Information Technology (IT) Versus Operational Technology (OT)

- IT Network
- Corporate Offices
- Control Center
- Solar Generation
- Distribution Substation
- Wind Generation
- Hydroelectric Generation
- Transmission Substation
- Fossil Fuel Generation
- Wind Generation
- Substation
- Wind Generation
- Wind Generation
- Substation
- Substation
Challenges With Traditional Ethernet in OT Applications

- Designed on plug-and-play model
- Lacks cybersecurity profile
- Exhibits undesirable behavior
- Uses reactive failover
- Provides topology-dependent performance
- Difficult to test
Slow Network Healing

**RSTA**

*Healing time*

50 ms or longer in 10-node ring
Ethernet Challenges in OT Applications

- Slow healing time (can be > 50 ms)
- Unpredictable behavior
- No visibility of communications between devices
- Lack of security profile
- Difficulty testing
SDN Meets OT
Application Requirements

- ✔ Fast healing (failover)
- ✔ Cybersecurity
- ✔ Network visibility
- ✔ Determinism
- ✔ Low latency
SDN Principle
Decision-Making Separated From Ethernet Switch

Control Plane

Data Plane
- Flows (rules) are configured in the controller
- Flows are “pushed” to SDN switches
- Traffic is custom engineered
- Every packet is inspected
How SDN Works

Control plane inspects each Ethernet packet and performs the following functions:

- **Match fields**: Matches rules based on a portion of the Ethernet packet.
- **Instructions**: Performs one or more programmed actions.
- **Counters**: Increments counters and sends counter data to a centralized point.
Multilayer Matching Rules Forward
Approved Packets

SDN Flow Match Rule

Ingress Port
Layer 1
Ethernet Header
Layer 2
IP Header
Layer 3
TCP/UDP Header
Layer 4
Payload
OpenFlow Match / Action Example

Layer 2 Unmanaged Switch

<table>
<thead>
<tr>
<th>Physical Port ID</th>
<th>Src MAC</th>
<th>Dst MAC</th>
<th>Ether Type</th>
<th>VLAN ID</th>
<th>IPv4 Src</th>
<th>IPv4 Dst</th>
<th>TCP/UDP Src</th>
<th>TCP/UDP Dst</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

00:30:A7:06:11:97

Action

Output Forward Port 4

Packet

SDN Switch

1        2

3        4
### OpenFlow Match / Action Example

#### Layer 2 Unmanaged Switch

<table>
<thead>
<tr>
<th>Physical Port ID</th>
<th>Src MAC</th>
<th>Dst MAC</th>
<th>Ether Type</th>
<th>VLAN ID</th>
<th>IPv4 Src</th>
<th>IPv4 Dst</th>
<th>TCP/UDP Src</th>
<th>TCP/UDP Dst</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>1.1.1.2</td>
<td>2.2.2.2</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

**Action**

Output Forward Port 3

---

**Packet**
OpenFlow Match / Action Example
Layer 2 Unmanaged Switch

<table>
<thead>
<tr>
<th>Physical Port ID</th>
<th>Src MAC</th>
<th>Dst MAC</th>
<th>Ether Type</th>
<th>VLAN ID</th>
<th>IPv4 Src</th>
<th>IPv4 Dst</th>
<th>TCP/UDP Src</th>
<th>TCP/UDP Dst</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>1.1.1.2</td>
<td>2.2.2.2</td>
<td>*</td>
<td>TCP 20000</td>
</tr>
</tbody>
</table>

Action
Output Forward Port 4

Packet
Reactive SDN in Operation

Typical IT SDN

SDN Switch → Rule → SDN Switch → Rule → Relay

Controller

Computer

Rule → SDN Switch

Packet

Relay
Proactive SDN in Operation

Typical OT SDN

- SDN Switch
- Rule
- Relay
- Controller
- Computer
- SDN Switch
- Rule
- Packet
Proactively Engineered Traffic for Reliability

Primary Path
Backup Path
Secondary Path
## SDN Fast Failover Versus STA

<table>
<thead>
<tr>
<th>Product</th>
<th>Topology</th>
<th>Healing Method</th>
<th>Healing Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer 1 Ethernet Switches</td>
<td>10-node ring</td>
<td>STA (Rapid PVST)</td>
<td>97 ms</td>
</tr>
<tr>
<td>Manufacturer 2 Ethernet Switches</td>
<td>4-node ring</td>
<td>STA (RSTP)</td>
<td>60 ms</td>
</tr>
<tr>
<td>Manufacturer 3 Ethernet Switches</td>
<td>10-node ring</td>
<td>STA (RSTP)</td>
<td>10 ms</td>
</tr>
<tr>
<td>SDN Switches</td>
<td>10-node ring</td>
<td>SDN Fast Failover</td>
<td>&lt;100 µs</td>
</tr>
</tbody>
</table>
Predefined SDN Failover

Monitors health of primary and backup links

Determines on which path to forward packets

if primary_link == UP
    use(primary_link);
else
    use(backup_link);
Cybersecurity Benefits

Enhanced security model
Employs deny-by-default architecture

Secured control plane
Eliminates MAC table and BPDU spoofing

Better situational awareness
Provides visibility of flows on the network
Cybersecurity Benefits

**Communications awareness**
Visibility of conversations between devices

**Packet inspection**
Every packet is inspected; detection of unauthorized or malicious packets

**Performance and security**
Increased performance with addition of security (not typical with traditional Ethernet)
Physical connections and flows are visible

Conversations between devices are visible

Testing Logical Connections

Local Connections

<table>
<thead>
<tr>
<th>From Automation Controller</th>
<th>From Relay</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>ARP</td>
</tr>
<tr>
<td>UnicastBidirectional Success</td>
<td>UnicastBidirectional Success</td>
</tr>
<tr>
<td>GOOSE</td>
<td>GOOSE</td>
</tr>
<tr>
<td>MulticastBidirectional Success</td>
<td>MulticastBidirectional Success</td>
</tr>
</tbody>
</table>
Application Visibility

Physical Connections

SDN Switch
Syslog IDS
Router
SDN Switch
Relay
Relay
Relay
SDN Switch
Relay
GPS Clock
Automation Controller

Logical Connections
Packet-Forwarding Control by Application

Traffic can be engineered to take different paths based on application.
## Traditional Ethernet Versus OT SDN

<table>
<thead>
<tr>
<th></th>
<th>Failover</th>
<th>Cybersecurity</th>
<th>Network Visibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional Ethernet</td>
<td>Slow &gt; 50 ms</td>
<td>Very low device communication has no security model</td>
<td>Low information about device conversations not available</td>
</tr>
<tr>
<td>SDN</td>
<td>Fast &lt; 100 μs</td>
<td>High devices communication is by permission and can be controlled</td>
<td>High information about device conversations is available</td>
</tr>
</tbody>
</table>
Different Ways of Thinking About Networking

Traditional Ethernet
1. Build network
2. Connect devices

SDN
1. Determine which devices need to communicate
2. Engineer the traffic specific to those devices
Successful application of SDN in electrical substations

- DNP3 protocol for SCADA
- GOOSE protocol for high speed protection

SDN allows engineers to design network

- Improved performance
- Cybersecurity
- Network visibility
Questions