OTSDN – What is it? Does it help?

Dennis Gammel

Schweitzer Engineering Laboratories, Inc.

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security | cred-c.org

Important Aspects of Critical OT Networks

- Determinism and low latency
- Precise time
- Fast fault detection, isolation, and recovery
- Cybersecurity defense in layers
- Monitoring, self-testing, and alarming
- Maintainability, testing and diagnostics
- High MTBF hardware

Message Delivery Performance Criteria Defined by International Standards

IED performance requirements

IEC 61850, IEC 60834, IEC 15802, IEEE 802.1

Latency specifications

IEC 61850, IEC 60834, IEC 15802, IEEE 802.1

Speed

IEC 61850

Message Delivery Quality Criteria Defined by International Standards

Dependability and security requirements

IEC 61850, IEC 60834

Availability requirements

IEC 61850, IEC 60834, IEEE 802.1

Reliability metrics

IEC 61850, IEEE 1613, IEC 60870

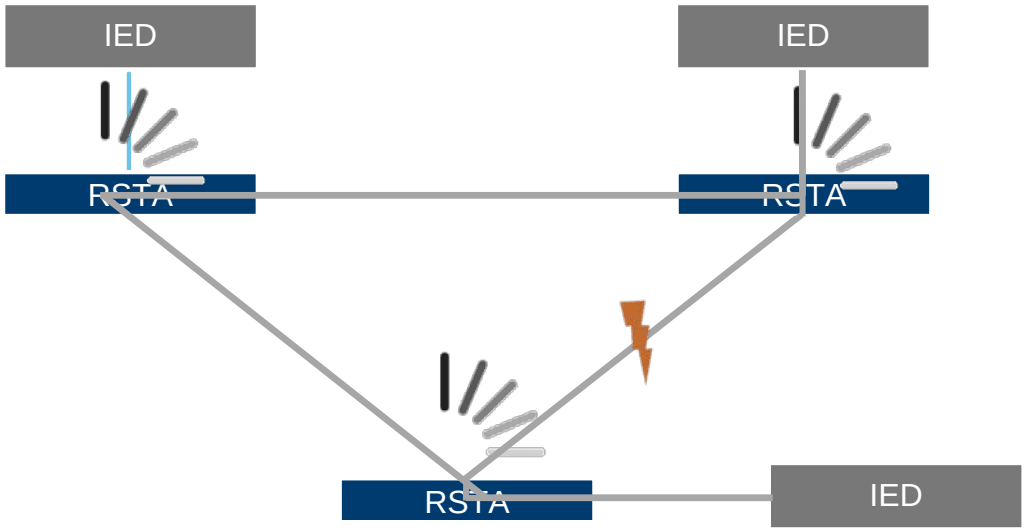
International Standards Dictate Protection Signal Exchange Acceptance Criteria

- Signal < 3 ms packet transit < 1 ms 99.99% of the time
- Signal <18 ms packet transit <15 ms 0.01% of the time
- Zero dropped GOOSE messages per year, <9 extra messages every 24 hours

Challenges With Traditional Ethernet Switching

- Designed for plug and play
- Conveniently does things “we don’t want”
- Reactive failover
- Topology dependent performance
- Difficult to achieve 100% test coverage

Network Healing Using IEC 62439-1 RSTA



Peer-to-peer RSTP informs RSTA

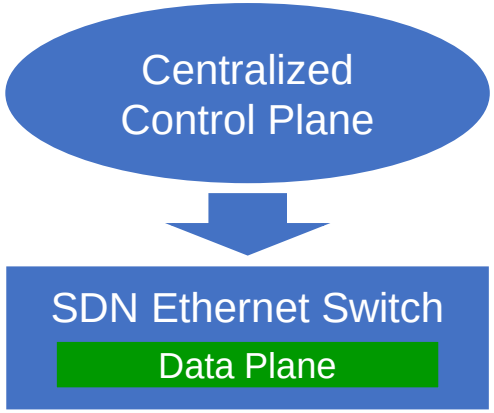
Introducing SDN

Traditional Ethernet Switch

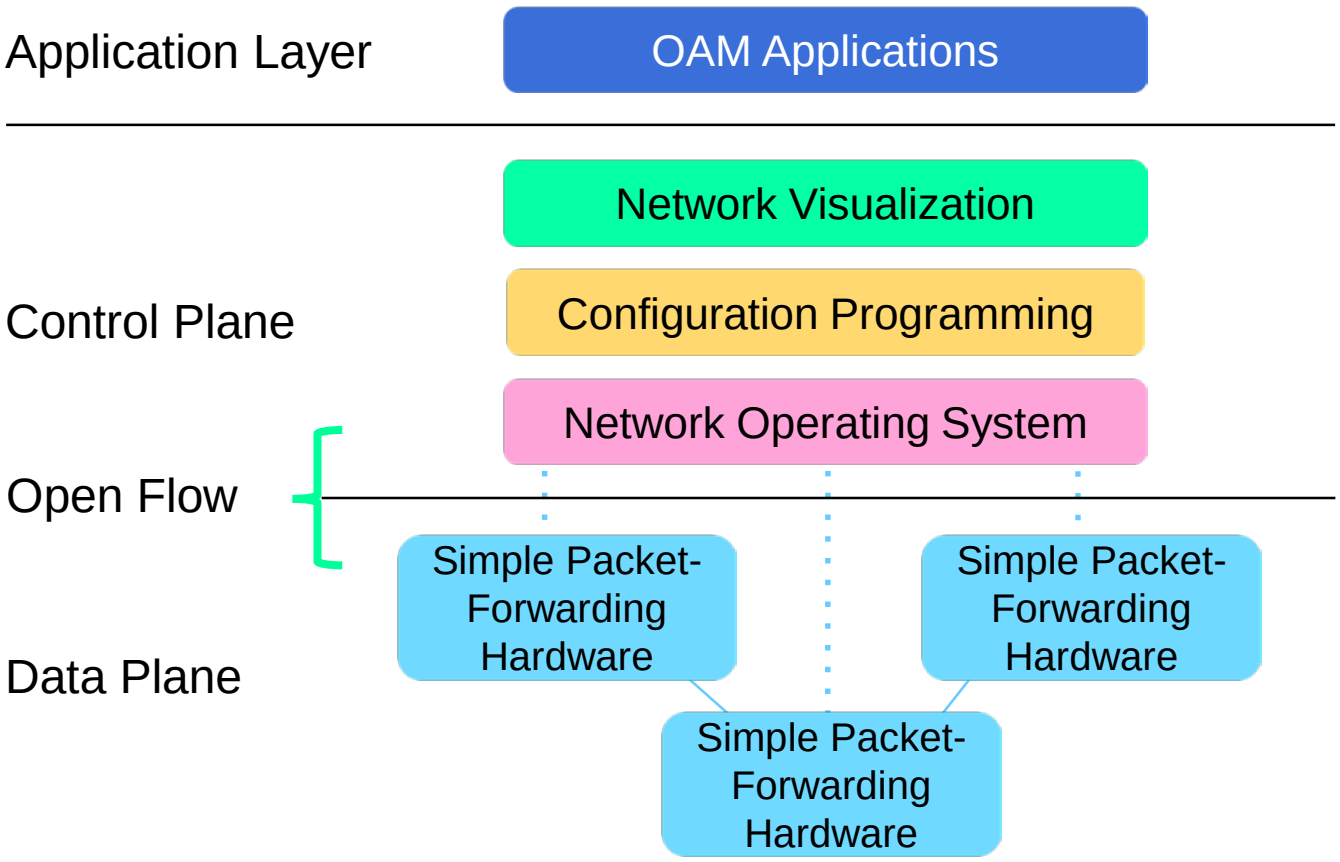
Individual Control and Data Planes

Software-Defined Networking (SDN) Switch

Centralized Control Plane, Individual Data Plane



Introducing SDN and OpenFlow

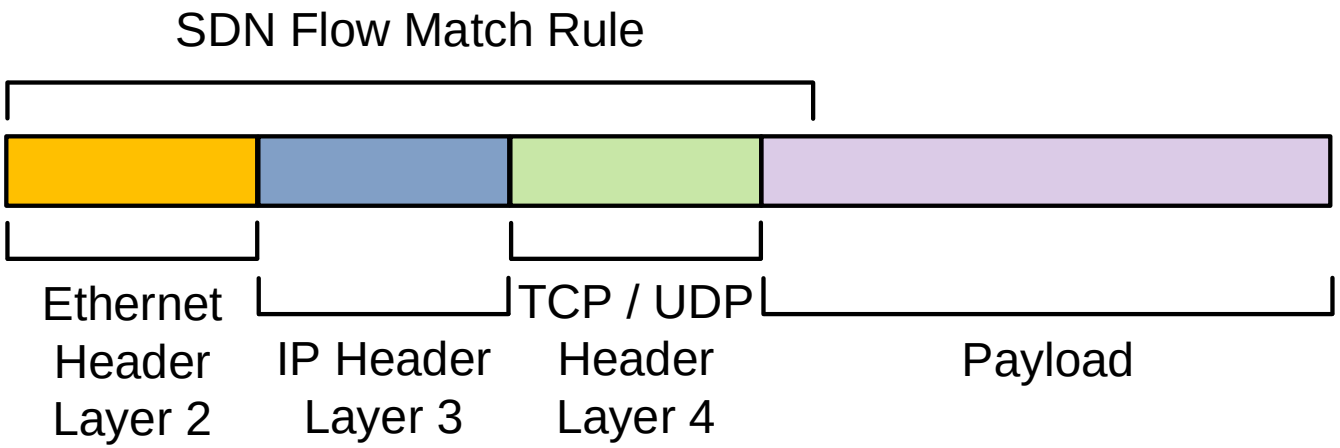


How SDN Works

Data plane inspects each Ethernet packet
and performs one or more

- Match fields – match rule based on first 4 layers of the Ethernet packet
- Instructions – perform one or more programmed actions
- Counters – increment counters and send counter data to centralized point

Multilayer Match Rules Forward Packets

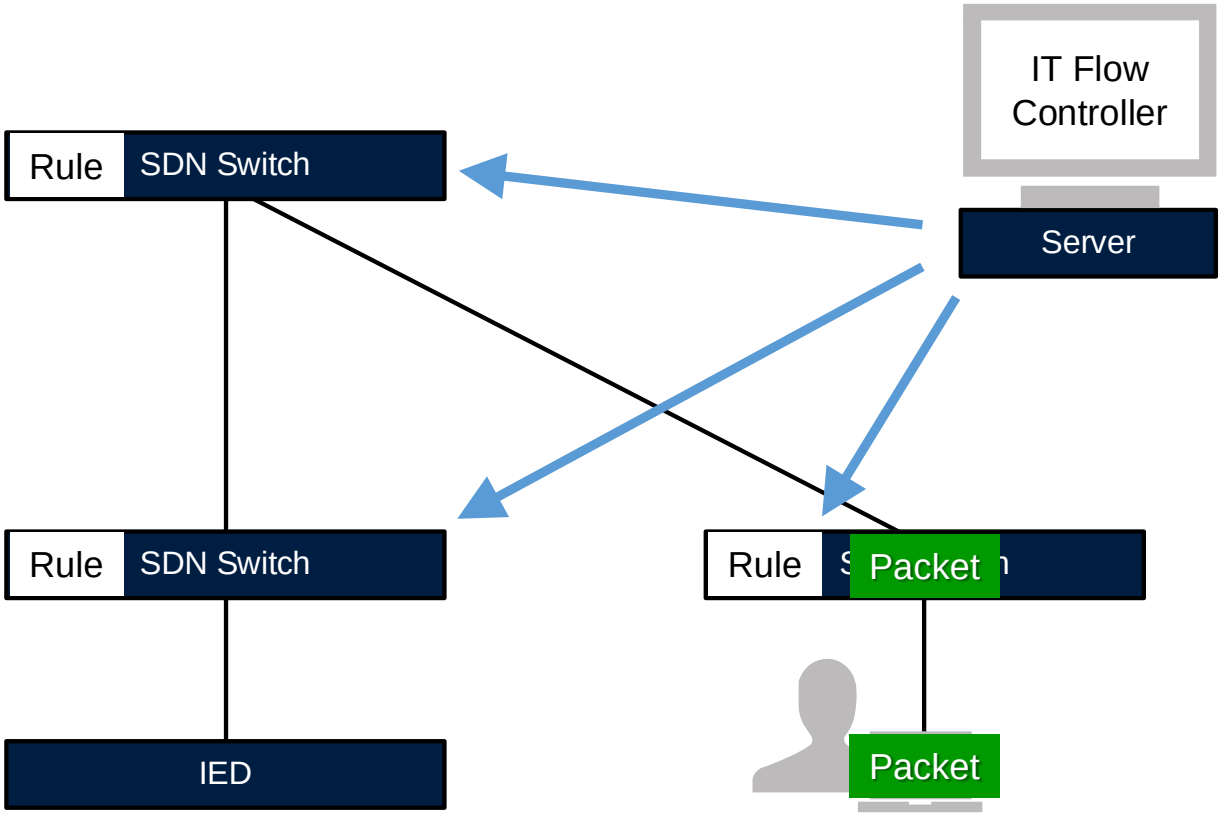


OTSDN vs Traditional SDN

Static vs Reactive Flows

- Traditional SDN uses reactive flows to dynamically respond and adapt to changes in the network and traffic
  - Focus is on bandwidth utilization and latency rather than determinism
  - Continuous learning and flow management
  - Uncertain network performance at any given time
  - SDN Controller performance bottleneck

Reactive IT SDN in Operation

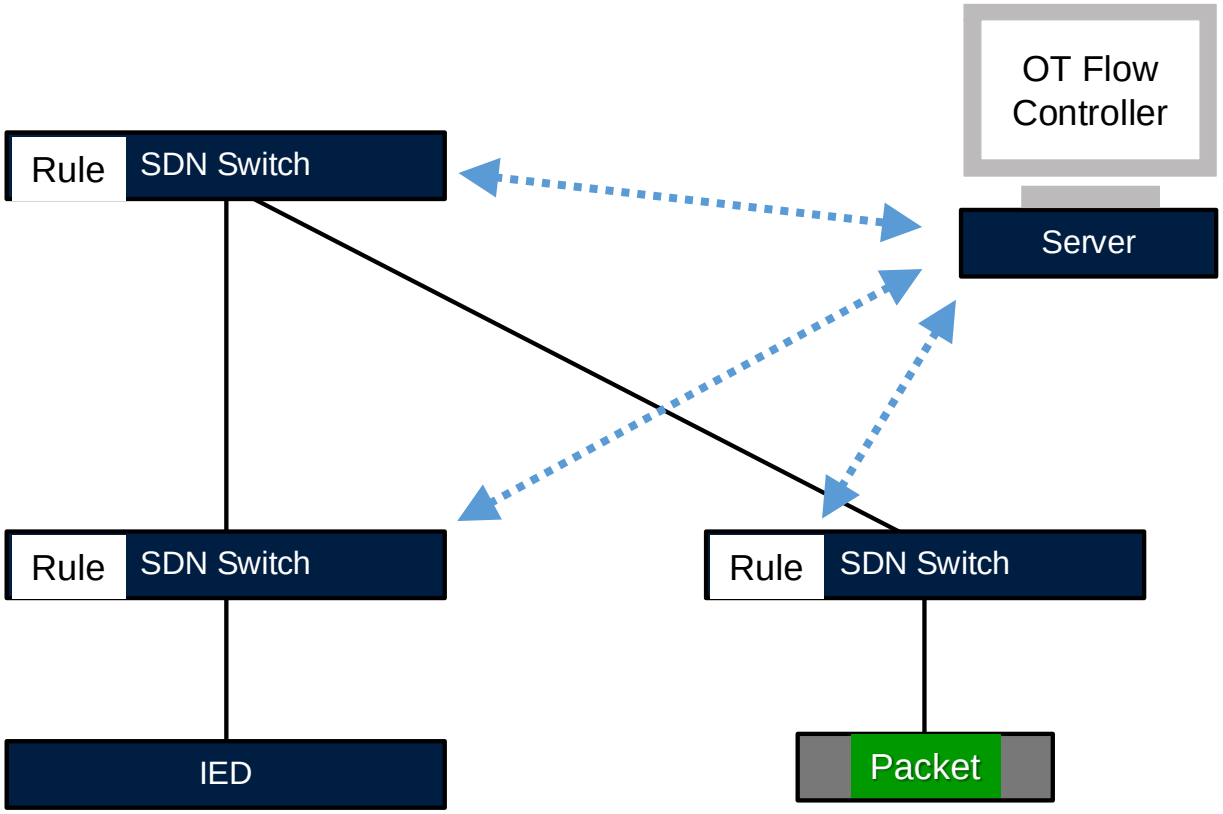


OTSDN vs Traditional SDN

Static vs Reactive Flows

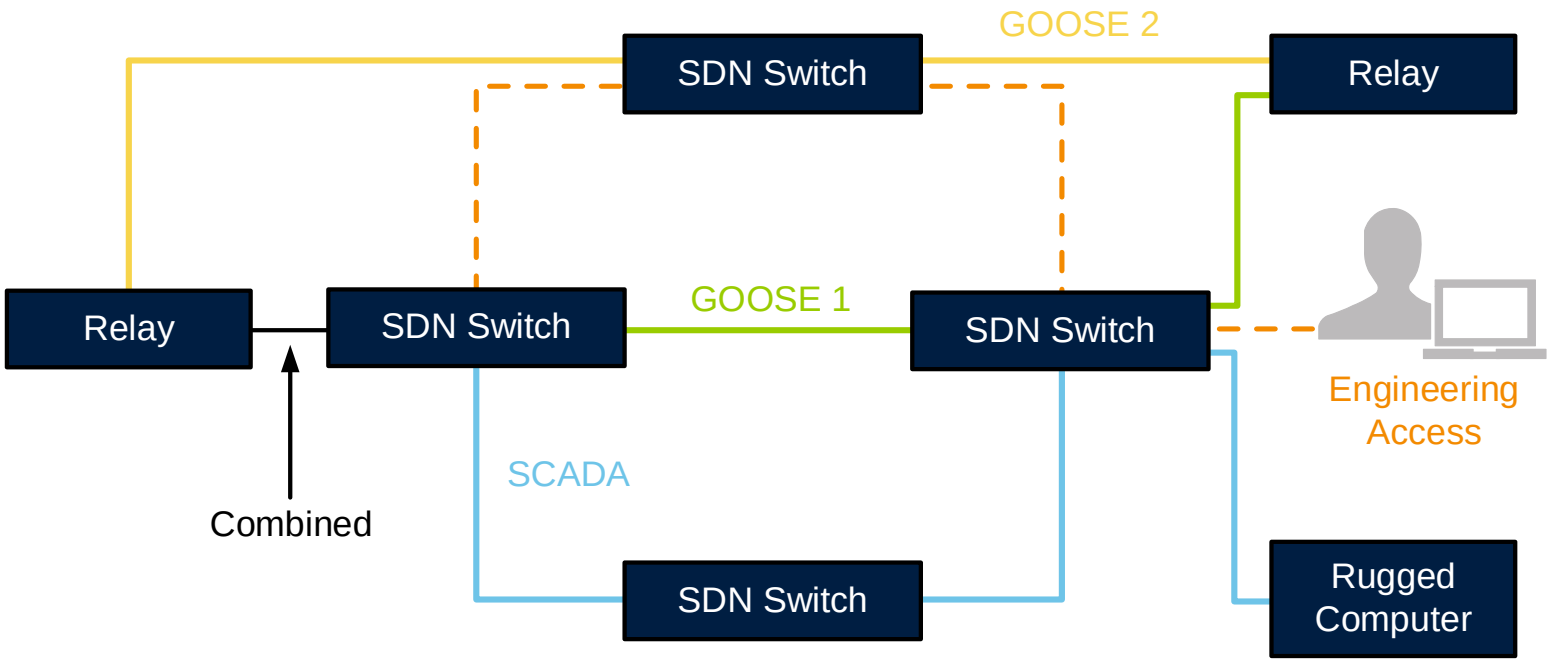
- OTSDN is uses static flows for proactive engineering of known network configuration
  - Static flows can be used because all traffic is known
  - Networks never have new traffic or devices without official change order
  - New or unexpected traffic will be dropped
  - Network state and performance is always known and as designed

Proactive OT SDN in Operation



Design Traffic Where Paths Are Based on Requirements and Applications

Flow Controller Is Not Required for Network Operation



OTSDN - Cybersecurity at Every Network Hop

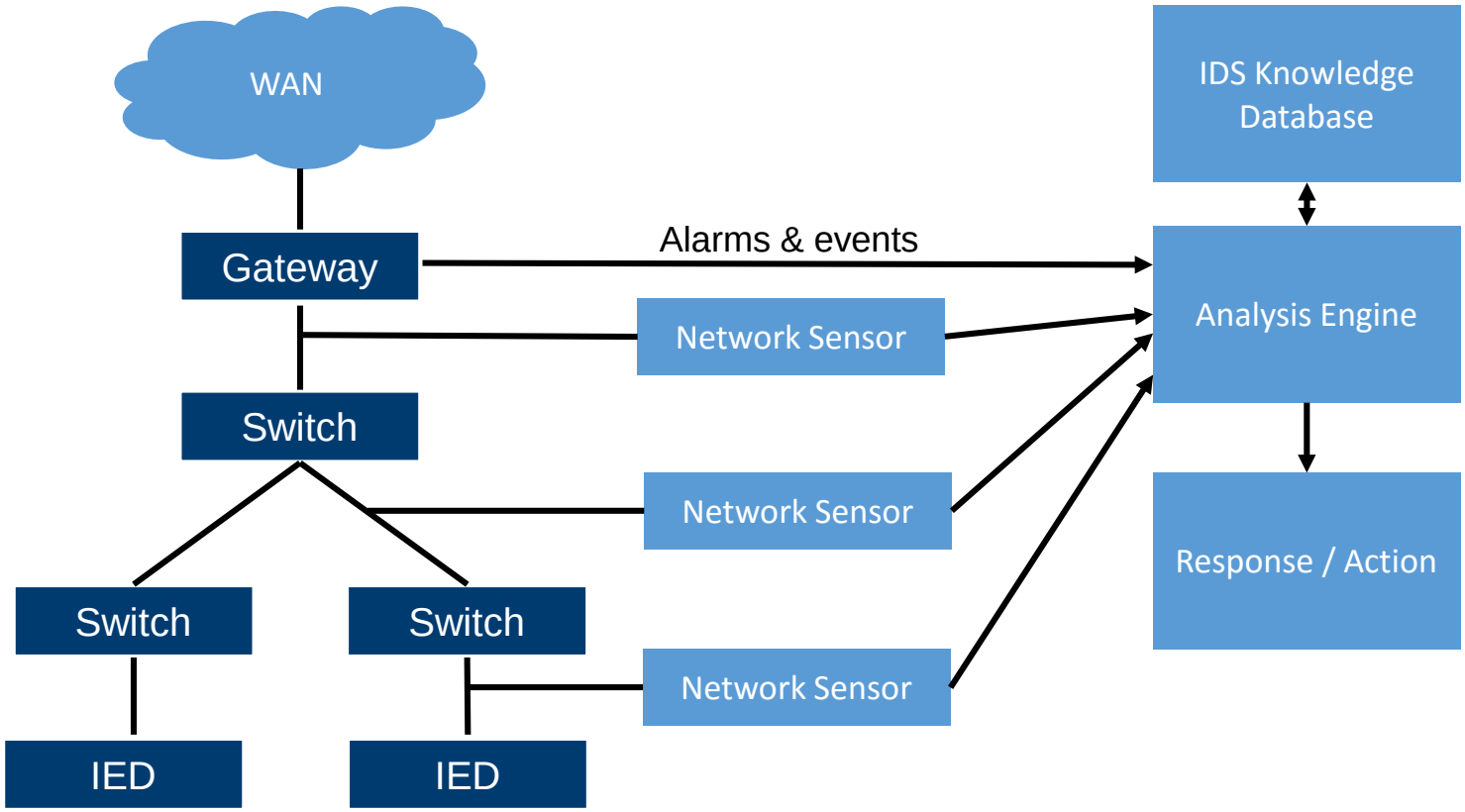
- Only allow traffic that is required and only to the places it is needed.
  - No ARP Cache poisoning
  - No Broadcast storms
  - No BPDU attacks
- Hosts only see traffic for destined them and nothing else

No traffic injection from unexpected locations

- Locked down flows restrict what traffic is allowed on the network at every point
- Spoofing a device MAC/IP address is difficult
- Packets that match flow rules must originate from predetermined location.
- Any attempt to spoof a device from an alternate location raises alert and tracked

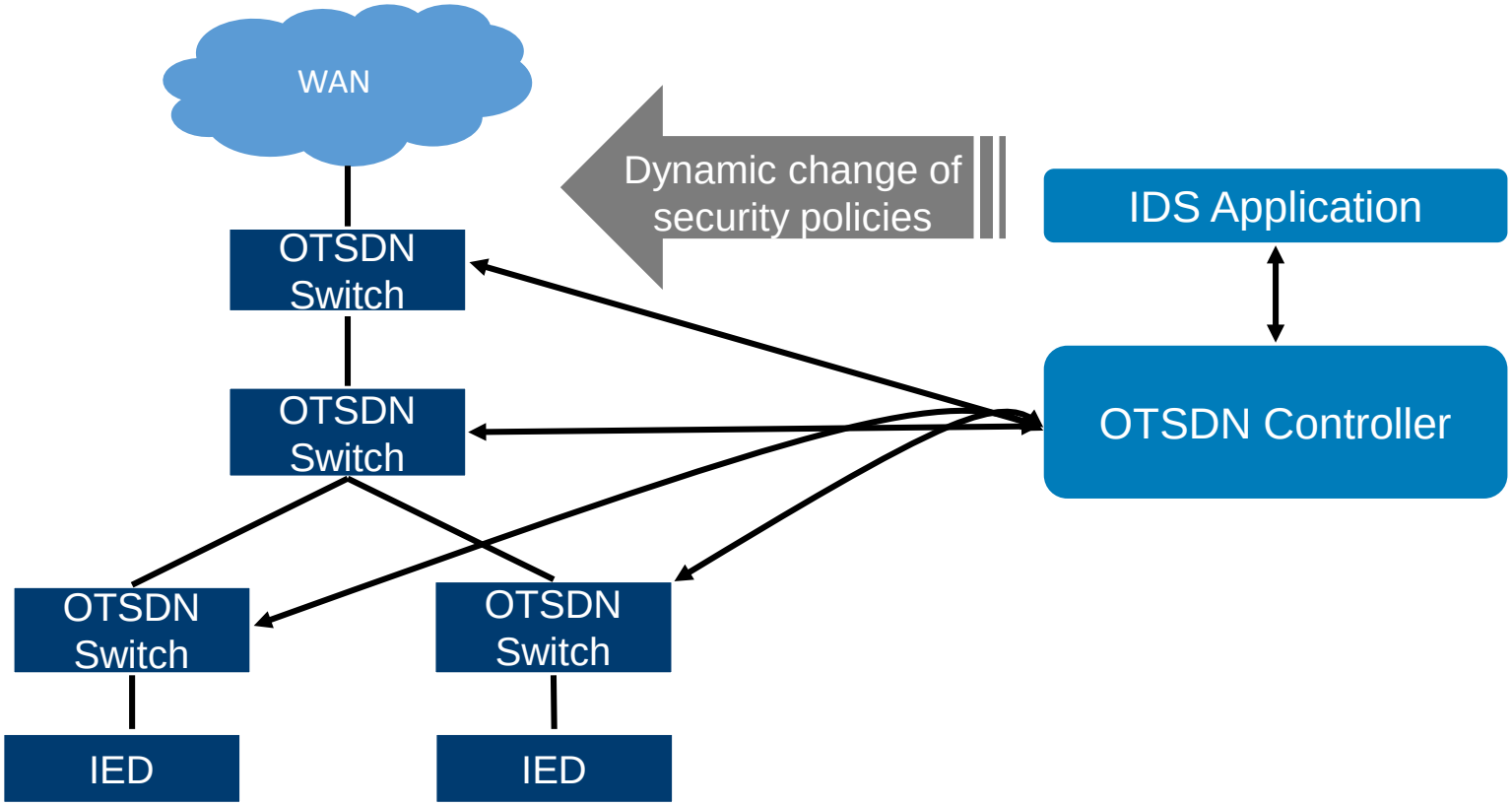
Traditional Intrusion Detection System

External with Slow Action Response



OTSDN Intrusion Detection System

Integrated With Fast Dynamic Response



Targeted IDS

- All needed traffic is engineered to go where it is needed
- Any unmatched traffic can be easily be discarded or sent to an IDS
- IDS will ONLY see the traffic that was not already engineered
  - IDS will be burdened much less than watching all traffic
  - More scrutiny can be given to this unwanted traffic

Targeted Deep Packet Inspection

Focus DPI processing only where it is needed

- Individual Flow(s) from individual switch(es) can easily be sent to a DPI processor.
  - The DPI process can determine if the packets should be allowed on the network.
  - If allowed, send it back to the OTSDN switch for further processing, otherwise drop/log.
- Reduces burden on the DPI device by only processing the chosen stream of data.

Conclusion

- OTSDN is standard technology with different methodology
- Purpose engineered networks allow deny-by-default cybersecurity at every hop in the network
- Deterministic failover with traffic metrics
- New approach to IPS, IDS, and DPI
- Multipath capable / Application based circuits
- Controlled change management and network access

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

http://cred-c.org

@credcresearch

facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security