

Independent Submission  
Internet-Draft  
Intended status: Informational  
Expires: 6 September 2022

K. Makhijani  
L. Dong  
Futurewei  
5 March 2022

Virtualization of PLC in Industrial Networks - Problem Statement  
draft-km-iotops-iiot-frwk-02

## Abstract

Conventional Programmable Logic Controllers (PLCs) impose several challenges on factory floors as their numbers and size on the factory floors/plants continues to grow. Virtualized PLCs can help overcome many of those concerns. They can improve the automation in Industry control networks by simplifying communication between higher-level applications and low-level factory floor machine operations. Virtual PLCs provide an opportunity to integrate a diverse set of non-internet protocols supporting Industrial-IoT and IP connections to improve coordination between applications and field devices. Besides automation, virtual PLCs also enhance programmability in industry process control systems by abstracting control functions from I/O modules. However, to achieve desired outcome and benefits, both operational and application networks should evolve.

This document introduces virtual PLC concept, describes the details and benefits of virtualized PLCs, then focuses on the problem statement and requirements.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 6 September 2022.

Internet-Draft

iiot-vplc

March 2022

## Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Terminology</a>	<a href="#">4</a>
<a href="#">2.1.</a>	<a href="#">Acronyms</a>	<a href="#">5</a>
<a href="#">3.</a>	<a href="#">Virtualized PLCs</a>	<a href="#">5</a>
<a href="#">3.1.</a>	<a href="#">Definition</a>	<a href="#">6</a>
<a href="#">3.2.</a>	<a href="#">Limitations with Physical PLCs</a>	<a href="#">6</a>
<a href="#">3.2.1.</a>	<a href="#">Integrated Application Control Loop</a>	<a href="#">6</a>
<a href="#">3.2.2.</a>	<a href="#">Single purpose to Multipurpose</a>	<a href="#">7</a>
<a href="#">3.2.3.</a>	<a href="#">Simulation and Analytics</a>	<a href="#">7</a>
<a href="#">3.2.4.</a>	<a href="#">Managing Complexity</a>	<a href="#">7</a>
<a href="#">3.3.</a>	<a href="#">Benefits and Opportunities</a>	<a href="#">8</a>
<a href="#">3.3.1.</a>	<a href="#">Processing Capabilities</a>	<a href="#">8</a>
<a href="#">3.3.2.</a>	<a href="#">Flexibility and Efficient Resource Use</a>	<a href="#">8</a>
<a href="#">3.3.3.</a>	<a href="#">Interoperability and Optimization</a>	<a href="#">8</a>
<a href="#">3.3.4.</a>	<a href="#">Device Density on Factory Floor</a>	<a href="#">8</a>
<a href="#">3.4.</a>	<a href="#">Incremental Realization Approaches</a>	<a href="#">9</a>
<a href="#">3.4.1.</a>	<a href="#">Softwarized PLC</a>	<a href="#">9</a>
<a href="#">3.4.2.</a>	<a href="#">Local Disaggregation of Control and I/O Modules</a>	<a href="#">9</a>
<a href="#">3.4.3.</a>	<a href="#">Fully Virtualized PLC</a>	<a href="#">10</a>
<a href="#">4.</a>	<a href="#">Problem Statement</a>	<a href="#">10</a>
<a href="#">4.1.</a>	<a href="#">Overview of Industrial Network Architecture</a>	<a href="#">10</a>
<a href="#">4.2.</a>	<a href="#">Associating virtualized PLCs with IO Devices</a>	<a href="#">11</a>
<a href="#">4.3.</a>	<a href="#">Expectations from the Networks</a>	<a href="#">12</a>
<a href="#">4.3.1.</a>	<a href="#">Hierarchical Structure</a>	<a href="#">12</a>
<a href="#">4.3.2.</a>	<a href="#">Safety and Reliability of Operations</a>	<a href="#">12</a>
<a href="#">4.4.</a>	<a href="#">Multiprotocol Supporting PLCs</a>	<a href="#">12</a>
<a href="#">4.5.</a>	<a href="#">Identification of virtualized PLC</a>	<a href="#">13</a>
<a href="#">4.6.</a>	<a href="#">Security Aspects</a>	<a href="#">13</a>
<a href="#">5.</a>	<a href="#">Requirements</a>	<a href="#">13</a>
<a href="#">5.1.</a>	<a href="#">Virtualized PLC Requirements</a>	<a href="#">13</a>

<a href="#">5.2.</a>	Key Performance Indicator Requirements . . . . .	<a href="#">15</a>
<a href="#">5.3.</a>	Network Related Requirements . . . . .	<a href="#">16</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">17</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">17</a>
<a href="#">8.</a>	Acknowledgements . . . . .	<a href="#">17</a>

<a href="#">9.</a>	Informative References . . . . .	<a href="#">17</a>
<a href="#">Appendix A.</a>	<a href="#">Appendix A.</a> Purdue Model (ICA-95) . . . . .	<a href="#">19</a>
<a href="#">A.1.</a>	Separation between Manufacturing and Enterprise Networks . . . . .	<a href="#">20</a>
<a href="#">A.2.</a>	Collaborating with SDOs with Industry Network Focus . . . .	<a href="#">21</a>
	Authors' Addresses . . . . .	<a href="#">22</a>

## [1.](#) Introduction

Programmable Logic Controllers (PLCs) have been instrumental to the growth of automation in industrial process control. Industry 4.0 and similar initiatives have put even more emphasis on automation of the entire production process. For example, a typical workflow in the Smart Factory to manufacture customized orders (reconfigurable manufacturing [[RECONF](#)]) is executed autonomously, comprising several related and inter-dependent processes. In this workflow, all the dependencies and transitions occur seamlessly without human intervention – such as requesting inventory before it becomes unavailable, dispatching a request for specific maintenance, performing quality control on the material, and adjusting operations automatically.

This type of system-level automation requires close coordination between PLCs (low-level machine controlling components) on the factory floors and the high-level decision-making software. However, in the current Industry control architecture, PLC operations are isolated from higher-level components; they operate in an entirely different proprietary hardware environment. Moreover, the number of PLCs on a floor are growing along with their physical size to support faster processors and more memory. This makes management of PLCs with different type of hardware even more difficult. Although PLCs can be customized, they are designed for limited set of controls, therefore their extensibility is limited. To overcome above mentioned challenges it should be possible to incorporate multiple control functions in a hardware-agnostic platform.

Virtualization is a proven technique to abstract software logic from the underlying hardware. Information Technology (IT) has proven that virtualization benefits cost savings, flexibility, and efficient resource usage. In the context of Industrial networks, virtualization serves to integrate IT and OT software components, which are essential for integrated automation.

This document describes the 'virtualized PLC' concept and its realization. In [Section 4](#) limitations in physical PLCs are covered along with the benefits of virtualized PLC. Finally, [Section 5](#) discusses requirements to support virtualized PLCs and their impact on the network.

## [2.](#) Terminology

### Industrial Control Network:

Industrial control networks are the interconnection of equipment used to operate, control, or monitor machines in the industry environment. It involves different levels of communications - between field bus devices, digital controllers, and software applications.

### Industry Automation:

Mechanisms that enable the machine to machine communication by use of technologies that enable automatic control and operation of industrial devices and processes leading to minimizing human intervention.

### Control Loop:

Control loops are part of process control systems in which desired process response is provided as an input to the controller, which performs the corresponding action (using actuators) and reads the output values. Since no error correction is performed, these are called open control loops.

### Feedback Control Loop:

Feedback control loop is a system in which the output of a control system is continuously measured and compared to the input reference value. The controller uses any deviation from the input value to adjust the output value for the desired response. Since there is a feedback of error signal to the input, these are called closed control loops.

Programmable logic controllers (PLC):

Industrial computers/servers to control manufacturing processes such as assembly lines.

Supervisory Control and Data Acquisition (SCADA):

Software System to control industrial processes and collect and manage data.

Distributed Control Systems (DCS):

Systems of sensors and controllers that are distributed throughout a plant.

Manufacturing Execution System (MES):

Systems that connect production equipment across the factory floor or multiple plants or sites.

Fieldbus Devices:

Operational Technology field devices include valves, transmitters, switches, actuators, etc.

Virtualized PLC (vPLC):

A software component of PLC, in which the control part of factory devices is decoupled from the I/O component. With vPLCs, the I/O stays local to the machines (sensors, actuators, and drives), while the controller logic lives as a software service implemented over RT- hypervisors.

Scan-Cycle:

A scan cycle is the time to read the inputs, execute the program (e.g., ladder logic), and update the outputs. The actual scan time is affected by the processing speed of the PLC, the size of the program, the type of instructions used in the program. In virtualized PLCs, general-purpose processor speed and memory are much higher than most physical PLCs.

## [2.1.](#) Acronyms

- \* HMI: Human Machine Interface

- \* MES: Manufacturing Execution System
- \* CIN: Converged Industrial Network
- \* IIC: Industrial Internet Consortium
- \* IDMZ: Industrial Demilitarized Zone
- \* PLC: Programmable Logic Controller
- \* PDU: Protocol Data unit
- \* SCADA: Supervisory Control And Data Acquisition
- \* DCS: Distributed Control System
- \* OT: Operational Technology
- \* IT: Information Technology

### [3.](#) Virtualized PLCs

#### [3.1.](#) Definition

Programmable Logic Controllers (PLCs) are specialized physical devices (or computers) that are used to control the operation of machines by coordinating the input sensors (temperature, pressure, position, vibration, humidity, torque, etc. readings) to the output actuators (such as motion control, voltage change, pressure valves, etc.). PLC components include a control unit, memory (to store the data, state, and process control instructions), and I/O modules to communicate with Fieldbus devices (sensors and actuators) using different standard or proprietary protocols.

Compared with commodity CPUS, most PLC control unit processing power is extremely low, whereas new complex process control applications require sophisticated and faster compute capabilities. Utilizing

commodity-grade CPUs for many PLC function blocks provides higher compute and memory for PLC programs by separating its control unit and memory from the physical PLCs. This will leave only I/O modules connected to the devices. Thus,

Virtualized PLC is a hardware-agnostic abstraction of the control unit and memory functions of a PLC. It is hardware-independent and still needs an interface to communicate with the I/O modules.

The concept has been discussed both in research [[PLC-40](#)] and industry [[VPLC-DRAGOS](#)] [[VPLC\\_IIC](#)] [[VPLC\\_CONV](#)]. In the following section motivation for virtualized-PLCs.

### [3.2.](#) Limitations with Physical PLCs

#### [3.2.1.](#) Integrated Application Control Loop

Application performance is improved with better coordination between applications and field devices. One way to achieve this is when seamless sharing of both data and control operations, and it is possible when both application and controller software use a common language or interface. Today OPC-UA model is well-established and provides a protocol-independent data model for the standard representation of several Fieldbus protocols and requires a translation layer. The use of software PLCs can unify the collection of data and control processes even more efficiently since the software PLCs are already hardware-independent.

Like IT, the manufacturing and process industry is evolving to a non-monolithic mode of system operations. In a large-scale industrial operation, several control processes run simultaneously and have high-performance requirements.

#### [3.2.2.](#) Single purpose to Multipurpose

Currently, PLC controllers are designed for a single purpose long-term use. There is an implicit expectation that PLC functions and corresponding I/O devices will not be replaced for many years once installed. This paradigm makes it difficult for industries to handle changing requirements and can be prohibitive to adopting new technologies and deploying new types of sensors that could provide

better monitoring. With virtualized PLC, re-programming control logic to tweak the assembly line becomes a lot easier.

### [3.2.3.](#) Simulation and Analytics

Physical PLCs are difficult to troubleshoot. Upon failures, operators have to manually study the log files to generate traces from historical data. Since Virtual PLCs are hardware-agnostic, they are almost identical to their simulation counterparts. When replayed with actual historical event data, the run-time state of a PLC at any instance in the past can be recreated, which would help to troubleshoot and root-cause failure events. It is difficult to do this type of root-cause analysis with physical PLCs.

### [3.2.4.](#) Managing Complexity

Complexity is a trait of overall system architecture. With Physical PLCs, the plant-floors will continue to deploy proprietary protocols and PLCs, leading to either managing solutions from different vendors or being locked into one vendor-provided solution. While the former adds to the complexity, the latter may not use innovation outside a specific vendor.

Architecturally, PLCs require a lot of different types of connections, such as PLC-PLC (peer to peer), PLC-SCADA, PLC-HMI, etc. Depending on the interface and protocol, scaling PLCs would lead to a higher number of gateways (and more wiring) that are difficult from a maintenance perspective and can also cause poor performance. With physical PLCs, heterogeneity of protocol interface will not go away.

Faults with PLC input/output (I/O) modules and field devices account for 80 percent of system failures. Common causes of failure include the rugged environment that devices are subjected to. In some cases, consolidating different PLCs on a single powerful PC and protecting a single node (hosting several PLCs) from failures of a power outage, electromagnetic or radio frequency interference is a lot easier than protecting a high number of PLCs. In other cases, PLCs can be placed in the edge network, separated from the rugged environment.

## [3.3.](#) Benefits and Opportunities



### [3.3.1.](#) Processing Capabilities

Virtualization enables running software on commodity hardware. One of the most important benefits is using more sophisticated processors to perform complex computations beyond legacy PLCs (floating point, arithmetic operations, counters, etc.). Currently, there are already PLC control units supported on FPGAs [[FPGA PLC](#)] indicating the need for faster and parallel processing. Virtualization will enable further integration of such different With the availability of high-en.

### [3.3.2.](#) Flexibility and Efficient Resource Use

Traditional PLCs are fixed-function controllers typically used for specific jobs on the factory floor. Today, software-based PLCs are available for general-purpose commercial hardware, but they have been mainly used for simulation and training purposes. Now there is more emphasis on customizations which will require PLCs to be programmed every time a new custom product is requested, leading to longer manufacturing cycles. Virtualization can enable running multiple instances with its own set of allocated resources. Thus, it will be possible to run different configurations for different customizations simultaneously with efficient use of resources only on-demand.

Moreover, when virtualized PLCs and IT applications are on the same platform, it is possible to have close coordination between the OT and IT functions. Although it may not be compelling, virtualized PLCs potentially eliminate the need for dedicated PLCs on the floor, creating space and reducing the number of interconnections.

### [3.3.3.](#) Interoperability and Optimization

Having abstracted PLC logic allows using a common communication protocol, thus improving interoperability between different vendors supplied I/O modules. Besides improving performance, this approach also simplifies configuration, configuration, and monitoring.

### [3.3.4.](#) Device Density on Factory Floor

With the innovations in IoT devices, it is anticipated that there will be newer ways to measure, monitor, and collect various environment-specific metrics; this signifies an even larger number of devices and a corresponding increase in the number of controllers. Virtualization can further simplify control of a considerably high number of devices through a single PLC, thereby reducing some network resource requirements.

While applications and services are beginning to get disaggregated, PLCs' virtualization is very early stage.

### [3.4.](#) Incremental Realization Approaches

Once virtualized, a PLC may be placed flexible anywhere in the network and closer to the higher-level applications. However, expanding beyond a factory site is a drastic change from the existing isolated OT mindset. To address such concerns, the following different approaches are possible:

#### [3.4.1.](#) Softwarized PLC

This is the basic approach with minimal change and minimal impact. A PLC software is virtualized and runs on proprietary or commodity hardware supporting legacy I/O modules. This type of change is isolated to a specific PLC functionality, and the only benefit is hardware independence. Potentially, there is a one-to-one replacement of physical to software PLC.

#### [3.4.2.](#) Local Disaggregation of Control and I/O Modules

In addition to above approach, the software component of PLC (its control unit) runs on commodity hardware; I/O modules are separated from the PLC to provide a clear separation between I/O and programmable components. It requires trivial I/O interconnects to do trivial Fieldbus frame forwarding to I/O modules which may not require any memory or processing capability as shown in Figure 1.

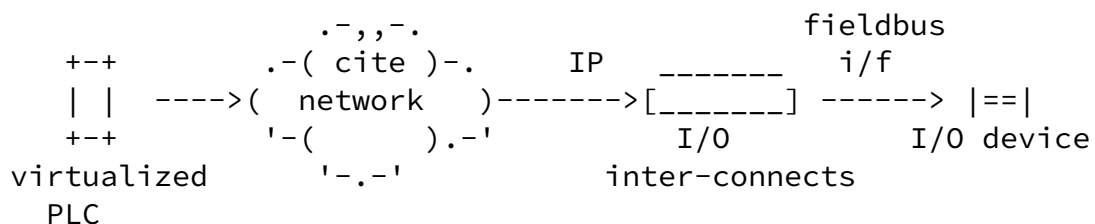


Figure 1: virtualization of PLC and separation from I/O devices

Utilizing IT-style virtualization infrastructure, different instances of virtualized PLC may run simultaneously on a single machine, or even different types of PLCs may run together as a single instance of virtualized PLC. A clean separation between PLC logic from I/O module allows changes to PLC logic and I/O devices independently. With this level of hardware independence, a virtualized PLC can be instantiated on the same hardware and SCADA, HMI, or ICS components providing close integration of these entities.

Internet-Draft

iiot-vplc

March 2022

Since the location of virtualized PLC is within the manufacturing zone, there is no impact on the security design.

### [3.4.3.](#) Fully Virtualized PLC

Eventually, virtualized PLCs may be placed anywhere (in the cloud, edge, or on-site) in a location-independent manner. All the benefits considered in [Section 3.4.2](#) apply with an advantage of leveraging multi-tenant edge-compute infrastructure as a tenant.

However, the network will be required to provide more security and safety mechanisms.

## [4.](#) Problem Statement

The addition of PLC virtualization capabilities impacts the PLC device and the network elements in the infrastructure. Design considerations must be made to ensure that such impacts facilitate automation by simplifying configurations, improving operations and management, and reducing process-change overheads. Nevertheless, it is a change from the current state of the Industrial Networks.

This section describes the challenges, starting with brief information on the current architecture to set the context.

### [4.1.](#) Overview of Industrial Network Architecture

The physical network architecture for process control, as shown in Figure 2 is rigidly hierarchical. Note that the figure is over-simplified, and in general, each level will have additional hierarchies to extend the networks for scale. For example, a PLC controlling a group of Fieldbus devices may, in turn, be controlled by another PLC controller [[networked-PLC](#)] that runs ProfiNet protocol because both sets of devices are interdependent. For such cases, protocol translation gateways are required. Several network switches are needed to interconnect gateways and numerous devices on the factory floor.

The hierarchical architecture comprises security-oriented zones known

as ICA-95 model (or Purdue model see [Appendix A](#)) in which each zone contains well-defined levels. Among the three zones (Manufacturing, IDMZ, and Enterprise), the enterprise zone network is all IP, while the manufacturing and IDMZ network on the factory floor is a combination of IP and Industrial protocols. The communication across the zone tends to get complex as each zone runs over different network technologies. A large number of IP-based firewalls and translation gateways are deployed in all the zones to control data movement between IT and OT networks.

Industry control systems (SCADA, HMI, MES) perform complex operations. They collect data from devices and simultaneously administer several process control loop instances to handle complex processes. Traditional best practices indirectly required data delivery from L2 to L3 levels in reports, which caused a significant time lag.

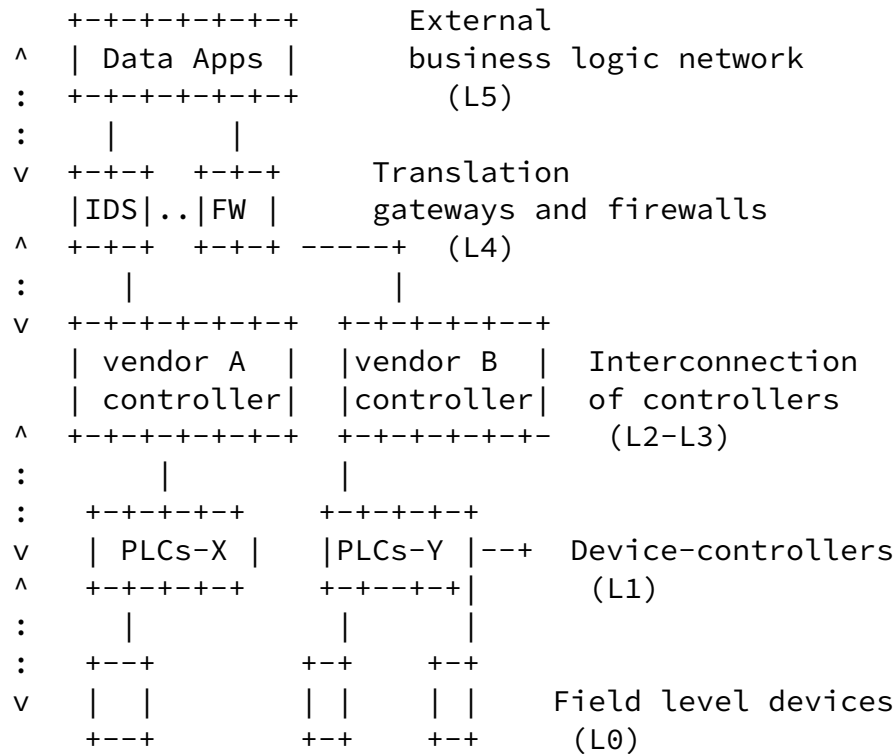


Figure 2: Hierarchy of Functions Industrial Control Networks

#### [4.2.](#) Associating virtualized PLCs with IO Devices

A physical PLC is generally associated with a few I/O devices and is directly connected. The I/O modules are not required to authenticate or verify the connection. A virtualized PLC is a software instance; it may now be anywhere in the network; therefore, the system must authenticate the virtualized PLC and I/O device connection pairing. This is necessary to maintain the reliability and safety of the system and prevent unauthenticated PLC from interacting with the software. The association must be done under the constraint that I/O modules are basic devices without any compute capability. Thus, the network should provide these functions through gateways or interconnecting devices.

#### [4.3.](#) Expectations from the Networks

The magnitude by which compute capability is improved allows a single virtualized controller to handle more complex and faster scan cycles. Then, the network to manage communication delays, packet formation, processing, and forwarding overheads become critical to overall system performance. Harnessing compute power at a lower cost from edge-compute platforms is expected for several reasons. It is anticipated that edge-networks will offer general purpose compute and store capabilities for latency-sensitive applications. This piece of infrastructure can serve many sites and needed not be owned but can be leased, providing cloud-like services. It is a big change from the traditional Purdue model or ICA architecture.

Thus, the plant-floor networks are now extended to edge networks expanding the security zones creating 'new' requirements for multi-tenancy support (isolation and network segmentation) in OT networks. Note that in IT networks, these technologies are mature and already standardized.

##### [4.3.1.](#) Hierarchical Structure

Virtualized PLCs and their flexible placement require flat structure so that flow of information is context based and need not follow strict hierarchy. Hierarchical flow of information is not always

efficient and is centralized. It does not inherently support autonomous decision making which is central to Industry 4.0 type of initiatives. In contrast, a distributed architecture with some form of centralized view will be ideal since it combines both autonomous operations and global view.

#### [4.3.2.](#) Safety and Reliability of Operations

The Fieldbus modules and PLCs are designed to perform for long period of times. The commands or operations dispatched from virtual PLCs must conform to same safety standards. Similarly, the communication between PLC control unit and I/O module is highly reliable and such data losses must be prevented.

#### [4.4.](#) Multiprotocol Supporting PLCs

A virtualized PLC can act as a single logical controller to communicate with a different group of I/O devices over one or more non-internet protocols such as Modbus, Profibus, CANbus, Profinet [[SURV](#)], etc. Since each protocol specifies its packet format, different translation gateways are generally needed. Thus, a multi-protocol virtual PLC can reduce the number of gateways.

However, the challenge is to provide a standard communication format for different I/O devices. Since it is not feasible to have a single flat Fieldbus protocol due to address scale limitations (limited address space up to 256 devices), an I/O interconnect is required to perform format translation. Then the packet on the wire should be multi-protocol aware. i.e., virtualized PLC needs to know what type of Fieldbus device it is communicating with at the other end.

#### [4.5.](#) Identification of virtualized PLC

The Fieldbus devices are serial buses and identify PLC as a device with a specific bus address. It may be required for virtualized PLC to support dual addresses, one exposed for the I/O module and the other for IT applications. Converged IT/OT networks should leverage specifics of factory floors designs and assign device ids based on machine locations and context. As an example, a device with basic address 0x14 may be defined as 'device 0x14, cell 'C1' and factory

floor 'F1', PLC bus address '0x1' in the communication path. The reachability to a specific I/O module should have complete information from virtualized PLC.

#### [4.6.](#) Security Aspects

The fundamental paradigm of security as described in ICA-95 architecture changes with virtualized PLC since those PLCs won't be in the local manufacturing zone. The zone-aware security will not apply.

Instead, the system will need a multi-dimensional security profile. The first one encompasses both enterprise and manufacturing zones, and the second is location-specific, i.e., using secure channels such as VPN, IPSEC, etc.

### [5.](#) Requirements

#### [5.1.](#) Virtualized PLC Requirements

A virtualized PLC's function and operation should be identical to that of physical PLC. The following requirements relate to virtualized PLC's reachability, identification, and discovery (or attachment) in the network.

##### \* Addresses scope

The virtualized PLC is expected to be an IP-addressed endpoint when communicating with higher-level applications. However, southbound communication may require some structured addressing scheme to reach

the Fieldbus device in the network (e.g., see [[semantic-addressing](#)] and [[asymmetric-addr](#)]). There is no need to enforce IP addresses for Fieldbus devices since they are constrained devices, and IP may not be the most suitable address structure. A uniquely reachable address space for all the Fieldbus I/O devices and PLCs is required such that intermediate network elements know how to route (or switch) to those addresses. Moreover, as the scale of the industry network grows, there will be many 'same' types of devices with limited address space (a Fieldbus or ModBus address limits up to 256) all across the floor. It is maybe desirable to support variable-length identifiers to handle both IT servers and I/O module-type devices.

#### \* Converged Namespace

Addresses are resolved from namespaces. It should be possible to associate all the endpoints (OT and IT) as part of their system-defined namespace. The solution should not require different operations and management schemes for industry I/O modules vs. IT applications. It will improve security by verifying an endpoint against a namespace. However, each vertical sector should be able to choose its namespace. For example, In some cases, the classification may be based on a level (PLCs, cell sites, type of application, etc.), and the corresponding address is derived by concatenating them together since factory devices do not change their location often in the topology.

#### \* Network Identifiers:

Virtualized PLC should be identifiable by what application it can talk to or the service they are part of [[semantic-addressing](#)]. The network identification is required for setting up security or firewall policies. Note: legacy devices do not have network identifiers, and deeper packet inspection will be required to identify a specific PLC. Alternately [[semantic-addressing](#)] may be useful in structuring the identifiers.

#### \* Legacy support:

Virtualized PLCs and legacy PLCs must co-exist with support for deployed protocol formats and their core capabilities. This is needed to maintain non-disruptive operations.

#### \* Auto-configuration:

Procedures should be efficient, i.e., comparable to the processing capabilities of the I/O devices. On-boarding procedures (manual or automatic) must have built-in or well-defined authentication.

#### \* Controller and Fieldbus Pairing:

Virtualized PLCs must support a secure method of pairing authenticating with their I/O devices. Virtualization allows



multiple PLCs to control (or at least monitor) the same device. This can potentially lead to conflicts in device operation. Therefore, careful access control mechanisms are required to prioritize operation across the PLCs.

#### \* Efficient Transport Protocol

Currently, factory-floor Fieldbus devices do not directly use any transport protocols designed for the purpose, e.g., [[MQTT\\_SPEC](#)] and [[OPC\\_ARCH](#)]. The data collected from sensors is encapsulated in TCP. Alternate native transport based on principles of MQTT type of protocols could help to improve the traffic efficiency in industrial networks.

### [5.2](#). Key Performance Indicator Requirements

#### \* Process Control

Performance depends on the deterministic behavior of devices. A virtualized PLC must maintain all deterministic and low latency attributes of physical PLC.

#### \* Safety mechanisms

To keep a factory floor hazard and accident-free environment, the virtualized PLC must implement mechanisms for proper operation of a device, including commands sent from virtualized PLC that must not exceed thresholds and are error-free and valid for the Fieldbus operation.

#### \* Deterministic or Time Sensitive Service Guarantees

Mechanisms should be implemented to assure time-sensitive delivery of traffic. For this, [[DETNET](#)] or TSN technologies can be used.

#### \* Security

Mechanisms should be implemented to protect against man-in-the-middle attacks. Encryption overheads must be budgeted from virtualized PLC to Fieldbus to maintain process control latency. Due to low processing power, lightweight mechanisms should be devised.

### [5.3.](#) Network Related Requirements

The topologies in the manufacturing zones do not change frequently, and devices are designated in a zone or a cell for long-term use. Such observations can help simplify network designs. Industry networks could substantially benefit from a hybrid software-defined networking and distributed routing approach. Former for initial provisioning (or controlled bootstrapping), latter for reachability and health of the fabric. Such hybrid techniques eliminate the need for implementing complex routing protocol features.

#### \* Backward Compatibility

Seamless integration of virtualized PLCs must be supported. The network must support legacy traffic, and its performance should be no worse than before the inclusion of virtualized PLCs.

#### \* Efficiency of connections

Industrial networks have different connection endpoints, such as PLC-PLC, PLC-SCADA, SCADA-IT-Systems, PLC-Firewalls, PLC-gateways, PLC-I/O modules. Without subscribing to a specific wire format, a flexible packet format should be designed to address smooth connections between any of the above endpoints. It implies that a variety of endpoints interconnect in an identical fashion without requiring device-specific translations. Efficient connections lead to less processing or states in the network with improved resiliency and performance. There may be opportunities to design packet formats with minimal overheads by using in-band programmability paradigms that carry embedded metadata and control information relating to reachability, latency, jitter, reliability, and exceptions characteristics. This approach is expected to reduce configurations and the number of policies required for data steering through the network. Existing methods that may be used, evaluated or extended include IP with TSN, DETNET[DETNET], reachability headers SCHC, IPv6 compression schemes, or may be evaluated against newer schemes.

#### \* Traffic segmentation support

As virtualized PLCs are spun off like VMs, connectivity with fieldbus devices will be affected. It should not have adverse effect on deterministic, low latency behavior on the other segmented traffic (i.e., connectivity between another set of endpoints). Each segmented traffic may be associated with a different protocol or traffic profile, including legacy traffic format and profiles. The methods to support segmentation include virtual network technologies inside the fabric such as VxLAN, VPNs, etc.

Internet-Draft

iiot-vplc

March 2022

#### \* Resilient and Extensible Topologies

The industry network protocols must not limit to a constrained physical topology. It must support a multi-path distributed connectivity framework to prevent bottlenecks traffic concentration.

#### \* Dynamic Bandwidth Management

Even industrial networks generate a high volume of data from the sensors. Managing bandwidth for different types of data (operational, control, statistics) should be supported through existing QoS or in-band monitoring technologies.

### [6.](#) IANA Considerations

This document requires no actions from IANA.

### [7.](#) Security Considerations

The architecture at the very least must adhere to the security guidance provided by ICS-95.

### [8.](#) Acknowledgements

### [9.](#) Informative References

[asymmetric-addr]

Makhijani, K. and L. Dong, "Requirements and Scenarios for Industry Internet Addressing", Work in Progress, Internet-Draft, [draft-km-industrial-internet-requirements-00](#), 10 June 2021, <<https://datatracker.ietf.org/doc/html/draft-km-industrial-internet-requirements-00>>.

[DETNET]

Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", [RFC 8655](#), DOI 10.17487/RFC8655, October 2019, <<https://www.rfc-editor.org/rfc/rfc8655>>.

[FPGA\_PLC]

Huabing, Z., Benlei, L., Bolin, D., and F. Xiao, "Research on FPGA-based Programmable Logic Controllers' Technology",

TELKOMNIKA Indonesian Journal of Electrical  
Engineering Vol. 11, DOI 10.11591/telkomnika.v11i12.3701,  
December 2013,  
<<https://doi.org/10.11591/telkomnika.v11i12.3701>>.

[IIC] "Industry IoT Consortium", n.d.,  
<<https://www.iiconsortium.org>>.

Makhijani & Dong

Expires 6 September 2022

[Page 17]

---

Internet-Draft

iiot-vplc

March 2022

[IIC\_TALK] William Diab, W., "Overview of IIC – Building the IIoT Ecosystem", 12 October 2021, <[https://github.com/iot-dir/Meetings/blob/main/20211012/slides/Diab\\_IIC\\_Overview\\_for\\_IETF\\_1021\\_rev2.pdf](https://github.com/iot-dir/Meetings/blob/main/20211012/slides/Diab_IIC_Overview_for_IETF_1021_rev2.pdf)>.

[ISA95] "ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod) Enterprise-Control System Integration – Part 1: Models and Terminology", n.d., <<https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95>>.

[MQTT\_SPEC] "MQTT Version 3.1.1 Plus Errata 01", December 2015, <<http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html>>.

[networked-PLC] "Should PLCs be networked?", 4 October 2004, <<https://www.plantengineering.com/articles/should-plcs-be-networked>>.

[OPC] "Open Platform Communications", n.d., <<https://opcfoundation.org>>.

[OPC\_ARCH] "OPC 10000-1 – Part 1: Overview and Concepts", 2 November 2017, <<https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-1-overview-and-concepts/>>.

[OPC\_INFO] "OPC-UA Information Model Specifications", n.d., <<https://opcfoundation.org/developer-tools/specifications-opc-ua-information-models>>.

[PLC-40] Azarmipour, M., Elfaham, H., Gries, C., and U. Epple, "PLC 4.0: A Control System for Industry 4.0", IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society, DOI 10.1109/iecon.2019.8927026, October 2019, <<https://doi.org/10.1109/iecon.2019.8927026>>.

[RECONF] Koren, Y., "Reconfigurable Manufacturing System", CIRP Encyclopedia of Production Engineering pp. 1417-1423, DOI 10.1007/978-3-662-53120-4\_6629, 2019, <[https://doi.org/10.1007/978-3-662-53120-4\\_6629](https://doi.org/10.1007/978-3-662-53120-4_6629)>.

[semantic-addressing]

Jia, Y., Trossen, D., Iannone, L., Shenoy, N., and P. Mendes, "Gap Analysis in Internet Addressing", Work in

Makhijani & Dong

Expires 6 September 2022

[Page 18]

---

Internet-Draft

iiot-vplc

March 2022

Progress, Internet-Draft, [draft-jia-intarea-internet-addressing-gap-analysis-01](https://datatracker.ietf.org/doc/html/draft-jia-intarea-internet-addressing-gap-analysis-01), 23 October 2021, <<https://datatracker.ietf.org/doc/html/draft-jia-intarea-internet-addressing-gap-analysis-01>>.

[SURV] Galloway, B. and G. Hancke, "Introduction to Industrial Control Networks", IEEE Communications Surveys & Tutorials Vol. 15, pp. 860-880, DOI 10.1109/surv.2012.071812.00124, 2013, <<https://doi.org/10.1109/surv.2012.071812.00124>>.

[VPLC-DRAGOS]

Scott, A., "Programmable Logic Controller Virtualization", 8 February 2019, <<https://www.dragos.com/blog/industry-news/programmable-logic-controller-virtualization/>>.

[VPLC\_CONV]

Cruz, T., Simoes, P., and E. Monteiro, "Virtualizing Programmable Logic Controllers: Toward a Convergent Approach", IEEE Embedded Systems Letters Vol. 8, pp. 69-72, DOI 10.1109/les.2016.2608418, December 2016, <<https://doi.org/10.1109/les.2016.2608418>>.

[VPLC\_IIC] Lou, D., Graf, U., and M. Tseng, "Virtualized Programmable Logic Controllers. An Industrial Internet Consortium Tech Brief", 7 September 2021,

<<https://www.iiconsortium.org/pdf/IIC-Edge-vPLC-Tech-Brief-20210907.pdf>>.

Appendix A. Appendix A. Purdue Model (ICA-95)

The International Society of Automation (ICA) has developed a model [ISA95] to describe automated interfaces between enterprise and control systems. In this widely deployed hierarchical model, five levels are defined and they follow a strict ordering of interfaces across the levels. At the lowest level 0, are the physical devices while enterprise applications are at level 5. In between these two levels, there are several supervisory, management, and intermediate data collection applications that provide information to

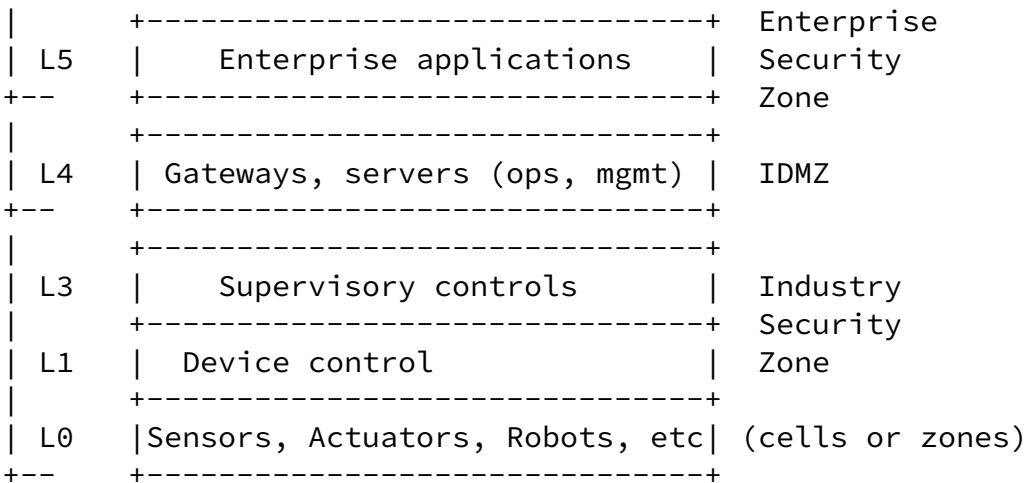


Figure 3: ISA 95 or Purdue model of Automation Pyramid

A.1. Separation between Manufacturing and Enterprise Networks

The ICA-95 architecture recommends hierarchy, thereby a separation

between factory devices and applications through three different security zones called Manufacturing, DMZ and enterprise zones as shown in Figure 3 as below:

- \* Enterprise Security Zone: The IT applications reside in enterprise networks and perform tasks necessary for business operations such as inventory control, supply-chain logistics, schedule and capacity planning. They need to collect data from the OT systems in order to make those decisions.
- \* Industrial Demilitarized Zone: The OT and IT networks were designed to prevent direct communication between them. The IDMZ serves as an information sharing layer between the IT and OT (L4 and L3) systems. This indicates that additional security rules, inspection and protection of device identity and access is necessary when transiting from L3 to L4.
- \* Manufacturing Zone: Consists of Levels 0 through 3 site wide

production system. Operations at level 3 (L3) Support site-wide view of the production system. They also provide data to L4. Area supervisory control (L2) performs operation and control over a zone or smaller area in a production floor. Each area has specific set of tasks or operations to perform. Basic control at level 1 (L1) is for the actual control of the equipment. The L1 components such include PLCs; they send commands to L0 equipments to perform tasks (e.g. start motor, alter pressure level, or reduce motor speed). Finally, actual process takes place at level 0 (L0). At this level for the process equipments performing actual operations are performed. This include equipment and devices such as motors, pressure

valves, temperature, speed, etc sensors, etc.

The devices or controllers at level 1 are the ones of specific interest for virtualization and the corresponding challenges are covered in later section.

#### [A.2.](#) Collaborating with SDOs with Industry Network Focus

The paradigms of networking in OT are quite different than IP based best-effort networking protocols. Yet, IETF protocols are extensively used in OT applications. Often, it is not possible to get contributors directly from the OT sectors, then it would make more sense to coordinate with well-established consortia where OT scenarios and requirements are discussed may be utilized. Two well established foundations are IIC [[IIC](#)] and OPC-UA [[OPC](#)]. For example, a [[IIC TALK](#)] provided overview of IIC activities.

Industrial IoT Consortium (IIC) provides use cases, scenarios, and best-practice frameworks to solve specific problems and solution pain points. It is a rich resources of case studies and demonstrations of different test beds. The IIC itself is not involved in standards development, but may help in formalizing requirements, further insights into solutions developed in IETF, and potentially help adoption of those solutions.

Open Platform Communications-Unified Architecture (OPC-UA) provides interoperability across different hardware platforms using a standard data model. It standardizes various information models, corresponding client-server architecture and defines necessary access mechanisms to those information models. The OPC-UA is an abstraction



layer to provide common interface to different data look-up and event notifications. A number of information models are provided by OPC-UA can be found here [[OPC INFO](#)]. For example, OPC has a specification on PLCs. It abstracts PLC specific protocols (such as Modbus, Profibus, etc.) into a standardized interface allowing HMI/SCADA systems to interface with a middleware that converts generic-OPC read/write requests into device-specific requests and vice-versa.

Note: OPC-UA information model similar to YANG?

IETF solutions will focus on leveraging or extending IETF technologies for IT and OT integration which is at the infrastructure or communication layer. Thus, providing protocols that could potentially benefit higher-level OPC-UA work.

Both IIC and OPC could provide guidance for the standards work.

#### Authors' Addresses

Kiran Makhijani  
Futurewei  
Santa Clara, CA 95050,  
United States of America  
Email: [kiran.ietf@gmail.com](mailto:kiran.ietf@gmail.com)

Lijun Dong  
Futurewei  
Santa Clara, CA 95050,  
United States of America  
Email: [lijun.dong@futurewei.com](mailto:lijun.dong@futurewei.com)