Communications, protocols and information modeling: The fundamentals of IoT, IIOT, M2M, industrie 4.0

Thomas Burke

OPC Founder & Visionary

Thomas.Burke@opcfoundation.org
NEW • ONLINE NOW & IN STORES SOON

CONNECTED COFFEE

NESPRESSO PRODIGIO ESPRESSO MACHINE with MILK FROTHER

The newest Nespresso machine is also the smartest, thanks to smartphone compatibility.

GET CONNECTED

Smartphone connectivity and alerts for water, capsule stock and descaling keep you in-the-know on your machine’s status.

$299.00 + SHIPS FREE
The racket, has gyroscopes, accelerometers and a piezoelectric sensor in the handle. These sensors pick up a variety of data, including where the ball hits the strings, how much power goes into a shot and how much spin a player puts on a ball.
The value of IIoT ........

Often expressed in mind-boggling numbers
OPC Foundation

- Broad Vision
  Secure, reliable, multi-vendor, multi-platform, multi-domain information interoperability from sensor to enterprise

- International Scope
  ◦ Non profit organization (founded 1995)
  ◦ Companies from Automation & IT
  ◦ Standard: OPC UA is IEC62541

- Deliverables
  ◦ Open Specification
  ◦ Tools: certification tools
  ◦ Compliance Labs

- NOTE: Professional OPC UA Toolkits are the ecosystem

OPC Members

OPC Board

- Microsoft, SAP, Siemens, Beckhoff, Honeywell, Yokogawa, and others
- New members coming soon
# The Industrial Interoperability Standard

*OPC UA: The industrial framework enabling secured, standardized data and interfaces*

## Interoperability
- **Independent:** Vendor, Platform, Market and OS
- **Discoverable Service Oriented Architecture (SOA)** independent of the transport method
- **Run by a Non-Profit (OPC Foundation)**
- **60M install base** and exponential growth
- **Scalability:** From Sensor to Cloud

## Data Modelling
- **Rich data modeling** (preserves data context)
- Vendors can extend the data model of each product (Companion Specification)
- Maps domain specific protocols, e.g. BACNet | MTConnect | Weihenstephan…
- Maps domain specific information e.g. Robotics, Machine Vision, …

## Security
- **Secure by Design**
- Based on **open security standards**
- **Authentication | Encryption**
- **Evolves** with Security Industry standards
- **Scalable security**
Upcoming Global OPC UA Initiatives

**United States**
Industrial Internet (Consortium)
Smart Manufacturing
Industry 4.0

**EU / Western Europe**
- Austria: Industrie 4.0 Österreich
- Belgium: Factories of the future
- Czech Republic: Průmysl 4.0
- Denmark: MADE
- France: L’Industrie du Futur
- Germany: Industrie 4.0
- Hungary: IPAR4.0
- Italy: Industria 4.0

**China**
Made in China 2025

**Japan**
Robot Revolution Initiative
Society 5.0

- **Industrial Internet**: US concept (GE) but Industrial Internet Consortium global and collaborates with Industry 4.0 Platform.
- **UK**: Industry 4.0 and 4IR initiative. Post-Brexit unknown.
- **China**: Industry 4.0 the framework of “Made in China 2025”
- **Japan**: several initiatives, collaboration Industry 4.0 Platform.
Example testbeds with integrated OPC UA:

1. SMART MANUFACTURING CONNECTIVITY FOR BROWN-FIELD SENSORS
2. TIME SENSITIVE NETWORKING (TSN) TESTBED
3. SMART FACTORY WEB TESTBED

https://www.iiconsortium.org/pdf/IIC_PUB_G5_V1.0_PB_20170228.pdf
## Industrie 4.0 Requires OPC UA

### Industrie 4.0 Full
**Target:** standards, norms and research, > 5 years

**Definition of full Industrie 4.0 properties incl. strategic outlook**

### Industrie 4.0 Ready
**Target:** manufacturers, < 5 years

**What are the minimum properties that products must have in order to participate in the Industrie 4.0 network?**

### Industrie 4.0 Basic
**Target:** customers, today

**Which products are currently well prepared for Industrie 4.0?**

<table>
<thead>
<tr>
<th>Industrie 4.0 communication</th>
<th>Industrie 4.0 services and conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer of product data and data files for interpretation or simulation, for example: product data in standardised form. The product can be addressed via the network, supplies and accepts data, Plug &amp; Produce via Industrie 4.0-compliant services.</td>
<td>Definition still open (service system). General interface for loadable services and messages regarding statuses. Essential basic services that an Industrie 4.0 product must support and provide.</td>
</tr>
<tr>
<td><strong>T</strong></td>
<td><strong>O</strong></td>
</tr>
<tr>
<td><strong>M</strong></td>
<td><strong>O</strong></td>
</tr>
<tr>
<td>Manufacturer makes data that is relevant for the customer available/accessible online with the aid of identification, e.g. PDF via http(s).</td>
<td>Description of the device interface available digitally.</td>
</tr>
<tr>
<td>Product addressable online via TCP/UDP&amp;IP with at least the information model from OPC-UA.</td>
<td>Information such as statuses, error messages, warnings, etc. available via OPC-UA information model in accordance with an industry standard</td>
</tr>
</tbody>
</table>

**Every I4.0 Implementation Level Officially Requires OPC UA**
Robotics Uses OPC UA to Implement Industrie 4.0
Specific Models
- Use case specific models
- Industry specific models
- Device / machine specific models

Companion Information Models
- PLCopen, ADI, FDI, FDT, BACnet, MDIS, ISA95, AutomationML, MTConnect, AutoID, VDW, EUROMAP, Robotics, Vision Systems, IEC 61850/61400, Sercos, Powerlink, PROFINet, ...

Developed with partner organizations

OPC Foundation Responsibility
OPC UA = IEC 62541
OPC Foundation strategy:
- Rules for OPC UA CS developed together with partners
- Predefined process for joint OPC UA CS
- Templates to ensure standardized format and potential certifications
- Compliance
- Intellectual Property
- Working Processes

Markets: https://opc.foundation.org/markets-collaboration/
- Automation
- Building Automation
- Energy
- Engineering
- Measurement
- Oil & Gas
- Transportation
VDMA represents the breadth of the manufacturing industry

VDMA has more than 3200 member companies

- Agricultural Machinery
- Air Conditioning and Ventilation
- Air Pollution Control
- Air-handling Technology
- Building Control and Management
- Cleaning Systems
- Compressors, Compressed Air and Vacuum Technology
- Construction Equipment and Building Material Machines
- Drying Technology
- Electrical Automation
- Electronics, Micro and Nano Technologies
- Engine Systems for Power and Heat Generation
- Engines and Systems

- Fire Fighting Equipment
- Fluid Power
- Food Processing Machinery and Packaging Machinery
- Foundry Machinery
- Gas Welding
- Hydro Power
- Integrated Assembly Solutions
- Large Industrial Plant Manufacturing
- Lifts and Escalators
- Machine Tools and Manufacturing Systems
- Machine Vision
- Materials Handling and Intralogistics
- Measuring and Testing Technology

- Metallurgical Plants and Rolling Mills
- Metallurgy
- Micro Technologies
- Mining
- Plastics and Rubber Machinery
- Power Systems
- Power Transmission Engineering
- Precision Tools
- Printing and Paper Technology
- Process Plant and Equipment
- Productronic
- Pumps + Systems
- Refrigeration and Heat Pump Technology
- Robotics

- Robotic + Automation
- Security Systems
- Software and Digitization
- Surface Treatment Technology
- Textile Care, Fabric and Leather Technology
- Textile Machinery
- Thermal Turbines and Power Plants
- Thermo Process Technology
- Valves
- Waste Treatment and Recycling
- Wind Energy
- Woodworking Machinery

OPC UA CS Release (Candidate)
OPC UA CS under development
Awareness existent
Growing into new markets

- 2016: Commercial product OPC UA in chip
- 2018: OPC UA in Microsoft IoT chip
  Azure Sphere: IoT chip for secured connection
- 2018: Industrial kitchen equipment
  HKI association modelled 13 devices
**OPC Technology: History and Future**

**Clouds**
- SCADA, MES, ERP,

**IT Network**
- OPC Classic: OLE for Process Control
- OPC UA: Technology and OS independent

**HMIs**
- OPC Client
- OPC Server
- OPC UA Client
- OPC UA Server
- "SOA PLC"

**Machine Control**
- PLC
- OPC UA Server
- "SOA PLC"

**Field Level**
- OPC Server
- OPC UA Server
- Pub/Sub

**Edge/Cloud**
- Pub/Sub Controller to Controller
- Pub/Sub

**Today**
- OPC UA

**Industrial mobile apps**
- OPC UA - over TSN
- OPC UA - over 5G

**Time**
OPC UA: Security analyzed by BSI

Who: Federal Office for Information Security (German Government BSI)
Why: Because of relevance of OPC UA for German Industry
  - Analysis of specification
  - Analysis of Reference Implementation
Result: Available on BSI web
Commented version on OPC web www.opcfoundation.org/security

See also video from BSI „Results Security Analysis“
OPC Youtube Channel
Communication Reliability

- OPC UA recovers from communication loss

- OPC UA ensures robust and reliable communication
  - Keep-alive monitoring
  - Buffering of data and acknowledgements
  - Fast recovery in case of communication errors
  - Redundancy concepts
Vertical Integration

Enterprise Network
- UA Client
- UA Server

Operations Network
- UA Client
- UA Server

Plant Floor Network
- UA Client
- UA Server

- UNIX, Linux, ...
- Linux, VxWorks, QNX, ...

Device data
- Firewall
- ERP
- MES
- Configuration
Microsoft commitment to OPC UA

Dedicated engineering team focused on adding OPC UA support to Microsoft products located in Munich, directly reporting to Azure IoT directors in Redmond.

Download flyer here
Brownfield integration: Gateways!

Before USB
DIN Keyboard / Centronics printer / PS2 mouse

Transition
Use adopters to connect old and new world

With USB

Benefit:
Consistent, compatible data model for all machines, plus security!

Market of gateways
- <$500
- Connect to PLCs or fieldbus systems
- No changes to machines required!
Data Security

Key Concepts
Trustworthiness: Key System Characteristics

IT World

OT World

IIoT World (Industrie4.0)

Safety | Security | Resilience | Reliability | Privacy
Data Security

Data at Rest

Data in Process

Data in Motion
Key Security Concepts

- **Trusted Information (CIA triad)**
  - Confidentiality
  - Integrity
  - Availability

- **Access Control (AAA principle)**
  - Authentication
  - Authorization
  - Accounting (Auditability)
Key Security Concepts

- Confidentiality
  → Protecting privacy of message contents

- OPC UA Information and Functionality
  Prevented by confidentiality controls

- Changed Value: Variable Y Value 0
Key Security Concepts

- **Integrity**
  - Not manipulating the content of a message

![Diagram showing OPC UA Information and Functionality with integrity controls preventing unauthorized changes.](image-url)
Key Security Concepts

- **Availability**
  - Resilient to DoS threats, maximizing availability
Key Security Concepts

- Application: Authentication and Authorization

- Software Certificate

- Application Instance Certificates

- OPC UA Information and Functionality (e.g. read, write)
Key Security Concepts

- **User**: Authentication and Authorization

1. **Authenticate User** (e.g. username and password)
2. **Authorize for specific operations and information** (e.g. writing a specific value)

OPC UA Information and Functionality (e.g. read, write)
Key Security Concepts

- **Auditability**
  - Tracking important interactions

OPC UA Defines Audit Parameters and to be included in audit records.
Layered conceptual communication model

OPC UA Client

Application Layer

Communication Layer

Transport Layer

Software Authentication
User Authentication
User Authorization
Execute UA Functions

OPC UA Server

Application Layer

Communication Layer

Transport Layer

App Authentication
Encryption, Signing
Protect message

UA TCP, HTTPS
Binary, XML
Encoding/Decoding

Allow to choose appropriate abilities to meet various requirements

- Level 3 Apps: Internet accessibility and Security (e.g. HTTP & XML, E & S)
- Level 2 Apps: High speed and Security (e.g. UA TCP & BIN, S)
- Level 1 Apps: High speed and Small-footprint (e.g. UA TCP & BIN)
Communication Layer Security

- **Confidentiality** → Encrypting of Messages

- **Integrity** → Signing of Messages

- **Availability** → Minimal message processing before authentication

Examples:
- Restricting message size
- No security related error codes returned
Communication & Application Layer Security

- Authentication of applications
  - Application instance certificates
  - Certificate Authority (CA)

- Authentication of users
  - Username / password, WS-Security Token or X.509 certificates,
  - Fits into existing infrastructures like Active Directory

- Authorization (Server Specific)
  - Fine-granular information in address space (Read, Write, Browse)
  - Writing of meta data, calling methods

- Auditability
  - Generating audit events for security related operations
Thank you!

Thomas Burke
President
OPC Foundation
Thomas.Burke@opcfoundation.org