The Misconfigured Network

How common network misconfigurations impact ICS reliability and security

SANS 2019

Steve Stock
Industrial Cybersecurity Business Manager
aeSolutions

Bio

Steve Stock

Industrial Cybersecurity Business Manager

- ISA Certified Cybersecurity Professional Instructor
- Cisco Certified Network Professional (CCNP)
- Global Industrial Control Security Professional (GICSP)

25 Years of Experience in Telecommunications and Industrial Networking

- Industrial Cybersecurity Assessments
  - (Gap, Vulnerability, and Risk Assessments)
- Routing and Switching
- Wireless Communications
- Network Design and Commissioning
- Network Remediation

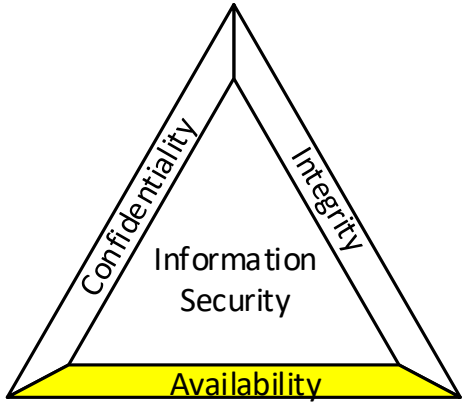
Agenda

- What's the problem?
- How is ICS security and availability impacted?
- Case study
- Live demonstration
- Questions

What's the Problem?

Common misconfigurations found in today's

Process Control Networks impact ICS security and threaten Availability



Category	Description	Common Misconfiguration
access port	Connects a single end device to the network	• Access port configured with VLAN used for trunk native • Access port assigned to default VLAN 1 • Unused port administratively "UP"
trunk port	Connects two network switches together	• Trunk port configuration inconsistent with connected switch • Trunk port configured to allow all VLANs to traverse link • Access port with multiple connected devices
Virtual LAN (VLAN)	Segments traffic into logically separate networks	• Trunk native VLAN allowed over trunk • Unused port assigned to active VLAN • VLAN database contains unassigned VLANs • Interface with default configuration; not configured
spanning-tree protocol (STP)	Protocol that is intended to prevent switching loops when redundant paths are available	• Access port with portfast disabled • Trunk port configured with portfast enabled • STP topology not enforced; dynamic STP root elections

Spanning Tree Primer

- Spanning Tree Protocol (STP)
  - STP is used in OSI Layer 2 switched networks to prevent switching loops
  - An election process is used to determine the root switch (priority + MAC)
  - All port forwarding decisions are made with respect to the root (shortest path)
  - Redundant connections to the root switch are blocked to prevent loops
  - Changes to the network topology can cause STP re-convergence
  - Network is temporarily unavailable during the topology change

ICS Security Impacts

The focus of this presentation is around how these common misconfigurations impact PCN Availability.

However, there are some security concerns raised when these common misconfigurations are present.

- Unauthorized access to network segments
- VLAN hopping (switch spoofing)
- VLAN hopping (double tagging)

ICS Availability Impacts

Many of the common misconfigurations can severely reduce PCN Availability and impact operations

- Loss of Process View / Control
- Process shutdowns
- Increase spanning-tree convergence times
- Potential to introduce switching loops
- Unexpected / undesirable spanning-tree topologies

Case Study: Background

- An Oil & Gas refinery attempted to upgrade two legacy Process Control Network switches in their Alky Unit with like and kind components
- Resulted in widespread PCN outages (6 Process Units)
- The PCN had to be restored to previous state with the legacy switches
- Until this is remediated, the refinery must accept the operational risk
  - *If one of these legacy switch fails, it can't be replaced because it will cause PCN outages and loss of view / loss of control across many of its operating units*
- Contributing factors

Access ports configured with VLAN used for trunk native

Outdated firmware / IOS

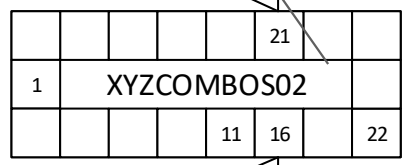
Spanning tree topologies not enforced

PLC on trunk native VLAN

Access port configured with VLAN used for trunk native

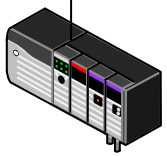
Switch	Time	Event
XYZCOMBOS02	10:48:15	Host 0000.bcd1.ba13 in vlan 1000 is flapping between port Gi0/16 and port Gi0/21
XYZCOMBOS02	10:48:30	Host 0000.bcd1.ba13 in vlan 1000 is flapping between port Gi0/16 and port Gi0/21
XYZCOMBOS02	10:48:45	Host 0000.bcd1.ba13 in vlan 1000 is flapping between port Gi0/16 and port Gi0/21
XYZCOMBOS02	10:49:01	Host 0000.bcd1.ba13 in vlan 1000 is flapping between port Gi0/16 and port Gi0/21
XYZCOMBOS02	10:49:16	Host 0000.bcd1.ba13 in vlan 1000 is flapping between port Gi0/16 and port Gi0/21
XYZCOMBOS02	10:49:31	Host 0000.bcd1.ba13 in vlan 1000 is flapping between port Gi0/16 and port Gi0/21

```
interface GigabitEthernet0/21
 description Uplink to XYZCCRS01_2-5
 switchport trunk native vlan 1000
 switchport trunk allowed vlan
248,280,312,344,358,368,453,1000
 switchport mode trunk
 switchport nonegotiate
```



XYZCCRS01_2/5

```
interface GigabitEthernet0/16
 switchport access vlan 1000
 switchport mode access
 speed 100
 duplex full
 no cdp enable
 spanning-tree portfast
```



Allen-Br_D1:BA:13

SwitchName	PortNumber	ConnectedMAC	Vendor
XYZENGSVCSS01	GigabitEthernet0/21	00:00:BC:D1:BA:13	Allen-Br
XYZENGSVCSS02	GigabitEthernet0/21	00:00:BC:D1:BA:13	Allen-Br
XYZALKYS01	GigabitEthernet1/1	00:00:BC:D1:BA:13	Allen-Br
XYZALKYS02	GigabitEthernet1/1	00:00:BC:D1:BA:13	Allen-Br
XYZALKYS03	GigabitEthernet1/0/25	00:00:BC:D1:BA:13	Allen-Br
XYZALKYS04	GigabitEthernet1/0/25	00:00:BC:D1:BA:13	Allen-Br
XYZALKYS05	GigabitEthernet0/25	00:00:BC:D1:BA:13	Allen-Br
XYZALKYS06	GigabitEthernet1/1	00:00:BC:D1:BA:13	Allen-Br
XYZATRS01	GigabitEthernet1/1	00:00:BC:D1:BA:13	Allen-Br
XYZCCRDCSR01	GigabitEthernet1/0/2	00:00:BC:D1:BA:13	Allen-Br
XYZCCRDCSR02	GigabitEthernet1/0/2	00:00:BC:D1:BA:13	Allen-Br
XYZCCRS01	GigabitEthernet2/5	00:00:BC:D1:BA:13	Allen-Br
XYZCOMBOS01	GigabitEthernet0/21	00:00:BC:D1:BA:13	Allen-Br
XYZCOMBOS02	GigabitEthernet0/16	00:00:BC:D1:BA:13	Allen-Br
XYZCOMBOS03	GigabitEthernet0/25	00:00:BC:D1:BA:13	Allen-Br
XYZCOMBOS05	GigabitEthernet1/1	00:00:BC:D1:BA:13	Allen-Br
XYZDDUS01	GigabitEthernet1/1	00:00:BC:D1:BA:13	Allen-Br
XYZDDUS02	GigabitEthernet1/1	00:00:BC:D1:BA:13	Allen-Br
XYZFGRS01	GigabitEthernet1/0/25	00:00:BC:D1:BA:13	Allen-Br

Outdated Firmware / IOS

Network switches with outdated IOS

In this case study, 21 of 39 PCN switches were running IOS versions that were 5+ years old.

SwitchName	Manufactur	Model Number	Firmware	Release Date
XYZDDUS01	Cisco	IE-3000-8TC	12.2(55)SE5	02/16/12
XYZDDUS02	Cisco	IE-3000-8TC	12.2(55)SE5	02/16/12
XYZCOMBOS06	Cisco	IE-3000-8TC	*12.2(58)SE2*	12/22/11
XYZATRS01	Cisco	IE-3000-8TC	15.0(2)EY3	11/19/13
XYZSRUCEMS01	Cisco	IE-3000-8TC	15.0(2)EY3	11/19/13
XYZALKYS01	Cisco	IE-3000-8TC	15.0(2)SE6	04/28/14
XYZALKYS02	Cisco	IE-3000-8TC	15.0(2)SE6	04/28/14
XYZALKYS06	Cisco	IE-3000-8TC	15.0(2)SE6	04/28/14
XYZCOMBOS04	Cisco	IE-3000-8TC	15.0(2)SE6	04/28/14
ENGINEERING-SVCS-SW1	Cisco	WS-C2960G-24TC-L	*12.2(58)SE2*	12/22/11
ENGINEERING-SVCS-SW2	Cisco	WS-C2960G-24TC-L	*12.2(58)SE2*	12/22/11
XYZCOMBOS01	Cisco	WS-C2960G-24TC-L	*12.2(58)SE2*	12/22/11
XYZCOMBOS02	Cisco	WS-C2960G-24TC-L	*12.2(58)SE2*	12/22/11
XYZPSS01	Cisco	WS-C2960G-48TC-L	*12.2(58)SE2*	12/22/11
XYZPSS02	Cisco	WS-C2960G-48TC-L	*12.2(58)SE2*	12/22/11
XYZUFS01	Cisco	WS-C2960G-48TC-L	*12.2(58)SE2*	12/22/11
XYZUFS02	Cisco	WS-C2960G-48TC-L	*12.2(58)SE2*	12/22/11
XYZGHTS01	Cisco	WS-C2960S-24TS-L	15.2(1)E3	05/08/14
XYZGHTS02	Cisco	WS-C2960S-24TS-L	15.2(1)E3	05/08/14
XYZALKYS05	Cisco	WS-C2960S-24TS-S	12.2(55)SE7	01/31/13
XYZCOMBOS03	Cisco	WS-C2960S-24TS-S	12.2(55)SE7	01/31/13

Cisco Bug ID: CSCea46385

The user receives the following error message: "%ETHCNTR-3-LOOP_BACK_DETECTED" on a Cisco Catalyst switch that runs Cisco IOS® Software.

The problem is aggravated if there are a large number of Topology Change Notifications on the network.

Outdated Firmware / IOS

Network switches with outdated IOS

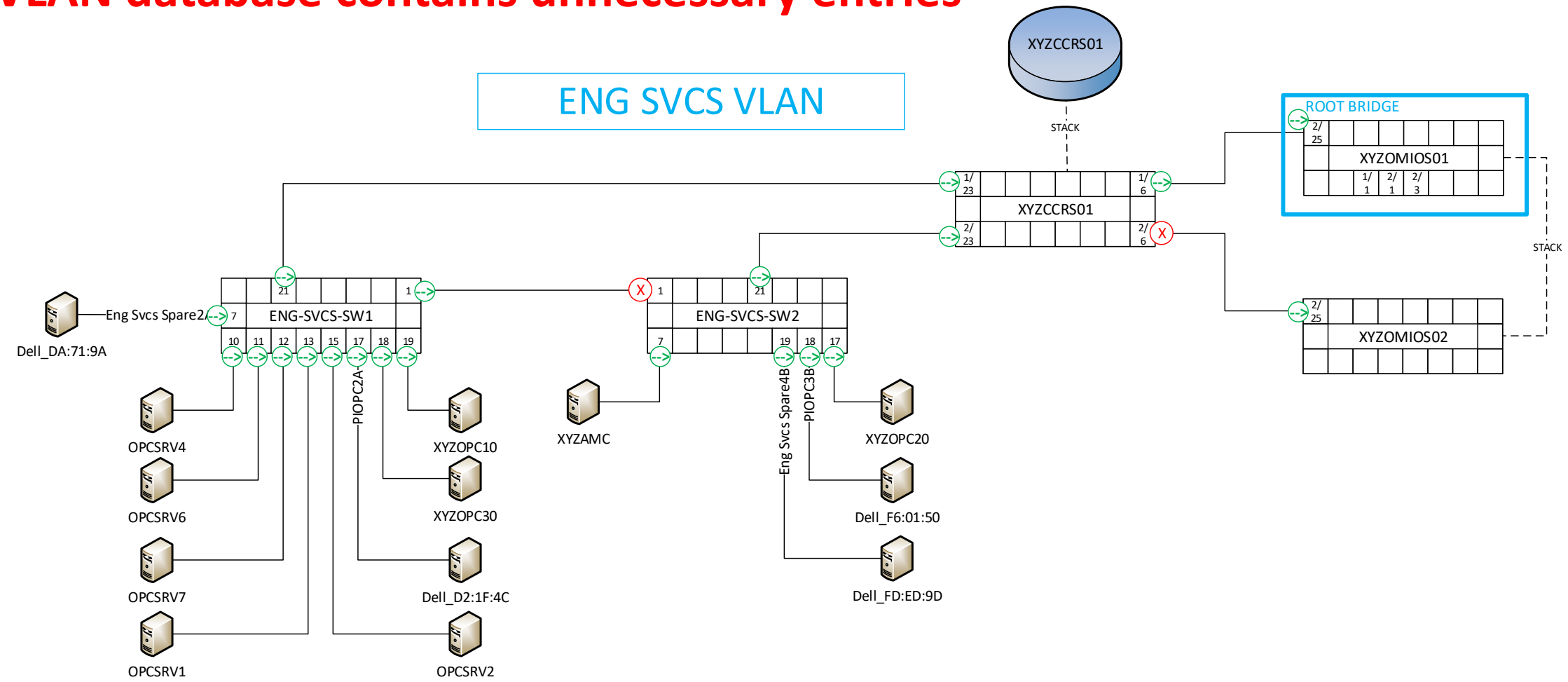
During the network event, six of the PCN switches were caught in a continuous cycle of “loop-back detected” resulting in ports going into an “err-disable” (shutdown) state. Logs pulled from these switches show the cycle of events:

Switch	Time	Event
XYZFGRS01	13:51:42	Attempting to recover from loopback err-disable state on Gi1/0/25
XYZFGRS01	13:51:45	Interface GigabitEthernet1/0/25, changed state to up
XYZFGRS01	13:51:46	Line protocol on Interface GigabitEthernet1/0/25, changed state to up
XYZFGRS01	13:51:52	Loop-back detected on GigabitEthernet1/0/25.
XYZFGRS01	13:51:52	loopback error detected on Gi1/0/25, putting Gi1/0/25 in err-disable state
XYZFGRS01	13:51:53	Line protocol on Interface GigabitEthernet1/0/25, changed state to down
XYZFGRS01	13:51:54	Interface GigabitEthernet1/0/25, changed state to down
XYZFGRS01	13:56:53	Attempting to recover from loopback err-disable state on Gi1/0/25
XYZFGRS01	13:56:55	Interface GigabitEthernet1/0/25, changed state to up
XYZFGRS01	13:56:56	Line protocol on Interface GigabitEthernet1/0/25, changed state to up
XYZFGRS01	13:56:56	Line protocol on Interface GigabitEthernet1/0/1, changed state to down
XYZFGRS01	13:56:57	Interface GigabitEthernet1/0/1, changed state to down
XYZFGRS01	13:57:03	Loop-back detected on GigabitEthernet1/0/25.
XYZFGRS01	13:57:03	loopback error detected on Gi1/0/25, putting Gi1/0/25 in err-disable state

Spanning Tree Topology Not Enforced

Spanning tree topology not enforced &

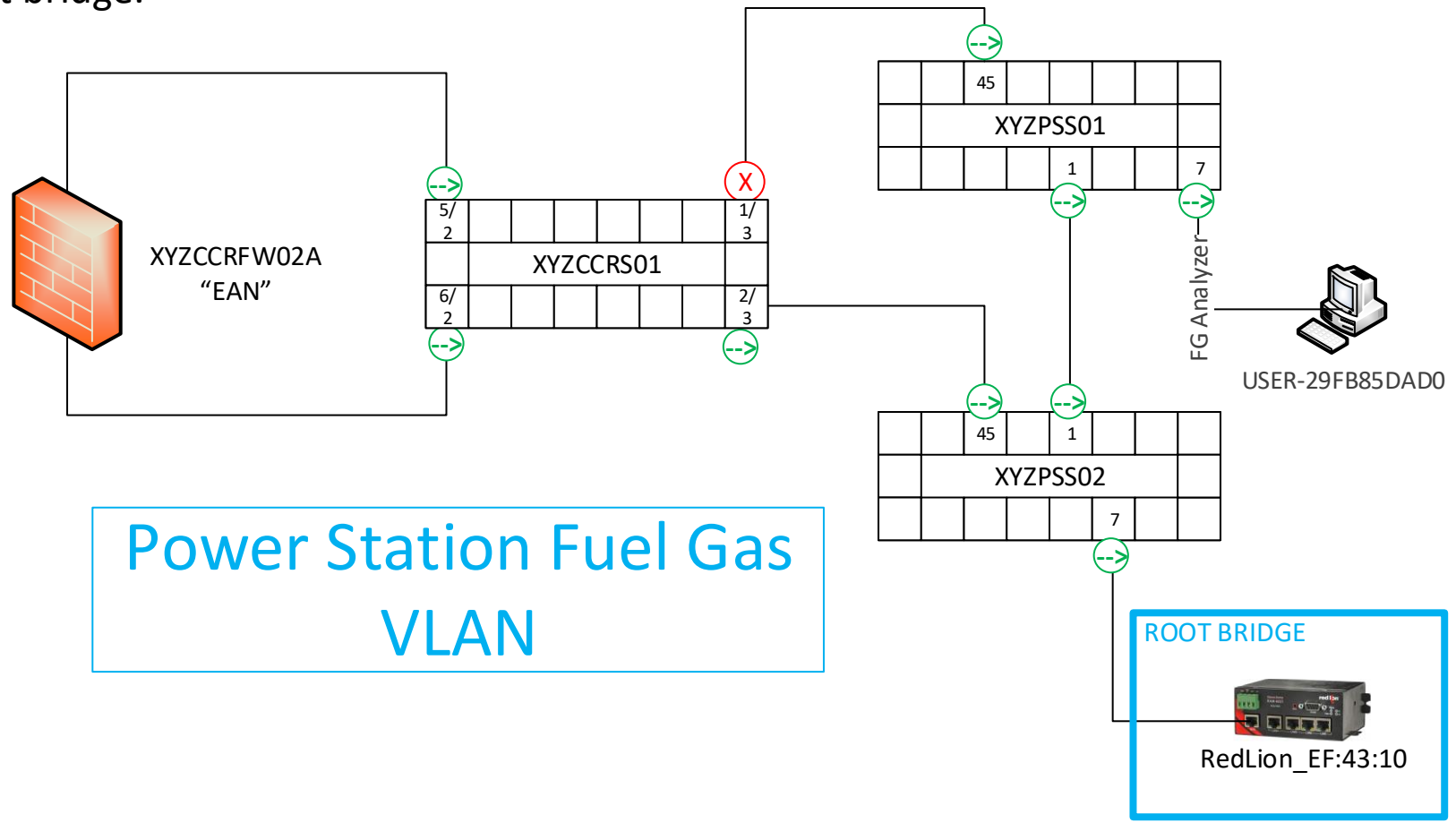
VLAN database contains unnecessary entries



End Device Becomes Root Switch

Access port participating in STP election

If STP priorities are left as default and access ports are allowed to participate in the election, end devices can become the root bridge.



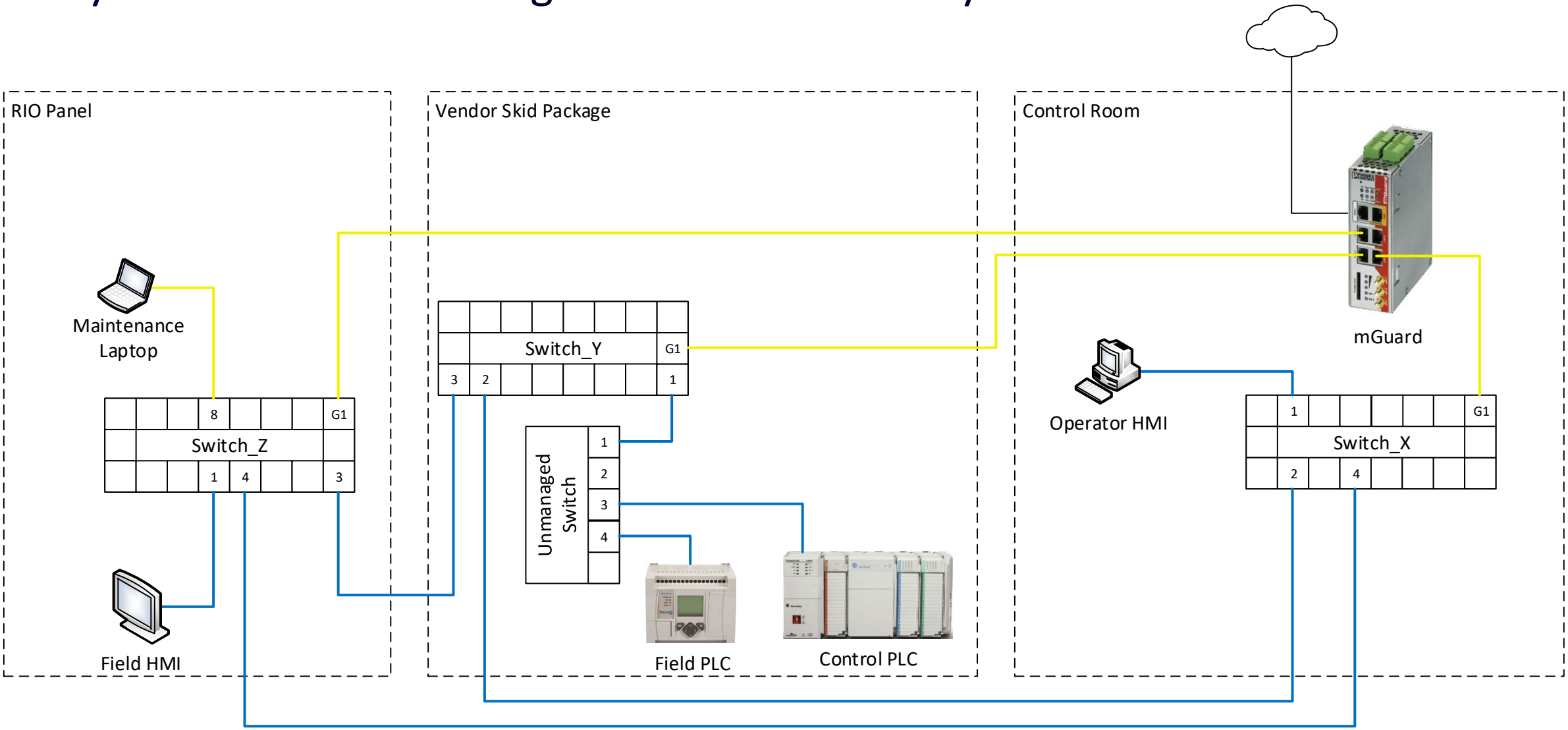
Case Study: Results

The configuration files and event logs of **39** PCN switches were evaluated. Analysis of the **1,191** physical switch interfaces revealed **1,980** common misconfigurations.

Misconfiguration	Affected Interfaces	Percentage
Access port configured with VLAN used for trunk native	114	11.7%
Access port with multiple connected devices	68	7.0%
Access port assigned to default VLAN 1	0	0.0%
Access port with portfast disabled	209	21.4%
Interface with default configuration, not configured	48	4.0%
Trunk native VLAN allowed over trunk	161	97.6%
Trunk port configuration inconsistent with connected switch	18	10.9%
Trunk port configured to allow all VLANs	45	27.3%
Trunk port configured with portfast enabled	5	3.0%
Unused port administratively UP	605	50.8%
Unused port assigned to active VLAN	575	48.3%
VLAN table contains unassigned VLANs (458 total entries)	341	74.5%

Demo: PCN Overview

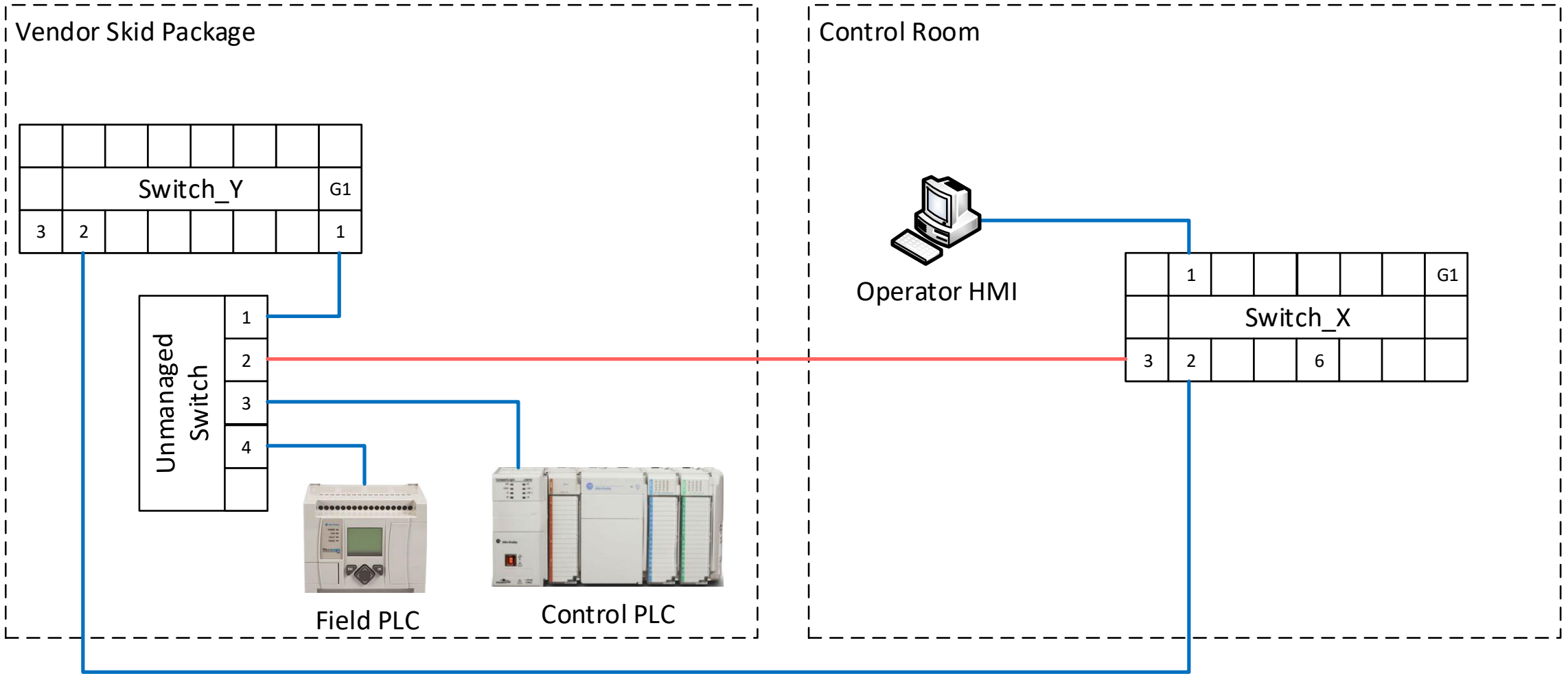
Physical Network Drawing for the “XYZ Refinery” used in this demonstration



Demonstration 1 – Switching Loop

Access ports misconfigured and use of unmanaged switches in PCN

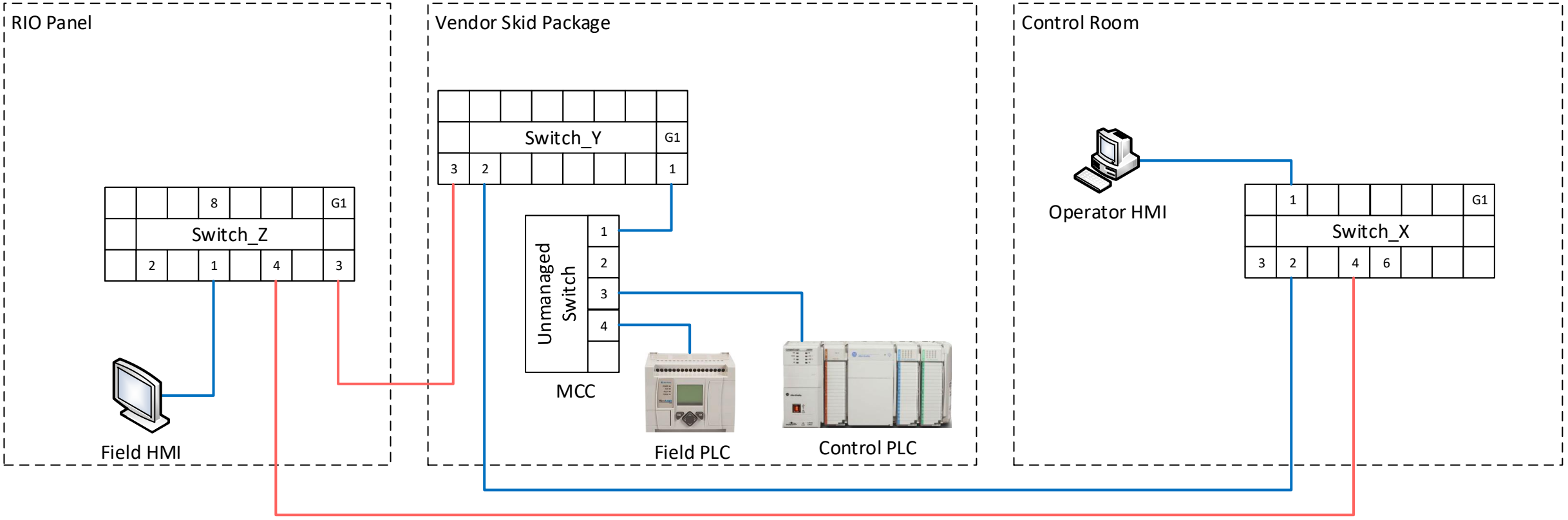
Create redundant link between Operator HMI and Control PLC



Demonstration 2 – STP Topology Change

Spanning Tree Topology not Enforced

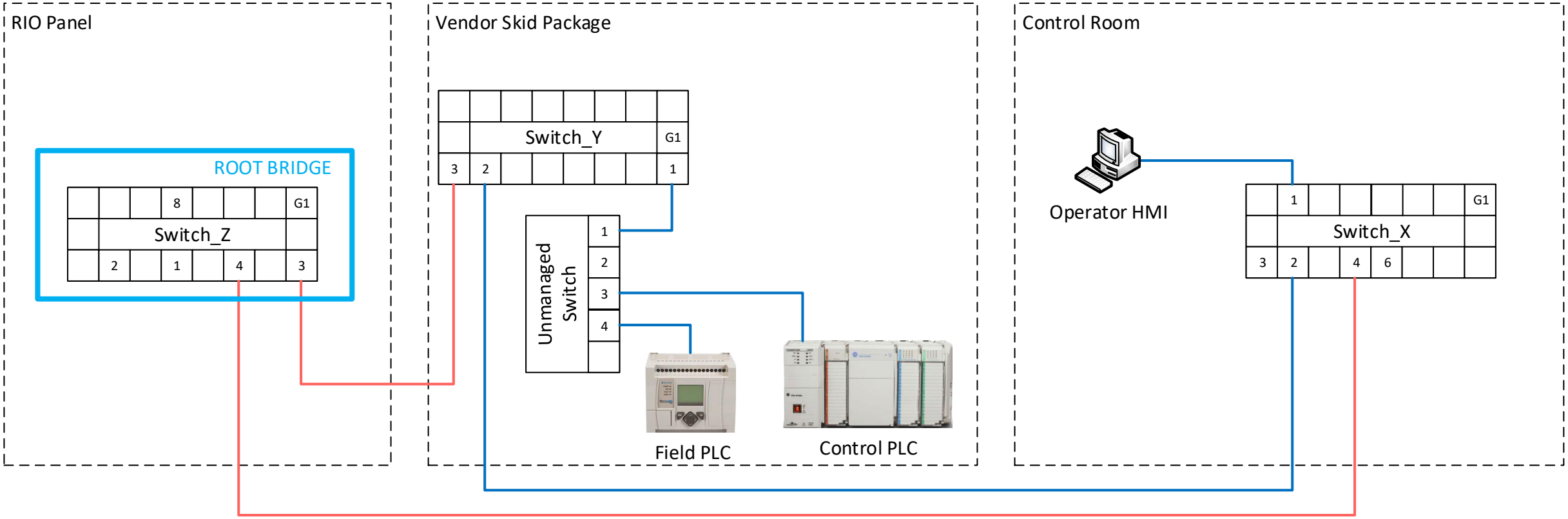
PCN maintenance window – Upgrade Switch_Z



Unexpected STP Topology Change

Spanning Tree Topology not Enforced

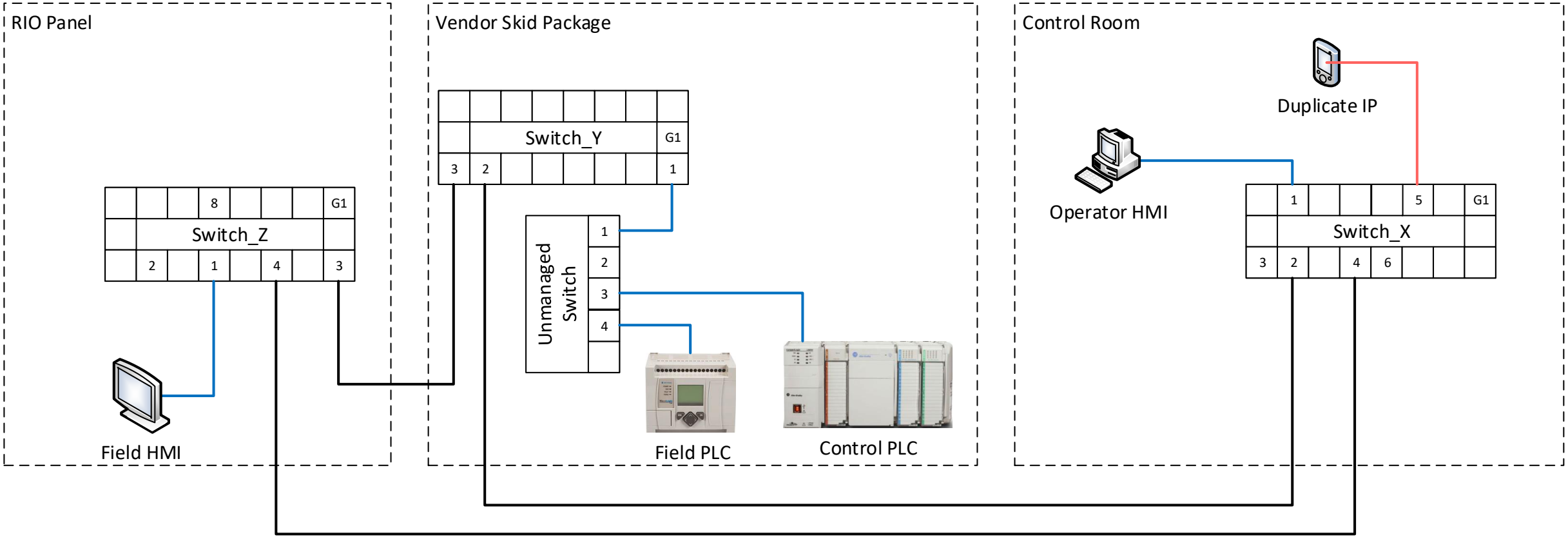
Maintenance in unrelated area impacts PCN



Demonstration 3 – Duplicate IP

Unused port assigned to active VLAN

Devices connected to such a port would be able to communicate to all other devices in the VLAN and commonly the entire PCN if not restricted by a firewall or router with Access Control Lists (ACLs).

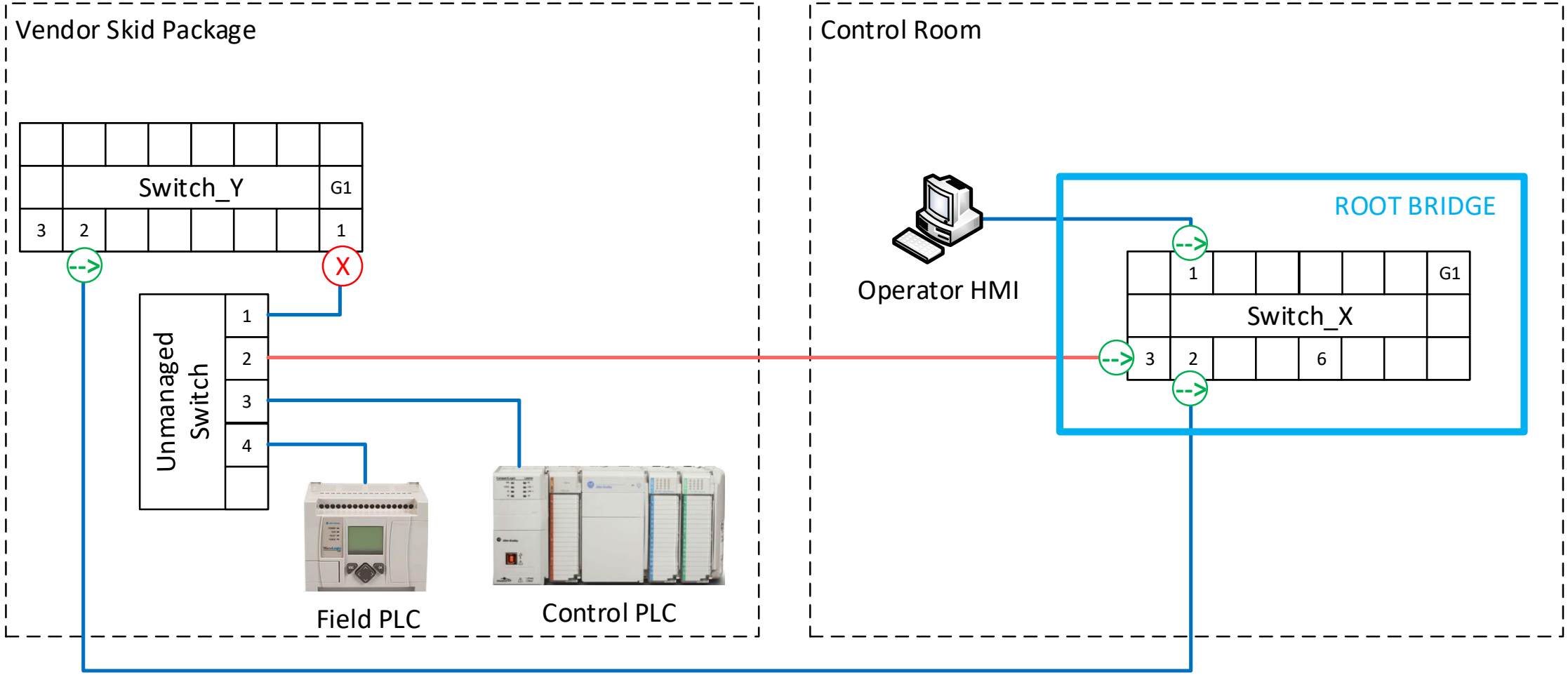


Let's fix it

- Unused switch ports
  - Configure unused ports as access ports and "nonegotiate"
  - Create an unused VLAN, place unused ports in this vlan
  - Administratively shutdown unused ports
- Trunk ports
  - Only allow necessary VLANs across trunks
  - Don't assign ports to the trunk native VLAN
- Spanning tree
  - Set root priorities to create predictable and efficient topologies
  - Ensure STP participation is correctly configured
- VLANs
  - Remove unused VLANs from the vlan database

Demonstration 4 – Prevent Switching Loop

STP topology is enforced and switch ports are configured correctly



Demonstration 5 – STP Topology Stability

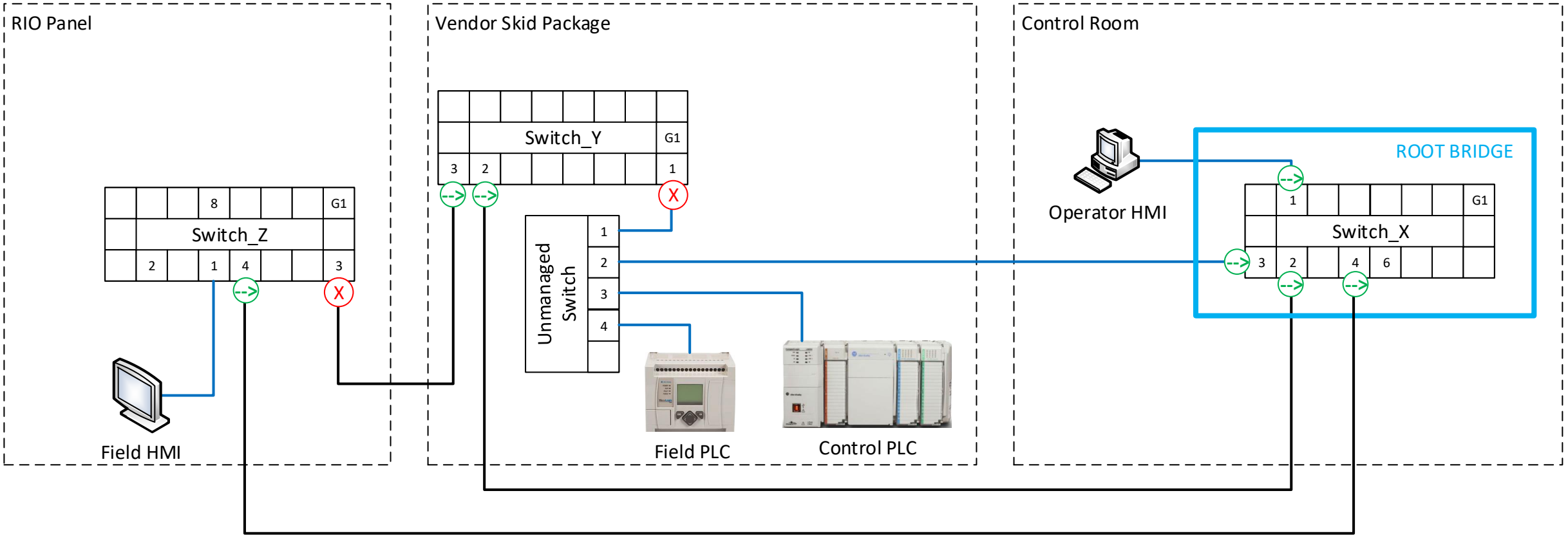
STP priorities are set

Creates predictable and efficient STP topologies

Switch_X.log - Notepad

File Edit Format View Help

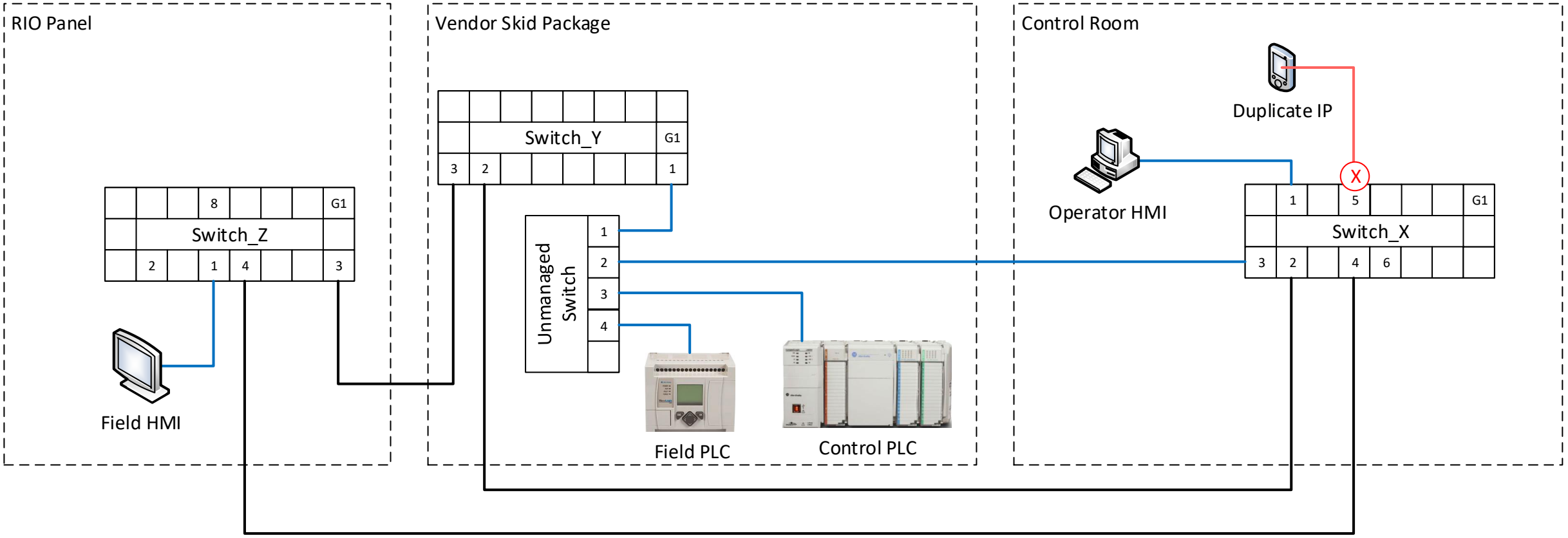
```
Switch_X#show spanning-tree detail

 VLAN0200 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 4096, sysid 200, address f47f.354a.7f80
  Configured hello time 2, max age 20, forward delay 15
  We are the root of the spanning tree
```



Demonstration 6 – Prevent Duplicate IP

Unused ports configured and shutdown

Prevents unexpected or unauthorized connections to the PCN



Last words

- Optimize Your Process Control Network
  - Identify, document, and mitigate common networking misconfigurations
  - Enforce spanning tree topologies
  - Update network device firmware/operating systems
  - Train staff on applicable policies and industry best practices

Thank You.

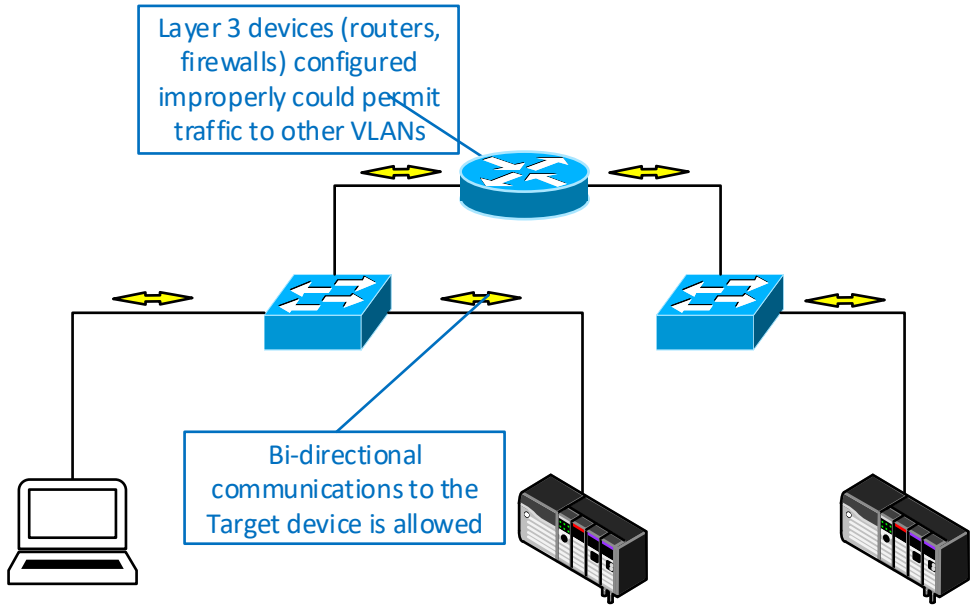
The Misconfigured Network

Steve Stock
steve.stock@aesolns.com

Security Impact – Unauthorized Access

Often, switch ports are configured to be members of active VLANs and left administratively up. The unauthorized device can simply connect to the live port and communicate to other devices on the VLAN

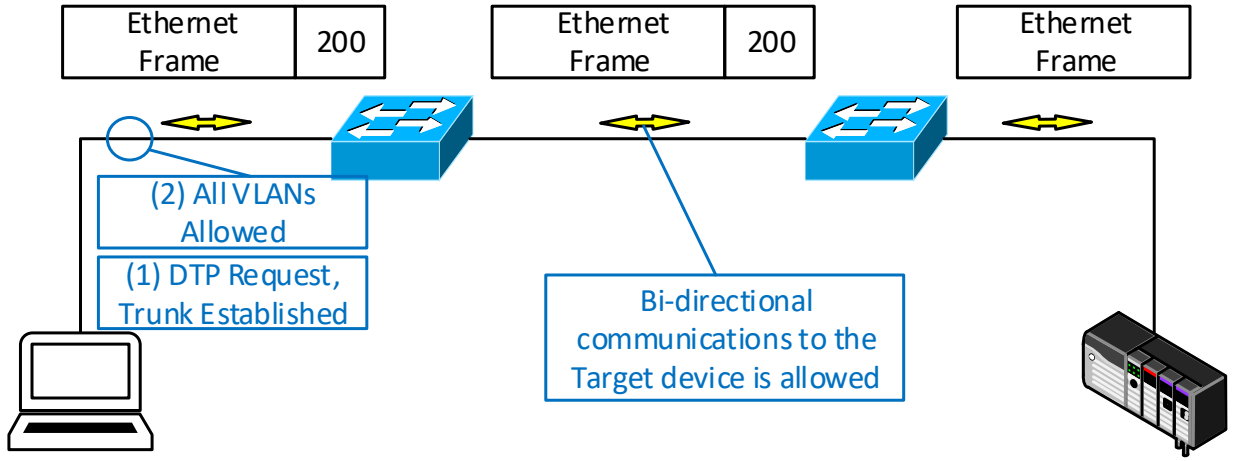
- Misconfigurations that can introduce this vulnerability
  - Unused (trunk) port administratively UP
  - Unused port assigned to active VLAN
- Mitigations
  - Move unused ports to an unused VLAN
  - Don’t allow unused VLAN over trunks
  - Explicitly configure unused ports as access ports
  - Configure access ports to “nonegotiate”
  - Administratively shutdown unused ports



Security Impact – Switch Spoofing

Also known as switch spoofing, allows unauthorized access to another VLAN by negotiating a trunk with the switch

- Misconfigurations that can introduce this vulnerability
  - Unused (trunk) port administratively UP
  - Interface with default configuration, not configured
- Mitigations
  - Move unused ports to an unused VLAN
  - Don’t allow unused VLAN over trunks
  - Explicitly configure the port to be an access port
  - Configure access ports to “nonegotiate”
  - Administratively shutdown unused ports



Security Impact – Double Tagging

Allows traffic from one VLAN to transmit data to a device in different VLAN

- Misconfigurations that can introduce this vulnerability
  - Unused (trunk) port administratively UP
  - Interface with default configuration, not configured
  - Access port configured with VLAN used for trunk native
  - Access port assigned to default VLAN 1
  - Trunk native VLAN allowed over trunk
  - Trunk port configured to allow all VLANs
- Mitigations
  - Assign an unused VLAN as the trunk native
  - Avoid using the trunk native VLAN for any other purpose