PLC Data Table Misinformation
Finding Vectors for Data Manipulation

Tim Conway  
Technical Director - ICS and SCADA, SANS Institute

Jeff Shearer  
Industrial Cybersecurity Consultant, SANS Institute
Why This?

- Numerous methods via traditional IT attacks against networks, assets, or cyber enabled devices – many demos performed impacting communications

- IT / OT device targets / protocol targeting – DNP3 protocol attacks, numerous Metasploit modules, specific scan criteria, real world attacks

- Longer dwell time within target environments, understanding or mapping what normal looks like, attack with a plan – Demos across numerous ICS conferences, real world attacks
Why Now?

- Routine reports and occurrence in many geographies
- Growing but limited events occurring in specific geographies
- Nation state military events
What are the top three (3) threat vectors you are most concerned with? Rank with “First” being the threat of highest concern.

- Devices and “things” (that cannot protect themselves)... 44%
- Internal threat (accidental)
- External threats (hacktivism, nation states) 35%
- Extortion, ransomware or other financially motivated...
- Phishing scams
- Malware families spreading indiscriminately
- Integration of IT into control system networks 25%
- External threats (supply chain or partnerships)
- Internal threat (intentional)
- Industrial espionage
- Other
200+ participants
66% NA | 25% EMEA | 9% ROW

Job Role & Duties
47% have “Security” in job title
56% hold ‘hands-on’ security roles

Responsibilities
31% IT+OT | 37% IT | 27% OT
ICS COMPONENT DATA

From which *control system components are you collecting and correlating data?* Select all that apply.

- Computer assets (HMI, server, workstations) running commercial OS (Windows, UNIX, Linux)
- Network devices (firewall, switches, routers, gateways)
- Control system applications
- Remote access appliances, including modems
- Connections to the field SCADA network
- Wireless communication devices and protocols
- Physical access systems
- Plant historian
- Control system communication protocols
- Embedded controllers or components (e.g. PLCs, IEDs)
- Mobile devices
- OLE for process control (OPC)
Ukraine 2015

Remote Access

Industrial Protocols

Controllers

Instruments

IO

HMI's

ICs Files

Fieldbus

Networks

Havex Dragonfly

Actuators

Industrial Wireless

All Have Been Shown To Expose Your Operations
Data Foundations within the Purdue Model are Only as Solid as the Integrity of Data In/Out of PLC/PAC
Data Foundations within the Purdue Model are Only as Solid as the Integrity of Data In/Out of PLC/PAC
Data Foundations within the Purdue Model are Only as Solid as the Integrity of Data In/Out of PLC/PAC

The genesis of data starts here and the foundation on which data integrity is built.
But there’s a Catch……..

PLC responds to inputs. Good or bad, calibrated or not, the PLC responds however it’s programmed to respond.
PLC / PAC Simplified Internal Architecture

Permit Action Input = Electrically True

Permit Action Input

Permit Action Output

Permit Action Output = Electrically True

Code Execution Engine

Data Table

I/O

Non-I/O

Communication

PLC

Write Config PB From HMI

Move Source: New Setpoint Destination: Current Setpoint

Write Config From HMI

Action Output

Action Output

PLC / PAC Simplified Internal Architecture

1) Read Input

Move
Source: New Setpoint
Destination: Current Setpoint

Write Config PB From HMI

Permit Action Input = Electrically True

Permit Action Output = Electrically True
PLC / PAC Simplified Internal Architecture

1) Read Input
2) Update Input Image Data Table

Move
Source: New Setpoint
Destination: Current Setpoint

 Permit Action Input = Electrically True

 Permit Action Input

 Permit Action Output

 Permit Action Output = Electrically True

Code Execution Engine

Data Table

I/O

Non-I/O

Communication

PLC

Action Output

Write Config PB From HMI

Write Config From HMI

© 2018 SANS Institute
All other copyrights and trademarks are hereby recognized
PLC / PAC Simplified Internal Architecture

1) Read Input
2) Update Input Image Data Table
3) Code Executes and Determines Output Status

Permit Action Input = Electrically True
Permit Action Output = Electrically True

Code Execution Engine
Data Table
I/O
Non-I/O
Communication

Permit Action Input
Write Config PB From HMI
Move Source: New Setpoint Destination: Current Setpoint

Action Output

© 2018 SANS Institute
All other copyrights and trademarks are hereby recognized.
**PLC / PAC Simplified Internal Architecture**

1. Permit Action Input = Electrically True
   - Permit Action Input
   - Permit Action Output

2. Data Table
   - Communication
   - I/O
   - Non-I/O

3. Permit Action Input
   - Write Config PB From HMI

4. Move
   - Source: New Setpoint
   - Destination: Current Setpoint

   - Read Input
   - Update Input Image Data Table
   - Code Executes and Determines Output Status
   - Output Image Data Table Updated
PLC / PAC Simplified Internal Architecture

1) Read Input
2) Update Input Image Data Table
3) Code Executes and Determines Output Status
4) Output Image Data Table Updated
5) Output(s) Written

Permit Action Input = Electrically True
Permit Action Output = Electrically True
If you have access to the Data Table and you know how the PLC/PAC is programmed, you can affect the behavior of the PLC.
PLC / PAC Simplified Internal Architecture

Our Actual Temp is 31.5 degrees C

Output 0%

Our Setpoint is 26 degrees C. Our PID output would be off

Heat Output = Electrically False
Our Actual Temp is 18.4 degrees C

Our Setpoint is 26 degrees C. Our PID output would be on

1) Skeletor or Jeff changes the Engineering High Span Value
2) Actual Temperature drops due to span change
3) Actual Temp is less than Setpoint
4) PID Calculates “On” %
5) Output(s) Written

Heat Output = Electrically True
PLC / PAC Simplified Internal Architecture

The idea is it looks and behaves like normal operation.

![Diagram showing PLC and PAC architecture with various components like Code Execution Engine, Data Table, I/O, Non-I/O, Communication, and a control panel showing temperature and setpoint values.]

- Our Actual Temp is 18.4 degrees C
- Our Setpoint is 26 degrees C. Our PID output would be on
- Heat Output = Electrically True
- No Alarms
- Output 100%

The idea is that it looks like normal operation.
PLC / PAC Simplified Internal Architecture

Permit Action Input = Electrically True
- Permit Action Input

Data Table
- I/O
- Non-I/O

Communications
- PLC

Code Execution Engine
- Permit Action Input

Move Source: New Setpoint
Destination: Current Setpoint
- Write Config PB From HMI
- Write Config From HMI

Action Output
- From PLC

You could change the program but that is more “expected”. It’s much harder to track data changes.
If the PLC is the Castle, where are the holes in the castle wall?

- Code Execution Engine
- Data Table
- I/O
- Non-I/O
- Communication
- PLC
- Permit Action Input
- Write Config PB From HMI
- Move Source: New Setpoint Destination: Current Setpoint
- Action Output
- Input
- Output
- Instruments
- Controllers
- Servers
- OPC, HMI, Historian
- Programming Terminals

© 2018 SANS Institute
If the PLC is the Castle, Where are the holes in the Castle Wall?

One Piece of Misinformation Can Spread to Many Consumers or Cause the Control to Not Behave As Intended
Building Bridges

**Stage 1**
- Adversary has successfully performed the necessary elements of the Stage 1 Kill chain
- To have an ICS effect, the adversary needs to move into the elements of the Stage 2 ICS Kill Chain

**Stage 2**
- Trusted connections
- Vendor access
- Support personnel remote access
- System backup or alternate site replication tasks
- System Mgmt. communications - patching, monitoring, alerting, configuration and change Mgmt.
- Data historians
- Direct access dial up
- Waterholing attacks
- Social Engineering
- When the adversary has identified a path into the ICS environment, the Stage 2 ICS Kill Chain elements can be acted upon
Is it hard to get access to Level 0/1?
Contracted Services, Remote Support and Connectivity Makes for Easier Access to the Lower Levels of the Purdue Model

1. Scanner to Adapter process data
2. Scanner to Adapter configuration
3. Scanner to adapter across zones
4. SCADA and HMI to Adapter (PLC)
5. Scanner to Scanner
6. Engineering PC to Adapter, scanner, and HMI for configuration and diagnostics
7. Enterprise to Adapter (e.g., energy object)
8. Configuration tool to network infrastructure
9. Local Machine Remote Access
10. Enterprise remote access
Is it hard to get access to Level 0/1? Contracted Services, Remote Support and Connectivity Makes for Easier Access to the Lower Levels of the Purdue Model

1. Scanner to Adapter process data
2. Scanner to Adapter configuration
3. Scanner to adapter across zones
4. SCADA and HMI to Adapter (PLC)
5. Scanner to Scanner
6. Engineering PC to Adapter, scanner, and HMI for configuration and diagnostics
7. Enterprise to Adapter (e.g., energy object)
8. Configuration tool to network infrastructure
9. Local Machine Remote Access
10. Enterprise remote access

New Paths to Lower Levels

Plants want to consume Contracted Services data so they create a connection
Demo Architecture

1) Programming Terminal via Ethernet
2) Programming Terminal via HART modem
3) Instrument Programming Port
4) NFC, Bluetooth, Collaborative
Demo Architecture: OPC Client Writes To PLC Data Table

1) OPC Client Enumerates the Tag list
2) OPC converted Read/Write to appropriate protocol
3) Write Changes to PLC Data Table
4) Program Operates with new Values
DEMO
<table>
<thead>
<tr>
<th>ItemID</th>
<th>Sub Value</th>
<th>Sub Quality</th>
<th>Sub Updates</th>
<th>Update Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>[OandGSummit]Change_IE2C_Config</td>
<td>0</td>
<td>Good</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>[OandGSummit]BitMarchEn</td>
<td>0</td>
<td>Good</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>[OandGSummit]Local:1:Ch0Data</td>
<td>85</td>
<td>Good</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>[OandGSummit]E2_Slot3.Ch0HighEngineering</td>
<td>2260</td>
<td>Good</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>[OandGSummit]E2_Slot3.Ch0LowEngineering</td>
<td>-454</td>
<td>Good</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>[OandGSummit]E2_Slot3.Ch0AlarmDisable</td>
<td>0</td>
<td>Good</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Actual Temperature**

**Hi Engineering Scaling**
### OPC Client Writing Configuration Recap

#### Actual Temperature

<table>
<thead>
<tr>
<th>Item ID</th>
<th>Sub Value</th>
<th>Sub Quality</th>
<th>Sub Updates</th>
<th>Update Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>[OandGSummit]Change_IE2C_Config</td>
<td>0</td>
<td>Good</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>[OandGSummit]BitMarchEn</td>
<td>0</td>
<td>Good</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>[OandGSummit]Local:3:i.Ch0Data</td>
<td>-6</td>
<td>Good</td>
<td>58</td>
<td>1</td>
</tr>
<tr>
<td>[OandGSummit]IE2_Slot3.Ch0HighEngineering</td>
<td>1800</td>
<td>Good</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>[OandGSummit]IE2_Slot3.Ch0LowEngineering</td>
<td>-454</td>
<td>Good</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>[OandGSummit]IE2_Slot3.Ch0AlarmDisable</td>
<td>0</td>
<td>Good</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Hi Engineering Scaling Change Causes False Temperature Reading
Defend Against OPC Client Writes To PLC Data Table

1) External Access Limited to Read Only
2) OPC ClientEnumerates the Tag list
3) OPC converted Read/Write to appropriate protocol
4) Write Changes Blocked To PLC Data Table
DEMO
PLC Reconfigures HART Card

1) Design software starts ladder code reconfiguration of HART Card
2) PLC code executes and send reconfiguration commands to HART Card
3) Reconfiguration to HART Card causes respanned operation
4) Program Operates with new Values
Instruments Communicate to PLC/PAC Data Tables. Ladder Code Can Manipulate Instruments. Vector to Non-routable networks

- A typical plant will have multiple vendors of instruments
- Instrument vendors pick the supported protocols and they implement to a “standard”
- Most implemented protocols do not bake security into the protocol
- False sense of security thinking that a non-routable protocol can’t be reached

4.3.3 HART Pass-through Messaging

The HART Pass-Through Command can be used to send any HART command including universal, common practice or device specific, directly to a field device via ladder.

All HART pass-through commands require a series of messages to be exchanged. First, a pass-through init must be sent to the HART module to initiate the pass-through command. The HART module will respond to the request with a request reply that includes a handle that can be used to obtain the pass-through message response. Once the handle is received, the user may issue a pass-through query to obtain the status of the
Demo Architecture: Re-span Instrument without PLC Knowledge

1. Instrument Configuration Software
2. Analog Input
3. HART Card
4. PLC

Data Table

CIP
Analog/HART

Temp Xmitter
4-20ma + HART

Temp Xmitter HART

Ethernet

Instrument Programming Port

1) Instrument configuration software reconfigures HART 4-20ma span
2) New span updates PLC Data Table
3) Program Operates with new Values
Demo Architecture: Re-span Instrument without PLC Knowledge

Before Re-span

After Re-span
DEMO
Demo Architecture: Reconfigure Instrument without Instrument Software Knowledge

1. PACTware HART Configuration Software
   - PACTware w/ HART Modem
   - Programming Terminal

2. PLC
   - Analog In
     - CIP
     - Analog/HART

3. HART Card
   - CIP
   - Analog/HART

Instrument Programming Port

1) Instrument configuration software reconfigures HART 4-20mA span
2) New span updates PLC Data Table
3) Program Operates with new Values
PACTware Generic Framework For Reading HART Values
PACTware Generic Framework For Writing HART Values
Original Instrument Software is Still Reporting Fahrenheit but Correct Celsius Value

Sensor: 29.6 °F
Loopcurrent: 7.13 mA

Recap
PACTware Shows Mixed C and F
Reconfigure HART Transmitter via Cell Phone

1) Transmitter Software used to modify configuration
2) New span updates PLC Data Table
3) Program Operates with new Values
Reconfigure Instrument Via Cell Phone

Recap
Actual Temperature Before Re-span of Temp Xmitter
PIDE - Off

Recap

Note the use of CVEU and CV% outputs

ON/OFF PID control!
SRTP allows TWO ranges

Use PROG parameters

© 2018 SANS Institute
all other copyrights and trademarks are hereby recognized

49
After Re-span of HART Temp Xmitter, Actual Temperature is reporting lower, PIDE goes to 100%
Summary: Methods of Defense

Methods of Defense:

• If you know there are constants, make the program use data type “constant”
• Some vendor’s products can limit access to Data Table entries to design tools
  • You still need to defend the workstation with the design tools
• You need to boundary check the inputs to the PLC Data Table
• Physical security is still key to instrumentation and I/O networks
• Physical devices that limit process variables are still needed
End Of Presentation