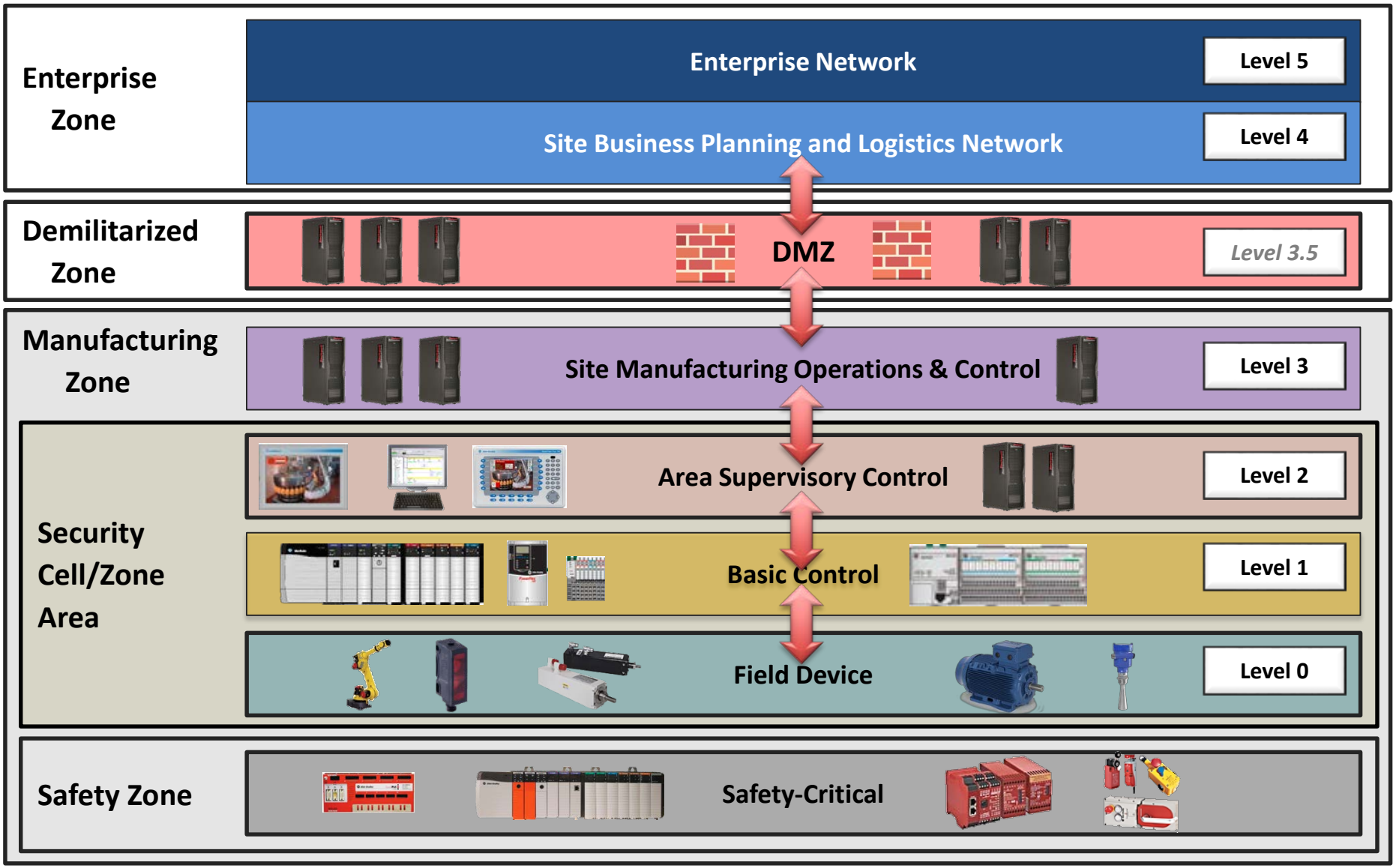
VERACITY

Cybersecurity for the New Industrial Network

One Platform. Complete Visibility. Total Control.

REVIEW OF INDUSTRIAL CONTROL SYSTEMS (ICS)



SEGMENTS FOR INDUSTRIAL CONTROL SYSTEMS

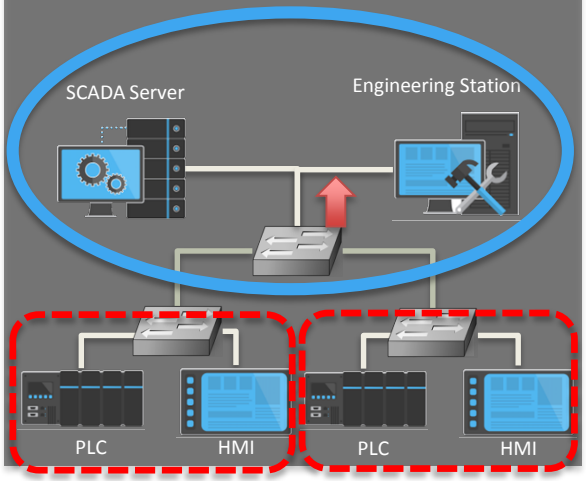
COMMONALITIES

- Long Life Cycles
- M2M Communication
- Protocols
- Deterministic Communication
- Vendors/Devices

INDUSTRIAL NETWORK SECURITY CHALLENGES

VISIBILITY

Unknown connected assets, active scanning not an option

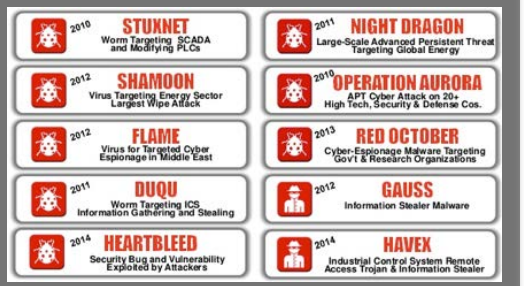


COMPLEXITY

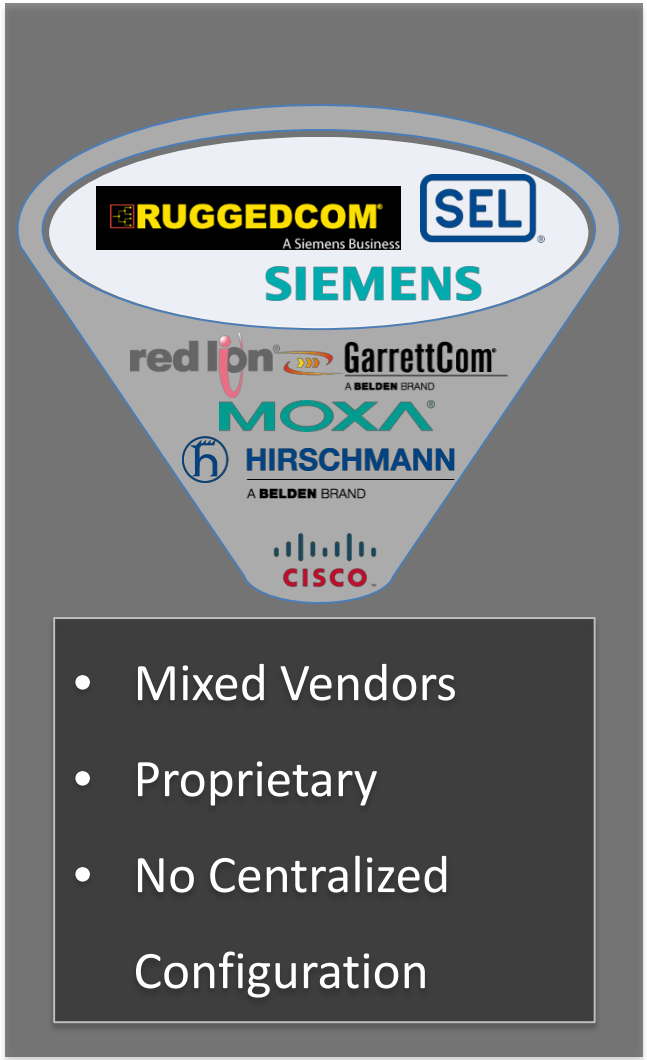
Long life cycles/mixed mode architectures, Lack of SME's

RISK

Insider: Misconfiguration/Misuse and Emerging and targeted threats



INDUSTRIAL NETWORKING CHALLENGES

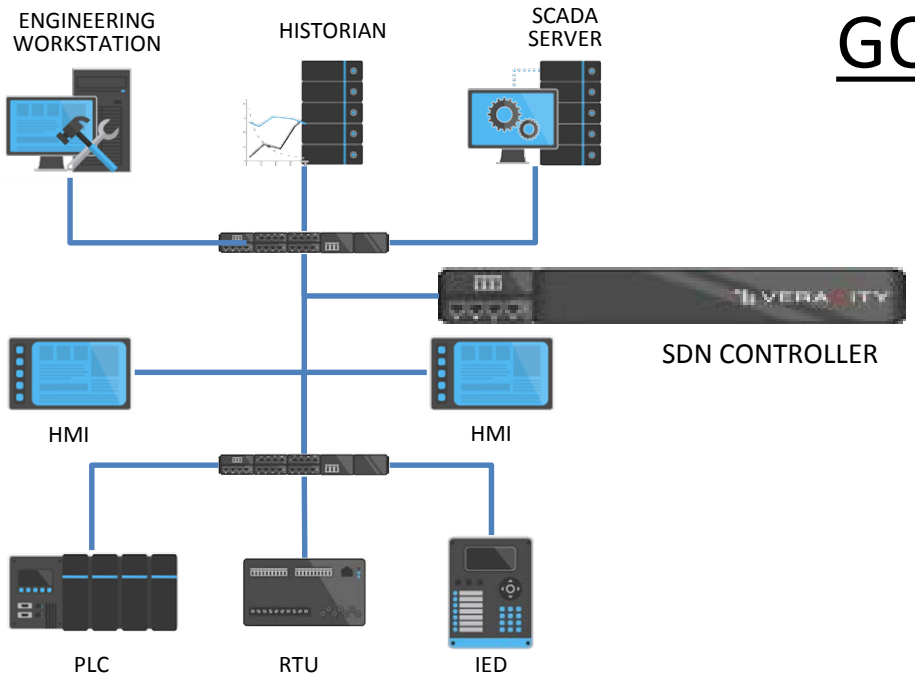


- Network Operational Requirement at Odds with Cybersecurity Needs
- Limited Security Controls at Switch (e.g. ACL, Enable/Disable Port, etc.)
- Little to No Auditing of Configurations
- Network Misconfigurations are Common
- Industrial Redundant Protocols/Ring Topologies Increase Complexity

GOALS TO ADDRESS IDENTIFIED PROBLEMS

Problem	Convergence Solution
IT vs. OT	System to enable real-time peer review configuration changes between IT & OT
NW vs. Cybersecurity	System that unifies network orchestration and cybersecurity policy
DiD vs. Design based upon Threat	System that enables DiD best practices/standards of segmentation/security zones BUT, designed for different threat levels to the system
Lack of OT Cybersecurity SME's	• System that SIMPLIFIES network configuration and orchestration. • System that SIMPLIFIES cybersecurity policy.

SOLVING THE NETWORK VISIBILITY PROBLEM



GOAL: Situational Awareness

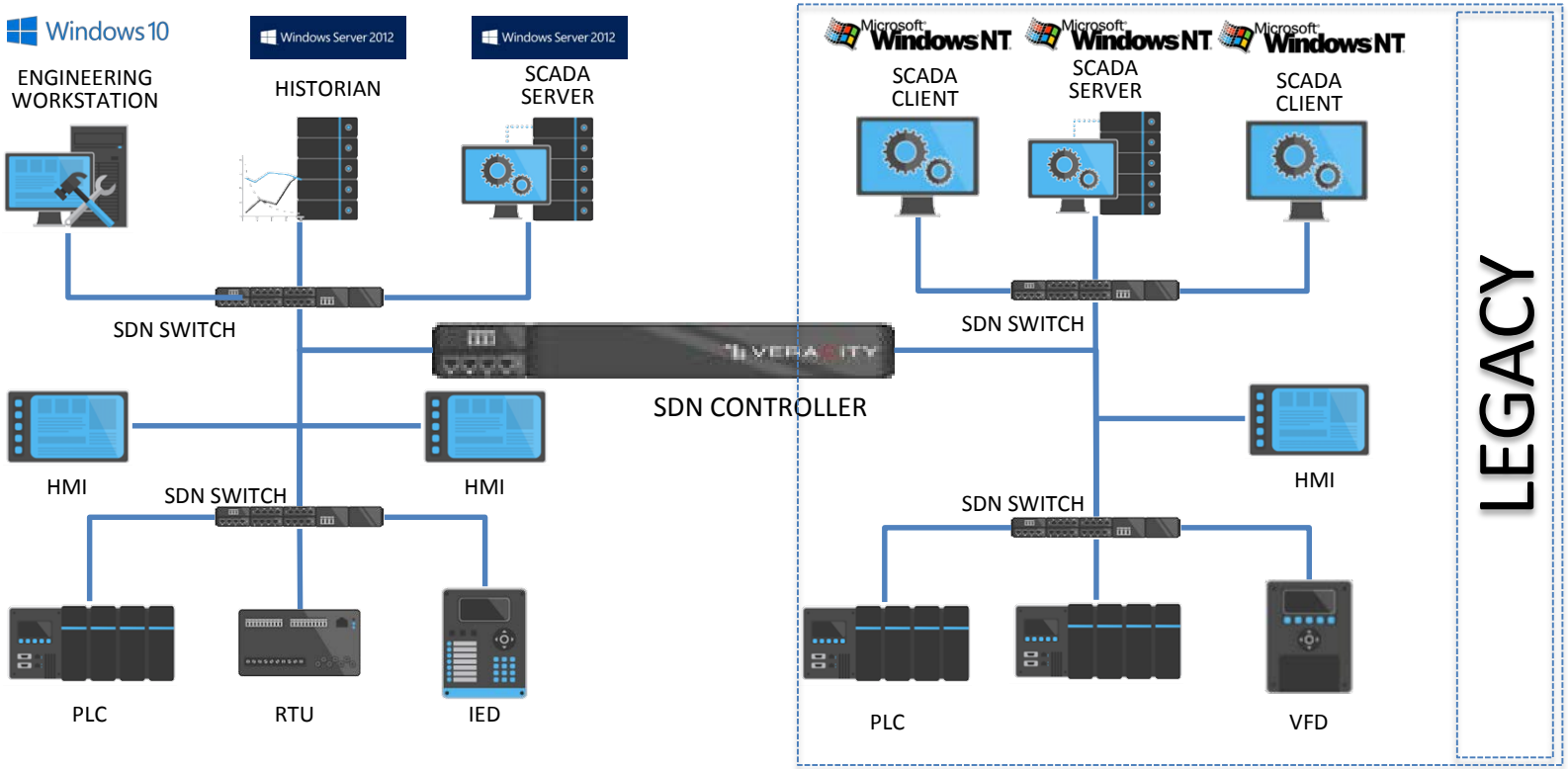
LEARNING MODE

- Node captured (e.g. MAC/IP)
- Communication Partners Captured (e.g. PLC <-> HMI)
- Conversation Captured (e.g. Protocol Type)
- Characterization & Classification of Node Type (e.g. PLC, HMI, etc.)
- Generation of Signature for each networked node based upon attributes of device and communication

HISTORICAL DATA

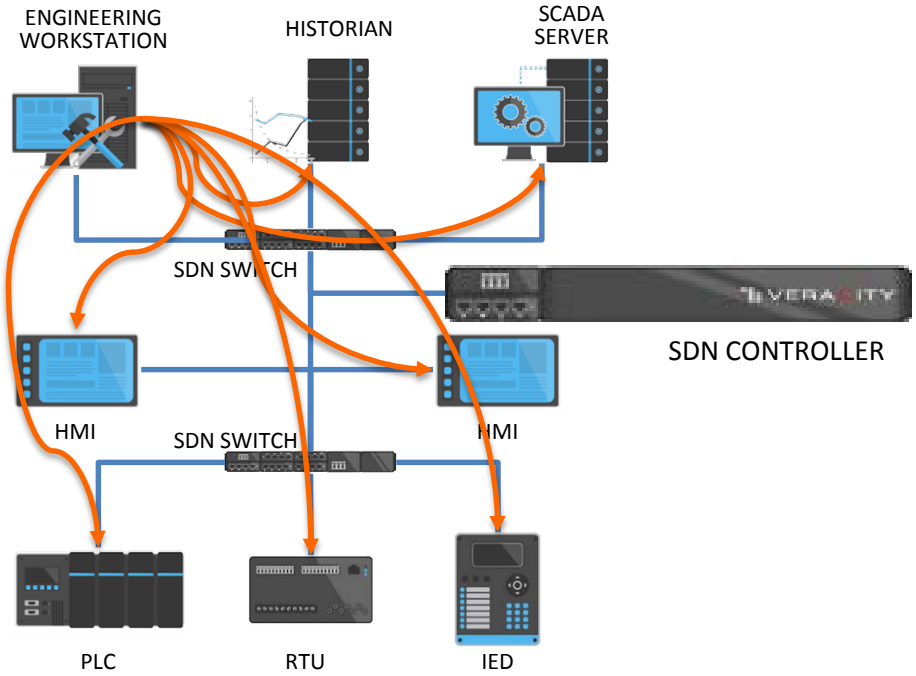
- Every device, every communication request and every protocol request stored in long term data store
- Communication Partners Captured (e.g. PLC <-> HMI)
- Conversation Captured (e.g. Protocol Type)

SOLVING THE LEGACY/MIXED MODE ENVIRONMENTS PROBLEM



- Whitelisting of allowed communications
- Classification & Prioritization of Messages (Protocols)
- System generated “Flows” for shortest path/load balanced (based upon MsgClass/Security Policy)

IDENTIFICATION OF COMMUNICATION BEHAVIORS



Config Learning Mode:

- Isolation of conversation types
- Configuration changes dropped by default
- Allows authentication, authorization and access even for insecure legacy devices
- Full traceability of all configuration changes for IR support

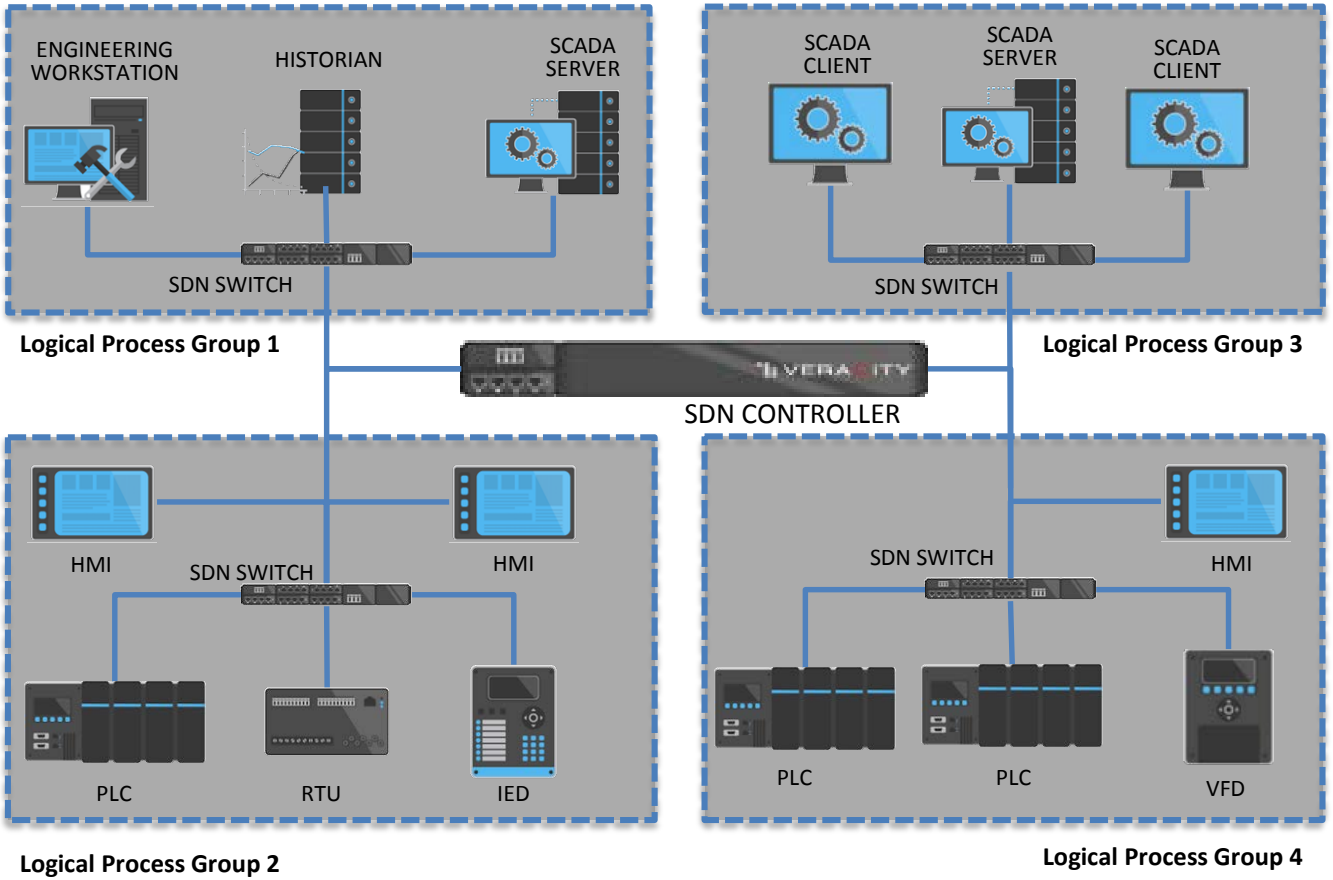
- Protocol identification
  - Identify OpCodes/Function codes used in conversation between devices
  - Establish conversation/network baseline
  - Identify “Runtime” conversations from “Engineering/Configuration” conversations

Future Experiments

- Identify/Record time based OpCodes for discrete processes
- Identify/Record related and sequential OpCodes for continuous processes

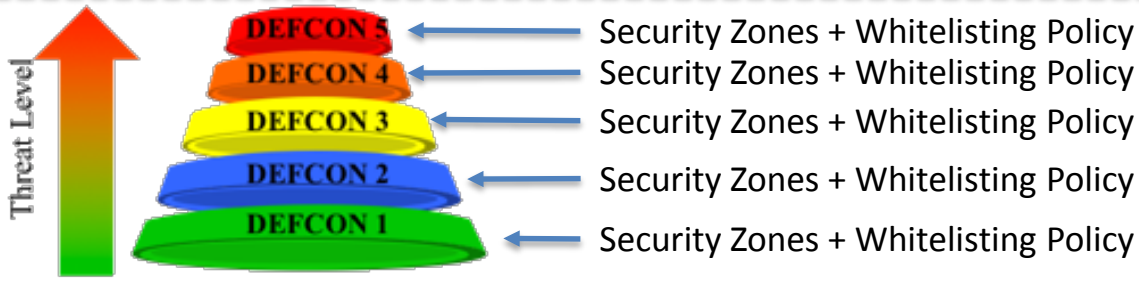
Create Behavioral Models

PROGRAMMABLE SEGMENTATION & ZONE/ENCLAVES



Learning Mode:

- Generate Logical Process Groups
- User Defined Sub Zones
- Communication Across Zones Encrypted (Src egress/Dst ingress)



GOAL: DEFCON 5 – Most Restrictive/Ensure Mission Critical Function Only

FOUNDATIONAL PLATFORM ENABLEMENTS

- FOLLOWING ARE USE CASES THAT ARE ENABLED BY THE PLATFORM

PROVIDE A NEW PARADIGM FOR DETECTION

Detect network mapping/scanning techniques

- E.g. send false IP used addresses in response to ARPScan
- E.g. send false OS information in response to OS fingerprinting

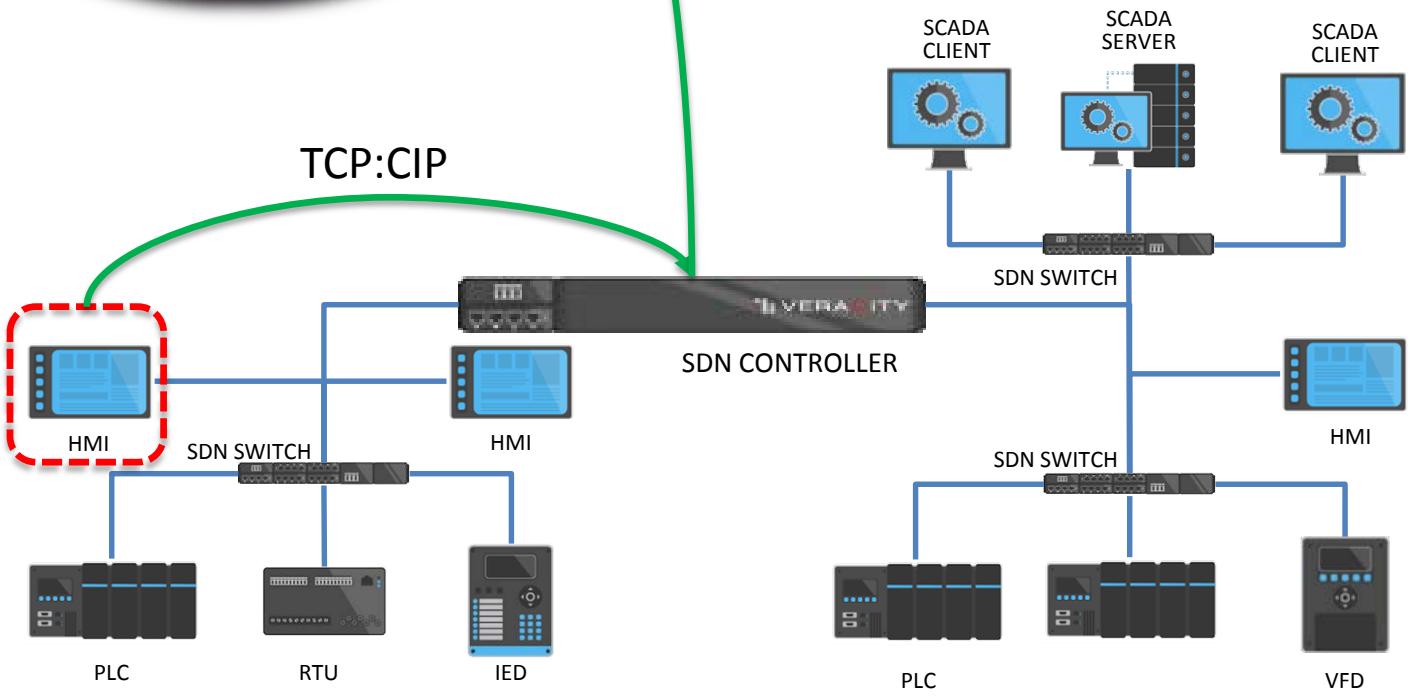
VERACITY

Current Security Control Focus

Recon
Weaponize
Deliver
Exploit
Install
Command & Control
Action on Objectives

PROVIDE ON DEMAND IR REMOTE IR SUPPORT

- On demand request for filterable network streams for analysis
- Remediation capabilities (e.g config/policy)
- Historical configuration changes of policy
- Historical comparison of all network changes



MACHINE LEARNING FOR CYBER PHYSICAL SYSTEMS

- SIMULATION SYSTEM FOR ICS NETWORKS
  - Mininet
  - Industrial Virtual Switch
  - Python simulators for Industrial Protocols (ModbusTCP, CIP, DNP 3, GOOSE)

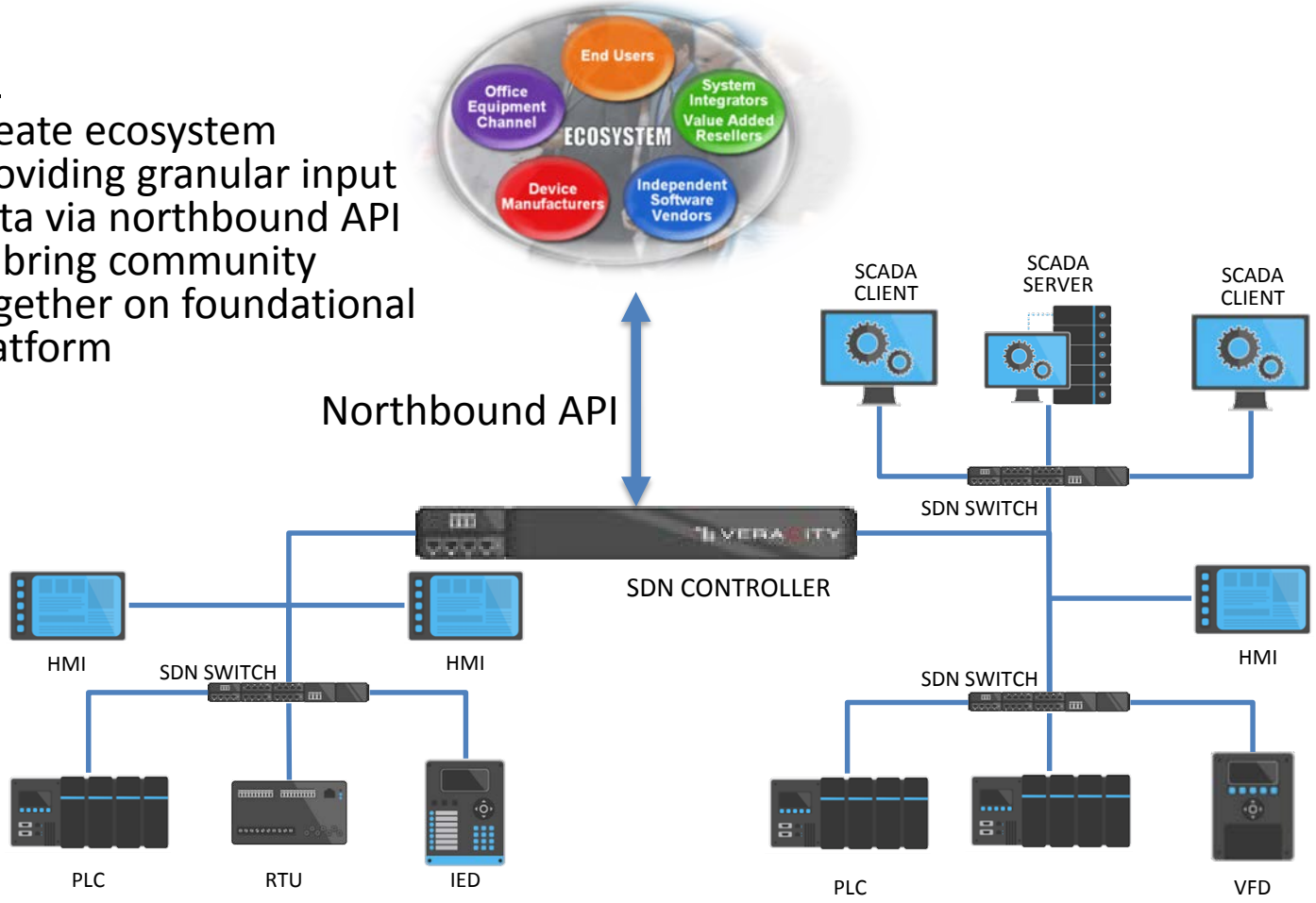
- GENERIC ICS PROTOCOL SIMULATOR FRAMEWORK
  - Extract all (good) communication sequences and put in data store
  - Industrial Virtual Switch
  - Develop generic simulator that can load any protocol and play selected message sequences
  - Generate data store based upon known malicious communication sequences

- MACHINE LEARNING TO DERIVE MODEL OF CYBER PHYSICAL SYSTEM/PROCESS
  - Creation of sandbox honeynet that models physical process but is obfuscated
    - ICS Communication simulator
  - Redirect adversaries to logical port into honeynet
  - Capture TTP's of adversary

OPEN NORTHBOUND API TO PARTNERS/CUSTOMERS

GOAL:

- Create ecosystem providing granular input data via northbound API to bring community together on foundational platform



- CHALLENGE:
  - Ensure the integrity of applications interfacing with the platform
  - Establishing trust and maintaining trust

Company Leadership

Savvy Veterans with 150+ Years Of Cybersecurity, ICS, SDN & Big Data Experience

PAUL MYER
CEO- Network Security

ROGER HILL
CTO – Industrial Networks

PANKAJ BERDE
CDO – Software Defined Networking

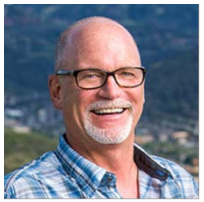
BILL GUERRY
CFO

Board

JOHN VIGOUROUX
Board

Steve Litchfield
Board

Advisors



Tom Bennett
Security CEO, Entrepreneur

ROBERT HUBER
Former President Critical Intelligence

ERIC COSMAN
OIT Concepts Co-Chair, ISA 99
Dow Chemical

Thank You For Your Time

One Platform. Complete Visibility. Total Control.