Forging Trustworthy IIoT Systems Using OPC UA

Thomas Burke

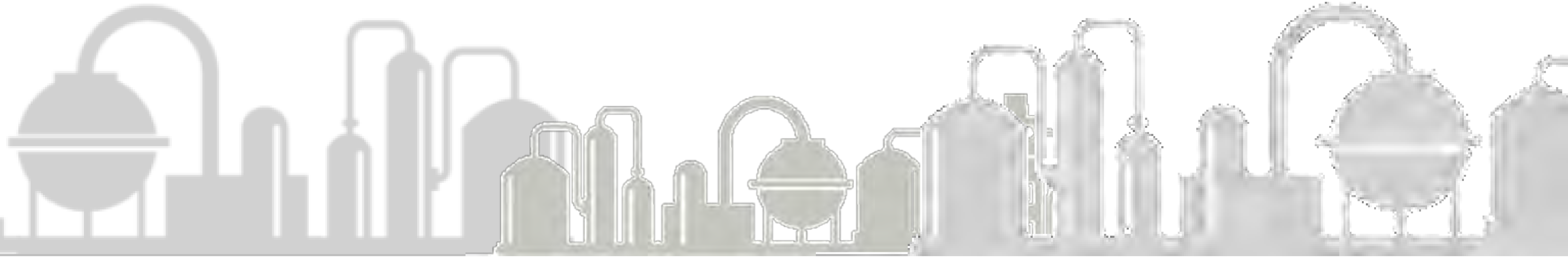
President, OPC Foundation

Darek Kominek

Marketing Manager, Matrikon (Honeywell)

OPC Foundation Mission Statement

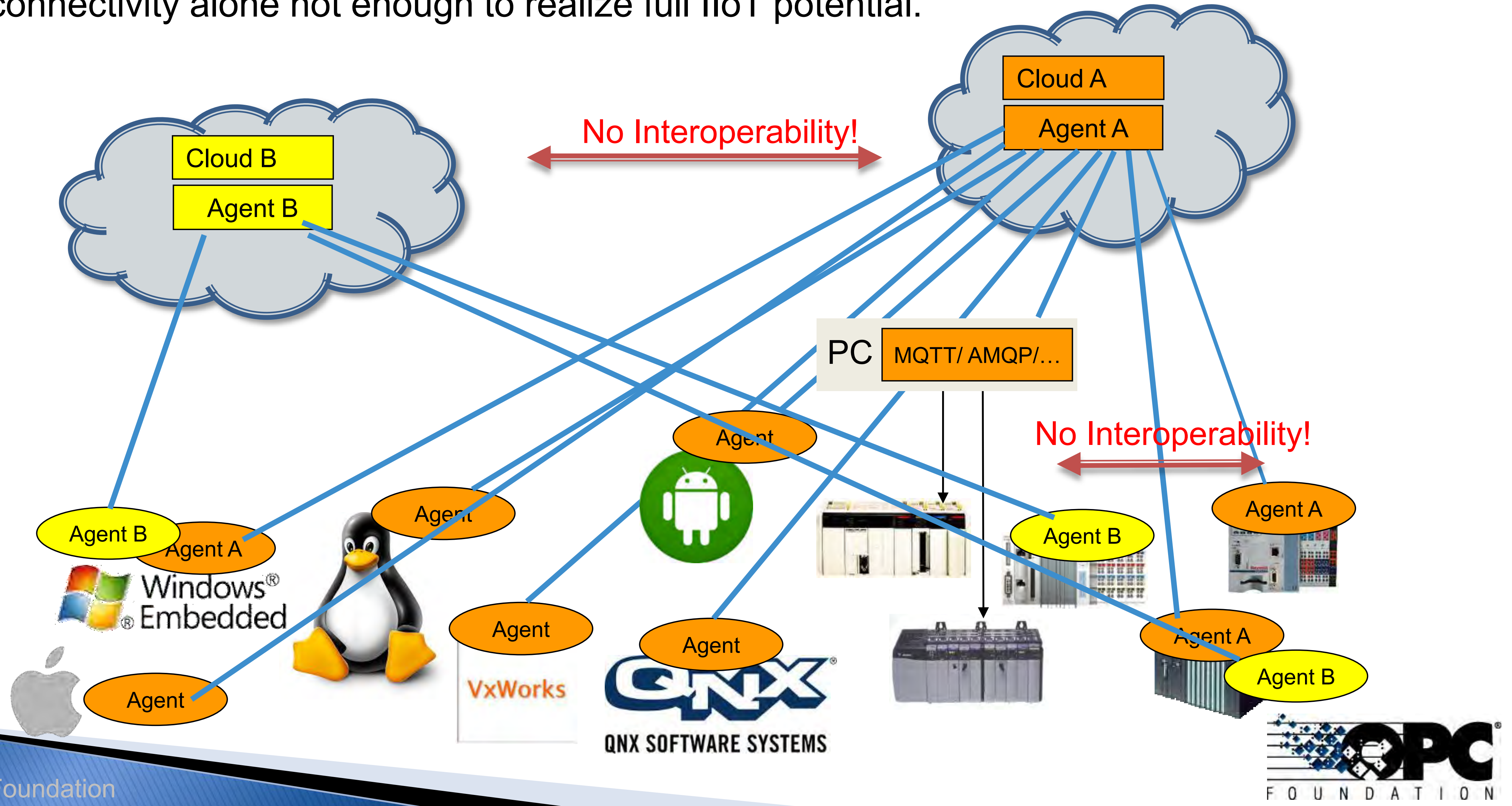
The mission of the OPC Foundation is to manage a global organization in which users, vendors and consortia collaborate to create data transfer standards for multi-vendor, multi-platform, secure and reliable interoperability in industrial automation.



© 2018 OPC Foundation

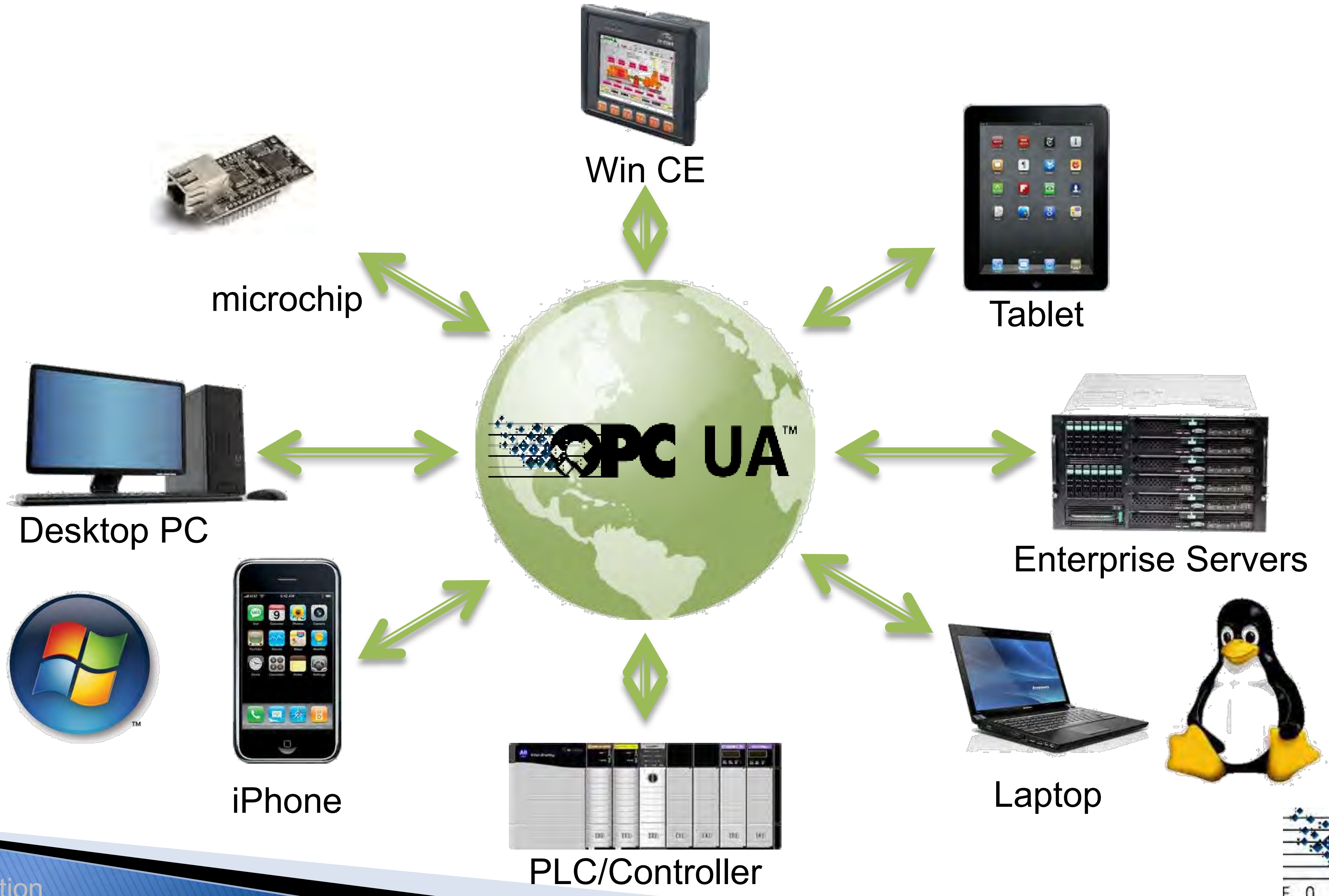
Connectivity without Interoperability

Data connectivity alone not enough to realize full IIoT potential.



© 2018 OPC Foundation

OPC Vision: Facilitating Industrial Interoperability

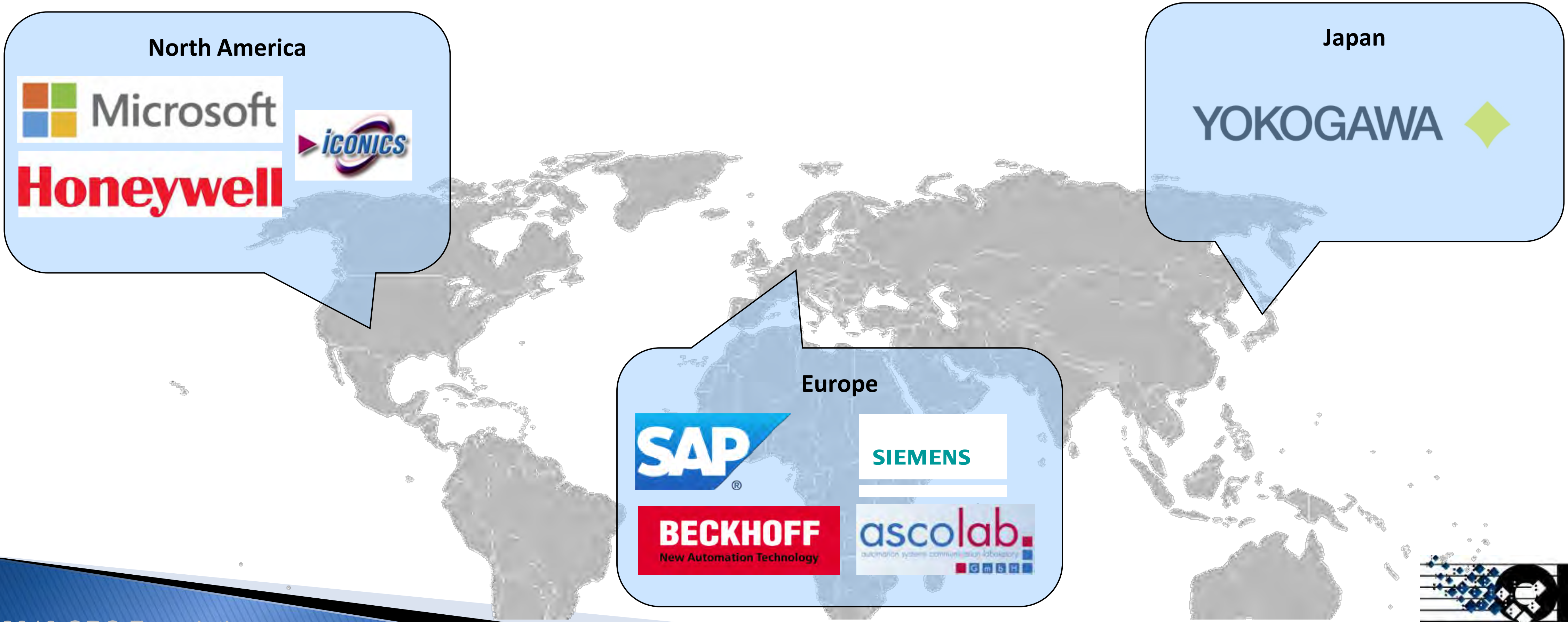


© 2018 OPC Foundation

OPC UA

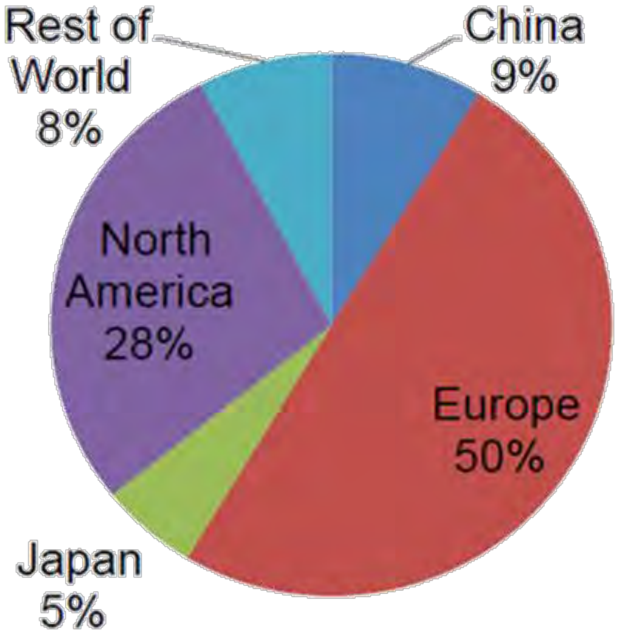
OPC Foundation: Board of Directors

- International board – democratic elections by members every year
  - Companies from Automation & IT
  - All over the world

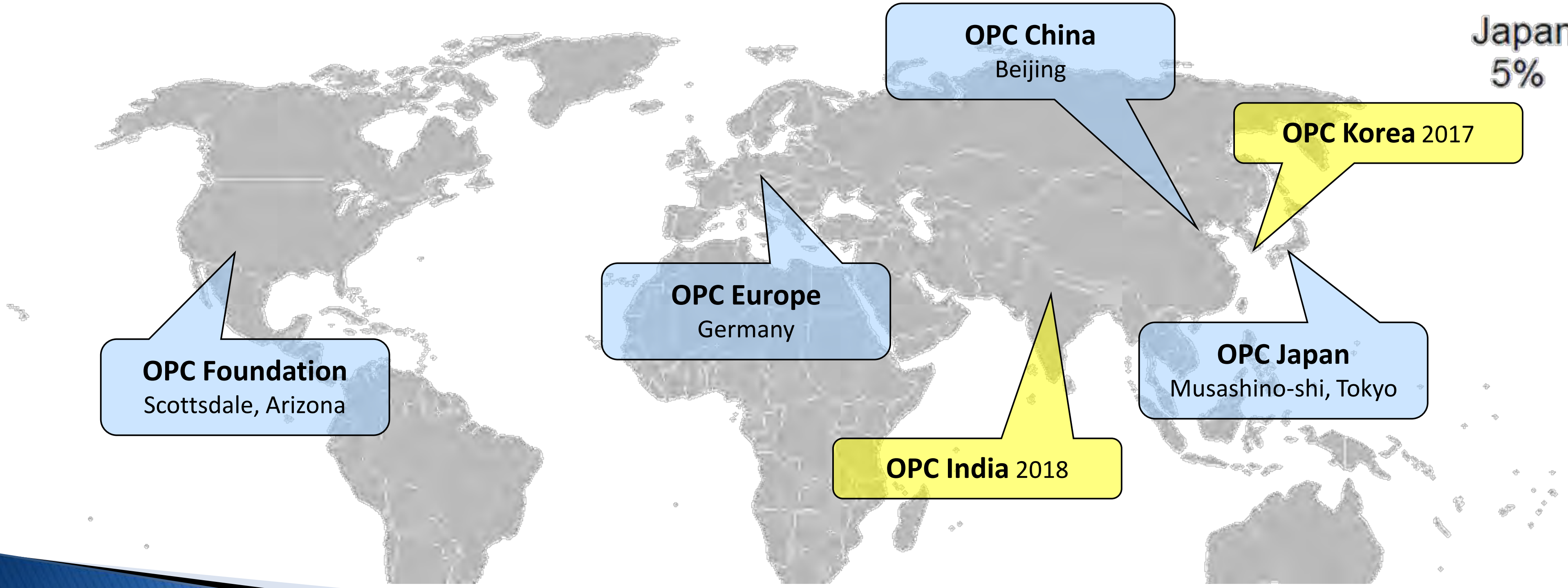


© 2018 OPC Foundation

OPC Foundation: Membership



- An International Organization
  - Companies from Automation & IT
  - International standard IEC62541



OPC China Beijing

OPC Korea 2017

OPC Europe Germany

OPC Foundation Scottsdale, Arizona

OPC Japan Musashino-shi, Tokyo

OPC India 2018

© 2018 OPC Foundation

OPC Foundation: Class A members

ABB ALSTOM aspentech azbil BAKER HUGHES BECKHOFF Rexroth Bosch Group

B&R Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING CISCO SYSTEMS DASSAULT SYSTEMES EATON Powering Business Worldwide EMERSON. Process Management FANUC

FESTO Fuji Electric GE HITACHI Inspire the Next Honeywell IBM

JTEKT KONGSBERG KUKA Lenze Leuze electronic the sensor people LG CNS

MHPS GROUP METAWATER METTLER TOLEDO Microsoft MITSUBISHI ELECTRIC Changes for the Better

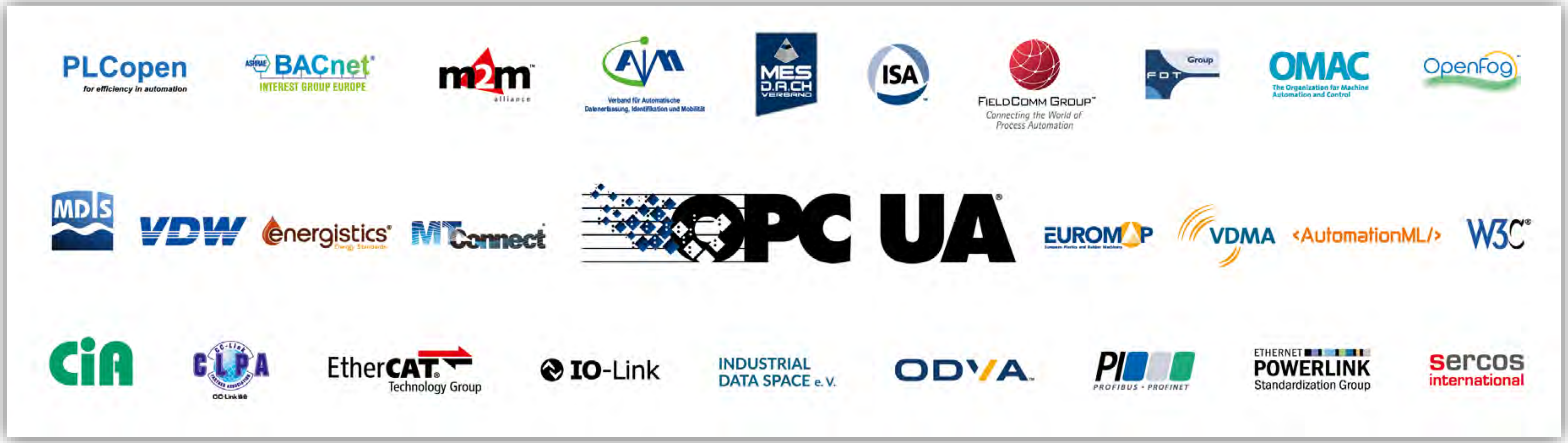
NATIONAL INSTRUMENTS™ OMRON OSIsoft. PHOENIX CONTACT RENESAS

Rockwell Automation SAP® Schlumberger Schneider Electric SEW EURODRIVE

SICK Sensor Intelligence. SIEMENS Solar Turbines A Caterpillar Company splunk> TOSHIBA Leading Innovation

Hewlett Packard Enterprise Valmet WAGO® YOKOGAWA OPC® FOUNDATION

OPC UA: Enabling Standards Body Collaboration



Oil & Gas	Building Automation
Utilities	Manufacturing
Pharmaceutical	Mining

© 2018 OPC Foundation

industrial internet® CONSORTIUM

Plattform INDUSTRIE 4.0

Made in China 2025

Internet +

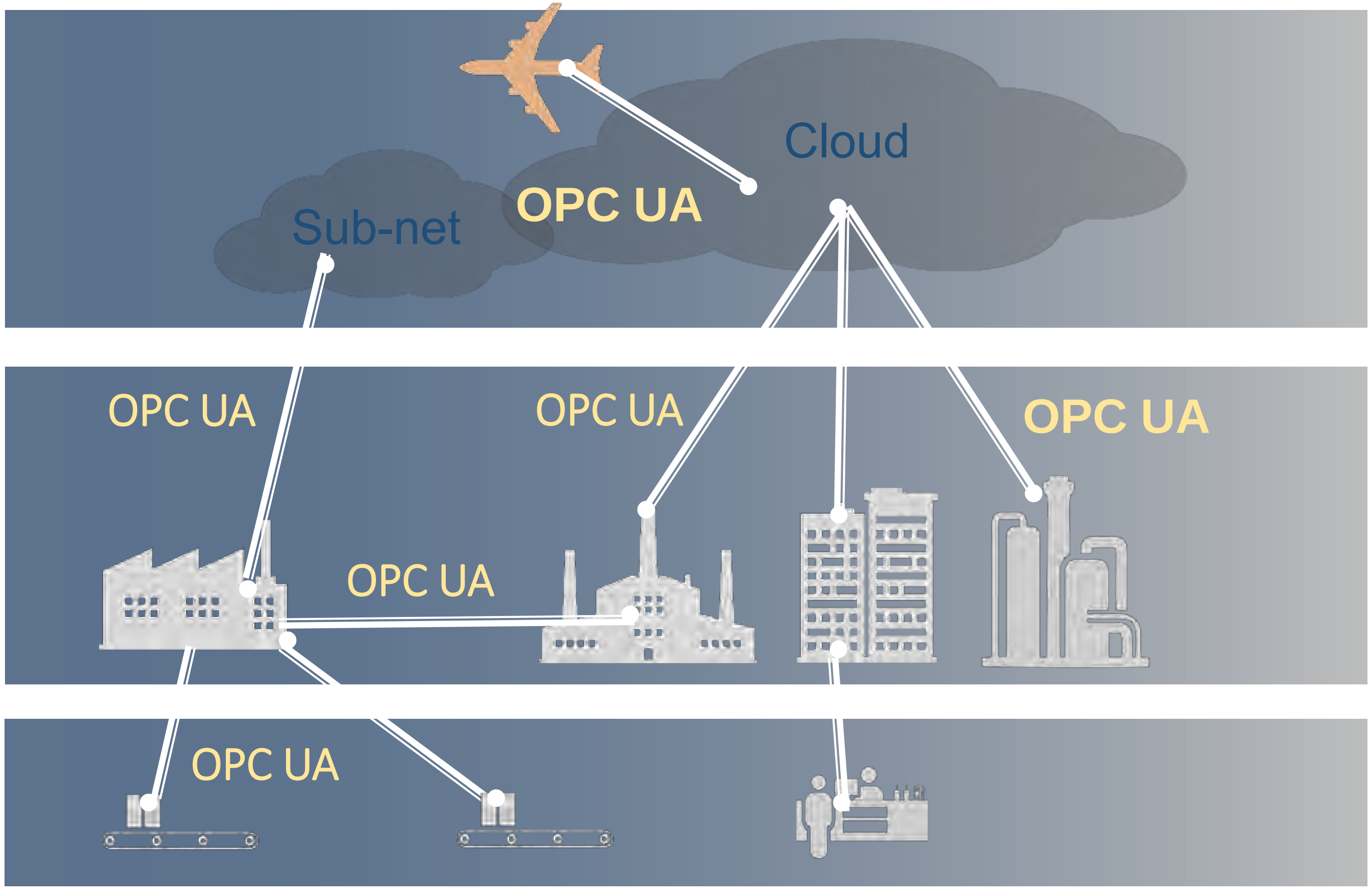
> “The only communication technology for industrial environments that I currently know of which provides integrated security functionality and also offers performance potential to tackle the challenges of Industrie4.0 is OPC UA.”

Holger Junker
Head of Cyber-Security in Critical IT-Systems
German Office for Information

Bundesamt
für Sicherheit in der
Informationstechnik

OPC UA In The IIoT Context

OPC UA – Paving the way for the IIoT



© 2018 OPC Foundation

IIoT & I4.0

- IIoT systems affect all aspects of a business so must be considered from multiple viewpoints (example from IIRA):

Business	• Business Value & ROI • Cost of Maintenance
Usage	• New device registration in plant and cloud system • How information is accessed, users added
Functional	• Component Interoperability in and across five functional domains: • **Control, Operations, Information, Applications, and Business**
Implementation	• Architecture, component distribution, topology • interfaces, protocols, behaviors, etc.

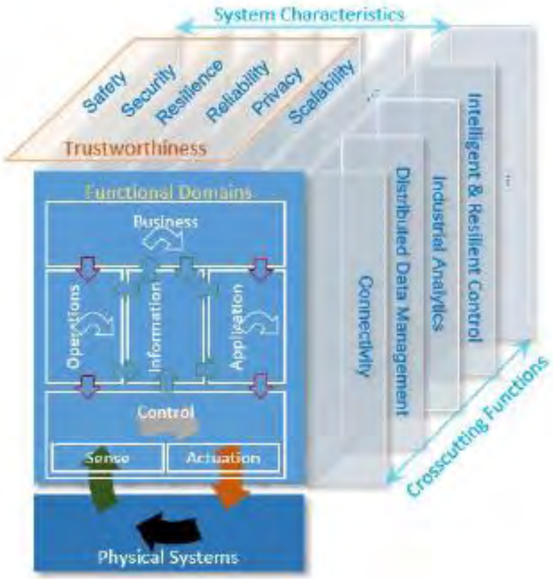
- Few standards meet the core connectivity standard criteria set out in IIRA
  - **OPC UA is a core connectivity standard (IIRA)**
  - **OPC UA is the main connectivity standard for I4.0 (RAMI)**

© 2018 OPC Foundation

Next Gen Infrastructure: IIRA & RAMI

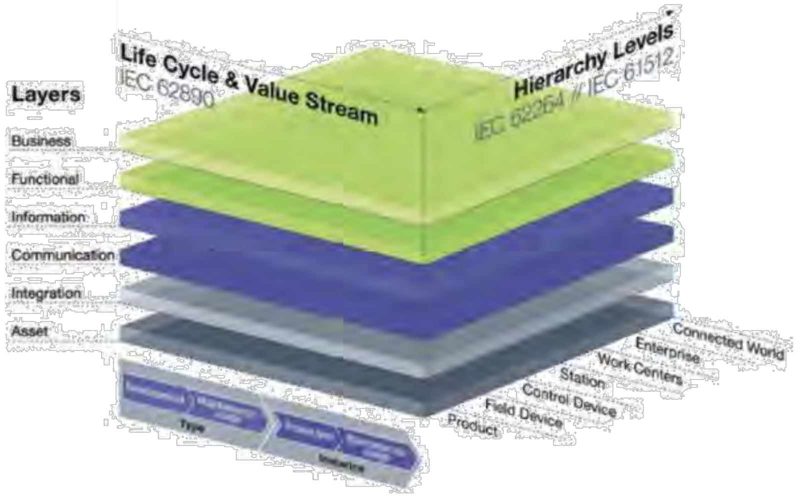
- **Frameworks** offer a structured, systematic way to discuss and evaluate solutions for IT and OT convergence.

Industrial Internet Reference Architecture (IIRA)



PLATTFORM INDUSTRIE4.0

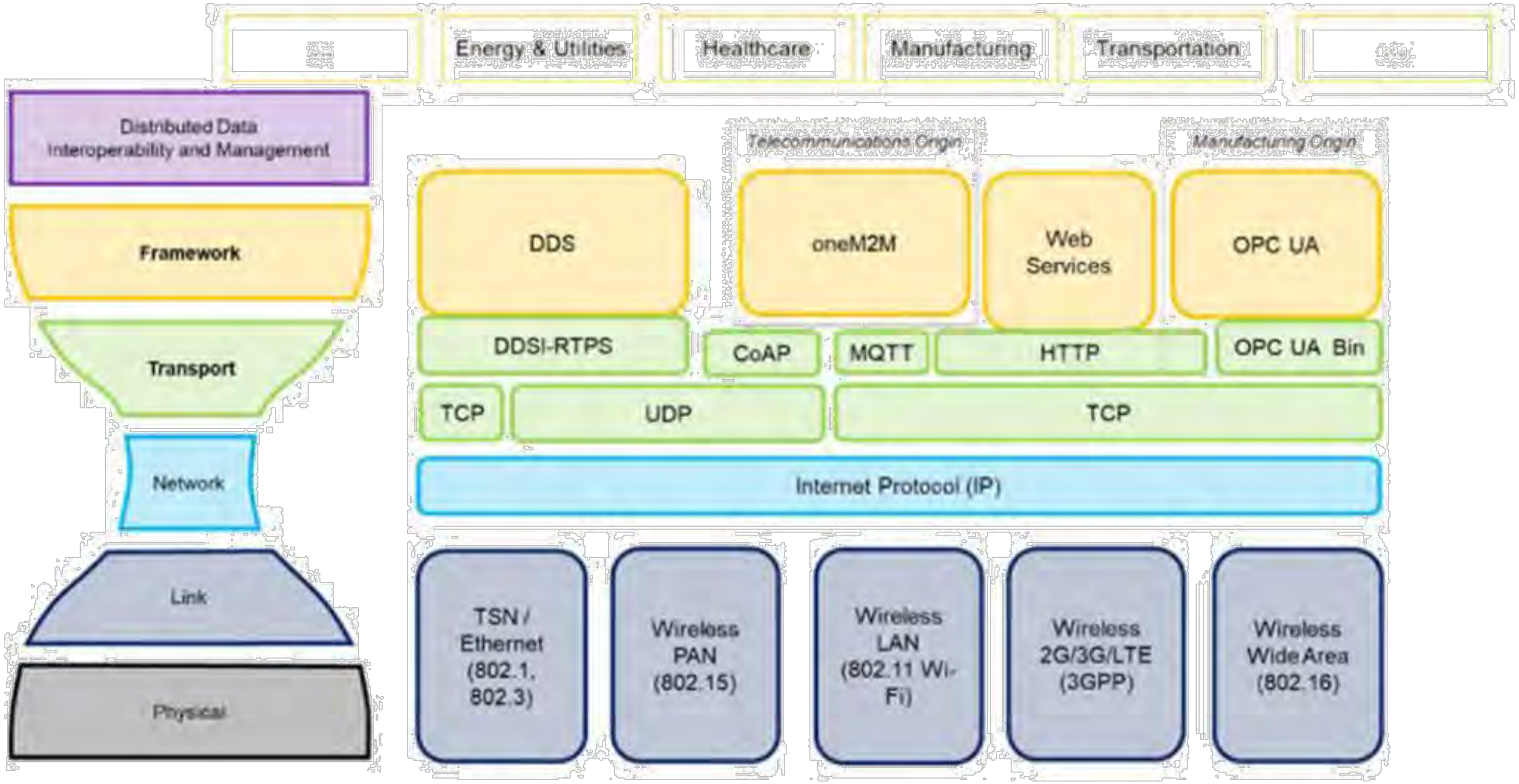
Reference Architecture Model Industrie 4.0 (RAMI)



- Seamless, reliable, and cost effective system interoperability is crucial to IIoT

© 2018 OPC Foundation

OPC UA: A Core IIRA Connectivity Standard

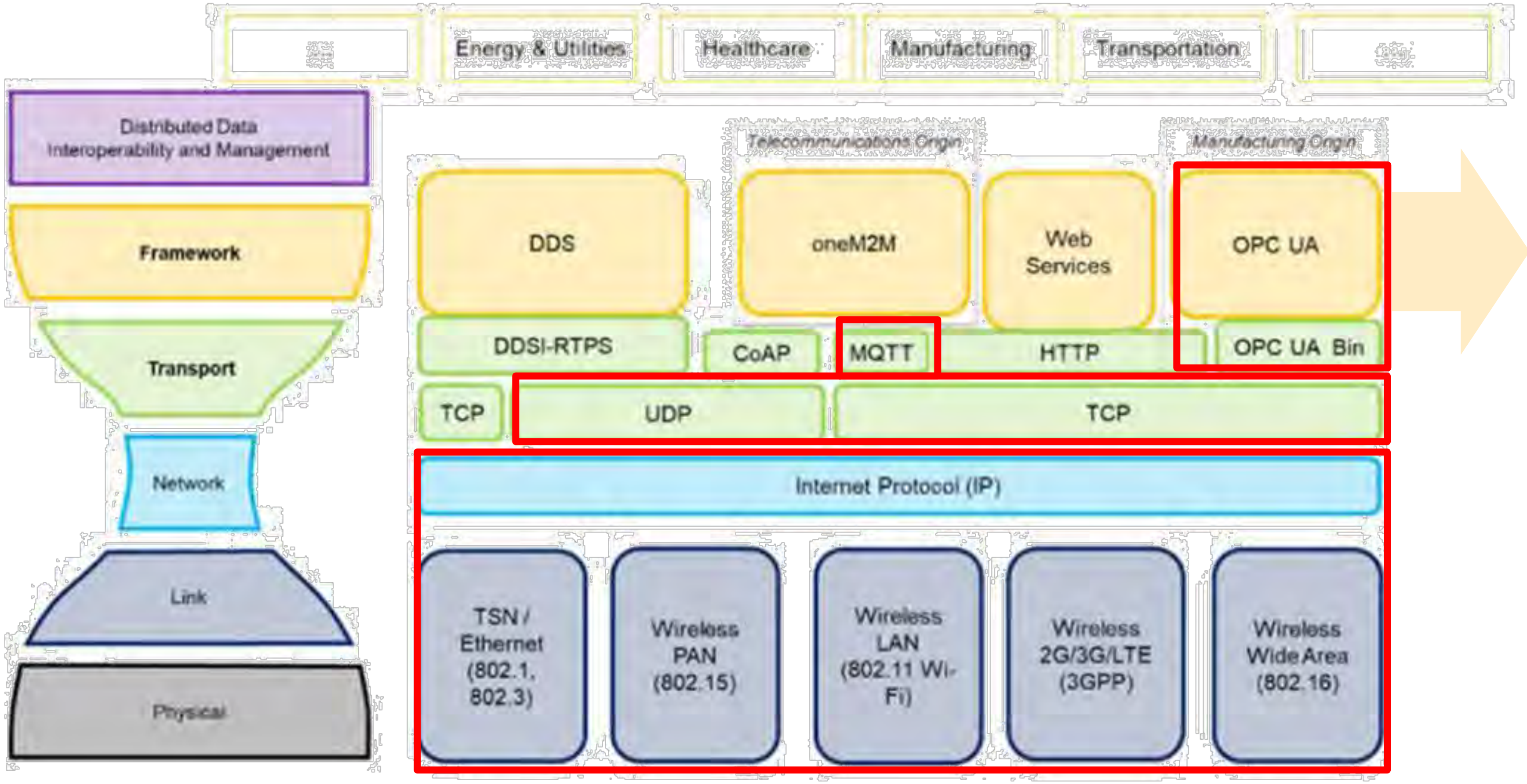


Source: Industrial Internet Consortium (www.iiconsortium.com)

© 2018 OPC Foundation

OPC UA Meets The Requirements

- Number of Core Data Standards kept as small as possible to minimize complexity



Source: Industrial Internet Consortium (www.iiconsortium.com)

CRITERIA EXAMPLES:

✓ Syntactic Interoperability
✓ Secure
✓ Performant
✓ Scalable
✓ Reliable
✓ Resilient
✓ Open Standard
✓ International Adoption
✓ Vendor Agnostic
✓ SDKs Available
(Open Source + Commercial)

© 2018 OPC Foundation

Data Security

Key Concepts

With Connectivity Comes the Need for Security

- Industrial Control System (ICS) Cyber attacks are accelerating

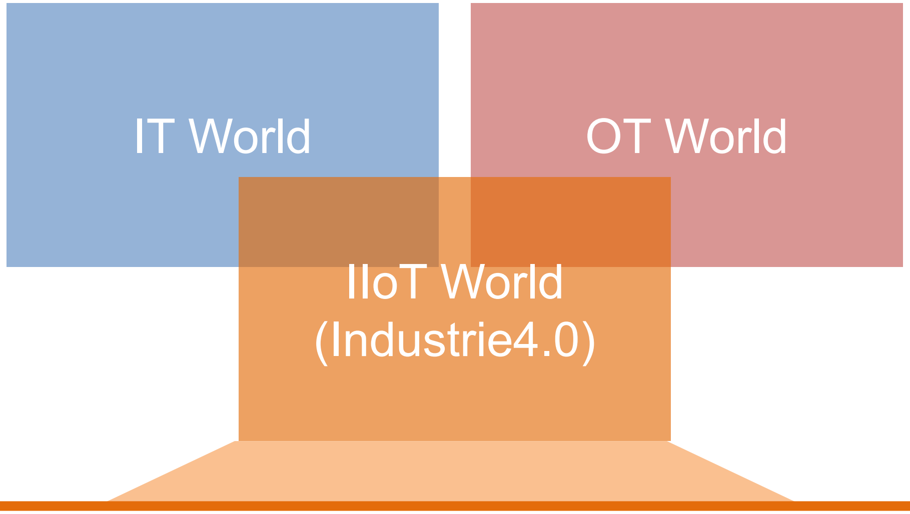
Stuxnet - Iran, 2010

Crash Override - Ukraine, 2016

Reuters

© 2018 OPC Foundation

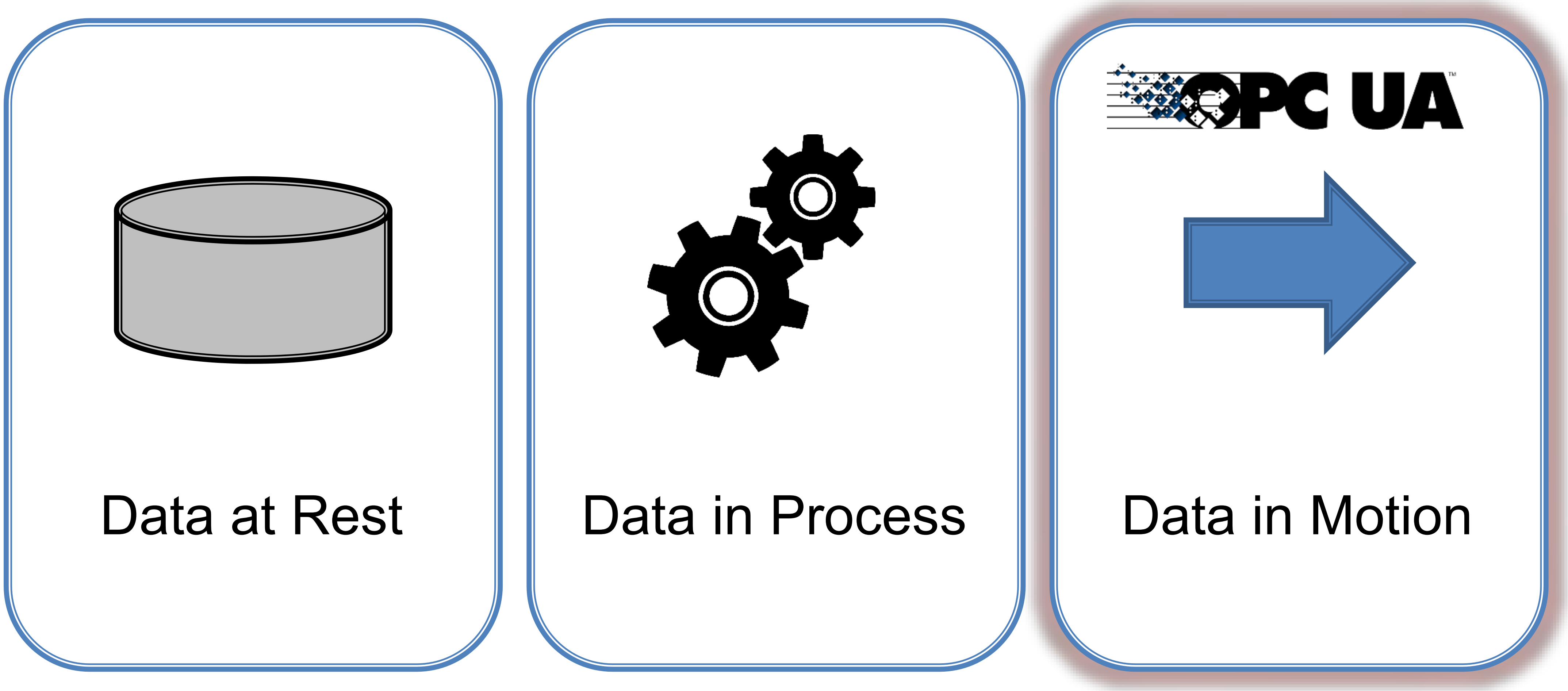
Trustworthiness: Key System Characteristics



Safety | **Security** | Resilience | Reliability | Privacy

© 2018 OPC Foundation

Data Security



Data at Rest

Data in Process

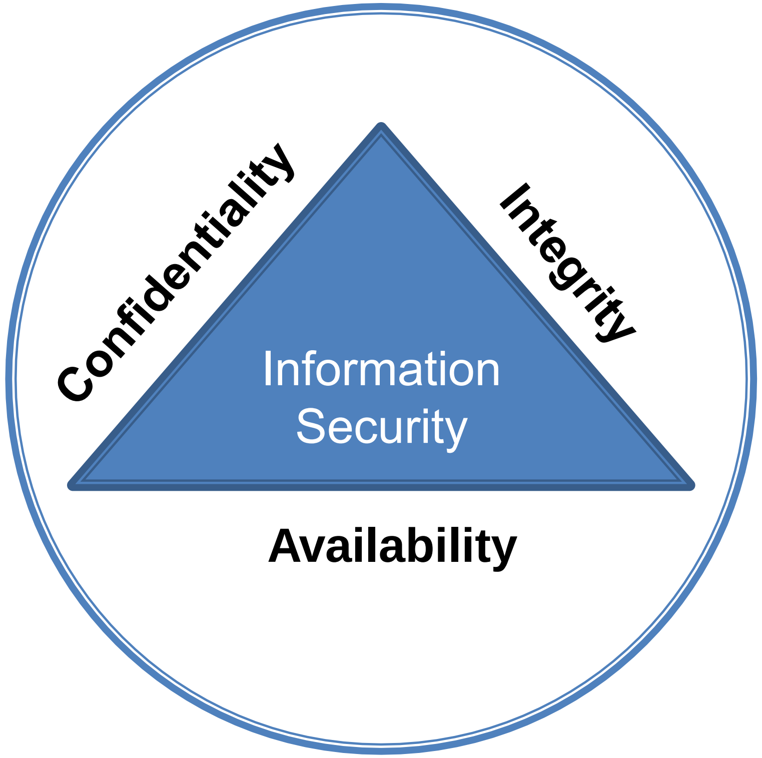
Data in Motion

© 2018 OPC Foundation

Key Security Concepts

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

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



© 2018 OPC Foundation

OPC UA

Secure by Design

OPC UA: Secure By Design

1) Concepts
2) **Security Model**
3) Address Space Model
4) **Services**
5) Information Model
6) **Mappings**
7) **Profiles**
8) Data Access
9) Alarms and Conditions
10) Programs
11) Historical Access
12) **Discovery**
13) Aggregates
14) PubSub

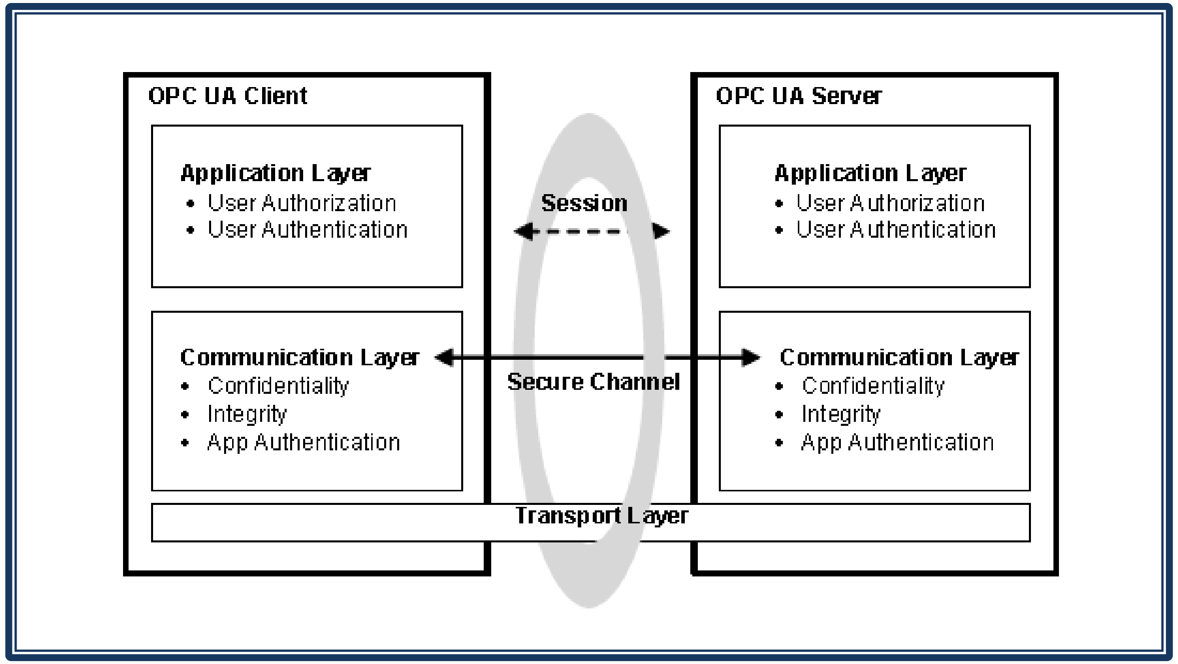
Red: directly relevant for IT security

© 2018 OPC Foundation

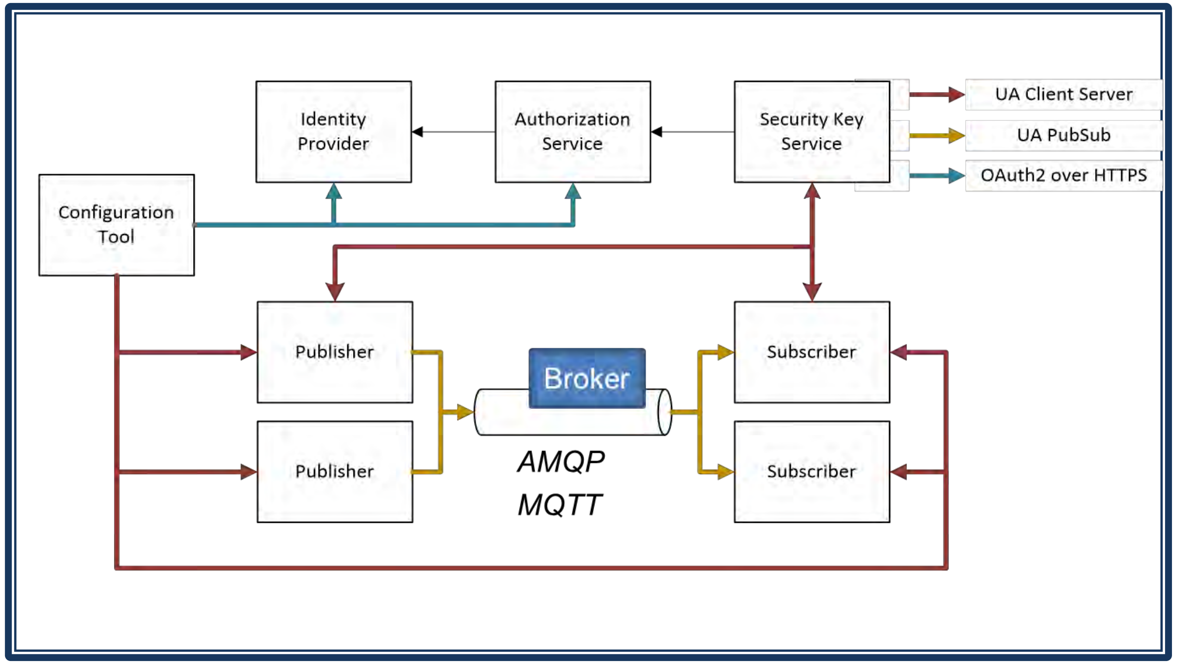
Solid Security Foundation

- OPC UA addresses the core security aspects:

Client-Server Architecture



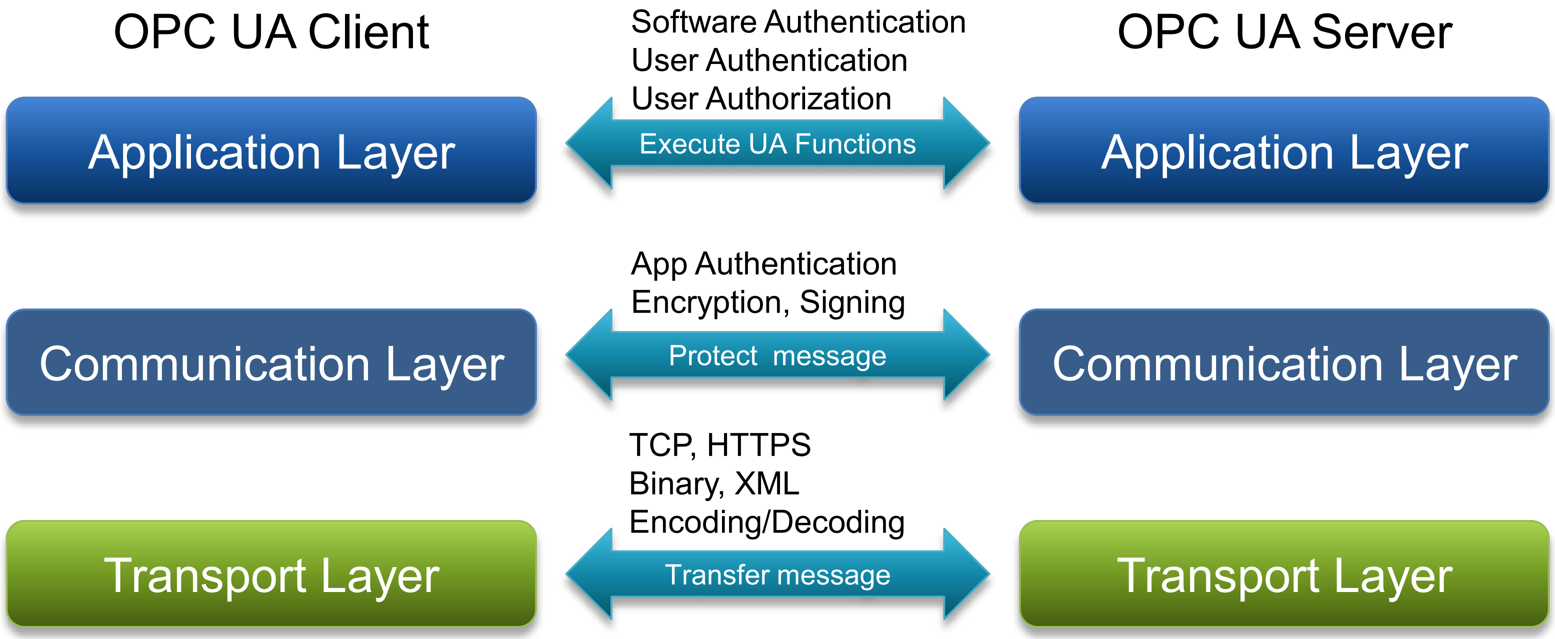
Publish-Subscribe Architecture



© 2018 OPC Foundation

Layered Communications

- Layered conceptual communication model



OPC UA Client

OPC UA Server

Software Authentication
User Authentication
User Authorization

Application Layer ↔ Execute UA Functions ↔ Application Layer

App Authentication
Encryption, Signing

Communication Layer ↔ Protect message ↔ Communication Layer

TCP, HTTPS
Binary, XML
Encoding/Decoding

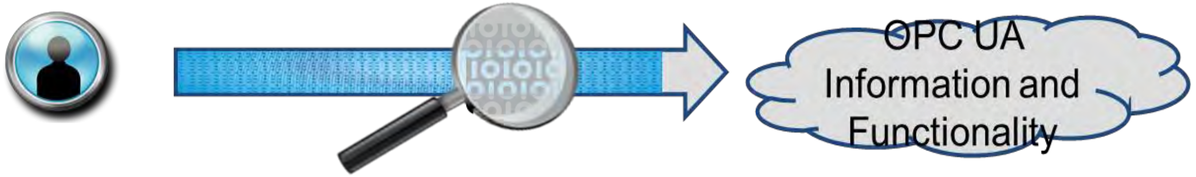
Transport Layer ↔ Transfer message ↔ Transport Layer

- 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)

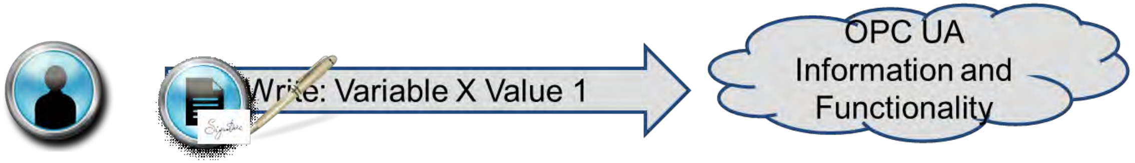
© 2018 OPC Foundation

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

© 2018 OPC Foundation

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

© 2018 OPC Foundation

OPC UA Security

Assessment & Evolution

Examples of Attack Types Addressed

- **Message Flooding**
  - Minimize processing of packets before they are authenticated
- **Eavesdropping** – record and capture packets
  - Encryption
- **Message Spoofing** – attacker forges messages from client/server
  - Message signing, valid Session ID, Channel ID, timestamp, …
- **Message Alteration & Replay** – messages captured, modified, resent
  - Session IDs, *Secure Channel* ID, Timestamps, Sequence# and Request IDs
- **Malformed Messages**
  - Validating message structure and valid parameter values or discard
- **Server Profiling, Session Hijacking**, etc…

© 2018 OPC Foundation

Threats according to OPC UA Part 2

	Authentication	Authorization	Confidentiality	Integrity	Auditability	Availability
Message Flooding						X
Eavesdropping			X			
Message Spoofing		X		X		
Message Alteration		X		X		
Message Replay		X				
Malformed Messages				X		
Server Profiling	X	X	X	X	X	X
Session Hijacking	X	X	X			
Rogue Server	X	X	X		X	X
Compromising User Credentials		X	X			

Threats and Impact on Security Objectives

© 2018 OPC Foundation

Effectiveness of OPC UA Measures

Bundesamt für Sicherheit in der Informationstechnik

OPC UA Security Analysis

02/03/2017

security-Mode	Layer or Service	Denial of Service	Eavesdropping	Message Spoofing	Message Alteration	Message Replay	Malformed Messages	Server Profiling	Session Hijacking	Rogue Server	Compromising User credentials	Repudiation
None		🟨	🟥	🟥	🟥	🟩	🟧	🟧	🟩	🟧	🟩	🟨
Sign		🟨	🟥	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟩
SignAndEncrypt		🟨	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟩

🟥 : no protection

🟧 : low protection

🟨 : Protection which restricts the possibilities of an attacker, but does not prevent this type of attack

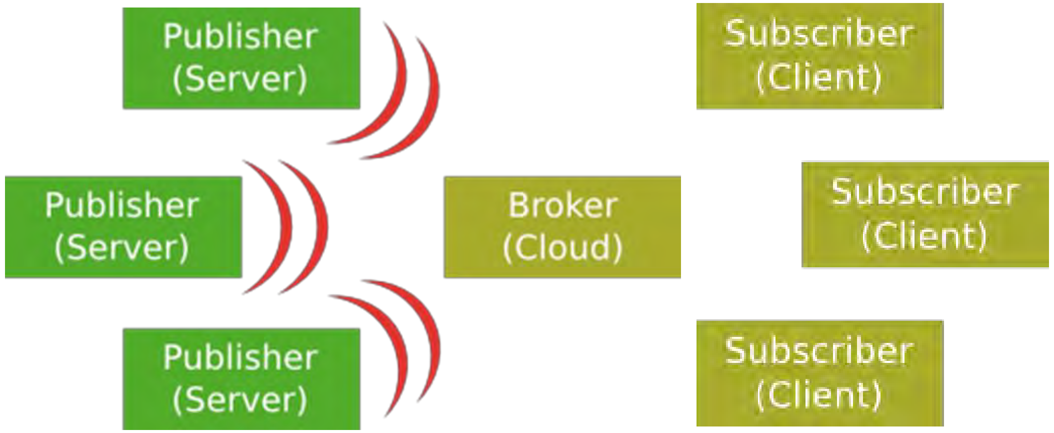
🟩 : effective protection (attacks of this type require cryptographic attacks)

Source: BSI, "OPCUA Security Analysis" (02/03/2017)

© 2018 OPC Foundation

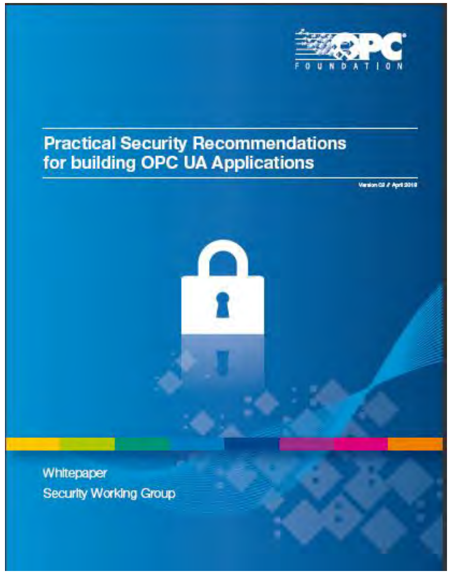
New Security related features in 1.04

- PubSub
  - JSON Web Token (JWT)
- Roles & Claim Based security
- Security Management
- Session-less Service calls



© 2018 OPC Foundation

Conclusion



Practical Security Recommendations for building OPC UA Applications

Version 02 / April 2018

Whitepaper

Security Working Group

OPC UA is secure-by-design:

- Implements CIA
  - **Confidentiality** and **Integrity** by signing and encrypting messages
  - **Availability** by minimum processing before authentication
- Implements AAA
  - **Authentication** and **Authorization** of Users and Application instances
  - **Auditability** by defined audit events for OPC UA operations
- Facilitates use of different levels of security to match application/hardware
- OPC UA continually evolving to meet new threats and capabilities

Use of OPC UA security enhances overall system security (defense in depth)

© 2018 OPC Foundation

Thank You.

Thomas Burke
thomas.burke@opcfoundation.org
OPC Foundation

Darek Kominek, P.Eng. (Alberta, Canada)
darek.Kominek@matrikonopc.com
Matrikon®

© 2018 OPC Foundation