MOSAICS
2020
INDUSTRY
DAY

SEL

Securing FRCS with OT SDN

Simplified
DESIGNING
& TESTING

DENY-BY-
DEFAULT
Access Control

Less Than
100 µs
Failover Times

Centralized Network
VISIBILITY &
DIAGNOSTICS

<u>What is OT SDN?</u>

1. Designed specifically to meet FRCS Ethernet requirements
2. Think of it as a networking Remedial Action Scheme
3. Communication flows must be traffic engineered
4. “Stateless” Firewall ACL on the network level
5. Complete control over packets on the LAN

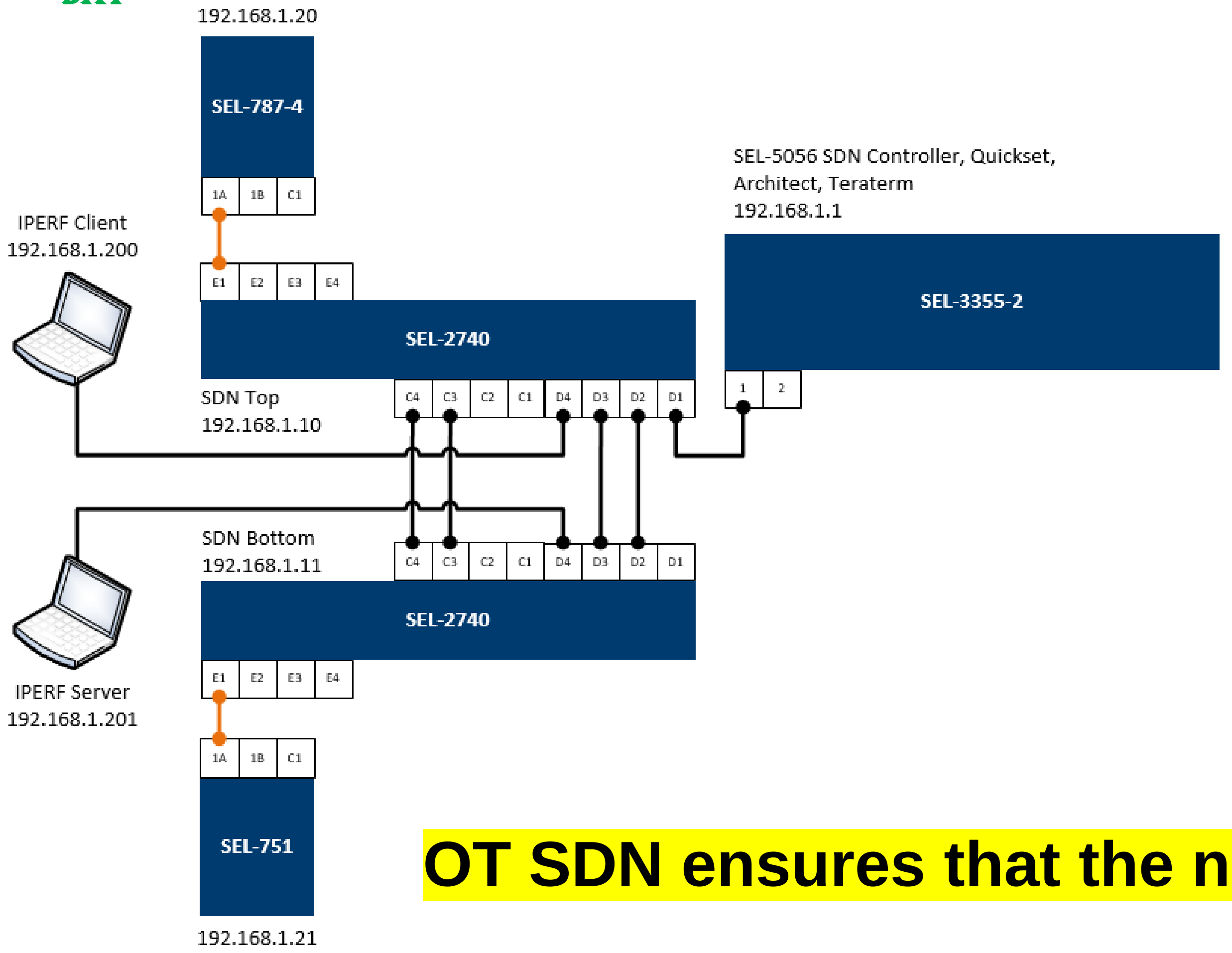
<u>Why OT SDN for FRCS?</u>

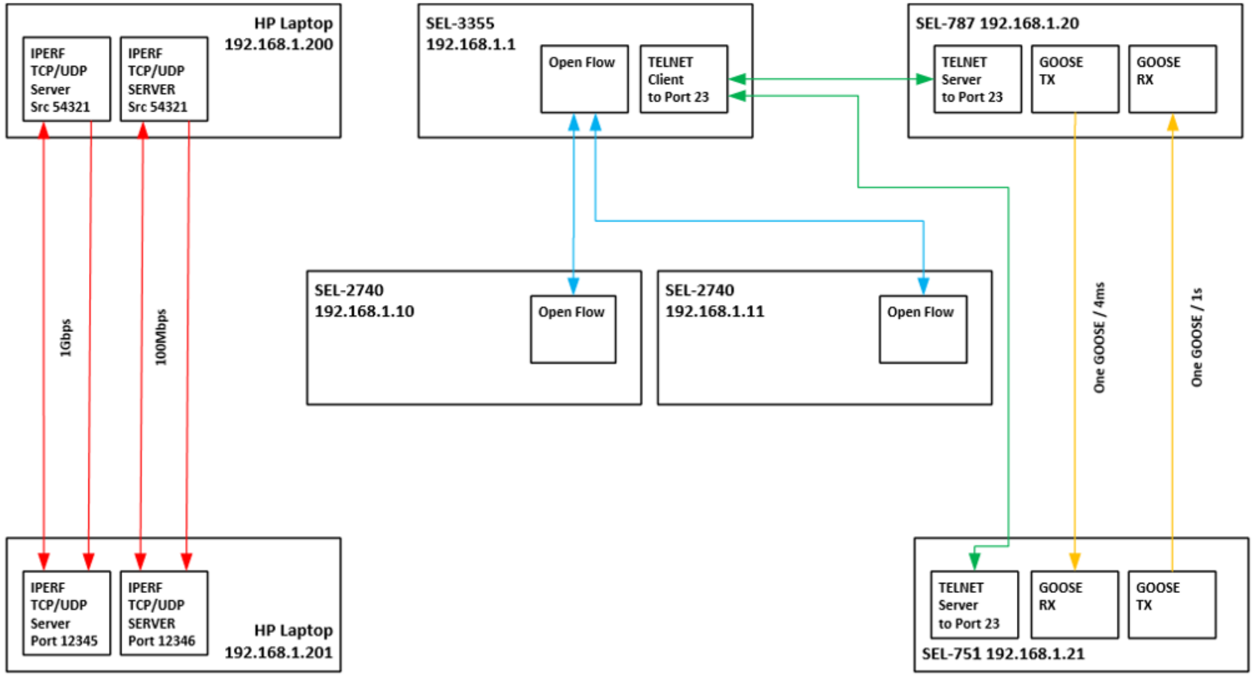
1. Ethernet spec'd, designed and purposed for Control Systems (Security and Performance)
2. Fully interoperable with legacy networks
3. Built and tested to exceed harsh environmental conditions

MOSAICS
2020
INDUSTRY
DAY

Network Diagram + Dataflow Diagram
=
Baseline & Asset Management

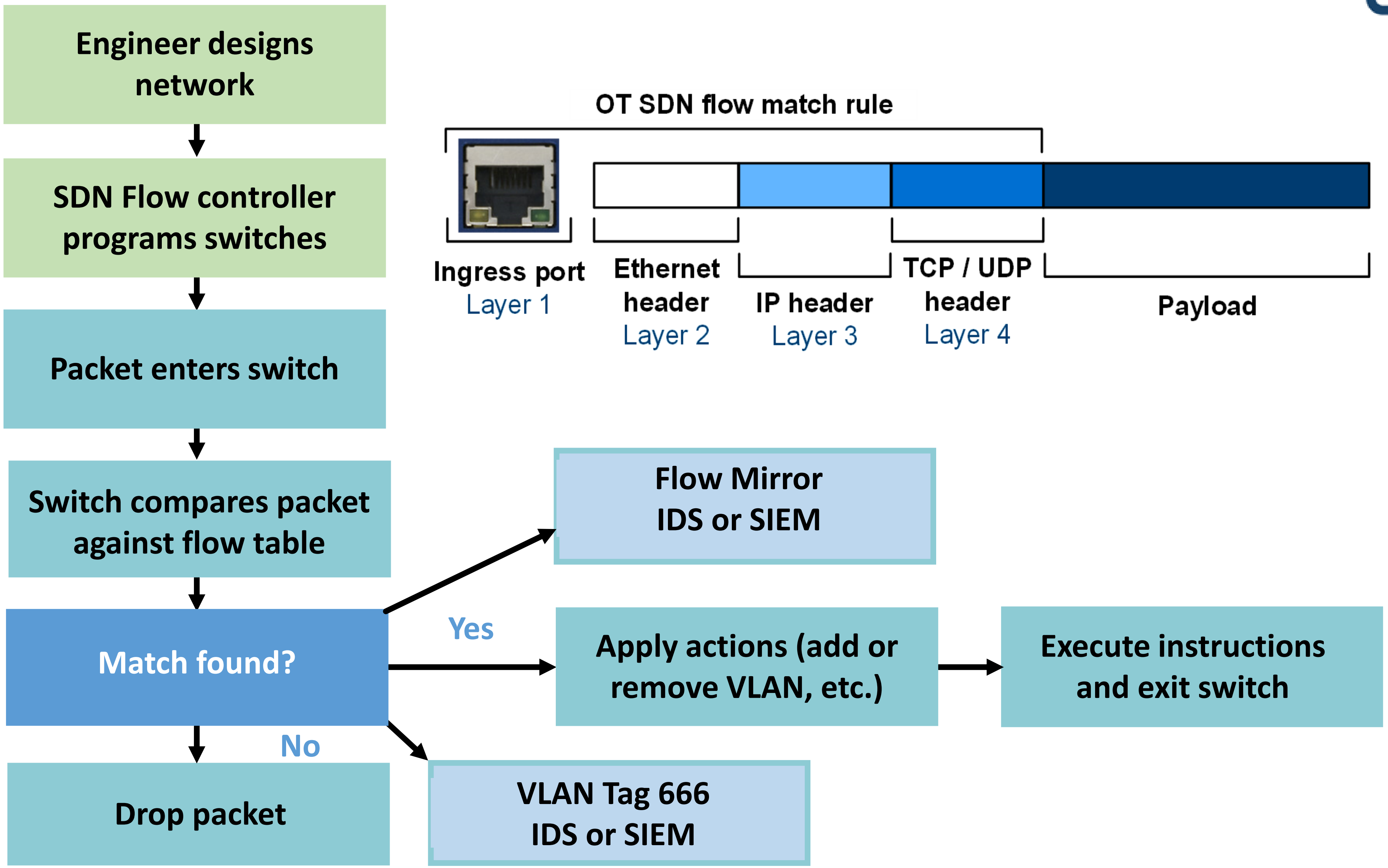
SEL





OT SDN ensures that the network enforces plans and policy!

How OT SDN Works



Engineer designs network

SDN Flow controller programs switches

Packet enters switch

Switch compares packet against flow table

Match found?

Yes

Flow Mirror IDS or SIEM

Apply actions (add or remove VLAN, etc.)

Execute instructions and exit switch

No

Drop packet

VLAN Tag 666 IDS or SIEM

OT SDN flow match rule

Ingress port Layer 1

Ethernet header Layer 2

IP header Layer 3

TCP / UDP header Layer 4

Payload

MOSAICS
2020
INDUSTRY
DAY

Current FRCS Network SITREP

1. FRCS on siloed networks

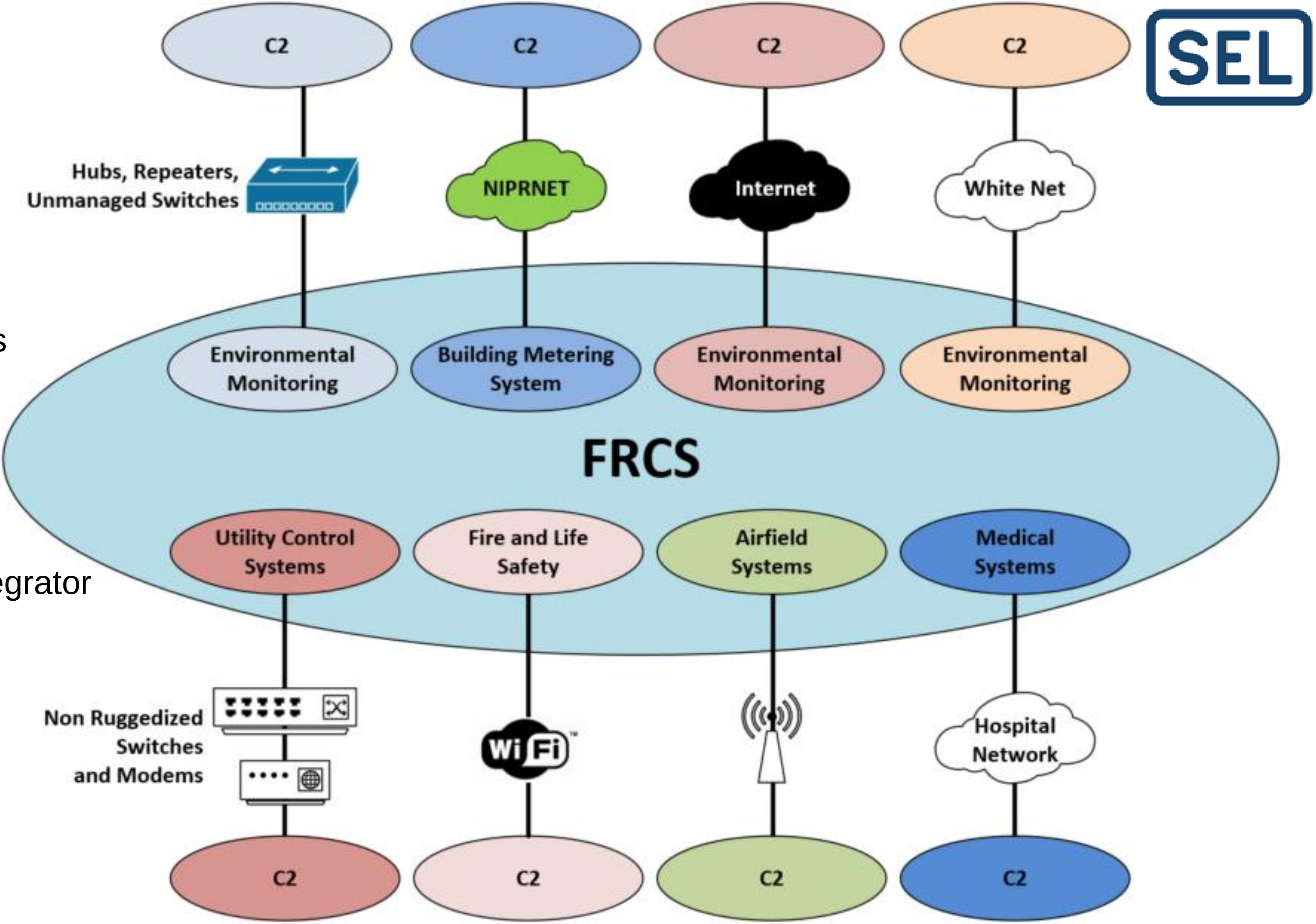
2. No baseline (ND + DFD)

3. Little ability to monitor

4. Remote Access from Integrator

5. No system owners

6. Myriad of aging networks



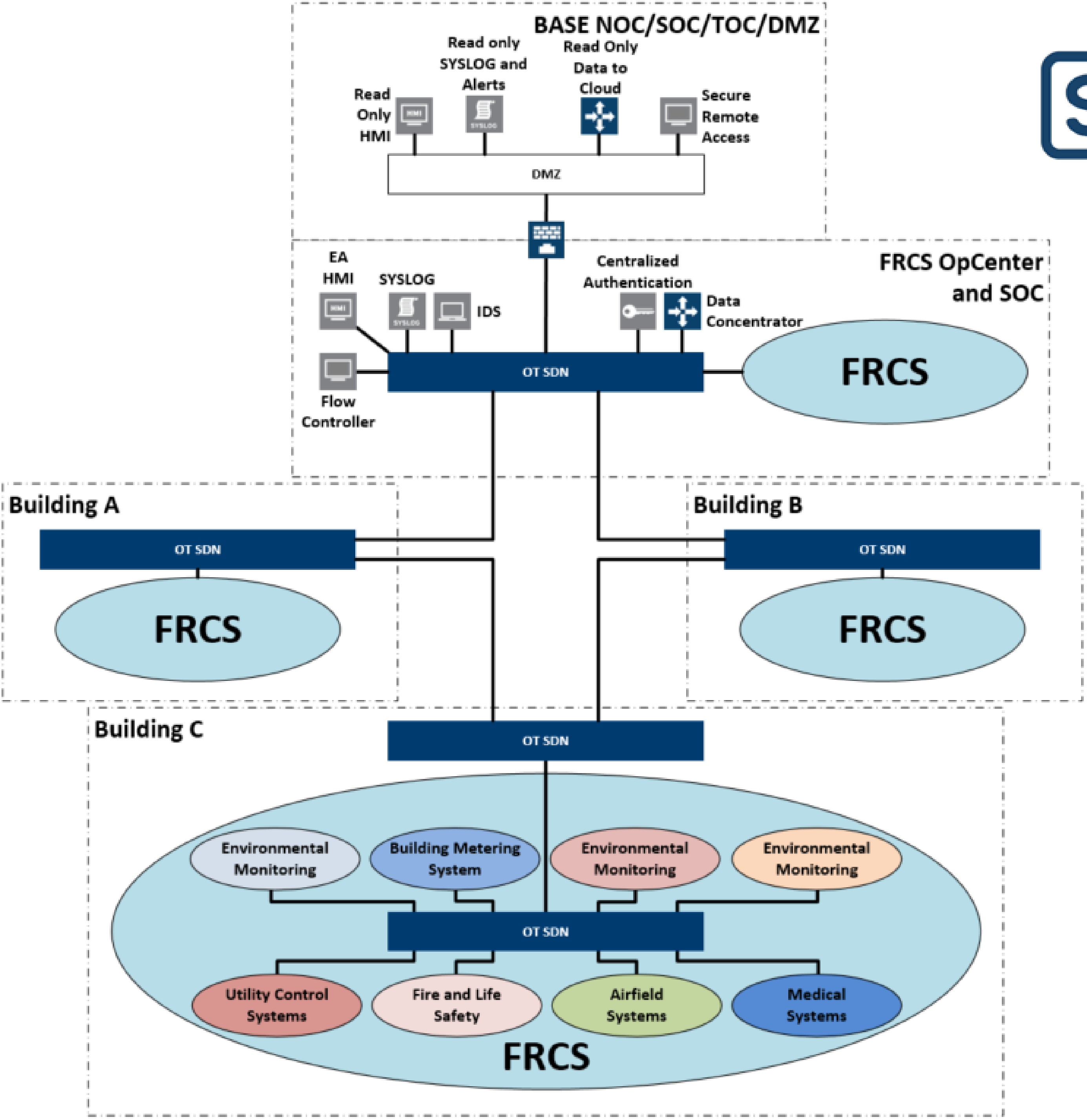
SEL

MOSAICS
2020
INDUSTRY
DAY

Future FRCS Networks with OT SDN

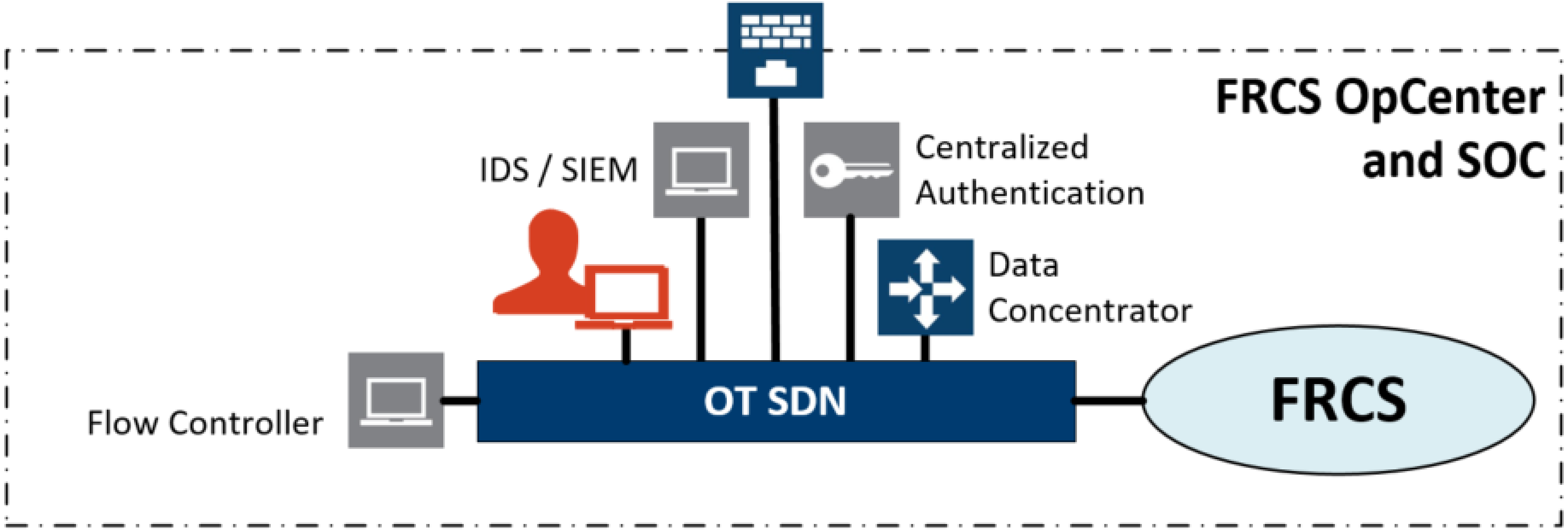
SEL

1. Provide a single FRCS network
2. Significantly save physical infrastructu
3. Deny by Default & Flow by Flow contro
4. Reduced complexity
5. Centralized Authentication
6. Secure Remote Access
7. Visibility to all FRCS devices
8. Integrates all FRCS into a single IDS and SIEM
9. IEEE 1613 environmentally hardened



Pivoting or Enumeration

- Adversary “lives off the land” and gain access to HMI/EA System
- OT SDN telemetry and diagnostic data monitor on a flow by flow basis
- Adversary must enumerate network to discover additional targets
- Any traffic that does not match flow rules is sent to IDS/SIEM
- Any new device’s gratuitous ARP is sent to IDS/SIEM



MOSAICS
2020
INDUSTRY
DAY

SEL

Current OT SDN Wayahead

1. DISA APL Spring 2021
2. Site ATO pending for Project Level (40 plus buildings with microgrid)
3. Pilots on 4 bases + 1 Veterans Hospital
4. Pilots turning into projects for major control system owners
5. Integrators creating their own tools to increase their implementing capacity

Tim Watkins

Tim_Watkins@selinc.com

Office 509.336.4429 Cell 509.592.3546

Dennis Gammel

Dennis_Gammel@selinc.com

Office 509.336.7981 Cell 509.592.3546