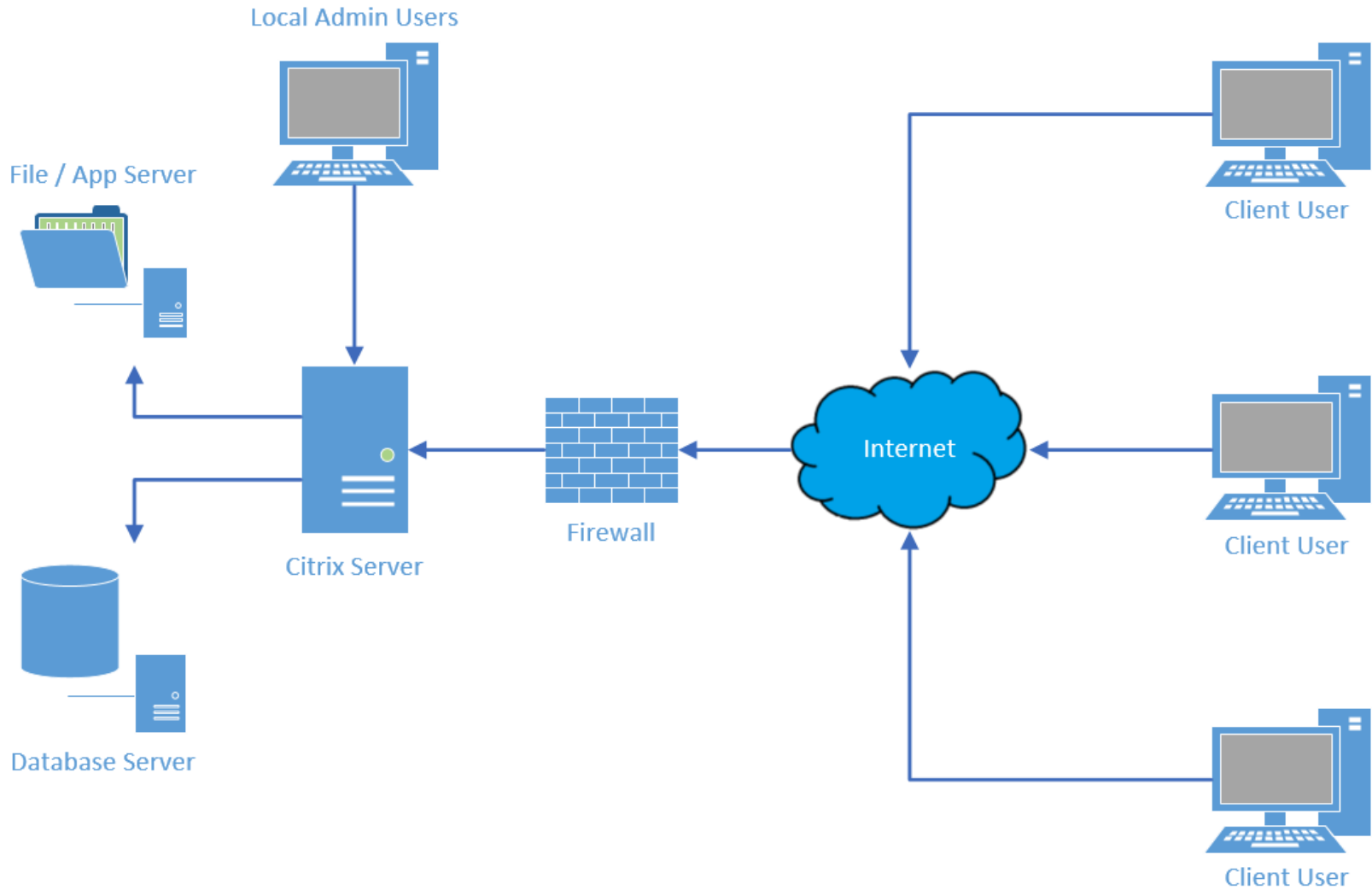




Engineering Analysis, Intelligent Solutions

SMARTPLANT INSTRUMENTATION (SPI) THIN CLIENT CYBERSECURITY Citrix Implementation

Basic Thin Client Environment



Associated Documents (intools.ini)

SmartPlant Instrumentation - PROMO_A (As-Built)

File Modules Edit Actions SmartPlant Tools Window Help

Close Gaurita R... EDE Index Specific... Wiring Process Di... Calculation Loop Diag... Hook-Up... Calibration Maintenance ODP Document... Help

Domain Explorer

Browser Manager Browser View - New 0056, Diff. Pressure Instr.

Tag Number	Manufacturer	Model	P&ID No.	General Service	Notes	Process Fluid	Max. Pressure	Oper. Pressure
P1 FT 0058	YOKOGAWA	EJA110A-EMS-4G-93CDN/FU	PLX-PID-P1-0009	NATURAL GAS FROM P1-111	A permanent SS nameplNatural Gas (Methane)			616
P1 FT 0504	"	"	PLX-PID-P1-0001	NATURAL GAS PURGE TO F				
P1 FT 0001 A	YOKOGAWA	EJA110A-EMS-4B-9CINN/FU	PLX-PID-P1-0004	P1-108-D ZINC OXIDE GUA 1	A permanent SS nameplNatural Gas			550
P1 FT 0001 B	YOKOGAWA	EJA110A-EMS-4B-9CINN/FU	PLX-PID-P1-0004	P1-108-D ZINC OXIDE GUA 1	A permanent SS nameplNatural Gas			550
P1 FT 0001 C	YOKOGAWA	EJA110A-EMS-4B-9CINN/FU	PLX-PID-P1-0004	P1-108-D ZINC OXIDE GUA 1	A permanent SS nameplNatural Gas			550
P1 FT 0001 D	"	"	PLX-PID-P1-0001	FEED GAS TO AMMONIA #:				
P1 FT 0002 A	"	"	PLX-PID-P1-0005	S45# STEAM TO MIXED FEE				
P1 FT 0002 B	"	"	"	"				
P1 FT 0002 C	"	"	"	"				
P1 FT 0003 A	"	"	"	"				
P1 FT 0003 B	"	"	"	"				
P1 FT 0003 C	"	"	"	"				
P1 FT 0004	"	"	"	"				
P1 FT 0005 A	"	"	"	"				
P1 FT 0005 B	"	"	"	"				
P1 FT 0031	"	"	"	"				
P1 FT 0032	"	"	"	"				
P1 FT 0040	"	"	"	"				
P1 FT 0051	"	"	"	"				
P1 FT 0053	"	"	"	"				
P1 FT 0057	"	"	"	"				
P1 FT 0057 A	"	"	"	"				
P1 FT 0063 A	"	"	"	"				
P1 FT 0063 B	"	"	"	"				
P1 FT 0064	"	"	"	"				
P1 FT 0074	"	"	"	"				
P1 FT 0108	"	"	"	"				
P1 FT 0117	"	"	"	"				
P1 FT 0140	"	"	"	"				
P1 FT 0140 A	"	"	"	"				
P1 FT 0140 B	"	"	"	"				
P1 FT 0140 C	"	"	"	"				
P1 FT 0209	"	"	"	"				
P1 FT 0212	"	"	"	"				
P1 FT 0229	"	"	"	"				
P1 FT 0341	"	"	"	"				

Associated Documents

Global path:
C:\Windows\Temp

Tag number:
P1 FT 0140 A

Document	Description	Location
dbprofilmanager.exe	DB Profile Manager	C:\Program Files (x86)\SmartPlant\
dbsetup.exe	DBSetup	C:\Program Files (x86)\SmartPlant\
import.exe	Import Module	C:\Program Files (x86)\SmartPlant\
intools.ini	Configuration File	C:\Program Files (x86)\SmartPlant\
main.exe	Admin Module	C:\Program Files (x86)\SmartPlant\

Associate...
Dissociate...
Open

intools.ini - Notepad

```

File Edit Format View Help
[DATABASE]
AUTOCOMMIT=0
COMMIT=100
CONTINUE=N
DATABASE=PROMO
DATABASEPASSWORD=
DBMS=MSS
DBPARAM=CONNECTSTRING='DSN=PROMO;UID=SPI_DBAMN_PROMO;PWD=██████████',PBCATALOGOWNER='SPI_DBAMN_PROMO',DISABLEBIND=1
DSN=PROMO
LOCK=RU
LOGID=██████████
LOGPASSWORD=██████████
MSS=2014
PROMPT=110
SECURITYSCHEMAPASSWORD=██████████
SERVERNAME=██████████
STAYCONNECTED=1
    
```

Domain Explorer

Items

- P1 FE 0140
- P1 FT 0140 A
- P1 FT 0140 B
- P1 FT 0140 C
- P1 FV 0140
- P1 FY 0140
- P1 FY 0140 A
- P1 FY 0140 B
- P1 FY 0140 C

Associated Documents (Main.exe)

SmartPlant Instrumentation - PROMO_A (As-Built)

File Modules Edit Actions SmartPlant Tools Window Help

Close Generate R... EDE Index Specificati... Wiring Process Da... Calculation Loop Dvgs Hook-Ups Calibration Maintenance DDP Document...

Domain Explorer

Browser Manager Browser View - New 0056,Diff. Pressure Instr.

Tag Number	Manufacturer	Model	P&ID No.	General Service	Notes:	Process Fluid	Max. Pressure
P1 FT 0058	YOKOGAWA	EJX110A-EMS4G-93CDN/FL	PLX-PID-P1-0009	NATURAL GAS FROM P1-171. A permanent SS nameplate	Natural Gas (Methane)		61
P1 FT 0504	*	*	PLX-PID-P1-0001	NATURAL GAS PURGE TO F			
P1 FT 0001 A	YOKOGAWA	EJA110A-EMS4B-9CINN/FU	PLX-PID-P1-0004	P1-108-D ZINC OXIDE GUA 1. A permanent SS nameplate	Natural Gas		55
P1 FT 0001 B	YOKOGAWA	EJA110A-EMS4B-9CINN/FU	PLX-PID-P1-0004	P1-108-D ZINC OXIDE GUA 1. A permanent SS nameplate	Natural Gas		55
P1 FT 0001 C				Permanent SS nameplate	Natural Gas		55
P1 FT 0001 D							
P1 FT 0002 A							
P1 FT 0002 B							
P1 FT 0002 C							
P1 FT 0003 A							
P1 FT 0003 B							
P1 FT 0003 C							
P1 FT 0004							
P1 FT 0005 A							
P1 FT 0005 B							
P1 FT 0031							
P1 FT 0032							
P1 FT 0040							
P1 FT 0051							
P1 FT 0053							
P1 FT 0057							
P1 FT 0057 A							
P1 FT 0063							
P1 FT 0063 A							
P1 FT 0063 B							
P1 FT 0064							
P1 FT 0064 A							
P1 FT 0064 B							
P1 FT 0074							
P1 FT 0074 A							
P1 FT 0108							
P1 FT 0108 A							
P1 FT 0108 B							
P1 FT 0108 C							
P1 FT 0117							
P1 FT 0117 A							
P1 FT 0140							
P1 FT 0140 A							
P1 FT 0140 B							
P1 FT 0140 C							
P1 FV 0140							
P1 FY 0140							
P1 FY 0140 A							
P1 FY 0140 B							
P1 FY 0140 C							
P1 FE 0140							
P1 FE 0140 A							
P1 FE 0140 B							
P1 FE 0140 C							
P1 FT 0209							
P1 FT 0212							
P1 FT 0229							
P1 FT 0341	YOKOGAWA						

Associated Documents

Global path:
C:\Windows\Temp

Tag number:
P1 FT 0140 A

Document	Description	Location
dbprofilemanager.exe	DB Profile Manager	C:\Program Files (x86)\SmartPlant\I...
dbsetup.exe	DBSetup	C:\Program Files (x86)\SmartPlant\I...
import.exe	Import Module	C:\Program Files (x86)\SmartPlant\I...
intools.ini	Configuration File	C:\Program Files (x86)\SmartPlant\I...
main.exe	Admin Module	C:\Program Files (x86)\SmartPlant\I...
intsetup.exe		
regedit.exe		
EXCEL.EXE		
WINWORD.EXE		
cmd.exe		

Associate...
Dissociate...
Open

Domain Administration - PROMO_A

File Options Activities Reports Tools Add-Ins DBA SmartPlant Window Help

Close Domain Project Owner Nam. Conv. Explorer User-Defin... Help

Domain Definition

Domain: PROMO_A

Number:

Description:

Administrator: DBA

Domain schema name: PROMO_A

Plant hierarchy separator:

Domain type

Engineering company
 Owner operator
 Exclusive claim mode

Domain usage: None

Domain features

Activity tracking
 Audit trail options
 Cable type dependency
 Single mode
 Default plant use
 KKS mode

Workflow

Instrumentation and process data: None

Specification title block

Custom title block assignment method: Special (used in Specifications module c...

Items

- P1 FE 0140
- P1 FT 0140 A
- P1 FT 0140 B
- P1 FT 0140 C
- P1 FV 0140
- P1 FY 0140
- P1 FY 0140 A
- P1 FY 0140 B
- P1 FY 0140 C

Associated Documents (Regedit.exe)

SmartPlant Instrumentation - PROMO_A (As-Built)

The screenshot displays the SmartPlant Instrumentation interface. On the left, the 'Domain Explorer' shows a tree view of instrument tags. The main window contains a table of instrument data. A dialog box titled 'Associated Documents' is open, showing a list of documents associated with the selected tag. The 'Registry Editor' is also open, showing the 'HKEY_LOCAL_MACHINE' tree.

Tag Number	Manufacturer	Model	P&ID No.	General Service	Notes:	Process Fluid	Max. Pressure
P1 FIT 0058	YOKOGAWA	EJX110A-EMS4G-93CDN/FU	PLX-PID-P1-0009	NATURAL GAS FROM P1-17	1. A permanent SS namepl	Natural Gas (Methane)	
P1 FIT 0504	*	*	PLX-PID-P1-0001	NATURAL GAS PURGE TO F			
P1 FT 0001 A	YOKOGAWA	EJA110A-EMS4B-9CNN/FU	PLX-PID-P1-0004	P1-108-D ZINC OXIDE GUA	1. A permanent SS namepl	Natural Gas	
P1 FT 0001 B	YOKOGAWA	EJA110A-EMS4B-9CNN/FU	PLX-PID-P1-0004	P1-108-D ZINC OXIDE GUA	1. A permanent SS namepl	Natural Gas	
P1 FT 0001 C					inent SS namepl	Natural Gas	
P1 FT 0001 D							
P1 FT 0002 A							
P1 FT 0002 B							
P1 FT 0002 C							
P1 FT 0003 A							
P1 FT 0003 B							
P1 FT 0003 C							
P1 FT 0004							
P1 FT 0005 A							
P1 FT 0005 B							
P1 FT 0031							
P1 FT 0032							
P1 FT 0040							
P1 FT 0051							
P1 FT 0053							
P1 FT 0057							
P1 FT 0057 A							
P1 FT 0057 B							
P1 FT 0063 A							
P1 FT 0063 B							
P1 FT 0064							
P1 FT 0108							
P1 FT 0117							
P1 FT 0140							
P1 FE 0140							
P1 FT 0140 A							
P1 FT 0140 B							
P1 FT 0140 C							
P1 FT 0209							
P1 FT 0212							
P1 FT 0229							
P1 FT 0341	YOKOGAWA						

Associated Documents Dialog:

Global path: C:\Windows\Temp

Tag number: P1 FT 0140 A

Document	Description	Location
dbprofilemanager.exe	DB Profile Manager	C:\Program Files (x86)\SmartPlant\I...
dbsetup.exe	DBSetup	C:\Program Files (x86)\SmartPlant\I...
import.exe	Import Module	C:\Program Files (x86)\SmartPlant\I...
intools.ini	Configuration File	C:\Program Files (x86)\SmartPlant\I...
main.exe	Admin Module	C:\Program Files (x86)\SmartPlant\I...
intsetup.exe	Internal Setup	C:\Program Files (x86)\SmartPlant\I...
regedit.exe	Regedit	C:\Windows\regedit.exe
EXCEL.EXE		
WINWORD.EXE		
cmd.exe		

Registry Editor:

Name	Type	Data
(Default)	REG_SZ	(value not set)
Database	REG_SZ	DEMO
Driver	REG_SZ	C:\Windows\SysWOW64\sqlncli11.dll
LastUser	REG_SZ	DEMO
Server	REG_SZ	SVVDEVPROSP01\SWVDEVPROSP0101

Associated Documents (VBA)

SmartPlant Instrumentation - PROMO_A (As-Built)

File Modules Edit Actions SmartPlant Tools Window Help

Close Generate R... EDE Index Specificiti... Wiring Process Da... Calculation Loop Dwgs Hook-Ups Calibration Maintenance DDP Document ... Help

Domain Explorer

Browser Manager Browser View - New 0056,Diff. Pressure Instr.

Tag Number	Manufacturer	Model	P&ID No.	General Service	Notes:	Process Fluid
P1 FT 0058	YOKOGAWA	EJX110A-EMS4G-93CDN/FU	PLX-PID-P1-0009	NATURAL GAS FROM P1-17	1. A permanent SS nameplate	Natural Gas (Methane)
P1 FT 0504	*	*	PLX-PID-P1-0001	NATURAL GAS PURGE TO F		
P1 FT 0001 A	YOKOGAWA	EJA110A-EMS4B-9CN/FU	PLX-PID-P1-0004	P1-108-D ZINC OXIDE GUA 1.	A permanent SS nameplate	Natural Gas
P1 FT 0001 B	YOKOGAWA	EJA110A-EMS4B-9CN/FU	PLX-PID-P1-0004	P1-108-D ZINC OXIDE GUA 1.	A permanent SS nameplate	Natural Gas
P1 FT 0001 C	YOKOGAWA	EJA110A-EMS4B-9CN/FU	PLX-PID-P1-0004	P1-108-D ZINC OXIDE GUA 1.	A permanent SS nameplate	Natural Gas
P1 FT 0001 D	*	*	PLX-PID-P1-0001	FEED GAS TO AMMONIA #:		
P1 FT 0002 A	*	*	PLX-PID-P1-0005	545# STEAM TO MIXED FE		
			PLX-PID-P1-0005	545# STEAM TO MIXED FE		
			CNN/FU:PLX-PID-P1-0005	545# STEAM TO MIXED FE 1.	A permanent SS nameplate	Steam
			PLX-PID-P1-0002	P1-101-J DISCHARGE		
			CNN/FU:PLX-PID-P1-0002	P1-101-J DISCHARGE	1. A permanent SS nameplate	Air
			CNN/FU:PLX-PID-P1-0002	P1-101-J DISCHARGE	1. A permanent SS nameplate	Air
			3CNN/PLX-PID-P1-0002	P1-101-J 4TH STAGE DISCH	1. A permanent SS nameplate	Air
			B-BA03:PLX-PID-P1-0010	LEAN BENFIELD TO CO2 AE 1.	A permanent SS nameplate	Benfield
			B-BA03:PLX-PID-P1-0010	LEAN BENFIELD TO CO2 AE 1.	A permanent SS nameplate	Benfield
			PLX-PID-P1-0006	TOTAL PURGE GAS TO FUE		
			PLX-PID-P1-0005	TOTAL FUEL FROM 116-F		
			CNN/FU:PLX-PID-P1-0011	SYN GAS TO P1-103-J	1. A permanent SS nameplate	Syn Gas (H2, N2)
			CNN/FU:PLX-PID-P1-0005	STEAM TO AIR HEATER	1. A permanent SS nameplate	Steam

Associated Documents

Global path: C:\Windows\Temp

Tag number: P1 FT 0140 A

Document	Description	Location
dbprofilemanager.exe	DB Profile Manager	C:\Program Files (x86)\SmartPlant\I
dbsetup.exe	DBSetup	C:\Program Files (x86)\SmartPlant\I

Microsoft Visual Basic for Applications - Book1 - [Module1 (Code)]

File Edit View Insert Format Debug Run Tools Add-Ins Window Help

Ln 1, Col 1

Project - VBAProject

VBAPROJECT (Book1)

- Microsoft Excel Objects
 - Sheet1 (Sheet1)
 - Sheet2 (Sheet2)
 - Sheet3 (Sheet3)
 - ThisWorkbook
- Modules
 - Module1

Properties - Module1

Module1 Module

```

Sub Test ()
    Call Shell("c:\windows\System32\cmd.exe", vbNormalFocus)
End Sub
    
```

c:\windows\System32\cmd.exe - pathping www.google.com

```

[-4] [-6] target_name

Options:
-g host-list      Loose source route along host-list.
-h maximum_hops  Maximum number of hops to search for target.
-i address        Use the specified source address.
-n               Do not resolve addresses to hostnames.
-p period         Wait period milliseconds between pings.
-q num_queries    Number of queries per hop.
-w timeout        Wait timeout milliseconds for each reply.
-4               Force using IPv4.
-6               Force using IPv6.

C:\Users\blake.biernacki\Documents>pathping www.google.com

Tracing route to www.google.com [74.124.63.102]
over a maximum of 30 hops:
 0  SUUDEUPROSP101.contechnet.com [172.21.1.42]
 1  172.21.1.4
 2  172.21.1.2
 3  66.60.229.161
 4  cache.google.com [74.124.63.102]
    
```

Citrix Implementation

- 80% of companies tested exposed sensitive data.
- Most were vulnerable to arbitrary code execution.
- All issues lied on a poor implementation of Citrix and Applications.
- Some people believe that providing access only to a single application provides some measure of security. Remember, this is not the case.
- “Using the access rules we had acquired at the time, we were able to read the information, including passwords, which gave us system administrator access to every server [several hundred] in the organization. That level of access not only gave us complete control of their systems, but we could have deleted any audit trail we might have left.”

Citrix Implementation

- Advise Citrix Admins of these issues
- Ensure the system is locked down through penetration testing
- Confirm access to specific roles for users
- Use dual layer authentication
- Do not use restriction policies as a replacement for antivirus
- Have a thorough and complete understanding of your network environment

Q&A / Discussion

