Operations and Control Networks Model

A Systematic Approach to Operational and Information Technology Convergence

Kiran Makhijani[*], Cedric Westphal[*], Mohit P. Tahiliani[ʒ],

Richard Li[*], Lijun Dong[*]
[*]Future Networks & Technologies Lab, Futurewei Technologies, USA
[ʒ]Dept. of CS and Engg. (NITK), Surathkal, Karnataka

Outline of the Talk

- Motivation
  - Similarity and Diversity in Process Automation Systems
- IT and OT Networks
  - Convergence and challenges with existing approaches
- Proposal – main contribution
  - Generalized Operation and Control Model
  - Supporting Technologies
- Case Study: Virtualized PLCs
- Discussion on Review Comments

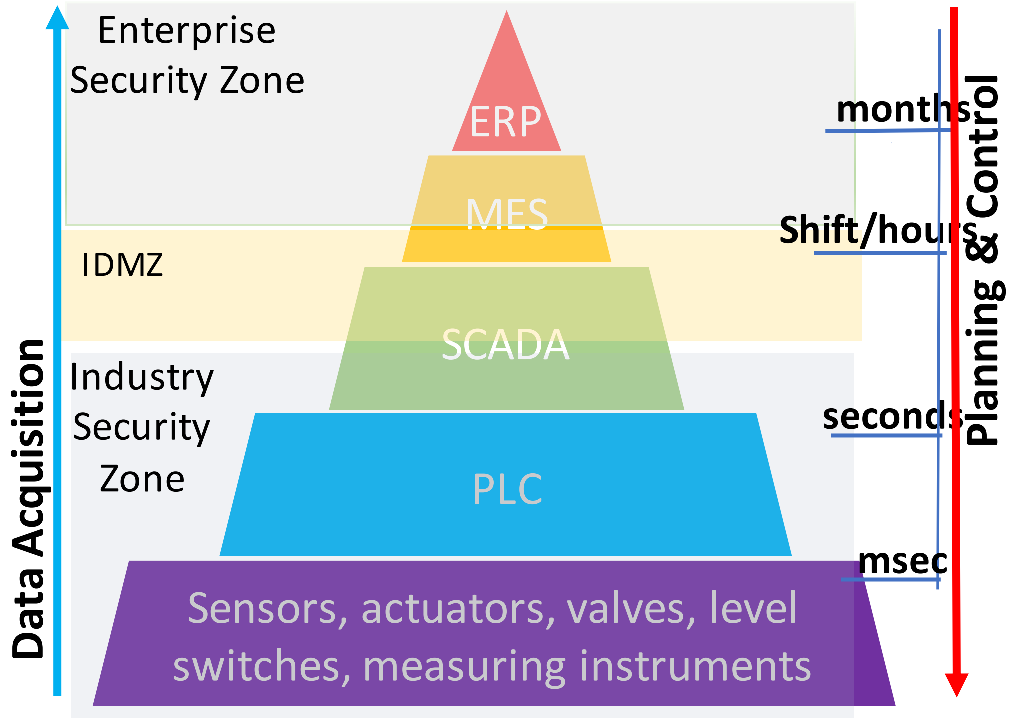
Once upon a time…

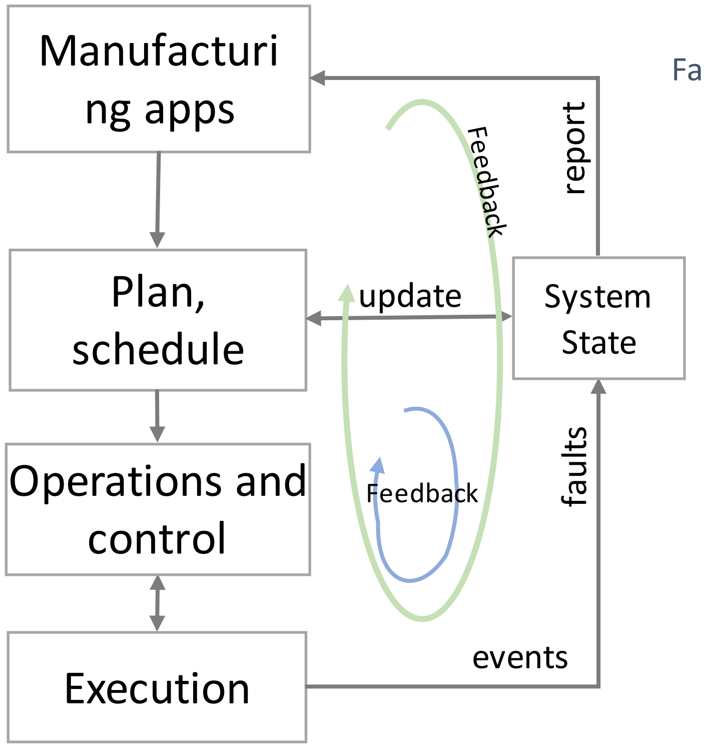
The story about the IT and OT Convergence continues…

- So far, the convergence of Operational Technologies and Information Technologies has been significant from the application's point of view.
- With an increasing support for software-based approaches and virtualization lines between the OT and IT components is becoming blurry.
- Often software to analyze the acquired data and decides to alter process control. This requires reliable, deterministic and lossless networks.
- Emerging integration of Internet of Things: They emit large volumes of short-sized data at regular intervals.

First Contribution: Describe the requirements from the networks in industrial automation applications without associating to a communication technology

Purdue Model - Architectural Limitations





Adopts Hierarchical Approach

3 separate zones, OT and IT zones separated by IDMZ.
Data will first get collected, batched and then sent to Enterprise zone.

Challenges that drive OCN Model and framework

Timescale Challenges:

Faster, manufacturing and customization cycles
Data Acquisition is slow – can't react fast enough

Operations Challenges:

Hierarchy prevents adapting to new infrastructures leveraging virtualization and compute intensive

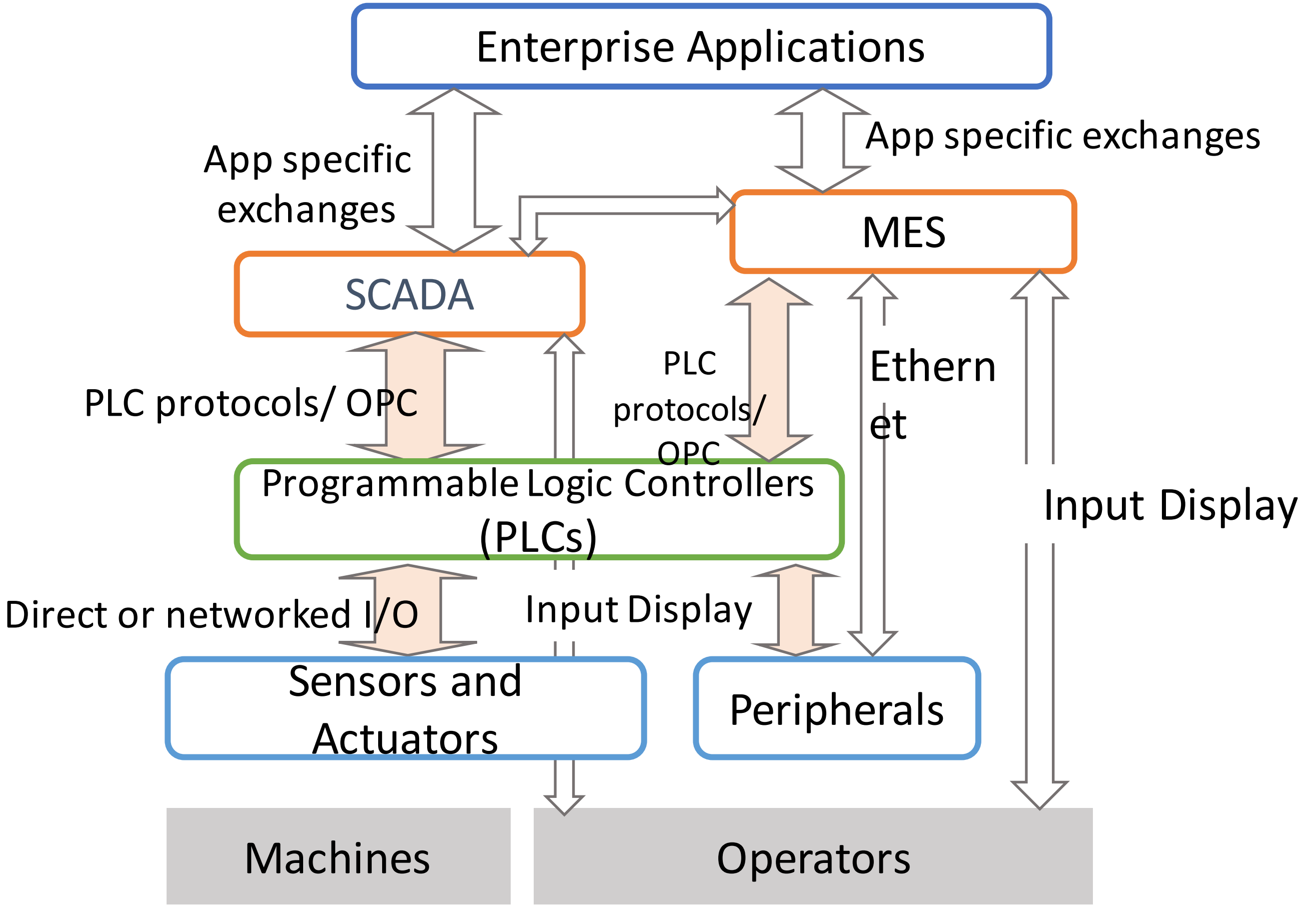
Security Design Challenges:

Constrained movement of data prevents direct application to operations feedback.
Difficult to close cloud-edge-device continuum
Air-gapped model does not work

Multi-Stakeholder Challenges:

Indirect access to data collected, i.e., process to involve 3rd parties are extremely complex and slow.

Common Process Automation Systems



Need for Uniform Network Interface and Technologies is Expanding

- OT services from enterprise applications are achieved through end-to-end communication between the software and I/O field devices.
- The data acquisition (via SCADA) and the operations control programs (MES) have overlapping protocols and still different communication paths.
- Incompatibilities between a variety of fieldbus protocols require Use of translation gateways overcomes interop concerns.

Source: https://www.ordinal.fr/en/scada-and-mes-the-pyramids-secret.htm

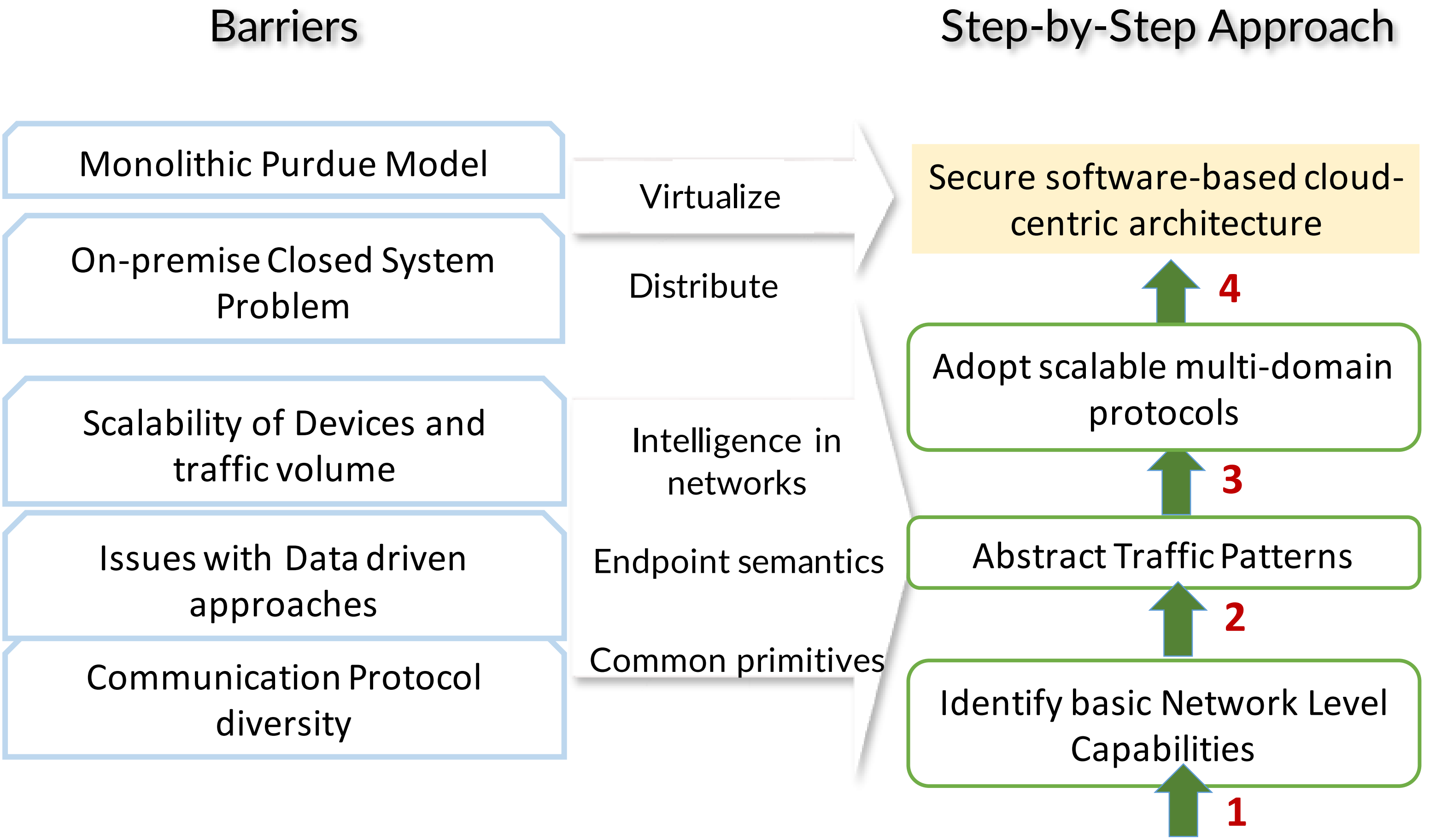
Dealing with Data

- Data Driven Approaches
  - OPC-UA is based on normalizing data format
  - Bloated encapsulations
  - Good for applications but not always useful with delay-intolerant control operations.
- Growth in adoption of IoT devices (sensors)
  - Shop floors have to deal with lot more data and devices.
  - More co-relation of data acquired from various sources
  - Need compute power, state of the art data-processing application software such as ML algorithms, Big-data processing.

On-premise Closed System Problem

- As the data volumes grow, the OT infrastructure gets more expensive.
- This means maintaining shop floor as mini data center - a persuasive argument for adoption to distributed approach
- Often cost prohibitive in terms of resources and equipment cost, especially for smaller sites.
- Does not improve security footprint when it comes to exposing on-site data to third-party stake holders.

A Systematic Proposal to IT/OT Convergence



Barriers

Monolithic Purdue Model

On-premise Closed System Problem

Scalability of Devices and traffic volume

Issues with Data driven approaches

Communication Protocol diversity

Virtualize

Distribute

Intelligence in networks

Endpoint semantics

Common primitives

Step-by-Step Approach

Secure software-based cloud-centric architecture

4

Adopt scalable multi-domain protocols

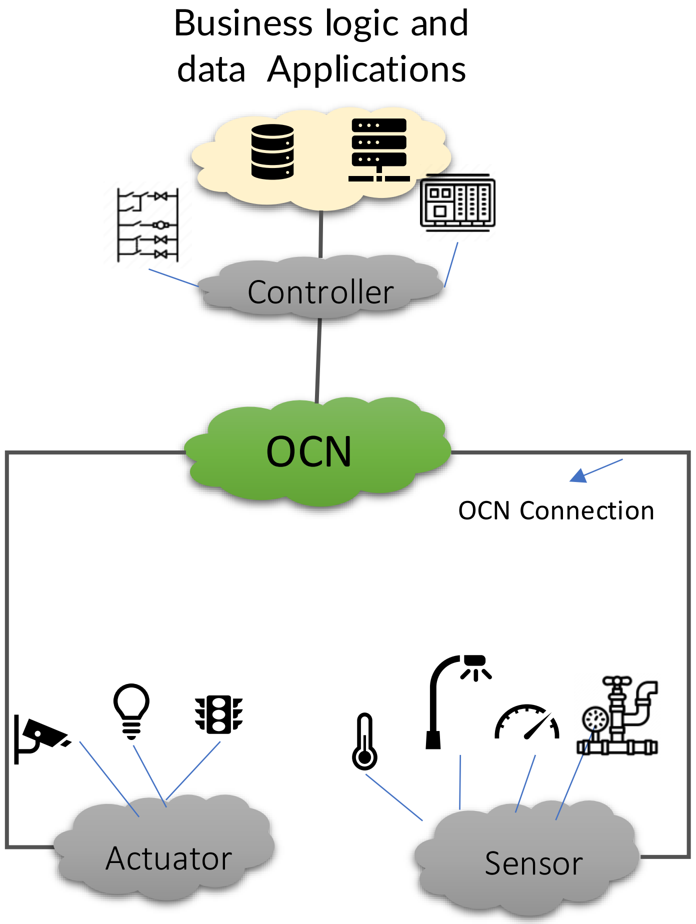
3

Abstract Traffic Patterns

2

Identify basic Network Level Capabilities

1



Operations and Control Network (OCN)

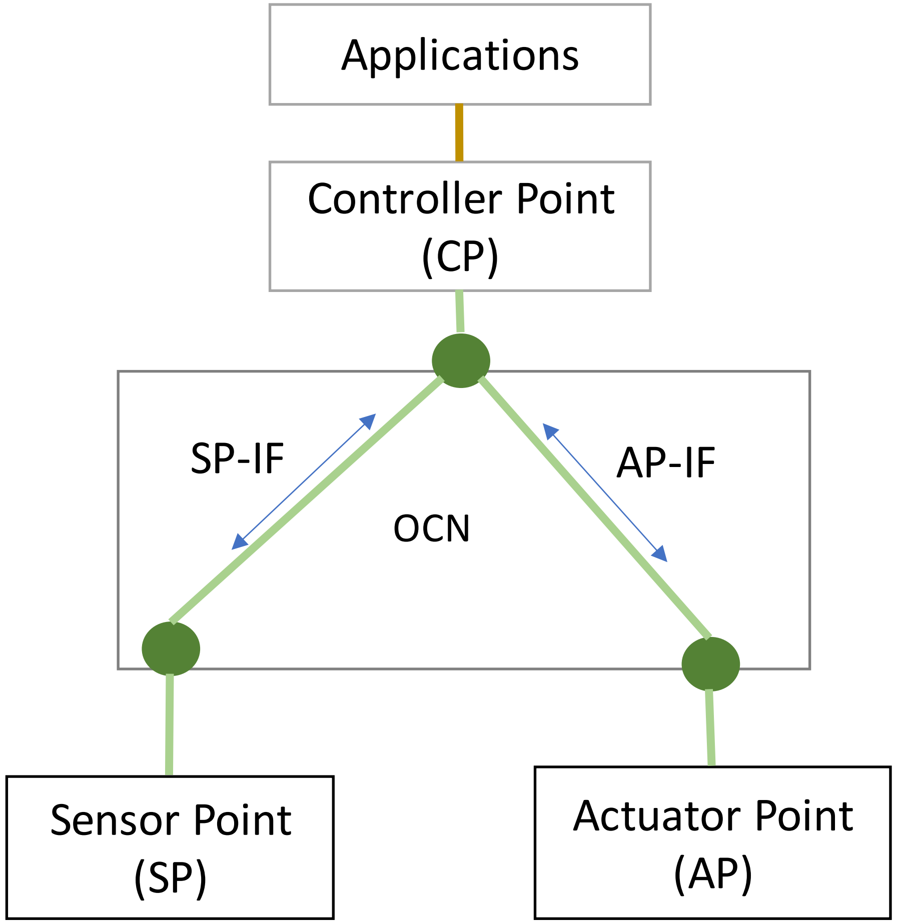
- An attempt to generalize a network for control systems based on two aspects
  - That the field devices do not operate on their own.
    - Instructed by controllers to do certain actions and read certain sensory data.
    - Those controllers can be of any form-factor (small, large, lots of processing power, etc.)
  - For a given application the behavior and operations are well-defined.
    - Characteristics of sensors are quite specific. Emitting data towards controller.
    - Actuator properties – Write and readback type of commands.

- Rationale:
  - The model works identically for both local or remote operations. This allows technology agnostic, location agnostic, multi-domain communications

OCN Reference model

We can start by thinking of OCN as an abstraction of control systems.

- With key logical role-based Reference points
  - Actuators
  - Sensors
  - Controller
- Then standardize
  - (a) interfaces and
  - (b) common message types and
  - (c) corresponding network-constraints



OCN Messages and network characteristics

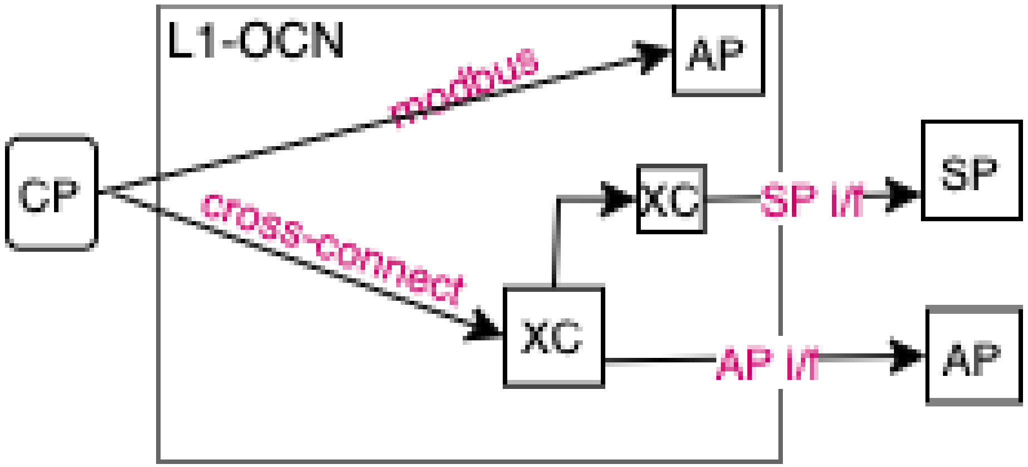
Per Packet Network Information

- On-time messages
  - At the specified time.
- Bounded latency messages
  - With in a specified time interval
- Periodic messages
  - Regular telemetry data
- Order of Messages
  - because field devices do not buffer packets. Network should ensure this

Network Design Goals

- Reliability
  - Ensure packet losses are detected and reported because each message is a command to the controller.
- Safety
  - Of operation and overall system. No late (stale) packets, no duplicate packets (operate machine twice)
- Synchronization
  - Common reference for timestamps
- Security

OCN Realization (L1-OCN)



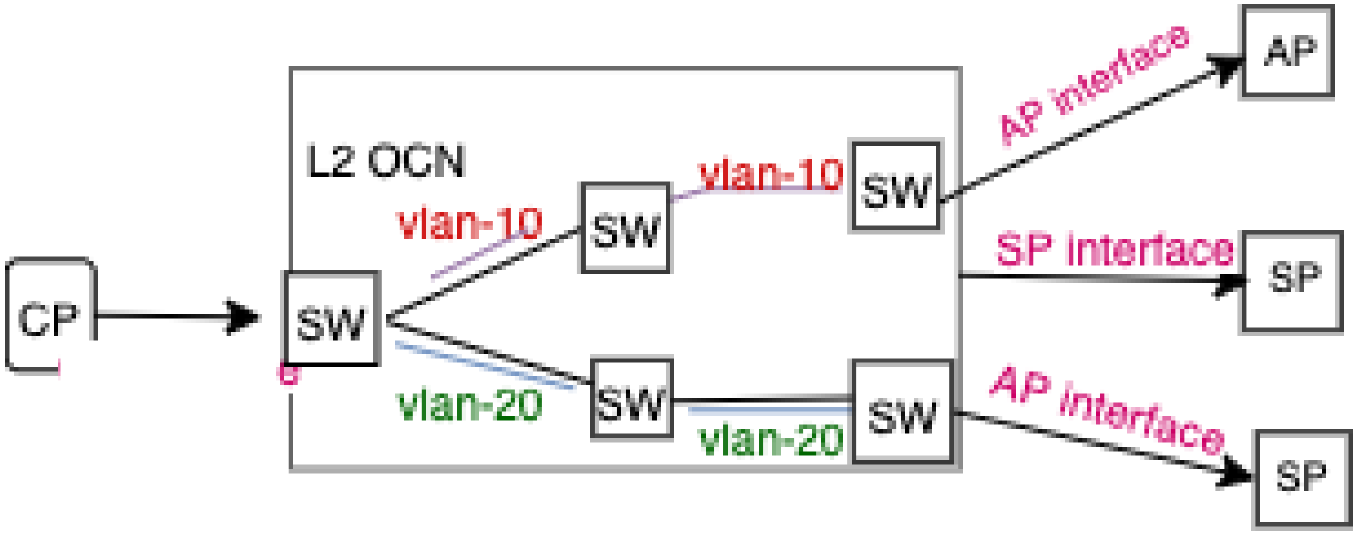
L1-OCNs provide point-to-point connections between the cp and SP/AP

Supports several capabilities – time-constraints, synchronization

Potential support via optical cross-connects, Modbus, Profibus

Limitations of scalability, extensibility in terms of distance and features.

OCN Realization (L2-OCN)



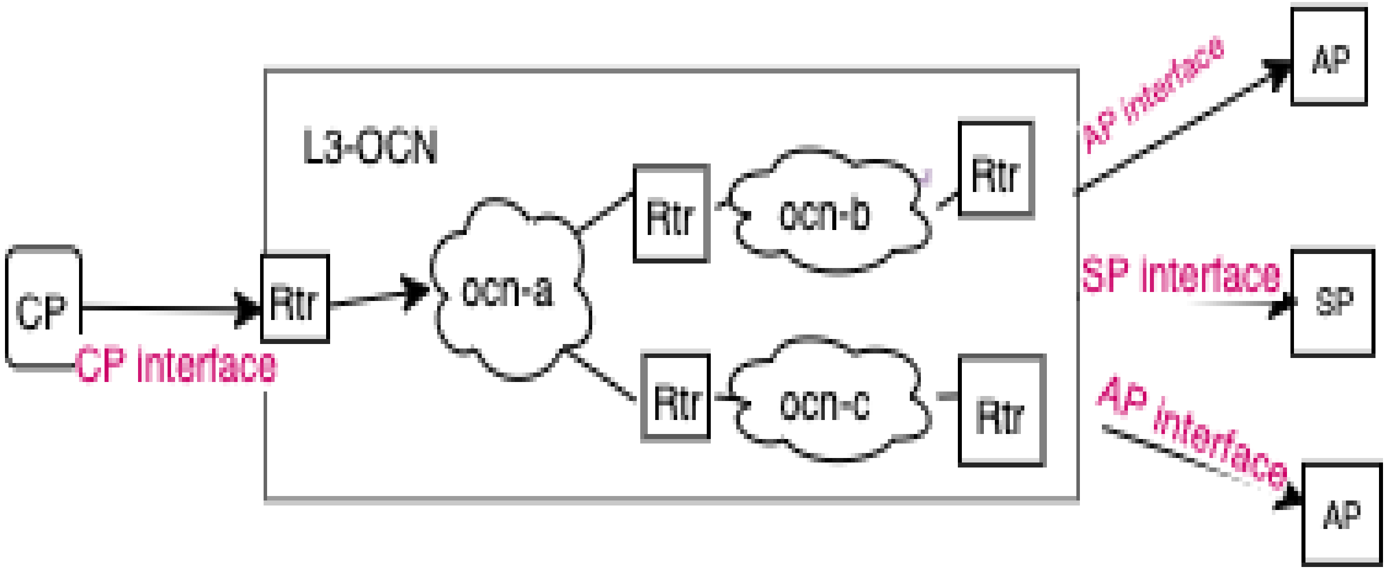
L2-OCNs provide a LAN based multi-point connections

Supports several capabilities – time-constraints, synchronization

Potential support via Ethernet R/T, TSN

Limitations of multi-domain scalability, no standard application to network interface

OCN Realization (L3-OCN)



L3-OCNs provide multi-domain, multi-topology capabilities

L3 networks are not designed for OT applications.
But Potential to extend all the features
Potential support via DetNet

Limitations of multi-domain scalability, no standard application to network interface

Virtualized PLCs

- Programmable Logic Controller (PLCs) are central to OCN.
- Last component in OT environment that can be software-ized.
- Offloading PLCs over powerful hardware allows support for complex compute-intensive operations in a predictable manner.
- Resolve concerns depending on the
  - ***latency-bounds*,**
  - ***deterministic feedback control loops***,
  - reliability, and security → not covered in the scope of this paper

Virtual PLC Feasibility using OCN

Latency Management

$$N_L = \frac{N_B}{T_R} + \frac{D}{S} + D_P + D_Q$$

- D_P Processing Delay (*constant*)
- D_S Serialization delay *(minimal)*
- D_Q Queuing delay (avg. µsec x hops)
- D_{PR} Propagation delay *(*dist*/ (2/3 x* c *))*
- N_B Packet size (bits)
- T_R Transmission rate (in bps)

Latency due to distance is about

- 5 μsec per km*
- 5ms per 1, 000 km

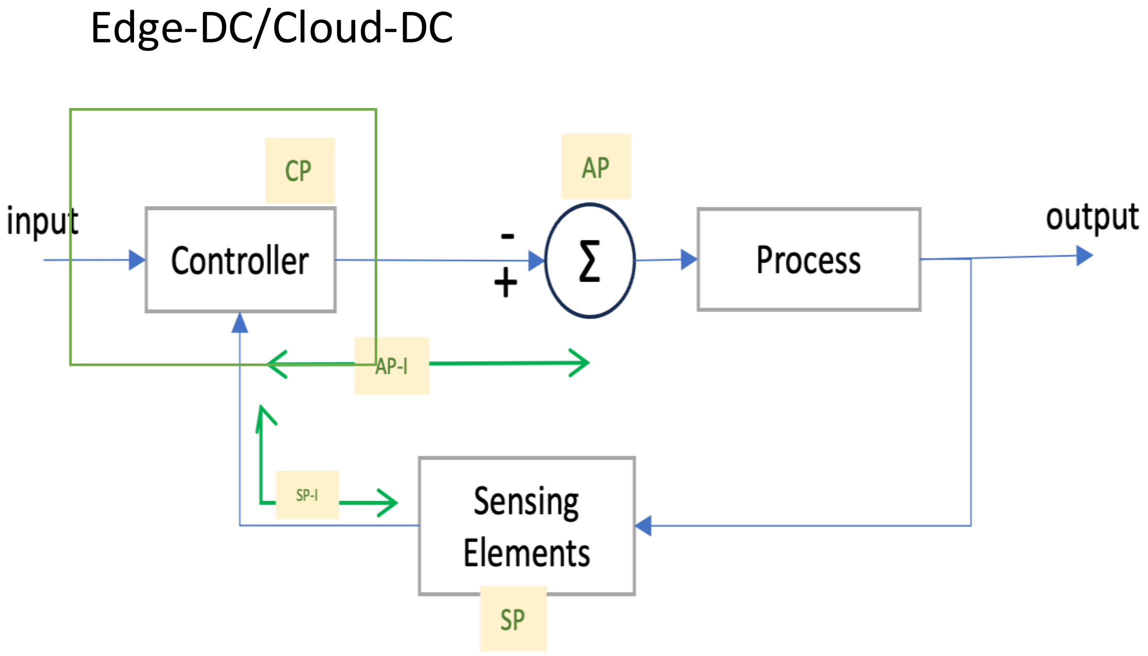
* Based on 10G link

Feasible to support remote process control for latency bounds under *10 ms* applications.

Managing queuing delays addressed via [9] and [14] (see references)

Virtual PLC Feasibility using OCN

Feedback Control Loops



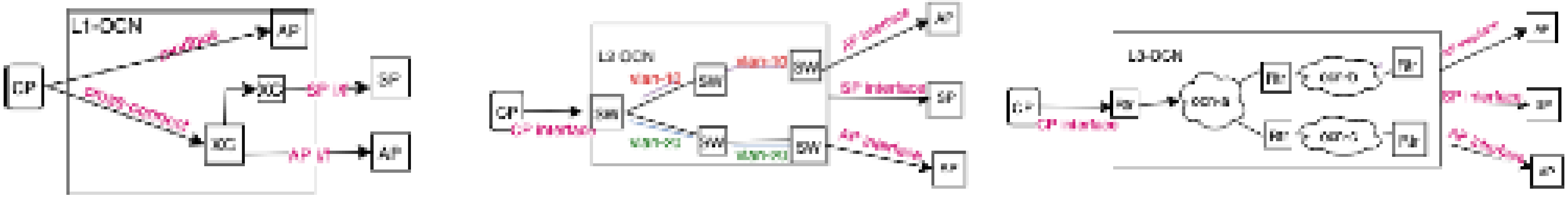
- The PLCs maintain a system or process state
  - By observing sensor values
  - Adjusting actuators’ outputs.

- Within the bounds of latency using standard CP<->AP and SP<->CP interfaces, over the network, same feedback control loop can be instantiated from either edge or cloud.

Challenge: Meeting the requirements of different traffic patterns

For example, how OCN ensures no packet loss and faster detection for an application where there are high volume of data traffic coming from others.

- To some extent, Both TSN, and direct point-to-point connections between CP and AP/SP are OCNs.
- The model is an abstraction for recognizing application specific requirements. Not having to concern with the details of the networks.
- OCN does not promote there is one single mechanisms for packet loss mitigation. But networks can adopt any. Such as packet replication along two different paths (PROF), or other methods.



(a) Physical Layer cross-connects

(b) Media Access Layer LANs

(c) Inter-network multi-technology domains

Challenge: Implementing QoS

QoS architectures have a long history, and OCN are not exceptions

- **applications send QoS requests (bandwidth, delay, jitter**, etc) then typically an **admission control system** admits or denies the requests and allocates the required resources.

- The model depends on resource reservation and admission control mechanisms that were not covered in the paper, but those functions are common to any resource reservation infrastructure.
- We believe that OCN model is specific to process automation. The messages and primitives are specifically described for process commands and the end points associated. Admittedly, it is easier to understand OCN as an advanced QoS model specifically designed for the remote automation.
- Another key difference we see is that QoS is a flow-based architecture which is not the case in OCN. In this paper we abstract traffic as single unit of commands or instructions between the endpoints of a specific type. The traditional QoS architecture is neither universal, nor does it facilitate OT/IT convergence.

Challenge: Integration with Lower Layers

Is OCN a Control plane for IETF DetNet? Or for some other underlying networking layer?

Not necessarily so.

- We consider OCN as a declarative model.
- Being technology-agnostic in OCN model endpoints rely on data plane capabilities.
- And to support programmability and dynamic changes, control plane can be an expensive solution.
- In some ways it is more comparable with OPC-UA

Summary

- In this position paper, we recommend a generalized OCN Model
    - For a large variety of automation applications
    - The generalization supports an evolutionary approach

- Key components of the model’s structure are,
    - Identification of traffic patterns as message types
    - Reference I/O Endpoints – sensors (SP) and actuators (AP)
    - Intelligent reference endpoint as controllers (CP)
    - Communication behavior between

- Validation through virtualized PLC case study.