Use Cases for a CIP Companion Specification for OPC UA

Paul Brooks
Manager, Technology
Business Development
Rockwell Automation

Ken Hopwood
Software Architect
ProSoft Technology

Frank Latino
Product Manager
Festo Corporation

Steven Roby
Sr. Principal S/W Engr
Honeywell HPS

Presented at the ODVA
2020 Industry Conference & 20th Annual Meeting
March 4, 2020
Palm Harbor, Florida, USA

Abstract

Having concluded their first round of requirements capturing for vertical integration of **Common Industrial Protocol** (CIP) devices to cloud applications, the Common Industrial Cloud Interface (CiCi) Special Interest Group (SIG) has determined that a key element of an overall solution is an OPC UA companion specification for CIP devices. Based on this conclusion, a plan is currently under development between OPC Foundation and ODVA for a joint working group to produce this companion specification. In order to ensure that this companion specification meets the requirements of both ODVA members, and of users of CIP technologies the CiCi SIG is now refining those requirements to specifically address companion specification relevant use cases.

This paper explores the user stories and use cases against which that OPC UA companion specification shall be developed. It recaps the work done in the CiCi SIG and benchmarks it against the Device Integration model best practices inside OPC Foundation. It will take advantage of some of the recent lessons learned within OPC Foundation that are being addressed in their Harmonization Working Group and will propose a harmonization model that will allow CIP Technologies to integrate seamlessly with the latest OPC UA specifications.

Keywords

EtherNet/IP, OPC UA, Companion Specification,

Definition of Terms in This Paper

The terms in this paper are represented in *Italic* style.

Term 1 -- Description

Related Work

This paper builds on two key areas – the prior work of the ODVA CiCi SIG as presented in [1] as well as the OPC Foundation Field Level Communications Initiative. The goal of this initiative is to deliver an open, cohesive approach to implement OPC UA including TSN and associated application profiles. This will advance the OPC Foundation providing vendor independent end-to-end interoperability into field level devices for all relevant industry automation use-cases. The OPC Foundation vision of becoming the worldwide industrial interoperability standard is advanced by integrating field devices and the shop floor. A new set of working groups is identifying, managing and standardizing the OPC UA relevant topics focused on industrial automation including:

- harmonization and standardization of application profiles like IO, motion control, safety, system redundancy
- standardization of OPC UA information models for field level devices in online and offline scenarios e.g. device description including diagnostics
- mapping of OPC UA application profiles related to real-time operations on Ethernet networks including TSN
- definition of certification procedures

1. Megatrend in Global Manufacturing

Commonly called Industry 4.0, end users of automation products, machine builders and component suppliers are seeing new opportunities to integrate the automation value chain, reduce costs through new business models and implement new techniques for process optimization. The key technology that makes this possible is the internet, coupled with mass data storage and securable real-time global access to this stored data.

This megatrend is most visibly demonstrated from two angles – top down national governments are implementing smart manufacturing initiatives to enable competitiveness of their local manufacturing base; bottom up corporations are providing delivery platforms to monetize digitization domain expertise.

Two examples from the multiple government led smart manufacturing initiatives, together with their core claims are listed below:

- Plattform Industrie 4.0 in Germany: “For Industrie 4.0, it is not the computer that is the core technology, but rather the Internet. Digitalising production is gaining a new level of quality with global networking across corporate and national borders: the Internet of Things, machine-to-machine communication and manufacturing facilities that are becoming ever more intelligent are heralding a new era: the fourth industrial revolution, Industrie 4.0.” [2]
- Industrial Value Chain Initiative in Japan: “The Industrial Value chain Initiative (IVI) is targeting to turn linked factories and connected manufacturing into reality. In some cases, the result that developing a new system at the enterprise as a whole or at its manufacturing site is needed. In other cases, the challenge may be solved through small improvement efforts (kaizen) by applying IoT tools.” [3]

Similarly, two examples of corporate delivery programs and their goals are:

- The Connected Enterprise from Rockwell Automation: “New insights that are revealed through better data access can help you reduce bottlenecks, implement demand-based decisions, and improve maintenance. Greater digitization can help you reduce downtime and improve profitability.” [4]
- Azure IoT from Microsoft “Organizations across all industries are using Azure IoT to invent new lines of business, improve productivity, and reduce waste by using AI and machine learning to quickly process massive quantities of data from all kinds of IoT devices.” [5]

Common factors of all these initiatives are:

- Enterprises need to consolidate information across multiple plants
- Supply chain and value chain partners need to share information during the operational phase of a plant
- Cloud technologies must be used to secure and distribute information, abstracted from local assets

2. Previous work of the Common Industrial Cloud Interface CiCi SIG

At the ODVA Annual Meeting in 2017, CiCi SIG proposed a reference architecture as a basis for their work, shown below in section 3. In addition, the CiCi SIG presented a number of use cases, which are not duplicated in this document, although some are extended. These use cases are organized under different phases of a device's life cycle. The use case explored in this document will be extended to consider the life cycle of more complex automation assets, i.e. a machine or collection of machines. Finally, the use case titles were followed by references to a set of communication patterns between a cloud application and a target gateway device. These communications patterns are explained below the use case titles and are still relevant to realizing these use cases as well as the extended ones described in this white paper. In November of 2018, the CiCi SIG proposed a 'thin slice' approach to their work. This approach is explained in section 6 Thin-slice Approach for CiCi, and the conclusions assume that it will be expanded to address the user stories documented in section 5 User Stories (Use Cases).

Commissioning

- Out-of-the-box definitions (Inquiry, Command)
- Cloud Registration / backend business setup (Inquiry, Command)
- On-boarding/Provisioning (Inquiry, Command)
- Context of device in application (Inquiry, Command)
- Control/Application loading (Inquiry, Notification, Command)

Operating

- Monitoring (Telemetry)
- Maintenance (Telemetry, Command)
- Calibration (Inquiry, Command)
- Diagnosis (Telemetry)
- Alarms/Events (Notifications)
- Enable/Disable (Command)
- Optimization / Changing Parameters / Programs (Telemetry, Command)
- Software/Firmware updates (Inquiry, Notification, Command)
- Device Replacement (Inquiry, Command)

Decommissioning

- Removing a device (Telemetry, Command)

Communication Patterns

- Telemetry - Telemetry is data flowing from a device or gateway to the cloud. It is the most commonly used pattern

- Inquiry – Inquiry is a request from a device or gateway to the cloud for some needed information and a response is expected. e.g. Is there a new software update available? Is there a definition or profile for a device recently discovered on the automation network?

- Notification – Notification is a device or gateway publishing a notice of a state or condition of interest that should be consumed by the cloud and presented to a user for some action.

- Commands – Commands are instructions sent from the cloud to a device or gateway in order to initiate some action. This action could be taken by the device itself, e.g. reboot or reset, or it could an action taken by an application, e.g. browse the automation network to discover any new devices.

3. Reference Architecture

The use cases and technical requirements for data transfer white paper proposed a Reference Architecture for a CiCi gateway solution [1].

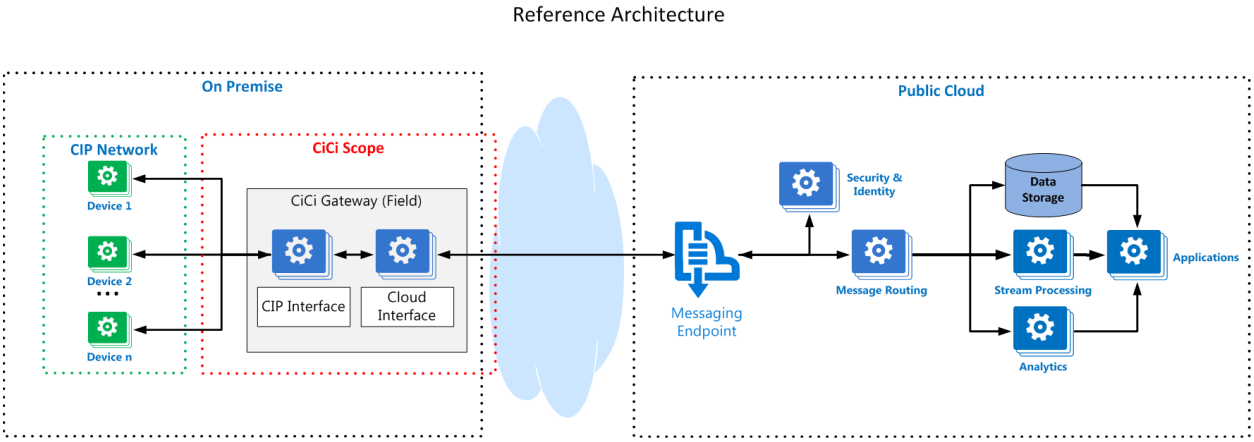

Figure 1 – CiCi Reference Architecture (2017)

This reference architecture assumes that within a plant (on-premises) the user is concerned with only one communications technology.

This paper will expand the reference architecture to assume a need to support information coming from multiple communications technologies

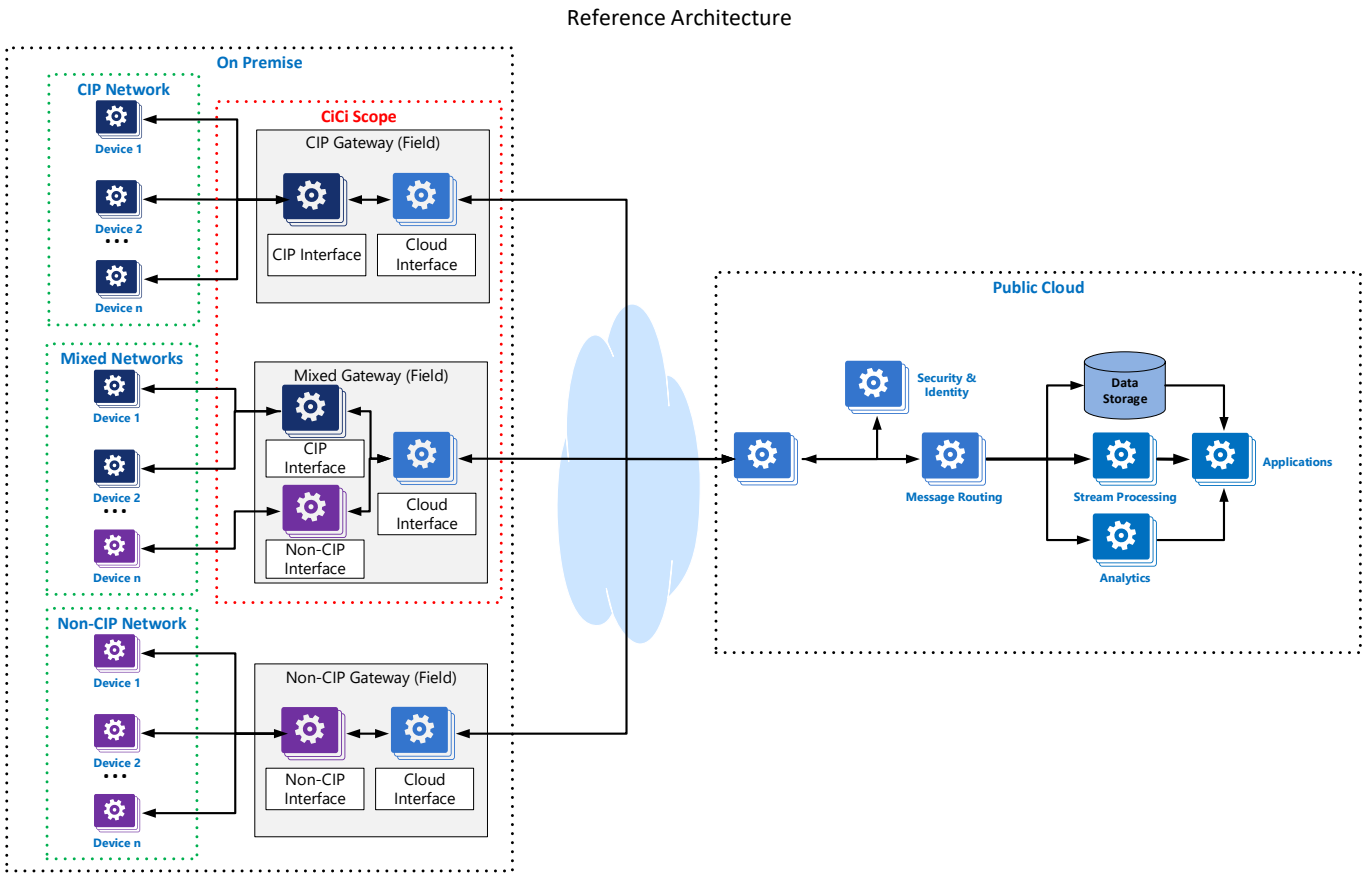

Figure 2 –Reference Architecture (2020)

In writing this paper, the assumption is that OPC UA is a critical partner technology and that joint work will be performed in order to deliver a companion specification. Through the rest of this paper it is assumed that:

- the cloud interface will use an OPC UA information model
- the cloud interface will use OPC UA transport mechanisms (MQTT, AMQP or HTTPS)
- the cloud interface will use OPC UA defined cybersecurity roles, authentication and encryption

The use cases/user stories below will attempt to explain why these are reasonable assumptions.

4. The Industrial Value Chain

In this section we define the stakeholders, both from the perspective of the types of organization, companies and other entities that add value to an EtherNet/IP device through its supply chain, together with the human roles fulfilled across those entities.

Stakeholders represent the legal entities who have interest in a particular story. There may be multiple legal entities who hold a stake in a particular story. For instance, time saved by a system commissioner employed by an SI, contracted to a machine builder and working in a manufacturing plant is supporting three stakeholders.

Stakeholder	Description
Plant Owner	An end-user of automation components. A plant owner is most concerned about the operational phase of an automation system's lifecycle and will make standardization decisions to manage that lifecycle cost. A plant owner will typically outsource system design and implementation to an outsourced partner (or sometimes an in-house centralized function) within a defined framework and against defined deliverable Key Performance Indicators and Service Level Agreements.
EPC/System Integrator	Engineering Procurement Contractors (EPC) take turnkey responsibility for an entire plant construction. An EPC will typically be contracted directly by an end user. System Integrators take a similar turnkey responsibility for the control and automation system, either for a plant unit or for an individual piece of equipment. Consequently, system integrators may be contracted by plant owners, EPCs or machine builders. Both groups have split responsibilities in that they must operate as a representative for their customer, making decisions in their customers' best interests, but will frequently have been contracted on a lowest cost bid.
Machine/Skid Builder	Machine and Skid Builders will provide a piece of equipment that directly and mechanically affects production. Skids are typically deployed in processing applications and take their name from the mechanical framework in which they are deployed. An example is a compressor which takes air at atmospheric pressure and provides a high-pressure supply to drive secondary equipment. A machine in a food application may be a vertical form fill and seal machine whose primary purpose is to take in two flows of material, one the primary product and the second a web or primary packaging, and seal a defined package around a measured amount of product. Machine/skid builders are today looking for new business models to generate recurring revenue.

Stakeholder	Description
Device Vendor	Device vendors sell Automation Components. They will develop, mass produce, and sell device types which must frequently be produced over many years and multiple backwards-compatible releases with revised hardware and/or incremental functional enhancements.Device vendors' principal concerns are about: • the manufacturing cost of their automation component • the time to market of a new product • the performance of the product in its target application • the ability to implement functionality over and above the base features of the standard Software, Controllers, I/O, Drives, Servos, Instruments, Sensors etc. vendors may be considered as device vendors.

These descriptions are not intended to tell any given user story. They are simply intended to provide enough context for the author of a user story to select the most appropriate actor.

Actor Job Title	Description
Business Manager	Decisions will be primarily taken for non-technical reasons and will be driven by business strategy, direction and financial impact to their operations. A device vendor will be considering product available market, differentiation against other technologies and ability to differentiate with their competition. A machine/skid builder will be considering total cost of deployment of their machines including commissioning and potential to deliver annualized services. A system integrator/EPC will be considering total cost of ownership for their customers and expandability to future services.
Engineering Director	Decisions will typically be taken for operational reasons and driven by Key Performance Indicators - to reduce number of engineering hours, to mitigate risk of deployment, or to future proof the implementation. More than any other persona the engineering director will be prepared to purchase at a higher price based on Unique Selling Points (USP) in order to remove risk to other projects or overruns. The engineering director will typically be responsible for standardization decisions that implement multiple plants/machines/skids, rather than point decisions on a single implementation. At a device vendor and machine/skid builder, the Product Security Officer falls into this category of actor.

Actor Job Title	Description
Product Developer	Product developers are employed by device vendors. They are rarely responsible for deciding which communication technology to implement in an off-the-shelf automation component. However, they are a key consultant in prioritizing developments which are competing for their time. Factors that they will report on are: • Time needed and complexity to implement the technology. • Performance of a component using that technology. • Ability to implement differentiating capabilities with that technology. Product developers report into engineering directors and will typically execute detailed research/reporting to support decisions taken by the engineering director
Process Engineer	Process Engineers are responsible for defining the way in which a product is made, or how a process operates. They will be responsible for the algorithms deployed by the Controls Engineer and their role can include the definition and management of recipes or machine settings. The Process Engineer may also hold responsibility for the optimization of operations to meet given quality standards. A desire to achieve continuous improvement of production may drive the decisions a Process Engineer may take.
Controls Engineer	The Controls Engineer is responsible for the design of an automation or control system prior to commissioning. Their primary responsibility is the programming/configuration of the application code in a PLC, PAC or DCS (etc.) necessary to execute algorithms defining operation of a piece of equipment. In support of this function, they are typically responsible for the integration of automation devices into the controller engineering tools and the parameterization of those devices with all information necessary for their correct functional operation. As part of their responsibility, they may also be responsible for defining access rules and for putting systems in place to protect against incorrect or unintentional modification of the automation control system The controls engineer is likely to be more intimately engaged in the technical details of EtherNet/IP and OPC UA than any other actor (apart from the original product developer). A controls engineer will generally be responsible for selecting the devices that must be integrated into the control system and the technologies used for that integration. When employed by a Plant Owner, the Controls Engineer will typically be part of a centralized team independent of any single plant. Within the Controls Engineer actor, there are multiple disciplines including Safety Engineer, PLC Programmer and Process Automation Engineer, all of whom fulfill essentially the same function but with differing expertise.

Actor Job Title	Description
HMI Engineer	The HMI engineer is responsible for design and configuration of all human machine interfaces, including machine level embedded HMIs, plant wide supervisory control systems, manufacturing execution systems and enterprise dashboards. The HMI engineer is likely to be familiar with OPC UA Client-Server, Data Access, Historical Access, Events and Alarming functionality and desire consistent interfaces across multiple industrial protocols.
Network Engineer	The network engineer is responsible for design and configuration of the network infrastructure and implementation of network security technologies. At the machine or skid level, the network engineer will often be the same individual as the controls engineer. Within EPC/SI and Plant Owners, the network engineer will generally be a specialist with little knowledge/understanding of control systems and their devices. They will frequently report into the IT department and be responsible for the security of a system and the service level delivered to individual subsystems. They will consider the control systems to be only a subset of users of the overall network, while also recognizing the criticality of that system.
System Commissioner	The System Commissioner is responsible for startup of a system once it has been installed in a manufacturing/processing plant. In small system integrators and EPCs, the commissioning engineer may have operated as controls engineer earlier in the project lifecycle. In machine/skid builders, the commissioning engineer may never have met the controls engineer in-person as they may work in different continents or the machine design may be many years old. The System Commissioner will not be involved in technology decision making. However, they operate at the most expensive point in a system's lifecycle - where all capital has been spent but no production has started and so technologies that minimize their time are valued by both business managers and engineering directors.
Data Scientist	The Data Scientist is responsible for applying mathematical technics to data streams collected from automation asset in order to optimize production, discovering root causes of plant inefficiency. Data Scientists harvest large datasets from plant floor operations and use statistical analysis and artificial intelligence tools to identify previously unrecognized linkages and variances in data values. They then work with subject matter experts (usually other Actors) to eliminate the sources of these variants. Data Scientists will always prefer technologies which: • Present information at source with context • Require no other actors to extract that data from the plant • Enable storage and analysis of data using commercial technologies. Roles for this Actor are evolving with AI technologies. An example is a relatively new role is a Machine Learning (ML) Engineer.

Actor Job Title	Description
ML Engineer	ML Engineer is an emergent role that is incrementally taking over Data Scientist activity. ML Engineer replaces Data Scientist activities that involve repetitive actions and actions that can be fully automated. For example, ML model characterization and data-to-ML model mapping is a fully automated process. ML Engineer is familiarized with modern ML modeling frameworks that remove the need for ML level coding. ML Engineer has a direct dependency on Data Engineer during the dataset preparation and ML-model consolidation.
Maintenance Technician	The Maintenance Technician is responsible for ensuring ongoing operation of plants through their multi-year operational cycle. While rarely the decision maker in a technology decision, they are key influencers and are typically the most trusted consultant for the plant manager. Some of the issues that will drive their advice are: • Time to replace failed components. • Proper Spare Parts management and storage • Ability to predict, plan and execute maintenance intervention. • Longevity of the technology (e.g. typically a 20-year operational life). • Ease of availability of external skilled staff. • Intuitive operation (as it may be 5 years from training to first use!).
Maintenance Support	Maintenance Support is typically an outsourced function from a plant owner and typically functions remote from the plant. It therefore represents a significant cost saving for the plant owner, providing technology choice enables it. Maintenance support is typically associated with either a product type supplier or with an equipment type supplier. Typically, maintenance support is enabled by: • Ability to deep dive into the internals of a piece of equipment; potentially accessing information not visible to any other actor. • Ability to historically analyze performance over time. • Ability to remote operate these components (within safety bounds). Maintenance support typically does not have any knowledge of plant operation or function.

Actor Job Title	Description
Instrument/Drive Technician	The instrument/drive technician typically has deep expertise on a particular type of device giving them skills to configure that device for a specific application. They typically work with or in parallel the system commissioner and use dedicated tools (ranging from hand-held configurators through to full-fledged PC based software applications) for the devices that they are configuring. Frequently (and especially when this is an outsourced skill) they will have no access rights to any other engineering tools. It is critical that once the Instrument/Drive Technician has completed their work, the configurations that they have created persist throughout the lifecycle of the equipment configured and are propagated to multiple duplicates of that equipment.
Plant Manager	The plant manager is typically the budget holder for new investments including automation technology. The plant manager will be most interested (through the lifecycle of an investment) in: Worker Safety Time to market for the product manufactured in their plant Capital investment required to start producing (multi-vendor interoperability impacts this) Operational costs including: Production throughput Operational effectiveness (% of working time that production is running) Energy consumption Flexibility in reconfiguration for future demands Expandability Longevity
Security Officer	The Security Officer has no direct stake in production operations or technologies. They, and the team that reports to them, are responsible for ensuring that there is no unauthorized access to production operations (whether from an outside hacker, inside bad actor or former employee). They are also charged with ensuring that the propagation of viruses (worms, malware, ransomware etc.) is restricted and that reasonable measures are taken to ensure resilience against these threats. They are responsible for the management of proprietary data entering and leaving facilities. The Security officer will typically assume that any cyber-security mechanisms will be breached and is also responsible for minimizing reputational damage when this occurs.
Process Operator	The Process Operator is responsible for monitoring and controlling the actual process. This role will need to have a view into the big picture of operations, monitor and optimize equipment performance, and identify possible problems with plant operations. They are responsible as the first-line of defense to raise alerts to Supervisors or Control Engineers when there are problems with the system. This would include alarms/alerts received regarding the Cloud Interface infrastructure.

5. User Stories (Use Cases)

5.1. Optimizing Production Processes

As a Plant Manager I want to enable my Data Scientist to be able to access data from my assets, so this data can be analyzed and used to optimize production.

As a Data Scientist, I want to be able to discover my assets and their associated devices that may provide useful data for analysis, so these devices can be further queried for the data they may contain.

As a Product Developer, I want to expose only data that are useful for optimizing the specialized asset, so data collection is simplified for customers and plant operators.

As a Business Manager at a Device Vendor, I want to enable my Data Scientist to be able to access some data from my Devices, so that my Data Scientists/specialists can make recommendations that result in operational improvements.

As a Plant Manager, I want to only expose data that will not disrupt the operation of my assets, so that unnecessary downtime can be avoided.

As a Process Engineer, I want to assign data reading resources, so that there is adequate bandwidth for operating my facility and providing data for analytics.

As a Security Officer, I want to guarantee that only authorized connections can be made to my assets and only authorized devices can be discovered and authorized data can be read.

The native protocols of the devices in these use cases are not important to achieving the desired outcomes. In most operations, there are mixtures of vendors and protocols in use. What is important is enabling these actors to have access to data contained in their assets. The “shape” or context of the data is also very important to the value of the data. More context makes it easier to provide valuable insights. Also, data scientists use different tools that are aligned with cloud technologies, largely due to the significant amounts of data storage and process power required. These technologies are evolving to be able to take advantage of computing power on the “edge,” but they still require services or mechanism that will discover devices on the network, specifically for CIP devices, pull information from the data available and present that data in a standardized way to applications on-premise and on the cloud.

5.2. Machine/Skid Builder/Integrator offering remote service of own supply

As the business manager of a machine builder, I want to offer value added annualized services to my customers. In the long term, this will be leasing machines on a usage basis, but the next step my users are prepared to take is outsourcing maintenance. In order to deliver these services, I am prepared to invest significantly in additional instrumentation from multiple vendors and software in the machines that I deliver. I want to be able to create parts of the information model in controllers that is only available for me to access – I consider this information to be mine and not my customers and not for use by other service providers. In order to simplify access, I want to be able to deploy a single gateway function (either in a standalone compute appliance or embedded in the controller I select) which will provide connectivity to my own historical cloud storage. I want this gateway to be able to securely deliver my proprietary information together with standardized and vendor specific information from the components, together with application specific information in controllers and information from discrete devices in the machines.

For the machine builder, supporting the native protocol required at a plant is critical to their business – essentially the same machine will be delivered using both CIP and third-party protocols to the different plants – it is only in hybrid plants that the machine builder may have any autonomy.

However, like the data scientist the machine builder will have a strong preference for a single cloud-friendly protocol to deliver consistent information from all of the plants.

This story brings a new requirement which is around role-based security – that the provision of information to the cloud is controlled by the machine builder and not by the user of that machine.

Further delivery requires input from the plant network engineer who will be responsible for appropriate creation of firewall rules. The fewer technologies deployed, the less work and more importantly, the less risk created.

5.3. Increased service delivery

As I increase the number of machines on which I deliver these services, I will want to adjust the information that is delivered to my cloud storage based on experience gained. I must be able to make these changes without physical access to the gateways. I must be able to document and enforce a service agreement with my users about changes that can be made to the running system.

Also, like the data scientist, they will have a strong preference to be able to select variables for monitoring long after commissioning – to avoid replicating the entire machine database in the cloud.

5.4. Provide information from inside a machine for Data Analysis

As a data scientist working for a Plant Owner, I want to get "important" or pre-selected data and context from my assets so that I don't have to understand or learn each asset in my enterprise.

Extending from story 5.1 Optimizing Production Processes, the data scientist will prefer technologies supported by their cloud vendor, with no concern for the technologies supported by the Device Vendor. The selection of cloud drives communications and not the other way round!

More importantly, the data scientist cannot be assumed to have any domain expertise in either field level devices or communications technologies. Consistent semantics across components, technologies, machines and plants are critical to their success. This means that in the CIP driven plants, all devices must present their metadata using common and well-defined terms and meanings/interpretations. But for the data scientist, whether the plant is CIP driven or third party driven is irrelevant – they want to see the same semantic definitions presented in both cases. This is even more true for the hybrid plant.

To facilitate this device discovery, services to collect the metadata available in each device, and a method to build the metadata into an information model without manual configuration, will be important for adoption.

It is worth noting that the OPC Foundation has a program running called "Harmonization" to address this problem within their own family of companion specifications. Our objective should be to minimize the pain to our users and that we do not increase it.

5.5. Device vendor offering remote service of own supply

As a Business Manager at a Device Vendor I want to connect to devices when then are used by either machine builders or end users, so that I can offer remote services to ensure the devices I have supplied are operating properly.

For this purpose, a plant operator needs to grant access to the installed devices for the device vendor but only to the devices of interest. As a device vendor, I want to setup an ad-hoc and exclusive connection to the device and I also may setup a continuous monitoring routine. As a plant operator, in order to allow remote access to devices, I want full control on the permission levels and time, when the access occurs (is allowed to happen). As plant operator, I need to be able to notify the subscribers of a device's data about the potential un-availability of function.

In many ways, this story is identical to the machine builder stories, but with completely different cloud suppliers and information flows involved. Our objective must be to ensure a single approach supports both stakeholders.

A key value is that plant maintenance technicians cannot be practically expected to have expertise in every device in their plant. This support may be delivered in an ad-hoc manner, rather than the programmed and scheduled manner of machine builder support.

5.6. Asset management of installed base

As a plant owner I want to be able to establish an asset management system in my plant, which is able to read the asset management / identification parameters from each device/component (hardware/software) that is installed in my plant, so that it is possible

- *to search for components (hardware/software) for which a recall action, Software termination or a hotfix/update exists.*
- *to create a complete inventory list of all installed and communicating components (hardware/software) for easier root cause analysis in case of failure.*

Asset management is typically performed across multiple plants with common identification approaches needed for all devices. Again, this means commonality between CIP and third-party technologies to deliver the anticipated value.

It should also be noted that the security officer is a key stakeholder in the asset management use case, having a responsibility to respond to vulnerability notifications from vendors and put in place remediation plans.

5.7. Anyone has access to data in Devices

As a product developer of a new and innovative software application, running on a blade server (on-prem or in-cloud) I want to be able to find all of the components (controllers or devices) that have potentially useful information using off-the-shelf browse mechanisms. I do not expect the original developers to have planned for my use. I know that some of those devices will provide me information directly and some will be represented by aggregators or other edge-gateway type devices. Once I have found useful information I want to be able to read it whenever I want using off-the-shelf mechanisms. While my task will be made easier with devices because of the consistency of their information models, I do not expect to have knowledge of any specific mechanisms (state machine, application relationships etc.) to read that information.

This is probably the most import Industry 4.0 related story in this paper, in which the value of a project is derived from application of software and not directly by the device or automated system. In this case, the communication technology will be determined solely by the software developer and it is the responsibility for CIP devices to provide data for these applications in the desired mechanism(s).

These software applications will be customized based on the installed base of devices and equipment, so discoverability of information contained in CIP devices will be needed. In addition, both on-line and off-line enumeration of information may be needed as some applications may require configuration prior to delivery. The following applications may be considered applicable to this story:

- IoT Gateways
- HMI, SCADA or MES
- Analytics, including Machine Learning
- Energy Management
- Predictive Maintenance

5.8. Browsing the network for optional information

A story where the user wants to browse the network to find optional information – e.g. to identify all instruments whose calibration date expires in the next 6 months. Not every device has this information

5.9. Common diagnostic view

As a process operator of a machine at a manufacturing plant I want the diagnostics for all of the components in my system to be automatically aggregated into a single user view. I want to be able to filter this view to isolate network diagnostics, component diagnostics and application diagnostics. Where there is time available, in the device (and I know that not all devices will support time), I want it to be presented as a common wall clock time and I want any timestamps to be generated at the lowest level in the architecture where time is available in the system and for that time to be maintained with the diagnostic.

This story requires a significant level of integration between the CIP plant level technology and the OPC UA 'up-link' technology. Some of this integration may require extensions to the CIP protocol to be made possible and others may result in conformance-testable gateway functionality.

5.10. Minimize number of Security Servers

As an Engineering Director at a system integrator, I want to deploy the smallest number of security technologies and servers possible to cover all of the sub-systems that I am delivering, of which industrial automation is a subset. Further, I want to avoid the risk of forcing my customers to deploy a security server solely for the control systems that I deploy.

Proliferation of security technologies across communications technologies is already becoming a source of pain for many users, generating a need to manage authentication and key servers for each. As the companion specification is developed, it must address the needs for integration of security across technologies as well as the integration of information.

5.11. A Common and Consistent Security Policy

As the Security Officer, my role is to minimize the security risk to the operations of my organization. I want to ensure that the desire for easier and faster access to production information is achieved in a way that protects the intellectual property of the organization. As well as considering both the IT and OT domains on-premise, I will want to ensure that any off-site storage of my organization's proprietary data is managed in a way that minimizes the chances of it being compromised.

As part of my role, I need to ensure that tools are in place to allow the organization to define and implement rules for access and authentication, whilst providing accounting capabilities so that access can be monitored and reviewed. I will define policies – based on a risk assessment – that need to be implemented to mitigate against these risks.

A specification for cloud connectivity therefore needs to reflect industry best practice, allowing a solution to build on the strengths of each domain, while preserving end-end security. It needs to address aspects such as the interaction between internal and external technologies and policies – as well as to provide the means to address practical aspects such as defining policies and procedures for the management of servers. Definition and rights of roles needs to be consistent from device to cloud.

5.12. Alarmable Conditions and Scenarios

As a Process Operator at a manufacturing plant, I need to be able to monitor all devices, including edge devices and cloud interfaces such that if they go into alarm, I need to have a common troubleshooting procedures to be able to know what I can do myself, or when to alert a supervisor.
If the devices create an actionable event, such as a confirmable message on a process control system, I need the content of the message to provide clear instructions to be able to take the proper action.

5.13. Common Maintenance Activity

As a Maintenance Technician, I need to be able to replace equipment based on regular maintenance schedules, or in the case of faulty equipment, and I need to have clear indications (via logs, alarms or maintenance recommendations) as to which devices need replacing. This could be equipment such as an edge gateway or a cloud interface hardware. I need to have access to spare parts in a timely fashion from a storage depot or maintenance back office. The replacement of this equipment should be intuitive, or clear replacement procedures readily available online, or physically printed on site.

5.14. Brownfield Installation Improvement with Regulations

As a Plant Manager responsible for a pharmaceutical production operation that is currently validated by the Food & Drugs Agency (FDA) I am being tasked to provide additional data of my processes to support Good Manufacturing Practices (GMP)facilitate an energy management campaign for ISO 50001, and other overall operational improvements.

This data includes asset, diagnostic and process data. Asset data can include device type codes, revisions, catalog, and serial numbers. Diagnostic data may include alarms, fault codes, memory faults, etc. Process data would be values such as pressure, flow, temperature, etc.

My current system has CIP devices with interesting data that I can use. I may also need to add a third-party device (non-CIP) to my network for additional data. I would need a gateway to collect this data, possible contextualize the data, and send it to a cloud for monitoring and analysis.

A variance to the risk assessment for validation protocol can be written since we are not modifying/changing the control program, any devices or functionality to the production operation. It is important that we do not have to undergo revalidation to save time, costs while retaining optimal uptime.

It is necessary to have a gateway that is secure, does not receive inputs from the cloud, only pulls data from devices and pushes it to the cloud. It should also have an ability to contextualize some data before sending to the cloud if needed. This should not impact the validated process and equipment, and, provide a risk-free way of data collection for analysis. There must be no programming or commissioning changes required at the PLC/DCS.

6. Thin-slice Approach for CiCi

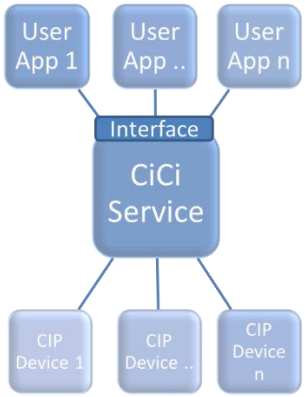

Figure 3 - CiCi Service

The premise of the CiCi SIG was that Cloud vendors have “preferred gateways” that can be used by a “User” application to send data to/from cloud. Therefore the task of ODVA is to provide an <interface> that “User” applications could use with the following functions:

- Browsing / Discovery of CIP devices on the local subnet
- Provide Identity Object information from discovered CIP devices
- Provide Connected/Not-Connected status of any valid CIP device address
- Return an EDS file from the device, if it exists
- Return values of parameters that are defined in an EDS file
- Return values for parameters or assemblies as defined in a Device Profile

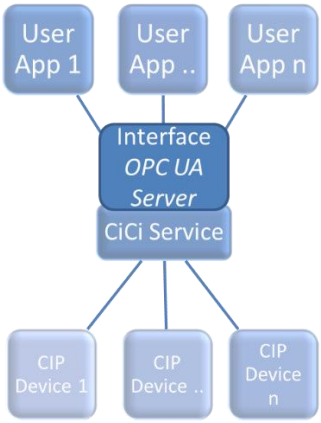

Figure 4 - CiCi OPC UA North Side Interface

The CiCi SIG concluded that a well-defined “interface” would eventually require similar basic functionality as an OPC UA Server for security, diagnostics, discovery as well as data types and the production of data – functionality that does not exist within the CIP suite today in a directly applicable format.
Review of several OPC UA companion specifications confirmed that similar “thin slice” functionality has been defined for other standards i.e. IO-Link.
A CiCi Service should be scoped to provide functionality similar to other OPC UA companion specifications, combined with work to represent any CIP objects in an OPC UA Server
Increasing functionality of the “interface” beyond what could be defined in an OPC UA companion specification would likely be “device management” functions that may be defined by xDS or other SIGs.

7. OPC Foundation Companion Specifications

Figure 5 Scope of OPC UA Within an Enterprise, demonstrates OPC Foundation's self-declared goal [6]. As can be seen, the focus is primarily on vertical integration from the device to software applications, both on-premise and cloud-based.

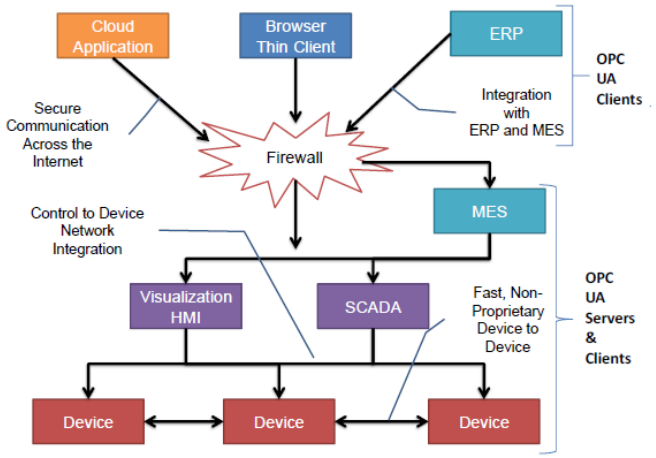

Figure 5 Scope of OPC UA Within an Enterprise

However, they recognized, as articulated in user stories 5.1, 5.4, 5.6, 5.7 and 5.9, that the consumer of information used in devices is unlikely to have detailed knowledge of the field level protocols used in the interaction between controller and device. In April 2019, the Foundation published specification Part 100: Device Information Model to provide the harmonized interface called for to create the north side interface (Figure 4 - CiCi OPC UA North Side Interface) by CiCi SIG's November 2018 proposal.

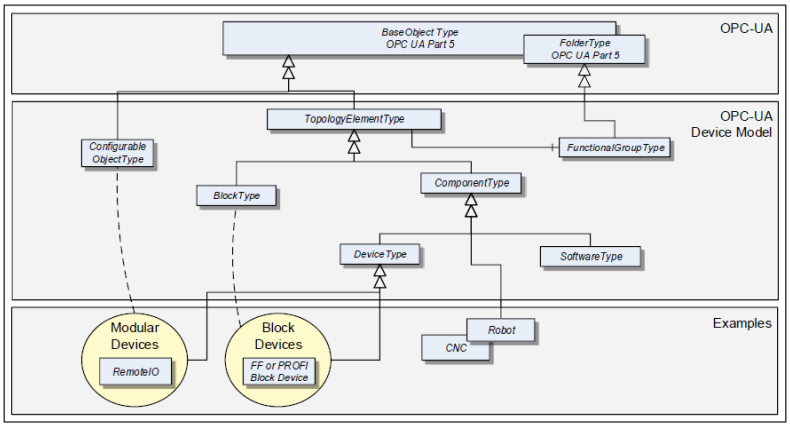

Figure 4 – Device model overview

Figure 6 OPC UA Device Model

8. Conclusions of CIP Requirements for OPC UA Companion Specification

In order to validate the assumptions made in section 3 Reference Architecture, we must address two questions:

- Do the use cases require technologies not available in the CIP family of specifications?
- Are these technologies readily available within OPC UA and are they acceptable to our actors?

In this table, a ✔ represents a capability largely in place that can be used essentially as is. A (✔) represents a capability partially in place that requires completion in a CIP-OPC UA context

Capability	Actor	Story	CIP	OPC UA
Discovery from Cloud	Data Scientist	5.1	(✔)	(✔)
Human readable information model in device	Data Scientist	5.1		✔
Discovery in plant	Data Scientist	5.1, 5.7, 5.8	(✔)	(✔)
Role based security	Product Developer Business Manager	5.1, 5.5		✔
Gateway Function	Process Engineer Controls Engineer	5.1, 5.2, 5.13, 5.14		(✔)
Common semantic presentation of devices using varying protocols	Data Scientist Controls Engineer	5.1, 5.2, 5.3, 5.4, 5.7, 5.8, 5.9, 5.14	(✔)	(✔)
Device Level implementation	Business Manager	5.2	✔	
Contextualization	Business Manager	5.2, 5.14		✔
Granular Data Privacy	Business Manager	5.2		✔
Cloud supplier independence	Business Manager	5.2, 5.14		✔
Vendor specific information model	Business Manager	5.2	✔	✔
Firewall friendly	Networks Engineer	5.2, 5.14		✔
Data reads changeable in run-time	Data Scientist	5.3, 5.7, 5.14	✔	✔
Cloud supplier pre-integration	Data Scientist	5.4		✔
Automatic model generation	Data Scientist	5.4, 5.14		
Single in-plant security management	Plant Manager	5.5, 5.14		
End-end security	Security Officer	5.5		(✔)
Notifications	Maintenance Technician	5.5, 5.12, 5.13		✔
Asset Management	Plant Owner Maintenance Technician	5.6, 5.13, 5.14		(✔)
Rich Identity	Maintenance Technician Security Officer	5.6	(✔)	(✔)
Consistent Diagnostic Model	Maintenance Technician Plant Operator	5.9		(✔)
Common presentation of time	Maintenance Technician	5.9		✔
Unified Alarming	Maintenance Technician Plant Operator	5.9, 5.12, 5.13		✔

Capability	Actor	Story	CIP	OPC UA
IT Centric Security	Plant Manager Security Officer	5.10, 5.11		
IT Integrated Security Policy Management	Plant Manager Security Officer	5.11, 5.14	(✔)	(✔)
Security Audit	Plant Manager Security Officer	5.11, 5.14		✔
Automated Replacement of Devices	Maintenance Technician	5.13	✔	

Our conclusion from this is that there is a compelling case for generation of an OPC UA companion specification for CIP to OPC UA Gateways, based on the assumptions:

- the cloud interface will use an OPC UA information model
- the cloud interface will use OPC UA transport mechanisms (MQTT, AMQP or HTTPS)
- the cloud interface will use OPC UA defined cybersecurity roles, authentication and encryption

This is because almost all of the functionality missing from CIP is available already in UA; it is a far simpler task to integrate CIP using a companion specification, potentially supplemented with enhancements to the CIP specifications than creating a competing approach from scratch. The functionality which is missing from OPC UA is typically device centric functionality long-standing in CIP specifications and ODVA core competency.

References

[1] S. C. Briant and T. Whitehill, "Use Cases and Technical Requirements for Data Transfer," in *ODVA Industry Conference and 18th Annual Meeting*, Palm Harbor, Florida, USA, 2017.

[2] Plattform Industrie 4.0, "https://www.plattform-i40.de/PI40/Navigation/EN/Industrie40/WhatIsIndustrie40/what-is-industrie40.html," [Online].

[3] Industrial Value Change Initiative, "https://iv-i.org/wp/en/about-us/whatsivi/," [Online].

[4] Rockwell Automation, "https://www.rockwellautomation.com/en_NA/capabilities/connected-enterprise/overview.page," [Online].

[5] Microsoft, "https://azure.microsoft.com/en-us/overview/iot/," [Online].

[6] OPC Foundation, "https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-100-device-information-model/," [Online].