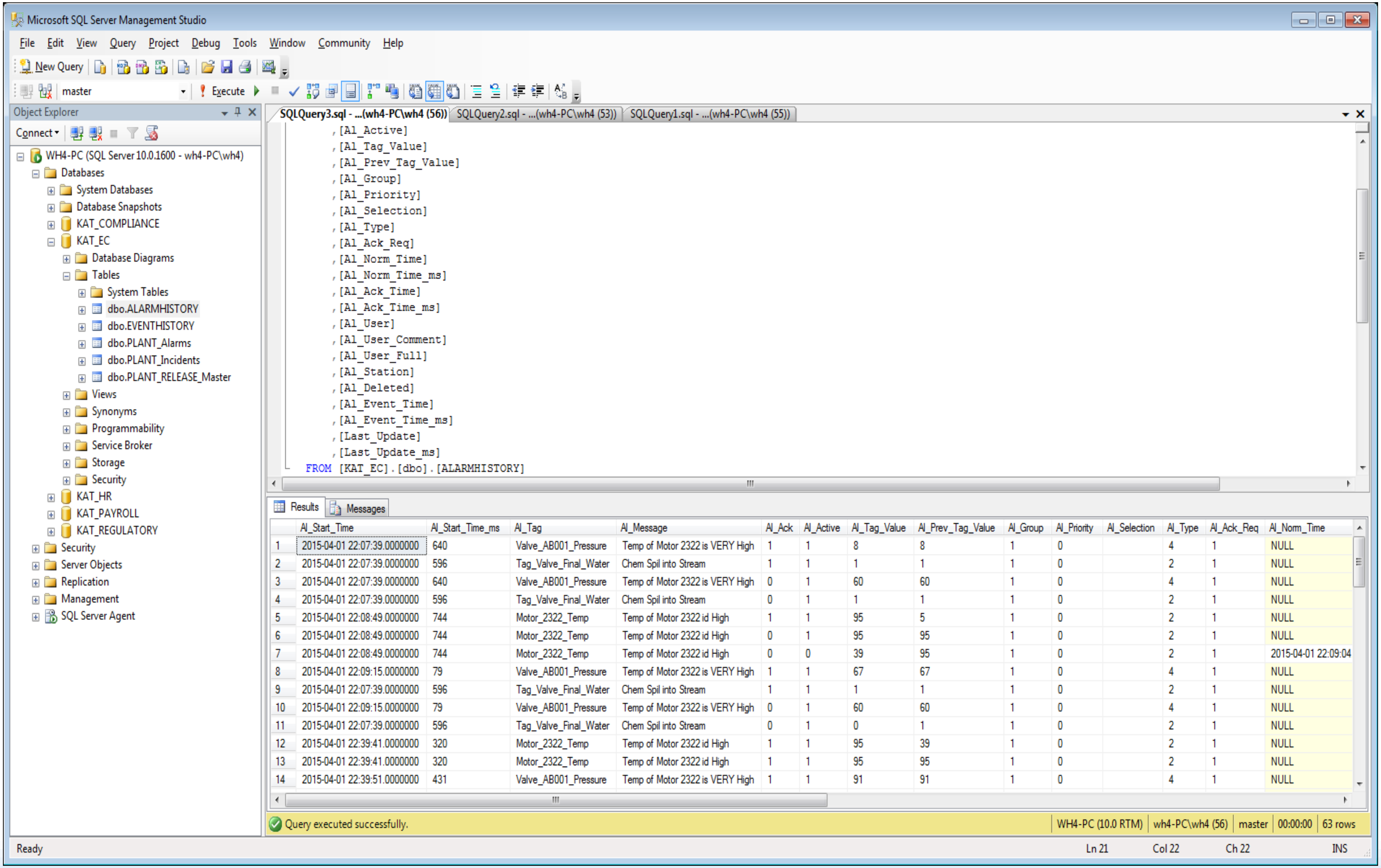


```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP 1000 [TOTAL_VOL_RELEASE]
      ,[CO2_VOL_RELEASE]
      ,[CADMIUM_VOL_RELEASE]
      ,[CYANIDE_VOL_RELEASE]
      ,[MERCURY_VOL_RELEASE]
      ,[ZINC_VOL_RELEASE]
      ,[LEAD_VOL_RELEASE]
      ,[SUSPENDED_SOLIDS_RELEASED]
      ,[TREATED]
      ,[TREATED_TIMESTAMP]
      ,[BATCH_NUMBER]
      ,[SHIFT_NUMBER]
      ,[ENTRY_ID]
  FROM [KAT_EC].[dbo].[PLANT_RELEASE_Master]
```

	L_RELEASE	CYANIDE_VOL_RELEASE	MERCURY_VOL_RELEASE	ZINC_VOL_RELEASE	LEAD_VOL_RELEASE	SUSPENDED_SOLIDS_RELEASED	TREATED	TREATED_TIMESTAMP	BATCH_NUMBER	SHIFT_NUMBER	ENTRY_ID
1		2	2	2	2	2	Y	2015-04-01 22:39:57.000	2212	22	1
2		0.0339	0.1314	2.52E-05	0.33	0.3	Y	2015-04-01 18:05:49.000	KAT_BH_41201518549	2	2
3		0.0332	0.1315	6.24E-05	0.33	0.3048	Y	2015-04-07 12:48:27.000	KAT_BH_472015124827	1	3
4		0.033	0.1346	5.8E-06	0.33	0.3072	Y	2015-04-07 12:49:22.000	KAT_BH_472015124922	1	4

Query executed successfully.

LAB – SQL Server 2008

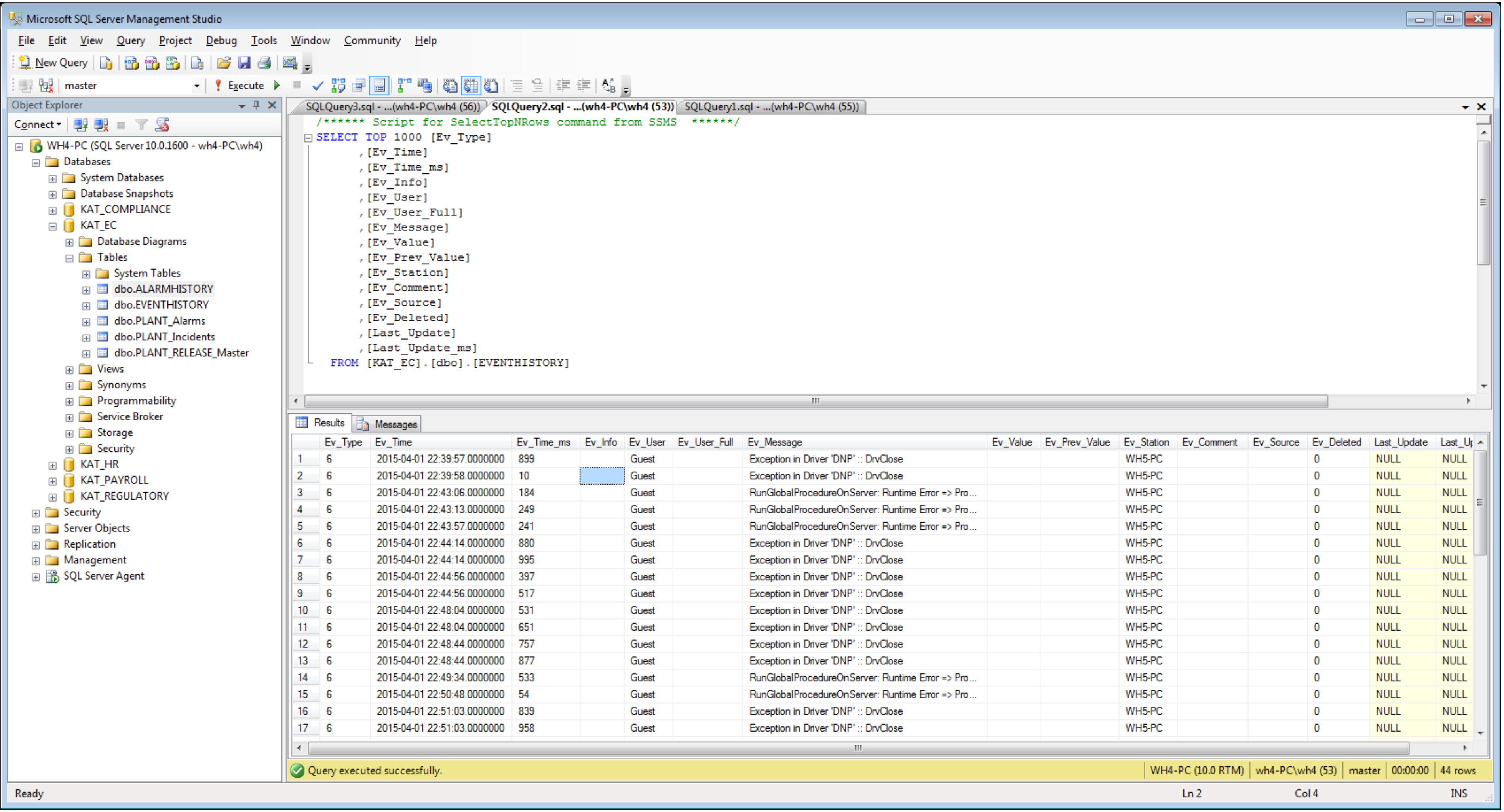


```
      ,[Al_Active]
      ,[Al_Tag_Value]
      ,[Al_Prev_Tag_Value]
      ,[Al_Group]
      ,[Al_Priority]
      ,[Al_Selection]
      ,[Al_Type]
      ,[Al_Ack_Req]
      ,[Al_Norm_Time]
      ,[Al_Norm_Time_ms]
      ,[Al_Ack_Time]
      ,[Al_Ack_Time_ms]
      ,[Al_User]
      ,[Al_User_Comment]
      ,[Al_User_Full]
      ,[Al_Station]
      ,[Al_Deleted]
      ,[Al_Event_Time]
      ,[Al_Event_Time_ms]
      ,[Last_Update]
      ,[Last_Update_ms]
  FROM [KAT_EC].[dbo].[ALARMHISTORY]
```

	Al_Start_Time	Al_Start_Time_ms	Al_Tag	Al_Message	Al_Ack	Al_Active	Al_Tag_Value	Al_Prev_Tag_Value	Al_Group	Al_Priority	Al_Selection	Al_Type	Al_Ack_Req	Al_Norm_Time
1	2015-04-01 22:07:39.0000000	640	Valve_AB001_Pressure	Temp of Motor 2322 is VERY High	1	1	8	8	1	0		4	1	NULL
2	2015-04-01 22:07:39.0000000	596	Tag_Valve_Final_Water	Chem Spil into Stream	1	1	1	1	1	0		2	1	NULL
3	2015-04-01 22:07:39.0000000	640	Valve_AB001_Pressure	Temp of Motor 2322 is VERY High	0	1	60	60	1	0		4	1	NULL
4	2015-04-01 22:07:39.0000000	596	Tag_Valve_Final_Water	Chem Spil into Stream	0	1	1	1	1	0		2	1	NULL
5	2015-04-01 22:08:49.0000000	744	Motor_2322_Temp	Temp of Motor 2322 id High	1	1	95	5	1	0		2	1	NULL
6	2015-04-01 22:08:49.0000000	744	Motor_2322_Temp	Temp of Motor 2322 id High	0	1	95	95	1	0		2	1	NULL
7	2015-04-01 22:08:49.0000000	744	Motor_2322_Temp	Temp of Motor 2322 id High	0	0	39	95	1	0		2	1	2015-04-01 22:09:04
8	2015-04-01 22:09:15.0000000	79	Valve_AB001_Pressure	Temp of Motor 2322 is VERY High	1	1	67	67	1	0		4	1	NULL
9	2015-04-01 22:07:39.0000000	596	Tag_Valve_Final_Water	Chem Spil into Stream	1	1	1	1	1	0		2	1	NULL
10	2015-04-01 22:09:15.0000000	79	Valve_AB001_Pressure	Temp of Motor 2322 is VERY High	0	1	60	60	1	0		4	1	NULL
11	2015-04-01 22:07:39.0000000	596	Tag_Valve_Final_Water	Chem Spil into Stream	0	1	0	1	1	0		2	1	NULL
12	2015-04-01 22:39:41.0000000	320	Motor_2322_Temp	Temp of Motor 2322 id High	1	1	95	39	1	0		2	1	NULL
13	2015-04-01 22:39:41.0000000	320	Motor_2322_Temp	Temp of Motor 2322 id High	1	1	95	95	1	0		2	1	NULL
14	2015-04-01 22:39:51.0000000	431	Valve_AB001_Pressure	Temp of Motor 2322 is VERY High	1	1	91	91	1	0		4	1	NULL

Query executed successfully. | WH4-PC (10.0 RTM) | wh4-PC\wh4 (56) | master | 00:00:00 | 63 rows

LAB – SQL Server 2008

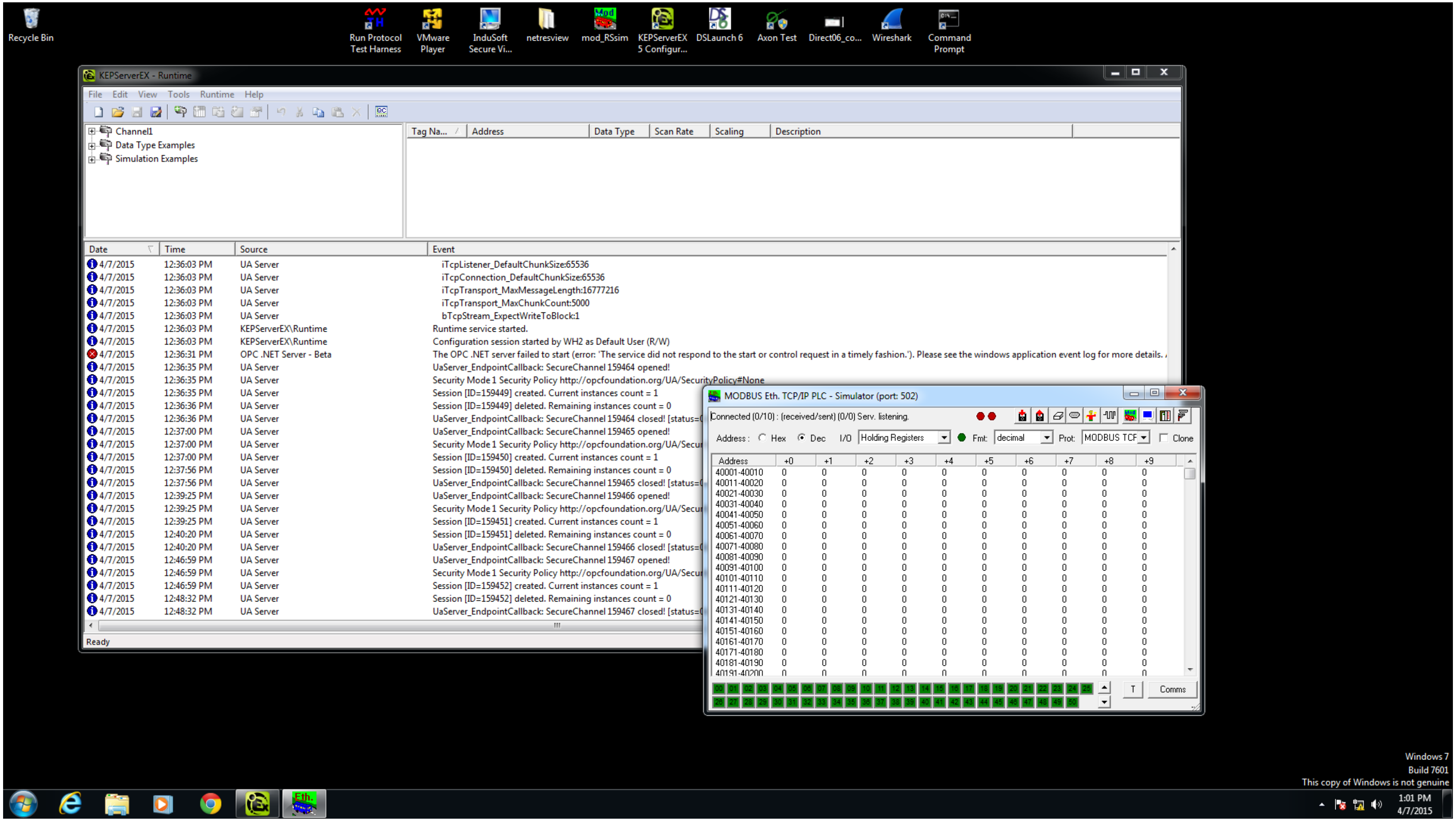


```sql
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP 1000 [Ev_Type]
      ,[Ev_Time]
      ,[Ev_Time_ms]
      ,[Ev_Info]
      ,[Ev_User]
      ,[Ev_User_Full]
      ,[Ev_Message]
      ,[Ev_Value]
      ,[Ev_Prev_Value]
      ,[Ev_Station]
      ,[Ev_Comment]
      ,[Ev_Source]
      ,[Ev_Deleted]
      ,[Last_Update]
      ,[Last_Update_ms]
  FROM [KAT_EC].[dbo].[EVENTHISTORY]
```

	Ev_Type	Ev_Time	Ev_Time_ms	Ev_Info	Ev_User	Ev_User_Full	Ev_Message	Ev_Value	Ev_Prev_Value	Ev_Station	Ev_Comment	Ev_Source	Ev_Deleted	Last_Update	Last_Up
1	6	2015-04-01 22:39:57.0000000	899		Guest		Exception in Driver 'DNP' :: DrvClose			WH5-PC			0	NULL	NULL
2	6	2015-04-01 22:39:58.0000000	10		Guest		Exception in Driver 'DNP' :: DrvClose			WH5-PC			0	NULL	NULL
3	6	2015-04-01 22:43:06.0000000	184		Guest		RunGlobalProcedureOnServer: Runtime Error => Pro...			WH5-PC			0	NULL	NULL
4	6	2015-04-01 22:43:13.0000000	249		Guest		RunGlobalProcedureOnServer: Runtime Error => Pro...			WH5-PC			0	NULL	NULL
5	6	2015-04-01 22:43:57.0000000	241		Guest		RunGlobalProcedureOnServer: Runtime Error => Pro...			WH5-PC			0	NULL	NULL
6	6	2015-04-01 22:44:14.0000000	880		Guest		Exception in Driver 'DNP' :: DrvClose			WH5-PC			0	NULL	NULL
7	6	2015-04-01 22:44:14.0000000	995		Guest		Exception in Driver 'DNP' :: DrvClose			WH5-PC			0	NULL	NULL
8	6	2015-04-01 22:44:56.0000000	397		Guest		Exception in Driver 'DNP' :: DrvClose			WH5-PC			0	NULL	NULL
9	6	2015-04-01 22:44:56.0000000	517		Guest		Exception in Driver 'DNP' :: DrvClose			WH5-PC			0	NULL	NULL
10	6	2015-04-01 22:48:04.0000000	531		Guest		Exception in Driver 'DNP' :: DrvClose			WH5-PC			0	NULL	NULL
11	6	2015-04-01 22:48:04.0000000	651		Guest		Exception in Driver 'DNP' :: DrvClose			WH5-PC			0	NULL	NULL
12	6	2015-04-01 22:48:44.0000000	757		Guest		Exception in Driver 'DNP' :: DrvClose			WH5-PC			0	NULL	NULL
13	6	2015-04-01 22:48:44.0000000	877		Guest		Exception in Driver 'DNP' :: DrvClose			WH5-PC			0	NULL	NULL
14	6	2015-04-01 22:49:34.0000000	533		Guest		RunGlobalProcedureOnServer: Runtime Error => Pro...			WH5-PC			0	NULL	NULL
15	6	2015-04-01 22:50:48.0000000	54		Guest		RunGlobalProcedureOnServer: Runtime Error => Pro...			WH5-PC			0	NULL	NULL
16	6	2015-04-01 22:51:03.0000000	839		Guest		Exception in Driver 'DNP' :: DrvClose			WH5-PC			0	NULL	NULL
17	6	2015-04-01 22:51:03.0000000	958		Guest		Exception in Driver 'DNP' :: DrvClose			WH5-PC			0	NULL	NULL

```
Query executed successfully.   WH4-PC (10.0 RTM) | wh4-PC\wh4 (53) | master | 00:00:00 | 44 rows
```

LAB – Simulators MODBUS and OPC



```
Date        Time         Source                 Event
4/7/2015    12:36:03 PM  UA Server                iTcpListener_DefaultChunkSize:65536
4/7/2015    12:36:03 PM  UA Server                iTcpConnection_DefaultChunkSize:65536
4/7/2015    12:36:03 PM  UA Server                iTcpTransport_MaxMessageLength:16777216
4/7/2015    12:36:03 PM  UA Server                iTcpTransport_MaxChunkCount:5000
4/7/2015    12:36:03 PM  UA Server                bTcpStream_ExpectWriteToBlock:1
4/7/2015    12:36:03 PM  KEPServerEX\Runtime    Runtime service started.
4/7/2015    12:36:03 PM  KEPServerEX\Runtime    Configuration session started by WH2 as Default User (R/W)
4/7/2015    12:36:31 PM  OPC .NET Server - Beta The OPC .NET server failed to start (error: 'The service did not respond to the start or control request in a timely fashion.'). Please see the windows application event log for more details.
4/7/2015    12:36:35 PM  UA Server              UaServer_EndpointCallback: SecureChannel 159464 opened!
4/7/2015    12:36:35 PM  UA Server              Security Mode 1 Security Policy http://opcfoundation.org/UA/SecurityPolicy#None
4/7/2015    12:36:35 PM  UA Server              Session [ID=159449] created. Current instances count = 1
4/7/2015    12:36:36 PM  UA Server              Session [ID=159449] deleted. Remaining instances count = 0
4/7/2015    12:36:36 PM  UA Server              UaServer_EndpointCallback: SecureChannel 159464 closed! [status=(
4/7/2015    12:37:00 PM  UA Server              UaServer_EndpointCallback: SecureChannel 159465 opened!
4/7/2015    12:37:00 PM  UA Server              Security Mode 1 Security Policy http://opcfoundation.org/UA/Secu
4/7/2015    12:37:00 PM  UA Server              Session [ID=159450] created. Current instances count = 1
4/7/2015    12:37:56 PM  UA Server              Session [ID=159450] deleted. Remaining instances count = 0
4/7/2015    12:37:56 PM  UA Server              UaServer_EndpointCallback: SecureChannel 159465 closed! [status=(
4/7/2015    12:39:25 PM  UA Server              UaServer_EndpointCallback: SecureChannel 159466 opened!
4/7/2015    12:39:25 PM  UA Server              Security Mode 1 Security Policy http://opcfoundation.org/UA/Secu
4/7/2015    12:39:25 PM  UA Server              Session [ID=159451] created. Current instances count = 1
4/7/2015    12:40:20 PM  UA Server              Session [ID=159451] deleted. Remaining instances count = 0
4/7/2015    12:40:20 PM  UA Server              UaServer_EndpointCallback: SecureChannel 159466 closed! [status=(
4/7/2015    12:46:59 PM  UA Server              UaServer_EndpointCallback: SecureChannel 159467 opened!
4/7/2015    12:46:59 PM  UA Server              Security Mode 1 Security Policy http://opcfoundation.org/UA/Secu
4/7/2015    12:46:59 PM  UA Server              Session [ID=159452] created. Current instances count = 1
4/7/2015    12:48:32 PM  UA Server              Session [ID=159452] deleted. Remaining instances count = 0
4/7/2015    12:48:32 PM  UA Server              UaServer_EndpointCallback: SecureChannel 159467 closed! [status=(
```

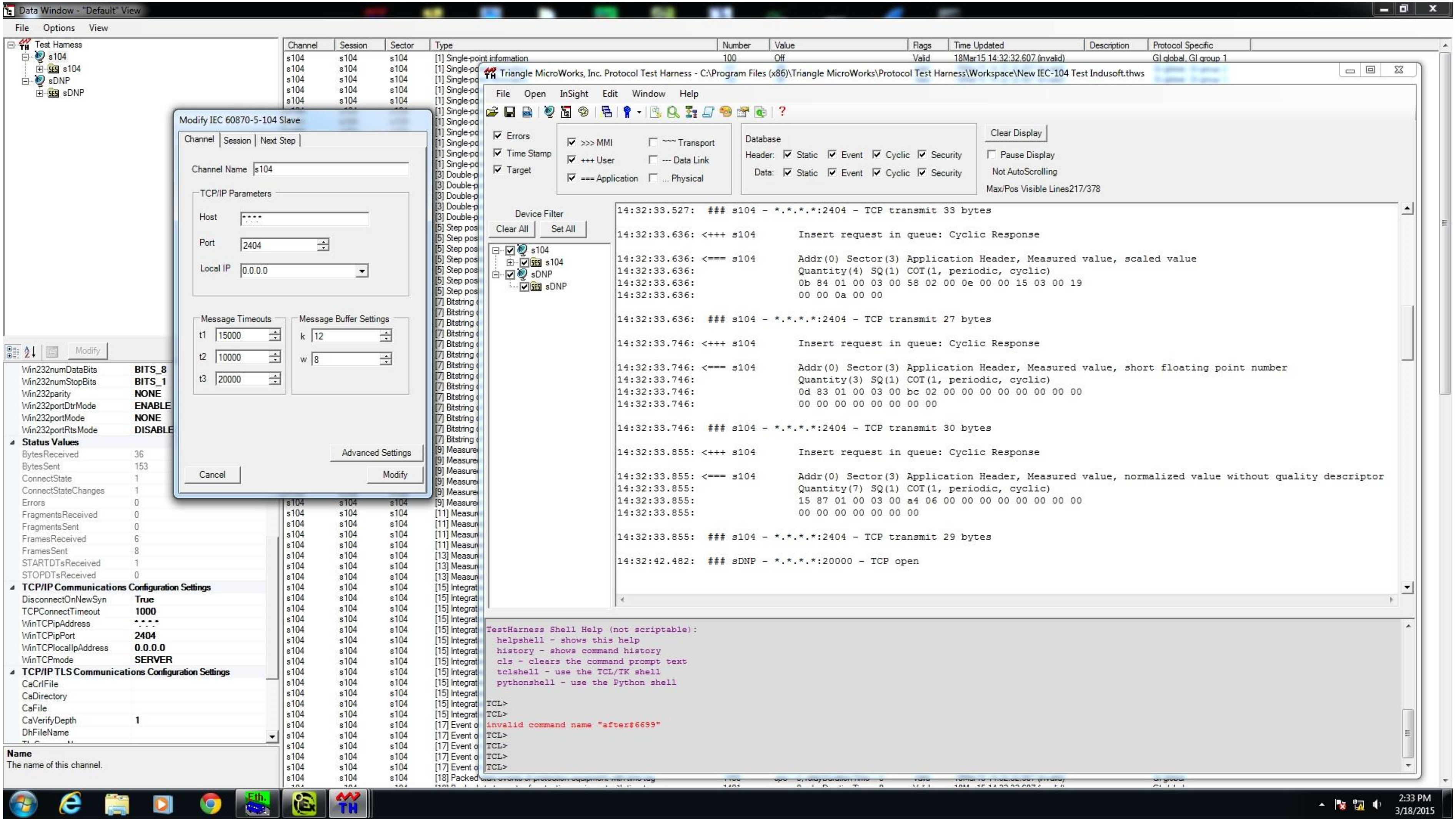
MODBUS Eth. TCP/IP PLC - Simulator (port: 502)

Connected (0/10) : (received/sent) (0/0) Serv. listening.

Address : ○ Hex ● Dec I/O Holding Registers ● Fmt: decimal Prot: MODBUS TCF □ Clone

Address	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
40001-40010	0	0	0	0	0	0	0	0	0	0
40011-40020	0	0	0	0	0	0	0	0	0	0
40021-40030	0	0	0	0	0	0	0	0	0	0
40031-40040	0	0	0	0	0	0	0	0	0	0
40041-40050	0	0	0	0	0	0	0	0	0	0
40051-40060	0	0	0	0	0	0	0	0	0	0
40061-40070	0	0	0	0	0	0	0	0	0	0
40071-40080	0	0	0	0	0	0	0	0	0	0
40081-40090	0	0	0	0	0	0	0	0	0	0
40091-40100	0	0	0	0	0	0	0	0	0	0
40101-40110	0	0	0	0	0	0	0	0	0	0
40111-40120	0	0	0	0	0	0	0	0	0	0
40121-40130	0	0	0	0	0	0	0	0	0	0
40131-40140	0	0	0	0	0	0	0	0	0	0
40141-40150	0	0	0	0	0	0	0	0	0	0
40151-40160	0	0	0	0	0	0	0	0	0	0
40161-40170	0	0	0	0	0	0	0	0	0	0
40171-40180	0	0	0	0	0	0	0	0	0	0
40181-40190	0	0	0	0	0	0	0	0	0	0
40191-40200	0	0	0	0	0	0	0	0	0	0

LAB – Simulators DNP and IE104 contd.



Data Window - "Default" View
File Options View
Test Harness
s104
s104
sDNP
sDNP
Triangle MicroWorks, Inc. Protocol Test Harness - C:\Program Files (x86)\Triangle MicroWorks\Protocol Test Harness\Workspace\New IEC-104 Test Indusoft.thws
File Open InSight Edit Window Help
Device Filter
Clear All
Set All
Clear Display
Modify IEC 60870-5-104 Slave
Channel
Session
Next Step
Advanced Settings
Cancel
Modify

Channel	Session	Sector	Type	Number	Value	Flags	Time Updated	Description	Protocol Specific
s104	s104	s104	[1] Single-point information	100	Off	Valid	18Mar15 14:32:32.607 (invalid)		GI global, GI group 1

Channel Name: s104

TCP/IP Parameters
Host: *.*.*.*
Port: 2404
Local IP: 0.0.0.0

Message Timeouts
t1: 15000
t2: 10000
t3: 20000

Message Buffer Settings
k: 12
w: 8

☑ Errors
☑ Time Stamp
☑ Target

☑ >>> MMI
☑ +++ User
☑ === Application
☐ ~~~ Transport
☐ --- Data Link
☐ ... Physical

Database
Header: ☑ Static ☑ Event ☑ Cyclic ☑ Security
Data: ☑ Static ☑ Event ☑ Cyclic ☑ Security

☐ Pause Display
Not AutoScrolling
Max/Pos Visible Lines217/378

```
14:32:33.527:  ### s104 - *.*.*.*:2404 - TCP transmit 33 bytes

14:32:33.636: <+++ s104       Insert request in queue: Cyclic Response

14:32:33.636: <=== s104       Addr(0) Sector(3) Application Header, Measured value, scaled value
14:32:33.636:                 Quantity(4) SQ(1) COT(1, periodic, cyclic)
14:32:33.636:                 0b 84 01 00 03 00 58 02 00 0e 00 00 15 03 00 19
14:32:33.636:                 00 00 0a 00 00

14:32:33.636:  ### s104 - *.*.*.*:2404 - TCP transmit 27 bytes

14:32:33.746: <+++ s104       Insert request in queue: Cyclic Response

14:32:33.746: <=== s104       Addr(0) Sector(3) Application Header, Measured value, short floating point number
14:32:33.746:                 Quantity(3) SQ(1) COT(1, periodic, cyclic)
14:32:33.746:                 0d 83 01 00 03 00 bc 02 00 00 00 00 00 00 00 00
14:32:33.746:                 00 00 00 00 00 00 00 00

14:32:33.746:  ### s104 - *.*.*.*:2404 - TCP transmit 30 bytes

14:32:33.855: <+++ s104       Insert request in queue: Cyclic Response

14:32:33.855: <=== s104       Addr(0) Sector(3) Application Header, Measured value, normalized value without quality descriptor
14:32:33.855:                 Quantity(7) SQ(1) COT(1, periodic, cyclic)
14:32:33.855:                 15 87 01 00 03 00 a4 06 00 00 00 00 00 00 00 00
14:32:33.855:                 00 00 00 00 00 00 00

14:32:33.855:  ### s104 - *.*.*.*:2404 - TCP transmit 29 bytes

14:32:42.482:  ### sDNP - *.*.*.*:20000 - TCP open
```

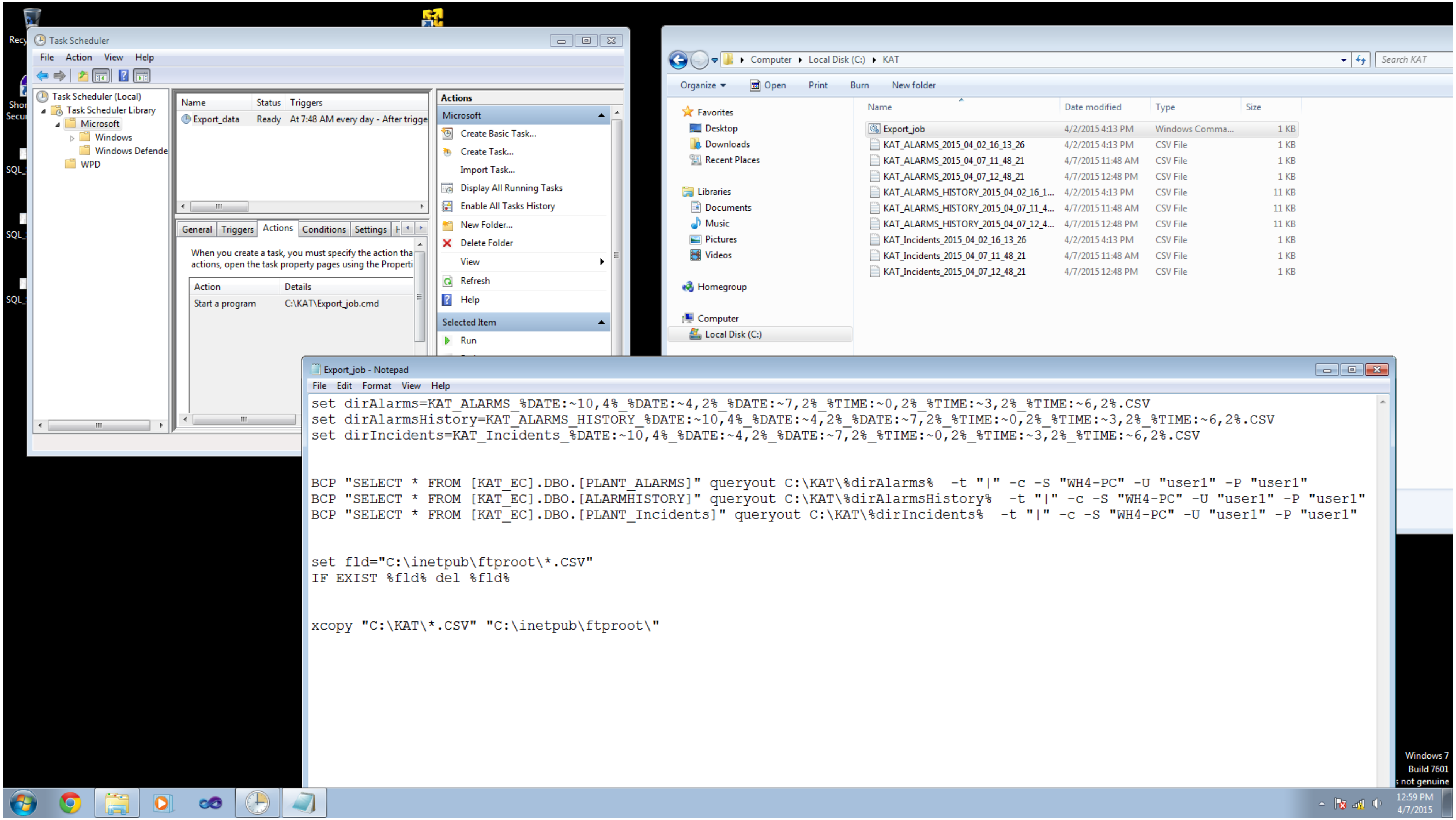
```
TestHarness Shell Help (not scriptable):
  helpshell - shows this help
  history - shows command history
  cls - clears the command prompt text
  tclshell - use the TCL/TK shell
  pythonshell - use the Python shell

TCL>
TCL>
invalid command name "after#6699"
TCL>
TCL>
TCL>
TCL>
```

Win232numDataBits	BITS_8
Win232numStopBits	BITS_1
Win232parity	NONE
Win232portDtrMode	ENABLE
Win232portMode	NONE
Win232portRtsMode	DISABLE
Status Values	
BytesReceived	36
BytesSent	153
ConnectState	1
ConnectStateChanges	1
Errors	0
FragmentsReceived	0
FragmentsSent	0
FramesReceived	6
FramesSent	8
STARTDTsReceived	1
STOPDTsReceived	0
TCP/IP Communications Configuration Settings	
DisconnectOnNewSyn	True
TCPConnectTimeout	1000
WinTCPipAddress	*.*.*.*
WinTCPipPort	2404
WinTCPlocalIpAddress	0.0.0.0
WinTCPmode	SERVER
TCP/IP TLS Communications Configuration Settings	
CaCrlFile	
CaDirectory	
CaFile	
CaVerifyDepth	1
DhFileName	

Name
The name of this channel.

2:33 PM
3/18/2015

LAB – Batch FTP Jobs



Name	Status	Triggers
Export_data	Ready	At 7:48 AM every day - After trigge

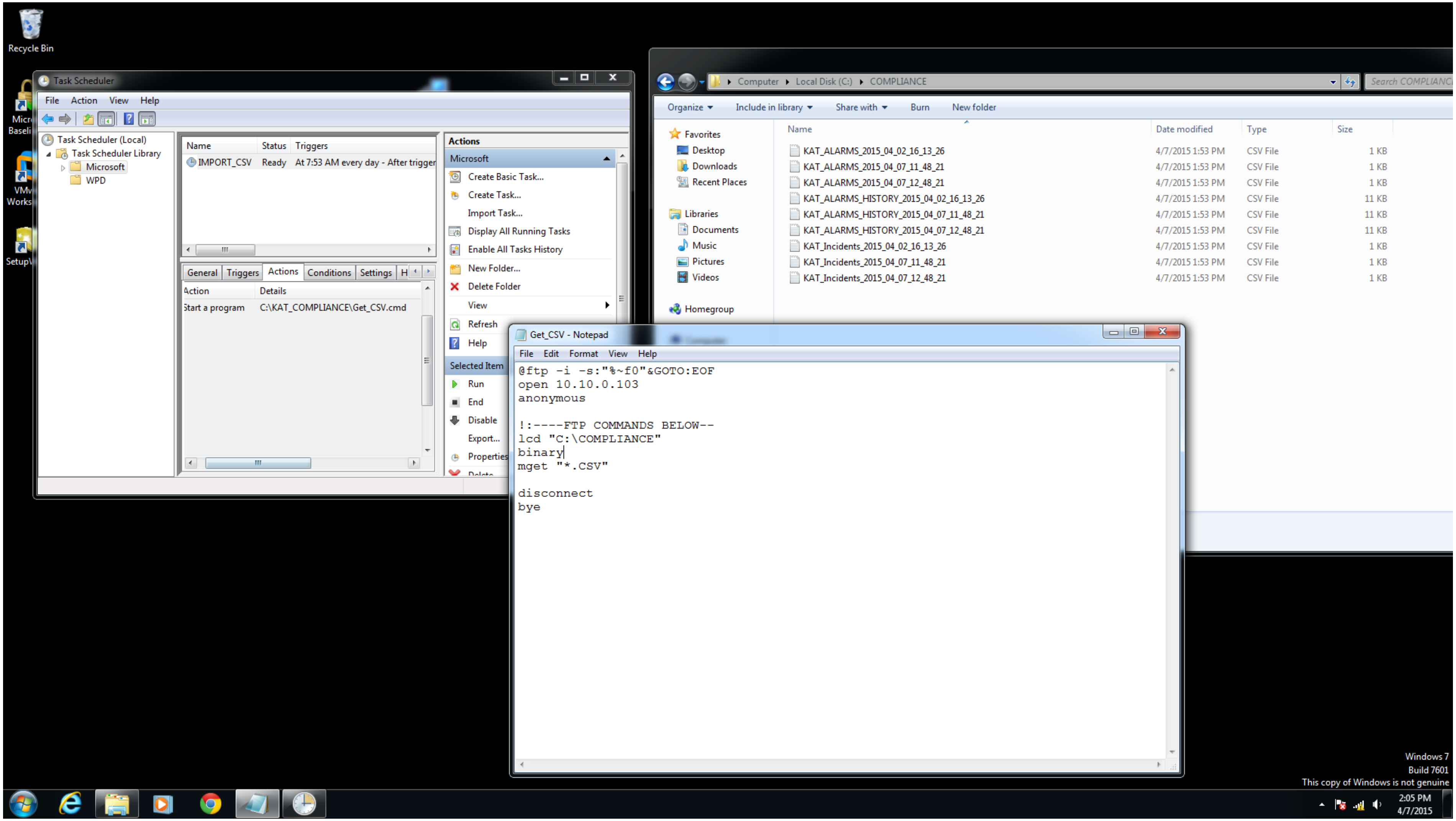
When you create a task, you must specify the action tha
actions, open the task property pages using the Properti

Action	Details
Start a program	C:\KAT\Export_job.cmd

Name	Date modified	Type	Size
Export_job	4/2/2015 4:13 PM	Windows Comma...	1 KB
KAT_ALARMS_2015_04_02_16_13_26	4/2/2015 4:13 PM	CSV File	1 KB
KAT_ALARMS_2015_04_07_11_48_21	4/7/2015 11:48 AM	CSV File	1 KB
KAT_ALARMS_2015_04_07_12_48_21	4/7/2015 12:48 PM	CSV File	1 KB
KAT_ALARMS_HISTORY_2015_04_02_16_1...	4/2/2015 4:13 PM	CSV File	11 KB
KAT_ALARMS_HISTORY_2015_04_07_11_4...	4/7/2015 11:48 AM	CSV File	11 KB
KAT_ALARMS_HISTORY_2015_04_07_12_4...	4/7/2015 12:48 PM	CSV File	11 KB
KAT_Incidents_2015_04_02_16_13_26	4/2/2015 4:13 PM	CSV File	1 KB
KAT_Incidents_2015_04_07_11_48_21	4/7/2015 11:48 AM	CSV File	1 KB
KAT_Incidents_2015_04_07_12_48_21	4/7/2015 12:48 PM	CSV File	1 KB

```
set dirAlarms=KAT_ALARMS_%DATE:~10,4%_%DATE:~4,2%_%DATE:~7,2%_%TIME:~0,2%_%TIME:~3,2%_%TIME:~6,2%.CSV
set dirAlarmsHistory=KAT_ALARMS_HISTORY_%DATE:~10,4%_%DATE:~4,2%_%DATE:~7,2%_%TIME:~0,2%_%TIME:~3,2%_%TIME:~6,2%.CSV
set dirIncidents=KAT_Incidents_%DATE:~10,4%_%DATE:~4,2%_%DATE:~7,2%_%TIME:~0,2%_%TIME:~3,2%_%TIME:~6,2%.CSV


BCP "SELECT * FROM [KAT_EC].DBO.[PLANT_ALARMS]" queryout C:\KAT\%dirAlarms%  -t "|" -c -S "WH4-PC" -U "user1" -P "user1"
BCP "SELECT * FROM [KAT_EC].DBO.[ALARMHISTORY]" queryout C:\KAT\%dirAlarmsHistory%  -t "|" -c -S "WH4-PC" -U "user1" -P "user1"
BCP "SELECT * FROM [KAT_EC].DBO.[PLANT_Incidents]" queryout C:\KAT\%dirIncidents%  -t "|" -c -S "WH4-PC" -U "user1" -P "user1"


set fld="C:\inetpub\ftproot\*.CSV"
IF EXIST %fld% del %fld%


xcopy "C:\KAT\*.CSV" "C:\inetpub\ftproot\"
```

LAB – FTP Destination Screen



Name	Status	Triggers
IMPORT_CSV	Ready	At 7:53 AM every day - After trigger

Action	Details
Start a program	C:\KAT_COMPLIANCE\Get_CSV.cmd

Name	Date modified	Type	Size
KAT_ALARMS_2015_04_02_16_13_26	4/7/2015 1:53 PM	CSV File	1 KB
KAT_ALARMS_2015_04_07_11_48_21	4/7/2015 1:53 PM	CSV File	1 KB
KAT_ALARMS_2015_04_07_12_48_21	4/7/2015 1:53 PM	CSV File	1 KB
KAT_ALARMS_HISTORY_2015_04_02_16_13_26	4/7/2015 1:53 PM	CSV File	11 KB
KAT_ALARMS_HISTORY_2015_04_07_11_48_21	4/7/2015 1:53 PM	CSV File	11 KB
KAT_ALARMS_HISTORY_2015_04_07_12_48_21	4/7/2015 1:53 PM	CSV File	11 KB
KAT_Incidents_2015_04_02_16_13_26	4/7/2015 1:53 PM	CSV File	1 KB
KAT_Incidents_2015_04_07_11_48_21	4/7/2015 1:53 PM	CSV File	1 KB
KAT_Incidents_2015_04_07_12_48_21	4/7/2015 1:53 PM	CSV File	1 KB

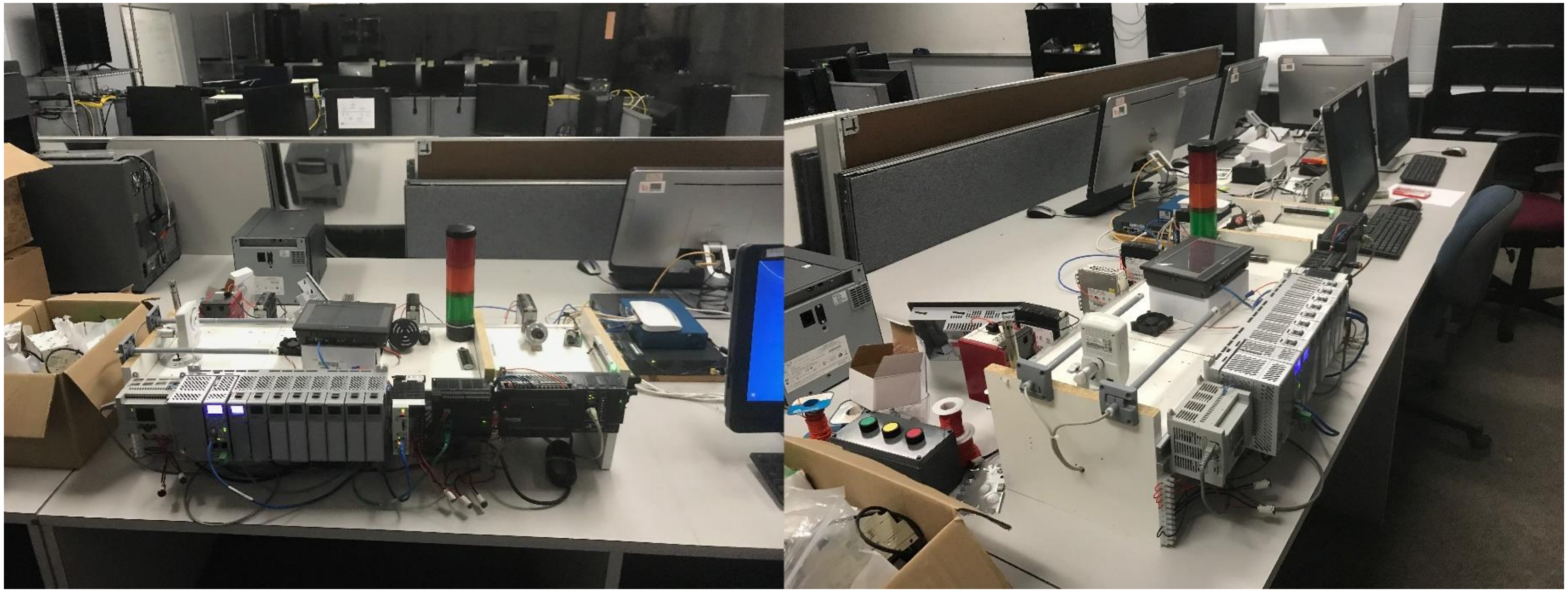
```
@ftp -i -s:"%~f0"&GOTO:EOF
open 10.10.0.103
anonymous

!:----FTP COMMANDS BELOW--
lcd "C:\COMPLIANCE"
binary
mget "*.CSV"

disconnect
bye
```

LAB – Completed Deliverables

1. Functional and Operational LAB for SCADA research
2. Implementation of top **5** Oil & Gas Industry SCADA network protocols (MODBUS/TCP-IP, KOYO-ECOM, ARTI, OPC, DNP3, IE104) in the lab
3. Demonstrate the ability to use vulnerability, penetration testing and forensic tools
4. Documentation for Lab maintenance
5. Define a course material/lab exercises for students interested in SCADA vulnerability assessments, SCADA penetration-testing and SCADA forensics

LAB – Lab Then and Now!

Budget of $50 in 4 months with vendor donated industrial hardware



Now .. after an external Grant

Q&A